Detection of Hidden Tunnel Attack in Mobile Ad-Hoc Network

Mahendra Dhole[1], Anand Gadwal[2]

[1]Department of Computer Science & Engineering, M.Tech, TCET Indore, M.P., India

[2]Department of Computer Science & Engineering, Professor, TCET Indore, M.P., India

Abstract: ***Mobile ad-hoc network is an infrastructure less and self-organizing concept of network organization. Due to the ad-hoc environment of network there are various security and safety issues arises in the network such as routing security issue and data forwarding security issue. These security issues decrease the network performance in terms of throughput and other performance parameters like packet delivery ratio and routing overhead. The security of network resources is breaches by the malicious nodes which may moreover internal or external. Malicious nodes influence the network working by putting the numerous kinds of attacks. This work proposed a technique to detect wormhole attack which played via malicious node. To detect the malicious node or attacker various scheme have advised by researches which focus round trip time of packet. The advised schemes DelPHI and Packet Travel Time have some drawbacks like reliability, message overhead, and delay. This particular work is proposed to resolve the drawbacks of these schemes by evaluating the performance parameters of network.***

Keywords: Mobile ad-hoc network, security, malicious nodes, wormhole attack, round trip time

1. Introduction

Mobile ad hoc network is an infrastructure less network is not having any steady infrastructure for the communication and it is dynamic in nature. Each node in that type of network can communicate directly with other nodes in the network and there is no necessity of any centralized network access point. A significant thing about these types of networks is that these networks are not having any routers but the wireless nodes work as a routers and a host. These networks don’t have any static or fixed topology.

Wireless mobile ad hoc network has mobile nodes that use wireless transmission to communicate. In these types of networks the nodes are movable and the motion of nodes might be random or periodical .With node mobility nature of nodes, the nodes contain limited battery power & limited bandwidth. In nonappearance of centralized access point or administrator the source & destination communicate via multiple hops. The MANET is also known as a multi hop wireless network. It is an autonomous collection of mobile nodes or users.

1.1 Security Principles

In MANET, each and every networking functions such as routing and packet forwarding, are execute by nodes themselves in a self-organizing manner. Security includes a group of investments that are sufficiently funded. In favor of these reasons, securing a mobile ad -hoc network is extremely challenging. The goals to check if mobile ad-hoc network is secure or not are as follows:

1.1.1 Availability

Availability means sharing information so as to make sure consistency among redundant resources. Data replication has been broadly used to improve data availability in distributed systems, and we will apply this method to MANETs. By replicating data on mobile nodes which are not the owners of the original data, data availability can be enhanced because there are several replicas in the network and the possibility of finding one copy of the data is higher.

1.1.2 Confidentiality

Confidentiality is occasionally called secrecy or privacy. MANET uses an unlock medium, so usually all nodes inside the direct transmission range can get the data. One method to maintain information confidential is to encrypt the data, and another procedure is to use directional antennas. It also means that the transmitted data can simply be accessed by the anticipated receivers.

1.1.3 Integrity

Integrity assures that a message being passed is never corrupted. The integrity utility can be provided using cryptography hash function along with some type of encryption. When trading with network safety the integrity service is often provided implicitly by the authentication service.

1.1.4 Authentication

Authentication is basically a process carried out by two parties in order to recognize one another. Without authentication, an unauthorized node could effortlessly “come in” and use the existing resources within the network. The Problem gets of inferior quality if the unauthorized node be a malicious user. So, it is necessary to have a method for preventing an “outsider” from being element of the network.

1.1.5 Non repudiation

Non repudiation means that parties can confirm the transmission or reception of information with another party, i.e. a party cannot falsely deny having received or sent certain data. By producing a signature used for the message, the entity cannot later on deny the message. In public key cryptography, a node A signs the message by means of its private key. All the other nodes can verify the signed message by using A's public key, and A is not deny that its signature is attached to the message.

1.1.6 Anonymity

Anonymity means all the information that can be used to recognize owner or present user of node should default be kept private and not be distributed by node itself or the system software. It provides the all probable information that can be used to identify the vendor.

1.1.7 Authorization

Authorization is used to allocate different access rights to different rank of users. This property assigns dissimilar access rights to different types of users. For example a network management can be performed by network administrator only. Authorization is a procedure in which an entity is issued a credential which privileges and permissions it has and cannot falsify by the certificate authority.

1.2 Weakness

Weakness in security system is also called vulnerability. An ad hoc technique may be vulnerable to illegal access because the system is not verify a user's identity ahead of allowing data access. Wireless mobile ad hoc network is extra vulnerable than wired network. Some of the vulnerabilities or weaknesses are given below:

1.2.1 Absence of centralized management: Wireless mobile ad hoc network is not having any centralized check or management server or node. The nonexistence of centralized management makes difficult to discover any type of attacks because it is not easy to monitor and manage the traffic in an extremely dynamic and large scale MANET.

1.2.2 Scalability: With the mobility of nodes, network topology of ad-hoc network altering all the time. That's why in MANET scalability is a main issue concerning security. Security mechanism must be able of handling a large network as well as minor ones.

1.2.3 Cooperativeness: Routing algorithm for mobile ad hoc networks generally assumes that nodes are cooperative and non-malicious. It results to a malicious attacker which can effortlessly become a main routing agent and disrupt network operation by disobeying the protocol conditions and specifications.

1.3 Wormhole Attack

Mobile ad hoc networks are open to many of the attacks due to many reasons such as wireless links between nodes, insufficiency in infrastructure, nonexistence of centralized monitor or management, limited physical Protection, and the resource constraints. A particularly security attacks called as wormhole attack or hidden tunnel attack is utilized in the ad-hoc networks [1, 4, 5]. One malicious node captures packets from one place in the network and tunnels the captured packets to another malicious node at another place as shown in the Figure 1, which replays them locally.

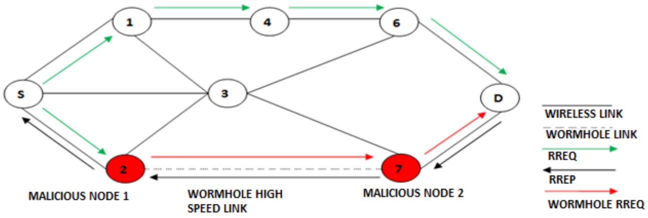

Figure 1: Wormhole Attack in Ad Hoc Network

2. Related Work

The applications of MANET range from simple wireless home and office networking. Security aspects play an important role in all of these application scenarios given the vulnerabilities inherent in wireless ad hoc networking from the very fact that radio communication takes place. The above research work contents a related work, which can cover dimensions of study.

Wormhole attack is one of the significant attacks which create a serious threat in the wireless networks, especially for location- based wireless security systems and ad hoc wireless routing protocols. H. S. Chiu and K. S. Lui [3] proposed a method for detection of wormhole attack called Delay per Hop Indication (DelPHI). The sender is capable to detect both kinds of wormhole attacks by discovering the delays of different paths to the receiver. This method does not requires synchronized clocks or special hardware furnish mobile nodes. The result analysis of the DelPHI has been examined by simulations. The result of simulation shows that DelPHI has gain greater than 95% in detecting normal path and gain greater than 90% in detecting wormhole attack, in the absence of background traffic. The result of simulations has also shown that DelPHI can gain greater than 85% detection rate for both normal and tunneled paths with the background traffic. The problem of message overhead is the limitation of DelPHI which is also addressed in this paper.

A. S. Alshamrani [2] proposed a detection and prevention method called Packet Travel Time algorithm for MANET. This mechanism initially uses the same process of calculating the RTT's (round trip time) which are used in transmission time mechanism (TTM) among two successive nodes. Furthermore it monitors all of the transmitted packets in the network. After forwarding the RREQ packet, each and every node records the sending time (ts) and save sending time (ts) values in memory and the time when it overhears its neighbor rebroadcast the RREQ packet (th). Furthermore each node compute the PTT value with (PTT=th-ts) and each node save the PTT value until it receives the RREP and append PTT value in the particular part which is formed by the destination. When source node receives the RREP, it calculates the RTT between every two successive nodes by the similar process that has been discussed in TTM and then these values has compared with the values of PTT's and locate if there is any wormhole link in the route. Table 1 shows the sending and receiving time values of all nodes received by source node and the calculation done by the source node.

Table 1: Sending and Receiving Time Values of all Nodes

NODES	*RREQ Sending Time*	*RREP Receiving Time*	*Calculation done by source node*
S	0	32.5	32.5
A	1.5	31	29.5
W1	6.5	29.5	23
W2	12	24.5	12.5
B	13.5	19.5	6
C	15	18	3

RTT's between nodes are:

```
RTT's:            3        6.5        10.5         6.5        3
NODES:      S---------A---------W1----------W2---------B----------C
```

The value of PTT's received at source node shown in Table 2.

Table 2: Values of PTT's at Source Node

NODES	*RREQ Sending Time*	*RREP Overhearing Time*	*PTT'S*
S	0	1.5	1.5-0=1.5
A	1.5	6.5	6.5-1.5=5
W1	6.5	12	12-6.5=5.5
W2	12	13.5	13.5-12=1.5
B	13.5	15	15-13.5=1.5
C	15	-	-

3. Problem Statement

Security is the main issue in Mobile Ad Hoc Network when data transmission is performed inside un-trusted wireless network. Black hole, Wormhole, Gray hole and lots of attacks have been identified and solutions for these attacks have been proposed. Wormhole attack is more harmful attack because two or more malicious nodes generate a virtual tunnel in the network. Researcher's had proposed many solution for wormhole attacks, but the existing methods have some drawbacks like reliability and routing overhead.

The mechanism DelPHI [3], able to tackle both of the wormhole attacks by computing delay or hop value to provide as the pointer of detecting wormhole attacks. The DelPHI scheme avoids the requirement of synchronization and it does not need any special hardware therefore it provides high power efficiency but it has several drawbacks such as, reliability and message overhead and in the case where all of the paths are tunneled, this method is not supportive.

The another method PTT (Packet Travel Time) algorithm in mobile ad-hoc networks [2], also able to tackle both the wormhole attacks by calculating RTT (Round Trip Time) between two successive nodes and PTT(Packet Travel Time), but this mechanism also have some drawbacks.

1) requires clock synchronization
2) calculating RTT of two successive nodes
3) Observe the RREQ packet forwarding of its neighbours for calculating PTT.

All type of communication or say data transmission in MANET is based on mutual trust between the participating nodes. Due to dynamic topology and lack of centralized monitoring, MANETs are vulnerable to various security attacks. Hence, obtaining a secure and trustworthy path in MANET is still a real challenge.

The main objective of this research work is to find secure and trustworthy path for data transmission in MANET which is free from wormhole attack. This research also overcomes the problems of existing methods like reliability, requirement of clock synchronization and routing overhead.

4. Proposed Methodology

The proposed solution is given for detection of wormhole attack in MANET. The proposed algorithm based on the concept in which the node broadcast route request packet to all its neighbor nodes. Then it calculates the delay between two nodes and transmission power of neighbor node. If transmission delay and transmission power are maximum then the node is suspicious, otherwise the node is normal. The suspicious path is eliminated in route discovery process for data transmission in the network.

4.1 Algorithm of Proposed Solution

```
Algo dworm (N,i)
{
Declare Td, Tp, Flag=0, RTT, Pr , r ; //Td Transmission
Delay between two hops, Tp Transmission Power, RTT
Round Trip Time, Pr Radiant Power and r Radius.
   Repeat i=1 to N
   {
      node [i] → (RREQ, node [i+1]);
      //Calculate Td, Tp
      Td [i] = RTTi – RTTi+2 ;
      Tp [i] = Pr / 4πr2
       if (Td [i] > Td [i+1] and Tp [i] > Tp [i+1] ;
        {
          Flag = 1;
        }
        Else
       {
          Flag = 0;
        }
    }
        if (Flag = = 1)
        {
        Node is malicious;
         }
         Else
        {
         Node is normal;
         }
         Go to step 1;
  }
```

4.2 Flow chart of algorithm

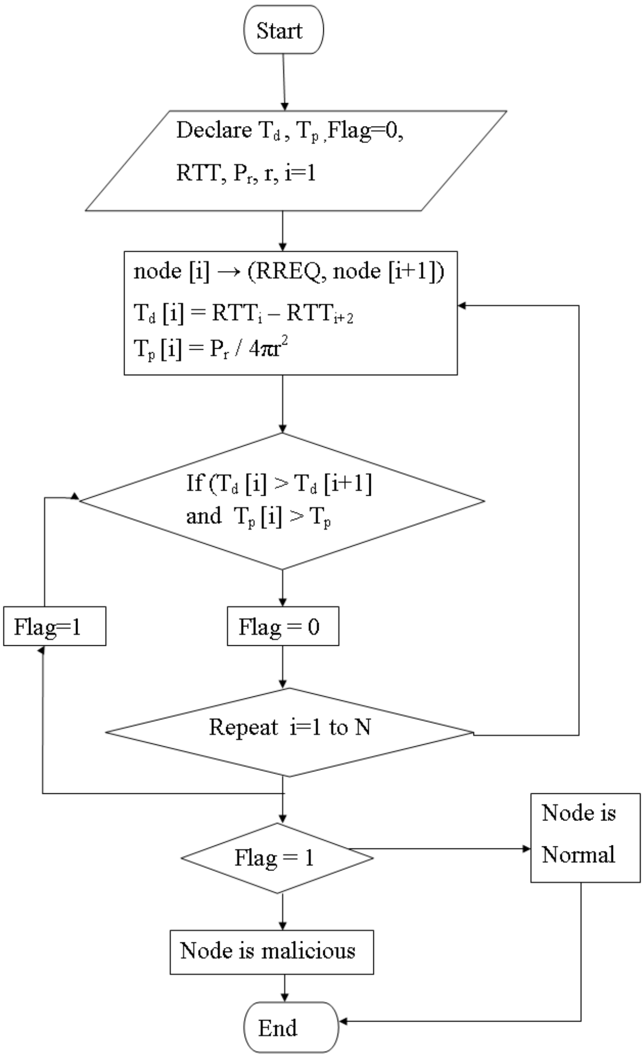
Start
Declare T_d, T_p, Flag=0,
RTT, P_r, r, i=1
node [i] → (RREQ, node [i+1])
T_d [i] = $RTT_i - RTT_{i+2}$
T_p [i] = $P_r / 4\pi r^2$
If (T_d [i] > T_d [i+1]
and T_p [i] > T_p
Flag=1
Flag = 0
Repeat i=1 to N
Flag = 1
Node is Normal
Node is malicious
End

Figure 2: Flow chart

This algorithm is used in simulation to detect the wormhole attack due to the malicious node. And this algorithm is reliable because it works against wormhole attack and used to detect attack. This particular algorithm does not require clock synchronization and it calculates round trip time of each & every node. So that it can increase the performance of the network considering evaluation parameters such as packet delivery ratio, throughput, and routing overhead.

5. Simulation

5.1 Tools Used

Network Simulator-2: Aim of network simulator 2 (NS2) is to support research and education in networking field. Network simulator 2 (NS2) is develop using object oriented language object oriented variant of Tool Command Language (OTCL) and C++. Results are obtained by trace files of Network simulator 2 have to be processed further by another tools like Network Animator (NAM), AWK, PERL script etc.

5.2 Simulation Parameters

To prepare simulation for desired network utility the following given simulation parameters are considered.

Table 3: Simulation Parameters

Radio-propagation	Propagation/TwoRayGround
Antenna model	Antenna/OmniAntenna
Routing protocol	AODV
Simulation dimension	750 X 550
Initial energy in Joules	100
Simulation time	100 seconds
Traffic	TCP
Channel type	Channel/Wireless Channel
Number of nodes	35
Queue Size	50
Packet Size	512 bytes

5.3 Simulation Scenario

Simulation has done considering three network scenario. The first is normal scenario in which every node of network behaves normal. Second one is worm scenario in which malicious nodes take wormhole attack. Last is proposed network scenario in which malicious node is detected. The following figures show nam window of network scenario. Figure 3 shows the network animator window which is also called as simulation window in which source and destination nodes are identified. And the circles which are spreading over the various nodes are the transmission range. This network animator window has a feature to see it in many ways like play, pause, forward, fast forward etc.

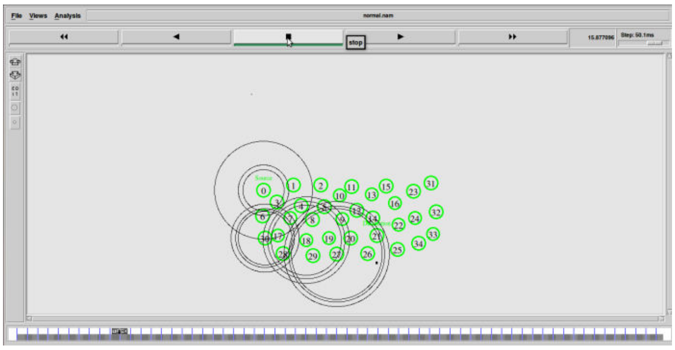

Figure 3: nam window show data transmission in network scenario

6. Result Analysis

This chapter presents results of proposed approach and comparison. Proposed approach play important role in ad-hoc network security to find malicious node with minimization of packet drop ratio. Reliability and throughput of network is enhanced as result of this approach. The results of proposed approach are analyzed on the basis of various network parameters. Result analysis deals with obtaining the results of each scenario which created in this work such as normal, attack, proposed scenario etc.

http://dx.doi.org/10.21275/v5i6.NOV164827

6.1 Result Parameters

The proposed approach result consider following network key parameters:
6.1.1 Packet Delivery Ratio
6.1.2 Throughput
6.1.3 Routing Overhead

6.1.1 Packet Delivery Ratio

Packet delivery ratio (PDR) calculated by total number of received packet divided by total number of sent packet. Figure 4 is the Xgraph which shows the packet delivery ratio with respect to the time in seconds. From the result we can see that packet delivery ratio of normal scenario is higher and it gets little bit lower in proposed scenario scheme and in the worm scenario it firstly gets more lower then little bit upper which shows the decrement.

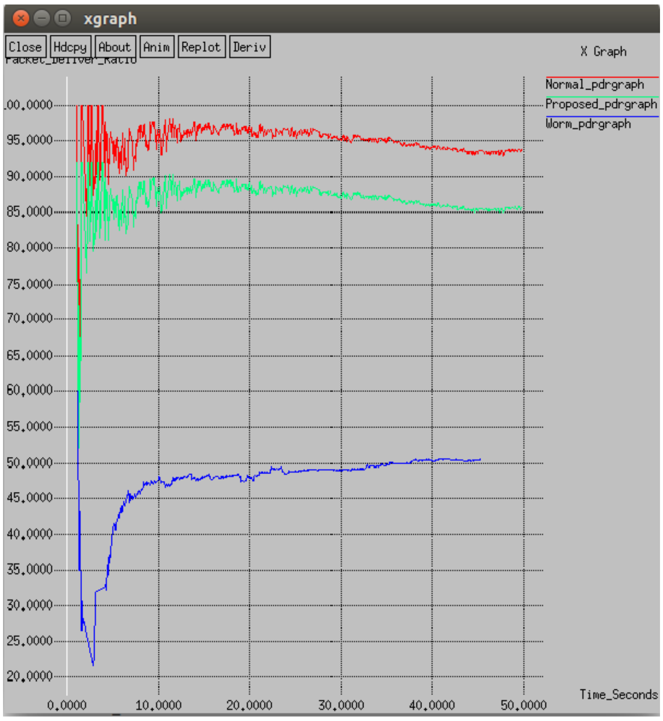

Figure 4: Packet delivery ratio

6.1.2 Throughput

The throughput is determined by the successful received packet at per unit time. It is measured in bits, bytes or packets per seconds. Figure 5 is the representation of Xgraph which presents the throughput which is in packets per second with respect to the time in seconds. From the result we can see that throughput shown in normal scenario is higher and it gets little bit reduced in proposed scenario scheme and in the worm scenario it gets more lower which shows the decrement in throughput.

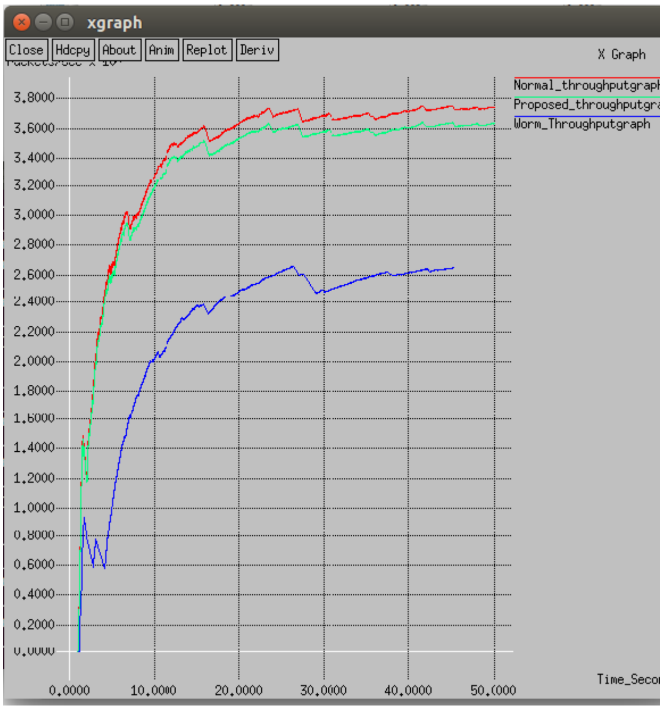

Figure 5: Throughput Graph

6.1.3 Routing Overhead

Routing Overhead is determined by the number of routing packets traversed in the network during route discovery. It is measured in packets per flow or session. Figure 6 presents the Xgraph of Routing Overhead which is in number of routing packets with respect to the time in seconds. From the result we can see that the number of routing packets shown in normal scenario is higher and it gets little bit reduced in proposed scenario scheme but in the worm scenario it gets little lower in the starting and then remains constant.

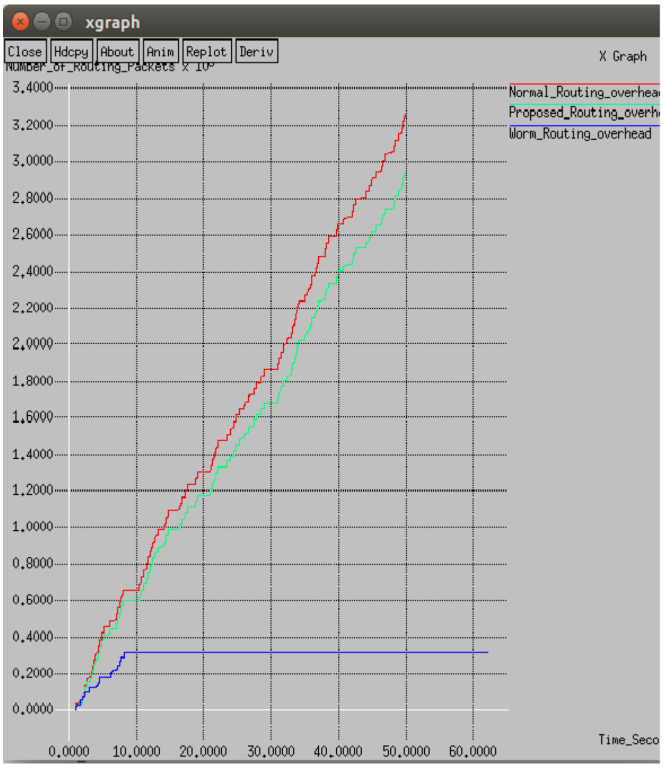

Figure 6: Routing Overhead

7. Conclusion

Wormhole attacks can degrade network performance significantly in ad hoc network and harms the network security. Wormhole attacks detection is quite complicated. This work, describes types of security attacks. After describing security attacks, the existing wormhole detection techniques are discussed. Finally, by analyzing the advantages and disadvantages of all the existing techniques, a technique to detect wormhole attack in ad hoc networks has been proposed. The proposed technique is simulated using NS-2 (Network Simulator-2) by considering different simulation parameters like number of nodes, traffic type, topography, connection type and energy of nodes. The performance of proposed techniques is evaluated by results of simulation considering evaluation parameters such as packet delivery ratio, throughput and routing overhead. Result shows that performance of these network parameters is improved up to certain level.

8. Limitations and Future Scope

Proposed approach limited to only detect hidden tunnel variants of wormhole attack instead of prevention. Remaining variants of wormhole attack does not handle by this. It is also implemented in only reactive routing strategy. Proposed approach is only able to detect attack rather than prevention. It has high computation overheads. In future, other kinds of wormhole attacks also can be focused such as exposed, high transmission power etc. considering other different routing protocols. Furthermore prevention approach will be focused against of wormhole attack.

References

[1] Pallavi Sharma, Aditya Trivedi, “An Approach to Defend Against Wormhole Attacks in Ad Hoc Network using Digital Signature”. IEEE ISSN 978-1-61284-486-2/2011.
[2] A. S. Alshamrani, “PTT: Packet Travel Time Algorithm in Mobile Ad Hoc Networks”, IEEE, 2011.
[3] H. S. Chiu and K. S. Lui, “DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks”, IEEE, 2013.
[4] 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.
[5] E. A. Mary Anita, V. Thulasi Bai, “Defending Against Wormhole Attacks in Multicast Routing Protocols for Mobile Ad Hoc Networks” 978-1-4577-0787-2/2011 IEEE.
[6] M. Azer, S. E. Kassas and M. E. Soudani, “A Full Image of the Wormhole Attacks towards Introducing Complex Wormhole Attacks In wireless Ad Hoc Networks”, International Journal of Computer Science and Information Security, vol. 1, no. 1, May 2009.
[7] Xiaomeng Ban, Rik Sarkar, Jie Gao, “Local Connectivity Test to Identify Wormholes in Wireless Networks” ACM 978-1-4503-0722-2/11/05. May 2011.
[8] R. S. Khinwar, A. Jain, J. P. Tyagi, Dec 2011,”Elimination of Wormhole Attacker Node MANAT Using Performance Evaluation Multipath Algorithm” International Journal of Engineering and Technology and Advanced Engineering, Volume 1, Issue 2, Pp. 40-47.
[9] Sunil Taneja, Ashwani Kush, “ A Survey of Routing Protocols in Mobile Ad Hoc networks” International Journal of Innovation Management and Technology, Vol.1 August 2010, ISSN 2010-0248.
[10] Shishir k. Shandilya, Sunita sahu, “A trust based security scheme for rreq flooding attackin manet”, international journal of computer applications (0975 – 8887)volume 5– no.12, august 2010
[11] Neha Singh, Sumit chaudhary, Kapil kumar verma, “Explicit query based detection and preventiontechniques for ddos in manet”, international journal of computer applications (0975 – 8887) volume 53– no.2, september 2012
[12] Jakob Eriksson, Shrikant V. Krishnamurty and Michalis Faloutsos 2006, “True link: A Practical Countermeasure to the Wormhole Attack in Wireless Networks” 14th IEEE International Conference on Network Protocols pp. 75-84.
[13] Ankita Gupta, Sanjay Prakash Ranga, 2012 “WORMHOLE DETECTION METHODS IN MANAT” International Journal of Enterprise Computing and Business System.
[14] T. Sakthivel, R. M. Chandrasekaran, 2012 “Detection and Prevention of Wormhole Attacks in MANATs Using Path Tracing Approach” European Journal of Scientific Research ISSN 1450-216X Vol.76 No.2 (2012), pp.240-252.
[15] Aarti and Dr. S. S. Tyagi, “Study of MANET: Characteristics, Challenges, Application and Security Attacks”, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 5, May 2013.
[16] V. Singla, A. Kumar and R. Singla, “CBR and TCP based Performance Comparison of Various Protocols of MANET: A Review”, National Journal on Advances in Computing and Management, vol. 1, no. 2, October 2010.
[17] R. H. Cheng, T. K. Wu and C. W. Yu, “Highly Topology Adaptable Ad Hoc `Routing Protocol with Complementary Preemptive Link Breaking Avoidance and Path Shorting Mechanisms”, Springer, 2010.
[18] A. Hinds, M. Ngulube, S. Zhu and H. A. Aqrabi, “A Review of Routing Protocols for Mobile Ad-Hoc Networks (MANET)”, International Journal of Information and Education Technology, vol. 3, no. 1, February 2013.
[19] G. K. Patnaik and M. M. Gore, “Trustworthy Path Discovery in MANET - A Message Oriented Cross-correlation Approach”, IEEE, 2011.
[20] Saurabh Gupta, Subrat Kar, S. Dharmaraja, “WHOP: Wormhole Attack Detection Protocol Using Hound Packet” 978-1-4577-0314-0/2011 IEEE.
[21] Rajbir Kaur, M. S. Gaur, V. Laxmi, “A Novel Attack Model Simulation in DSDV Routing” 978-1-4244-8704-2 IEEE 2011.

[22] Y. C. Hu, A. Perrig and D. B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", IEEE, 2003.

[23] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", Network and Distributed System Security Symposium, San Diego, California, USA, February 2004.

[24] T. V. Phuong, N. T. Canh, Y. K. Lee, S. Lee and H. Lee, "Transmission Time Based Mechanism to Detect Attacks", IEEE, 2007.

[25] Radhika Saini, Manju Khari, "Defining Malicious Behavior of a Node and its Defensive Methods in Ad Hoc Network" International Journal of Computer Applications (0975-8887) Volume 20-No.4, April 2011.

Author Profile

Mahendra Dhole received his B.E. degree in Computer Science from RGPV University and Vikrant Institute of Technology and Management, Indore, India, in 2013. Now he is persuing in M.Tech. Final Semester in Computer Science from RGPV University and TRUBA Collage of Engineering and Technology, Indore, India and his Research topic is "Detection of Hidden Tunnel Attack in Mobile Ad Hoc Networks". His other research interests include Software and Web Development and Data Mining techniques.