IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor: 6.252

Volume 2, Issue 7, May 2022

Detection and Security Analysis of Wormhole Attacks in MANETS

Nimisha C. J.[1] and Dr.Geetha G.[2]

Department of Electronics and Communication Engineering
NSS College of Engineering, Palakkad, Kerala[1,2]

Abstract: *This paper includes the survey of detection and security analysis of wormhole attack in MANET. MANET stands for Mobile Ad-hoc Network which is also called a wireless Ad-hoc network that consists of a set of mobile nodes connected wirelessly in a self- configured, self-healing network without having a fixed infrastructure. MANETs are susceptible to many security attacks as they use wireless medium for communication such as wormhole attacks. This attack involves two or more than two malicious nodes and the data packet from one end of the malicious node is tunnelled to the other malicious node at the other point, and these data packets are broadcasted. Intrusion detection systems are the solution for detecting wormhole attacks in MANET. This work deals with the various detection techniques and the types of wormhole modes in order to analyse the wormhole attack.*

I. INTRODUCTION

The Wireless sensor networks (WSNs) are networks of spatially dispersed and dedicated sensors that monitor and record the physical conditions of the environment and forward the collected data to a central location. WSNs can measure environmental conditions such as temperature, sound, pollution levels, humidity and wind. As the WSN technologies are developing to balance the load and expand the lifetime of the network, efficient network topologies are required. The WSNs are considered as networks formed by the computing devices. This technology is entirely different from traditional networks. The main features of the WSN are it serves energy, storage, and computation and bandwidth constraints. WSN composed of around thousands of sensor nodes which can be distributed in a wide range. WSN is commonly used in areas like weather monitoring, disaster management, security, intrusion detection, and tac- tical surveillance.

Ad-hoc networks are wireless infrastructure-less networks. They are suitable where setting infrastructure is either not feasible or is costly. The most interesting feature of ad -hoc network is that the functions of components that provide infrastructure like switches, routers, etc. are performed by nodes present in the network. MANETs are used for military applications such as ensuring the timely flow of information. Due to fast and easy deployment they are also used to establish communication and provide rescue services after earthquakes. MANETs are also used for on-the- fly collaborative computing outside an office environment. They are also used in communication dispatch systems for taxis to guide the route, inform about passenger pickups, etc. They are also used in personal networking like cell phones. One of the challenges in MANETs is to provide high-security requirements with constrained resources. The security requirements in MANETs are comprised of node authentication, data confidentiality, anti-compromise and resilience against traffic analysis. To identify both trustworthy and unreliable nodes from a security standpoint, the deployment sensors must pass a node authentication examination by their corresponding manager nodes or cluster heads and unauthorized nodes can be isolated from MANETs during the node authentication procedure. Similarly, all the packets transmitted between a sensor and the manager node must be kept secret so that eavesdroppers cannot intercept, modify and analyze, and discover valuable information in MANETs.

MANETs are easily compromised by attackers due to wireless communications use a broadcast transmission medium and their lack of tamper resistance. Therefore, an attacker can eavesdrop on all traffic, inject malicious packets, replay older messages, or compromise a sensor node. Generally, sensor nodes are most worried about two major security issues, which are privacy preserving and node authentication. Privacy means the data confidentiality is achieved under security mechanism, and hence it allows network communications between sensor nodes and the manager station to proceed securely. In addition, a well-structured authentication mechanism can ensure that no unauthorized node is able

DOI: 10.48175/568

to fraudulently participate and get sensitive information from MANETs.

As a result, several schemes have been proposed to secure communications in MANETs. The main goal of the security services in the MANETs is to provide data and information protected from any types of attacks. The various security requirements in MANETs, which are as follows:

1. Availability: It is essential that the resources are available in the operational network for the message to move on and ensures that the nodes can utilize the resource and the network also.
2. Authorization: It ensures that authorized sensors provide information to the services in the operational network.
3. Authentication: It implies that sensor nodes in the communication are genuine and have proper access to the network.
4. Confidentiality: It ensures that the message in the communication network cannot be read and understood by the attackers.
5. Integrity: It refers that the message is not altered or tampered with while it was on the network communication. By simply injecting additional packets, the entire packet can be changed.

Since ad hoc networks are used in many different situations, their requirements and complexities are different and hence there are five different categories in which protocols are divided:

1. Source Initiated Protocols: In reactive routing, route is created only when the source requests a route to destination. When the request is encountered a route discovery procedure is invoked. The procedure includes flooding of special route request packets to the network starting with immediate neigh- bours. Active routes are maintained by route maintenance procedure.
2. Table-Driven Protocols: Proactive protocol is based on the traditional distance vector routing mechanism, called Bellman-Ford routing algorithm. In this protocol routers collect routing information from their neigh- bours and compute shortest paths to each node. This routing information is then passed to other nodes which in turn update their routing information. This protocol helps in maintaining up-to-date information of all routes from each node to every other node in the network.
3. Hybrid Protocols: Hybrid protocol is a combination of on-demand and table-driven protocol. Proactive routing is used where there are lesser route changes while reactive routing is used in the core of the network. Since this protocol combines the two proto- cols, the performance can be improved.

II. SECURITY ATTACKS ON MANETs

The purpose of securing wireless multi hop net- works is to prevent misuse of nodes resources and protect the information. Requirements of effective security architecture are authentication, confidentiality, integrity, availability and non-repudiation. In the wireless sensor network, two types of attacks are mainly due to the transmission medium's nature:

- **Active Attacks**

  A typical WSN consist of mainly three elements. That include normal sensor nodes, base station or sink and anchor nodes. Mobility feature can be added in either of these three elements.

- **Passive Attacks**

  In Passive attacks, the attackers only intend to steal valuable information like passwords and confidential data. Passive attack includes receiving data analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic and capturing authentication information such as pass- words, and does not manipulate network activities. MANETs are vulnerable to the most popular types of attacks and threats, such as wormhole attacks. A wormhole attack is a serious issue that records the packets from one location of the network and tunnels them to another location to degrade the performance of the wireless network and disrupt the most routing protocol. Wormhole attack is a type of network layer attack which is carried out using more than one malicious node. The nodes used to carry out this attack are superior to normal nodes and are able to establish better communication channels over long ranges. The idea behind this attack is to forward the data from one compromised node to another malicious node at the other end of the network through a tunnel.

As a result, the other nodes in the WSN can be tricked into believing that they are closer to other nodes than they really are which can cause problems in the routing algorithm. The compromised nodes may temper with the data packets.
The attack normally works in two phases. In the first phase, the wormhole nodes get themselves involved in several routes. In the second phase, these malicious nodes start exploiting the packets they receive. These nodes can disrupt the network functionality in a number of ways. For example, these nodes can confuse the protocols that depend on node location or geographic proximity, or the colluding nodes may forward data packets back and forth to each other in case of virtual tunnel so as to exhaust the battery of other intermediate nodes. Wormhole nodes can drop, modify, or send data to a third party for malicious purposes.
Depending upon whether wormhole nodes put their identity into packets headers when tunnelling (visibility), they are classified as:

Open Wormhole: In this case the data packets are first sent from the source to a wormhole which tunnels them to the other wormhole that transmits them to the destination. The other nodes in the network are ignored and not used for data transfer. Node's identity is contained in the packet header. The nodes update the packet header and encapsulate its identity (MAC address) when it has a packet to send. After receiving the packet, the malicious node includes its identity in the header like all other nodes. Hence the legitimate nodes are aware of the presence of the wormhole nodes but do not know that they are wormhole nodes. These wormhole nodes may not be necessary be malicious. Here both the malicious nodes are visible.

Half-open Wormhole: In this case the data packets are sent from the source to a worm- hole which directly transmits them to the destination. One malicious node is visible to the legitimate nodes as it updates its entries in the packet header and the other node is invisible.

Closed Wormhole: In this case the data packets are directly transferred from the source to the destination in a single hop making them fictitious neighbours. It is also known as hid- den attack. It doesn't affect the packet header at the time of route discovery and hence legitimate nodes don't know its existence.The malicious nodes transmit the packet to its partner node through the tunnel. After the packet is received at the other end the node may drop it or forward it.

Based on the absence or presence of identities of malicious nodes and their packet forwarding behavior during tunnelling and replaying of packets, the wormhole attack occurs in two different modes, namely hidden and exposed modes, respectively.

Hidden Mode: In this mode, the malicious nodes present in the network do not manipulate the content of the data packets and the AODV packet header while transferring the packets from one end of the tunnel to the other end.

Exposed Mode: The attacker manipulates the contents of data packets in exposed mode by including its identity while transferring packets in the tunnel. However, the malicious nodes do not mess with the AODV packet header, and it remains unaltered.

III. ROUTING PROTOCOLS USED IN WORMHOLE ATTACK DETECTION

A. Proactive Routing Protocols

Proactive routing protocols are table-driven protocols that maintain and update routing table using the routing information taken from the neighbors on a continuous basis. in these protocols select the path form the source to destination, where source node and each intermediate node selects the next hop. Using routing table look up, and forwarding the packet to the next hop until destination receives the packet. Drawback of these protocols is the proactive overhead due to route maintenance and fast route updates to cope with node mobility. Ex- ample of proactive routing protocol is the DSDV.

B. Reactive Routing Protocols

Reactive routing protocols find a route from source to the destination node only when need to send data. Reactive routing protocols are suited with high node mobility for networks or where the nodes transmit the data infrequently. Some examples of reactive routing protocols include Ad Hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), Dynamic MANET On Demand (DYMO), Temporally Ordered Routing Algorithm (TORA).

1) Ad-Hoc On-Demand Distance Vector Protocol: The AODV protocol builds routes between nodes only if they are requested by source nodes. AODV is therefore considered an on-demand algorithm and does not create any extra traffic for communication along links. The routes are maintained as long as they are required by the sources. They also form trees to connect multicast group members. AODV makes use of sequence numbers to ensure route freshness. They are self-starting and loop-free besides scaling to numerous mobile nodes.

In AODV, networks are silent until connections are established. Network nodes that need connections broadcast a request for connection. The remaining AODV nodes forward the message and record the node that requested a connection. Thus, they create a series of temporary routes back to the requesting node.

A node that receives such messages and holds a route to a desired node sends a backward message through temporary routes to the requesting node. The node that initiated the request uses the route containing the least number of hops through other nodes. The entries that are not used in routing tables are recycled after some time. If a link fails, the routing error is passed back to the transmitting node and the process is repeated.

2) *Dynamic Source Routing (DSR):* The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes.

DSR allows the network to be completely self- organizing and self-configuring, without the need for any existing network infrastructure or administration. It is a reactive protocol and all aspects of the protocol operate entirely on-demand basis. It works on the concept of source routing. Source routing is a routing technique in which the sender of a packet determines the complete sequence of nodes through which, the packets are forwarded.

The advantage of source routing is:intermediate nodes do not need to maintain up to date routing information in order to route the packets they forward. The protocol is composed of the two main mechanisms of “Route Discovery” and “Route Maintenance”. If a node has a packet to send, it at- tempts to use this cache to deliver the packet. If the destination does not exist in the cache, then a route discovery phase is initiated to discover a route to destination, by sending a route request. Thisrequest includes the destination address, source address and a unique identification number.

If a route is available from the route cache, but is not valid any more, a route maintenance procedure may be initiated. A node processes the route request packet only if it has not previously processes the packet and its address is not present in the route cache.

3) Dynamic MANET On Demand (DYMO): The DYMO routing protocol is successor to the popular Ad hoc On-Demand Distance Vector (AODV) Routing protocol and shares many of its benefits. DYMO can work as both a pro-active and as a reactive routing protocol, i.e., routes can be discovered just when they are needed. In any way, to discover new routes the following two stepstake place:

A special “Route Request” (RREQ) messages is broadcast through the MANET. Each RREQ keeps an ordered list of all nodes it passedthrough, so every host receiving an RREQ message can immediately record a route back to the origin of this message. When an RREQ message arrives at its destination, a “Routing Reply” (RREP)message will immediately be passed back to the origin, indicating that a route to the destination was found. On its way back to the source, an RREP message can simply back trace the way the RREQ message took and simultaneously allow all hosts it passes to record a complementary route back to where it came from.

So as soon as the RREP message reaches its destination, a two-way route was successfully recorded by all intermediate hosts, and exchange of data packets can commence.

4) *Temporally Ordered Routing Algorithm (TORA):* TORA (Temporally Ordered Routing Algorithm) is a source initiated on demand routing protocol. The main objective of TORA is to limit message propagation in the highly dynamic mobile computing environment. It means, it is designed to reduce communication overhead by adapting local topological changes in ad hoc network. Another main feature of TORA routing protocol is the localization of control packets to a small region (set of nodes) near the occurrence of a topological changes due to route break. Hence, each node of the network required to contain its local routing and topology information about adjacent nodes.

TORA supports multiple routes to transmit data packet between source and destination nodes of mobile ad hoc network. In short, TORA exhibits multipath routing capability. The TORA's opera- tion can be compared to that of water flowing downhill toward a sink node through a grid of tubes that model the routes in the real world net- work. The tube junctions represent the nodes, the tube themselves represent the route links between the nodes, the tube's water represents the packets flowing between nodes through the route links towards the destination.

C. Hybrid Routing Protocols

Hybrid routing protocols combine the advantages of various approaches of routing protocols into a single protocol. The Zone Routing Protocol (ZRP), is one such hybrid protocol that combines both the proactive and reactive routing approaches.

1) Zone Routing Protocol (ZRP): If a packet's destination is in the same zone as the origin, the proactive protocol using an already stored routing table is used to deliver the packet immediately. If the route extends outside the packet's originating zone, a reactive protocol takes over to check each successive zone in the route to see whether the destination is inside that zone. This reduces the processing overhead for those routes. Once a zone is confirmed as containing the destination node, the proactive protocol, or stored route-listing table, is used to deliver the packet.

In this way packets with destinations within the same zone as the originating zone are de- livered immediately using a stored routing table. Packets delivered to nodes outside the sending zone avoid the overhead of checking routing tables along the way by using the reactive protocol to check whether each zone encountered contains the destination node.

Thus, ZRP reduces the control overhead for longer routes that would be necessary if using proactive routing protocols throughout the entire route, while eliminating the delays for routing within a zone that would be caused by the route-discovery processes of reactive routing protocols. ZRP divides its network in different zones. Each node may be within multiple overlapping zones, and each zone may be of a different size. The size of a zone is not determined by geographical measurement. It is given by a radius of length, where the number of hops is the perimeter of the zone. Each node has its own zone.

IV. VARIOUS WORMHOLE DETECTION TECHNIQUES

A. Distance and Location Based Detection

In location-based routing, the node does not need to make complex computations to find the next hop, as routing decisions are taken using the lo- cation information. Location- based protocols are very efficient in terms of routing data packet as they take the advantage of pure location information instead of global topology information Location-based protocols uses the locationinformation of nodes to provide higher efficiency and scalability. It requires three facts. First, each node in the network must know its own location information by GPS or by any other methods. Second, each node must be aware of its neighbour nodes' location, which are one-hop away from it. Third, the source node must be aware of the location of destination node.

1) Packet Leash Technique: The packet leashes are the method that are used to prevent against wormhole attack. It can be grouped either geo- graphical or temporal. Geographical leash ensures that receiver of the packet is within a range from the sender. Temporal leash ensures that packet lifetime ends after certain time, which restricts the maximum travel distance.

2) Geographical Leashes: In this method the receiver of the packet is located within a certain range from the sender and each node must know its own location using GPS. When packet is sent by a node then it inserts its own location (ps) and packet is sent at time (ts) in the header of packet. When the packet reaches to next node, the location of the receptor of packet (pr) and time of received packet (tr) is compared with the values of sender.

3) Temporal Leashes: In temporal leashes, an expiration time is considered to each transmitted packet. It means there are time limit in temporal leash, the sender of packet prevents broadcasting packets more than distance L. Before a packet is sent by sender at time(ts), the expiration time of packet is calculated and added to the packet. when packet received by the next neighbor node at its local time (tr) now this time is compared with the expiration time of packet (te). the packet is drop only when trite.

DOI: 10.48175/568

B. Special Hardware Based Approaches

1) SECTOR- (SECure Tracking Of node encounteRs)*:* These are a set of mechanisms for the secure verification of the time of encounters between nodes in multi-hop wireless networks. This information can be used notably to prevent wormhole attacks (without requiring any clock synchronization), to secure routing protocols based on last encounters (with only loose clock syn- chronization), and to control the topology of the network. SECTOR is based primarily on distance- bounding techniques, on one-way hash chains and on Merkle hash trees. We analyze the communication, computation and storage complexity of the proposed mechanisms and we show that, due to their efficiency and simplicity, they are compliant with the limited resources of most mobile devices.

2) MAD-mutual authentication with distance bounding protocol: A distance bounding protocol enables one party to determine a practical upper bound on the distance to another party. It is an effective countermeasure against mafia fraud attacks which do not alter messages between users but only relay messages. The main idea of distance bounding protocols is to repeat fast bit exchanges. One party sends a challenge bit and another party answers with a response bit and vice versa. By measuring the round-trip time between the challenge and the response, an upper bound on the distance between users can be calculated. If messages are relayed, the round-trip time increases and thus mafia fraud attacks can be detected.

C. Hop Counting Method

1) DelPHI (Delay Per Hop Indication Technique): In this technique delay per hop is deter- mined in every path and it is proved that delay per hop for the genuine path is always shorter than the wormhole path. If the path has observably high delay per hop, then the corresponding path is affected by wormhole. It can detect both hidden and exposed wormhole attacks. Delphi works in two phases first is Data Collection and second is Data Analysis and Detection. The advantages of DelPHI are that it does not require and position information, clock synchronization and it does not require the mobile nodes that equipped with special hardwires, thus it provides higher power efficiency.

D) Connectivity-based Approaches

A wormhole that can decode packets can choose to tunnel only traffic between two select nodes over a short distance; such wormholes have a minimal impact on network topology and may not be easily detected by such approaches. This approach is localized and do not use any special hardware or location information for attack detection. The detection algorithm looks for forbidden substructures in the connectivity graph, it should not be present in a legal connectivity graph. They use unit desk graph model that have long been used to create an idealized model of multi-hop wireless networks.

E) Secure Neighbor Discovery Approaches

Securely discovering one’s neighbors is an effective technique for countering wormhole attacks. This approach has two steps. In the first step, neighboring list of each node is being built. In the second step, a collaborative detection scheme for wormholes is used, where a node monitors the traffic travelling in and out of its neighbors. The fundamental mechanism used is local monitoring. Nodes monitor the traffic travelling in and out of its neighboring nodes and use a data structure for first and second hop neighbors. This protocol manages the malicious node and removes its ability to cause future problems.

F) Watchdog

Watchdog knows the misbehavior of nodes by duplicating packets and maintaining a buffer for newly sent packets. A sent packet is matched with overheard packet, if matching occur then discards that packet. If packet is timeout then increase the failure tally for the node. And if tally exceeds the thresholds, then node will misbehave. In Watchdog implementation, it is supposed that communication in bidirectional symmetry on each link in nodes that want to communicate. When a node receive message from a node then node could instead have a received message at the time will implement watchdog. It maintains a buffer of lately sent packets and matches each overheard packet with the packet present in buffer. However,

DOI: 10.48175/568

the approach has few limitations and it is not able to detect the misbehavior node during receiver collisions, ambiguous collisions, false misbehavior and collusion.

G) Method Based on Timing Calculation

***1) True Link**:* TrueLink is wormhole detection technique that depends on time-based mechanisms. TrueLink verifies that there is a direct link for a node to its adjacent neighbor node. Using TrueLink to detect wormhole involves 2 phases named rendezvous and validation. Rendezvous phase is performed with firm timing factors in which nonce exchange between two nodes takes place. In validation phase both the nodes authenticate each other to prove that they are the originator of corresponding nonce. The main disadvantage of TrueLink technique is that it works only on IEEE 802.11 devices that are backward compatible with a firmware update.

2) Round Trip Time (RTT): In this method constructing a list of neighbors, finding possible routes between source and destination and finding location link based on RTT. Check the number of neighbors and try to find malicious node when RTT is over limit. This is impractical for real life implementation because they assume that network builds with same hardware and software and all nodes are uniquely identified.

H) New Technique based on Routes Redundancy and Time- based Hop Calculation

The main idea of this technique is to create all possible routes when sending Route Request packet (RREQ) from source to destination and then use those routes as reference of each other. to find malicious nodes with suspicious behavior within the network. This detection scheme based on three combinational steps which are route redundancy, route aggregation, and Round-Trip Time (RTT) calculation. Those combinations are required to receive the true shortest path and detect malicious nodes whose create wormhole tunnel. Routes redundancy is started when source sends RREQ using all possible ways to destination. All routes that connect source to destination are listed together with number of hops from every route of network. Some routes collected in the same relay point before aggregating destination, so all nodes that join the network are listed and the behavior of malicious nodes detected. The RTT calculation and number of hops of all listed routes are compared for detecting suspicious route. Nodes with suspicious behavior in network are isolated and will not be considered for transmission.

I) A Hybrid Approach for Detection

It is a hybrid technique based on the concept of watchdog and Delphi. Watchdog (packet drop) and RTT based technique Delphi are based on the assumption that the packet drops and RTT of aroute in the network are very closely related to the value of its HC (hop count) and distance. In practical WSN environments, there exist probability that a normal route without wormhole with a small distance and short value of HC may produce a high value of RTT and packet drop value due to traffic congestion and other reasons. Conversely, aroute in the sensor network that is infected with wormhole with a lengthy distance may result in providing a low value of RTT. This may be due to the small packet processing delays by all in- between nodes. Furthermore, there may be less packet drop by an attacker to force AODV to follow the wormhole affected path. For these rea- sons, sometimes wormhole exposure performance is compromised when separately watchdog and Delphi are used in realistic WSN environments.

J) Wormhole Resistant Hybrid Technique

WRHT makes use of the information about the packet drop and the delay per each hop and for the complete route in the sensor network. The foundation behind WRHT is to build up a wormhole detection methodology that is able to manage every category of wormholes and is possible for every type of WSN device and scenarios of the network, without the earning of significant computational costs. WHRT is considered as an extension to AODV protocol. The proposed WRHT allows the source node in the sensor network to calculate the wormhole presence probability for a path in addition to HC information.

During the AODV route discovery phase, per hop time delay probability () is calculated in order to discover the presence of wormhole in the path. This information can be further used for the calculation of time delay probability for the complete path, that is, . In the next phase of the WRHT, per hop packet loss probability () is calculated. This is further used for the

DOI: 10.48175/568

calculation of packet loss probability for the complete path, that is the values of and are used for making the decision whether a path P contains a wormhole or not. This will help the AODV to take a secure path for the transmission.

V. DETECTION FEATURES OF WORMHOLE ATTACK

A. Location

In case of wormhole attack, location is a very important feature. If we know the exact location of mobile nodes, then it would be very easy to build a graph of the network. One way of implementing this system is to equip each node in the network with a Global Positioning System (GPS) device. To reduce cost, some special nodes having GPS receiver can be deployed at specific locations in the network to get locations of the neighboring nodes. The relative location information can also be collected by using special antennas, which are able to detect the direction from which the data is received. The use of GPS device or special antenna will increase the cost of nodes and make the network more expensive. This will also decrease the battery timing of mobile nodes. By using exact or relative location as a detection feature can also increase the False Positive Rate (FPR), as in MANETs nodes change their positions frequently.

B. Time

The time feature can also be helpful in worm- hole attack detection. The route having wormhole attack will have more average time per hop as com- pared to the normal rout e. To calculate accurate time difference between source and destination, all nodes in the network should be equipped with tightly synchronized clock. The time difference can also be calculated without tightly synchronized clock where source node sends a special lightweight Hello message to the destination and records the sending time of the packet. When the destination node receives that Hello message, it replies with a Hello-Reply message. The difference between sending and receiving time is calculated and is divided by two after excluding the processing time at source, destination, and intermediate nodes. Then the average time of each hop is calculated. To implement a synchronized clock is a difficult and expensive task in MANETs.

C. Hop Count

The hop count feature can also be used as a detection parameter. A path through wormhole nodes contains a smaller number of hops as compared to the normal path because hop count does not increase when the message moves through the private channel between malicious nodes. Some techniques find the presence of wormhole by using hop count information in association with time or location. Average time for a single hop is calculated by dividing the total hops by total time or distance. If the average hop time or distance is gr eater than the normal preset hop time, then thepath contains malicious nodes. Techniques based on average time or distance may require synchronized clock or GPS device respectively.

D. Neighborhood

The basic property of wormhole attack is to represent two non-neighbor nodes as neighbors. So, the wormhole can also be detected by getting data about neighboring node. Such techniques collect and maintain the data related to immediate (one hop) neighbors of a node while some other techniques try to identify the wormhole attack by keeping and analyzing the data of two-hop neighbors collected by Hello message. These techniques face problems in dense networks where each node contains many neighbors. Therefore, to keep and analyze data up to two-hop neighbors require more memory, storage, and processing power.

E. Data Packets

Some intrusion detection techniques tr y to detect wormhole nodes on the basis of ratio of data packets received and sent. In these techniques, all nodes are set in promiscuous mode so that they can listen data packets in their neighborhood. The nodes record the number of packets received and forwarded by their neighboring nodes in a table so that they can estimate the state of their neighbors whether they drop, modify, or forward data packets to some node other than the destination node. On the basis of this information, they calculate trust value of each neighboring node. Although this is a simple technique, it can work effectively in large networks with high mobility.

F. Route Reply

Route Reply (RREP) is also used as a detection feature to detect wormhole attacks. On receiving a request for a fresh route, a node sends RREP message to the source node if it is the destination node or have a fresh route to the destination node. The wormhole nodes usually violate this condition to launch the attack. Since RREPs are unicasted only, nodes that want to keep record of the RREPs have to be set in the promiscuous mode, which can affect the network efficiency.

G. Route Request

Route Request (RREQ) is the most important feature for on-demand routing in MANETs. Like RREP, it is also used with some other features to detect wormhole attacks. As each RREQ generated by a source node normally reaches every node in the network, IDSs based on RREQ mostly have simple computations and require fewer resources as compared to other methods

VI. CONCLUSIONS

Mobile Ad-hoc Networks (MANETs) are infrastructure-less, self-configured, and self- maintained wireless networks. These networks have more security threats due to lack of central point of control as compared to fixed networks. Wormhole attack is one of the most severe routing attacks, which is launched by two colluding nodes by establishing a private channel between them. Wormhole attacks in WSNs are rigorous attacks that can be launched easily even in sensor networks with implementing authenticity and confidentiality. Addressing of wormhole attacks is a crucial issue as far as security of WSNs is concerned, since wormhole attacks are difficult to detect. This is because wormhole attacks can be launched in several modes, with each one enforcing its own unique requirements for the detection method.

This paper presents the features that could be used to detect the wormhole attack. These features are discussed in detail with their merits and demerits. Along with the explanation of these techniques a qualitative comparison of all wormhole detection technique has been done. This paper provides a brief view about the routing protocols for detection. Based on the existing approaches Path T racing Approach will be helpful to detect wormhole at- tack in the network. In the near future, performance of Wormhole attack with respect to different parameters can be analyzed.

REFERENCES

[1] Vrutik Shah and Dr. Nilesh Modi, "Responsive Paramete based on AntiWorm Approach to Prevent Wormhole Attack in Ad hoc Networks", ACEEE Int. J. on Network Security, Vol. 5, PP. No. 1, January 2014.

[2] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion- Detection System for MANETs", IEEE Transactions on Industrial Electronics, Vol. 60, No. 3, March 2013.

[3] Kamini Singh and Gyan Singh, "Review on Wormhole Security and Their Detection Scheme", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 4, Issue 1, January 2014.

[4] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, And Lixia Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions", IEEE Wireless Communications, February 2004.

[5] M. Sookhak, M. R. Eslaminejad, M. Haghparastand I.in FauziI Snin "Detection Wormhole in Wireless Ad hoc networks" IJCST, Volume 2, Issue 7, October 2011.

[6] Mohit Jain and Himanshu Kandwal "A Survey on Complex Wormhole Attack in Wireless Ad Hoc Networks", International Conference on Advances in Computing, Control, and Telecommunication Technologies, IEEE computer society 978-0-7695-3915- 7/09 in 2009.

[7] Zubair Ahmed Khan and M. Hasan Islam, "Wormhole Attack: A new detection technique", IEEE , 978-1-4673-4451-7/12 , 2012.

[8] Venkata C. Giruka and Mukesh Singhal, "Secure Routing in Wireless Ad-Hoc Networks", Springer Science, Chapter 6, Wireless Network Security, 2007.

[9] Sudhir Agrawal, Sanjeev Jain, and Sanjeev Sharma, "A survey of routing attacks and Security measures in mobile Ad hoc networks" in journal of computing volume 3, issue, ISSN2151- 9617 1, January 2011.

[10] Yih-Chun Hu, Adrian Perrig and David B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", IEEE INFOCOM 2003.

[11] Yashpal singh Gohil, Sumegha Sakhreliya, and Sumitra Menaria , “A Review On: detection and prevention of wormhole attack in MANET” , International Journal of Scientific and Research Publications, Volume 3, Issue 2, ISSN 225.

[12] Majid Meghdadi, 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.

[13] Yih-Chun Hu, Adrian Perrig and David B. Johnson, “Wormhole Attacks in Wireless Networks”, Member, IEEE.

[14] Srdjan C apkun, LeventeButtya n, and Jean-Pierre Hubaux ,“SECTOR: Secure Tracking of Node Encounters in Multi- hop Wireless Networks” , ACM Workshop on Securityof Ad Hoc and Sensor Networks (SASN), October 31,2003.

[15] Nishant Sharma and Upinderpal Singh, “Various Approaches to Detect Wormhole Attack in Wireless Sensor Networks”, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.2, February-2014.

[16] Hon Sun Chiu and King-Shan Lui, “DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks”, IEEE, O-7803-9410-O/06/, 2006.

[17] Soo-Young Shin and Eddy Hartono Halim, “Wormhole Attacks Detection in MANETs using Routes Redundancy and Time-based Hop Calculation”, IEEE,978-1-4673- 4828- 7/12, 2012.

[18] Pushpendra Niranjan, Prashant Srivastava, Raj kumar Soniand RamPratap, “Detection of wormhole attack using hop count and time delay analysis”, International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012.

[19] Jakob Eriksson, Srikanth V. Krishnamurthy, and Michalis Faloutsos, “TrueLink: A Practical Countermeasure to the wormhole Attack in Wireless Networks” 14th IEEE International Conference on Network Protocols, pp. 75-84, 2006.

[20] Z. Tun and A. H. Maw, “Wormhole attack detection in wireless sensor networks,” 2008.

[21] Xu Li, Nathalie Mitton, Amiya Nayak, and Ivan Stojmenovic, “Localized Load Balancing for Geographic Routing in Wireless Ad Hoc Networks”, in International Conference on Communications - Wireless Networks Symposium - IEEE ICC-WN 2012.

[22] Majid Meghdadi, 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.

[23] Yih-Chun Hu, Adrian Perrig and David B. Johnson, “Wormhole Attacks in Wireless Networks”, Member, IEEE.

[24] Srdjan C apkun, LeventeButtya n, and Jean-Pierre Hubaux ,“SECTOR: Secure Tracking of Node Encounters in Multi- hop Wireless Networks”, ACM Workshop on Securityof Ad Hoc and Sensor Networks (SASN), October 31,2003.

[25] Nishant Sharma and Upinderpal Singh, “Various Approaches to Detect Wormhole Attack in Wireless Sensor Networks”, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.2, February-2014.

[26] Hon Sun Chiu and King-Shan Lui, “DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks”, IEEE, O-7803-9410-O/06/, 2006.

[27] Soo-Young Shin and Eddy Hartono Halim, “Wormhole Attacks Detection in MANETs using Routes Redundancy and Time-based Hop Calculation”, IEEE,978-1-4673- 4828- 7/12, 2012.

[28] PushpendraNiranjan, PrashantSrivastava, Raj kumar Soniand RamPratap, “detection of wormhole attack using hop count and time delay analysis”, International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012.

[29] Jakob Eriksson, Srikanth V. Krishnamurthy, and Michalis Faloutsos, “TrueLink: A Practical Countermeasure to the wormhole Attack in Wireless Networks” 14th IEEE International Conference on Network Protocols, pp. 75-84, 2006.

[30] Z. Tun and A. H. Maw, “Wormhole attack detection in wireless sensor networks,” 2008.

[31] Xu Li, Nathalie Mitton, Amiya Nayak, and Ivan Stojmenovic, “Localized Load Balancing for Geographic Routing in Wireless Ad Hoc Networks” in International Conference on Communications - Wireless Networks Symposium - IEEE ICC-WN 2012.

[32] Parag Kumar Guha Thakurta, Rajeswar Guin and Subhansu Bandyopadhyay,” An Efficient Approach for Detecting Wormhole Attacks in AODV Routing Protocol”, Springer 2018.

[33] Parvinder Kaur, Dalveer Kaur, Rajiv Mahajan,” Wormhole Attack Detection Technique in Mobile Ad Hoc Networks”, Springer 2017.

[34] Tu T. Vo1, Ngoc T. Luong, Doan Hoang,” MLAMAN: a novel multi-level authentication model and protocol for preventing wormhole attack in mobile ad hoc network”, Springer 2018.

[35] Singla Neelima, Singh Ramanjeet,” Wormhole Attack Prevention and Detection in MANETs Using HRL Method”, International Journal of Advance Research, Volume 3, Issue2,2017.

[36] Praveen Kataria ,mithilesh kumar ,” Hop Count Based Conjunction Control Wormhole Detection Approach for MANET ”, International Journal of Scientific Research & Engineering Trends Volume 2, Issue 2,2016.

[37] Dhruvi Sharma, Vimal Kumar and Rakesh Kumar,” Prevention of Wormhole Attack Using Identity Based Signature Scheme in MANET”, Springer India 2016.

[38] Farhan Abdel-Fattah, Khalid A. Farhan, Feras H. Al-Tarawneh, Fadel AlTamimi“Security Challenges and Attacks in Dynamic Mobile Ad Hoc Networks MANETs”, IEEE 2019.

[39] Amar Singh Chouhan, Prof. Vikrant Sharma, Upendra Singh,“A Modified AODV Protocol to Detect and Prevent The Wormhole using Hybrid Technique”, International Conference on Electronics, Communication and Aerospace Technology(ICECAT),IEEE 2017.

[40] Parvinder Kaur, Dalveer Kaur, Rajiv Mahajan, “Simulation Based Comparative Study of Routing Protocols Under Wormhole Attack in Manet”, Springer 2017.ia 2016.

DOI: 10.48175/568