IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. VI (May-Jun. 2014), PP 84-91
www.iosrjournals.org

Implementation and Comparison of a New Wormhole Detection Technique with Existing Techniques

Gauri Mathur[1], Raj Karan Singh[2], M. Vijaya Raju[3]
[1]*Department of CSE/IT, Lovely Professional University, Punjab, India*
[2]*Department of CSE/IT, Lovely Professional University, Punjab, India*
[3]*Department of CSE/IT, Lovely Professional University, Punjab, India*

Abstract: *Mobile Ad hoc networks are increasingly popular these days as they function without major requirements of state of the art infrastructure and the fact that they can function without the need for a central controlling authority. The widespread usage of the MANETs (Mobile Ad hoc networks) also poses some serious problems in them. Because of the high availability of MANETs and improper security measures make the MANETs a ready target for attackers which adopt both active and passive approach to attack the MANET. A classic attack on a MANET is a DOS attack of which wormhole attack is most noteworthy as it is easy to deploy and can cause great damage to the network. In the wormhole attack, an adversary connects two distant points in the network using a direct low-latency communication link in the MANET which is called as wormhole link. Once a wormhole is established, the adversary captures the wireless transmissions on one end and send them through the wormhole link and replays them on the other end. There are many methods available for wormhole detection which include in some cases the use of sophisticated hardware and in other cases makes some modification to the already present information in the MANET. The presence of a wormhole may also be detected in some cases by the use of time delays or geographical locations. A wormhole can be detected when the network has already been set up and wormhole nodes try to penetrate at a later time and secondly when the wormhole nodes were already present in the time of network setup. In this paper, we adopt a new approach which is different from the already existing approaches of wormhole detection. The approach adopted by us has the benefit of saving memory and processing which is an improvement over the other techniques of wormhole detection. It also advocates the use of a modified routing table wherein the routing table will be modified to have an extra consisting of full paths of each node next to the hop. Using this approach of modified routing table, we can identify suspicious links long before the attack takes place and starts disturbing the network. This approach is implemented on various routing protocols with the help of NS3 and a comparative analysis has been made for the same. A comparison of this approach with some other techniques of wormhole detection is also carried out to highlight the effectiveness and efficiency of this approach.*

Keywords: *wormhole, detection, hop count, routing table*

I. Introduction

A MANET is very popular these days because of the ease of setup it offers. The ease of setup stems from the fact that there is no presence of a central controlling authority in a MANET. Furthermore, each of the constituent devices in a MANET can move independently in any way and hence the links to other devices change often. Other major reason for the popularity of MANETs is the widespread growth and penetration of mobile devices and advancements in the field of wireless networking. MANETs can be visualized as a type of Wireless ad hoc network which generally has a routable networking environment built on top of a Link Layer ad hoc network.

The MANET protocols can be roughly categorized as Table-driven (proactive) routing protocols and On-demand (reactive) routing protocols. Some of the most popular routing protocols are AODV (Ad hoc On-Demand Distance Vector) routing protocol and DSDV (Destination Sequence Distance Vector) routing protocol. Although a MANET has many advantages and offers the ease of set up, however its own specific features pose a serious challenge for security solutions and leaves it vulnerable to a wide array of problems. A part of the problem stems from the fact that many of the protocols used in MANETs do not consider security. A MANET suffers from the vulnerabilities of wired networks, prime among whom are eavesdropping, denial of service, spoofing etc. To make matters worse, there are further problems which build on and prey on the cooperative nature of routing algorithms. Among the prime threats to a MANET of particular note is the wormhole attack. Wormhole refers to an attack on MANET routing protocols in which colluding nodes create an illusion that two remote regions of a MANET are directly connected through nodes that appear to be neighbors but are actually distant from one another[1]. A wormhole attack is particularly severe and most destructive in a MANET as the attackers are linked by a high-speed connection and are generally present on the two ends of a network. The basic methodology adopted in the wormhole attack is the advertising of the false path which makes the information pass through the malicious nodes, thereby leaving the information susceptible to misuse. Here in this paper, we have made use of a new detection technique which helps in identifying and isolating the colluder nodes present in a wormhole attack, thereby limiting the damage done by the wormhole. The technique makes use of a modified routing table which has been enhanced and altered to contain among other things the destination nodes, the path which can be used to traverse the network along with the number of hops. We have successfully implemented this technique on AODV and DSDV MANET routing protocols in NS3. We compare and contrast the implementation on these specific protocols and carry out a comparative analysis of this new technique with the already existing techniques of wormhole detection like packet leashes, DELPHI, SECTOR, SAW, DAW and directional antenna methods.

II. Wireless Routing Protocols

2.1 Ad Hoc On-Demand Distance Vector Routing (AODV)

AODV protocol which offers the unique advantage of not putting extra burden on the existing lines in a network, along with lesser requirements of memory and calculation is based on the fact that there is not much going on in the network until a connection from one node to the other is required [9]. At this point, the needy node which requires a connection broadcasts a request for the same. Other nodes present in the AODV network, forward this message, in turn recording the node they hear the broadcast request from. This in effect creates an explosion of temporary routes back to the node which required the connection. On receipt of such a message by a node which already has a route to a desired node, it sends a message backwards through a temporary route to the node requesting the transfer. This node will now begin using the route which has the least number of hops through other nodes. All the entries which are unused in the routing table are recycled after sometime. If a link is to fail, then it results in a routing error which is passed back to the transmitting node and the entire process is repeated. This protocol aims to lower the number of messages in order to conserve the capacity of the network. It makes use of sequence numbers to eliminate the repeating route requests which have already passed on.

2.2 Destination-Sequenced Distance Vector Routing (DSDV)

DSDV protocol is yet another protocol which is quite popularly used in the MANETs. It follows a table-driven routing scheme and is based primarily on the Bellman-Ford algorithm. The main aim of this particular protocol is to provide a solution to the routing loop problem. This protocol utilizes the scheme of sequence numbers, which are generated if a link is present; else in its absence an odd number is used. The generation of the sequence number is done by the destination, however it is sent by the emitter in the next update accompanied by the sequence number. The distribution of routing information between the nodes is done by swamping the entire information infrequently as compared to subsequent smaller incremental updates which are carried out more often. The selection of the best route by the router is done by choosing the latest sequence number on the receipt of new information, otherwise if the sequence number matches the one which is present in the table then the route which is more advantageous is chosen. The entries which are not used for a while are dubbed as stale entries and these along with the routes using those nodes as next hops are deleted.

2.3 Wormhole Detection Techniques

A lot of techniques have been proposed to successfully detect a wormhole attack and minimize the damage done by such an attack. These techniques involve monitoring the behavior of neighboring nodes and sending of RREQ messages to destination. If a node acting as the source node, does not receive the RREP message within a specified time limit, it detects the presence of a wormhole attack and adds the route to its wormhole list. There are also techniques which are based on detecting an abrupt decrease in the path lengths which could serve as a possible symptom which could aid in the detection of a wormhole attack. Packet leash is yet another mechanism for finding and setting up defense against wormhole attacks. This mechanism is further subdivided into 2 subcategories namely geographical and temporal leashes. SECTOR is another such wormhole detection technique presented by Capkun. Then there is DELPHI which makes use of hop count as well as delay per hop in order to find the wormhole.

III. Simulation And Analysis Method

The simulation method was carried out with the help of Network Simulator 3 (NS3) which is a discrete event simulator for Internet systems. The target area of NS3 is networking research and is widely used in the research of MANETs. The proposed approach modifies the existing routing table to take into account the destination nodes, path followed from the source node to the destination node, number of hops required to reach a certain node. In order to implement the same in NS3, we modeled and included special classes to accommodate for changes to the routing table, for injecting and proliferating the colluder nodes in a MANET thereby introducing the wormhole attack. The concept of inheritance came in handy to derive the subsequent classes from the base class which was our modified routing table. A new class was introduced and inducted which had data members and member functions to locate, confirm and blacklist the colluder nodes. This class thrived on the concept of public inheritance to accommodate the base classes and successfully implemented the said procedure for both AODV and DSDV protocols. A simulation run for 17 nodes created 100m apart bearing IP addresses starting from 10.0.0.1 onwards was done for both AODV and DSDV. The implementation of the proposed approach on these two protocols was compared on the following metrics:-

1. Ease of implementation of the approach.
2. Accuracy of detection of wormhole by the use of the approach in the protocols.
3. Time taken to detect the wormhole in the two protocols.
4. Adaptability to changing external factors.

In the subsequent part of this paper we have compared the new approach with already existing approaches such as packet leashes, DELPHI and SECTOR method. The comparison was carried out on the following parameters:-

1. Ease of setup which included the cost incurred in implementation of a said method.
2. Accuracy of detection of the colluder nodes.
3. Amount of overheads involved in setting up a particular technique.
4. Time required for the successful detection of a colluder node.

Table I Simulation Parameters

Simulator Used	Network Simulator 3
MANET Protocols Used	AODV, DSDV
Simulation time	100 seconds
Simulation area	500m X 500m
Number of nodes	17
Number of source	One which is fixed

Before starting the simulation in NS3, additional C++ classes were inducted to accommodate the destination node, path from the source node to the destination node, number of hops to the destination node. An additional class served to induce the wormhole into the network and advertise the false path. The concept of constructors helped to induce and member functions advertised the path passing through the colluder nodes. Another class served to implement the proposed wormhole detection technique which included member functions to check the nodes with high usage density. In order to confirm the same pattern with neighbors, this information was checked and solicited from the neighboring nodes as well. Once a reply confirming the high usage of nodes was received, in order to say that these are indeed the colluder nodes, we sent encrypted messages to the nodes. Only the legitimate nodes were able to process the encrypted message thereby bringing out the colluder nodes. Next a member function sent a blacklisting message asking the nodes to exclude the colluder nodes from communication. We ran the simulation for 100 seconds for 17 nodes by instantiating objects belonging to the said classes. NetAnim was used to depict the network prior to wormhole and after the infiltration of colluder nodes.

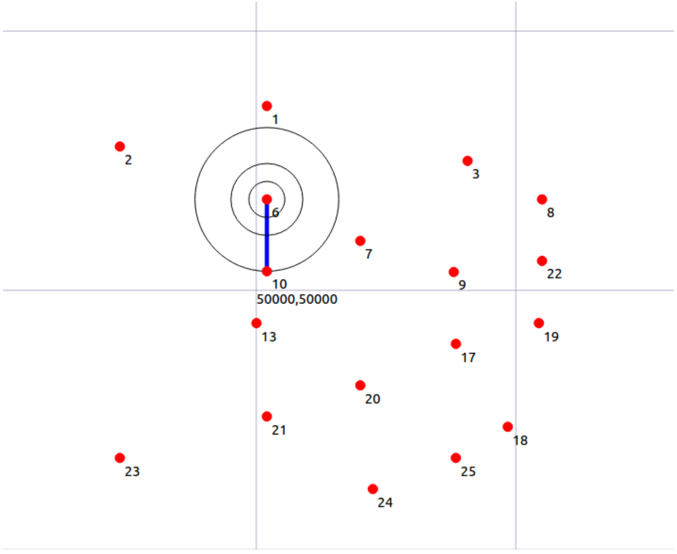


Fig. 1. NetAnim depiction without wormhole attack

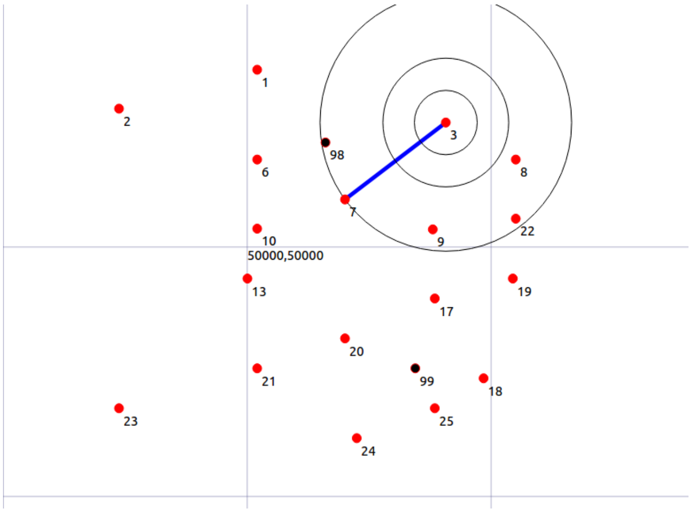


Fig. 2. NetAnim depiction with wormhole attack

3.1 Simulation Results

Simulation runs were done by varying the protocol used from AODV to DSDV. The number of nodes varied from 17 to 40 to identify the difference.

3.2 Ease Of Implementation

Compared to the DSDV and AODV, the algorithm is easier to implement in DSDV as compared to AODV as the routes frequently change in response to the network requirements whereas in DSDV this is not the case. Every time the route gets updated, the nodes with high usage density would need to be recomputed, hence the confirmation process will need to determined again thereby leading to the isolation of the colluder nodes every time.

3.3 Accuracy Of Detection Of Colluder Nodes

The proposed new approach for wormhole detection detects the wormhole with more accuracy in case there are no failures or restructuring of the network. Since in case where a network failure is not involved and all the nodes function normally the wormhole detection by the proposed approach is very accurate and quick. However in case the network undergoes restructuring or a link fails in the network, then since the DSDV network is unable to detect this quickly and efficiently, the proposed approach performs better on AODV protocol.

3.4 Time Taken To Detect The Wormhole

The time taken to detect the wormhole using the proposed new approach will be less in DSDV protocol as compared to the AODV protocol since the AODV protocol suffers from high latency time in route finding. In the AODV routing protocol for mobile ad hoc networks, the network is silent until a connection is needed and the node which needs to communicate broadcasts the request for connection, all this needs some time and hence increases the time taken. This is in contrast to the DSDV protocol in which the routing table is present for every node. However in case of an update in the network (i.e. network failure or restructuring) the information travels very slowly in case of DSDV protocol as compared to the AODV protocol, hence in this particular scenario the wormhole nodes are detected quickly in AODV as compared to DSDV.

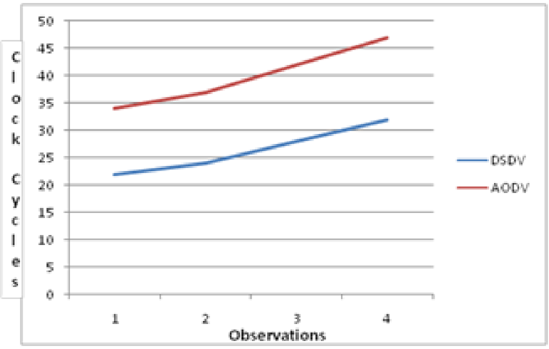


Fig. 3. A line graph depicting the amount of clock cycles required by DSDV and AODV

3.5 Adaptability To Changing External Factors

The new wormhole detection technique will perform better on the AODV protocol as compared to the DSDV protocol in the face of changing external factors as AODV protocol broadcasts a request to locate the best possible route as soon as a node needs to broadcast a request whereas the same is not present in the case of DSDV protocol. If there is a change in any external factor (example a malfunctioning node), it is bound to be detected very quickly in case of AODV, hence the wormhole detection by this approach will be more effective.

IV. Wormhole Detection Techniques

4.1 Packet Leash

Packet leash [2] is a mechanism for detecting and thus defending against wormhole attacks. The general idea behind the packet leash wormhole detection technique is to restrict the maximum distance that a packet can travel by adding certain information to this packet. This technique may be further subdivided into two categories namely geographical and temporal leashes. In case of a geographical leash, we ensure that the intended receiver of the packet is present at a certain distance from the sender of the packet. On the other hand, in case of temporal leashes, we put an upper limit on the lifetime of the packet (i.e. the time till which the packet is alive) and this helps in restricting the maximum distance this packet can travel. Both of these variants can help us in detecting a wormhole as the recipient of the packet can analyze the packet to find out if the packet has travelled further than what was allowed by its leash.

4.2 Delphi

The Chiu et al. [3] proposed the Hop Count delay per hop indication [DELPHI] method. In this particular method, one needs to monitor both the hop count and delay per hop indication. This method is built on the assumption that in case a packet is rescheduled, then the propagation for one hop is very high in case of a wormhole attack because the actual path in this case will be very high as compared to the path which is being advertised. The wormhole detection is a two step process in which in the first step, the route information from sender to receiver is collected. Here every sender will take into account a timestamp and attaches the timestamp on a special DREQ packet and signs it before sending it on its way to the receiver. On the receipt of this packet by a node for the first time, it includes its node ID and increases it hop count by 1 and the next time it receives this packet, it discards it. The receiver will send out DREP packets for each dislodge path received by it. This process is repeated thrice, thereby making it possible to select the shortest delay and hop count information for wormhole detection. The second portion of this process includes considering the round trip time (RTT) by calculating the time discrepancy between the packets sent to the neighbor and the reply received from it.

4.3 Sector

Capkun et al. [4] presented SECTOR, which does not require any lock synchronization and location information, by using Mutual Authentication with Distance-Bounding (MAD). In this method, a node say NODE X makes an approximate estimate of distance to another node Y by including a one-bit challenge in its transmission range and the node X immediately responds to it. This method makes use of time of flight to detect whether X is a neighbor of Y or not.

4.4 Saw And Daw

Both in Saw [6] and DaW [7] similar propositions are made. These two techniques of wormhole detection are available in MANETs. If we compare DAW keeping into mind the precision of alarms, DAW performs better than SAW. The accuracy of wormhole detection is also more in DAW as compared to SAW.

4.5 Directional Antennas

Directional antennas have been extensively studied in the general literature [3]. In directional antennas, the various nodes in the networks make use of specific “sectors” of the antennas to communicate with one another [5]. A node receiving a message from its neighbor has some information about the location of neighbor and needs to maintain the legitimate and accurate sets of neighbors. In case it realizes that the transmission is from a false neighbor it ignores these messages.

4.6 Proposed New Detection Technique

The following tasks are carried out in order to successfully detect the presence of a wormhole in a MANET [8].

1) Task 1:
First of all, the node will check the routing table to determine the nodes with high usage density. Once it is determined that certain nodes have high density, then a request is sent to the neighboring nodes to determine if the same high usage density is present in the routing table of the neighboring nodes as well.

2) Task 2:
On the receipt of a processing request by a node, a node checks its own routing table to determine if the same pattern exists, it sends an affirmative reply to the node having sent the request.

3) Task 3:
On the receipt of a confirmation reply, it cannot still be said with certainty if a wormhole is present in the MANET or is the reason for the reply the physical location of the nodes which have caused this path to be followed. In order to be sure, another confirmation step is adopted and we ensure that the nodes present at the ends of a suspected wormhole send some sort of encrypted messages to each other. All the legal and normal nodes along the path will be able to understand these encrypted messages (it is based on the assumption that the colluder nodes cannot decrypt the encrypted messages and therefore they cannot process this information). In addition to this the nodes add their own signatures/stamps or flags to aid identification. All this is attached to the encrypted packet payload.

4) Task 4:
On the receipt of an encrypted message a destination node searches for signatures/stamps or flags for the nodes which were on that path. All this is done to determine if the node was a legitimate node or not. If every node which is on the path has added its own signature to the encrypted message then every node is considered as a legitimate node. In case of the missing signatures of a node which is on the path, a wormhole presence is considered.

5) Task 5:
As the source node receives encrypted reply and once the presence of a wormhole is confirmed, the next step is to isolate these nodes (colluder nodes) so that these nodes do not fall into any path which is to be used for communication in the network. In other words we need to blacklist these nodes.

6) Task 6:
Once the wormhole is confirmed, both end nodes broadcasts a blacklisting message. The blacklisting message contains a list of colluder nodes which are not to be used for communication and furthermore any path update or any future request from them is not to be entertained.

Comparison of the proposed approach with techniques which are already present:-

4.7 Ease Of Setup

The proposed new technique of wormhole detection is very easy to setup as it requires a modification of routing table to accommodate certain parameters as opposed to the packet leashes technique which require the presence of extra hardware such as synchronized clocks which may include cesium-beam clocks, each node needs to be aware of its own location (GPS co-ordinates) and hence needs hardware which can aid in finding the GPS co-ordinates [10]. In the DELPHI method for wormhole detection, the packet size may become large in case the path is long. There is also extra overhead which is involved in the processing and analysis of hop information coming from various nodes. SECTOR method dictates the use of special hardware which is needed to respond to one-bit challenge which can be used for estimating the distance to another nodes present in the network. This hardware should be such that it is capable of responding to the one-bit challenge without delay. In addition to this special hardware, SECTOR also requires time synchronization and hence highly accurate clocks are needed in order to detect wormholes.

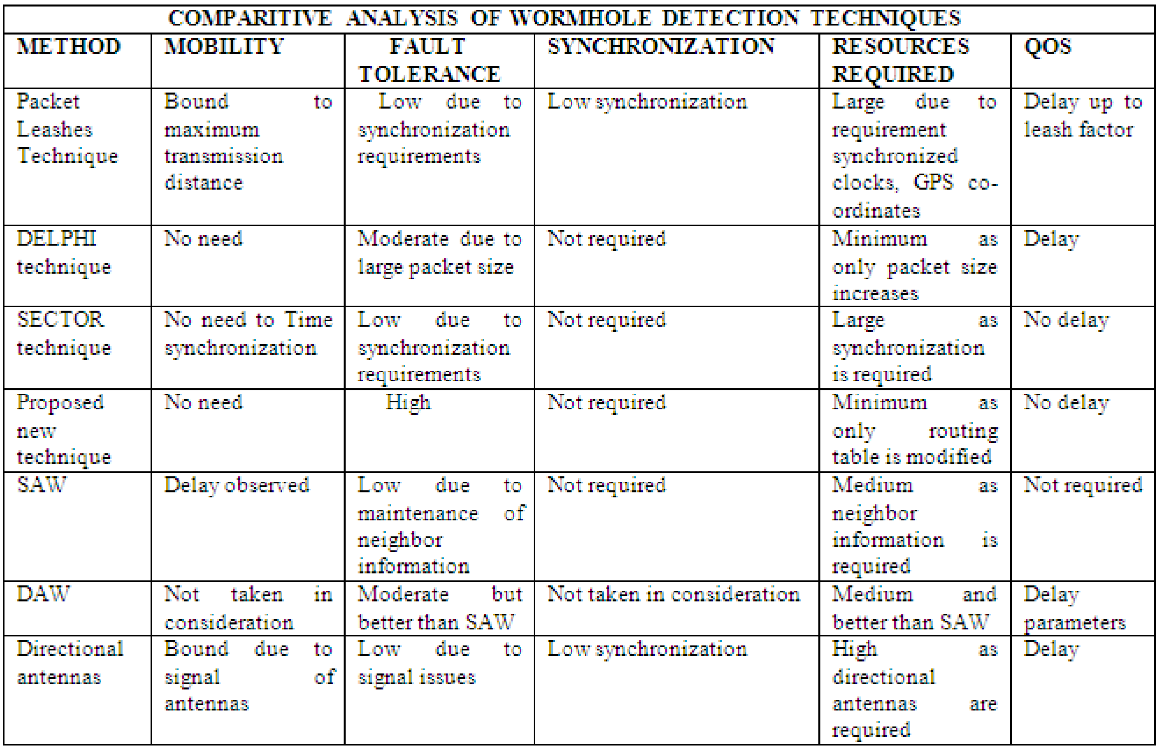
4.8 Accuracy Of Detection Of Wormholes

The proposed technique of wormhole detection detects the presence of colluder nodes fairly accurately as compared to other techniques such as packet leashes and SECTOR. Since packet leashes and SECTOR both are dependent on tightly synchronized clocks, hence in case of loose synchronization of the clocks, the colluder nodes cannot be detected as accurately as in the case of the new technique which does not require a clock at all. In case of packet leashes, we also require GPS co-ordinates without which the detection of colluder nodes may not be accurate. The DELPHI method does not detect a false alarm, however the same is confirmed by the proposed technique as we send encrypted messages to confirm the existence of a wormhole attack.

4.9 Amount Of Overheads Required

The proposed technique involves the use of a modified routing table. Essentially we are enhancing the routing table to include certain metrics which were not there and which can aid in the successful and efficient detection of a wormhole. These include the provision to hold the hops and the path. Thus the overhead in this technique is the increased size of the routing table because of these additions. In case of packet leashes, we append the current position of a node and transmission time to a packet, thereby enhancing the packet size. On the receipt of the packet, the receiving node, computes the distance to the sender and analyzes the time it takes for the packet to travel the path. This increases the computational load a bit. In addition to these, synchronized clocks are required which results in extra overhead in terms of clocks and the tight and loose synchronization pose their own issues. Although the DELPHI method of wormhole detection fares better than the other techniques discussed here in terms of overheads, it still results in a large packet size in case we are covering a large network. Also extra computational resources are consumed to process and analyze the hop information at various nodes. SECTOR once again requires the overhead because it requires tightly synchronized clocks which has a double impact as firstly the overhead is incurred for acquiring the clock and then to keep it synchronized.

Table II Comparison Of New Technique Of Wormhole Detection With Existing Ones



COMPARITIVE ANALYSIS OF WORMHOLE DETECTION TECHNIQUES					
METHOD	**MOBILITY**	**FAULT TOLERANCE**	**SYNCHRONIZATION**	**RESOURCES REQUIRED**	**QOS**
Packet Leashes Technique	Bound to maximum transmission distance	Low due to synchronization requirements	Low synchronization	Large due to requirement synchronized clocks, GPS co-ordinates	Delay up to leash factor
DELPHI technique	No need	Moderate due to large packet size	Not required	Minimum as only packet size increases	Delay
SECTOR technique	No need to Time synchronization	Low due to synchronization requirements	Not required	Large as synchronization is required	No delay
Proposed new technique	No need	High	Not required	Minimum as only routing table is modified	No delay
SAW	Delay observed	Low due to maintenance of neighbor information	Not required	Medium as neighbor information is required	Not required
DAW	Not taken in consideration	Moderate but better than SAW	Not taken in consideration	Medium and better than SAW	Delay parameters
Directional antennas	Bound due to signal of antennas	Low due to signal issues	Low synchronization	High as directional antennas are required	Delay

V. Conclusion

In this paper, we have presented the implementation of a new technique which helps in detection of wormholes by modifying the routing table. The technique was successfully implemented on both the AODV and DSDV MANET routing protocols. The simulator used was Network Simulator 3. Based on the properties of these two MANET routing protocols and the results of the simulation we can conclude that the algorithm can be implemented easily on DSDV in comparison to AODV, the accuracy with which colluder nodes are detected is more in AODV as it responds better to network failures and restructuring. When it comes to detecting a wormhole, it can be inferred that it gets detected easily in case of DSDV as compared to AODV. When we talk about adaptability to changing external factors, then AODV is more suited for the suggested approach as compared to DSDV. The latter part of this paper compares the suggested approach with other approaches of wormhole detection such as packet leashes, DELPHI and SECTOR methods. It can be inferred that the proposed technique is easier to setup as compared to packet leashes as in packet leashes special hardware is required to find the GPS co-ordinates and to keep them synchronized, DELPHI method does not use specialized hardware but has the disadvantage of increased packet size as the path is long. SECTOR method uses special hardware to respond to one-bit challenge and synchronized clocks as well. The proposed approach also detects the wormholes pretty efficiently and accurately when compared to packet leashes and SECTOR method and is comparable to the DELPHI method. Also, the overheads required in case of the suggested approach are very low when compared with SECTOR, DELPHI and packet leashes methods of wormhole detection. So we can conclude that the suggested approach can be implemented effectively in other MANET routing protocols also in addition to AODV and DSDV and that it is comparable to some of the other wormhole detection techniques such packet leashes, DELPHI and SECTOR methods.

Acknowledgement

We wish to acknowledge our colleagues for contributing towards the successful preparation of this paper.

References

[1]. Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, Nov. 2008 “Analysis of wormhole Intrusion Attacks In MANETS”,IEEE Military Communications Conference,MILCOM 2008.

[2]. Yih-Chun Hu, Adrian Perrig, David B. Johnson, 2003 “Packet Leashes : A Defence against Wormhole Attacks in Wireless Networks”, Twenty-Second ANNUAL Joint Conference of IEEE Computer and Communications , pp. 267-279.

[3]. Chiu, HS; Wong Lui KS, 2006 “DELPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks”,In Proceeding of International Symposium on Wireless Pervasive Computing, pp. 6-11.

[4]. Srdjan Capkun, L.evente Buttyan, and Jean-Pierre Hubaux, 2003 “SECTOR: Secure Traking of Node Encouters in Multi-hop Wireless Networks,”In Proceedings of 1st ACM Workshop on Security of Ad hoc and Sensor Networks (ACM SANS), pp. 21-32.

[5]. Lingxuan Hu and David Evans, Feb. 2004 “Using Directional Antennas to Prevent Wormhole Attack “,In Proceedings of the Network and Distributed System Security Symposium, pp. 131-141.

[6]. M.S.Sankaran, S.Poddar, P.S. Das, S.Selvakumar “A Novel Security Model SaW: Security against Wormhole attack in Wireless Sensor Networks”, In Proceeding of International Conference on PDCN, 2009.

[7]. Khin Sandar Win “Analysis of Detecting Wormhole Attack in Wireles Sensor Networks”,World Academyof Science, Engineering and Technology, 2008,pp.422-428.

[8]. Khan, Zubair Ahmed, and M. Hasan Islam (2012), “Wormhole Attack: A new detection technique”, International Conference on Emerging Technologies (ICET), October 8-9, 2012, Islamabad.

[9]. Rutvij H. Jhaveri1, Ashish D. Patel, Jatin D. Parmar, Bhavin I. Shah (2010), "MANET Routing Protocols and Wormhole Attack against AODV",IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010.

[10]. Lazos, L.; Poovendran, R.; Meadows, C.; Syverson (2005), P.; Chang, L.W.; , "Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach," Wireless Communications and Networking Conference, 2005 IEEE , vol.2, no., pp. 1193-1199 Vol. 2, 13-17 March 2005.