ISSN 2320-9984
Volume 5 Issue 4| December 2017 ISSN: 2320-9984 (Online)
International Journal of Modern Engineering & Management Research
Website: www.ijmemr.org

# An Approach to Provide Security Against Wormhole Attack in MANET

**Aatmprakash Dwivedi**
*M.Tech. Research Scholar*
*Branch Cyber Security*
*Takshshila Institute of Engineering & Technology*
*Jabalpur (M.P.), [INDIA]*
*Email: daatmprakash@gmail.com*

**Abhishek Pandey**
*Assistant Professor*
*Department of Computer Science & Engineering*
*Takshshila Institute of Engineering & Technology*
*Jabalpur (M.P.), [INDIA]*
*Email: abhishekpandey@takshshila.org*

***Abstract*****—***Demand of infrastructure less, self -working, self-configuring, communication networks have brought about the formation of mobile Adhoc networks (MANET). MANET is extremely valuable over traditional networks in damaging conditions. In MANET all mobile devices work agreeably for route discover and information transmission. Due to its broadcast nature of transmission, and cooperative model of working, routing the traffic is a tedious task in MANET. Routing protocols are constantly focused by attackers to damage network. Routing protocols in MANET should be robust against different security dangers. Adhoc on-demand distance vector routing (AODV) protocol generally used and studied in the territory of mobile adhoc networks. In order to prevent MANET from wormhole attack a new method is proposed. In this work, wormhole attack in MANET is detected and prevented by using Hop Count, Reverse Trip Time and Link Length method. According to the scheme, hop count specifies the actual reverse trip time from source to destination. To find the presence of tunnel, the source will compare calculated reverse trip time with actual reverse trip time and to verify the presence of tunnel, the source will compare calculated link length with actual link length of the links in paths. This scheme provides a security to mobile ad hoc networks from both short as well as long wormhole tunnels. Network simulator is used to evaluate the performance of mobile ad hoc network. The simulation results show that the proposed scheme outperformed in terms of throughput and packet delivery ratio*

***Keywords:*****—***MANET, AODV, Wormhole Attack, Routing Protocol, Security, Packet Delivery Ratio, Throughput*

## 1. INTRODUCTION

Mobile Ad-hoc Networks (MANET) are infrastructure fewer networks so security is the main issue. Different methods have been proposed so far to prevent MANETs from various kinds of attacks. Out of these attacks, wormhole attack is the main threat. Two intrusion detection techniques [1] are enhanced that will use clusters and show how clusters can be used in order to give the ability to detect wormhole attack and isolating them from routing process. After that two routing protocols are taken OLSR is Optimized Link State Routing Protocol (proactive) and AODV is Ad-hoc On-Demand Distance Vector Routing Protocol (reactive) in order to find which protocol is more vulnerable to wormhole attack [2]. The finding shows that AODV is more vulnerable to wormhole attack compared to OLSR. Further, a statistical analysis approach is used and it provides better security and performance as compared to conventional AODV [3], an improved

clustering based approach in which the entire network is partitioned into different clusters and each cluster will have a Cluster Head, which controls all the nodes in the cluster and plays the role of a controlling authority in MANET and Out of band wormhole attacks that are launched by exploiting AODV routing protocol are eliminated effectively [4], a lightweight technique is able to detect and remove the wormhole attack to a greater extent and gives the lowest total packet loss rate compared with AODV under attack and the other techniques [5], an identity-based signature scheme does not require distribution of any certificate among nodes so it decreases computation overhead and the performance of the network is evaluated in terms of end-to-end delay, packet delivery ratio, packet loss rate [6]. Some other techniques [7]-[10] are also proposed in order to prevent wormhole attacks.

In this paper, wormhole attack is detected and prevented by using hop count, reverse trip time and link length between the nodes The proposed system firstly detects the presence of wormhole tunnel by using hop count and from the hop count actual reverse trip time is determined which is later on compared by the calculated reverse trip time and then detects the wormhole nodes using link length. The performance of the network is also analyzed which shows improved value of throughput and packet delivery ratio. The network's performance is simulated using NS2 simulator.

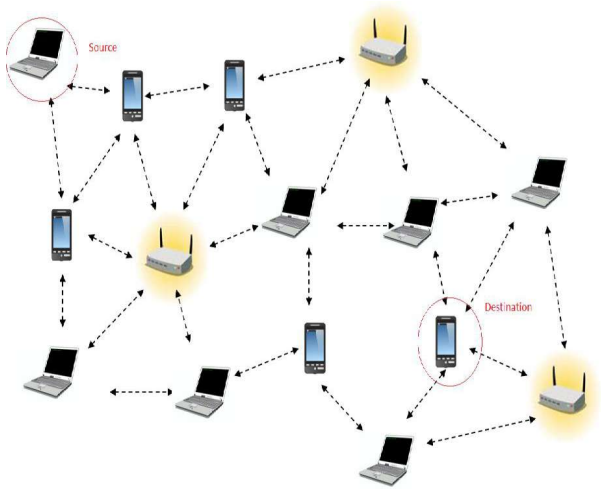


*Figure 1. MANET*

## 2. BACKGROUND

Basically, MANET can be categorized into first, second and third generations. The first generation came up with "packet radio" networks (PRNET), and were sponsored by DARPA in the early 1970s. It has evolved to be a robust, reliable, operational experimental network. The PRNET used a combination of ALOHA and CSMA approaches for medium access, and a kind of distance-vector routing to provide packet-switched networking to mobile battlefield elements in an infrastructure less, hostile environment. The second generation evolved in early 1980's when SURAN (Survivable Adaptive Radio Networks) significantly improved upon the radios (making them smaller, cheaper, and power-thrifty), scalability of algorithms, and resilience to electronic attacks. Important developments during this period include GloMo (Global Mobile Information System) and NTDR ( Near Term Digital Radio) The goal of GloMo was to provide office-environment Ethernet-type multimedia connectivity anytime, anywhere, in handheld devices. Channel access approaches were now in the CSMA/CA and TDMA molds, and several novel routing and topology control schemes were developed. The NTDR used clustering and link- state routing, and self-organized into a two-tier ad hoc network. Now used by the US Army, NTDR is the only "real" (non-prototypical) ad hoc network in use today. The third generation evolved in 1990's also termed as commercial network with the advent of Notebooks computers, open source software and equipment's based on RF and infrared. IEEE 802.11 subcommittee adopted the term "ad hoc networks." And the concept of commercial (non-military) ad hoc networking had arrived. Within the IETF, the Mobile Ad Hoc Networking (MANET) working group was horn, and sought to standardize routing protocols for ad hoc networks. The development of routing within the MANET working group and the larger community forked into reactive (routes on-demand) and proactive (routes ready-to-use) routing protocols 141. The 802.1 1

subcommittee standardized a medium access protocol that was based on collision avoidance and tolerated hidden terminals, making it usable, if not optimal, for building mobile ad hoc network prototypes out of notebooks and 802.11 PCMCIA cards. HIPERLAN and Bluetooth were some other standards that addressed and benefited ad hoc networking.

## 3. AODV PROTOCOL

The AODV routing protocol is designed for adhoc mobile networks and it can handle uni-cast routing and as well as multicast routing [2, 3, 4]. This protocol has the advantageous features of both DSR and DSDV algorithms and this protocol is an example of On-demand routing protocol which means the routes will be created only when there is a demand and also it maintains the routes only as long a they are needed. Creating and maintaining the routes in the network only when they are needed/demand makes this AODV protocol very useful and also a good algorithm for mobile ad hoc networks (MANET) [5]. All the nodes in the network have routing tables of their own and they also maintain sequence numbers in order to avoid looping problems [5]. If a source node wants to send some data to a destination node and if it doesn't have a route to the destination at that time then the source node broad castes route request (RREQ) packet throughout the network [2, 6]. The nodes will reply with a RREP if either the destination node or the intermediate node which is on the way to find the destination node. A node which receives the PREQ will send a reply (RREP) only if it is either the destination or if it is a path/route to the destination with a corresponding sequence number and only when that number is greater than or equal to the number which contains the RREQ [2]. In cases like this the nodes will uni-casts a RREP to the source, otherwise; the nodes will rebroadcast the RREQ. The nodes will discard the RREQ and do not forward them if they have been processed those already. And the RREP will set up forward pointers to the destination by propagating back to the source nodes [2, 7, 8] When the source node receives the RREP, it records the latest sequence number to the requested destination and this process is called as Forward Path setup [9]. The intermediate nodes that receives another RREP after they had propagated the previous RREP towards the source, it then checks and compares the new destination sequence number of the new RREP with the previous RREP. These intermediate nodes updates their routing information and propagates a new RREP only when, 1. The destination sequence number is greater or 2. The new sequence number is same but the hop count is small or it will just skip the new RREP. This process ensures that this algorithm is not making any loops and only the most effective is chosen [5]. If the data packets keep travelling from one node to another node along a certain path only then the route remains active otherwise the links will timeout and then be deleted from the routing tables of the intermediate nodes. In situations like where the links break while the route is being active then the node upstream of the link break generates a route error (RERR) to the source node to inform that it is not reachable to the destination (s). After the source node receives this (RERR) message, then even if the source node still needs the route then it will reinitiate the route discovery to that destination [4, 10]. Route Discovery Mechanism in AODV: If the source node "A" wants to initiate communication with destination node "E" as shown in the Figure 4.1, then it will make a connection between itself and the destination and will generate a route request message (RREQ). This message is then forwarded to the neighbouring nodes, and the neighbouring nodes will forward this control message to their neighbouring nodes. This process of finding destination node continues until the destination node is located itself or the node that has the fresh route to the destination. Once an intermediate node with enough fresh routes is located or destination node is located, they generate the route reply message (RREP) and send it back to the source node. When RREP reaches back to the source node, a route or the path is established between the source node "A" and destination node "E". Once the route is established between "A" and

"E", node "A" and "E" can communicate with each other. Figure 5 depicts the exchange of control messages between source node and destination node.

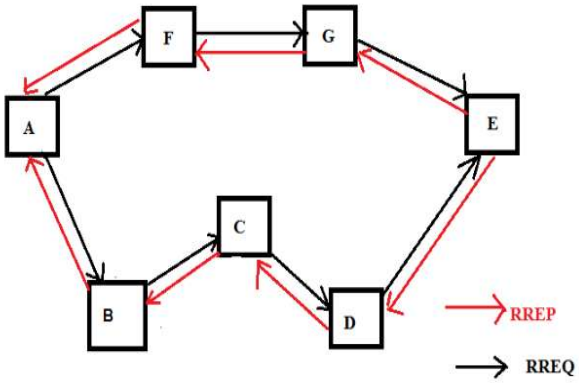


Figure 2. Route Discovery Mechanisms

**Route Maintenance Mechanism:** When there is a link down or a link breakage between destinations that causes one or more than one links unreachable from the source node or neighbour's nodes, then the RERR message is generated by the node and sent to the source node. If there is a route from "A" to "E" via "D", and if there is a link breakage "D" and "E", then the node "E" will generate and send the RERR message to the source node "A" informing the source node that there is a route error. The scheme is as shown in the Figure 3.

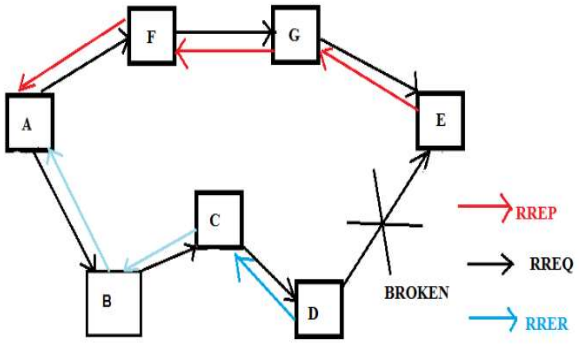


*Figure 3. Route Error Message*

## 4. WORMHOLE ATTACK

A wormhole attack is specifically serious attack on MANET routing where two attackers are connected through a high speed off-channel link (tunnel) which are critically placed at distinct ends of the network. Wormhole tunnel will then start gathering the data packets and relay the same to some other location. Malicious nodes will create an illusion in a network and make genuine nodes to believe that they are adjoining neighbours. An intruder can collect and manipulate network traffic by attracting and by passing a large amount of network traffic through wormhole. Each ROUTE REQUEST (RREQ) packet is tunnelled to the destination target node of the REQUEST for the application of wormhole attack. Normal routing protocol process is to be followed when the destination node's neighbour hear this REQUEST packet which will rebroadcast that copy of REQUEST and then abandon all other received ROUTE REQUEST packets activated from this same Route Discovery. Any routes other than the routes which are being explored can be prohibited by this attack. In addition to that the attack can even prevent routes more than two hops long from being exposed, if the attacker is near the initiator of Route exploration. Consider figure 1 malicious node that is red in color will broadcast its RREQ to its neighbour nodes which is originally broadcasted to perform a wormhole attack. Destination node will also receive the RREQ request so it will follow a normal routing process and discard all other received ROUTE REQUSET packets. The malicious node will create a link to another malicious node which is the neighbour of the source node which is dotted here in the figure known as wormhole tunnel. The tunnel in turn to be a shortest path to reach the destination as it may have less count of hop compared to normal routes. Various kind of attack such as DOS attack, Eavesdropping, and fabrication can be performed with the use of this privilege. Wormhole attack is able to bring down the entire routing system in MANET The attacker actually facilitate useful services more efficiently connecting the network, if the attacker achieves this tunnelling reliably and honestly and no loss is done. The attack can still be launched even if confidentiality and authenticity is provided over the communication and even if the intruder has no cryptography keys.

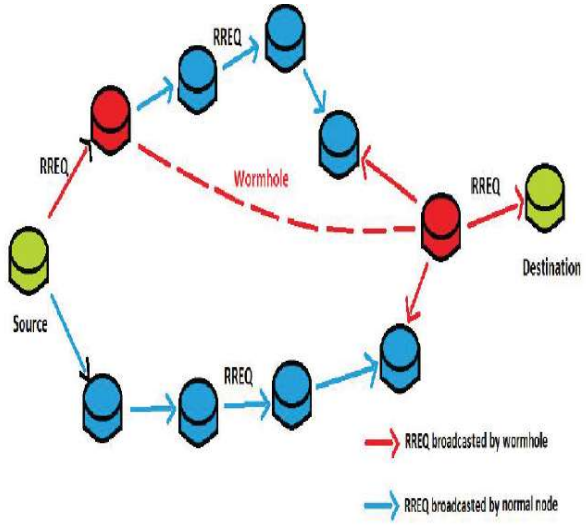


*Figure 4. Wormhole Scenario*

## 5. RELATED WORK

There are various research has been proposed by researchers in MANET to secure communication network against Wormhole attack. A wormhole attack is variable in its behaviour and nature so it provides an ample area of exploration and thus distinct research have been suggested for the detection of wormhole attack. Some of review of Literature related to this work as follows-

**Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks,", 2011.[37]** Packet Leash in is a mechanism to detect and defend against wormhole attacks. The mechanism proposes two types of leashes for this purpose: Geographic and Temporal. In Geographic Leashes, each node knows its precise position and all nodes have a loosely synchronized clock. Each node, before sending a packet, appends its current position and transmission time to it. The receiving node, on receipt of the packet, computes the distance to the sender and the time it took the packet to traverse the path. The receiver can use this distance anytime information to deduce whether the received packet passed through a wormhole or not.. When temporal leashes are used, the sending node append the time of transmission to each sent packet ts in a packet leash, and the receiving node uses its own packet reception time tr for verification. The sending node calculates an expiration time te after which a packet should not be accepted, and puts that information in the leash.

**T. Sakthivel and R.M. Chandrasekaran. "Detection and Prevention wormhole Attack in MANET using Path Tracing Approach".2012 [34]**The proposed work introduced "Detection and Prevention wormhole Attack in MANET using Path Tracing Approach". For route discovery, DSR protocol is used. In order to detect the wormhole, prior per hop distance field, per hop distance field and timestamp fields are added to the header of each packet. Author(s) consider both prior per hop distance and per hop distance so as to compare the difference between the two distances. If the difference is too large that exceeds the maximum threshold value, then wormhole is detected. These wormhole node are then isolated from the network.

**Priyank Nayak, Akshay Sahay, Yogadhar Pandey "Detection** and **Prevention of Wormhole Attacks in MANETs using Detection Packet" 2013** [26] In this work, they present a general mechanism, without use of hardware, location information and clock synchronization called detection packet for detecting malicious node in network. Detection Packet has three fields: processing bit, count to reach next hop and time stamp. Timestamp is used for strongly detection with conformance at wormhole attack. Here detection packet can easily be included in the wide range of ad hoc routing protocol with only significant change in the existing protocol to defend against wormhole attack. Here DSR protocol is use for route establishment and NS-2 for simulations.

**RTT - J.** Zhen **and S. Srinivas. Preventing replay attacks for secure routing in ad hoc networks. 2014 [1]** In this they described about specialized hardware along with directional antenna for fast sending of one -bit challenge and distance-bounding protocol securing node tracking can be encountered in multiple hop networks. Using special hardware can be a tedious task so another approach

known as Time of flight based approach is proposed. Round Trip Time [1] mechanism is advised in this approach. RTT is prolonged as a time that is required by node A for sending Route Request (RREQ) message to node B receiving time of Route Reply (RREP) message. Node A will determining among A and all its nearby nodes. As the RTT among two fraudulent neighbours is greater than among two legitimate neighbours, Node A can easily classify both fraudulent and legitimate neighbours. Every node in the network calculates RTT between itself and all its neighbours. Implementation approach is easy as it doesn't require different hardware; in exposed attacks fraudulent neighbours are devised so, it cannot detect exposed attacks.

**Jagadhri, Haryana,India et al "Detection & Prevention of Wormhole attack on AODV Protocol in Mobile Adhoc Networks (MANETS)" 2014 [21]**In this paper a solution is proposed to prevent the network against wormhole attack. A secret key is used for encryption and decryption of hello packets. Because of this only authentic nodes will remain in the network, non-authentic nodes (wormhole node) will be discarded. As a result communication can take place only between the trusted nodes. So malicious node cannot enter into system and communication is secured. In this work we choose AODV as routing protocol for MANET, a pair of wormhole nodes is selected for performing wormhole activity. And simulation is done on NS 2.34 with 36 nodes. Simulation clearly shows that our method is well effective in preventing the network against wormholeattack.

**DelPHI - D. A. Maltz and D. B. Johnson and Y. Hu. The dynamic source routing protocol (DSR) for mobile ad hoc, 2015 [2]** Delay per Hop(DelPHI)[2] is derived as an another approach which can detect both exposed and hidden wormhole attacks also known as hop count/delay per hop based approach. Every possible disarticulate route between a source and a destination are determined in DelPHI. Standard delay time per hop on each path is calculated along with its delay time and length of each route Wormhole can be easily revealed with the use of these values. The path with a wormhole tunnel will have higher Delay per Hop (DPH) value. The disadvantage of this method is that it doesn't consider mobility.

**Muhammad Imrana, et al "Analysis of Detection Features for Wormhole Attacks in MANETs" 2015 [32]**This paper presented the features that could be used to detect the wormhole attack. These features are discussed in detail with their pros and cons. The possible limitations of Intrusion Detection Systems (IDSs) are also discussed. This work provides a basis to build an efficient IDS to detect wormhole attacks in MANETs. According to our analysis, the techniques based on route request (RREQ) or hop count would be better than other techniques to detect wormhole attacks.

**Ashka Shastri, et al, "A Wormhole Attack in** Mobile **Ad-hoc** Network**: Detection and Prevention", 2016. [22]** In these proposed approach named "Hop Based Analysis" the wormholes nodes are determined when the sudden decrement in the average hop count of a path from the source node to destination node had been noticed as compared to the other paths because the path with wormholes nodes has smaller hop count.

**Mithilesh Kumar et al, "Hop Count Based Conjunction Control Wormhole Detection Approach for MANET -2016,** [30] A simple technique for detecting wormholes in ad hoc networks is presented in the paper. This method employs routing variation between neighbours to determine the existence of a wormhole. The technique is localized, requires only a small overhead, and does not have special requirements such as location information, accurate synchronization between nodes, special hardware etc. The technique has been tested through simulations for different distributions of nodes for wormholes and different connectivity models. Under all the evaluated scenarios, the technique demonstrates excellent detection probabilities

with few false alarms that depend on the value of threshold.

## 6. PROBLEM STATEMENT

Mobile Ad-hoc Networks (MANET) are infrastructure fewer networks so security is the main issue. Different methods have been proposed so far to prevent MANETs from various kinds of attacks. Out of these attacks, wormhole attack is the main threat. Two intrusion detection techniques [1] are enhanced that will use clusters and show how clusters can be used in order to give the ability to detect wormhole attack and isolating them from routing process. After that two routing protocols are taken OLSR is Optimized Link State Routing Protocol (proactive) and AODV is Ad-hoc On-Demand Distance Vector Routing Protocol (reactive) in order to find which protocol is more vulnerable to wormhole attack [2]. The finding shows that AODV is more vulnerable to wormhole attack compared to OLSR. Further, a statistical analysis approach is used and it provides better security and performance as compared to conventional AODV [3], an improved clustering based approach in which the entire network is partitioned into different clusters and each cluster will have a Cluster Head, which controls all the nodes in the cluster and plays the role of a controlling authority in MANET and Out of band wormhole attacks that are launched by exploiting AODV routing protocol are eliminated effectively [4], a lightweight technique is able to detect and remove the wormhole attack to a greater extent and gives the lowest total packet loss rate compared with AODV under attack and the other techniques [5], an identity-based signature scheme requires distribution of any certificate among nodes so it increases computation overhead and the performance of the network is evaluation will be enhanced in terms of end-to-end delay, packet delivery ratio, packet loss rate [6].

There is a need to propose some techniques in order to prevent wormhole attacks.

### *6.1 Research Objective*

The main objective of this work is to minimize the threat of wormhole attack in Mobile Ad-hoc Networks by preventing and detecting long as well as short wormhole tunnels in the network.

To reduce the computation overhead arises due to evaluation of secret key which is distributed among nodes during communication.

## 7. PROPOSED METHODOLOGY

The objective of this research is to minimize the threat of wormhole attack in Mobile Ad-hoc Networks by preventing and detecting long as well as short wormhole tunnels in the network. In order to detect and prevent wormhole attack, H-R-L (Hop Count-Reverse Trip time-Link Length) method is used and the proposed technique works as follows:

1. Source broadcasts Route Request (RREQ) to its neighbour nodes and finds the route to destination
2. Nodes check their routing table and if no route exists, it re-broadcast RREQ message to its neighbours
3. The process continues until request reaches to destination and destination will send route reply to source
4. Now, source will check the presence of tunnel in the suggested route & forwards channel request (CREQ) message to nodes and asks for their location coordinates
5. Nodes reply with channel reply (CREP) message and forward their location coordinates to source
6. Source calculates Reverse Trip Time (RTT) taken to receive the CREP and if calculated RTT is

greater than actual value, confirms presence of tunnel

7. Now source calculates link length of links present in the path and if calculated link length is more than the actual length, wormhole nodes are detected

8. Source informs all other nodes to not communicate with detected wormhole nodes.

## 8. SIMULATION RESULT

### *A. Simulation Setup*

**Table 1. The simulation parameters used in the work.**

| Parameter | Value |
|---|---|
| Channel | Wireless |
| Propagation Model | Two Ray Ground |
| Mobility Model | Random Way Point |
| Routing Protocol | AODV |
| Number of nodes | 50 |
| Mac | 802.11 |
| Antenna | Omni Directional |
| Initial Energy | 50 Joules |
| Network Area | 1300m * 1300m |
| Queue Drop | Tail |
| Simulation time | 25 sec |
| Theoretical value | 0.02184 |

The channel used is wireless and propagation model is two ray ground because when the signal received consists of a line of sight and multi-hop components, it predicts path loss. The number of nodes used is 50 and antenna used is omnidirectional. The queue used is drop tail. In this queue, when the queue is filled with maximum capacity then the newly incoming packets are dropped until queue have sufficient space to accept more packets.

### *B. Packet Delivery Ratio*

Figure 8 shows the comparison of PDR (packet delivery ratio) of the network achieved after using proposed scheme and the existing scheme. The proposed scheme showed the better value of packet delivery ratio at 0.95 whereas the value of packet delivery for the existing scheme is 0.64. This means less number of data packets was dropped after application of proposed scheme which also means the data transmission was more efficient and secure.

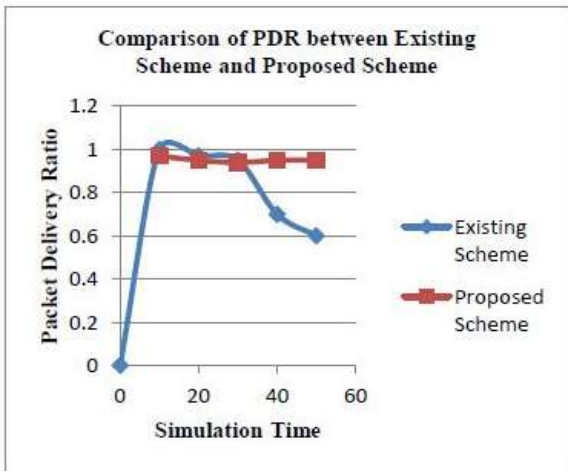


*Figure 5. Comparison of Packet Delivery Ratio between Proposed Scheme and Existing Scheme*

### *C. Throughput*

Figure 6 shows the comparison of the throughput of network achieved after applying the existing scheme and the proposed scheme. The graphs have been plotted against simulation time which is time taken to simulate the network. The value of throughput achieved with our proposed scheme is 36 kbps and that with the existing scheme is approx 5 Kbps. This shows that our proposed scheme outperforms the existing scheme.

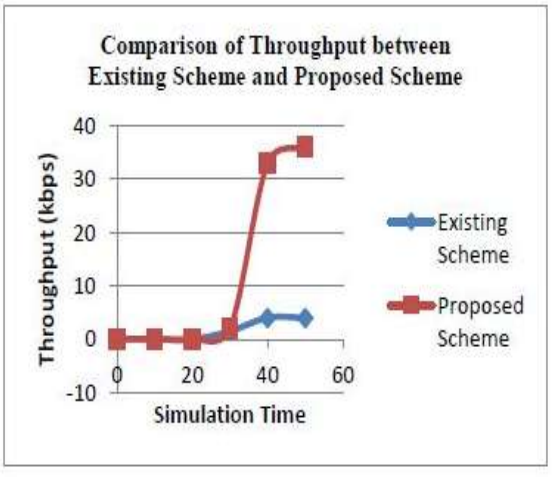


*Figure 6. Comparison of Throughput of Network between Proposed Scheme and Existing Scheme*

## 9. CONCLUSION

MANET being susceptible and insecure for different types of attacks so it requires a decisive, energetic and a secure technique that can be immediately expanded and use dynamic routing. Security is very crucial for MANET. Among all possible attacks in MANET, wormhole attack is very severe attack as it will significantly degrade network performance to network security. A illegitimate node records and regulate data traffic at one point and tunnels it to a plotting node far away, which gives response it locally that can either brought down the route installation process in wormhole attack. Wormhole attack is a very dangerous attack and many researchers have proposed many techniques in order to detect and prevent MANETs from wormhole attacks. In the proposed work, the technique successfully detects and prevents the wormhole attack for both tunnels short and long tunnels. The performance of the network was analyzed using parameters: packet delivery ratio and throughput. Both these factors tend to show an improved performance of the network. This shows that the proposed scheme has performed effectively.

## 10. FUTURE SCOPE

A remarkable chunk of effort has been completed on clarifying wormhole attack Problem. According to the need of networks, solutions may vary and choice is available based on cost and need of security In future, the proposed technique can be used to detect rushing attack in which the nodes rush the route request messages to the destination earlier than other nodes using the tunnel

## REFRENCES:

[1] Mahdi Nouri, Somayeh Abazari Aghdam, Sajjad Abazari Aghdam, "Collaborative Techniques for Detecting Wormhole Attack in MANETs", International Conference on Research and Innovation in Information Systems (ICRIIS), IEEE, November 2011.

[2] Mohammad Sadeghi, Saadiah Yahya, "Analysis of Wormhole attack on MANETs using different MANET routing protocols", Fourth International Conference on Ubiquitous and Future Networks (ICUFN), IEEE, July 2012.

[3] Saurabh Upadhyay, Brijesh Kumar Chaurasia, "Detecting and Avoiding Wormhole Attack in MANET Using Statistical Analysis Approach", Advances in Computer Science and Information Technology Networks and Communications, Springer, Vol. 84, pp. 402-408, 2012.

[4] J. Anju, C. N. Sminesh, "An Improved Clustering-Based Approach for Wormhole Attack Detection in MANET", 3rd International Conference on Eco-friendly Computing and Communication Systems, IEEE, pp. 149-154, 2014.

[5] Hosny M. Ibrahim, Nagwa M. Omar, Ebram K. William, "A Lightweight Technique to Prevent Wormhole Attacks in AODV", International Journal of Computer Applications, Vol. 104, October 2014.

[6] Dhruvi Sharma, Vimal Kumar, Rakesh Kumar, "Prevention of Wormhole Attack Using Identity-Based Signature Scheme in MANET", Computational Intelligence in Data Mining, Vol. 2, pp. 475-485, 2015.

[7] Juhi Biswas, Ajay Gupta, Dayashankar Singh, "WADP: A wormhole attack detection and prevention technique in MANET using modified AODV routing protocol", 9th International Conference on Industrial and Information Systems (ICIIS), IEEE, December 2014.

[8] Rajan Patel, Anal Patel, Nimisha

Patel, "Defending Against Wormhole Attack in MANET", Fifth International Conference on Communication Systems and Network Technologies, IEEE, 2015.

[9] S. B. Geetha, Venkanagouda C Patil, "Evaluating the Research Trends and Techniques for Addressing Wormhole Attack in MANET", International Journal of Computer Applications, Vol. 110, No. 6, January 2015.

[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, Vol. 4, Issue 8, pp. 80 – 85, August 2015.

[11] RTT - J. Zhen and S. Srinivas. Preventing replay attacks for secure routing in ad hoc networks. In ADHOC-NOW, LNCS 2865

[12] DelPHI - D. A. Maltz and D. B. Johnson and Y. Hu. The dynamic source routing protocol (DSR) for mobile ad hoc.

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

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

[15] Reshmi Maulik, 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).

[16] Muhammad Imrana, Farrukh Aslam Khanb, Tauseef Jamala, Muhammad Hanif Durad, Analysis of Detection Features for Wormhole Attacks in MANETs International Workshop on Cyber Security and Digital Investigation (CSDI 2015).

[17] Mekhala Chattopadhyay, Mrs. Saswati Mukherjee, An Approach To Detect Wormhole Attack In Aodv Based Manet Jadavpur University Kolkata-70003.

[18] Detection and prevention of wormhole attacks in MANETs using path tracing approach,http:// www.academia.edu/6771876/ Detection_and_Prevention_of_Worm hole_Attacks_in_MANETs_using_Pa th_Tracing _Approach.

[19] Marianne Azer, Sherif El-Kassas, Magdy El-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.

[20] Manjeet Singh, Gaganpreet Kaur, "A Surveys of Attacks in MANET" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 6, June 2013.

[21] Jagadhri, Haryana,India et al "Detection & Prevention of Wormhole attack on AODV Protocol in Mobile Adhoc Networks (MANETS)" International Journal Of Engineering And Computer Science ISSN:2319-7242Volume 3 Issue 9 September 2014 Page No. 7979-7985.

[22] Ashka Shastri, et al, "A Wormhole Attack in Mobile Ad-hoc Network: Detection and Prevention" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 6, 2016.

[23] Mr. L Raja, Capt. Dr. S Santhosh Baboo "An Overview of MANET: Applications, Attacks and Challenges" International Journal of Computer Science and Mobile Computing, Vol.3 Issue.1, January-2014, pg. 408-417.

[24] Md. Majharul Haque1, Md. Shakil Ahamed Shohag2, Abu Sadat Mohammed Yasin3, Sadia Binte Anwar4 "Mobile Ad-Hoc Network Security: An Overview" International Journal of Scientific Research Engineering & Technology (IJSRET) Volume 2 Issue 8 pp 504-511 November 2013 www.ijsret.org ISSN 2278 – 0882

[25] Neeraj Verma "A Review of Different Routing Protocols in MANET" International Journal of Advanced Research in Computer Science, Volume 8, No. 3, March – April 2017

[26] Priyank Nayak, Akshay Sahay, Yogadhar Pandey "Detection and Prevention of Wormhole Attacks in MANETs using Detection Packet" International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 1216 ISSN 2229-5518.

[27] 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.

[28] Anal Patel, Nimisha Patel, Rajan Patel "Defending Against Wormhole Attack in MANET" 2015 Fifth International Conference on Communication Systems and Network Technologies.

[29] Aakanksha Kadam, Niravkumar Patel, Vaishali Gaikwad "Detection and Prevention of Wormhole attack in MANET" International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 03 Issue: 03 | Mar-2016

[30] Mithilesh Kumar et al, "Hop Count Based Conjunction Control Wormhole Detection Approach for MANET" International Journal of Scientific Research & Engineering Trends Volume 2, Issue 2, March-2016, ISSN (Online): 2395-566X

[31] Achint Gupta, Dr. Priyanka V J, Saurabh Upadhyay "Analysis of Wormhole Attack in AODV based MANET Using OPNET Simulator" International Journal of Computing, Communications and Networking, 1 (2), September 2012

[32] Muhammad Imrana, Farrukh Aslam Khanb,*, Tauseef Jamala, Muhammad Hanif Durada "Analysis of Detection Features for Wormhole Attacks in MANETs" International Workshop on Cyber Security and Digital Investigation (CSDI 2015)

[33] Juhi Biswas, Ajay Gupta, Dayashankar Singh "A Wormhole Attack Detection And prevention Technique in MANET using Modified AODV routing Protocol" International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 03 Issue: 03 | Mar-2016

[34] T. Sakthivel and R.M.

Chandrasekaran. "Detection and Prevention wormhole Attack in MANET using Path Tracing Approach". 2012.

[35] Honglong Chena,b,Wei Louc,d, ZhiWang, Junfeng Wue Zhibo Wang, Aihua Xia "Securing DV-Hop localization against wormhole attacks in wireless sensor networks" in Volume 16, Part A, January 2015, Pages 22–35, Volume 16, Part A, Elsevier 2015, Pages 22–35

[36] Jie Zhou1, Jiannong Cao, Jun Zhang1, Chisheng Zhang and Yao Yu, "Analysis and Countermeasure for Wormhole Attacks in Wireless Mesh Networks on a Real Test bed" in 26th IEEE International Conference on Advanced Information Networking and Applications, 2012.

[37] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in Proc. of IEEE INFOCOM, 2010.

[38] Harris Simaremare and Riri Fitri Sari. Performance Evaluation of AODV variants on DDOS, Blackhole and Malicious Attacks, International Journal of Computer Science and Network Security, VOL-11, June 2011, pp.

[39] Agrawal, N., Mishra, N. RTT Based Wormhole Detection Using NS-3. International Conference on Computational Intelligence and Communication Networks (CICN), pp.861-866, 14-16 Nov. 2014.

[40] Chaurasia, U.K., Singh, V. MAODV: Modified wormhole detection AODV protocol. Sixth International Conference on Contemporary Computing (IC3), pp.239-243, 8-10 Aug. 2013.