ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Prevention of Gray Hole Attack in Mobile Ad Hoc Network

Shaily[1], Shashi lata [2]

M.Tech Scholar, Department of ECE, Advance Institute of Technology, Palwal, Haryana, India[1]

HOD, Department of ECE, Advance Institute of Technology, Palwal, Haryana, India[2]

ABSTRACT: Security is a necessary component for mobile ad hoc network (MANET). For providing security against intruder, researchers are working particularly on the security issues in MANETs, and several mechanisms are introduced for secure routing protocols within the networks. Our introduced work shows a more effective solution for determining a gray hole attack with low communication cost in the MANET, which is specifically susceptible compared to infrastructure-based networks because of its mobility and shared broadcast behaviour. As an antagonist can deploy gray hole attack successfully in the network. The introduced technique that based on digital signature (DS) is determined the attacker information by hop count technique. The routing information of real data is arrived to which intermediary node and the next hop information is available at that node is ensure by DS mechanism. The gray hole attacker node Identification (ID) is sent in network by that in future intruder is not participating in routing process. The introduced security mechanism determines and offers the negative effect against routing misbehaviour through malicious attack. Here we perform the comparison among routing performance of normal scenario, Attack scenario and DS technique. The performance of general multipath routing and introduced DS mechanism is almost equal. The intruder has decreased the entire routing performance but noted that in existence of attacker, routing misbehaviour is totally block by the introduced DS technique and retrieves 95 % of data in comparison of normal routing.

KEYWORDS: AOMDV, DS, MANET, Gray hole attack, Routing misbehaviour.

I. INTRODUCTION

Mobile ad hoc network is a set of nodes that do not based on any infrastructure to manage the network link. They may behave as a destination, source or as a router. It also neglects a single point of failure because of its behaviour of dynamic configuration. The routing protocol in a MANET can be classified into three categories i.e. table-driven/proactive, on-demand/reactive and hybrid one. They offer several applications that involves disaster relief, military application, distributed and collaborative computing, wireless sensor network (WSN), networks of visitors at health, airport and business. Security protocol development in ad hoc network is not an easy task because of its unique features of ad hoc wireless network, i.e. insecure operational environment, shared broadcast channel, lack of association among nodes, lack of central administration, limited existence of resource and physical susceptibility. An intruder can easily deploy the security attacks because of security breaches in the network [1, 2, 3, 4]. This paper is presented in the following four sections.

A mobile ad-hoc network (MANET) is a group of independent mobile nodes that can interact to one another through radio waves. The mobile nodes that are within radio range of one another can directly interact, while others require the aid of intermediary nodes to forward their packets. These networks are completely dispersed, and can work at any place without the support of any infrastructure. This feature builds these networks highly reliable and robust. Two non-adjacent devices can interact only if other devices among them are in MANET and are wishing to send packets for them. However, the nodes are mobile; the network configuration may change frequently and unpredictably over time. Due to lack of centralized management, all the network services i.e. finding of configuration and message delivering are executed by nodes themselves. Security is a mechanism that is as protected as its weakest link. So, for making MANETs protected, all its weak points are to be determined and solutions to build all those weak points safe, are to be taken. Mobile ad-hoc networks are inclined to a huge no. of security attacks [2].

The basic reality that MANET lack permanent infrastructure and utilize wireless connection for communication builds them very predisposed to an antagonist's spiteful attacks. Intruders are critical security attacks in ad-hoc networks

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

which can be used with no trouble by exploiting vulnerability of on-demand routing protocols i.e. AODV. The intrusion Detection System (DS) is not only determines the attack malicious but also prevents attacks introduced by both single and multiple nodes and the Detection and managing routing misbehaviour under MANET [3]. We attempt to arrive up to the particular solution increases network performance by the support of decreasing production of control (routing) packets as well as successfully opposing attacks against mobile ad-hoc networks [1]. One of the significant concerns associated to ad hoc networks is to offer a secure interaction among mobile nodes in a hostile atmosphere. The behaviour of mobile ad hoc networks introduces a range of challenges to the security design. These involve an open decentralized peer-to-peer architecture, a shared wireless channel and a highly dynamic configuration. This last point is where the significant issue for MANET security lies the MANET can be arrived very easily by subscribers, but also by malicious intruders. The MANET routing protocol are generally categorized in three classes [4] i.e. proactive, reactive and hybrid. The Multipath protocol i.e. AOMDV [5] set up more than one path for data forwarding and achieving in MANET.

II. BACKGROUND

Routing information is gathered only when it is required, and route determination is based on forwarding route queries across the network. The primary benefit of reactive routing is that the wireless medium is not subject to the routing overhead data for routes that may never be utilized. While reactive protocols do not have the static overhead needed by updating seamless routing tables, they may have considerable route discovery delay, can also append an important amount of control traffic to the network because of query broadcasting

AODV is a reactive/on-demand routing protocol. In AODV, when a route to new destination required, a source node flood a route request (RREQ) packet to discover a route to the target node. A valid route can found when a RREQ arrives a destination node either itself or an intermediary node with a fresh route to the target node. A fresh route is a legal route entry for the target node whose related sequence no. is higher than sequence no. of RREQ packet. A route is made existed by unicast a route reply (RREP) packet to a source node. A RREP packet is unicast by a target or an intermediary node. When a connection break in a route is determined, a route error (RERR) packet is utilized to observe other participating nodes [5].

This protocol contains two phase (1) Route Discovery and (2) Route Maintenance. AODV utilizes Route Re Request (RREQ), Route Reply (RREP) control messages in Route Discovery stage and Route Error (RERR) control message in Route Maintenance stage .The header information of this control messages can be viewed in detail. Generally, the nodes participating in the communication can be categorized as source node, a destination node and an intermediary node. With every role, the nature of a node actually changes [3]. When a source node wishes to link to a target node, first it analyses in the available route table, as to whether a fresh route to that destination node is existed or not. If a fresh enough route is existed, it utilizes the same. Else the node starts a Route Discovery by flooding a RREQ control message to all of its neighbouring nodes. This RREQ message will further be sent (again flooded) by the intermediate nodes to their neighbouring nodes [4]. This mechanism will proceed until the target node or an intermediary node having a fresh route to the destination node. At this phase finally, a RREP control message is created. Hence, a source node after forwarding a RREQ waits for RREPs to be obtained.

Working of AODV

The RREQ consists of the node's IP address, current sequence no, broadcast ID and most current sequence no. for the destination known to the source node. The destination node, on reception of RREQ, ends a route reply (RREP) packet along the back path set up at intermediary nodes during the route discovery procedure. In case of a connection failure route error (RERR) packet is forwarded to the destination and source nodes. By the usage of sequence no., a source node is always capable to determine new valid routes. AODV describes three kinds of control messages for route maintenance [5].

Security Flaws in AODV

AODV is susceptible to routing attacks by malicious nodes because of possible paper applications. Although a conclusion may survey the important points of the paper, do not repeat the abstract as the conclusion. A conclusion might describe on the significance of the work or recommend applications and extensions basically designed to have characteristics i.e. integrity, authentication, non-repudiation and confidentiality. AODV can easily be manipulated by a malicious node to interrupt its routing.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

The following actions can be taken by an inside attacker to disrupt routing in AODV:

1) Change/forge RREQ or RREP packets.
2) Spoof source or destination IP address to pose as legitimate network node and hence obtain or drop data packets.
3) Create fake RERR packets to increase routing delay and decrease network performance [6].
4) Cause DoS by forwarding fake RREPs of highest sequence no. (i.e. Gray hole attack)[7].
5) Generate routing loops and launch sleep deprivation or resource consumption attacks to deplete node batteries.
6) Replay old routing messages or build a tunnel/wormhole.

Advantages and disadvantages

The main benefit of this protocol is having routes set up on need and that destination sequence no. is used to discover the latest route to the destination node [8]. The link setup delay is lower. One drawback of this protocol is that intermediary nodes can yield to inconsistent routes if the source sequence no. is very old and the intermediary nodes have a higher but not the latest destination sequence no., thus having stale entries [9]. Also, multiple route Reply packets in response to a single Route Request packet can yield to heavy control overhead and unessential bandwidth consumption because of periodic beaconing several Route Reply packets in reply to a single Route Request packet can result to heavy control overhead and unessential bandwidth consumption because of periodic beaconing Request packet can lead to heavy control overhead and unessential bandwidth consumption because of periodic beaconing

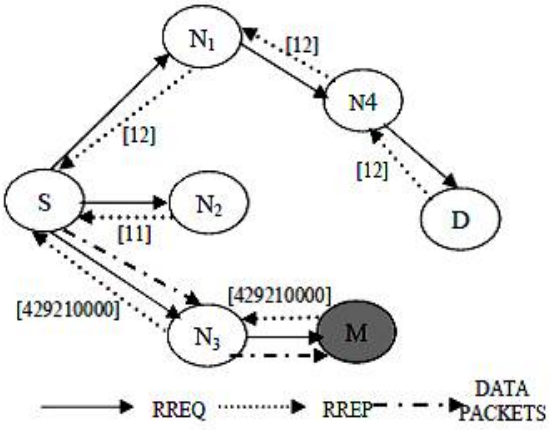

Fig 1: Traversal of Control Messages in AODV

However, the node S has a RREP control message with maximum destination sequence no. to that route, node S will neglect two genuine RREP control messages. The source node processed the incoming RREPs for consideration is illustrated. After a source node obtains a RREP message, it calls *Receive Reply (Packet P)* method one of the necessary function of AODV [11].

Gray hole attack caused by RREQ

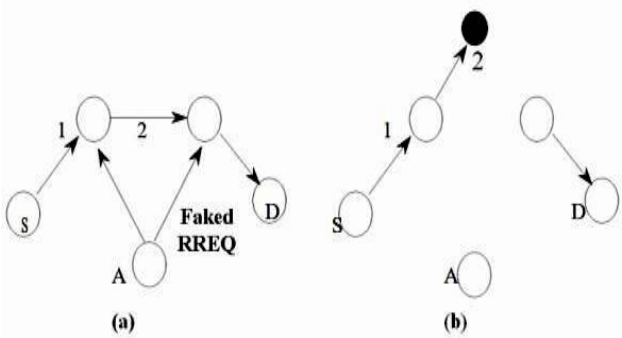

Fig 2: An attacker can send fake RREQ messages to form gray hole attack

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

The attacker can generate Gray hole attack by faked RREQ message as follows:
In RREQ Gray hole attack, the intruder set the type field to RREQ (1) adjust the source IP address to the originating node's IP address; Set the destination IP address to the destination node's IP address; Set the source IP address (in the IP header) to a non-available IP address (Gray hole); Increase the source sequence no. by minimum one, or reduce the hop count to 1.The intruder makes a Gray hole attack between the source node and the destination node by fraud RREQ message.

Gray hole attack caused by RREP
The intruder may create a RREP message to make Gray hole as follows: adjust the type field to RREP (2); Set the hop count field to 1;Set the source IP address as the source node of the route and the destination IP address as the destination node of the route, Increment the destination sequence no. by minimum one; adjust the source IP address (in the IP header) to a non-available IP address (Gray hole).The intruder unicasts the faked RREP[12] message to the originating node. When originating node receives the fraud RREP message, it will maintain its route to destination node through the non-available node. Then RREP Gray hole is made.

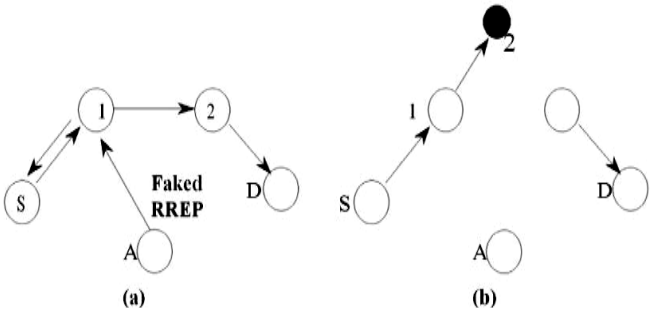

Fig 3: Gray Hole is formed by fake RREP

III. PROPOSED ALGORITHM

Proposed Algorithm to Identify and Prevent from Attack:
Algorithm: To detect and prevention from attack.
Type of attacker = Black hole as a Malicious attacker
Steps:
Begin

i. Establish a network for n number of nodes.
ii. Define sender, receiver nodes.
iii. Find out all neighbors of source node.

For sender to receiver

i. Sender Send Route Request message to neighbor nodes for finding the destination
ii. If next node is destination Then direct path is established
iii. Else Broadcast the RREQ to next neighbors and maintaining the hop count information.
iv. If destination (receiver) is found then select the route of minimum hop count and deliver data through that minimum hop count path h.
    a) Multiple paths are selected on the basis of hop counts h1, h2, h3…….. hn, n=1,23…
    b) Σ Hn = (h1, h2, h3…….. hn) up to destination is Minimum then select for data sending and next route of hop count h1, h2, h3 …….. hn ≥ Min is select for multiple path.

For destination to source

i. Select the path with minimum hop counts
ii. Unicast RREP to pervious node with digital signature
iii. Verify digital signature
iv. If (all signatures are valid)
v. Establish a path for data transfer.
vi. If (Any intermediate or destination node is malicious node)

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

vii. Then add the malicious node information in malicious node column and again rebroadcast Route request (RREQ) .

IV. PERFORMANCE EVALUATION AND SIMULATION RESULTS

The packets obtaining in MANET is not being on any administrator and supervision. The data delivery in that type of network is not secure. In this graph we showed the throughput analysis in case of normal Network, Attack and introduced DS technique. The packet per unit of time in case of attack is almost negligible in network but in case of introduced DS technique the throughput is much better in comparison of attacker in 60, 80 and 100 nodes scenario. The throughput in case of normal scenario routing is about greater than 3500 packets/seconds and not less than 600 packets/seconds. It means that the throughput in case of DS is more in comparison of normal scenario. The cause behind is that if the attacker is available in established path then in that case that path is not chosen for data delivery to managing the reliability and the next optional path is selected more reliable and strong that decreases packet dropping and enhances data delivery in existence of attacker.

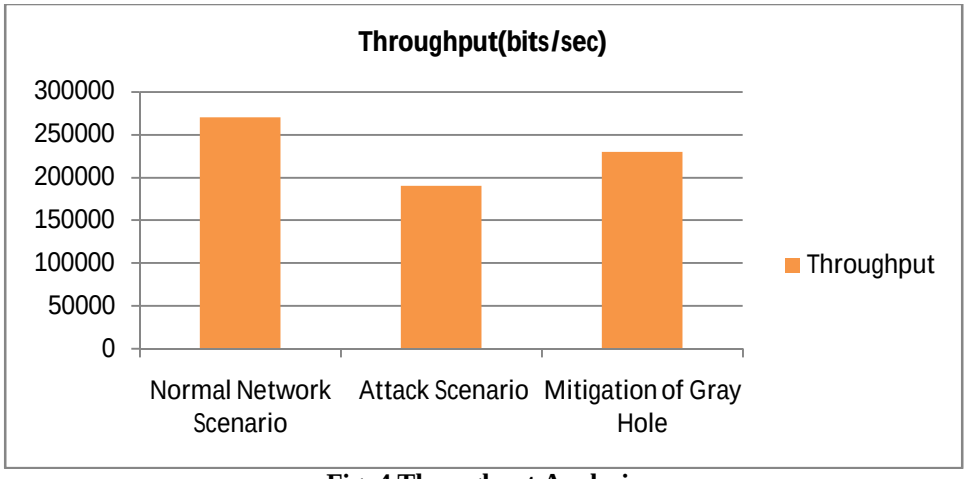

Fig. 4 Throughput Analysis

VI. CONCLUSION & FUTURE WORK

The absence of central coordination system, security is the significant issue in MANET. The data packets in network are delivering in between sender and recipient through routing technique of link establishment. The performance is evaluated in 60, 80 and 100 nodes scenario. The intruders are losing the all data packets that are the cause of routing misbehaviour in MANET. The malicious attacker action is wedged by introduced DS security mechanism and offers the attacker free network. The AOMDV protocol offers the alternative if the issue in accessible path is happened. The routing performance is evaluated by performance metrics in case of normal scenario AOMDV routing, Malicious Attack and introduced DS mechanism. The introduced DS scheme determined the attacker through next hop information of data delivery and also sends the Identification of node ID of intruder in network. If that ID is available in routing establishment then the alternative route is chosen for data delivery. The routing performance of AOMDV protocol and DS scheme on AOMDV is almost equal that means nearly the network is provides equivalent performance. In attacker module degrades the whole performance of network but in existence of attacker their activities are entirely blocked by DS scheme after determining them in network. Furthermore, after dump the network performance by attacker introduced DS scheme recovers 95 % of data loss in comparison of normal AOMDV. In future we also apply this DS technique on other routing attacks i.e. wormhole attack and Grey-hole attack. Also examine the impact of attack on energy consumption of mobile nodes i.e. the major or only source of communication. Without energy available nodes in MANET are not survived for a long time.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

REFERENCES

[1] Fatima Ameza, Nassima Assam and Rachid Beghdad, "Defending AODV Routing Protocol Against the Gray Hole Attack", International Journal of Computer Science and Information Security, Vol. 8, No.2, 2010, pp.112-117.
[2] Nital Mistry, Devesh C. Jinwala and Mukesh Zaveri, "Improving AODV Protocol against Grayhole Attacks", International Multiconference of Engineers and Computer Scientists 2010, vol. 2, March 2010.
[3] Payal N. Raj and Prashant B. Swadas,"DPRAODV: A dynamic learning system against gray hole attack in AODV based Manet", International Journal of Computer Science Issues, Vol. 2, Issue 3, 2010, pp: 54-59.
[4] Hoang Lan Nguyen and Uyen Trang Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks", International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, April 2006, pp. 149-149
[5] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah, "MANET Routing Protocols and Wormhole Attack against AODV", International Journal of Computer Science and Network Security, vol. 10 No. 4, April 2010, pp. 12-18.
[6] N. Shanthi, Dr. Lganesan and Dr.K.Ramar, "Study of Different Attacks on Multicast Mobile Ad hoc Network", Journal of Theoretical and Applied Information Technology, December 2009, pp. 45-51.
[7] Abhay Kumar Rai, Rajiv Ranjan Tewari and Saurabh Kant Upadhyay , "Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security, vol. 4 issue 3, July 2010, pp. 265-274.
[8] Jakob Eriksson, Srikanth V. Krishnamurthy, Michalis Faloutsos, "TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks", 14th IEEE International Conference on Network Protocols, November 2006, pp.75-84.
[9] Mahdi Taheri, Dr. majid naderi, Mohammad Bagher Barekatain, "New Approach for Detection and defending the Wormhole Attacks in Wireless Ad Hoc Networks", 18th Iranian Conference on Electrical Engineering,, May 2010, pp. 331-335.
[10] Dang Quan Nguyen and Louise Lamont, "A Simple and Efficient Detection of Wormhole Attacks", New Technologies, Mobility and Security, November 2008, pp. 1-5.
[11] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, "Analysis of Wormhole Intrusion Attacks in MANETs", Military Communications Conference, November 2008, pp.1-7.
[12] Maria A. Gorlatova, Peter C. Mason, Maoyu Wang, Louise Lamont, Ramiro Liscano, "Detecting Wormhole Attacks in Mobile Ad HocNetworks through Protocol Breaking and Packet Timing Analysis", Military Communications Conference, October 2006, pp. 1-7.
[13] Mani Arora, Rama Krishna Challa and Divya Bansal, "Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks", Second International Conference on Computer and Network Technology, 2010, pp. 102-104.
[14] Yih-Chun Hu, Adrian Perrig,and David B. Johnson, "Wormhole Attacks in Wireless Networks", IEEE Journal on Selected Areas in Communications, vol. 24 no. 2, February 2006, pp. 370-380.
[15] W. Weichao,B. Bharat, Y. Lu and X. Wu, "Defending against Wormhole
[16] Attacks in Mobile Ad Hoc Networks", Wiley Interscience, Wireless Communication and Mobile Computing, January 2006.
[17] L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multipath," IEEE Wireless Commuunication. and Networking Conference,
[18] I. Khalil, S. Bagchi, N. B. Shroff," A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", International Conference on Dependable Systems and Networks, 2005.
[19] L. Lazos, R. Poovendram, C. Meadows, P. Syverson, L.W. Chang, "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: a Graph Theoretical Approach", IEEE Communication Society, WCNC 2005.
[20] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", 11th Network and Distributed System Security Symposium, pp.131-141, 2003.
[21] L.Lazos, R. Poovendran, "Serloc: Secure Range-Independent Localization for Wireless Sensor Networks",ACM Workshop on Wireless Security, pp. 21-30, October 2004.
[22] W. Wang, B. Bhargava, "Visualization of Wormholes in sensor networks", ACM workshop on Wireless Security, pp. 51-60, 2004.
[23] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, "Gray Hole Attack in Mobile Ad Hoc Networks", ACMSE, April 2004, pp.96-97.
[24] Anu Bala, Munish Bansal and Jagpreet Singh, "Performance Analysis of MANET under Grayhole Attack", First International Conference on Networks & Communications, 2009, pp. 141-145.
[25] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Grayhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007, pp. 21-26.
[26] Geng Peng and Zou Chuanyun,"Routing Attacks and Solutions in Mobile Ad hoc Networks", International Conference on Communication Technology, November 2006, pp. 1-4.
[27] S. Lee, B. Han, and M. Shin, "Robust Routing in Wireless Ad Hoc Networks", International Conference on Parallel Processing Wowrkshops, August 2002.
[28] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato1, Abbas Jamalipour, and Yoshiaki Nemoto1," Detecting Grayhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, vol..5 no..3, Nov. 2007, pp.338–346.
[29] Nadia Qasim, Fatin Said, and Hamid Aghvami, "Performance Evaluation of Mobile Ad Hoc Networking Protocols", Chapter 19, pp. 219-229.
[30] G.S. Mamatha and S.C. Sharma, "A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS", International Journal of Computer Science and Security, vol. 4, issue 3, Aug 2010, pp. 275-284.