International Journal of Research and Development in Applied Science and Engineering (IJRDASE)
ISSN: 2454-6844

A Review on Mobile Ad-Hoc Networks Routing Protocols with Wormhole Intrusion Detection Algorithm.

Neha Verma
Computer Science & Engineering,
BBDU, Lucknow, India
er.nehaverma11@gmail.com

Yashi Singh
Computer Science & Engineering,
BBDNITM, Lucknow, India
yashisingh218@gmail.com

Abstract-- Ad Hoc system are well known and helpful on account of infrastructure less nature. Ad-**hoc Network is a gathering of hubs, in which singular hubs corporate by sending packets for each other to permit hubs to convey past direct transmission range. Security is principally worry with a specific end goal to give ensured correspondence between mobile nodes in hostile environments. Countless conventions for MANET has been proposed to empower brisk and effective system creation and rebuilding MANET (Mobile Ad-hoc Network) alludes to a multi-hop packet based wireless network made out of an arrangement of versatile hubs that can convey and move in the meantime , without utilizing any sort of settled wired foundation . MANET'S are really self arranging and versatile systems that can be shaped and distorted on-the-fly without the need of any concentrated organization. It by and large works by TV the data and utilized air as medium. It's telecasting nature and transmission medium likewise help assailant to disturb system. Numerous kind of assault should be possible on such Mobile Ad Hoc Network. The accentuation of this paper to study wormhole attack, some detection method and different techniques to prevent network from these attack.**

Keywords: AODV, MANET, Intrusion Detection, and Warm Hole Attack,.

1. Introduction:

A Mobile Adhoc Network is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others needs the aid of intermediate nodes to route their packets. Each of the node has a wireless interface to communicate with each other. [1] These networks are fully distributed, and can work at any place without the help of any fixed infrastructure as access points or base stations.

Figure 1 shows a simple ad-hoc network with 3 nodes. [1] Node 1 and node 3 are not within range of each other; however the node 2 can be used to forward packets between node 1and node 2. The node 2 will act as a router and these three nodes together form an ad-hoc network.

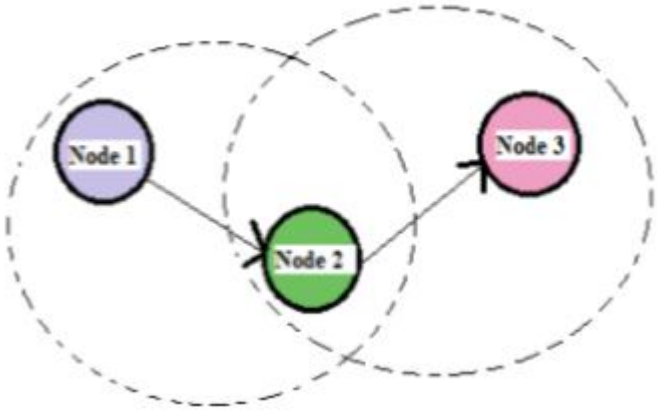

Fig. 1. Mobile Adhoc Network

Mobile ad hoc networks are autonomous systems comprised of a number of mobile nodes that communicate using wireless transmission. They are self-organized, self-configured and self controlled infrastructure-less networks. This kind of network has the advantage of being able to be set up and deployed quickly because it has a simple infrastructure set-up and no central administration. Obvious examples are in the military or the emergency services. One scenario is establishing communication between various agents in a disaster recovery operation where e.g. fire fighters need to connect to local ambulances and traffic control in circumstances where the normal communication infrastructure is destroyed or otherwise rendered unusable. In such situations a collection of mobile nodes with wireless network interface can form a transitory network. These networks are particularly useful to those mobile users who need to communicate in situations where no fixed wired infrastructures are available. However, the salient feature of creating a network 'on the fly' without requiring any prearranged infrastructure gave mobile ad hoc networks an appreciated interest in both industrial and military systems.

2. Related Work:

In multi-hop wireless systems, the need for cooperation among nodes to relay each other's packets exposes them to a wide range of security attacks. A particularly devastating attack is the wormhole attack, where a malicious node records control traffic at one location and tunnels it to another compromised node, possibly far away, which replays it locally. Routing security in ad hoc networks is often equated with strong and feasible node authentication

and lightweight cryptography. Unfortunately, the wormhole attack can hardly be defeated by crypto graphical measures, as wormhole attackers do not create separate packets. They simply replay packets already existing on the network, which pass the cryptographic checks. Existing works on wormhole detection have often focused on detection using specialized hardware, such as directional antennas, etc. In this work, we present a cluster based counter-measure for the wormhole attack, that alleviates these drawbacks and efficiently mitigates the wormhole attack in MANET. Simulation results on MATLab exhibit the effectiveness of the proposed algorithm in detecting wormhole attacks by **Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki (2009)** [1].
In this work, a new cluster based wormhole detection method has been proposed. In multi-hop wireless systems, the need for cooperation among nodes to relay each other's packets exposes them to a wide range of security threats including the wormhole attack. A number of recent works have been studied before proposing this new methodology. The proposed solution unlike some of its predecessors does not require any specialized hardware like directional antennas, etc for detecting the attackers. or extremely accurate clocks, etc. The simulation using 30 nodes and variable number of guard nodes prove the effectiveness of the proposed algorithm. Currently more studies are being done to analyze the performance of the proposed algorithm in presence of multiple attacker nodes.

Rutvij H. Jhaveri et. al. (2010) [2], according to them in this era of wireless devices, Mobile Ad-hoc Network (MANET) has become an indivisible part for communication for mobile devices. Therefore, interest in research of Mobile Ad-hoc Network has been growing since last few years. In this work we have discussed some basic routing protocols in MANET like Destination Sequenced Distance Vector, Dynamic Source Routing, Temporally-Ordered Routing Algorithm and Ad-hoc On Demand Distance Vector. Security is a big issue in MANETs as they are infrastructure-less and autonomous. Main objective of writing this work is to address some basic security concerns in MANET, operation of wormhole attack and securing the well-known routing protocol Ad-hoc On Demand Distance Vector. Their work would be a great help for the people conducting research on real world problems in MANET security.
MANETs require a reliable, efficient, scalable and most importantly, a secure protocol as they are highly insecure, self-organizing, rapidly deployed and they use dynamic routing. AODV is prone to attacks like modification of sequence numbers, modification of hop counts, source route tunneling, spoofing and fabrication of error messages. Although fabrication of source routes (cache poisoning) is not possible in AODV while DSR is prone to it. Wormhole attack is a real threat against AODV protocol in MANET. Therefore, trustworthy techniques for discovering and detection of wormhole attack should be used. We should keep in mind that some solutions may not work well in the presence of more than one malicious node, while some require special hardware and some solutions are very expensive. So, there is still a lot of room for research in this area to provide a more secured MANET.

The infrastructure of a Mobile Ad hoc Network (MANET) has no routers for routing, and all nodes must share the same routing protocol to assist each other when transmitting messages. However, almost all common routing protocols at present consider performance as first priority, and have little defense capability against the malicious nodes. Many researches have proposed various protocols of higher safety to defend against attacks; however, each has specific defense objects, and is unable to defend against particular attacks. Of all the types of attacks, the wormhole attack poses the greatest threat and is very difficult to prevent; therefore, **A.Vani et. al. (2011)** [3], focused on the wormhole attack, by combing three techniques. So that our proposed scheme has three techniques based on hop count, decision anomaly, neighbor list count methods are combined to detect and isolate wormhole attacks in ad hoc networks. That manages how the nodes are going to behave and which to route the packets in secured way.
In this study they analyzed the effects of wormhole attack in ad hoc wireless networks. They implemented an AODV protocol that simulates the behavior of wormhole attack in NS-2.In this method we have used very simple and effective way of providing security in AODV routing protocol against wormhole attack that causes the interception and confidentiality of the ad hoc wireless networks. Security against wormhole attack is provided by using a simple wormhole algorithm. This algorithm has better performance comparing to three individual methods [Hop count, Anomaly based, Neighbor list methods].The solution detects the malicious nodes and isolates it from the active data forwarding. As from the results we can easily infer that the performance of the normal AODV drops under the presence of worm hole attack.

In multihop wireless adhoc networks, cooperation between nodes to route each other's packets exposes these nodes to a wide range of security attacks. Also due to the vulnerability of the routing protocols, the wireless ad-hoc networks face several security risks. A particularly severe security attack that affects the adhoc network routing protocols, is known as the wormhole attack. The wormhole attack is carried out as a two phase process launched by one or more than one malicious nodes. In the first phase, these malicious nodes, called as wormhole nodes, try to lure legitimate nodes to send data via them by participating in the network. In the second phase, wormhole nodes could exploit the data & affect the communication by misbehaving. In this work **Pirzada Gauhar Arfaat, Dr. A.H. Mir (2011)** [4], have simulated the wormhole attack in wireless adhoc networks & Manet's. And then they evaluated & discussed the impact on the network by comparing the results without and with wormhole attack. The Wormhole attack was simulated using different scenarios. Thus they studied the impact of the wormhole attack on the respective networks. The parameters like throughput, packet loss and end-to-end delay were calculated using different scenarios for evaluating the impact on wireless adhoc networks and Manet's.

Wormhole attacks in wireless adhoc networks can severely deteriorate the network performance and compromise the security through spoiling the routing protocols and weakening the security enhancements. In this work we simulated the wormhole attack in AODV in wireless adhoc networks and Manet's and studied its impact on the performance of the network. For this purpose we modified & implemented a new AODV routing protocol which behaves as wormhole. We simulated different scenarios, where each one has one or two wormhole nodes that use the modified "B" AODV protocol. In different scenarios we changed the location of the wormhole nodes to evaluate the impact. Moreover, we changed the number of nodes in different topologies. The packet loss was measured. Similarly other parameters like throughput and end- to -end delay due to wormhole attack was calculated and
results were produced in the form of graphs using MS Excel 2010. The main advantage of this work is that it enlightens the vulnerabilities of the AODV protocol. Besides the study will help us to overcome the AODV protocol flaws so that it could be made more robust against the attack. Also the work presents the overall measurement of the impact when a network is under the wormhole attack and helps in designing the topology which is more robust. The limitation of the simulation is that the measurement of the impact on MANETs becomes difficult when the mobility of the nodes increases too much. The possible application of this work is that the study can help to determine the impact on other routing protocols and other layers also. Another application of our work is in determining the impact on sensor and mesh networks when under wormhole attack or other attacks as well.

A Mobile Ad hoc Network (MANET) is a collection of self configurable mobile node connected through wireless links. In MANET nodes which are within the range of each other can connect directly where as nodes which are not in the vicinity of each other rely on the intermediate node for communication. Each node in MANET can work as a sender, receiver as well as router. Communication in the network depends upon the trust on each other. In wormhole attacks, one malicious node tunnels packets from its location to the other malicious node. Such wormhole attacks result in a false route with fewer. If source node chooses this fake route, malicious nodes have the option of delivering the packets or dropping them. It is difficult to detect wormhole attacks because malicious nodes impersonate legitimate nodes The wormhole attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality. In this work, **Ajay Prakash Rai, Vineet Srivastava, and Rinkoo Bhatia (2012),** [5] analyzed wormhole attack nature in ad hoc and sensor networks and existing methods of the defending mechanism to detect wormhole attacks without require any specialized hardware. This analysis able to provide in establishing a method to reduce the rate of refresh time and the response time to become more faster.
In order to avoid the problem of using special hardware, a Round Trip Time (RTT) mechanism is proposed by Jane Zhen and Sampalli. The RTT is the time that extends from the Route Request (RREQ) message sending time of a node A to Route Reply (RREP) message receiving time from a node B. A will calculate the RTT between A and all its neighbors. Because the RTT between two fake neighbors is higher than between two real neighbors, node A can identify both the fake and real neighbors. In this mechanism, each node calculates the RTT between itself and all its neighbors. This mechanism does not require any special hardware and it is easy to implement; however it can not detect exposed attacks because fake neighbors are created in exposed attacks. The Delay per Hop Indicator (DelPHI) proposed by Hon Sun Chiu and King-Shan Lui, can detect both hidden and exposed wormhole attacks. In DelPHI, attempts are made to find every available disjoint route between a sender and a receiver. Then, the delay time and length of each route are calculated and the average delay time per hop along each route is computed. These values are used to identify wormhole. The route containing a wormhole link will have a greater Delay per Hop (DPH) value. This mechanism can detect both types of wormhole attack; however, it cannot pinpoint the location of a wormhole. Moreover, because the lengths of the routes are changed by every node, including wormhole nodes, wormhole nodes can change the route length in a certain manner so that they cannot be detected. Packet Leash is an approach in which some information in 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 mentioned above, 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. Unlike Packet Leash, Capkun et al. presented SECTOR, which does not require any clock synchronization and location information, by using Mutual Authentication with Distance-Bounding (MAD). Node A estimates the distance to another node B in its transmission range by sending it a one-bit challenge, which A responds to instantaneously. By using the time of flight, A detects whether or not B is a neighbor or not. However, this approach uses special hardware that can respond to a one-bit challenge without any delay as Packet leash.

Multicast is an efficient method to implement the group communication. In recent years, a number of different multicast protocols have been proposed for ad hoc networks. Robust and Scalable Geographic Multicast Protocol (RSGM) is one among them. RSGM is a geographic routing protocol which routes the data using the location of the nodes. Geographic routing protocols are known to be particularly vulnerable to attacks. One of the most powerful and serious attacks in adhoc networks is wormhole attack, preventing this attack has proven to be very difficult. In this work, an efficient method namely Multicast Authentication

Node Scheme is devised to detect and avoid wormhole attack in the RSGM protocol. This technique uses cryptographic concept to detect and prevent wormhole attack. **L. Sudha Rani , R. Raja Sekhar (2012),** [6], proposed system is simulated in network simulator (NS-2).
The Geographic multicasting routing mechanism has been presented in this work. Among the existing multicasting routing protocols the reason for selecting RSGM protocol is it handles empty zone problem very efficiently when compared to the other zone based protocols and it has an efficient source tracking mechanism which avoids the periodic flooding of source information. RSGM has the minimum control overhead and joining delay. The protocol can also scale to a large group size and a large network size, and can more efficiently support multiple multicast groups in the network. One possible attack on the RSGM protocol has been discussed in this work. The detection of such attack is difficult and is of course very much important. Multicast Authentication Node Scheme is the solution that is proposed to defend against the wormhole attack in RSGM protocol. This solution clearly shows that the protocol achieves higher Packet Delivery Ratio under all circumstances with different moving speeds, node densities, group sizes, and network sizes.

Mobile ad hoc networks (MANETs) is an infrastructure-less , dynamic network consisting of a collection of wireless mobile nodes that communicate with each other without the use of any centralized authority. Due to its fundamental characteristics, such as wireless medium, dynamic topology, distributed cooperation, MANETs is vulnerable to various kinds of security attacks like worm hole, black hole, rushing attack etc. In this work **Aarti et. al., (2013)** [7], studied mobile ad-hoc network and its characteristics, challenges, application, security goals and different types security attacks at different layers.
Due to dynamic topology, distributed operation and limited bandwidth MANET is more vulnerable to many attacks. In this work, **Aarti et. al., (2013)** [7] discussed MANET and its characteristics, challenges, advantages, application, security goals, various types of security attacks in its routing protocols. Security attack can classified as a active or passive attacks . Different security mechanisms are introduced in order to prevent such network.

Jyoti Thalor et. al., (2013) [8], according to them MANET (Mobile Ad-hoc Network) refers to a multi-hop packet based wireless network composed of a set of mobile nodes that can communicate and move at the same time , without using any kind of fixed wired infrastructure . MANET'S are actually self organizing and adaptive networks that can be formed and deformed on-the-fly without the need of any centralized administration. It generally works by broadcasting the information and used air as medium. It's broadcasting nature and transmission medium also help attacker to disrupt network. Many type of attack can be done on such Mobile Ad Hoc Network. The emphasis of this work to study wormhole attack, some detection method and different techniques to prevent network from these attack.
Wormhole refers to an attack on MANET routing protocols in which colluding nodes create an illusion that two remote regions of a MANET are directly connected through nodes that appear to be neighbors but are actually distant from one another. A wormhole attack is a particularly severe attack on MANET routing where two attackers, connected by a high-speed off-channel link, are strategically placed at different ends of a network. Consider Fig 2 [8] in which node A sends RREQ to node B , and nodes X and Y are malicious nodes having an out-of-band channel between them . Node X "tunnels" the RREQ to Y , which is legitimate neighbor of B. B gets two RREQ – A-X-Y-B and A-C-D-E-F-B. The first route is shorter and faster then the second, and chosen by B. Since the transmission between two nodes has rely on relay nodes, many routing protocols have been proposed for ad hoc network. In a wormhole attack, attackers "tunnel" packets to another area of the network bypassing normal routes as shown in Figure 1. The resulting route through the wormhole may have lower hop count than normal routes. In with this leverage, attackers using wormhole can easily manipulate the routing priority in MANET to perform eavesdropping, packet modification or perform a DOS attack . The entire routing system in MANET can even be brought down using the wormhole attack [8].

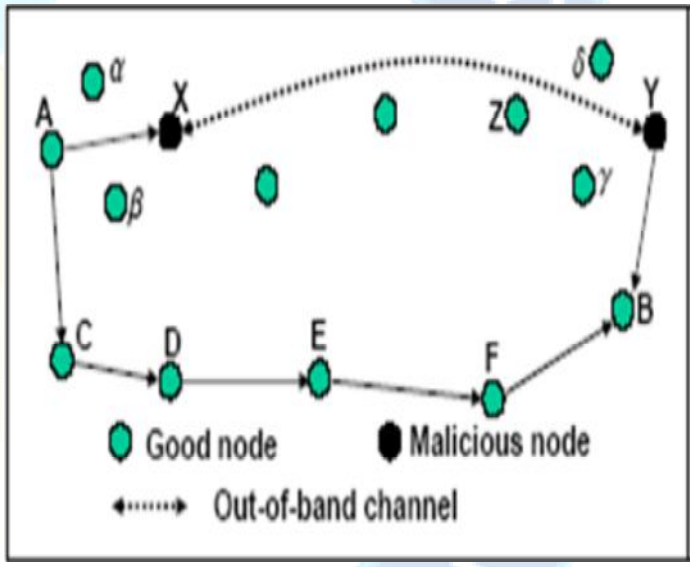

Fig. 2. The wormhole attack in MANET

Wormhole attacks in MANET significantly degrade network performance and threat to network security. Here we have basically surveyed the existing approaches which will help us in future to design a new approach for detecting the wormhole attack in Mobile Ad Hoc network .Overall a significant amount of work has been done on solving wormhole attack problem. We can't say one solution is applicable to all situations. So there is choice of solution available based on cost, need of security may lead better result, but can be costly, which may affect other networks need. Similarly some network require more security like military area network. A standard solution is still lacking, although several very useful solutions applicable to some networks have been described.

Mobile Adhoc Networks(MANET's) are refers to self organizing in nature. In MANET's communication is done through multi hops with dynamic topology. Mobile nodes

send data through wireless links, which means less secure environment and vulnerable to various attacks. There are various types of attacks which effect the data when it transfers from the source node to the destination node but wormhole attacks are most dangerous attacks and very frequently occurred in the wireless environment. In this work **Chandandeep kaur and Dr. Navdeep Kaur, (2014)** [9], discussed the various detecting and preventing techniques for wormhole attacks.

The Mobile Ad Hoc network is greatly influenced by wormhole attack .These attacks degrade the network performance and menace to network security .In this work various techniques are presented for detection and prevention of wormhole attacks .In future these approaches will help to efficiently remove the malicious nodes from the Mobile Ad Hoc networks .All above techniques based on different factors like cost ,need of security ,Quality of Service may lead better result but can be costly . So they cannot say that one solution is perfectly deal with all conditions .One factor may have effect on the other factor .Like some networks need more security like whether forecasting and military area may increase the cost. From all above solutions we can find the efficient method to prevent the wormhole attacks by equating all factors.

Mobile Adhoc Networks (MANET) are self organizing, decentralized networks and possess dynamic topology, which make them attractive for routing attacks. Attacks on ad hoc networks can be classified as passive and active attacks, depending on whether the normal operation of the network is disrupted or not. The security of the AODV and DSR protocol is compromised by a particular type of attack called 'Worm hole attack'. Wormhole attack is a network layer attack observed in MANET, which completely disrupts the communication channel. In This work **Mohamed Otmani, and Dr. Abdellah Ezzati, (2014)** [10], analysed the performance of AODV and DSR routing protocols with and without wormhole attack using Network Simulator 2. For analyzing the performance we considered total packets received, total bytes received, first packet received, last packet received, average end-to-end delay and throughput as measures.

The security of the Ad Hoc network routing protocols is still an open problem and deserves more research work. In this work, they analyzed effect of the Worm Hole attack in AODV and DSR routing. We have implemented Worm hole Attack against AODV and DSR routing protocol using Network Simulator 2, for analyzing the performance we considered total packets received, total bytes received, first packet received, last packet received, average end-to-end delay and throughput as measures. We presented the results of evaluation of both protocols. The results show that DSR performs better than AODV. Wormhole attack is a real threat against routing protocols in MANET .The detection and evasion of wormholes in an ad-hoc network is still considered as future challenging task.

The current demand of MANET is its security and robustness. MANET's operational performance also depends on security. An attacker can easily attack on MANET because of its open nature and bandwidth constraint. Most of research have been done on the MANET security. Wormhole attack is most severe threat to security of MANET. In which two faraway malicious nodes are linked to each other with high speed link called wormhole tunnel. Most of previous research work done on detection and prevention of wormhole attacks uses packet leashes, extra hardware (GPS, Directional Antenna etc.) and few modifies the source code of routing protocols to improve security. In this work, we propose a security model that will detect and avoid the wormhole attack in MANET using routing protocol i.e., AODV protocol. **Gulzar Ahmad Wani, and Dr. Sanjay Jamwal (2015)** [11], proposed security model has three phases. In the first phase, detection of malicious node is done by using Bogus RREQ and in second phase normal AODV operation is performed for detection of shortest path from source to destination. In the third phase, once again detection of attacker is done by using delay metric if there is presences of wormhole attack then it repeats from phase one otherwise selects the shortest route to destination discovered in phase second.

In this Work, they have proposed a security model that will detects and avoids the wormhole attack in Mobile Ad-hoc Network and makes MANET free from Wormhole attack. This proposed model is simple and does not use any hardware. In the first phase, it will detect the malicious node in MANET by using Bogus RREQ and then remove the involvement of malicious node in the Network and in second phase apply AODV protocol for finding the shortest route to the destination. In the last phase, it again checks for presence of wormhole attack using average delay. If there is presence of wormhole attack then start from phase one again otherwise select the route for data transmission that was discovered in second phase.

Samuel Jacob, D D Ambavade, and K T V Talele, (2015) [12] according to them the Mobile Ad hoc Networks (MANETs) is a collection of wireless nodes which interact with each other by sending packets to one another or on behalf of another node, without any central network infrastructure to control data routing. For communication, the nodes cooperatively forward data packets to other nodes in network by using the routing protocol. But, these routing protocols are not secure, thus paving the way for the MANET to be open to malicious attacks. A malicious attack which is commonly observed in MANET environment is wormhole attack. The objective of this work was to analyze the performance parameters of throughput, delay and packet loss in AODV with the existence of wormhole attack. Simulation results have shown that the performance parameters are affected very much when there is an attack due to wormholes.

The performance of an on- demand routing protocol i.e. AODV (Ad hoc on demand distance vector routing) is evaluated with and without wormhole attack. Three parameters of performance i.e packet delivery ratio, throughput, and average end to end delay have been considered. Results show that AODV performance gets badly affected by the wormhole attack.

Table1: Comparison Chart of different techniques

Detection Technique	Description	Merits	Demerits
Geographical leashes	Neighbour validation: Limit the packet travelling distance by using loose clock synchronization and location information.	Can find pinpoint location of wormhole.	Use of hardware device like GPS. High network overhead, huge storage required.
Temporal Leashes	Limit the propagation time of data packet using tight clock synchronization.	No extra hardware required.	Nodes must have accurate clock synchronization, huge storage required for authentication.
RTT (Round Trip Time)	Each node calculates the RTT between itself and all its neighbours to differentiate b/w fake and real neighbours.	Don't required any hardware. Easy to implement.	Cannot detect the attacks at all the time.
DELPHI	Delay time, length of each route are calculated and the average delay time per hop along each route is computed to identify wormhole.	Cannot detect the attacks at all the time.	Cannot pinpoint the wormhole location.
E2IW	Use the location information of the mobile nodes to find the presence of a wormhole.	Can find wormhole with a high detection rate and less overhead.	Need extra hardware. Costly.
TAODV	Describes Pre_AODV Wormhole Discovery Phase, Normal_AODV Route Establishment Phase and Post_AODV Wormhole Discovery Phase.	Detect the attack prior to sending the packets.	Increased end to end delay.

3. Conclusion:

As of late, with the appearance of globalization, the world is seeing a lofty improvement of secure MANET association with high degree of speed and accuracy. The world is changing itself into little and extensive pieces of social and business systems from a solitary township to a worldwide town which thusly makes the development with security issues bringing about high reliability level to the end to end clients. System assault location and dependable directing is indispensable for the future financial success and system security. Delicate figuring strategies, for example, fluffy rationale, neural systems, hereditary calculations are being embraced in demonstrating to decisively delineate standard MANET frameworks. In this paper, an endeavor has been made to audit the utilizations of cutting edge strategy based models utilized as a part of identification of pernicious hubs in MANET frameworks in view of models to be specific Geographical/Temporal rope, RTT, DELPHI, E2IW and TAODV applications. It is observed that AODV based distinctive models are broadly utilized as a part of late years for evaluation of amazing level steering along with attack disclosure, with most limited course following in MANET frameworks with streamlining on the premise of system and hub conduct criteria. The survey shows that grouping based models give practical gauges particularly on account of warm hole attack.

References:

[1] Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki, "A New Cluster-Based Wormhole Intrusion Detection Algorithm For Mobile Ad-Hoc Networks", International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 1, April 2009.
[2] Rutvij H. Jhaveri et. al., "MANET Routing Protocols and Wormhole Attack against AODV", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010.
[3] A.Vani et. al., " A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing In Ad Hoc Wireless Networks", International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 6 June 2011.
[4] Pirzada Gauhar Arfaat, Dr. A.H. Mir, "The Impact of Wormhole Attack on the Performance of Wireless Ad-Hoc Networks", IJCST Vol. 2, Issue 4, Oct . - Dec. 2011.
[5] Ajay Prakash Rai, Vineet Srivastava, and Rinkoo Bhatia, "Wormhole Attack Detection in Mobile Ad Hoc Networks",

International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 2, August 2012.
[6] L. Sudha Rani , R.Raja Sekhar, "Detection And Prevention Of Wormhole Attack In Stateless Multicasting", International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012.
[7] Aarti et. al., "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.
[8] Jyoti Thalor et. al., "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.
[9] Chandandeep kaur and Dr.Navdeep Kaur, "Detection and Prevention Techniques for Wormhole Attacks", International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 4926-4929.
[10] Mohamed Otmani, and Dr. Abdellah Ezzati, "Effects Of Wormhole Attack On AODV And DSR Routing Protocol Through The Using NS2 Simulator", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 2, Ver. XI (Mar-Apr. 2014).
[11] Gulzar Ahmad Wani, and Dr. Sanjay Jamwal, "Security Model to Detect and Avoid Wormhole Attack Using AODV Protocol", International Journal of Computer Science and Information Technologies, Vol. 6 (2) , 2015, 1044-1049.
[12] Samuel Jacob, D D Ambavade, and K T V Talele, "Performance Evaluation of Wormhole Attack In AODV" Int. Journal of Engineering Research and Applications, Vol. 5, Issue 1, (Part -6) January 2015, pp.70-72.