International Journal of Academic Research and Development
ISSN: 2455-4197
Impact Factor: RJIF 5.22
www.academicsjournal.com
Volume 2; Issue 5; September 2017; Page No. 789-792

An approach to detect and remove wormhole and black hole attacks from mobile ad-hoc network using BDS methodology

Harjit Kaur
Assistant Professor, Dr. B.R. Ambedkar Govt. College, Mandi Dabwali, Haryana, India

Abstract
MANET is distributed network in which all activities are executed by the nodes, these nodes are free to go in and out of the network at any point of time. All activities performed by the network like discovering the topology, delivery of data packets and internal management communications. These communications is performed without establishing any central administrator. When nodes, which are performing communication, are mobile nodes (i.e., moves from one position to another) then it is called a Mobile Ad hoc Network (MANET), MANET could be a set of self-configurable mobile nodes. In a MANET, communication between the mobile devices is carried out by some intermediate devices called routers. All routing functionality is merged into mobile nodes. Routing protocols helps to transfer the packets to destination. The very facts that mobile Ad-hoc network is innovative & difficult areas of wireless networks, makes it more vulnerable in term of flooding & routing attacks. Some attacks like Black Hole attacks, Wormhole attacks, Denial of Service attacks, that completely drops the packets in MANET, it has minimum shortest path to destination in the network without moving them to forward. Security is a critical challenge for unstructured network nodes participating in communication in Mobile Ad-hoc Network. In this paper, we provide a secure scheme to overcome such types of threats. The main aim of this work is to detection and removal of the Black Hole and Wormhole Attacks to protect the Network and improve the packet delivery fraction, using Bait scheme.

Keywords: MANET, nodes, wormhole attack, black hole attack, bait detection scheme (BDS), ad-hoc network

Introduction

A MANET is a high able and fast moving technology; it is a set of mobile nodes in which all nodes are transmitting data with each other directly or indirectly by passing the packets of messages in wi-fi community without any fixed infrastructures. Every node now not simplest acts as host but also act as a router [1]. Using the routing protocol in MANET for proper transfer of data packets from one point to another point. Some famous protocols are DSR, AODV and DSDV. The nodes can input and leave the ad-hoc community dynamically. Network topology changes dynamically because the nodes are mobile and it is difficult to retract them over time. Due to this dynamic nature, MANET suffers from various security issues than the conventional networks [2]. The security challenge has become a major concern. Mobile Ad-hoc network is generally used in applications such as Emergency rescue service, military communication by soldiers, Disaster Recovery. As MANET lack an infrastructure, they are showing to many threats. Wormhole and Black Hole is the most risky Threats in MANET [3].

Wormhole assault is the most intense threats of advert-hoc community. Its miles a sort of DOS risk, which may be very powerful in community layer. It is a co-operative attack because there is a need of two nodes that will act in co-operation on this attack, at two distinct edges of the network, taking part attacker nodes will occupy their robust strategic places. In this way, they are occupying dominant positions in a network so that they (nodes) can cover complete network and present to have the smallest path for transferring data [4]. By means of using direct Wi-Fi hyperlink these attacker nodes are linked together which is known as wormhole tunnel. At one end of wormhole tunnel, one node will collect packets in its local area and then those packets are transmitted to the other node at the other end of tunnel then this node will play again with those packets [5].

In a Black hole assault, a malicious node sends a fake RREP packet to the source node that has initiated a path discovery technique and so as to reveal itself as a destination node or an intermediate node to the actual vacation spot node to the course. In the sort of case the supply node could ship all of its statistics packets to the malicious node and the malicious node absorbs all facts packets. The malicious nodes draws all the packets by using cast course respond Packet (RREP) that's a faux shortest path to the vacation spot and drops all of the packets in place of forwarding it to the destination. The supply node sends its information packets via the malicious node to the vacation spot Black hollow attack might also additionally stand up due to a malicious node that is deliberately misbehaving, further to a damaged node interface. Anyhow, nodes in the network will continuously try and find a route for the vacation spot, which makes the node consume its battery in addition to dropping packets.

BDS scheme is used to detect the malicious node in Black Hole & Wormhole Attacks. On this scheme, the deal with of an adjacent node is used as bait destination address to bait

malicious nodes to send a fake reply RREP message and malicious nodes exact location in the network. In this work, the bait scheme will be modified according to the wormhole & Black Hole attacks.

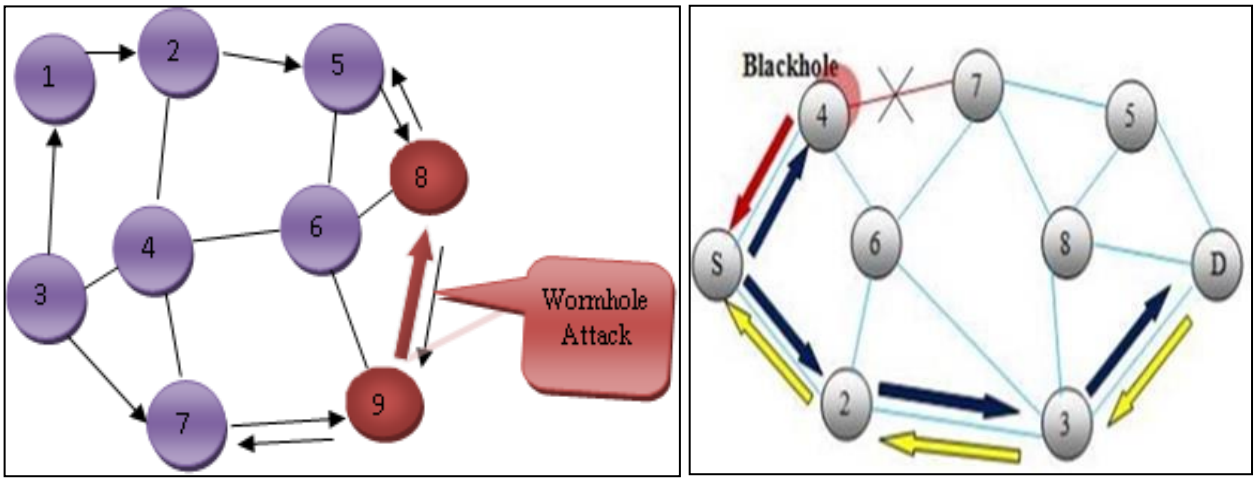

Fig 1: wormhole and black hole in MANET

Related Work

The idea of calculating trust values of nodes in order to find malicious or legitimate nodes in the network. Authors propose the way to protect in opposition to wormhole attack the use of aggregate of parameters like strength, range of connections and buffer length of a node based totally on these parameters consider price of a node is computed. Then this consider value of node is as compared with threshold cost of community consider. Based on this comparison it can be found that whether that selected node is either malicious or legitimate. The proposed methodology consists of two phases: First, do analysis of network parameter and threshold computation and secondly the security implementation on the existing routing protocol. Results are analyzed by extending AODV protocol and the performance of the proposed routing protocol is evaluated and compared with the AODV under attack [6].

This approach some nodes that are straightforward in terms of effective battery and range, are selected as again Bone Nodes (BBN). Each BBN generates numbers that are unique for that host. Whilst supply node desires to talk with the destination, it request nearest BBN for limited Ip (RIP). BBN on receiving the RIP sends one of the unused IP cope with which is selected randomly from the pool of unused IP address. Supply node sends RREQ for each the destination and RIP concurrently. If the source node gets RREP best from the vacation spot node and now not from the RIP, then the community is free from both the gray-hole and black hollow attacks. Source node (SN) can use that IP for further transmissions. If SN receives RREP from RIP then black hole detection is initiated. SN signals the neighboring nodes to enter into promiscuous mode in order that they pay attention no longer simplest to the packet destined to them, however additionally to the packet destined to the desired vacation spot node [7].

Wormhole attack that is susceptible assault in which two or extra malicious nodes shape a tunnel like structure to relay packets themselves. This type of assault may cause selective forwarding, fabrication and alteration of packets being sent. In this paper, an identification based totally signature scheme along with clusters is proposed for protecting community from wormhole attack. Cluster based architecture is used in which cluster heads are chosen in such a way that they cannot be malicious. This scheme operates in three phases [8].

Data Routing Information table (DRI) and Crosscheck methods are applied to detect cooperative black hole attack. DRI table is generated for each node, which contains two fields from and through. From contains information from which node data is routed. Through contains information through which node the data is routed [9].

In order to provide safe communication, author's present communication parameter based analysis model. Wormhole attack is one such attack in which two or more nodes can collectively access the bandwidth and communication can be perturbed. In this paper, a wormhole-infected network is defined and in order to perform the reliable communication in attacked network the work model is offered. Network model is generated for optimizing the communication to identify the safe communication node [10].

A new protocol named M-AODV that is a category of overhearing backup protocol primarily based on AODV. After that, security of proposed protocol is assessed, the authors simulate both protocols (M-AODV and AODV) under black hole and wormhole attacks, using no security solution. The proposed protocol is primarily based on overhearing the neighbors and steady comparison of the facts of important and opportunity tables and proposed protocol is determined to be secure and some assaults are tested on it. Wormhole attack is detected through overhearing the nodes. The effects display that M-AODV has been improved in phrases of packet delivery ratio, and the delay has been decreased as properly, but the quantity of overhead have been accelerated [11].

Proposed Method

In order to detect and reduce the wormhole and black hole nodes in the MANET the proposed technique will use the concept of the bait destination node only. It works in the following way:

- **Algorithm for Wormhole detection and prevention in MANET**

Case 1: First, the source node will randomly choose one of its neighbors as the BDS (bait destination) address.

Case 2: Now the source will broadcast the bait route request in the whole network.

Case 3: Considering the neighbor is the wormhole:
In this case second pair with which tunnel has been created by the bait, destination node will be located somewhere in the network. The source node will receive only one reply but in this reply, the path to bait destination will be going through some other node.

Case 4: Considering the neighbor is not the wormhole:
Source will have the reply from the neighbor itself whose address was used to send the bait route request and the source will also have a reply from the wormhole nodes that have created the tunnel in the Ad-hoc network.

- **Algorithm for Black Hole detection and prevention in MANET**

In BDS the source node selects an adjacent node as BDS (bait destination) address to send the bait malicious nodes a respond RREP communication. Detected and removed of malicious nodes from participating in the routing process.

Case 1: Initial Bait Step
To identify whether malicious nodes exists in the network, source node say nr selects the adjacent node as bait destination. If malicious node exists it sends RREP messages once it gets the RREQ'. If other nodes sends RREP message in addition to nr node, then this indicates that malicious node exists in the network.

Case 2: Transferred to Reactive Defense stage
When the route is established and if at the endpoint it is create that the data packet delivery ratio considerably wrong to the threshold, the detection and reduction method would be triggered again to detect for nonstop protection and real-time reaction efficiency. The threshold is a varying value in the range [80%, 90%] can be adjusted according to the current network efficiency. The initial threshold value is set to 87%. If the time of packet delivery ratio is less than the threshold then detection scheme will be triggered.

1. Since the node is one hop neighbor of the source node, so the reply must not have hop count greater than one in both the cases. This means that the reply that came from the nodes is false claiming path to destination, having hop count of more than one is false, and source node will put the nodes in the suspected list.
2. Now next step is to find out which nodes in the path are malicious nodes.
3. For this, the source node will send few test packets over the path and if the packet drops occur on any of the node, the source node will put that node as well as the predecessor node in the malicious node list.
4. Source will now send the original destination route request. Along with route request, it will inform the nodes to not communicate with the malicious nodes.
5. Now the normal communication will resume over the new path. The new path will not contain any black hole & wormhole nodes in it.

Performance evaluation

Simulation Results

Ns2-2.34 is used to evaluate the performance of the network using AODV Protocol, first without attack and later under different types of attack. In simulation we are using 40 mobile nodes with base routing protocol as AODV routing and have considered two similar environments for analysis about the behavior of AODV namely without attack, under wormhole attack and black hole attack. Different matrices like Data packet sent, Data packet received, Data packet drop, have been used to evaluate the performance of network. Table 1 is display parameter of simulation.

Table 1: Simulation Parameters

Number of Nodes	**40**
Physical medium	Wireless
Transmission Range	240m
Simulation Area	800 m* 800 m
Simulation Time	110 sec
Packet size	1.024 megabytes
Routing Protocol	AODV
Attack Type	Wormholes, Black Holes
MAC	IEEE 802.11
Detection Methodology	BDS
Traffic Type	CBR
Channel data rte	12 mb/s
Node Mobility	Random (0 – 25 mps)

Firstly, the estimation-based detection is applied for calculating level of nodes using bait scheme. Thereafter we analyze the performance of the network under two types of attacks within the network and also to capture, drop or unwanted packet spread over the network. This process identifies all the attacker nodes. The Table 2 below shows the identified wormhole and black hole attacker nodes 12, 25 and 32 whose unwanted packets flooded and Table 3 shows, Analysis of data packets that are sanded and received by the AODV protocol with black hole & wormhole attacks in mobile Ad-hoc Network. The proposed bait detection methodology detects simultaneous black hole, wormhole attack.

Table 2: Analysis of Attacker Node

Nodes	**Wormhole Attack with AODV**			**Black Hole Attack with AODV**	
	Packet spread	**Packet Drop**	**% Drop**	**Packet drop**	**% Drop**
12	35710	1605	4.49 %	1421	3.97 %
25	139526	1204	0.86 %	1094	0.78 %
32	68532	1146	1.67 %	110	0.16 %

Table 3: Analysis of Data Packets

	Packet send	Packet Received	Packet Drop
Normal AODV Protocol	4825	4115	710
Protocol with Wormhole	4360	3563	797
Protocol with Black Hole	2211	491	1720

Conclusion

An easy but effective BDS methodology has been proposed to detect different attack typed. The nodes in MANET communicate wirelessly with each other. The wireless environment of the communication makes nodes susceptible to many types of threats such as, wormhole & black hole attack. In present work, our objective to detection and remove of the wormhole & black hole attack. The proposed technique will use the idea of the bait destination node. The analysis of the generated table helps in identifying wormhole and black hole attacks.

References

1. Pooja Rani. Multiple Black Hole Detection Algorithm for AODV in MANET", IJESC. 2017, 7.
2. Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach", Member, IEEE Systems Journal. 2015, 9.
3. Umang Singh, "Secure Routing Protocols in mobile Ad hoc networks-A survey and Taxanomy", International Journal of Reviews in Computing. 2011, 7.
4. Farrukh Aslam Khan, Muhammad Imran and Hiader Abbas, A Detection and Prevention System against Collaborative Attacks in Mobile AD hoc Networks, Future Generation Computer System ELSEVIER. 2017, 68.
5. Xue Y, Nahrstedt K. providing fault ad hoc routing service in adversarial environments, Wireless Pers. Commun. 2004, 29.
6. Ashish Kumar Jain, Ravindra Verma. Trust-Based Solution for Wormhole Attacks In Mobile Ad Hoc Networks, Global Journal of Multidisciplinary Studies. 2015, 4.
7. Nital Mistry, Devesh C Jinwala, Mukesh Zaveri, Improving AODV Protocol against Blackhole Attacks, proceedings of the International Multi Conference of Engineers and Computer Scientists 2010 II - IMECS 210.
8. Dhruvi Sharma, Vimal Kumar, Rakesh Kumar, "Prevention of Wormhole Attack Using Identity Based Signature Scheme in MANET, Computational Intelligence in Data Mining, 2015, 2.
9. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative blackhole attacks in wireless ad hoc networks, in Proc. Int. Conf. Wireless Netw. 2003, 570-575.
10. Amit Kumar, Sayar Singh Shekhawat. A Parameter Estimation Based Model for Worm Hole Preventive Route Optimization", International Journal of Computer Science and Mobile Computing. 2015, 4.
11. Elham Zamani, Mohammadreza Soltanaghaei. The Improved Overhearing Backup AODV Protocol in MANET" Journal of Computer Networks and Communications, 2016. Article ID 6463157, 8. Hindawi.