An Enhanced Wormhole Detection and Prevention Technique in MANETs

Suraj Joshi[#1], Pankaj Dev Chadha[*2]

[#] *M.Tech. Scholar, Computer Science & Engineering Department, GIMT Kanipla, KUK*

[*]*Asstt. Prof., Computer Science & Engineering Department, GIMT Kanipla, KUK*

[1]surajjoshi1212@gmail.com, [2]er.pankajdev@gmail.com

***Abstract*— In wireless network many types of attacks can be initiated but most of them are relatively easy to detect because of their property of dramatically altering the network statistics but one different type of attack we have consider is very important when considering security issues of network, is wormhole attack, which is difficult to detect & can harm by directing important data to unauthorized nodes. During the route discovery process, a wormhole can relay route request and response messages between distant nodes, creating the appearance of shorter routes to destinations. Since the wormhole can be anywhere along a route, a source will have to detect its existence somewhere along the route when a node sets up the route (on-demand).**

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.

***Keywords*— - MANET, AODV, WAMAN.**

I. INTRODUCTION

Wireless technology is rapidly achieving popularity in both home as well as business networking. This is a growing technology and has replaced all most all wired network due to its great advantages. This technology will allow users to access services and information electronically, irrespective of their geographic position. Wireless Networks are classified in two classes - infrastructure network and infrastructureless (ad-hoc) networks. In these, the ad-hoc networks works without any pre-existing infrastructure. They are easy to deploy and set up at any place and time, hence it has decreased the dependence of the infrastructure. So ad-hoc networks became a very important technique these days because of its features. Routing is the main constraint in the working with ad-hoc network. Routing is the integral part of any kind of the network as it not only exchanges the data but also control the information in the form of packets with its respective connected nodes in its range. There are varieties of routing protocols available in the area of the mobile ad-hoc networks. Due to the popularity of these networks, it is important to improve the quality of service for these networks. There are many parameters on which the quality of service depends. Witnessing and simulating these parameters behavior by varying different parameters for improving the performance of the ad-hoc network is the motivation for the chosen topic.

A. Security Attacks

Securing wireless ad hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information .Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber-attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two types:

- **Passive Attacks:** Passive attack is the attacks that do not disrupt proper operation of network .Attackers snoop data exchanged in network without altering it. Requirement of confidentiality can be violated if an attacker is also able to interpret data gathered through snooping .Detection of these attack is difficult since the operation of network itself does not get affected.
- Active Attacks: Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to perform the attacks. Active attacks involve some modification of data stream or creation of false stream. Active attacks can be internal or external.

a. External attacks are carried out by nodes that do not belong to the network.

b. Internal attacks are from compromised nodes that are part of the network.

Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation (masquerading or spoofing), modification, fabrication and replication.

- **Blackhole Attack:**

An attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it. A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those. An attacker listen the requests in a flooding based protocol.

- **Wormhole Attack:**

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. Routing can be disrupted when routing control message are tunnelled. This tunnel between two colluding attacks is known as a wormhole .In DSR, AODV this attack could prevent discovery of any routes and may create a wormhole even for packet not address to itself because of broadcasting. Wormholes are hard to detect because the path that is used to pass on information is usually not part of the actual network. Wormholes are dangerous because they can do damage without even knowing the network.

- **Byzantine attack:** A compromised with set of intermediate, or intermediate nodes that working alone within network carry out attacks such as creating routing loops ,forwarding packets through non - optimal paths or selectively dropping packets which results in disruption or degradation of routing services within the network.
- **Rushing attack:** Two colluded attackers use the tunnel procedure to form a wormhole. If a fast transmission path (e.g. a dedicated channel shared by attackers) exists between the two ends of the wormhole, the tunneled packets can propagate faster than those through a normal multi-hop route. The rushing attack can act as an effective denial-of-service attack against all currently proposed on-demand MANET routing protocols, including protocols that were designed to be secure, such as ARAN and Ariadne.
- **Replay attack:** An attacker that performs a replay attack are retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions **[**17].
- **Location disclosure attack:** An attacker discover the Location of a node or structure of entire networks and disclose the privacy requirement of network through the use of traffic analysis techniques **[**18], or with simpler probing and monitoring approaches **[**12]. Adversaries try to figure out the identities of communication parties and analyze traffic to learn the network traffic pattern and track changes in the traffic pattern. The leakage of such information is devastating in security.
- **Flooding:** Malicious nodes may also inject false packets into the network, or create ghost packets which loop around due to false routing information, effectively using up the bandwidth and processing resources along the way. This has especially serious effects on ad hoc networks, since the nodes of these usually possess only limited resources in terms of battery and computational power. Traffic may also be a monetary factor, depending on the services provided, so any flooding which blows up the traffic statistics of the network or a certain node can lead to considerable damage cost.
- **Sinkhole:** In a sinkhole attack, a compromised node tries to attract the data to itself from all neighboring nodes. So, practically, the node eavesdrops on all the data that is being communicated between its neighboring nodes. Sinkhole attacks can also be implemented on Ad hoc networks such as AODV by using flaws such as maximizing the sequence number or minimizing the hop count, so that the path presented through the malicious node appears to be the best available route for the nodes to communicate.
- **Spoofing Attack:** In spoofing attack, the attacker assumes the identity of another node in the network; hence it receives the messages that are meant for that node. Usually, this type of attack is launched in order to gain access to the network so that further attacks can be launched, which could seriously cripple the network. This type of attack can be launched by any malicious node that has enough information of the network to forge a false ID of one its member nodes and utilizing that ID and a lucrative incentive, the node can misguide other nodes to establish routes towards itself rather than towards the original node.
- **RERR Generation:** Malicious nodes can prevent communications between any two nodes by sending RERR messages to some node along the path. The RERR messages when flooded into the network may cause the breakdown of multiple paths between various nodes of the network, hence causing a no. of link failures.
- **Jamming:** In jamming, attacker initially keep monitoring wireless medium in order to determine frequency at which destination node is receiving signal from sender. It then transmit signal on that frequency so that error free receptor is hindered.

- **Traffic Monitoring:** It can be developed to identify the communication parties and functionality which could provide information to launch further attacks .It is not specific to MANET, other wireless network such as cellular, satellite and WLAN also suffer from these potential vulnerabilities.
- **Eavesdropping:** The term eavesdrop implies overhearing without expending any expending any extra effort. In this intercepting and reading and conversation of message by unintended receiver take place. Mobile host in mobile ad-hoc network shares a wireless medium. Majorities of wireless communication use RF spectrum and broadcast by nature. Message transmitted can be eavesdropped and fake message can be injected into network.
- **Traffic Analysis:** Traffic analysis is a passive attack used to gain information on which nodes communicate with each other and how much data is processed.
- **Replay Attack:** The attacker collects data as well as routing packets and replays them at a later moment in time. This can result in a falsely detected network topology or help to impersonate a different node identity. It can be used to gain access to data which was demanded by replayed packet.
- **Sybil attack:** The sybil attack especially aims at distributed system environments. The attacker tries to act as several different identities/nodes rather than one. This allows him to forge the result of a voting used for threshold security methods. Since ad hoc networks depend on the communication between nodes, many systems apply redundant algorithms to ensure that the data gets from source to destination. A consequence of this is that attackers have a harder time to destroy the integrity of information.
- **Sinkhole attack:** The attacking node tries to offer a very attractive link e.g. to a gateway. Therefore, a lot of traffic bypasses this node. Besides simple traffic analysis other attacks like selective forwarding or denial of service can be combined with the sinkhole attack.
- **Syn flooding:** This attack is denial of service attack. An attacker may repeatedly make new connection request until the resources required by each connection are exhausted or reach a maximum limit. It produces severe resource constraints for legitimate nodes.
- **De synchronization attack:** In this attack, the adversary repeatedly forges messages to one or both end points which request transmission of missed frames. Hence these messages are again transmitted and if the adversary maintains a proper timing, it can prevent the end points from exchanging any useful information. This will cause a considerable drainage of energy of legitimate nodes in network in an end-less synchronization-recovery protocol.
- **Overwhelm attack:** In this attack, an attacker might overwhelm network nodes, causing network to forward large volumes of traffic to a base station. This attack consumes network bandwidth and drains node energy.
- **Blackmail:** A black mail attack is relevant against routing protocols that uses mechanisms for identification of malicious nodes and propagate messages that try to blacklist the offender.
- **Denial of service attack:** Denial of service attacks are aimed at complete disruption of routing information and therefore the whole operation of ad-hoc network.
- **Gray-hole attack:** This attack is also known as routing misbehavior attack which leads to dropping of messages. Gray-hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase nodes drops intercepted packets with a certain probability.
- **Selfish Nodes:** In this a node is not serving as a relay to other nodes which are participating in the network. This malicious node which is not participating in network operations, use the network for its advantage to save its own resources such as power.
- **Man-in-the-middle attack:** An attacks sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver to reply to the sender.
- **Fabrication:** The notation “fabrication” is used when referring to attacks performed by generating false routing messages. Such kind of attacks can be difficult to identify as they come as valid routing constructs, especially in the case of fabricated routing error messages, which claim that a neighbor can no longer be contacted.
- **Impersonation:** Impersonation attacks are launched by using other node's identity, such as IP or MAC address. Impersonations attacks are sometimes are the first step for most attacks, and are used to launch further, more sophisticated attacks.

II. LITERATURE SURVEY

Routing security in ad hoc networks is often equated with strong and feasible node authentication and lightweight cryptography. A wide variety of secure extensions to existing routing protocols have been proposed over the years. However, the majority of these protocols are focused on using cryptographical solutions to prevent unauthorized nodes from creating seemingly valid packets [10]. Unfortunately, the wormhole attack

cannot be defeated by cryptographical measures, as wormhole attackers do not create separate packets -they simply replay packets already existing on the network, which pass all cryptographic checks.

Virtually all generalized secure extensions proposed for currently popular routing protocols do not alleviate wormhole attacks. However, since wormhole attack such a severe thread to ad hoc network security, several researchers have worked on preventing or detecting wormhole attacks specifically. In this section, we summarize and discuss their efforts. In section 2.1, we discuss a technique called 'packet leashes', which allows preventing packets from traveling farther than radio transmission range.

A. Packet leashes

Perhaps the most commonly cited wormhole prevention mechanism is 'packet leashes' by Hu et al [1], [20]. Hu proposes to add a secure 'leash' containing timing and/or Global Positioning System (GPS) information to each packet on a hop-by-hop basis. Based on the information contained in a packet leash, a node receiving the packet would be able to determine whether the packet has traveled a distance larger than physically possible.

Hu proposes two different kinds of leashes: geographical leashes and temporal leashes. Geographic leashes require each node to have access to up-to-date GPS information, and rely on loose (in the order of ms) clock synchronization. When geographical leashes are used, a node sending a packet appends to it the time the packet is sent ts and its location.

B. Time-of-flight

Another set of wormhole prevention techniques, somewhat similar to temporal packet leashes [1], is based on the time of flight of individual packets. Wormhole attacks are possible because an attacker can make two far-apart nodes see themselves as neighbors. One possible way to prevent wormholes, as used by Capkun et al [7], Hu et al [8], Hong et al [14], and Korkmaz [15], is to measure round-trip travel time of a message and its acknowledgement, estimate the distance between the nodes based on this travel time, and determine whether the calculated distance is within the maximum possible communication range.

C. Wormhole discovery from wormhole's effect

Several researchers worked on the wormhole attack problem by treating a wormhole as a misbehaving link. In such approaches, a wormhole attack is not specifically identified. Rather, the wormhole's destructive behavior is mitigated.

Consider the scenario shown in figure 1[9] Say that originally intruders are creating a wormhole between nodes A and M. To the network, it seems that nodes A and M are direct neighbors, and the link between them is evaluated using a link rating system. When the rating system determines the link A-M to be lossy, it avoids it -which can be detected by the attackers. They can then simply move on: create a fake link between, say, nodes B and L, or even B and M. Since the methods proposed in [16] and [11] do not differentiate between poorly performing links and wormhole intruders, discovery of a bad link between A and M does not trigger a security investigation, and the attackers can thus indefinitely continue to disrupt the network.

D. Specialized techniques

A wide variety of wormhole attack mitigation techniques have been proposed for specific kinds of networks: sensor networks, static networks, or networks where nodes use directional antennas. In this section, we describe and discuss such techniques, commenting on their usability and the possibility of their use in general mobile MANETs.

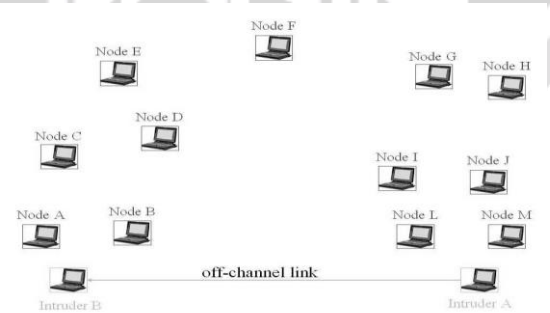

Figure 1: When a wormhole is treated as a misbehaving link, attackers are not detected and can create wormhole attacks targeting other nodes on the network.

E. Nodes with directional antennas

Directional antennas have been extensively studied in the general literature [9]. When directional antennas are used, nodes use specific 'sectors' of their antennas to communicate with each other, as shown in figure 2. Therefore, a node receiving a message from its neighbor has some information about the location of that neighbor; -it knows the relative orientation of the neighbor with respect to itself, as demonstrated in Figure 3. This extra bit of information makes wormhole discovery much easier than in networks with exclusively omni-directional antennas.

In [9], Hu and Evans propose a solution to wormhole attacks for ad hoc networks in which all nodes are equipped with directional antennas. Wormholes introduce substantial inconsistencies in the network, and can easily be detected.

F. Sensor networks: network visualization

Wang and Bhargava [10] introduce an approach in which network visualization is used for discovery of wormhole attacks in stationary sensor networks. In their approach, each sensor estimates the distance to its neighbors using the received signal strength. During the initial sensor deployment, all sensors send this distance information to the central controller, which calculates the network's physical topology based on individual sensor distance measurements. With no wormholes present, the network topology should be more or less flat, while a wormhole would be seen as a 'string' pulling different ends of the network together.

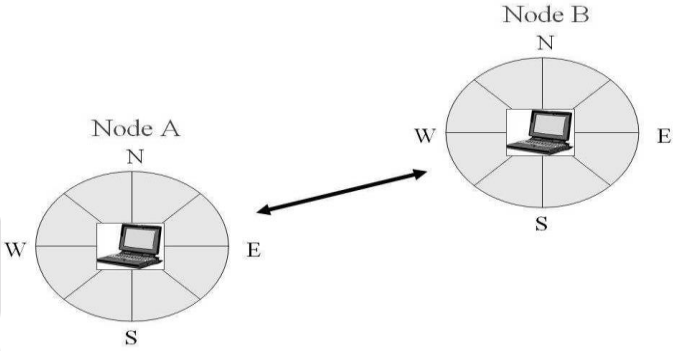

Figure 2.2: Nodes using directional antennas. When nodes A and B communicate, they send their messages on specific 'sectors': node A uses its North-East sector, node B -South-West. Therefore both nodes know how they are located with respect to each other. From knowing the sector on which it receives B's messages, A knows that B is located to the North-East. Had nodes A and B used omni-directional antennas, A would not be able to say anything at all about B's location.[9]

G. Sensor networks: use of location-aware guards

Lazos et al [17] develop a 'graph-theoretical' approach to wormhole attack prevention based on the use of Location-Aware 'Guard' Nodes4 (LAGNs). Lazos uses 'local broadcast keys' -keys valid only between one-hop neighbors -to defy wormhole attackers: a message encrypted with a local key at one end of the network cannot be decrypted at another end. However, the establishment of such keys is non-trivial in the possible presence of wormholes. Lazos proposes to use hashed messages from LAGNs to detect wormholes during the key establishment. LAGNs are assumed to be trusted, and, since their location is known, a node can detect certain inconsistencies in messages from different LAGNs if a wormhole is present. Without a wormhole, a node should not be able to hear two LAGNs that are far from each other, and should not be able to hear the same message from one guard twice.

H. Stationary networks: LiteWorp

Khalil et al [18] propose a protocol for wormhole attack discovery in static networks they call LiteWorp. In LiteWorp, once deployed, nodes obtain full two-hop routing information from their neighbors. While in a standard ad hoc routing protocol nodes usually keep track of who their neighbors are, in LiteWorp they also know who the neighbors' neighbors are, -they can take advantage of two-hop, rather than one-hop, neighbor information. This information can be exploited to detect wormhole attacks.

After authentication, nodes do not accept messages from those they did not originally register as neighbors. Also, nodes observe their neighbors' behavior to determine whether data packets are being properly forwarder by the neighbor, -a so-called 'watchdog' approach. LiteWorp adds an interesting wormhole-specific twist to the standard watchdog behavior: nodes not only verify that all packets are forwarded properly, but also make sure that no node is sending packets it did not receive (as would be the case with a wormhole) LiteWorp is, no doubt, interesting, but would not work at all in a scenario where node mobility is a factor. Since node's neighbors are determined and detected only once in LiteWorp, and the packets from non-neighboring nodes are rejected, no node movement is allowable. Therefore, LiteWorp is applicable to static networks only.

I. Networks with on-demand multipath routing: a statistical analysis approach

Song et al [19] approach the wormhole attack from a different angle. Song proposes a wormhole discovery mechanism based on statistical analysis of multipath routing. Song observes that a link created by a wormhole is very attractive in routing sense, and will be selected and requested (for routing) with unnaturally high frequency. This unusual route selection frequency can be statistically detected and used to identify wormhole links. Such statistical analysis approach is fundamentally different from the majority of others where, in general, wormhole detection is related to locating a node in absolute or relative terms (based on network topology, time of packet transmission, GPS coordinates, with respect to GPS-aware nodes, etc).

A cluster based wormhole attack avoidance technique introduced by [33]. The concept of hierarchical clustering with a novel hierarchical 32-bit node addressing scheme is used for avoiding the attacking path during the route discovery phase of the DSR protocol, which is considered as the under lying routing protocol. Pinpoint the location of the wormhole nodes in the case of exposed attack is also given by using this method.

Path Tracing (PT) algorithm offered by [30] to discover the wormhole attacks in MANET. PT computes the distance travelled per-hop by calculating RTT and speed of light. The distance is used to identify the abnormal routes. A normal distance is stored in the routing table which will be used as a threshold value for newly created paths. The network is such that it has loose clock synchronization. Per-hop distance is calculated by the source is also sent in the packet header. Each node in the path which receives the packet has to compare its calculated distance with the value that is present in the packet header. As a final check they test the number of appearances if there is a suspicious route in the routing table.

Modirkhazeni et al. [31] proposed neighbor discovery technique for handling wormhole attack. They look for data from unauthorized nodes/neighbors. It is assumed that nodes are static and number of nodes is fixed and every node identifies its authorized neighbors in initial stage and later rejects data from all nodes which are not authorized neighbors. The technique is quite effective in cases where we have static and fixed number of nodes. But it is not flexible in case where one need mobility and has no scalability.

The study by [21], introduced a protocol called Multi-path Hop-count Analysis (MHA), it is based on hop-count analysis to avoid the wormhole attack. Presumed that, too high or low of hop count is not fit well for the network. The novelty of the hop-count analysis in detecting wormholes, may be considered other similar works was issued before such as; [22]. In the method introduced by [23], the aim is detection of suspicious link and confirms them in the two steps; first, HELLO packet transmitted to all node located in transmission range. After HELLO request is received, node stores the senders address and delay time until next HELLO packet reached. For piggyback reply, the node adds the source recorded address and value of delay time. When destination node received the HELLO reply, the packet is checked and waits for information related to any outstanding requests. If there is no information available, then it treats as any other control packets.

The wormhole attack is particularly dangerous against many ad hoc network routing protocols in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of (and, thus a neighbor of) that node. For example, when used against an on-demand routing protocol such as dynamic source routing DSR) [3], [6] or ad hoc on-demand distance vector (AODV) [4], 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.

III. PROBLEM FORMULATION

A. Problem Definition

The central research dilemma is how to provide security protection to the network topology and the routing process in a wireless network. The major challenges include dynamic topology, decentralized control, limited resources, and the lack of information dissemination control. We investigate the problem in mobile ad hoc network environment. As building blocks for securing wireless network topology and routing, are of special interest for researchers.

During a wormhole attack **[**4], 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. For tunneled distances longer than the normal wireless transmission range of a single hop, it is easy for the attacker to make the tunneled packet than a normal multihop route. It is also possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire packet to be received before beginning to tunnel the bits of the packet, in order to minimize delay introduced by the wormhole. Due to the nature of wireless transmission, the attacker can create a wormhole even for packets not addressed to it, since it can overhear them in wireless transmission and tunnel them to the colluding attacker at the opposite end of the wormhole.

If the attacker performs this tunneling honestly and reliably, no harm is done; the attacker actually provides a useful service in connecting the network more efficiently. However, the wormhole puts the attacker in a very powerful position compare to other nodes in the network, and the attacker could utilize this position in a variety of ways. Furthermore, the attacker is invisible at higher layers; unlike a malicious node in a routing protocol, which can often easily be named, the presence of the wormhole and the two colluding attackers at either endpoint of the wormhole are not visible in the route.

B. Objective

Objective of our thesis is to avoid the Worm hole attack in the network and by initiating a new route discovery path. The new established path should give more delivery ratio and less delivery time. It should give increased throughput which shows that more packets are delivered to their destination now as compare to when Worm hole attack was there. The energy consumption should also get decreased.

The various objectives to formulate the problem can be outlined as follows:

- In this research we study few of wormhole Detection & Prevention techniques to identify wormhole attack in MANET.
- The objective of our work is to find an efficient method for Detection and Prevention of Worm hole in MANETs.

IV. PROPOSED WORK

A. Proposed Work

We suggest a new method to detect the wormhole attack in on demand routing protocol. Before each node transfers data, it is necessary to check node authentication that is important feature of security, to its nearest neighbor. For this purpose one approach is followed, which come to know wormhole node:

Provide a Digital Signature between sender & receiver node. According to this approach, the malicious node whose Digital Signature value does not match with the defined Digital Signature, cannot impersonate and use another node authentication.

Above written Proposed scheme can be easily understand through the algorithm shown in below.

Algorithm Steps for detection of wormhole node

1. Begin
2. Route discovery using AODV protocol by Sender node to the Fixed Destination.
3. Provide Digital Signature via sender node.
4. Compare the Digital Signature with Destination Node.
    a. If (satisfies criteria)
        i. then go to step 5.
    b. Else
        i. Wormhole Node Detected and infected node will be marked as Attacker_AODV_node and discard from the transmission line and go to step 5.(Worm_Att_DP)
5. Transmission starts.
6. These nodes are black listed by the nodes hence they are not involved in future routes in this particular network.
7. Whole process (from step1 to step 6) is repeated until we didn't get the specified goal. Goal can be:
    a. To get complete list of malicious nodes.
    b. To run for specified time.
    c. To run for specific number of packets etc.
8. End

Wormhole Detection and Prevention steps (Worm_Att_DP):

Step 1: Detection of Wormhole Attack

- Whenever a source node needs a route to destination the protocol starts route discovery. During route discovery, source node broadcast RREQ packets through neighboring nodes.
- If the destination address not matches with the RREQ packet then forwards it to its next hop. This process is repeated until it reaches the final destination.
- When source node starts sending packets, it sends to next node and that node sends to next until it reaches destination. The traversed path nodes are checked with the path nodes in routing table.
- If the traversed path nodes are not in the routing table, wormhole is detected and it is out band wormhole.

Step 2: Prevention of Wormhole Attack

- Wormhole nodes are announced to all other nodes. All nodes remove wormhole node id from its neighbor table and Routing Table.
- If any forwarding node receives the wormhole announcement node, it will send RERR message to source.

It will reinitiate route discovery process, and find the new path to the destination without wormhole node. Figure 3 describes the flowchart of proposed work.

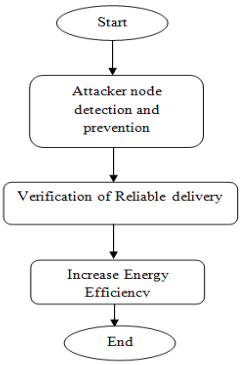

Figure 3: Flowchart of Proposed work

V. RESULT AND ANALYSIS

A. Simulation Model

The simulations were performed using Network Simulator 2 (Ns-2.34), particularly popular in the ad hoc networking community. The traffic sources are TCP. The source-destination pairs are spread randomly over the network. During the simulation, each node starts its journey from a random spot to a random chosen destination. This process repeats throughout the simulation, causing continuous changes in the topology of the underlying network. Different network scenario for different number of nodes and clusters are generated.

The model parameters that have been used in the following experiments are summarized in Table 1.

Table 1: Simulation Parameters

Parameters	**Value**
Simulator	NS 2.34
Simulation Area	500X500
Number of Mobile Nodes	35
Channel	Wireless
Routing Protocols	AODV
Simulation Time	200 Sec
Traffic Class	TCP
MAC Layer	802.11

B. Simulation

The simulation is performed to fulfill the research objective. The following figures show the simulation result with or without wormhole attacks. Transfer of packets for 35 Nodes using AODV protocol is shown in figure 4 in which no node is detected as wormhole attacker.

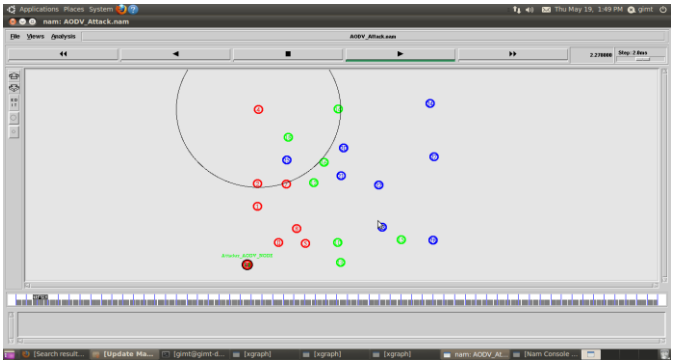

Figure 4: Transfer of packets for 35 Nodes using AODV

While Transfer of packets for 35 Nodes using AODV protocol is shown in figure 5 in which two nodes is detected as wormhole attacker. In figure 5 the node having black color and marked as AODV_Attacker_Node is the wormhole attacker detected after verification of digital signature.

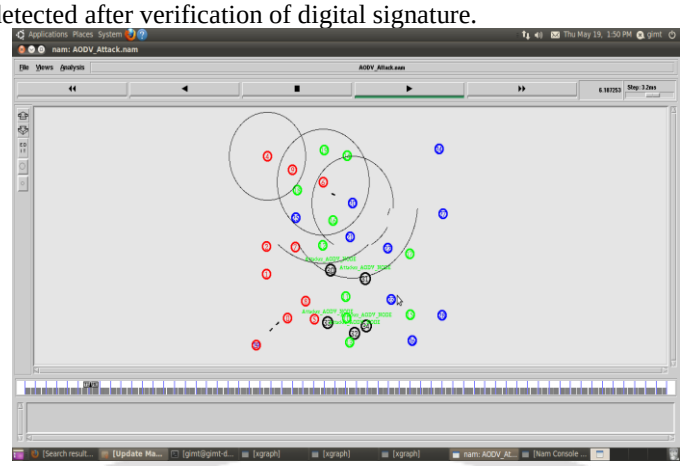

Figure 5: Transfer of packets for 35 Nodes with one node as wormhole

While Transfer of packets for 35 Nodes using AODV protocol is shown in figure 6 in which five nodes is detected as wormhole attacker. In figure 6 the node having black color and marked as AODV_Attacker_Node is the wormhole attacker detected after verification of digital signature.

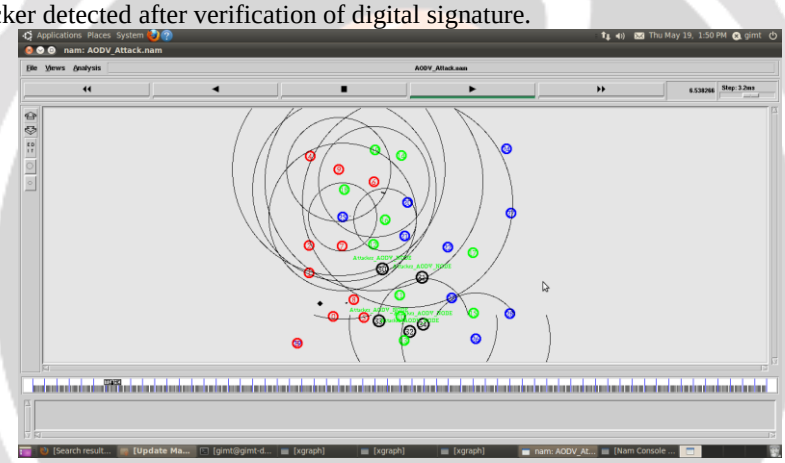

Figure 6: Transfer of packets for 35 Nodes with five nodes as wormhole

5.2 Results

Graph representation of the simulated environment for 35 Nodes using AODV approach is shown in figure 7 which include different parameters: Packet Delay, Throughput, Packet Lost.

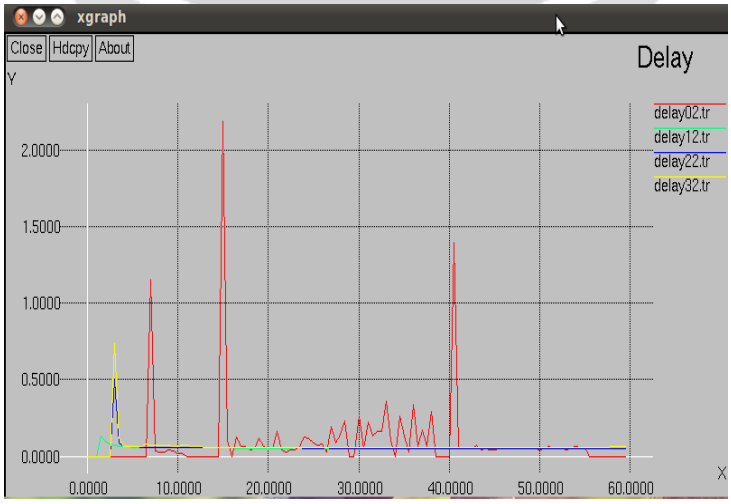

Figure 7: Graphical Representation of Delay packets for 35 Nodes

The graph represents Delay of individual trace files with respect to simulation time in millisecond of the simulated network. The Delay may vary based upon the trace file as shown in the graph. The units include the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted. The Delay calculated by ∑ (arrive time – send time) / ∑ Number of connections.

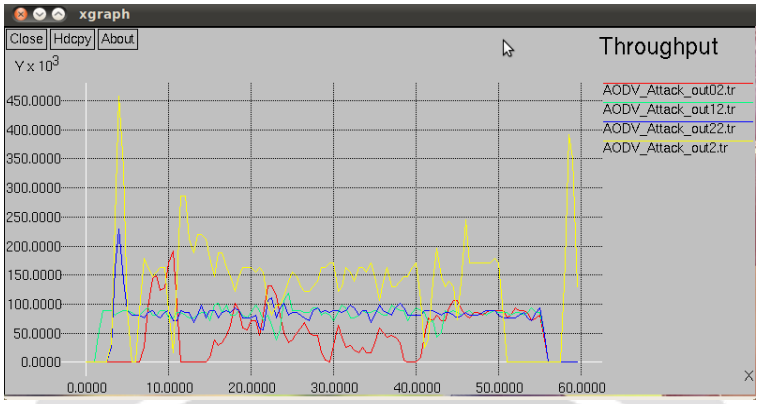

Figure 8: Graphical Representation of Throughput for 35 Nodes

The graph represents Throughput of individual trace files with respect to simulation time in millisecond of the simulated network. Throughput may vary based upon the trace file as shown in the graph as figure 8. The unit of throughput is (packet_size * recv * 8.0)/1000; #packet size * gives results in kbps.

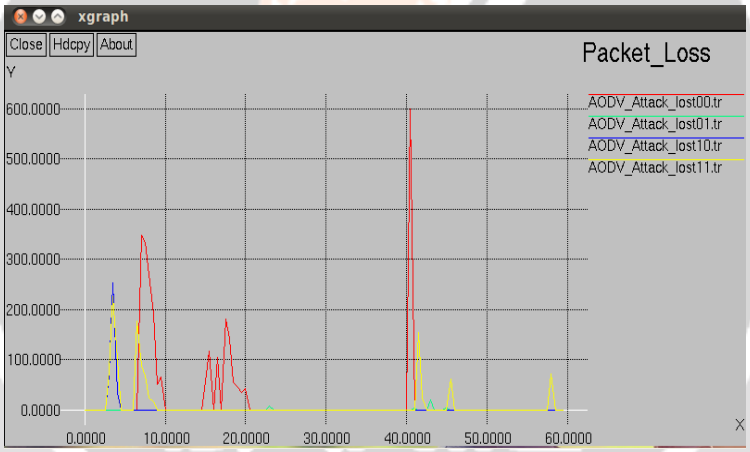

Figure 9: Graphical Representation of Packet Lost for 35 Nodes

The graph represents Packet Lost of individual trace files with respect to simulation time in millisecond of the simulated network. Packet lost may vary based upon the trace file as shown in the graph as figure 9. The unit of Packet Lost is (Number of packet send – Number of packet received). Figure 10 gives PDR v/s time for 35 nodes using AODV & Five nodes as wormhole.

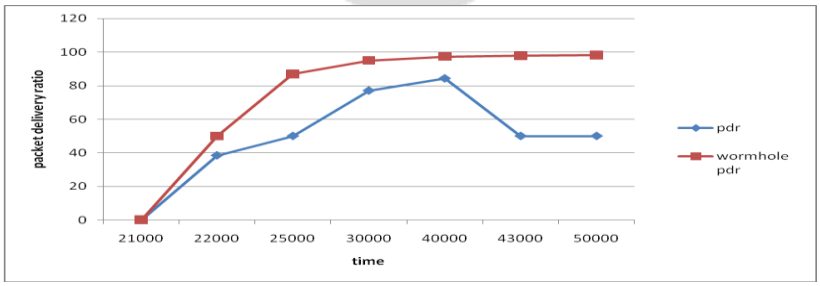

Figure 10: PDR v/s time for 35 nodes using AODV & Five nodes as wormhole

VI. CONCLUSION AND FUTURE SCOPE

A. Conclusion

Wormhole attacks are major problems that need to be addressed in wireless network security. Security of ad-hoc networks has recently gained momentum in the research society .Due to the open nature of ad hoc networks and their intrinsic lack of infrastructure, security exposures can be an impediment to basic network operation .Security solutions for MANET have to survive with a challenging environment together with limited energy and computational resources and lack of persistent structure of MANETS.

A wormhole is one of noticeable attack which is formed by two malicious nodes and a tunnel. In order to defend from wormhole attack we used the scheme which verifies the legitimate nodes in network through its digital signature. For checking the authentication of selected path, we used verification of digital signature of all sending node by receiving node. If there is no malicious node between the paths from source to destination, then source node creates a path for secure data transfer.

B. Future Scope

As we are detecting & preventing wormhole in the given work and also providing security by adding Digital Signature for nodes authentication, In future the work can be extended by adding some more security policies for preventing the data form intruders. Some more future aspects can be as follows:

- The work can be extended to study the robustness of Wireless Ad Hoc Networks for all types of protocols.
- A study can be conducted on the relationship between the average detection delay and the mobility of the nodes.
- More types of attacks including group attacks can be studied and their relations to the vulnerability of the protocols can be ascertained.

REFERENCES

[1] Y.-C. Hu, A. Perrig, D. B. Johnson, Packet leashes: a defense against wormhole attacks in wireless networks, INFOCOM 2003, Twenty-Second Annual Joint Conference of the IEEE Computer and Communication Societies, Vol. 3, March 30 -April 3rd 2003, pp. 1976-1986.

[2] S. Brands and D. Chaum, "Distance-bounding protocols," in Lecture Notes in Computer Science, vol. 839, Proc.Workshop Theory and Appl. Cryptographic Techniques on Advances in Cryptology—CRYPTO. Berlin, Germany, Aug. 1994, pp. 344–359.

[3] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in Mobile Computing, T. Imielinski and H. Korth, Eds. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.2

[4] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in Proc. 2nd IEEE Workshop on Mobile Comput. Syst. Appl., Feb. 1999, pp. 90–100.

[5] Frequently asked questions v4 for BAA 01-01, FCS communications technology, Defense Advanced Research Projects Agency. (2000, Oct.). [Online]. Available: http://www.darpa.mil/ato/solicit/baa01_01faqv4.doc

[6] D. B. Johnson, D. A. Maltz, and J. Broch, "The dynamic source routing protocol for multihop wireless ad hoc networks," in Ad Hoc Networking. Reading, MA: Addison-Wesley, 2001, ch. 5, pp. 139–172.

[7] S. Capkun, L. Buttyan, J.-P. Hubaux, SECTOR: Secure Tracking of Node Encounters in Multi-Hop Wireless Networks, October 2003, Processings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks.

[8] Y-C Hu, A. Perrig, D. Johnson , Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, Wise 2003, September 19, 2003, San Diego, California, USA.

[9] L. Hu, D. Evans, Using Directional Antennas to Prevent Wormhole Attacks, Proceedings of the 11th Network and Distributed System Security Symposium, pp. 131-141, 2003.

[10] W. Wang, B. Bhargava., Visualization of wormholes in sensor networks, Proceedings of the 2004 ACM workshop on Wireless Security, pp. 51-60, 2004.

[11] C. Chigan, R. Bandaru, Secure Node Misbehaviors in Mobile Ad Hoc Networks, Vehicular Technology Conference, 2004, VTC 2004, IEEE 60th, Volume 7, 26-29 Sept. 2004, pp. 4730-4734.

[12] L. Lazos, R. Poovendran, Serloc: Secure Range-Independent Localization for Wireless Sensor Networks, Proceedings of the ACM Workshop on Wireless Security, pp. 21-30, October 2004.

[13] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in Proc. Symp. Netw. Distrib. Syst. Security, Feb. 2004.

[14] F. Hong, L. Hong, C. Fu, Secure OLSR, Advanced Information Networking and Applications, AINA 2005, 19th International Conference On, Vol. 1, 25-30, pp. 713-718, March 2005.

[15] Korkmaz T., Verifying Physical Presence of Neighbours against Replay-based Attacks in Wireless Ad Hoc Networks, Information Technology: Coding and Computing 2005, ITCC 2005, International Conference On, 2005.

[16] A. Baruch, R. Curmola, C. Nita-Rotaru, D. Holmer, H. Rubens, On the Survivability of Routing Protocols in Ad Hoc Wireless Networks, Converence on Security and Privacy for Emerging Areas in Communications, SecureComm 2005, September 2005.
[17] L. Lazos, R. Poovendram, C. Meadows, P. Syverson, L.W. Chang, Preventing Wormhole Attacks on Wireless Ad Hoc Networks: a Graph Theoretical Approach, IEEE Communication Society, WCNC 2005.
[18] I. Khalil, S. Bagchi, N. B. Shroff, A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks, Proceedings of the 2005 International Conference on Dependable Systems and Networks (DSN'05).
[19] N. Song, L. Qian, X. Li, Wormhole Attack Detection in Wireless Ad Hoc Networks: a Statistical Analysis Approach, Parallel and Distributed Processing Symposium, 2005, Proceedings of, 19th IEEE International IPDPS'05, 04-08 April 2005.
[20] Y.-C. Hu, A. Perrig, D. B. Johnson, Wormhole Attacks in Wireless Networks, Selected Areas of Communications, IEEE Journal on, vol. 24, numb. 2, pp. 370-380, 2006.
[21] Jen, S.-M., C.-S. Laih, and W.-C. Kuo, A hop-count analysis scheme for avoiding wormhole attacks in MANET. Sensors, 2009. 9(6): p. 5022-5039.
[22] Djenouri, D., et al. On securing manet routing protocol against control packet dropping. in Pervasive Services, IEEE International Conference on. 2007. IEEE.
[23] Naït-Abdesselam, F., Detecting and avoiding wormhole attacks in wireless ad hoc networks. Communications Magazine, IEEE, 2008. 46(4): p. 127-133.
[24] Khalil, I., S. Bagchi, and N.B. Shroff, MOBIWORP: Mitigation of the wormhole attack in mobile multihop wireless networks. Ad Hoc Networks, 2008. 6(3): p. 344-362.
[25] Shaily Mittal, Prabhjot Kaur (2009),"PERFORMANCE COMPARISION OF AODV, DSR and ZRP ROUTING PROTOCOLS IN MANET'S", 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies, December 2009.
[26] Abdul Hadi Abd Rahman and Zuriati Ahmad Zukarnain "Performance Comparison of AODV, DSDV and I-DSDV Routing Protocols in Mobile Ad Hoc", European Journal of Scientific Research,Vol.31 No.4 (2009).
[27] K. Amjad, A.J. Stocker, "Impact of node density and mobility on the performance of AODV and DSR in MANETS", 7th International Symposium on Communication Systems Networks and Digital Signal Processing, July 2010, IEEE.
[28] Malhotra, A., D. Bhardwaj, and A. Garg. Wormhole attack prevention using clustering and digital signatures in reactive routing. in Networking, Sensing and Control (ICNSC), 2012 9th IEEE International Conference on. 2012. IEEE.
[29] Anitha, P. and M. Sivaganesh, Detection and Prevention of Wormhole Attack in MANETS using Path Tracing. International Journal of communications and networking systems, 2012. 1(2).
[30] Sakthivel, T. and R. Chandrasekaran, Detection and prevention of wormhole attacks in MANETs using path tracing approach. European Journal of Scientific Research, 2012. 76(2): p. 240-252.
[31] Modirkhazeni, A., et al., Mitigation of Wormhole Attack in Wireless Sensor Networks, in Trustworthy Ubiquitous Computing. 2012, Springer. p. 109-147.
[32] Ahuja, R., A.B. Ahuja, and P. Ahuja. Performance evaluation and comparison of AODV and DSR routing protocols in MANETs under wormhole attack. in Image Information Processing (ICIIP), 2013 IEEE Second International Conference on. 2013. IEEE.
[33] Banerjee, S. and K. Majumder, WORMHOLE ATTACK MITIGATION IN MANET: A CLUSTER BASED AVOIDANCE TECHNIQUE. International Journal of Computer Networks & Communications, 2014. 6(1).
[34] Rawat, C., Wormhole Attack Detection Protocol using Time Stamp with Security Packet. International Journal of Computer Science and Information Technologies, 2014. 5(1): p. 621-626.
[35] Anal Patel et. Al., "Defending Against Wormhole Attack in MANET", in International Conference on Communication Systems and Network Technologies, 2015.
[36] Aakanksha Kadam, Niravkumar Patel, Vaishali Gaikwad," Detection and Prevention of Wormhole attack in MANET" International Research Journal of Engineering and Technology (IRJET), Volume: 03 Issue: 03 | Mar-2016, pp 388-393.