Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 9, Issue. 5, May 2020, pg.175 – 180

Detecting and Avoiding Wormhole Attack in Wireless Adhoc Network using Improved DELPHI

Deepinder Kaur Punia; Er. Sukhpreet Kaur
CSE Department; Assistant Professor, CSE Department
Shri Guru Granth Sahib World University, India

ABSTRACT: The MANETs (Mobile Ad Hoc Network) refers to a multi-hop packet based upon wireless network that does not require any fixed infrastructure. Each node in the network act as the base station and the packets are forwarded to the required destination. Many kinds of attack can be done on this type of networks. In this paper we have described a method to detect the wormhole attack and to secure the path of the packets from these types of attacks using delay per hop method. Wormhole attack is a dangerous attack occurring in the routing protocols in the network layer. Using hop count method we isolate the node that is the cause of the wormhole attack in the network. This method neither used the synchronized clocks nor the special kind of hardware for detecting the wormhole. In this paper will help to pinpoint the malicious node and to isolate that node from the network. The performance of the network is improved.
Keywords: MANETs, Wormhole Attack, DELPHI, WGDD.

1. INTRODUCTION TO MANETS

A mobile ad hoc network (MANET) is a self-configuring, infrastructure-less network of mobile devices connected without wires. Ad hoc is Latin and means "for this purpose". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology. A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission. Some MANET are restricted to a local area of wireless devices such as group if laptop computers while, others may be connected to the internet [3].

2. WORMHOLE ATTACKS

Network layer in MANET uses ad hoc routing and does packet forwarding. In MANET nodes act as host and router. Therefore router discovery and router maintains in the MANET is effectively concern. Thus attacking on MANET routing protocol not only disrupt the communication on the network even worst it paralyzed the whole communication all over the network. Therefore, a security in network layer plays a vital role to ensure the secure data communication in the network [11]. In wormhole attack, a tunnel is created between two nodes that can be used to secretly transmit packets. In a wormhole attack, an attacker receives packets at one point in the network, tunnels them to another point in the network and then replays them into the network from that point. The wormhole attack is particularly a serious type of attack in ad hoc network. Routing protocols in which the nodes that does a packet transmission directly from some node consider themselves to be in range of (a neighbor of) that node. For example, when used against an on demand routing protocol such as DSR or AODV, a powerful application of the wormhole attack can be mounted by tunneling each ROUTE REQUEST packet directly to the destination target node of the REQUEST. When the destination node's neighbors hear this REQUEST packet, they will follow normal routing protocol processing to rebroadcast that copy of the REQUEST and then discard without processing all other received ROUTE REQUEST packets originating from this same Route Discovery.

© 2020, IJCSMC All Rights Reserved

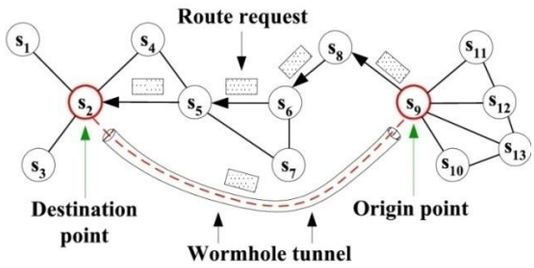


Fig 1. Wormhole Attack [11]

2.1 WORMHOLE ATTACK MODEL

Wormhole is classified into three types: closed, half open and open. Depending upon whether the type of attackers are visible on the route, packet forwarding behavior of wormhole nodes as well as their tendency to hide and show their identities.

2.1.1 Open Wormhole

In this mode, the attackers include themselves in the packet header. Nodes in network are aware of the malicious nodes present in the path but they would imitate that the malicious nodes are direct neighbors and the distance to be covered in less.

2.1.2 Half Open Wormhole

In this mode, they simply tunnel the packet form one side of wormhole to another side and it rebroadcasts the packet. The attacker node do not modifies the content of the data packet.

2.1.3 Close Wormhole

In this scenario both the source and destination feel themselves just one hop away from each other. Thus they will act as fake neighbours.

2.2 TYPES OF WORMHOLE ATTACKS

Wormhole attacks can be classified based on implementation technique used for launching it and also on the number of nodes involved in establishing wormhole. The wormhole attacks are divided into the following types.

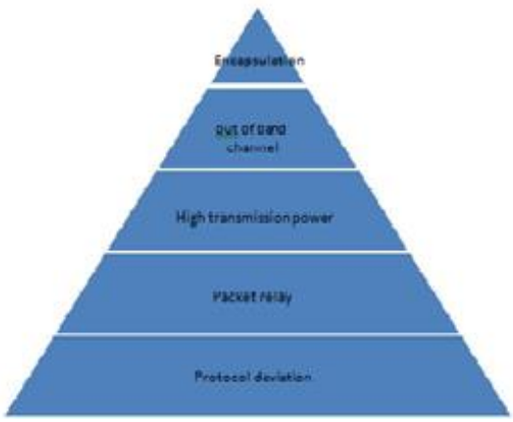


Fig 2. Description of Wormhole Attack Modes[12]

2.2.1 Wormhole using Packet Encapsulation

In this type of attack, the packets are encapsulated are sent between the malicious nodes. There exist a no of nodes between the two malicious nodes. This method prevents nodes from discovering paths that are more than two hops away.

2.2.2 Wormhole Using High Quality/Out of Band Channel

In this mode, the wormhole attack is launched by having a high quality, single hop, out of band link (called tunnel) between the malicious nodes. This tunnel can be achieved, for example, by using a direct wired link or a long range directional wireless link. This mode of attack is more difficult to launch than the packet encapsulation method since it needs specialized hardware capability. It is the attack which requires a hardware guide to connect two colluding nodes [12].

2.2.3 Wormhole Using High Power Transmission Capability

Is the method that uses the high power transmission capability in the network and with the help of these nodes communication can take place between the normal nodes from a long distance. It works as when a malicious node receives an RREQ, it broadcast the request at high power level. The node that is capable of hearing the high power broadcast it rebroadcasts the RREQ, towards the destination using this method, the malicious node increases its chance to be in the route established between the source and the destination even without the participation of another malicious node.

2.2.4 Wormhole Using Packet Relay

This type of wormhole attacks can be launched by one or more malicious nodes and this particular node also relays data packets of two distant nodes to convince them that they are neighbors. In literature this type of attack is also called “replay based attack”.

2.2.5 Wormhole Using Protocol Distortion

In this mode of attack is called “rushing attack” in literature. The routing protocols that are based on the shortest delay' instead of the 'smallest hop count' are at the risk of wormhole attacks by using protocol distortion. This mode of attack works on the fact that request forwarding is done by broadcasting and hence, reducing the MAC layer collision is important.

© 2020, IJCSMC All Rights Reserved

3. LITERATURE REVIEW

This section represents the various methods to detect and remove wormhole attack used by the various authors.

Ravinder .E, Vinaya Datt V Kohir and V.D Mytri, [3] in 2011, in this paper the authors have proposed a new Algorithm which introduces a mechanism of link failure prediction and accordingly perform a rapid local route repair. Simulation results shows that a new algorithm reduces end-to-end delay and packet dropping rate and increases packet delivery rate. AODV takes too much time to rebuild the route after a link break along the active route is broken. This time is too long for some application, such as the real time services of voice and video. The route rebuild time can be reduced if to reduce the recommended HELLO interval.

Rashmi Vijaywargiya, Prof. Kamlesh Chopra [4] in ,2009, In this paper the authors gave the survey analysis of various methods to detect the wormhole attack in MANET. Wormhole generally possess two properties In this paper we have studied the wormhole attack along with its properties and various method have been discussed for identification, removal, and prevention of wormhole attack and then they have been compared to one another so that effective methods should come forward . This study aims to combine some methods or to modify the one.

Chiu et al [5] in 2006 introduce a simple delay analysis approach, DelPHI, which calculates the mean value of the delay per hop for every possible route, based on sender initiation of detection packets, such as route requests (RREQ) and response by the receiver to every received detection packet. After collecting all responses, the sender computes the mean value of the delay per hop for each packet, with the assumption that a wormhole would have more hops than its hop count would indicate. The scheme then analyzes computed delays to determine if there is a large difference between any two of the values. As this scheme does not employ any confidentiality or authentication service, an attacker can easily deceive the sender.

Hu, Y.-C [6] in 2006 introduced a packet leash is an approach in which some information is added to restrict the maximum transmission distance of packet. There are two types of packet leashes: geographic leash and temporal leash. In geographic leash, when a node A sends a packet to another node B, the node must include its location information and sending time into the packet. B can estimate the distance between them. The geographic leash computes an upper bound on the distance, whereas the temporal leash ensures that a packet has an upper bound on its lifetime. In temporal leashes, all nodes must have tight time synchronization. The maximum difference between any two nodes' clocks is bounded by Δ, and this value should be known to all the nodes. By using metrics, each node checks the expiration time in the packet and determine whether or not wormhole attacks have occurred. If a packet receiving time exceed the expiration time, the packet is discarded.

Vrutik shah, and Dr.Nilesh Modi [10] in 2014 in this paper the author the recent advancement in the wireless technology and their wide-spread development have made remarkable enhancement in efficiency in the corporate and industrial and military sectors. The increasing popularity and usage of wireless technology is created a need for more secure wireless Ad hoc network. This paper aims and developed a new protocol that prevent wormhole attack as an Anti-worm protocol which is based on responsive parameters, that does not require as a significant amount of specialized equipment, trick clock synchronization, no GPS dependencies countermeasures.

Y.Xu [9] in 2007, In this paper the author proposes a distributed wormhole detection algorithm for wireless sensor networks, a potential technology for infrastructure of many applications. Currently, most sensor networks assume they will be deployed in a benign environment; however, when a sensor network is deployed in some hostile environment, attack (especially those like wormhole attacks that don't need to capture the keys used in the network) sensor may affect current sensor network and may even disable their functions. This paper proposes a distributed wormhole detection algorithm called Wormhole Geographic Distributed Detection (WGDD), that is based on detecting disorder of the networks which is caused by th existence of a wormhole inside the network. Since wormhole attack are passive, this algorithm uses a hop-counting technique as a probe procedure to detect wormhole attacks, then reconstructs local maps in each node, and after that, uses a feature called "diameter" to detect abnormalities caused by wormholes. The main advantage of using a distributed wormhole detection algorithm is that such an algorithm can provide the approximate location of a wormhole, which may be useful information for further defense mechanisms. Simulation Show that the proposed detection method has both a low False Toleration Rate (FTR) and a low False Detection Rate (FDR) in detection wormhole attacks.

Mohan Seth [9] in 2013 in this thesis the author studied about the Wormhole attacks that can destabilize or disable wireless sensor networks. In a typical wormhole attack, the attacker receives packets at one point in the network, forwards them through a wired or wireless link with less latency than the network links, and relays them to another point in the network. This paper describes a wormhole detection algorithm for wireless sensor networks, which detects wormholes based on the distortions they create in a network. There are two characteristics to keep tracks of all its neighboring nodes and checks if a node received is from its neighbor or not. The main advantage of the algorithm is that it can provide the approximate location of wormholes, which is useful in implementing countermeasures.

4. PROPOSED WORK

The advantage of Delphi is that it does not require clock synchronization and position information and it does not require the mobile nodes to be equipped with some special hardware, The Disadvantage of Delphi method is it cannot pinpoint the wormhole location. This disadvantage of Delphi method can be overcome by using Wormhole Geographic Distributed Detection which is another method to detect the wormhole attack and to pinpoint the location.

- We deployed the wireless ad hoc network in a fixed area and with the fixed number of nodes, the network deployed in decentralized in nature and each node is capable of moving freely from one to the other location.
- After deploying the wireless ad hoc network we established the path from the source to the destination with the help of the AODV routing protocol.
- The source node floods the route request packets in the network for the path establishment to the destination and the adjacent nodes of the destination will reply back to the source node with the route reply packets.
- After the sending of the route request packets and the route reply packets, we select the best path from the paths for sending the packets from the source to the destination.
- The malicious node existing in the path which will trigger wormhole attack and is responsible to increase the delay between the source and destination.
- By calculating the delay per hop for each node existing in the path the malicious node is detected.

© 2020, IJCSMC All Rights Reserved

- We keep track of the neighbors of each node in the network and its distance from the source node. This helps to find out the approximate location of the node responsible for the wormhole attack using the formula d =max(distance(b,c))/2 and distance is calculated , if coordinates of b and c are (x1,y1)and (x2,y2) then the distance will be $D = \sqrt{((x2 - x1)/2 + (y2 - y1)/2}$).
- After this the malicious node is removed from the network and new path is formed from the source to the destination to send the data packets.
- After this we plotted three graphs for the Throughput, Energy loss and Packet loss for the scenarios with and without the wormhole attack in the network. The results showed the great differences.

5. SIMULATION

Simulation is carried out in NS2 using 22 nodes in an area of 800*800. AODV routing protocol is used.

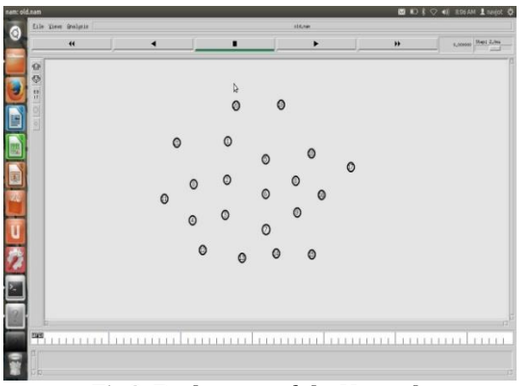


Fig 3. Deployment of the Network

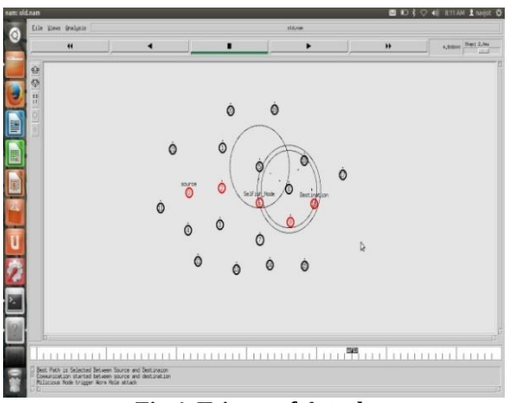


Fig 4. Trigger of Attack

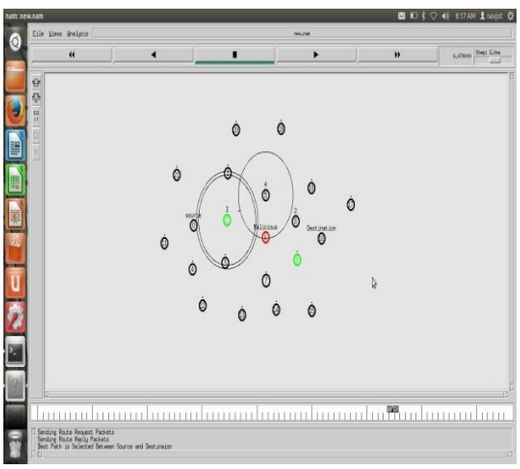


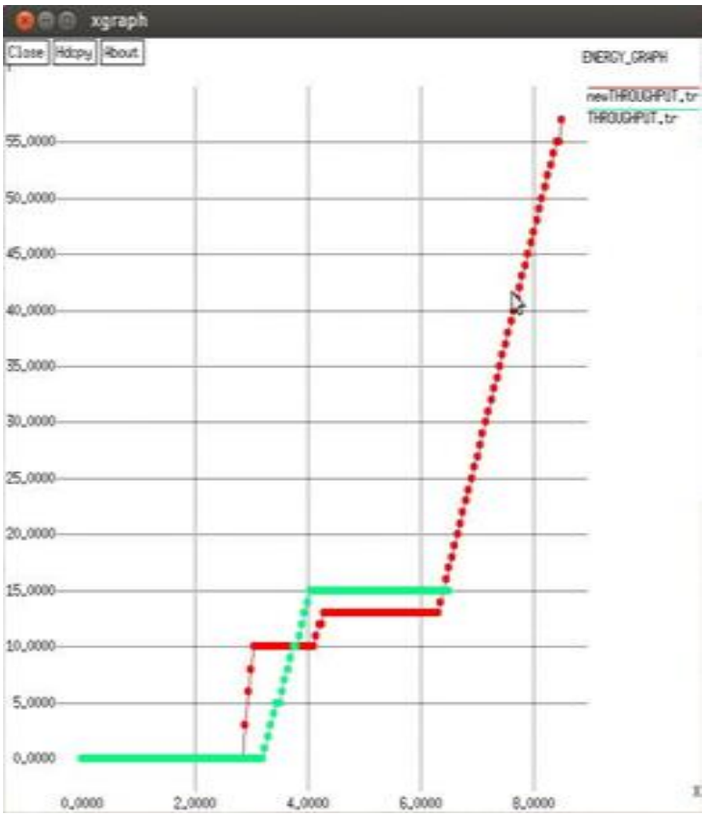
Fig 5. Forming a new path

© 2020, IJCSMC All Rights Reserved

6. RESULTS

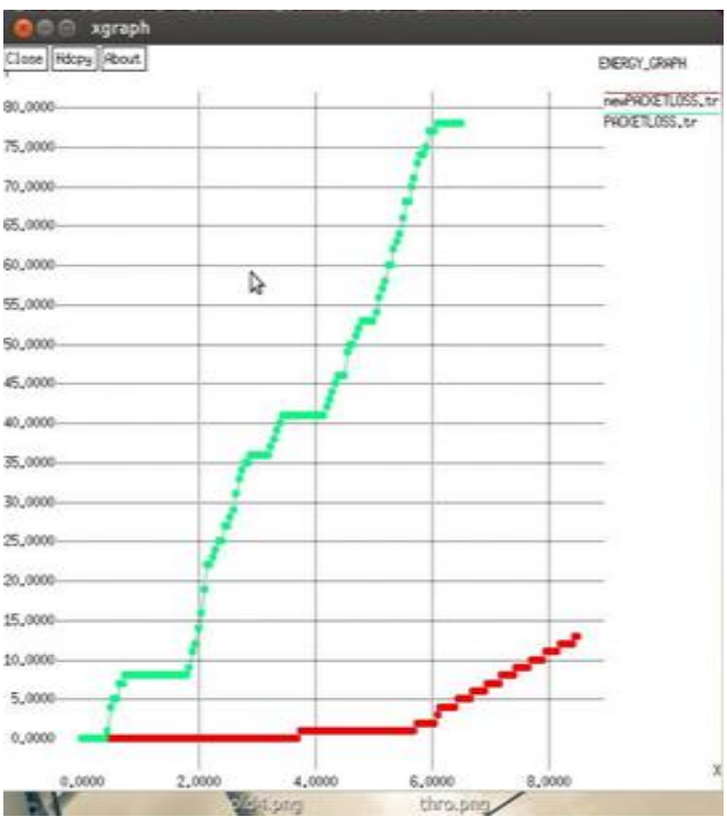
6.1 Throughput

The throughput of the network is enhanced through the use of new proposed technique.



6.2 Packet Loss

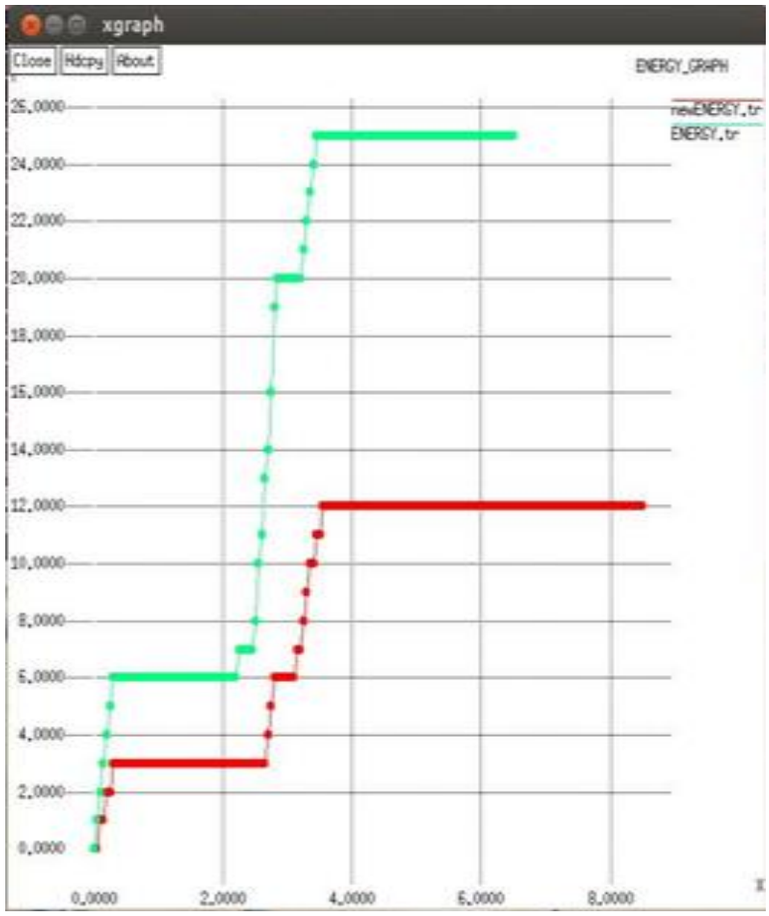
Due to removal of the malicious node from the network the hop count is reduced which results to decrease in the packet loss.



6.3 Energy Consumption

Energy consumed by the node was more in presence of wormhole attack. After the removal of this node less energy is consumed by the nodes.

© 2020, IJCSMC All Rights Reserved



7. CONCLUSION

When the mobile nodes are mutually true, it leads to the reliable data transmission between the mobile nodes. The security of the data packets plays an important role in data communication. There are many kinds of attacks that can take place in a network. As wormhole attack is one of the harmful attacks in MANETS so we studied about the method to detect and avoid the wormhole attack occurring in the network. To detect the wormhole attack we used the delay per hop method along with the wormhole geographical distributed detection method to pinpoint the location of the node responsible for the attack in the network which also removes the weak point of the delay per hop method.

REFERENCES

[1]. Nishant Sharma, Upinderpal Singh "Various Approaches to Detect Wormhole Attack in Wireless Sensor Network" IJCSMC, Vol. 3, Issue. 2, February 2014, pg.29-33.

[2]. Aarti and Dr. S.S Tyagi "Study of MANETS: "Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume-3, Issue-5, May 2013, ISSN: 2277 128X.

[3]. Donatas Sumyala, "Mobile ad hoc networks", IEEE Personal Communication Magazine, pp- 46-55, April 2003.

[4]. Rasmi Vijaywargiya , Prof. Kamlesh Chopra, "Comparative Study of Various Method of Detection of Wormhole Attack in MANET", International Journal of Research in Engineering Technology and Management, 2009, ISSN: 2347-7539.

[5]. Chiu, HS; Wong Lui KS, "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Network" 1st International Symposium on Wireless Pervasive Computing, 2006.

[6]. Hu, Y.-C., Perring, A., & Johnson, D. (2006), "Wormhole Attacks in Wireless Networks". IEEE Journal on Selected Areas in Communications, pp: 370-380, 2006.

[7]. A.Vani, D.Sreenivasa Rao, "Simple Algorithm For Detection and Removal OF Wormhole Attack for Secure Routing in Ad hoc Wireless Network", IJCSE, Volume-3, No-6, June 2011, ISSN: 0975-3397.

[8]. Yuron Xu, Guanling Chan, James Ford, Fillia Makedon. F(2007), "Distributed Wormhole Attack Detection in Wireless Sensor Networks", 2007.

[9]. Mohan Seth, "Detection of Wormhole Attack in Wireless Sensor Network", 2013.

[10]. Vrutik Shah, and Dr. Nilesh Modi, "Responsive Parameter based Antiworm Approach to Prevent Wormhole Attack in Ad hoc Network", ACEEE International Journal on Network Security, Volume-5, No-1, January 2014.

[11]. Nishant Sharma, Upinderpal Singh, "Various Approaches to Detect Wormhole Attack in Wireless Sensor Networks", Volume-3, Issue-2, pp: 29-33, February 2014.

[12]. Samiksha Suri "Different methods and approaches for the detection and removal of Wormhole Attack in MANETS", International journal of Engineering and technical research(IJETR), ISSN:2321-0869, VOLUME-1, Issue-5, July 2013.

© 2020, IJCSMC All Rights Reserved