International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

To mitigate black hole attack by using trusted AODV with MBH-modified AODV methodology for MANET

Prof. Dr. M. Narayana (ph.d), P.Ravinder Kumar, Nousheen Begum
[1]Head of the Department (ECE) JayaPrakash Narayana College of engg Mahabubnagar,Telangana,India
[2]Associate Professor JPNCE Mahabubnagar,Telangana,India
[3]M.Tech Scholar JayaPrakash Narayana College of engg Mahabubnagar,Telangana,India

Abstract:

A mobile ad-hoc network (MANET) is a wireless network such that nodes are move dynamically in network. In network layer so many attacks but introduce only collaborative black hole attack a group of black hole node easily employed against routing in mobile ad-hock networks called collaborative black hole attack. We introduce trusted AODV routing protocol which trust value calculate using tangent hyperbolic function. But here based on trust calculation some delay time should be high at some level of transmission time. So we propose a intelligent source based detection mechanism here to detect the multiple black hole nodes. The results show performance improvement ascompared to Trusted AODV protocol.

Keywords: MANET, AODV, Collaborative Black hole attack, trusted AODV, NS2.

1.Introduction:

A mobile ad-hoc network (MANET) is wireless and centralized network that means it's not recurred infrastructure. In MANET nodes behave dynamically nature. The dynamic natures of MANET make it more vulnerable[1]. In MANET so many attacks like black hole, collaborative black hole attacks. Black hole attack is a malicious node which absorbs all data packets in itself similar to a hole. This sucks in everything. In this way, all useful packets in the network are dropped. When a group of black hole node easily employed against routing in mobile ad-hoc networks. These types of attacks are called collaborative black hole attack[2]. Due to high mobility of node routing is big challenge in ad-hoc network.

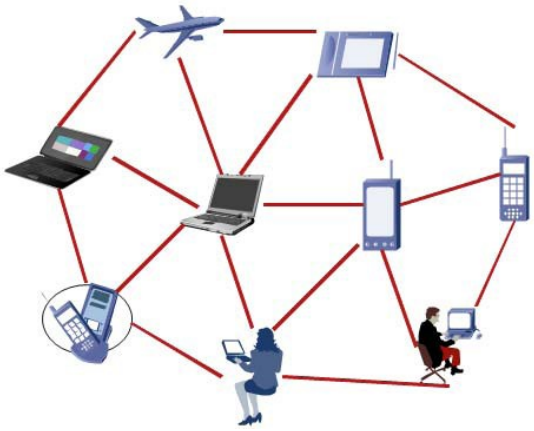

Fig1: Mobile ad hoc network architecture

1.1 AODV routing protocol working:

The routing protocol play main role in identifying and packet transmit from source node to destination node, through intermediate

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

nodes. Ad-hoc on demand distance vector routing (AODV) is a reactive routing protocol. AODV is provide a dynamic network connection and less processing, loads. AODV protocol is used sequence number to distinguish. Routing messages are fresh routing messages which broad cast in the network can be dividing into path discovery and path.

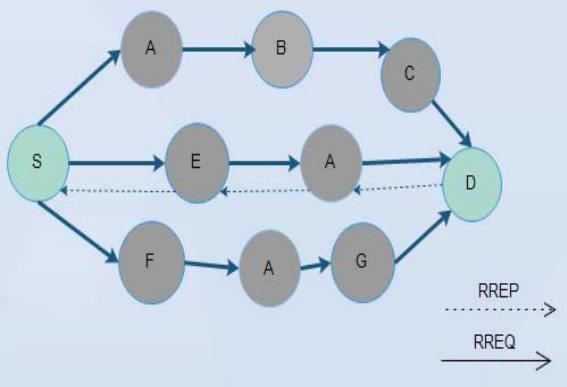

Fig2: working of AODV

1.2 Collaborative black hole attack:

Collaborative black hole attack a group of black hole node easily employed against routing in mobile ad-hoc networks.

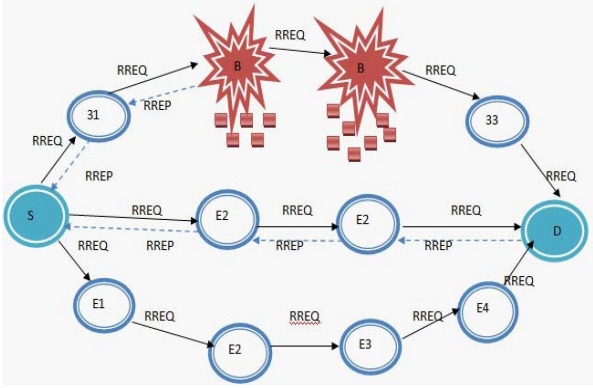

Fig3: collaborative black hole attack

1.3 Trusted AODV routing protocol:

Trusted hyperbolic AODV is a trusted routing protocol based on trust model for mobile ad-hoc network. Trusted hyperbolic AODV has many relevant features like nodes perform trusted routing behaviors mainly according to the trust relationships among them. A node that performs malicious behaviors will finally be detected and denied to the entire network[5].

a) Trust category of a node:

In this, AODV routing protocol is embedded along with the trust function. The communication between the nodes in the mobile ad-hoc network depends on the cooperation and the trust level with its neighbors. Based on the trust on neighbor and appropriate threshold values the nodes can be categorized in to the following.

1. **Unreliable:** The unreliable is the non trusted node. Means an unreliable node is a node with minimum trust level. Initially when any node joins the network, then this trust relationship with its all the neighbors are low or negligible that node is treated as unreliable.
2. **Reliable:** These are the nodes which have the trust level between the most reliable and unreliable. Means a node is reliable to its neighbor means it has received some packets through that node.
3. **Most reliable:** Most reliable are most trusted nodes or the nodes with highest trust level can be treated as most reliable. Here the higher trust level means neighbors had received or

transfer many packets successfully through this particular node.

During the route discovery phase of the AODV routing protocol, the trust value is also computed for all the neighbors of any node. The result of trust estimation function is the trust-status of all of neighbors as most reliable, reliable or unreliable.

1.4 Threshold value of a node:

Different threshold values are defined for different types of neighbors to become most reliable, reliable and unreliable. T_{ur}, T_r and T_{mr} are the threshold values for the unreliable, reliable and most reliable[5].

We setup a trust estimation function for the calculation of trust value:

T=tanh(R1+R2) (1)

Where tanh is an hyperbolic function, which has value

Tanhx=$(e^x-e^{-x})/(e^x+e^{-x})$ (2)

T=trust value

R1=ratio between the number of packets actually forwarded and number of packets to be forwarded

R2=ratio of number of packets received from a node but originated from others to total number of packets received from it.

2.Proposed system:

In this scheme, the source node broadcasts its own address and sequence number included into fake RREQpacket instead of destination address and destination sequence number. As the source node's sequence numberis the most recent and fresh sequence number. The other nodes do not have the latest or fresh sequence numberof the source node. When the intermediate nodes receive the fake RREQ packet, If the intermediate nodes havethe source sequence number greater than the one received in fake RREQ packet, it will reply with RREP packet.But in our case, the legitimate intermediate node will have the small source sequence number than described infake RREQ packet because only source node will have its latest or fresh enough sequence number. But if thereexist any black hole nodes in the network, then they will reply with the RREP packet as it will advertise itselfhaving the shortest path with the highest sequence number. So, the source node will detect the black hole nodesand will notify the other nodes about the black hole nodes so that the rest of the legitimate nodes will notcommunicate with black hole nodes. In previous papers, the destination sequence number is used by thesource node to compare the destination sequence number with the RREP packet's destination sequence numberbut in this case the source node may not have the fresh enough destination sequence number. As the source nodehad the old destination sequence number it used at the last time. In some papers, the RREP destination sequencenumber is compared with some threshold value but not given on which basis they calculated the threshold value.The parameters are not cleared while calculating the threshold value.

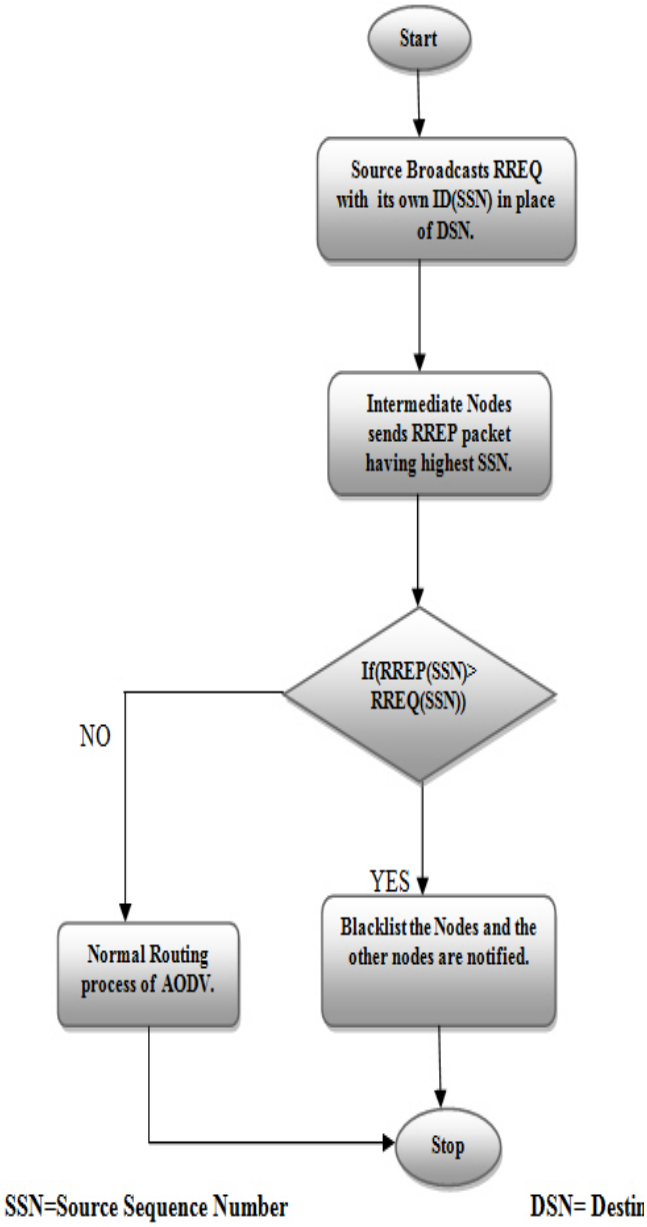

Fig4: flowchart of proposed method

a) The source node broadcasts the fake RREQ packet with its own source sequence number and Address in the destination sequence number and destination address in the RREQ packet fieldsrespectively.
b) When legitimate nodes receive the fake RREQ packet, it will compare the source sequence numberin fake RREQ packet it received with the sequence number of the source described in the table.
c) As the source node sends its own sequence number, it will be more obvious that it will be theLatest or fresh one. The intermediate node will have the source sequence less than the described infake RREQ packet. So it will not reply with RREP packet.

d) But, if there exist any black hole node in the network then it will reply with the RREP packet andAdvertises itself as having the shortest path with highest source sequence number.

e) The source node will then detect the black hole nodes exist in the network. And then send theALARM packet having the list of black hole nodes to the rest of the nodes.

3. Hardware Requirements:

System: Pentium IV 2.4 GHz.

Hard Disk: 50 GB.

Floppy Drive: 1.44 Mb.

Monitor: 18 VGA Color.

Mouse: Logitech.

Ram: 2048 Mb.

3.1Software Requirements:

Operating system: Ubuntu 14.04/linux mint/ red hat linux 9

Coding Language: otcl, c++

Tool: Ns-2.35

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

4. Results Analysis:

Throughput: Throughput is the average rate of successful message to deliver over a communication channel.

In this Graph shows and represents throughput and it shows a simulation time versus throughput. The Performance of algorithm improves throughput compare to existing Trusted AODV routing.

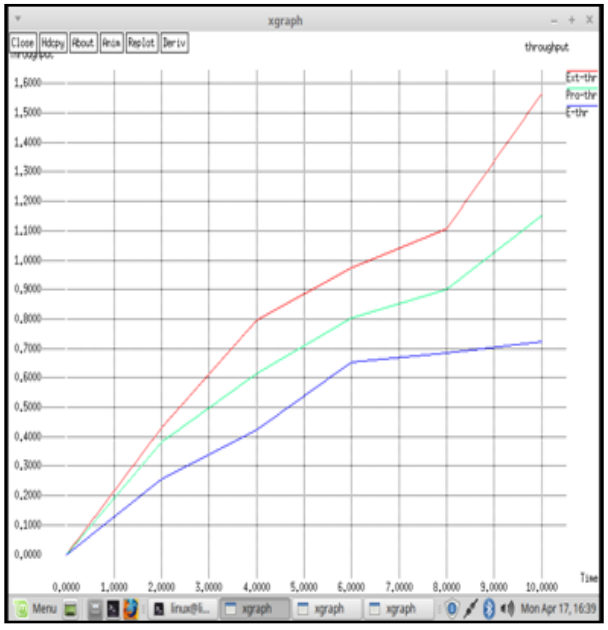

Fig.5. Threshold v/s Time

Energy: The amount of energy taken for a packet to travel from source to destination node.

In this Graph shows and represents energy consumption and it shows a simulation time versus energy. The Performance of algorithm improves energy values compare to existing Trusted AODV routing.

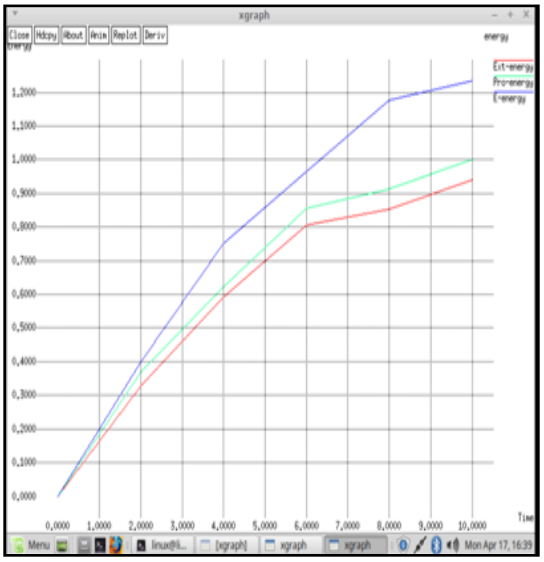

Fig.6. Energy v/s Time

Delay: Delay is the time taken for a packet to travel from source to destination node. With increase in number of malicious node delay of AODV increases.

In this Graph shows and represents end 2end delay and it shows a simulation time versus delay. The Performance of algorithm improves delay it means decrease the delay compare to existing Trusted AODV routing.

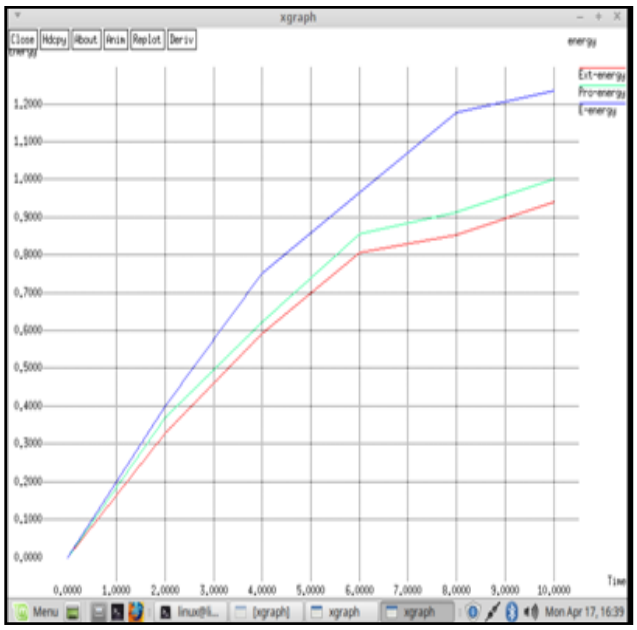

Fig.7. Delay v/s Time

4.1 Conclusion:

Security issues in MANET" is still one of the hottest areas of research. A lot of research has been devoted to the detection and prevention of black hole attack in MANET. The intelligent source based detection mechanism is proposed here to detect the multiple black hole nodes in MANET. After the detection of black hole nodes, the notification of black listed nodes to other nodes increases the network overhead which should be reduced in future. By using NS2 simulation. We are finding some conclusion. Throughput of intelligent source based detection mechanism is better compared to Trusted AODV, by increasing the time a little bit effect in throughput in both the case. Also, in future we will use a timer under which the detection will be done so that the delay of data packets can be decreased. In future, the focus of my research will be on detecting the cooperative black hole attack in MANET by using an intrusion detection system. In cooperative black hole, more than one black hole node can cooperate with each other in order to drop the data packets. It means black hole nodes work in a group to attack the ad hoc network. Also, there should be a generalized approach that can be worked for each other attacks like worm hole, gray hole, etc.

5. References:

[1]. Alka Chaudhary, V.N. Tiwari, " Design an Anomaly Based Fuzzy Intrusion Detection System for Packet Dropping Attack in Mobile Ad Hoc Networks" , 978-1-4799-2572-8/14/$31.00_c 2014 IEEE.page 256-261.

[2]. Animesh Patcha and Amitabh Mishra "Collaborative Security Architecture for Black Hole Attack Prevention in Mobile Ad Hoc Networks", Radio and wireless Conference, 2003. RAWCON'03. Proceedings 0-7803-7829-6/03/$17.00 0 2003 IEEE.Page 75-78.

[3]. Reshmi Maulik and Nabendu Chaki " A study on Wormhole Attacks in MANET", International Journal of Computer Information Systems and Industrial Management Applications ISSN 2150-7988 Volume 3 (2011) pp. 271-279.

[4] Chang Wu Yu, Tung-Kuang Wu, Rei Heng Cheng (2007) "A Distributed and Cooperative Black Hole Node Detection and EliminationMechanism for Ad Hoc Network". Paper presented at the PAKDD workshops, Nanjing, China, 22-25, pp. 538-549.

[5] E.A. Mary Anita, V. Vasudevan (2011), "Black Hole Prevention in Multicasting Routing Protocols for Mobile Ad hoc Networksusing Certificate Chaining", International Journal of Computer Applications, Volume 1, pp. 21-28.

[6] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao (2011), "A Survey of Attacks and Countermeasures in Mobile Ad HocNetworks", Human-centric Computing and Information Sciences, Springer, New York, pp. 1-16.

[7] Gurdeep Singh Bindra, Ashish Kapoor, Ashish Narang, Arjun Agrawal (2012), " Detection and Removal of Co-operativeBlackhole and Grayhole Attacks in MANETs", 2012 International Conference on System Engineering and Technology, Bandung,Indonesia, pp. 1-5.

[8] Hesiri Weerasinghe (2008) "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementationand Evaluation", Proceedings of the Future Generation Communication and Networking, Volume 2, pp. 362-367.

[9] Hemant Kumar, Dr. Ajit Singh (2012), "An Efficient Implementation of Digital Signature Algorithm with SRNN Public KeyCryptography", International Journal of Research Review in Engineering Science and Technology, Volume-1 Issue-1, June 2012, pp54-57.

[10] Hongmei Deng, Wei Li, and Dharma P.Agarwal (2002), "Routing Security in Wireless Ad Hoc Network", IEEE CommunicationsMagazine, Volume 40, Number 10, pp. 70-75.

[11] J.Sen ,S.Koilakonda and A.Ukil (2011), "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad HocNetworks," Intelligent Systems, Modeling and Simulation (ISMS), 2011 Second International Conference on , 25-27 Jan. 2011, pp.338-343.

[12] K. Lakshmi et al.(2010) "Modified AODV Protocol Against Black hole Attacks in MANET" International Journal of Engineeringand Technology Vol.2 (6), pp. 444-449.

[13Latha Tamilselvan and V Sankarnarayana (2008), "Prevention of Black Hole Attack in MANET", Journal of Networks, Volume 3,Number 5, pp. 13-20.

[14] Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Rosilah Hassan (2011) "A local Intrusion Detection Routing Security overMANET Network", IEEE, July 2011, Bandung, Indonesia, pp. 1-6.