A Survey on Different Types of Techniques Used Against Wormhole Attack in MANET

Deepika V. and John Singh K.

School of Information Technology and Engineering VITUniversity, Vellore, Tamil Nadu, India

**Abstract:** A Mobile Ad hoc Network (MANET) is an infrastructure less network that includes of the mobile nodes which are independent of each other and connected through a wireless network. This type of network always faces the security threats. Networks have different types of attacks, in that wormhole attack is one of the well-known and noticeable attacks. These type of attack lets the malicious node to pretend like it’s an actual node in the network and acts like it is the nearest node to the source node. And also it is capable of dropping the packets sent by the source node to the destination node. Earlier many approaches were proposed in order to avoid and reduce the wormhole attack. In order to provide an efficient method to overcome this problem, an efficient method is proposed which is capable of reducing the packet loss and assures the security. This proposed method is used along with the AODV (Ad hoc On demand Distance Vector) routing protocol which is capable of reducing packet loss and delay.

**Key words:** MANET • AODV • Routing Protocol

**INTRODUCTION**

In today’s hectic world communication plays an important role. And communication in MANET has become the more trending topic. MANET is an infrastructure less network where it works through mobile nodes. As it is an infrastructure less network security has become a key issue. Wormhole attack is one of the severe attack in network. And it is made possible by wormhole nodes which will possibly create a tunnel in between them. And once their establish communication between them, their transfer the data packets received from the source node pretending to be the actual node as a part of the network. These wormhole nodes appear to be neighboring nodes but there will be far apart from each other in reality. The wormhole nodes create an illusion, that there are neighboring nodes.

And the route used by them will look like a shortest route compared to the routes used by any normal nodes. Wormhole nodes are very vulnerable which are capable of grabbing the route pretending to be the nearest node and then could drop, alter the data packets which it received from the source node. Confidentiality and authenticity for data packets provided by the MANET becomes useless against the wormhole attack. Wormhole nodes proceed further regardless of the security provided by MANET.

In the process of wormhole attack, at first the malicious node M will attract the node which broadcasts the RREQ by pretending to be the node with the shortest path and will get the data packets from that particular node. Once the malicious node M receives the data packets from the actual node, it will send the data packets it received through the tunnel which is shared with another malicious node N. The tunnel is created by malicious nodes and pretend to be the neighboring nodes and have the shortest path. This type of tunnel can be classified into two type. One is the in band channel and the other one is the out band channel.

The in band channel can also be called as packets encapsulate channel, in which malicious node will get the data packets from the actual node and pretend to be the one of the legal node. Once it receives the data packets, it will also add the routing message along it. And it will send the same to the other normal nodes which are part of the routing process. In result it reduces the hop count and can attain the route. It records like no changes happened where neither of the routing protocols which works against attack will have no effect in the case of in band channel. In Fig 1, source node broadcasts RREQ and the malicious node M replies with RREP which in result source node concludes that malicious node M has the shortest path and transmits the data packets to it.
Malicious node adds the routing information in addition and sends the same to normal nodes. Once the same received by another malicious node N, it will fetch the original message sent by the source node and will broadcast the same to the destination node. In contrast as shown in Fig 2, rather than using the normal nodes in between them the malicious node will create a tunnel between them and will transmit the data packets in that channel.

**Related Works:** Wormhole attack is one of the vicious attack in network. In the case of wormhole attack, data packets sent to the actual nodes of the network are readdressed to the nodes which are not part of the network. This unauthorized nodes are said to be the so-called wormhole nodes. And this scenario is the result of the wormhole attack. This attack basically has two types of characteristics in which it either addresses itself as it is the nearest node from the intended sender or destroys it once it receives the packets or it interrupts the packet transfer in protocols like AODV and DSR [1]. And in order to detect and prevent the packets during data transfer, the wormhole detection function is added along with DSR protocol as part of it. So, when DSR protocol is active, it emerges the functionality alongside of its process and once any wormhole node is found then that affected node is added to the routing table of the node which carries the packet in order to avoid the path where the node resides.

Using cryptography alone to crypt data packets is not sufficient to prevent the packets from wormhole affected nodes from dropping the packets. The wormhole node doesn’t create packets instead they just route the packets from actual route by advertising themselves as they have the shortest path. When wormhole establishes channel, it receives the actual data from the actual nodes and damage or alter the data packets and forward the same to other nodes in the network. Wormhole node broadcast itself has an immediate neighbor though in real there are in distance from each other and gets the data packets from source node and make the actual nodes to communicate with the wormhole affected nodes without their knowledge or authentication. The process of wormhole attack can be divided into two segments which are initiated with two are more malicious nodes. The wormhole nodes pretend to be the legal node and broadcasts itself as nearest neighbor in result the source node forward the data packets. This process is the first segment of wormhole attack. In the second segment, the data packets received by the wormhole affected node either drops the packet or damages the packet in different ways. [2, 3]

Many solutions have been proposed by scholars to overcome the wormhole attack which is considered to be the most vicious attack of all attacks in the network security. And the solutions could fall under categories like statistics, time based, location based, key based and graphical based results. In the same way there are multiple solutions for detection and prevention of wormhole attack in the network. And the environment this attack takes place is listed like node monitoring, packet lashes, time to flight, directional antenna and so on. Even GPS based techniques against wormhole attack can be used but the only drawback is such techniques becomes useless under the areas where GPS doesn’t work. The consistency for time synchronization for the temporary packets delivery is practically impossible and couldn’t be achieved in the mobile ad-hoc networks. The techniques like hop count analysis, cluster based, neighbor node monitoring and statistical analysis doesn’t require any specific hardware for implementation or for preventing the wormhole attack though it works up to certain extent. Hop count analysis is one of the well-known solution for wormhole attack but as it causes high load in the network by flooding the network with routing messages for a single route discovery. Statistical analysis only work under multipath
on demand network protocols. In spite of many solutions against the wormhole attack, the attack itself evolves in different ways and affects the routing protocols. So, the need for an effective solution against wormhole attack is required as it is a very difficult attack to be detected of all the attacks in the network.

The methodology used in this technique is associated to the examination of attacks like wormhole in MANET. When the traffics are diverted to the nodes which are not part of the network then the existence of wormhole attack is proved. The traffics are diverted to the special node called wormhole node. The wormhole attack falls in two characteristics. The wormhole node broadcasts itself as it has the shortest route to the node which transmits the data and once the data packets are received by the wormhole node it will either drop the packets or alter the data in the packets. And it could take place in routing protocols like AODV, DSR. The data packets which are damaged or altered is consumed by the nodes which actually part of the network falls under the second characteristics. This technique works against the nodes which have an abnormal behavior while the data is being transmitted in the network. It focuses on detecting the nodes which misbehave by dropping or altering the data packets in the network. It also prevents the nodes which are affected by wormhole attack from sharing the transmission process to deliver the data packets to the destination node, it first needs to broadcast the RREQ by doing the route discovery all again. This technique works under DSR protocol by adding up the features of detecting the wormhole attack and preventing wormhole affected nodes in the network. This modified DSR not only detects the existence of the wormhole affected node but also prevents the affected nodes intruding into the network without disturbing or slowing down the performance in the network. It detects the affected nodes and the path it exists and simply it drops the node from the routing table and makes sure no further any of the nodes use the specified affected route for any of the communicational process. To calculate the performance of network jitter, delay and throughput are evaluated.

In the case of passive attack RTT (round trip time) mechanism is used in order to detect the malicious nodes which are not part of the actual network while identifying the neighbor list in both network and MAC layer. In the case of active attack, the wormhole affected node changes the packet header which in result data packets reach the wrong destination. To overcome that problem a flag is used which indicates the reception of data packets from the sent node which is involved in current transmission of data packets. The wormhole attack is detected based on the RTT of the data packets which is transmitted across the actual routers and the neighboring node numbers. This existing system [4] is divided into three segments. At first, neighbor list is constructed for each node which is involved in the routing process. Then the second segment traces the route from the source node and the destination node. Last segment detects the existence of wormhole link in the network to prevent the packets from the wormhole affected node. In the case of wormhole attack, the affected node gets the data packets at certain point and forwards the same to other location through the wired or wireless link in a high speed network. The so called wormhole attack in general is taken as a bidirectional though there are chances for it to be multidirectional where the data packets are forwarded to multiple nodes which are affected by wormhole node in a high speed network. And this type of attack can be either a passive attack or an active attack. Passive attack will break through the network and use the data packets but it will not damage the data packets. But an active attack not only breaks through the network and use the data packets which are being transmitted but also modifies the actual data in the packets.

The source node which is supposed to initiate the transmission process to deliver the data packets to the destination node, it first needs to broadcast the RREQ message to all its neighboring node. And resume the RREQ time by sending TREQ. And the same is done by the routers where the routers forward RREQ message to the other nodes and TREQ time is saved. And once this continues and finally reaches the destination node, it replies back with the RREP message. And the RREP message is forwarded in the route from which the RREQ is forwarded. Routers save the TRRPTimeonce it receives the RREP message. And the same continues until the RREP message reaches the source node. RTT is calculated by subtracting the time taken by RREP with the time taken by RREQ. The calculated RTT is forwarded to the source node for decision making and analyzing. And the RTT of all the intermediate nodes are calculated by the source node. And comes up with a threshold value. And the value of all the intermediate nodes are compare with the threshold value. If the value of intermediate node is even one value higher than the threshold value then the existence of wormhole attack in the network will be confirmed. At the time of route discovery, the time when RREQ sent and the time when RREP received by the node is noted. And the same is done for each and every set of nodes which send the
RREQ and receives the RREP. And this timings of sent node and received node are used to calculate the RTT. Based on that the route is chosen.

The wormhole attack is formed in a network by introducing a tunnel between two malicious nodes. The solution to overcome the wormhole attack is to break the communication with the wormhole nodes or breaking the tunnel for any further communication. And the wormhole attack is not at all affected by the usage of MAC protocols and the cryptography techniques in the data packets and in the network. To intrude the transmission process, the data packets are maliciously replayed. And the malicious node doesn’t have a need to know about the MAC protocols used in the routing process or the cryptography methods used to crypt the data packets to prevent it. As the malicious nodes simply replay packets as soon as the packets arrive without waiting for all the packets to be received. The transmission of data packets is really fast. And it is done even before realizing the existence of such attack. So it is possible to detect these wormhole attack by using the timing analysis. The attack cannot be stopped even by securing the data packets by applying authentication and confidentiality. Though the malicious node doesn’t have any cryptographic key to encrypt the data, still can proceed on replaying the packets. The difference between the other attacks and the wormhole attack is that the wormhole attack waits until each and every packet is received and then replays the entire packets but it is not the case for other attacks. Other attacks in contrast with wormhole attack doesn’t wait until all the packets received and just replays the packet one by one as soon as their received. CL-MAC [5] a cross layer MAC protocol is known as an efficient protocol for WSN cross layer MAC protocol. Comparison is done between the existing solutions and the CL-MAC protocol. Information of network exchange control and the two neighboring nodes are used to trace the shortest path to reach the sink which in result all the nodes which exists on the route can able to transmit the data packets once the route is finalized. The actual nodes which involve in the routing process has neighboring nodes that is not part of the network. Such neighboring nodes of the actual nodes which is not part of the routing process has to off their transceivers until the process is being completely finished. CL-MAC works really well under the following circumstance one is a secured network, second is a flat topology and the third is by using information of network exchange control and the two neighboring nodes are used to trace the shortest path. CL-MAC protocol is not taken into even smallest consideration for attackers. Routing protocols will lead to several security problems. And the channel which is used for transmitting the data packets is highly typical to be prevented from the attacks in the network. CL-MAC protocol makes sure that all the nodes which are actual nodes of the network are engaged within the network. So that the nodes that are part of the network will not be disturbed by the wormhole affected nodes. When a node from one path intends to communicate with a node from other path, at the time wormhole nodes may join the ends of the both paths and act as a part of the network. The wormhole node in the second path may stop the routing of data packets to the second path by cutting down the link between two paths.

Wormhole nodes may appear to be apart from each other but these nodes form a tunnel in between them which is nothing but a direct connection between these wormhole nodes. But these nodes address themselves as they have the shortest route and are appropriate for the data transfer. But once these wormhole nodes receive the data from the actual nodes, it will either delete the data or modify the actual content of the packet. Wormhole attack can be carried out in two ways (i) Packet Encapsulated Channel: when two nodes namely m1 and m2 form a channel between them once m1 receives RREQ (Route Request). And m1 forwards the RREQ to m1 in a predefined channel. Once m2 receives RREQ, it forwards till it reaches destination. Destination node sends the RREP (Route Reply) in the same route. And the same reaches the source node. (ii) Out-Band Channel: Over a wired network, two nodes can send data from long distance [5].

Wormhole attack can be classified into different form of attacks based on the behavior. There are classified into internal and external and also like internal and external attack. The attacker can use the either of the forms such as internal or external attack to affect the routing process in the network. Couple of nodes are used by the attacker in the case of wormhole attack. This couple of affected nodes use a tunnel or a private connection to communicate with each other in the ad hoc networks. This type of affected nodes once receives all the data packets it will forward it to the node which in result the node will broadcast the data packets all over the network. This changes will differ from the actual routing process and may cause of difficulty in the routing process in the ad hoc network. Wormhole attack along with the other attack in the network may take over the control of network traffic. Wormhole attack is one of challenging attack in the network especially in the AODV protocol in the mobile ad
hoc network. The classification of wormhole attack can be distinguished into out-band, in-band and self-sufficient wormhole. Regarding wormhole attack many researchers have proposed many methods to overcome wormhole attack in the network in MANET. By using the electromagnetic wave to detect the existence of wormhole attack in the network. Even for existence of wormhole attack in multiple routes many methods and algorithms were proposed [6]. Compared to the other attacks in the network Siebel attack is quite different where one node act as two or more nodes. By means of duplication, false identity and replication Sybil nodes are generated. This can be made possible by using a physical device. This type of Sybil attack is caused by attackers with more duplicated nodes and false identities. Existence of Sybil attack can be detected by using the mathematical derivation to validate it.

Combination of E-HSAM [8] and AODV-WADR-AES [9] is TSMI (Timed and Secured Monitoring Implementation) which is used for mitigating wormhole attack. AODV-WADR-AES method detects the existence of wormhole attack in the network. Only after ensuring that there is no trace of wormhole attack in the network, the data packets will be sent to the nodes in the network. In this method [10] DH (Diffie-Hellman) is used to minimize the intrusion of attackers in the network while moving packets from one node to the other node. The purpose of using DH (Diffie-Hellman) key is to help nodes to verify each other. Using AODV protocol the routes are obtained. And this is where the AODV-WADR-AES is of utmost use. This method is further proceeded. And it further proceeds by gathering the hop count at the time of route discovery. Once the route hop is confirmed to be greater than 3, then the AODV is started. Now by choosing 3 hop condition, the source node along with the destination node will authenticate each other by using the DH key of AES algorithm along with the time parameters. It is done during the identity verification. Once the authentication process is succeeded, the source nodes proceeds further by sending the data packets to the destination node. Though this method is considerably good for authentication process, this method has its own drawbacks. The drawbacks as follows (1) at the time of data transfer there is no assurance that the data packets are sent in secured path or the data packets itself is protected; (2) using AODV-WADR-AES only 3 hop routes are analyzed. And it is not efficient to use for less than or greater than 3 hops. This method fails in such condition and becomes useless. In such situations malicious nodes takes advantage and may do some damage to the data packets even before there are exposed by the algorithm.

In order to overcome the intrusion of hackers and to secure the data packets, the HSAM protocol [11] is used. This protocol is designed in the way where it prevents the malicious nodes from altering or damaging the data packets during the transmission in network. This method includes two counters. One counter counts the number of packets which are successfully delivered to the destination node. This counter is called as cpkt. And the other counter is called as cmiss which is used to count the number of packets that are dropped on the way to the destination node from the source node. And using the cpkt and cmiss the limit of tolerance is calculated. And the limit of tolerance is set to 20%. It is used in order to determine the secured route. When the specified ratio exceeds the threshold value then it is considered as unsecured route. In addition, this method uses the time window where the data is to be delivered to the destination node within the specified time limit. If not, then the route is assumed to be not a secured route. And acknowledgement time limit is also specified where the ack is to be sent to the source node within the specified time limit. If not then the data packet is presumed to be lost.

A malicious node is capable of recording the data packets in the specified time limit as mentioned in the HSAM [12]. The threshold with different timing is tested to know which one is the suitable threshold for AODV protocol and result as a more secured path. This concept is used in the EHSAM (enhanced HSAM) [8], HSAM and EHSAM are almost similar but there is one major difference between these two protocols. That is the protocols have their own way in transferring the data packets. In the case of HSAM, the actual data packets are divided into the sub parts in the size of 48 bytes which is sent to the destination node. And using the reactive approach, the data packets are sent once the route is confirmed to be secured. The data packets which are sub divided to transfer can be damaged by the malicious nodes. In result the chances of altering the actual data or damaging the original data increases. So, in order to overcome this problem E-HSAM[8] is used which makes use of duplicate sub parts which contains only random words that does not belong to the original data. Therefore the intruders cannot easily able to get the original data. The number of dumb packets sent is divided based on the actual payload size of the data packets. And the split value is considered as 48. The reason\
behind the split value and the size of the data packet is determined based on the limit of tolerance. For this the sufficient number of $c_{miss}$ and $c_{pkt}$ is needed. For the small data packets, the split value should be determined so that the reliable ratio of $c_{miss}$ and $c_{pkt}$ can be obtained.

And the next big difference is about the avoidance of route which contains malicious nodes. Modified self-developed method is used in order to avoid the routes which has malicious nodes. But in the case of E-HSAM, it uses the method similar to AODV for sending Route ERR back to the sender node. This method is used in order to avoid the malicious route by moving forward to the next sequence number in the routing table to choose an alter route for transmitting the data. And E-HSAM present the wormhole attack in a similar way than the HSAM. Sending dumb packets which is generated based on the size of the actual data in the network, when an malicious node tries to access the data then the original data will be prevented from exposing.

As the dumb data packets does not contain any original data it is of no use to the malicious nodes. The proposed TSMI (Timed and Secured Monitoring Implementation) approach [7] presents the weakness of both AODV-WADR-AES and E-HSAM. And it uses EHSAM to keep track of all routes which are greater than are lesser than the 3-hops between the source and the destination node. AODV-WADR-AES keeps track of the routes which has exactly 3=hops from the source node to the destination node in the network. Each data packet consists of the hash value in the AODV-WADR-AES to secure the data integrity. And blacklist table is maintained in order to avoid using the affected route twice. The blacklist is maintained by retrieving the malicious route in formation which is detected by both the AODV-WADR-AES and the E-HSAM. So, that the TSMI approach is presented to overcome the weakness in both AODV-WADR-AES and the E-HSAM. The broken link table sequence number is incremented each time to choose the alter path once the chosen path seems to be the affected route.

To keep track of the behavior and actions of data packets which is being transmitted from one to another in a network channel in WSN using certain techniques are discussed. Wormhole attack falls in different types based on their behavior and actions which is clearly stated in [14]. There have presented the types of wormhole attack in a paradigm and their classification in WSN. And the classification is done based on the OSI (Open System Interconnection) layers. It also explains the wormhole classification and the methods to detect the wormhole attack and techniques to prevent the data packets from the wormhole attack in the network by integrating the monitoring modules with the wormhole attack detection techniques a system is presented by sun [15]. The affected data packets are detected in the proposed model by using the EKF (Extended Kalman Filter) mechanism. The algorithm in this existing system is the combination of collective summation and the generalized probability. The ratio of both collective summation and the generalized probability is calculated to strengthen the sensitivity for detecting the wormhole affected nodes and the wormhole affected data packets. And the discussion about how the detection method effectively works alongside of the monitoring techniques to overcome the limitations in the detection methods is explained [13]. And also the mechanism of proposed work is explained to classify the difference between the emergency events and the malicious nodes.

Collecting information based on the user requirement on tariff a framework is built in WSN [16]. Alongside of the framework, two key process are used with the traffic information of retrieval and delivery is specified. In order to obtain the data packet information, 3 varieties of sensor nodes are deployed and one classified communication channel is established between the sensor nodes. In controlled MSN (Mobile Sensor Networks) various methods for tracking the target is used and the explanation on such various methods are explained in [17]. When the sensor nodes move, each and every time a target is fixed and it evaluates the present position of the target and predicts the next following position by using the second order prediction model. To obtain the current location of the target, the sensors are relocated. And the position of the sensor nodes are in the form of triangular based method. And each sensor node are allocated with one position of set by using the ant colony optimization algorithm. The combination of both the static nodes and the mobile nodes is used in hybrid sensor network.

In WSN (Wireless Sensor Network) [13] using a secured architecture the system works against the wormhole attack using cryptography as a part of it along with the digital signatures. There have used cryptographic technique to protect the data from the malicious nodes by monitoring the actions of data packets which is being transmitted from one node to the other node. An architecture is created based on the necessity for protecting the privacy of data by monitoring the actions of data in WSN. In such way where the actions of data packets are monitored and at the same time it ensures that the data packets are not altered are damaged by the malicious nodes. This system can able to identify the
malicious node for its actions of changing or damaging the data packets while being transmitted. This architecture is composed of network model, AES (Advanced Encryption Standard), Packet Generation, encryption, decryption and trusted authority.

The discussion of each module as follows: Network Model is considerably important in the architecture as it controls the access mode for data packets which are being transmitted from one node to other in the hop to hop process in the network. AES is one of the well-known algorithm in the field of cryptography for encryption and decryption using the same key. To preserve the privacy of the data, AES algorithm is included as part of the architecture for encrypting the data which is being transmitted in the network. AES algorithm ensures the data integrity in the packets at the time routing. And once the route is confirmed as safest route to transmit the data packets then only the data packets are forwarded in the route. The data packet delivery differs from one another based on the network and the cryptographic methods used. To highlight AES algorithm is used to increase the privacy of data packets and to reduce the loss or damage of data packets by the malicious nodes in the network.

And in general it keeps track of the behavior of the data packets. Packet generation is part of the architecture as it plays the part of secret key. Secret key is shared by the both sender and receiver as it is the key to cipher and decipher the data in the packets which requires some privacy and confidentiality for data to ensure that the data is not being hacked by some unauthorized nodes while transmitting in the network. Encryption is part of AES algorithm where the encoded data sent by the sender can be decrypted by the receiver only by providing the secret key shared by both the sender and the receiver. Decryption is also part of the AES algorithm where the secret key is generated the sender while encrypting the data. And the actual receiver only can able to decrypt the message by providing the secret key which is shared by both the sender and the receiver. And at last (TA) Trusted Authority is used as part of the architecture where it authenticates the digital signature. And each and every nodes are registered here. And at the same time it monitors the actions of the data packets being transmitted in the network. And the existing system [13] includes authentication method, secured channel to transmit the data, uses cryptography for encryption and decryption of data packets by providing symmetric key and also includes trusted authority.

Several applications were owned by LNC (Linear Network Coding) and in more specific by RLNC (Random Linear Network Coding) [18-20]. Optimization of information capacity is totally based on by allowing the nodes to transmit the received data in the same combination in the network. The prime goal of this existing system [18] is to identify the existence of the wormhole attack in the network as soon it enters rather than making a check throughout the entire network. And it mainly focuses on the wireless network coding system. Difference between the packet forwarding and the routing can be noticed based on the existing systems which are previously done in the traditional networks [21], [22-25]. In the case of network coding each and every node will use from the given inputs to the destined output in GF (2^n) except for the recipient nodes. Each and every node is represent in the form of vectors with m dimensions in the vector space V. The data packets which are sent by the source node will carry the information about the coded vector space. A packet is called as innovative packets if it is apparently independent from the other packets which are previously sent by the source node through the intermediate nodes.

In the field of network application, there are wide application for RLNC which is of in great use to improve the capacity of information in the means of utilization and throughput. Mainly in COPE, ExOR, MORE [26-29]. And it is really difficult to bring this ideas and solutions to implementation due to several reasons. Such as solution fails to satisfy the reality of vulnerable environment or their not sufficient research materials to the security problems in the current trend. The RLNC is exposed to various types of attacks such as byzantine attack, pollution attack and wormhole attack. But this system’s main objective is to expose wormhole attack in the RLNC network. Several solutions were proposed by various researchers to find the existence of wormhole attack and avoid it in the traditional networks. Such solutions can be split into two major categories. One is by making use of the spatial and temporal information and the other is by detecting based on the changes in the network topology using graph analysis. In [21] using packet leashes the existence of the wormhole attack is detected. And it is made possible by adding the sender node’s location information with the data packets itself. So the transmission which is physically impossible are detected. And in the case of [30] and [31], the existence of the wormhole affected node in the network is detected based on the time taken by the packets to travel around in the network to detect the existence of wormhole affected...
links. And the guard node is introduced to expose the existence of wormhole affected node by the local node. It is presumed in the case of network topology which are static. Applying space and time algorithm to detect the existence of wormhole attack in the network has two limitation though it work to certain extend to prevent the wormhole attack in the network. The first limitation is that the nodes is to be tightly synchronized in the network and the second limitation is that the location information of the source node is to be added within the data packets.

In the second category, visualization methods are used to detect the existence of wormhole affected links in the sensor network. Visualization methods are used to detect the wormhole affected links by easily identifying the abnormal changes of the network topology. In [24] the behavior of the wormhole attack in various ways is observed and the all possible changes made in the topology structure due to the existence of wormhole attack is also noted. Regarding connectivity in the wireless network coding systems it is explained in several ways in different dimension distinguished from the traditional networks. In result there is no liable solution for detecting the existence of wormhole attack in the network in the case of wireless network coding system.

All the possible damages that could be caused by a wormhole attack in the wireless network coding system is discussed in detailed [18]. Two algorithms were proposed in this system which make use of metric ETX to act contrary to the wormhole attack. Centralized algorithm is used as one among the algorithm which declares a central node. Central node monitors and controls the other nodes which are part of the network by analyzing the behavior of each and every node which involves in forwarding the data packets to the other node. By which it prepares against the wormhole attack by all possible ways when the attack is initiated in the network. The centralized algorithm is proven to be suitable for detecting the wormhole attack by deriving the lower bound of deviation. DAWN (Distributed detection Algorithm against Wormhole) is the other algorithm proposed to act against the wormhole attack in wireless network coding system. The main advantage of using DAWN is by removing the limitation which is listed in time and space of p tightly synchronized clock. To overcome the communication overhead, ratio of number of packets which are produced by the wormhole node and the overall data packets which are actually sent by the source node. And the communicational head is manageable if the density of the nodes are not too high. To strengthen the analysis, digital signature is used by both the distributed and centralized algorithms to limit the forgery of wormhole affected nodes.

There are several solutions proposed to overcome the wormhole attack in the network. And in specific WSNs and MANET which involves statistical based, location and time based and graph based to detect and act against the wormhole affected nodes in the network. When it comes to location and time based networks, each and every packet is sent along with the header information or the packet leashes to make sure that the packets received by the destination node are received in the order and to make sure no data packets are went missing. Packet leashes can be classified into two types. One is temporary leash and the other one is packet leash. In the case of geographical leash, the sender itself adds its own information and the time it is going to send the data packets to make it easier for the receiver node to calculate the distance from the sender node and the receiver node. In the case of temporal leash the sender node either includes expire time or sent time information along with the data packets to let the receiver node calculate the distance it travelled. The distance travelled by the data packets are calculated by using the time taken to transmit and the speed of transmitting data packets. Cryptography and time synchronization are two common types required to secure the data packets from exposing to any type of vulnerabilities which are being transmitted in the network. But in DTN (Delay Tolerant Network) it is assumed to be a difficult task to handle. In [33] directional antennas are used by the mobile nodes to find the neighboring nodes which in result can identify the existence of wormhole attack in the network. The nodes are said to be authentic neighbors when the direction of data packets sent by one direction is complete opposite to the direction in which the data packets are received by the receiver node. So based on the data packets sent and received by the sender and receiver are completely opposite directions by which the nodes validate each other. This proposed solution is used to detect the forged neighbors in the network but it is only effective when the intruder node consists of two endpoints. The requirement for the additional hardware is needed due to the limitation of detecting wormhole attack only when an intruder has two endpoints.

In the case of methods which are statistical based, existence of wormhole affected nodes are detected in the WSN (Wireless sensor Network) by applying chi-square test on the parameters which shows abnormal results.
when it is affected by wormhole attack. There are two mechanisms proposed in the case of statistical based methods. For detecting the neighboring nodes of sensors which are increasing, NTT (Neighbor Number Test) is used to achieve the information. To reduce the length of the all possible shortest path for sensors ADT (All Distance Test) is used. In this proposed mechanisms each and every node is required to send its neighbor list to the base station to construct an algorithm. And this base station should have information on the distribution of node before computing the hypothetical distribution. This process can only be used for detecting the existence of wormhole attack in the network but it is not possible to locate the exact position of the wormhole affected node. And the drawback of using the centralized base station is due to the consumption of huge quantity of communication and also coordination overheads. In the [34], a method is proposed which is another statistical based collects all the past information of neighbors to analyze the average number of neighbors. And when a neighbor count in the current process seems to be abnormal then it is compared with the history of neighbor count information. And it gives all statistical changes to be done once the existence of the wormhole attack is conformed in the network. This solution is proposed based on both the localized and distributed which in result leads to no overhead. In contrast the centralized approach faces packet overhead.

For detecting the existence of wormhole attack in the network a wormhole detection algorithm is proposed [35] by finding the restricted substructures in the graph which can be found only in the wormhole affected node. Once the existence of wormhole attack is confirmed by a node in the network, it will immediately alert all the other neighboring nodes which are part of the transmission process. Neighbor count is used as a method for the detection of wormhole attack. But this method all proposed in the WSN where the density of nodes is very high. So the existence of wormhole node will be easily identified. In contrast it is difficult to find the difference in the DTN. This existing system [32] is proposed to detect the wormhole attack by using a geographical based method in DTN. It is used to act against the forbidden network which is the art of wormhole attack in the network. This type of forbidden network is restricted from legal network. Because this type of forbidden network confirms the existence of wormhole attack in network. And this proposed method is more efficient by its simple working system, distributed and reduces overhead in the restricted topology. So this proposed DTN is more suitable in the low density as well as resource constrained nodes. In the case of an inefficient network model with nodes of high speed in network and propagation loss in the network. It is because the maintenance of information in the connectivity may not be accurate and in addition false information might be incurred. This proposed method is used for comparison of both the result obtained and the performance evaluation.

CONCLUSION

This paper reviewed several concepts, efficiency of algorithms, problems and solutions proposed by several scholars. And this paper focused on wormhole attack considering the severity of the attack in MANET. Several papers were been analyzed and discussed including the issues there have placed and the solutions there have proposed. Each and every paper discussed earlier have presented different security solutions which are more effective and efficient. So, suitable technique can be used to avoid or to prevent from wormhole attack on the basis of throughput, delay and so on.

REFERENCES


