International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P), Volume-6, Issue-3, November 2016

Detection Of Cooperative Black Hole Attack Using Prime Product Number

Prabhleen Kaur, Taranjit Singh

***Abstract*— A mobile ad-hoc network is a self-governing network that consists of nodes which communicate with each other without the need of any wired and wireless network, mobile ad-hoc network are more capable to security attacks due to its dynamic nature. To handle communication and determines the path of packets in network, a routing protocol plays a very important role in MANET. A node transferring information in form of packets which is a part of defined network, the routing protocol is good which is assumed when all the data packets received by source from destination successfully. In MANET, the principal routing protocol AODV is used. The security of AODV protocol is affected by malicious node attack, the malicious node claiming the freshest and shortest route to the destination by introducing a faked route reply in this attack. The malicious node discards the data packets whenever it arrives. For detection and removal of malicious node attack, this paper uses PPN (Prime Product Number) technique.**

***Index Terms*— AODV, Black Hole Attack, Cooperative Black Hole Attack, MANET**

I. INTRODUCTION

In Mobile Ad-hoc Network (MANET) mobile devices capable of changing their topologies dynamically that constitute a network, and MANET itself as a wireless configuring network. For peer devices the network nodes also act as routers rather that only act as ordinary nodes. The routers move freely and organize themselves randomly. There is no centralized gateway device to monitor the traffic so network topology may change rapidly and spontaneously within network. Since the medium is open for all nodes, both malicious nodes legitimate and can access it.

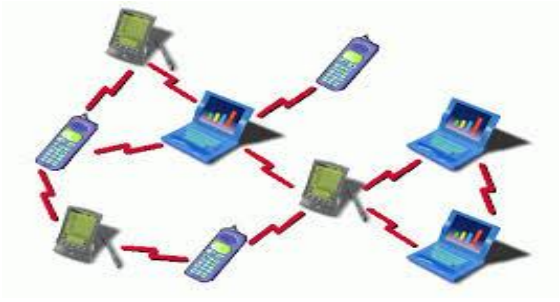


Fig1. Mobile Ad-Hoc Network

However, there are still many problems about MANETs, such as security problem, finite transmission bandwidth, and restricted hardware.

Prabhleen Kaur, Department of Computer Science & Engineering, BGIET, Sangrur, India
Taranjit Singh, Department of Computer Science & Engineering, BGIET, Sangrur, India

A. Security Attacks in MANET

On the basis of the behavior of attacks, the attacks can be classified into two parts i.e. passive attacks and active attacks.

1. Passive Attacks

This attack transferred the data to other nodes in network without interrupting the communication of the operation.

2. Active Attacks

An active attack is very serious attack in network that stops the flow of messages between the nodes.

a. Black Hole Attack

Black-hole attack is an active attack. In Black-hole attack, malicious node sends fake information by claiming that it has a fresh route to the destination node and hence source node (SN) selects the shortest path and go through that malicious node. When malicious node receives the packet it discards all the packets.

i. Single Black Hole Attack

In this attack only one node act as a malicious node while the other nodes will be genuine.

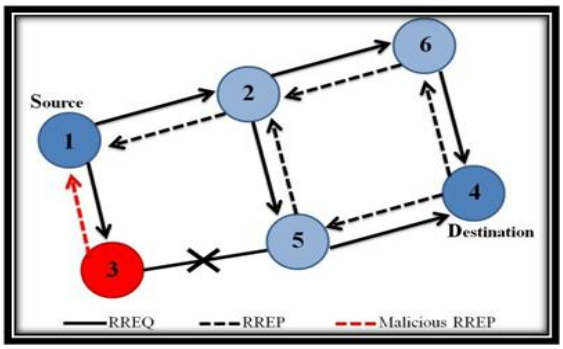


Fig2. Single Black Hole Attack

ii. Cooperative Black Hole Attack

In this attack at least two nodes act as a malicious nodes but the chances of more than two malicious nodes may occur.

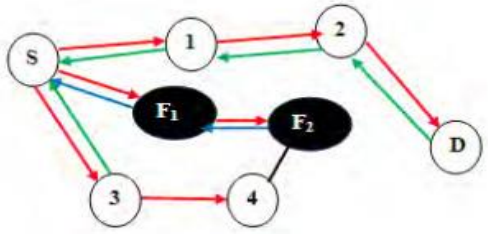


Fig3. Cooperative Black Hole Attack

II. RELATED WORK

Sapna Gambhir et.al (2013) [1] studied that a mobile ad-hoc network is an autonomous network which consists of nodes that communicate with each other with wireless channel. As compared to conventional wired and wireless networks, MANETs are more vulnerable to security. The principal routing protocol used in MANETs is AODV. The security of AODV protocol is affected by malicious node attack. By claiming to have the shortest and fastest route to the destination, a malicious node sends a faked route reply in this attack. However, when the data packets reach, the malicious node discards them. To overcome the problem of malicious node attack, the author represents PPN (Prime Product Number) scheme for detection and removal of malicious node.

Rashika Indoria et al. (2015) [2] evaluated that a wireless ad hoc network is a network where nodes can communicate with each other due to infrastructure less network. This infrastructure can be set up easily with very low cost. They have used Trust based AODV routing protocol with the addition of Fuzzy Logic to improving the security of routing protocol for MANET. Their aim is to provide the security of data packet against the black hole attacks. The throughput, packet delivery ratio parameters are used to examine the performance of AODV and TAODV.

Ali Abdulrahman Mahmood et.al (2015) [3] investigated that without using any infrastructure, mobile nodes dynamically change their topology in a wireless MANET. There are a lot of routing protocol for Ad-hoc network such as OLSR, AODV and ZRP. Malicious nodes continuously drop data packets and interrupt the correct operation of the routing protocol. This paper proposes the possibilities to detect the malicious node in the AODV routing protocol that cause black hole attack.

P. V. Venkateswara Rao et.al (2015) [4] proposed that MANET is capable to handle different kinds of attacks due to permanent properties. The popular attack in MANET is the Black Hole attack which is most common in the routing protocol AODV. In this paper, the authors simulate the Black-hole attack in AODV using NS2 Simulator for both SANETS and MANETS by changing node density in the context of responsive and non-responsive traffic. The simulation results shows when there is black-hole attack the performance of throughput, PDR is less and end-to-end delay, routing load is high.

Mr. Ramanpreet Singh et al. (2015) [5] said that Mobile Ad hoc network is a wireless network without having any fixed infrastructure. It consists of mobile nodes which are free in moving in or out in the network. This paper shows energy efficient modified AODV routing protocol using Clustering method in MANET. The AODV uses parameters PDR, energy consumption, end-to-end delay & throughput and detect the black hole attack & improve the energy level of MANET.

Swati Pokhariyal et al. (2015) [6] studied that Mobile Ad-hoc Network (MANET) provides a wireless medium for communication among various mobile nodes and provides an infrastructure-less network for communication. Black hole and Gray hole attack in MANETs are considered one of the most dangerous attacks due to their packet dropping characteristic. In this paper, the authors discuss their previous work for Black hole and Gray-hole node detection. Their proposed work on AODV protocol provides about 99% packet delivery ratio with better security and provides complete elimination of the attacker nodes from the network.

Tarek M.Mahmoud et al. (2015) [7] presented that MANETs are composed of a set of stations (nodes) communicating through wireless channels, without any support of fixed backbone in which nodes are allowed to join and leave the network at any point of time. In Black hole attack, malicious node uses the routing protocol to advertise itself as having the shortest path to the destination whose packets it wants to halt. They proposed Intrusion Avoidance System (IASAODV) which can be considered as modification of the AODV protocol and can be used to detect and avoid the black hole attack.

Anuj Ranaa et.al (2015) [8] constructed most demanding issue in MANETs is security or secure communication due to its various vulnerabilities. Characteristics that make MANETs down to various attacks such as infrastructure-less network environment, dynamically movement of nodes. Characterized attacks have more harsh affects on MANETs than single particular attacks. The simulation results are performed on various network metrics such as PDR, normalized routing overhead and end-to-end delay.

Sourabh Singh Vermaa* et.al (2015) [9] investigated that MANET can be affected by various kinds of attacks, as it has various mobile nodes which are disperse and needs cooperation to transfer traffic. One attack is flooding attack, which can have impact on QOS parameters of the network. The authors have shown variable flooding nodes that are flooding in network for different time intervals. NS2 is used to determine such malicious nodes and analyzed six different results which show severe effect of such attack on QOS and also shows how packet delivery fraction is inversely proportion with bandwidth occupied by flood request.

G.Vennila et.al (2014) [10] showed that MANET is a collection of wireless mobile node in which each node can communicate with each other without any infrastructure. The authors proposed an algorithm which is used to secure the DSR protocol and the algorithm was tested in MATLAB. The aim of this paper is to provide better security from Co-operative Black-hole attack in MANET and also tells how it affects the performance metrics i.e. throughput and delay of the network by comparing the network performance with and without black hole nodes.

Ravinder Kaur et.al (2014) [11] said that a mobile ad hoc network (MANET) is infrastructures less network in which mobile nodes communicate with each other without the use of any centralized network. In Black-hole attack a malicious node tells as having the shortest path to the node whose packets it want to stop. In this paper the authors are trying to find the best path for transferring the packet through Digital Signature. The verification technique which is used is Digital Signature.

Ms.Heena Bhalla (2012) [12] said that a Mobile ad-hoc network is a temporary network set up by wireless mobile nodes moving individually in the places that have no network infrastructure. The most prominent attack is the Black Hole Attack which drops all data packets in the network. Due to this attack the data packet do not reach the destination node on account of this attack, hence data loss will occur. In this paper they simulated MANETs with and without Black Hole Attack. Due to Black Hole Attack the average packet drop

increased from 0.25% to 90.69% and the throughput of the network decreased 93.56%.

III. PROPOSED METHODOLOGY

The routing misconduct can strictly reduce the working efficiency while working at routing layer. While the process of route discovery and maintenance.it is very difficult to find Misconduct behavior of node.ie either node will forward data or not. So it is difficult to make detection process more effect and accurate for changing the bad effect of nodes Prime Product Number (PPN) scheme is proposed. For detecting the misbehavior of nodes the basic idea of the PPN scheme is that, each node in the network has a specific prime number it will be taken as node identity and it cannot be changed acts as Node Identity and this identity must not be changed. Since MANET is prepared in cluster in cluster .so each node is the member of cluster .each cluster has cluster head which is responsible for finding issues in cluster. When any intermediate node/Destination Node generates RREP packet to the Source Node then it has to reply with Prime Product Number i.e. the product of prime numbers from destination node to the source node and some other information. If the information provided by node is right and prime product is fully divisible than it is called genuine node else node will be removed by PPN Schema In this paper, PPN scheme is presented in detail and evaluation of the PPN scheme as an add-on to the Ad-hoc On Demand Distance Vector Routing (AODV) protocol.

The cluster head node is responsible for maintaining the neighbor table in PPN schema. The neighbor table is used for maintaining information regarding nod for finding route .with the help of PPN Schema the intermediate node will discard path provided by nodes which provide wrong information and which are not fully divisible hence , malicious nodes will be steadily escaped by other non-malicious nodes in the network The PPN Schema trust on genuine nodes from which source node transfer data and consider them as genuine to transfer data packets. Initially source node (SN) finds secure route up to destination by broadcasting RREQ message information regarding cluster head and its prime product of all nodes from source to destination is maintained by intermediate node (IN)

In Product Number (PPN) after receiving RREP message from IN, SN with the help of its cluster head (CH) will divide the PPN with the Node IDs stored in neighbor table at CH will find that IN is trustworthy node. The information provided and prime product is fully divisible it means IN is trustworthy for SN and SN will start transmitting data from IN. else the IN is not genuine node SN will appeals as the malicious node and it will be removed and SN will not accept its RREP message.

A. Algorithm to Detect Malicious Node Attack in MANET's

Notation:

MN: malicious node N_{RREP}: RREP from an intermediate node

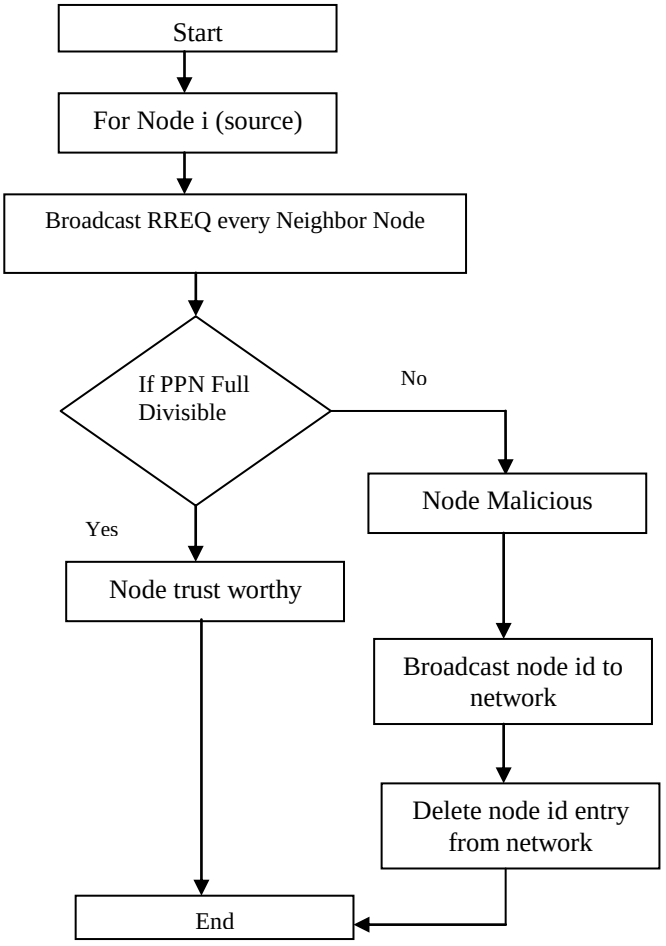
1. Begin
2. For (source node)
3. {
4. Broadcast RREQ packet to every neighbor node
5. Receive RREP
6. RREP will be choose among various reply having largest sequence number &minimum hop count and all other RREP buffered at originating node
7. Process RREP
8. }
9. If (prime product if fully divisible && replied info is right)
10. Declare node as trustworthy node
11. Else
12. {
13. Declare N_{RREP} as MN
14. Call removal of malicious node();
15. }

B. Removal Process of Malicious Nodes and Algorithm to Remove Malicious Nodes from MANET's

1) Cluster Head Node 5 adds Malicious Node M to the malicious list. Now, Node 5 broadcasts the malicious list to the whole network

2)

1. Begin
2. Respective CH adds MN to malicious node
3. Broadcast this list to the whole network
4. All nodes of the network after getting the malicious list find the node ID's of the malicious node in their table.
5. Each node flushes all the enters related to these node ID's from the respective tables
6. End



IV. EXPERIMENTAL SETUP

The algorithms performance has been observed and analyzed on the basis of result of simulation which is performed on the NS2. The NS2 framework is initially studied and then framework has been modified along with Timestamp approach in order to analyze various algorithms. Results are observed under low and high Traffic Environment.

S. No.	Parameter	Value(s)
1	Simulator used	NS 2.35
2	Simulation Time	10 sec
3	Simulation Area	1000 X 1000
4	MAC	802.11
5	Number of nodes	55
6	Speed of Nodes	2 to 16 (m/sec)
7	Mobility Model	Random Waypoint
8	Malicious Nodes	4

V. RESULT AND ANALYSIS

The analysis of Throughput with cooperative Blackhole attack and with PPN under Blackhole attack are shown in figure4 the shows that Throughput using PPN is high as compared to under Cooperative Blackhole our proposed technique the results are better.

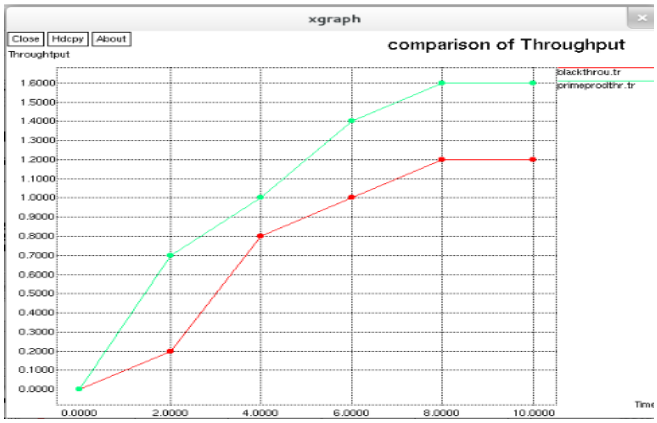


Figure4 Comparison of Throughput

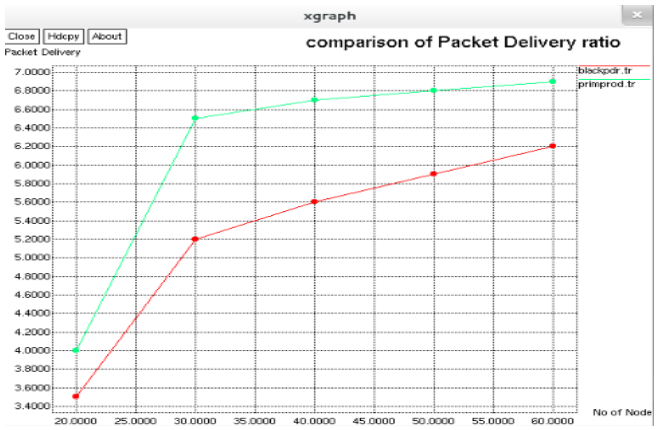


Figure5 Comparison of Packet Delivery Ratio

The analysis of Packet Delivery ratio between Cooperative blackhole Attack and PPN are shown in figure5 the shows that Delivery ratio using PPN is high as compared to cooperative blackhole attack but in our proposed technique the results are better as compared to cooperative black hole system.

VI. CONCLUSION

In this paper, for secure routing AODV with PPN a security protocol is proposed it is used for finding malicious nodes in MANET and make secure transmission form source to destination .for find misconduct behavior of nodes. The cooperative black hole attack is detected. PPN Schema is used for finding malicious nodes in network. In future the various attacks can be tested with proposed schema.

REFERNCES

[1] Sapna Gambhir, Saurabh Sharma YMCA University of Science, "PPN: Prime product number based malicious node detection scheme for MANETs", ISSN: 978-1-4673-4529-3/12/$31.00c 2012 IEEE, Volume1, Issue1, 2013

[2] Rashika Indoria, Deepak Motwani, "An Approach of Detecting Cooperative Black Hole Attack in MANET using Modified TAODV Protocol" (IJCA),Vol.129. No.12, November2015

[3] M.Sc.Ali Abdulrahman Mahmood, Dr. Taha Mohammed Hasan, M.Sc.Dhiyab Salman Ibrahim, "Modified AODV Routing Protocol to Detect the Black Hole Attack in MANET" (IJARCSSE), Volume 5, Issue 7, July 2015

[4] P. V. Venkateswara Rao, S. Pallam Setty, "Investigating the Impact of Black Hole Attack on AODV Routing Protocol in MANETS under Responsive and Non-Responsive Traffic", International Journal of Computer Applications (0975 – 8887) Volume 120 – No.22, June 2015

[5] Mr. Ramanpreet Singh, Mr. Ajay Kumar Dogra, "Performance evaluation of energy efficient modified AODV using clustering method in MANETs" (IJMCSA) Volume No.3, Issue No.1 (IJCSMC), Vol.4, Issue. 5, May 2015

[6] Swati Pokhariyal , Pradeep Kumar, "Shielding algorithm for Detection and Elimination of Black hole/Gray hole Attack in MANETs" (IJMCSA) Volume No.3, Issue No.1, January, 2015

[7] Tarek M.Mahmoud, Abdelmgeid A. Aly, Omar Makram M., "A Modified AODV Routing Protocol to Avoid Cooperative Black Hole Attack in MANETs" (IJCA), Volume 109 –No. 6, January 2015

[8] Anuj Ranaa,*, Vinay Ranab, Sandeep Gupta, "EMAODV: TECHNIQUE TO PREVENT COLLABORATIVE ATTACKS IN MANETs" 4th International Conference on Eco-friendly Computing and Communication Systems, ICECCS, 2015

[9] Sourabh Singh Vermaa*, Dr. R. B. Patelb, Dr. S. K. Lenkac, "Investigating Variable Time Flood Request Impact Over QOS in MANET" Procedia Computer Science 57 (2015) 1036 – 1041, 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015)

[10] G.Vennila, "Prevention of Co-operative Black Hole attack in MANET on DSR protocol using Cryptographic Algorithm" Volume 6 No.5, Oct 2014

[11] Ravinder Kaur, Jyoti Kalra, "Detection and Prevention of Black Hole Attack with Digital Signature" (IJARCSSE), Volume 4, Issue 8, August 2014

[12] Ms.Heena Bhalla, "PERFORMANCE ANALYSIS OF MANET BEFORE AND AFTER BLACK HOLE ATTACK", International Journal Computer Technology & Applications, Volume 3 (1), 273-276