International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Detection and Prevention of Cooperative Wormhole Attack in a MANET

Anuradha T[1], Padmashree S. Shedbalkar[2]

Department of Computer Science and Engineering, PDA College of Engineering, Gulbarga, Karnataka, India

M.Tech in Computer Science and Engineering, PDA College of Engineering, Gulbarga, Karnataka, India

Abstract: ***Mobile Ad hoc Networks (MANETs) are multi-hop, wireless, infrastructure less collection of self organizing mobile hosts that form a temporary cooperative network without the aid of any base station. Every node in the network is capable of functioning as a mobile router. Nodes are free to move arbitrarily, thus the network topology changes rapidly and randomly at unpredictable times. Because of dynamic topology nodes can enter and leave network at any time, during this, malicious nodes can enter and harms the network. So security is an essential service for wired and wireless network communication. There are many solutions to detect and prevent this attack like packet leashes, hop count analysis etc., but these methods do not provide perfect solution. In this paper a novel method has been focused on detection and prevention of the Cooperative wormhole attack using MD5 algorithm, packet filtering and implemented using AODV routing protocol. MD5 algorithm generates unique ids for all the nodes. Packet filtering and packet forwarding methods are also used for transferring the packets in secure path from source to destination. The experimental results are obtained by varying the concentration of wormhole nodes and are analyzed in terms of throughput, end to end delay and packet delivery ratio. The results demonstrate the efficiency of the proposed method.***

Keywords: MANETs, Wormhole Attack, AODV protocol, Message Digest 5(MD5)

1. Introduction

Mobile Ad hoc networks are wireless, infrastructure less, multi hop and Collection of self organizing mobile nodes that form a temporary co-operative network without the aid of any base station. There is no background network for the central control of the network operation, so control and management is distributed among the terminals. These nodes are independent and behave as both host as well as router to transfer the data. Each node in MANET has to maintain the communication range. Suppose if node moves out of range then it communicates hop by hop with the help of neighboring nodes. Due to mobility of nodes topology changes rapidly with varying time. Hence this dynamic topology nature of nodes can enter and leave the network at any time and even the malicious nodes can enter with these legitimate nodes and degrade the performance of network in terms of attacks. Here we are studying about the avoidance of wormhole attack in networks.

Wormhole Attack In wormhole attack the malicious nodes act as legitimate nodes and enter into the network due to dynamic topology. And using the address of other nodes the wormhole nodes involve in the network operation and creates the separate link between the adversaries and start transferring the data through that link is called wormhole tunnel. This wormhole tunnel connects the two nodes directly and behaves as shortest path and allows the data to enter in that path. And also it may modify the data or drop the data and never send to the particular destination. And identifying such nodes is very difficult. So wormhole attack is called as severe attack in MANETs.

2. Organization

Section 1 discusses the introduction, section 3 discusses the related work, section 4 discusses the proposed system, section 5 discusses the simulation results, and section 6 discusses the conclusion.

3. Related Work

There have been many studies in wormhole attack in MANET.

In [1] Author described the hop count and time delay analysis which is used to detect the wormhole attack by measuring the hop and time between the two nodes. Simulation has done in OPNET. In [2] Author used cluster based detection technique to identify the wormhole nodes. In [3] Author has given the overview of secure routing protocols and how these are used in MANET to transfer the data securely. In [4] Author discussed some detection and prevention methods of wormhole attack are packet leashes, sector and Delphi etc. In [5] Author declared security is important issue in MANET due to infrastructure less and autonomous. So security needs to make the routing protocol secure and to protect the data transmission by performing routing, mutual authentications, generation and secure exchange of session key. In [6] Author presented a novel threshold based algorithm for detection and prevention of cooperative black hole attack in a MANET. And performance is analyzed in terms of throughput, end to end delay and packet delivery ratio by varying the number of black hole nodes before and after the prevention of black hole attack. In [7] Author addressed some basic security concerns in MANET for wormhole attack on routing protocols. In [8] Author presented a novel trust based scheme for identifying

and isolating the wormhole nodes from the network. In [9] Author proposed a new DSR protocol to avoid the wormhole attack in MANETs. This proposed DSR protocol finds a new path to transfer the data.

The objective of the proposed paper is to avoid the wormhole nodes in MANETs by generating the unique digital signatures for all the nodes using MD5 algorithm. Performance is analyzed using three parameters throughput, Packet delivery ratio and end to end delay.

4. Proposed Work

The proposed method for detection and prevention of the cooperative wormhole attack uses AODV routing protocol. Message Digest 5(MD5) algorithm is used to generate the unique ids for all the nodes in the network. All the ids of the nodes are compared to identify the wormhole node. If two or more nodes having the identical ids are suspected as wormhole nodes. These wormhole nodes interrupt the packets from transferring. So by assigning higher transmission range to these nodes they move away from the network range and not involved in further communication. Once again route establishment phase takes place and deliver the data in secure path from source to destination.

4.1 Algorithm for Message Digest 5

Step 1: *Initialize the ip address of each node as message.*
Step 2: *The message is padded by 1 and 0. So that, its length is congruent to 448 modulo 512.*
Step 3: *A 64 bit representation of message is appended to the result of the previous step.*
Step 4: *The resulting message has a length that is an exact multiple of 512 bits.*
Step 5: *A four-word buffer (A,B,C,D) is used to compute the message digest. Here each of A,B,C,D, is a 32 bit register.*
Step 6: *These registers are initialized to the following values in hexadecimal:*

word A: 01 23 45 67
word B: 89 ab cd ef
word C: fe dc ba 98
word D: 76 54 32 10

Step 7: *Process message in 16-word blocks. Four auxiliary functions that take as input three 32-bit words and produce as output one 32-bit word.*

$F(X,Y,Z) = XY \vee not(X)\ Z$
$G(X,Y,Z) = XZ \vee Y\ not(Z)$
$H(X,Y,Z) = X\ xor\ Y\ xor\ Z$
$I(X,Y,Z) = Y\ xor\ (X \vee not(Z))$

Step 8: *The message digest produced as output, i.e, ABCD. with the low-order byte of A, and end with the high-order byte of D.*

4.2 Flow of work

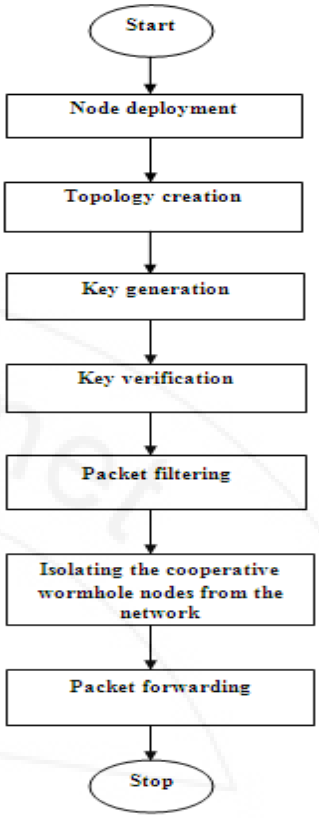

Figure 1: Architecture of the proposed system

Node deployment: Node deployment module creates the number of nodes in a particular area with a proper size.

Topology creation: This module provides the proper connection between the source and destination nodes using the routing protocols.

Key generation: Here we create unique ids for all the nodes in the network using message digest 5 algorithm.

Key verification: Key verification module checks the similar ids of all the nodes and is identified as wormhole node.

Packet filtering: Packet contains the id of current node and next hop node and is checked with the id of wormhole node every time before transmission. And if the packet contains the id of wormhole node then it stops sending the packets further else it forwards the packets to the destination.

Isolating the Co operative Wormhole nodes from the network: The nodes of mobile Ad hoc network have some coverage area called network range. Communication takes place in that network range only. These nodes are completely removed from the network range so that in future these eliminated nodes are not used in further communication.

Packet forwarding: Here once again route establishment takes place using the AODV routing protocol and finds the shortest path between the source and destination and send the data securely.

4.3 Algorithm: Detection and prevention of cooperative wormhole attack

Step 1: Let us initialize the total number of nodes as N and number of wormhole nodes as X. let S be the source node and D be the destination node.

Step 2: Input values for source and destination.

Step 3: Randomly assign the X wormhole nodes among N nodes.

Step 4: The source node S starts the route discovery phase by broadcasting the RREQ packet to all its neighboring nodes. If the neighboring nodes have the path to destination, they reply to source node S with RREP, otherwise they forward it to their neighboring nodes till the destination is reached.

Step 5: N nodes generate the unique ids using the MD5 (4.1) algorithm. If the nodes have identical ids the corresponding nodes is suspected as to be wormhole node else go to step 9.

Step 6: During data transmission, the packets are checked at all the nodes in the network. And if packet containing the id of suspected wormhole node, then wormhole node exists in that path then packet transmission is stopped.

Step 7: These detected wormhole nodes are discarded from the network range by assigning the higher transmission range. Hence these nodes not involve in further communication.

Step 8: New route discovery phase takes place after eliminating the cooperative wormhole nodes from the entire network. So that packets are transmitted from source to destination through the discovered path.

Step 9: The source node S forwards the packets to destination through the discovered path.

Step10: Compute the performance metrics namely throughput, end to end delay and packet delivery ratio.

Step11: Stop.

5. Simulation and Results

The simulation experiments are conducted using NS-2.34 simulator by using the proposed algorithm. The simulation runs for 5sec, 10sec, 15sec, 20sec and 25sec are carried out for detection and prevention of cooperative wormhole attack using MD5 algorithm and packet filtering approach is observed.

The performance is analyzed in terms of throughput, end to end delay and packet delivery ratio.

Throughput: It is the average number of packets delivered successfully per second. Fig 2 analyze the throughput for the varying number of wormhole nodes X=10%, 20%, 30%, 40% and 50% of total number of nodes N=50. Throughput degrades as number of wormhole nodes increases. And for 50% of wormhole nodes the graph shows the value zero due to unavailable of nodes (50% of total nodes are converted as wormhole nodes).

Table 1: Simulation parameters and their values

Parameters	Values
Packet size	1000 bytes
Simulator	NS-2.34
Transmission range	250mts
Number of wormholes	10%, 20%, 30% 40% and 50% of total nodes
Simulation run time	25 seconds
Number of mobile nodes	50 nodes
Topology	1000*1000(m)
Routing protocol	AODV
Traffic	Constant Bit Rate (CBR)

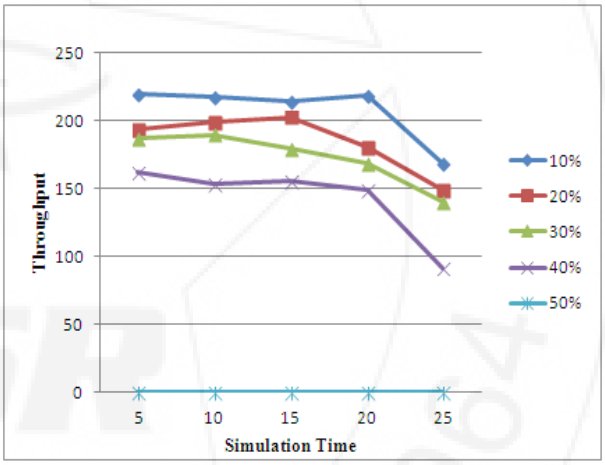

Figure 2: Throughput for varying number of wormhole nodes

End to end delay: It is the average time taken by the packet to reach the destination from the source node. Fig 3 shows the end to end delay for X=10%, 20%, 30%, 40% and 50% wormhole nodes of N=50 total nodes. And delay increases as the percentage of wormhole nodes increases. But for 50% of wormhole nodes the graph shows it is zero due to unavailable paths to transfer the data.

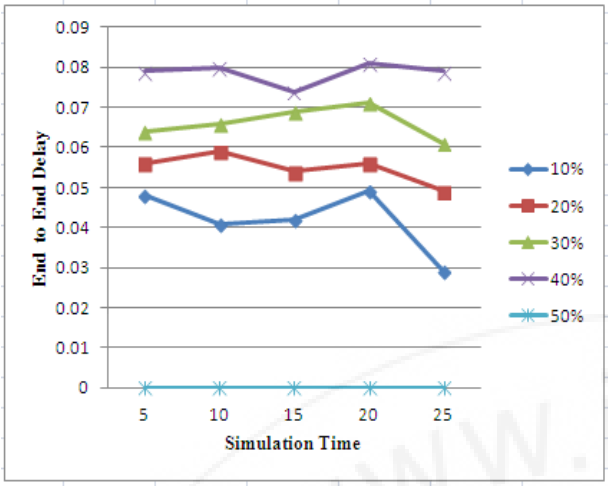

Figure 3: End to end delay for varying number of wormhole nodes

Packet delivery ratio: It is the ratio of total number of packets received successfully at the destination to the total number of packets sent by the source. Fig 4 determines the packet delivery ratio for varying number of wormhole nodes X=10%, 20%, 30%, 40% and 50% of N=50 total nodes. The graph for PDR decreases as the number of wormhole nodes increases. The graph shows it is zero for 50% of wormhole nodes due to unavailable paths to transfer the data.

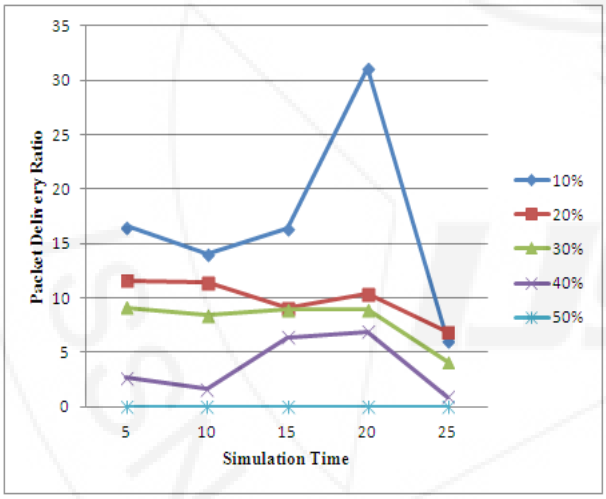

Figure 4: Packet delivery ratio for varying number of wormhole nodes

6. Conclusion

A mobile Ad hoc network (MANET) is most vulnerable for any kind of attacks. Hence a lot of security measures are required for the secured use of MANETs. In this paper, a method for detection and prevention of cooperative wormhole attack in MANETs has been proposed. The simulation experiments are carried out by varying 10%, 20%, 30%, 40% and 50% of concentration of wormhole nodes in the network and also by varying the simulation run time as 5sec, 10sec, 15sec, 20sec and 25sec. The simulation result shows that, as the concentration of wormhole nodes increases the performance of the network decreases. For evaluating the network performance three parameters PDR, throughput, and end to end delay has been used. In future work, the proposed method will be extended suitably to deal with other types of attacks in the network.

References

[1] Ajay Prakash Rai, Vineet Srivastava, Rinkoo Bhatia, “Wormhole Attack Detection in Mobile Ad Hoc Networks”, International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 2, August 2012.

[2] Amol V. Zade, Vijaya K. Shandilya, “A defense against Wormhole Attacks in Wireless Ad Hoc Networks using Cluster Technique”, Emerging Trends in Computer Science and Information Technology -2012 (ETCSIT2012).

[3] Jaspal Kumar, M. Kulkarni, Daya Gupta, “Secure Routing Protocols in Ad Hoc Networks: A Review”, Special Issue of IJCCT vol. 2 issue 2,3,4; 2010 for International Conference[ICCT-2010].

[4] Jyoti Thalor, Ms. Monika, “Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Network: A Review”, International Journal of Advanced Research in Computer Science and Software Engineering. Volume 3, Issue 2, Feb 2013.

[5] Kartik Kumar Srivastava, Avinash Tripathi, Anjnesh Kumar Tiwari, “Secure Data Transmission in MANET Routing Protocol”, Kartik Kumar Srivastava et al, Int.J. Computer Technology & Applications, Vol 3(6), 1915-1921. IJCTA, Nov-Dec 2012.

[6] P.S.Hiremath, Anuradha T, “Detection and Prevention of Cooperative Black Hole Attack in a MANET”, International Journal of Research in Computer and Communication Technology, Vol 3, Issue 5, May-2014.

[7] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar, Bhavin I. Shah, “MANET Routing Protocols and Wormhole Attack against AODV”, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010.

[8] Shalini Jain, Dr. Satbir Jain, “Detection and prevention of Wormhole Attack in Mobile Ad Hoc Networks”, International Journal of Computer Theory and Engineering, Vol 2, No. 1 February, 2010.

[9] Yudhvir Singh, Avni Khatkar, Prabha Rani, Deepika, Dheer Dhwaj Barak, “Wormhole Attack Avoidance Technique in Mobile Ad Hoc Networks”, UIET, MD University, Rohtak, India. 2013 Third International Conference on Advanced and Communication Technologies.