Volume 4, Issue 1, January 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Review on Wormhole Security and Their Detection Scheme

Kamini Singh
ME(IT)
Department of Computer Science and IT
IET DAVV, Indore (MP), India

Gyan Singh
ME(CS)
Department of Computer Science and IT
MITM , Indore (MP), India

Abstract ***Due to wireless communication in Mobile Ad hoc Network (MANET) it is vulnerable to different routing attacks. One of the severe network layer attack is wormhole attack, which totally disrupts the channel without disturbing the traditional routing protocol. In this paper, we have discussed about wormhole attack, its behavior and technique of its deployment, detection and prevention available currently. At last we suggested a cluster-based energy-efficient method to detect and prevent malicious node in the cluster.***

Keyword: MANET, AODV, WSN, Wormhole, Cluster-based.

1. INTRODUCTION

Wireless networks are very popular and useful today. There are two types of wireless networks Infrastructure based and infrastructure less(decentralised) [1].

Infrastructure basedNetworks: A network with fixed and wired gateways. When a mobile node goes out of range of one base station, then it connects tothe new base station.

Infrastructure less (ad hoc) Network: Each node of this network behaves as a router and work in the discovery and maintenance of routes to other nodes. In Latin, ad hoc word means "for this" further meaning "for this purpose only". In an ad hoc network-

- All nodes are mobile and connected in dynamic manner.
- No default router available.
- Potentially every node becomes a router, it must be able to forward traffic on behalf of others[2].

Wireless Ad-hoc networks are divided in three sub networks.

- Mobile Ad hoc networks
- Wireless Sensor network
- Wireless Mesh network

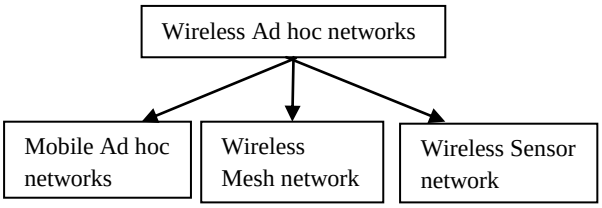

Figure 1: Classification of wireless Ad-hoc networks

1.1 MANET

Mobile ad hoc network (MANET) includes auto configuring nodes that can move freely and use wireless equipment for communication with each other. This network does not need a concentrated entity,connectivity is maintained in a decentralized way. The nodes communicate with each other by creating a multi-hop radio network, each node act as router which can receive and forward the data packets.

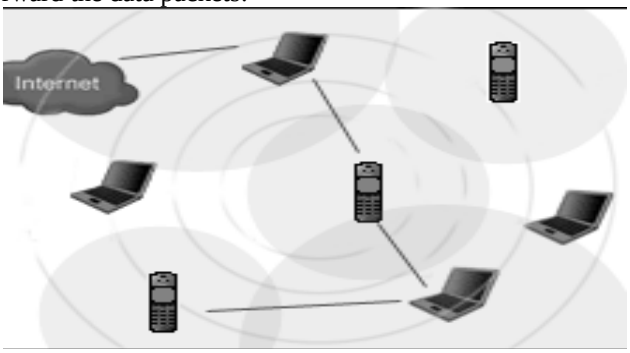

Figure 2: Example of mobile ad hoc network [10]

1.2 WMN

In a wireless mesh network (WMN) each node communicates with the other nodes via radio wave, transmits its own data and collaborates with the other nodes in order to relay their data.

1.3 WSN

Wireless sensor network (WSN) consists of a gateway or base station, which communicate with other wireless sensorsby a radio link. The received data via the sensor node, compressed, and transmitted to the gateway directly.The major concern in wireless ad-hoc network is secure, because sensor nodes have been deployed in the rough environment. If there are no security features in wireless sensor networks, the attackers caneffect on various parts like spreading false alarms, preventing the event detection, draining the energy of the network, the risk of failing the privacy and confidentiality of information and altering traffic [1].

1.4 MANET Issues:

The major issues [2] that affect the design, deployment, and performance of an adhoc wireless system as follows:

a) ***Power awareness****:* Since the nodes in an Ad-hoc network typically run on batteries and are deployed in hostile terrains, they have power requirements,onesignificant attribute of cluster-based routing is that it can make a dynamic topology appear less dynamic. In order to implement a dynamic hybrid routing scheme, efficient clustering algorithms must be designed.

b) ***Dynamic topology:*** The nodes are mobile and hence the network is self-organizing. Because of this, the topology of the network keeps changing over time.

c) ***Quality of service (QoS):*** Providing constant QoS for different multimedia services in frequently changing environment.

d) ***Multicast Routing:*** Designing of the multicast routing protocol for a constantly changing MANET environment.

e) ***Security****:* Security in an Ad-hoc network is extremely important in scenarios such as a battlefield. The five goals of security- confidentiality, integrity, authentication, availability and non repudiation.

f) ***Distributed network****:* MANET is a distributed wireless ad hoc network without any fixed infrastructure.

1.5 Routing Technology

The aim of routing in a MANET is to detect the most recent topology scenario of a continuously changing network for finding the valid route to a specific node. The routing protocols in a MANETare classified into two classes: Reactiverouting protocols (e.g. AODV, DSR, TORA) and Proactive routing protocols (e.g. OLSR,DSDV,CGSR). In the first type of routing, nodes find routes only when they have to send data to the destination node whose route is not known. While second one, nodes regularly exchange topology information, and hencenodes can have route information any time when they want to send data. Next we describe standard routing protocols that are researched actively, that is, AODV and OLSR.

AODV

AODV is a reactive routing protocol designed for a mobile ad hoc network. InAODV, when a source node S wants to send adata packet to a destination node D and does not have a route to D, it initiates the route discovery by broadcasting a route request (RREQ) to its neighbors. The immediate neighbors who receive this RREQ rebroadcast the same RREQ to the neighbors. This process is repeated until there reaches to the destination node.Upon receiving the first arrived RREQ,thenthedestination node sends a route reply (RREP) to the source node through the reverse path where the RREQ arrived. Same RREQ that arrives later will be ignored by the destination node.In addition, AODV enables intermediate nodes that have sufficiently fresh routes (with destination sequence number equal or greater than the one in the RREQ) to generate andsend a RREP to the source node [7][9].

OLSR

OLSR [9] is a proactive routing protocol that is,it is based on the periodic exchange of topology information. The key concept of OLSR issue of multipoint relays(MPR) to provide an efficient flooding mechanism by reducing the number of transmissions required. In OLSR,each node selects its own MPR from its neighbors.Each MPR node maintains the list of nodes that were selected as an MPR, this list is called an MPR selector list. Only nodes selected asMPR nodes are responsible for advertising, as well as forwarding an MPR selector list advertised by other MPRs.

Routing Messages in OLSR — Generally, in the OLSRprotocol, two types of routing messages are used, a HELLO message and a topology control (TC) message.A HELLO message is the message that is used for neighbor sensing and MPR selection. InOLSR each node generates a HELLO messageperiodically. A node's HELLO message contains its own address and the list of its one-hop neighbors.By exchanging HELLO messages, each node can learn a complete topology up to two hops. HELLO messages are exchanged locally by neighbor nodes and are not forwarded further to other nodes. A TC message is the message that is used for route calculation. In OLSR, each MPRnode advertises the TC messages periodically. ATC message contains the list of the sender'sMPRselected. In OLSR, only MPR nodes are responsible for forwarding TC messages. Upon receiving TC messages from all of the MPRnodes, each node can learn the partial network topology and can build a route to every node in the network.

In paper[4] some of the security attacks that MANETs are susceptible to, at different layers in the network are as shown in Table 1.

Table 1: Attacks in MANET

Layer	**Attack**
Mac	Jamming attack
Network	**Wormhole Attack** , Black Hole Attack,Byzantine Attack, Information Disclosure Attack, Man-in-Middle Attack, Neighbor Attack, Routing Attack, Stealth Attack
Transport	Session Hijacking Attack
Application	Repudiation Attack
Multilayer	DoS Attack, Sybil Attack, Misrouting Attack, Device Tampering Attack, Jellyfish Attack, Eclipse Attack

2. LITERATURE SURVEY

2.1 BACKGROUND

Wormhole attack is a network layer attack deployed by malicious nodes by creating a tunnel via which the packets are replayed to malicious nodes disrupting the communication channel and corrupting the routing process. Wormhole tunnel is formed by any two malicious nodes (generally at distant location) which collude together to create an illusion that they are one hop away, causing the routing of packets to happen through them as neighbor nodes. Once wormhole peers establish the tunnel successfully, they can replay, drop the packets or selectively forward them and tamper the packets [8].

Three types of wormhole attack are:

1. All Pass: In this wormhole node will not disturb the communication and allow all packets to be passed.
2. All Drop: In this not a single packet reach to destination, as all are dropped by malicious nodes.
3. Threshold: Wormhole drops the packet whose size is greater than or equal to the threshold size.

In an ad hoc network many works have been done on detecting and preventing wormhole attack specifically. Here we have discussed some existing technique to launch this attack and some discovery and prevention techniques.

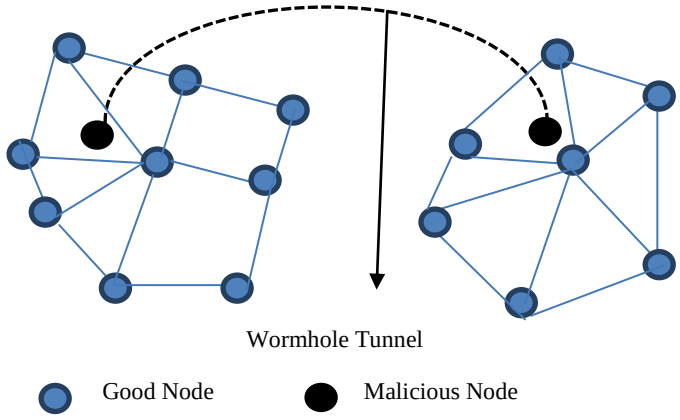

Figure 3: The wormhole attack

2.2 Wormhole Deployment Technique

Wormhole attacks can be launched using several modes, among these modes, we mention some of the modes:

***Wormhole using Encapsulation*:** In this mode a malicious node present one side of the network, hears their packet and tunnels it to a second colluding party at adistant location near the destination. The second party, then rebroadcasts the RREQ. The neighbors of the secondcolluding party receive the RREQ and drop any further legitimate requests that may arrive later on legitimatemultihop paths. The result is that the routes between the source and the destination go through the two colludingnodes that will be said to have formed a wormhole between them. This prevents nodes from discovering legitimate paths that are more than two hops away.Any routing protocol that uses the metric of shortest path to choose the best route is vulnerable to this mode of wormhole attack.This mode of wormhole attack is easy to launch since the two ends of the wormhole do not need to have any cryptographic information, nor do they need any special capabilities, such as a high speed wire line link or a high powersource [12].

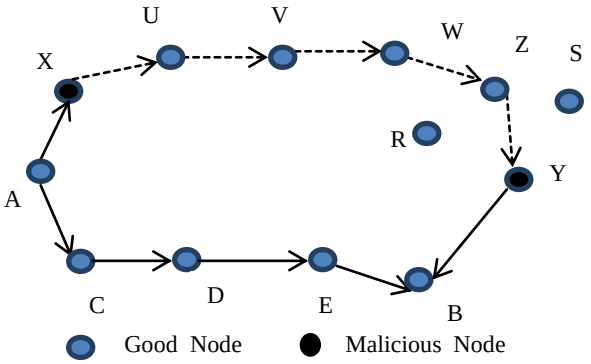

Figure4: Wormhole through packet encapsulation

Wormhole using Out-of-Band Channel: In this mode, the wormhole attack is launched by a high-quality, single-hop, out-of-band link (called tunnel) between the malicious nodes. This tunnel can be achieved, by using a direct wired link or a long-range directional wireless link [5].Consider the scenario depicted in Figure 5. Node A sends a RREQto 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 a legitimate neighbor of B. Node Y broadcasts the packet to its neighbors, including B. B gets two RREQs—A-X-Y-B andA-C-D-E-F-B. The first is both shorter and faster than the second, and is thus chosen by B[12].

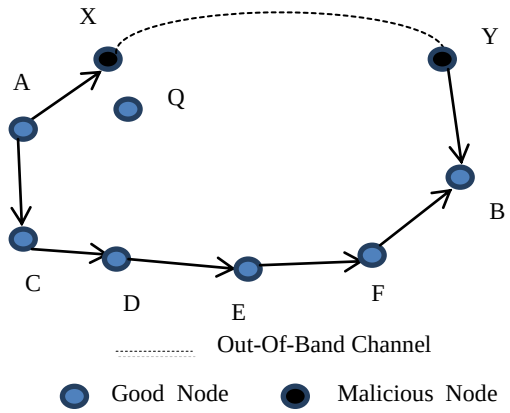

Figure5:Wormhole using Out-of-Band Channel

Wormhole Using High-power Transmission Capability: In this type of attack, only one malicious node having high-power transmission capability exists in the network and this node can communicate with other normal nodes from a long distance. When a malicious node receives the RREQ, it broadcasts the request at a high-power level. Any node that hears the high-power broadcast rebroadcasts the RREQ towards the destination. By this method, the malicious node increases its chance to be on the routes established between the source and the destination even without the participation of another malicious node. This attack can be mitigated if each sensor node is able to accurately measure the received signal strength.Figure 6 presents an example of a wormhole attack usinghigh-powertransmission. Consider that sensor nodes S(source) and Sink (destination) try to discover the shortest path between them in the presence of the one malicious node M with high-power transmission capability. Nodesbroadcasta RREQ, A and M1 receives the RREQ and rebroadcast it again. Node A can send the RREQ message to the sink in five hops (S-A-B-C-D-Sink), while the malicious node M is able to send it in four hops (S-M-CD-Sink). Hence, the sink chooses the second route since it appears to be the shortest path. This kind of attack is alsocalled as "black hole" attack[5].

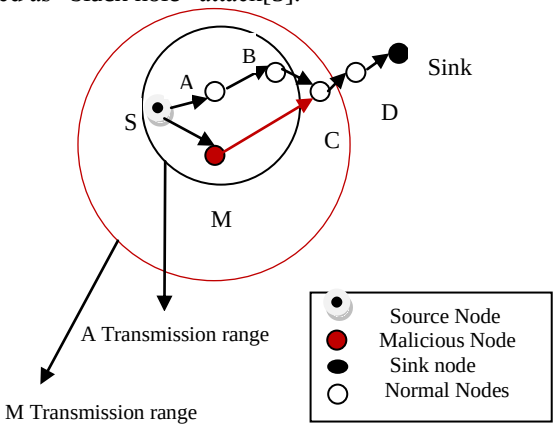

Figure 6: Malicious node increases its chance to be in theroutesestablished by using high-power transmission.

Wormhole Using Packet Relay: In this mode a malicious node relays data packets of two distant nodes to convince them thatthey are neighbours. It can be launched by even one malicious node. Cooperation by a greater number of malicious nodes serves to expand the neighbor list of a victim node to several hops. It is carried out by an intruder node X located within transmission range of legitimate nodes A and B, where A and B are notthemselves within transmission range of each other.Intruder node X merely tunnels, control traffic between Aand B (and vice versa), without the modification presumed by the routing protocol, e.g. without stating its address as the source in the packet header so that Xisvirtually invisible. Node X can afterwards drop tunneled packets or break this link at will. Two intruder nodes X and X′,connected by a wireless or wired private medium, can also collude to create a longer(and more harmful)wormhole, as shown in Figure 7[12].

Wormhole using Protocol Deviations: Thewormholeattack can also be launched through protocoldeviations. Duringthe RREQ transmission, the nodes typically back off for a random amount of time before forwarding reduce MAC layer collisions. A malicious node can create a wormhole by simply not complying with the protocol and broadcasting without backing off. The purpose is to let the request packet it forwards arrive first at the destination.The classification of such an attack facilitates the design of prevention and detection methods.

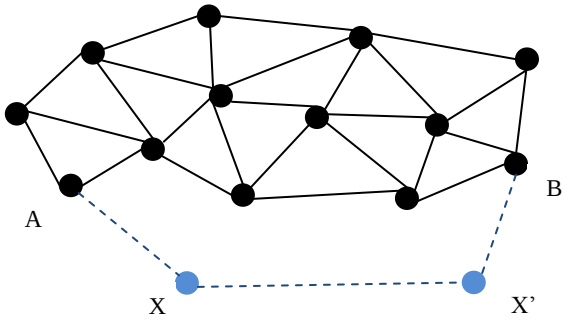

Figure7. A longer wormhole created by two colluding nodes

2.3 Detection and Solution of Wormhole Attack

A. Hop counting method and DelPHI

Both the hop count and delay per hop indication (Delphi) monitor for wormhole detection.The fundamental assumption is that the delay a packet experiences under normal circumstances for propagating one hop will become very high under wormhole attack as the actual path between the nodes is longer than the advertised path. It is a two step process.In the first phase the route information is collected from a set of disjoint paths from sender to receiver. Each sender will include a timestamp on a special DREQ packet, and sign it before sending it to the receiver. Each node upon receiving the packet for the first time will include its node ID and increase the hop count by 1 and discards the packet next time onwards. DREP packets will be sent by the receiver for each disjoint path received by it. This procedure is carried out for three times and the shortest delay as well as hop count information will be selected for wormhole detection. In the second phase, the round trip time (RTT) is taken by calculating the time difference between the packet, it had sent to its neighbor and the reply received by it. The delay per hop value (DPH) is calculated as RTT/2h, where h is the hop count to the particular neighbor. Under normal circumstances, a smaller h will also have smaller RTT. However, under wormhole attack, even a smaller hop count would have a larger RTT. If one DPH value for node X exceeds the successive one by some threshold, then the path through the node X to all the other paths with DPH values larger than it is treated as under wormhole attack[2][17].

B. Distance-bounding/Consistency-basedApproaches

The majority of researchers tries to prevent wormholesusing distance-bounding techniques[5], which allow two communicating sensor nodes to estimate the actual distance between them. Distance-bounding techniques are based on message traveling time information,directional antennas or geographical information. These techniques generally require specialized hardware and therefore they may be considered impractical for certain networks.

Message Traveling Time Information Solutions:

Message travelling time information is usually expressed in terms of round trip time (RTT). One way to prevent wormhole attack, is to measure RTT of a message and its acknowledgement, estimate the distance between nodes based on this travel time and determine whether the calculated distance is within the maximum possible communication range.

Special Hardware-based Solutions:

It is based on the fact that in adhoc networks with no wormhole link, if one node sends the packets in a given direction, then its neighbor will receive that packet from the opposite direction. Only when the directions are matched in pairs, the neighboring relation is confirmed. Necessarily each node requires a special hardware i.e. directional antenna [17].

C. Location and Time Based Solutions

Most of the proposed wormhole solutions inthe literatureare based on location or time. Packet leashes have been specifically two types:geographical and temporalleashes[1]. Geographical leash is one in which the sender inserts its own

position and sending them into the packet, the receiver will estimate the maximum distance between the sender and itself based on its own position and receiving time. If the distance exceeds the transmission range, the packet will be discarded. The other type is temporal leash. In this mechanism assumes that the maximum transmission speed of radio signal is the speed of light, thus the expiration time of a packet can be estimated using the maximum transmission range and the speed of light. The expiration time of the packet is inserted into the packet, and then thereceiver can check whether the received packet has expiredor not based on its receiving time. A drawback of packetleashes is that it requires extremely tight timesynchronization and GPS[3]. In Temporal Leashes, the sender appends the sending time to the packet and the receiving node computes a travelling distance of that packet assuming propagation at the speed of the light and using the difference between packet sending time and packet receiving time. This solution requires a fine grained synchronization among all nodes.

D. Time-of-flight

Another set of wormhole prevention techniques is similar to temporal packet leashes, is based on the time of flight of individual packets. One possible way to prevent wormholes 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 determines whether the calculated distance is within the maximum possible communication range. The basis of all these approaches is the following. The Round Trip Travel Time (RTT) α of a message in a wireless medium can be related to the distance *d* between nodes, assuming that the wireless signal travels with a speed of light *c*: d= δ*c/2 and δ =2d/c . The neighbor status of nodes is verified if *d* is within the radio transmission range *R*: *R* > *d* (*d* within transmission range) *R* >δ *c/2 and δ <2*R/c* .In essence, the use of RTT eliminates the need for tight clock synchronization required in temporal leashes: a node only uses its own clock to measure time. The approaches based on RTT that one node sends a packet to another; the answer should arrive very shortly, ideally within the amount of time a wireless signal would travel between the nodes. [13][19].

E. Visualization based method

Multi-dimensional scaling-visualization of wormhole (MDS-VOW) is used to detect wormhole attacks in static WSNs. In this approach using the received signal strength every node measures the distance to its neighbor. Based on measurements, base station calculates the network's physical topology. It is observed that the network with malicious nodes has different visualization from that with normal nodes. In absence of wormholes, topology should be more or less flat, where as in their presence 'string' pulling different ends of network are seen. It reconstructs the layout of the sensors using multidimensional scaling scheme. The anomalies, which are introduced by the fake connections through the wormhole, will bend the reconstructed surface to pull the sensors that are far away to each other. Therefore, MDS-VOW could locate the wormhole connections. In MDS-VOW, all sensor nodes are required to send their neighbor lists to the base station[17].

F. Graph theory method

According to this method, limited location-aware guard nodes (LAGNs) are nodes which have knowledge of location and origination that can be acquired by GPS receivers are used. Between each one hop neighbors, LAGNs use "local broadcast keys". To detect wormhole attack, it is not possible to decrypt the message that is encrypted with a local key – encrypted with the pair-wise key. Duringkey establishment, authors used hashed messages from LAGNs to detect wormholes. If a wormhole is present, node can detect certain inconsistencies in messages from different LAGNs. In the absence of the wormhole, a node should be unable to hear two LAGNs that are far away from each other [17].

G. Trust Based Model

Another significant method to detect wormholes is by the use of trust information. Nodes can monitor the behavior of their neighbor and rate them. Assuming that a wormhole drops all the packets it receives as in black holes, a wormhole in such a system should have the least trust level and can be easily eliminated. Drops in bottleneck in a network could be due to congestion, which could be triggered by improper routing, high TCP window sizes, sudden bursts of traffic from a node, etc. But all these drops occur in bursts and network gets reconfigured after congestion. For example, if there are a lot of drops in TCP, the window size is decreased. Hence, the drop of packets in bottleneck is generally high only during congestion after which it is brought down again[5][13].

Trust mechanism

Generally, the trust mechanism works in the following stages.

1) Node behavior monitoring: Each node monitors and records its neighbors' behaviors such as packet forwarding. This collected data will be used for trustworthiness evaluation in the next stage. The watchdog is a monitoring mechanism popularly used in this stage. The confidence of the trustworthiness evaluation depends on how much data a node collects and how reliable such data is.

2) Trust measurement: Trust model defines how to measurethe trustworthiness of a node. Several representative approaches to build thetrust model, which include Bayesian approach, Entropyapproach, Game-theoretic approach, and Fuzzy approach.The trust value of a node may be different when we use different trust models[16].

H. Watchdog

In this technique, watchdog identifies misbehavior of nodes by copying packets and maintained a buffer for recently sent packets. The overheard packets are compared with the sent packet, if packets are a match then discards those packets. If

the packet is timeout, increment the failure tally for the node. And if the tally exceeds the thresholds, then the node will misbehave. The implementation of watchdog technique is shown in figure 8.

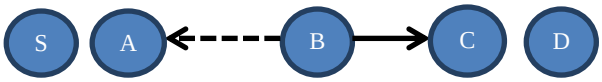

Figure8: Watchdog implementation

In this figure, it is assumed that bidirectional communication symmetry on every link between nodes that want to communicate. If a node can receive a message from a node at a time, then node could instead have received a message from node at the time will implement the watchdog. It maintains a buffer of recently sent packets and compares each overheard packet with the packet in the buffer, when forwards a packet from to with the help of, can overhear transmission and capable of verifying that has attempted to pass the packet towards. But this approach has some limitations and it is not detecting the misbehaving node during ambiguous collisions, receiver collisions, collusion and false misbehavior [18].

3. PROPOSED WORK

During the study it is observed that wormhole attack is much frequent attack on the MANET environment, which is easily deployable over a network. On observation, it is found that, due to high mobility, availability of resource is less in the MANET, security and most importantly energy is another major issue in MANET, thus a new kind of solution is required where end nodes are behaving as usual and organization of these nodes are energy efficient and secure by nature.

3.1 Solution Domain

A new infrastructure is developed for the avoidance of wormhole attack which is able to detect and prevent the attacks. The proposed system is implemented and simulated using the NS2 network simulator, used to analyze the quality of service parameters for evaluation of MANET performance over different network scenarios.

3.2 Methodology Used

In the proposed system nodes and devices are organized using a fixed infrastructure of MANET devices, where devices are categorized in the following manner.

Mobile nodes: These nodes are a collection of the mobile devices and follow the law of independent mobility; these nodes are those who actually uses the network and their services. These nodes are frequently participating in the communication. Additionally, able to send, receive and route data during communication sessions as the tradition of the MANET. But they only receive services from the nearest cluster heads.

Cluster Heads: These nodes are basically static access points which installed separately by the service provider. These nodes are participating in communication when intra-cluster communication occurs. The primary objective of these cluster heads, to monitor the communication between trusted nodes, when a new mobile node trying to communicate with internal cluster or trusted node then data sending and receiving is the main responsibility of these nodes.

Monitoring server: This device is used to calculate the trust value for securing the network from attack. In addition of that these nodes are also responsible for elimination of nodes that are performing malicious activities in the network.

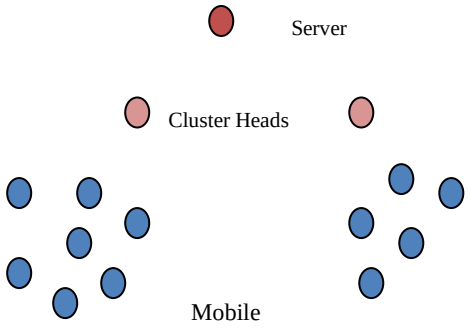

Figure 9: Show the proposed network

4. CONCLUSION AND FUTURE WORK

In this paper we address the various solutions available for wormhole attack in wireless Ad hoc networks. Firstly we have seen how wormhole can be launch in many different ways which are difficult to detect because it affect the network without knowing the cryptographic techniques used in implementation. The techniques for detection and prevention have both advantage and disadvantage. Example Distance-bounding/Consistency-based approach require specific hardware,in

Packet leashes/Geographic leashes synchronized clock and GPS is needed while in trust based technique if packet is drop by another reason such as collision , traffic then result is not accurate.Finally we have purposed a new, energy-efficient trust mechanism is to detect wormhole attack in AODV protocol and with the help ns-2 simulations implementation and performance is to be evaluated via comparing existing technique.

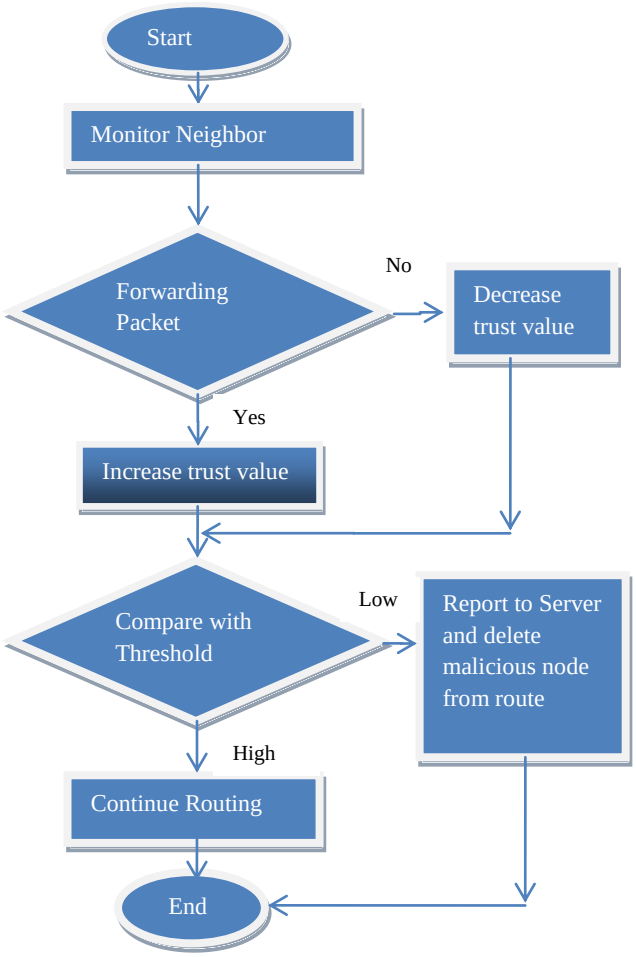

Figure 10: Detection of malicious node

REFRENCES

1. M .Sookhak ,M.R. Eslaminejad, M. Haghparastand I.in FauziISnin "*DetectionWormhole in Wireless Adhocnetworks*"IJCST , Volume 2, Issue 7, October (2011).
2. Mr. SusheelKumar , Vishal Pahal , SachinGarg "*Wormholeattack in Mobile AdHoc Network ", IRACST* – Engineering Scienceand Technology: An International Journal (ESTIJ), ISSN:2250 3498,Vol.2, No. 2, April (2012)
3. Marianne Azer, Sherif El-Kassas and Magdy El-Soudani "*A Full Image of the Wormhole Attacks Towards IntroducingComplex Wormhole Attacksin wireless Ad Hoc Networks*" in (IJCSIS) International Journal of ComputerScience and Information Security, Vol. 1, No. 1, May (2009).
4. RamandeepKaur,Jaswinder Singh "*Towards Security against Malicious Node attack in mobile adhocnetwork*" , inIJARCSSE, ISSN: 2277 128X , Volume 3, Issue 7,July2013.
5. MajidMeghdadi, SuatOzdemir and InanGüler "*A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks*" ,in IETETECHNICAL REVIEW,VOL 28 , ISSUE 2 ,MAR-APR 2011.
6. JyotiThalor ,Ms. Monika "*Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks*", in Volume 3,Issue 2, February 2013 ISSN: 2277 128X InternationalJournal of Advanced Research in Computer Science and Software Engineering(2013).
7. R.Sherine Jenny, N.Sugirtham" simulation based performance comparisionof*F AODV, DSR, FSR routing protocolwith worm hole attack "in IRACST* – International Journalof Computer Networks andWireless Communications(IJCNWC), ISSN: 2250-3501 Vol.3, No1, February (2013).
8. Vandana C.P, Dr. A. Francis SaviourDevaraj "*Evaluation of Impact of Wormhole Attack on AODV"* in Int. J.Advanced Networking and ApplicationsVolume: 04 Issue:04 1652-1656 ISSN : 0975-0290(2013).
9. Bounpandithkannhavong, Hidehisanakayama,Yoshiakinemoto and Nikato "*ASurvey of routing attacks in mobile adhoc networks" in IEEE* WirelesCommunication1536-1284/07/$20.00 (2007)

10. SudhirAgrawal, Sanjeev Jain, and Sanjeev Sharma *"Asurvey of routing attacks and Security measures in mobile Adhoc networks"* in journal of computing volume 3, issue, ISSN 2151- 9617 1,January (2011).
11. MangeshGhongeandProf. S. U.Nimbhorkar **"***Simulation of AODV under Blackhole Attack in MANET***"** in InternationalJournal of Advanced Research in Computer Science and Software EngineeringVolume 2, Issue 2,ISSN: 2277 128X February (2012).
12. MohitJain andHimanshuKandwal "*A Survey onComplex Wormhole Attack in Wireless Ad Hoc Networks in* 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies978-0-7695-3915-7/09 $26.00 (2009).
13. KhinSandar Win "*Analysis of Detecting Wormhole Attackin Wireless Networks*" in World Academy of Science, Engineering and Technology 24(2008).
14. YudhvirSingh,AvniKhatkar, Prabha Rani, Deepika, and DheerDhwaj Barak "*Wormhole Attack Avoidance Technique inMobile Adhoc Networks*" in IEEE 978-0-7695-4941-5/12 $26.00 (2013).
15. Ian F. Akyildiz ,Xudong Wang , and Weilin Wang "*Wireless mesh networks: a survey*" in Elsevier Computer Networks 47 -445–487(2005).
16. Youngho Cho and Gang Qu and Yuanming Wu "*Inside Threats against TrustMechanism with Watchdog and Defending Approaches in Wireless Sensor Networks*" IEEE CSSecurity and Privacy Workshops(2012).
17. PriyaMaidamwar and NekitaChavhan " *A survey on security issues to detect wormholeattack in wireless sensor network*" in International Journal on Ad Hoc NetworkingSystems (IJANS) Vol. 2, No. 4, October 2012.
18. PushpendraNiranjan, PrashantSrivastava, Raj kumarSonand Ram Pratap "*Detectionof wormhole attack using hop count andtime delay analysis*" in International Journal of Scientificand Research Publications, ISSN 2250-3153,Volume 2, Issue 4, April 2012.
19. Ajay PrakashRai, VineetSrivastava and Rinkoo Bhatia "*Wormhole Attack Detection in Mobile Ad HocNetworks"in*International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 2277-3754 ,Volume 2,Issue 2, August 2012.

