An Efficient Algorithm for the Detection of Exposed and Hidden Wormhole Attack

ZUBAIR AHMED KHAN*, SAEED-UR-REHMAN*, AND MUHAMMAD HASAN ISLAM*

RECEIVED ON 09.04.2015 ACCEPTED ON 16.09.2015

ABSTRACT

MANETs (Mobile Ad Hoc Networks) are slowly integrating into our everyday lives, their most prominent uses are visible in the disaster and war struck areas where physical infrastructure is almost impossible or very hard to build. MANETs like other networks are facing the threat of malicious users and their activities. A number of attacks have been identified but the most severe of them is the wormhole attack which has the ability to succeed even in case of encrypted traffic and secure networks. Once wormhole is launched successfully, the severity increases by the fact that attackers can launch other attacks too. This paper presents a comprehensive algorithm for the detection of exposed as well as hidden wormhole attack while keeping the detection rate to maximum and at the same reducing false alarms. The algorithm does not require any extra hardware, time synchronization or any special type of nodes. The architecture consists of the combination of Routing Table, RTT (Round Trip Time) and RSSI (Received Signal Strength Indicator) for comprehensive detection of wormhole attack. The proposed technique is robust, light weight, has low resource requirements and provides real-time detection against the wormhole attack. Simulation results show that the algorithm is able to provide a higher detection rate, packet delivery ratio, negligible false alarms and is also better in terms of Ease of Implementation, Detection Accuracy/ Speed and processing overhead.

Key Words: Wormhole Attack, Wormhole, Mobile Ad Hoc Network, Routing Table, Round Trip Time, Received Signal Strength Indicator.

1. INTRODUCTION

The charms of being connected without any physical medium are the keys to success of Wireless Networks. A MANET is a network which doesn't have a prominent infrastructure and nodes are free to move from one location to another. Nodes can join and leave based upon their needs. Because of its ease of deployment MANETs are mostly deployed in disaster struck and battlefield areas. In a MANET; since there is no pre built network infrastructure; each node which needs to sends data to a faraway node must rely on all the nodes which make the path between the source and destination node. Here each node works a router too in addition to its normal function. A MANET is built on the assumption that every node is honest and will honestly full its duties of routing too; but sadly this is far from the reality. It is highly probable that nodes starts indulging in malicious activity or join the network with wrong intentions.

* Center for Advanced Studies in Engineering, Islamabad.

Similarly the routing protocols that are built for MANETs were also based on the assumption that all nodes are honest and hence the section of security was overlooked. Because of the ease of access and absence of prominent network boundaries everyone can eavesdrop on the wireless communication, and may start some malicious activity.

MANETs are vulnerable to a number of attacks. In some of the attacks more than one attacker combine/synchronize their actions to launch some attack on a network e.g. Black hole, Sybil, Wormhole etc. Some of the attacks cannot be put under one classification category and their effects are scattered across many dimensions. These attacks can be a foundation point for other severe attacks and also can launch a number of different attacks. The range of possible malicious activities is quite large; however we are focusing on one particular of attack in the area of MANETs known as the Wormhole Attack.

In this paper a new architecture is proposed which is an enhanced version of our previous work [1]. We have tried to eliminate the limitations from our previous work and also upgraded it to cover all types of the wormhole attacks. In the new algorithm there is no longer any need to pass encrypted packets for wormhole confirmation. We are now able to detect both kinds of wormhole attack i.e. Hidden as Well as exposed attack. Although our previous work has also been proved to be quite effective and better than most of the published techniques in literature by independent researchers. Gauri, et. al. [2] have taken our algorithm and implemented it in NS3 as compared to our NS2 implementation, they proved that our technique provides ease of deployment,better detection accuracy and more real-time detection.

In a wormhole attack; two far apart nodes separated by many hops; combine their actions in such a way that they appear to be one hop apart to other nodes, as in Fig. 1. Since the path passing through the malicious nodes appear to be shorter; eventually all the network traffic get diverted through this path. Now this becomes an alarming situation in which the colluder nodes are in control of the whole network traffic and have the ability to cryptanalyze (if traffic is encrypted), shape, divert, drop or selectively drop the network traffic. Because of the possible malicious activity a wormhole type structure is forbidden an ad-hoc network otherwise the colluder nodes seems to be providing a very useful service by offering a shortest path. The severity of wormhole attack increases by considering the fact that it can be launched on networks where the traffic is even encrypted. It can also be launched against each and every type of protocol with the same severity level.

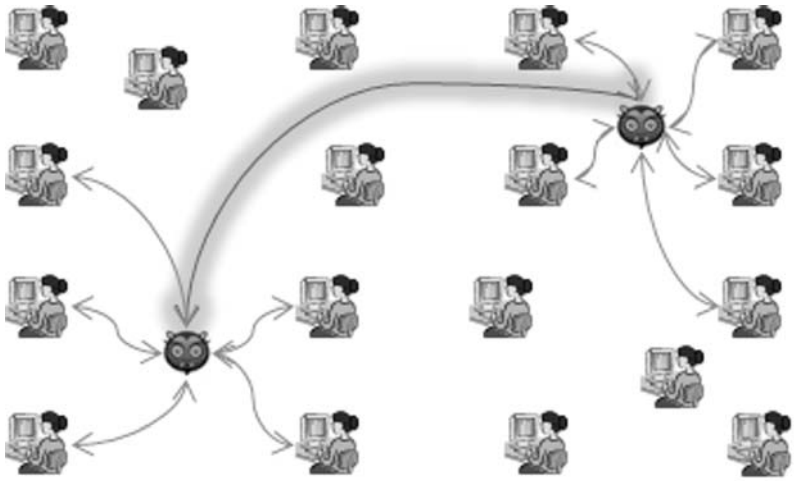

FIG. 1. WORMHOLE ATTACK

1.1 Types of Wormhole Attack

The wormhole attack can be launched in two modes, a hidden wormhole and an exposed wormhole. As the name suggests, in a hidden wormhole the attackers are not visible to normal network nodes. Whereas in an exposed wormhole attack the attackers are visible to the normal network nodes and appear in routing information. " Hidden Wormhole" nodes do not leave their trails in routing queries; instead there are other legitimate nodes which appear to be used excessively in links.

1.2 Effects of Wormhole Attack

The effects of wormhole attack have been explained in detail in our survey paper [3]. Some which are as follows but not limited to:

- Allows the attacker to:
- Gain unauthorized access,
- Disrupt routing
- Launch DoS (Denial of Service) attacks
- Launch the black hole attack (by dropping all data packets)
- Grey hole attacks (by selectively dropping data packets)
- Launch cryptanalysis Attacks
- Crack communication keys
- Degrades services at physical layer
- Surveillance/Alarm system corruption
- At the end legitimate paths cannot be found
- Some nodes might get isolated from whole network and will not be able to communicate at all.

The paper is organized as, in the first section we provide a short introduction of wormhole attack, second section covers the literature review, third introduces the concept of RSSI and RTT, fourth section explains our proposed architecture and the fifth section comprises of simulation results and future plans.

2. BACKGROUND AND RELATED WORK

The concept of Wormhole attack was introduced by Hu, et. al. [4], since then enormous amount of research has been done in the direction of mitigation the effects of wormhole attack. These efforts range across the whole possible domains i.e. from hardware based techniques to simple logic based techniques. These techniques can be called as Hardware Based (requiring new/extra hardware), Clock based (Requiring highly synchronized clocks), Packet Leashes based (Limiting packet traveling capabilities), RTT Based (Calculating Round Trip Time), TTL based (Managing Time to Live of Packets intelligently), Neighbor Based (Neighbor Collaboration) and there are a number of other detection techniques implemented also. However, most of the solutions are aimed towards only one type of the wormhole while others have some inherent types of limitations. We have listed down almost all of the proposed techniques present in literature in our survey paper [3]; therefore to reduce the size of literature section, we will be listing down only those techniques which are most relevant to our research i.e. the techniques based upon RTT and RSSI.

Following are the techniques that use the Round Trip time for the detection of wormhole attacks present along a path.

Song, et al. [5] proposed a three step based wormhole detection scheme. It is an RTT based scheme which comprises of responses comparisons from different nodes along the path.

Raju, et. al. [6] proposed an avoidance technique based upon average RTT. It is not aimed towards identification or detection of intruders.

Simsek, et. al. [7] proposed a distributed approach which considers nodes' neighbor densities and standard deviation to identify abnormality in the behavior. The algorithm can detect exposed wormhole but not the hidden wormhole.

Jain, et. al. [8] proposed a technique which monitors channel noise to identify replay and encapsulation of packets because of wormhole. This again can only detect exposed wormhole.

Upadhyay, et. al. [9] proposed a wormhole avoidance technique based upon statistical analysis. The algorithm monitors the average delay during path setup and statistics of inbound and outbound packets. Suspicious paths are blacklisted and are not used in future.

Song, et. al. [10] proposed SWAN (Statistical Wormhole Apprehension using Neighbours). The technique monitors the number of neighbours and any increase in the number of neighbours is assumed as wormhole. The technique doesn't perform detection of existing of nodes or countering the attackers.

Modirkhazeni, et. al. [11] proposed neighbour discovery technique for handling wormhole attack. They assumes the nodes are static and number of is fixed, hence any data from a node that is not in the initial neighbor list is assumed as an intruder. The technique is not much flexible in terms of addition of new nodes.

Vani and Rao [12] proposed a secure protocol for AODV which they have named WARDP. The algorithm choses link disjoint multi paths during the route discovery procedure in order to avoid wormhole. Wormhole is detected using the hop count detection. The algorithm is quite heavy in terms of memory and processing requirements.

Vijayalakshmi and Albert [13] proposed a new algorithm utilizing time based leashes (Limiting Packet Propagation Parameter LP3) and Neighbour monitoring technique (NAWA2) for prevention of wormhole. Neighbour collaboration is used to detect to colluders by monitoring the PDR (Packet Delivery Ratio) and Jitter. The approach might be good in detection of encapsulation sort of wormhole attack and may not perform well in case of other variants.

Tran, et. al. [14] proposed a new technique titled as TTM (Transmission Time based Mechanism) which also a collaborative approach based upon nodes along the path. Each node has to calculate RTT and pass along the path setup procedure. The links where the time taken is greater are identified as a wormhole link. The approach is likely to fail if higher transmission power is being used by the colluders.

Chui, et. al. [15] proposed DELPHI, Delay Per Hop Indication. Delay per hop from source to destination is observed for all paths. The approach is likely to detect only the encapsulation form of the wormhole attack. Other types (e.g. Out of Band or High transmission) of wormholes might use highly sophisticated hardware to reduce the delays. The approach only handles the detection of wormhole attack and cannot pin point the exact location of the wormhole nodes.

Capkun, et. al. [16] proposed SECTOR, The algorithm needs one-bit extra hardware for fast processing of detection (Fig. 2). This also a type of distance bounding leash algorithm. It may not need location information or tight time synchronization, it needs specialized hardware and efficient MAC handling for processing the challenge with minimal delay.

From the above review we can conclude that use of RTT alone is insufficient; since attackers might be able to use high speed links to make their delays undetected or use store and forward type of wormhole attack. In order to cater this we are proposing a technique that will combine RSSI and Routing table for the identification and detection of wormhole attack. To the best of our knowledge a technique which combines Routing Table, RTT and RSSI is not present in literature.

3. PROPOSED METHODOLOGY

As depicted in our previous work [1,3], there are not many solutions of wormhole attack present in literature which

try to handle both the hidden as well as the exposed wormhole attack. Hereby our aim is to propose a technique that can effectively detect both kinds of wormhole attacks.

The aim of our technique is to detect the wormhole attack in the easiest possible way. We are also eliminating the need of any extra hardware requirements. The proposed solution is free from fixed timing constraints or time synchronizations. We are avoiding the complex calculations of the location identification algorithms which are used for the detection of wormhole attacks. Here we are proposing a slightly modified algorithm from our previous Exposed Wormhole detection algorithm [1] to remove the requirement of encrypted traffic. However the applicability of our algorithm [1] has been verified by independent researchers [2]. They [2] have compared our algorithm to a number of other techniques and found it more lightweight, robust, low resource intensive and provides more real-time detection. We make the assumption that we have a homogeneous network in which all normal/legitimate nodes have same transmission ranges and powers. We will be detecting the wormhole by considering the following facts:

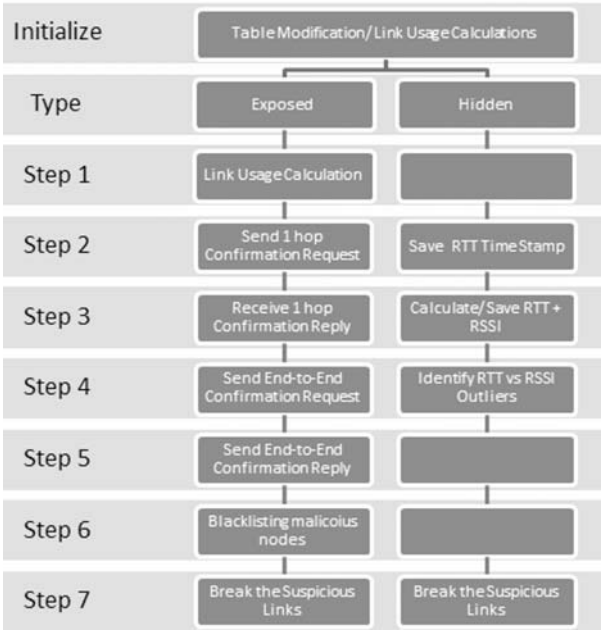

FIG. 2. MAIN BLOCKS OF DETECTION ALGORITHM

(1) A wormhole link will be present in more number of paths in the routing table of an infected node e.g. Consider Node-12 and 13 from Table 1 and Fig. 3.

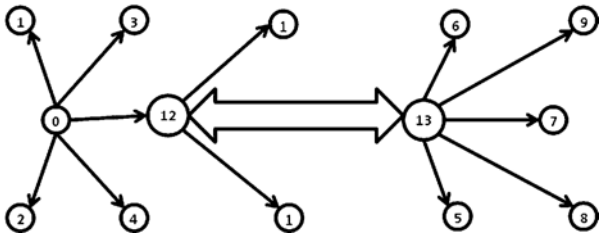

FIG. 3. EXPOSED WORMHOLE ATTACK, NODE 12 AND 13 ARE ATTACKERS WITH HIGHER TRANSMISSION POWERS

TABLE 1. ROUTING TABLE OF NODE 1 SHOWING ONLY PATHS EFFECTED BY WORMHOLE NODES (NODE-12 AND 13)

Destination	Next Hop	Metric	Sequence #	Path
0	0	1	154	->1->0
2	12	2	158	->1->12->2
5	12	3	156	->1->12->13->5
6	12	3	154	->1->12->13->6
7	12	3	154	->1->12->13->7
8	12	3	156	->1->12->13->8
9	12	3	158	->1->12->13->9
12	12	1	156	->1->12
13	12	2	154	->1->12->13

(2) The signal strength received from a wormhole node will not be of the order of a normal node. i.e. it will be higher than normal nodes.

(3) For an infected path, the Round Trip Time will be either larger than normal RTT or it will be very much lower, given the relation between the signal strength and RTT.

3.1 Detection Parameters

We are proposing a state of the art technique in which we will take into the account the RSSI and the RTT for the detection and identification of wormhole attackers.

3.1.1 Received Signal Strength Indicator

Researchers in [17-20] all uses RSSI for location estimation and/or malicious activity detection in their research. It is the voltage received by the receivers' circuit [17]. It can be said as the measured power received and which is calculated by squaring the magnitude of the received signals' strength. We can easily calculate RSSI upon the reception of data without any burden or overhead on the hardware, node energy or network bandwidth.

As the distance among the nodes increases the RSSI decreases [18], using this feature of RSSI is the main theme of our algorithm.

Given two antennas, the signal strength received is given as [19-20]:

$$P_r = P_t + G_r + G_r + 20\log_{10}\left(\frac{\lambda}{r\pi\pi}\right) \quad (1)$$

Where G_t and G_r are the antenna gains of the transmitting and receiving antennas respectively, lambda is the wavelength, and R is the distance between the antennas.

RSSI has been used in security solutions [20] for WSN, but it hasn't been used in MANET and especially for the detection of wormhole attack.

3.1.2 Round Trip Time

RTT or Round Trip Time is the measure of the time taken by a packet from a source node to a destination node and from the destination back to the source node [21]. It is the length of time it takes for a signal to be sent plus the length of time it takes for an acknowledgment of that signal to be received.

$$\mathbf{RTT} = \mathbf{T}_{receive} - \mathbf{T}_{transmit} \quad (2)$$

RTT is dependent upon data transfer rate, route delays, node delays, medium and number of hops between source and destination. RTT has also been used in a number of attack solutions in literature, but the problem with RTT is, that it is not sufficient alone for the detection of wormhole attack.

3.1.3 RSSI vs Distance between Nodes

The signal propagation model [22] states that RSSI (S_r) is related to the Sent Signal Strength (S_s) and the distance between Sender and Receiver (d_{sr}) by the equation:

$$S_r = S_s * \left(\frac{1}{d_{sr}}\right) \quad (3)$$

If S_s is kept Constant, S_r is inversely related to d_{sr}.

$$S_r \alpha \left(1/d_{sr}\right)^n \quad (4)$$

This means the greater the distance (d_{sr}) between the two nodes; the lower will be its RSSI (S_r)

Similarly, RTT of a packet is directly proportional to the distance (d_{sr}). An increase in the distance will generally mean an increase in the RTT.

$$RTT_i \alpha d_{sr} \quad (5)$$

In case of a wormhole free network if i is nearer than j, then the following two equations must hold:

$$RSSI_i - RSSI_j > \Delta_{RSSI} \quad (6)$$

$$RTT\text{-} - RTT\text{-} > \Delta_{RTT} \quad (7)$$

Where "Δ" is the error factor in calculations due to any sort of inconsistencies in the signal propagation. According to Equations (6-7), in a homogeneous network, the RTT of a one hop link will be inversely proportional to its RSSI. This means the nearer the node, the lower will be its RTT and higher RSSI, and vice versa [18].

3.2 Working of the Algorithm

Looking at the exposed wormhole attack, we can see that a malicious path is advertised (that exists between the colluder nodes), and all the normal nodes are forced to make all their routes using this malicious path. Thus, the entries in the routing tables of nodes will include entries of the malicious nodes as well.

3.2.1 Detection Methodology

Some of the routing protocols store full path from source to destination in routing tables of each node, however, for others which do not save full path, we have proposed a slight modification in the routing table that will help in the identification of malicious links [1].

The slight modification for some protocols is to store the full path from source to destination in routing table, e.g. in case of DSDV the routing table contains Sequence number, Source, Destination, Next Hop and Number of Hops only. We have to modify it to store the full path (additional field of Path) from source to destination.

The main idea here is that any link that is advertised by or consisting of the mischievous nodes will have a relatively higher usage ratio as compared to normal links e.g. Node 12 and 13 in Table 1. We are aiming to find those links for the detection of "Exposed" Wormhole attack e.g. Fig. 3. This is because in a wormhole free network it is very much unlikely for the same links to have higher usage ratio in routing tables of a node and all of its neighbors. A flow diagram shows the steps of the exposed algorithm in Fig. 4. We also assume that more than one node cannot be placed such that the same link will get a higher usage percentage for all nodes.

3.2.2 Link Usage Calculation

Whenever the routing table is updated, the algorithm gets the list of unique links along with the number of occurrences. For example, if link between some nodes (A & B) is present in "n" number of paths, its occurrence is "n".

For a link "i" its relative usage percentage ($Usage_i$) is calculated as:

$$Usage_i = \left(\frac{Occurence_i}{\sum_n Occurence} \right) \quad (6)$$

Once the usage percentage of each link is calculated, Link with abnormal usage percentage can be filtered out as:

$$\text{if } Usage_i > k * (\mathbf{max}\ (\mathbf{Usage}_j)) \Rightarrow \text{Suspicous} \quad (7)$$

Where max ($Usage_j$) represent the maximum value of link usages in the set of links excluding the link i (i.e. $Usage_i$) and "k" is fine tuning factor.

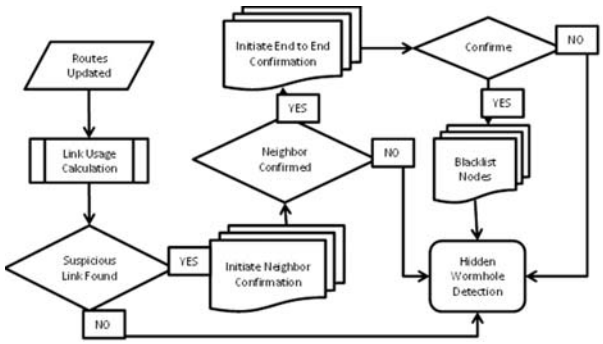

FIG. 4. FLOW OF EXPOSED WORMHOLE DETECTION

"k" is a factor that can be adjusted to fine tune the difference of percentage between normal and malicious links usage. If the percentage usage of a particular link is greater by a factor "k" from the maximum usage percentage of all other links we are suspecting a wormhole on that link. Table 2 shows link usage percentages for paths in the routing table of Node-0 in Fig. 3, usage for path from node-12 to 13 being clearly ahead of every other link.

3.2.3 RSSI Based Detection

Once a suspicious link is identified, we need to confirm whether it is a real intruder link or the geographical locations of the suspicious nodes make it look like a wormhole link. To do this confirmation we have proposed a simple yet efficient solution that involves usage of RTT and RSSI calculations.

Having made the assumption that we have all homogeneous nodes, the possibility of internal node option of wormhole is limited to only the encapsulation mode. This is because of the fact that no node will be able to create a link longer than one hop length. To create a wormhole intruders need to advertise a path that offers an improvement more than just one hop length, in that case they will need to use encapsulation in order to advertise a more attractive path.

The combination of RTT and RSSI opens up another option in the detection methodologies of wormhole attack.

TABLE 2. LINK USAGE PERCENTAGE FOR NODE 0

Link	Occurrence	Usage (%)
-> 1	1	7.14
-> 2	1	7.14
-> 12	1	7.14
-> 13	6	42.85
-> 5	1	7.14
-> 6	1	7.14
-> 7	1	7.14
-> 8	1	7.14
-> 9	1	7.14

RSSI is a feature that is available with every packet received and if used efficiently can help in detection of malicious activity [18]. It is already being used in the detection of various other wireless attacks [20]. RSSI is a ranging technology which needs little communications overhead, low implementation complexity and is also inexpensive [22].

For a link that is infected by a wormhole, Equation (6-7) will not hold. The reason behind this is that in case of an infected link RTT is being calculated for a link that in reality is not a one-hop link e.g. Node 0 to 7 in Fig. 7. This is because the existence of wormhole nodes (Node 12 and 13) will make it multi hop link and hence its RTT will increase automatically. On the other hand the RSSI for the infected link will also be higher because it will be calculated for a packet that has been received from a nearby node (Since the node (12 or 13) was not visible to normal nodes). We are utilizing this fact to identify the links that are infected by a wormhole.

In case of hidden wormhole identification only the one hop neighbor circle is enough for identification where as in case of exposed wormhole we need to calculate RTT and RSSI for the whole Path from source to destination.

3.2.4 Wormhole Confirmation

For a node (k) if the RTT of a neighbor (j) is greater than the maximum of RTT of all other neighbors; the RSSI of the neighbor (j) should be less than the minimum RSSI of all the other neighbors within an error band "Δ". "Δ" is the error factor in calculations due to any sort of inconsistencies in the signal propagation.

$$\text{If } RTT_j > \max(RTT_i)\ (i = 1\ldots\ldots n)$$

$$\Rightarrow RSSI_j < [\min(RSSI_i)] + \Delta\ (i = 1\ldots..n)$$

$$\text{If } RSSI_i > [\min(RSSI_i)] + \Delta\ (i = 1\ldots..n)$$

$$\Rightarrow \text{Wormhole Detected}$$

To have a clearer picture of the wormhole detection procedure, consider a simplified scenario, where we assume that node-12 and node-13 are the attackers in a hidden wormhole attack as in Fig. 7. Node-0 is connected to node-7 through a hidden wormhole link created by node-12 and node-13. Node-12 and node-13 are not visible to any other node in the network. Since node-12 and node 13 does not appear in the routing information, node-0 and node-7 will assume themselves as one-hop neighbors. Node-0 and node-7 will not be correct geographical neighbors but still they will be advertising one another as one-hop neighbors (due to the hidden wormhole). Therefore, normal nodes will add them to their routes because the path passing through node-0 and node-7 (and hence wormhole path) will be the shortest, resulting in higher usage ratio of link between node-0 and node-7. The block diagram of the detection procedure is given in Fig. 5.

Looking at Fig. 7, node-0 will see five normal nodes as its one-hop neighbors whereas in reality only four of them are its genuine neighbors. The challenge here is to correctly identify the path of the node which is not a genuine neighbor.

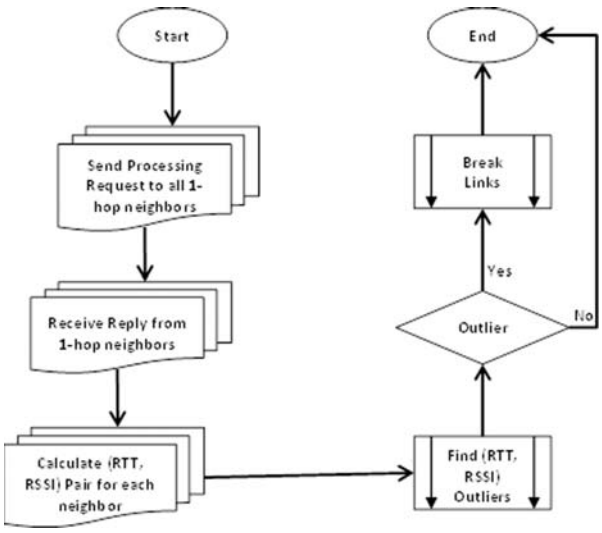

FIG. 5. FLOW OF HIDDEN WORMHOLE DETECTION

Node-0 will calculate RSSI and RTT for all of its neighbors and will store them. Now this list can be used for the detection of hidden wormhole. Each entry of the list will be evaluated according to Equation (6) and accordingly the RSSI and RTT of node-7 will not be according to the relation in Equations (6-7), because the actual communication distance between source and destination will be very small (i.e. because node-0 will be receiving traffic from a very much nearby node-12). The RSSI will be high and at the same time the RTT is also going to be quite high as compared to other neighbors of node-0. Therefore the link that points towards node-7 will be identified as a hidden wormhole infected link.

Although we have mentioned the hidden and exposed wormhole detection procedure separately, they run in tandem with one another and from code perspective there is very little separation between the two. A pseudo code of the whole system is given in Algorithm, Fig. 6 to explain the complete algorithm. A block diagram Fig. 2 shows the different blocks of the detection algorithm.

4. EXPERIMENTAL PROCEDURE AND TESTING

We have carried out the simulations using NS2 (version 2.35) network simulator. The mobility scenarios are generated by a Random way point model. The numbers of nodes tested in a terrain area of 1000x1000m are between 8 and 50. Each simulation was done for 100 seconds. Different scenarios based upon the Attraction and Strength of the wormhole were tested.

- **Attraction**: It is measure of the reduced number of hops that the wormhole offers, e.g. if a normal path may be 10 hops long and the wormhole path is only 3 hops long, then the attraction will be 7.
- **Strength**: It is the number of paths that are passing through the wormhole link.
- Based upon our simulations and their results we have identified three different kinds of nodes, because of their relation to the wormhole attack.

- **Not-Infected**: These nodes are not affected by the presence of wormhole in network
- **Infected**: These nodes are the ones that are affected directly or indirectly by the presence of wormhole in the network. We identify these nodes by the presence of infected paths in their routing tables.
- **Wormhole/Intruders/Attackers**: The goal is to identify these nodes and we have been able to detect them quite successfully in case of "Exposed Wormhole" and in case of "Hidden Wormhole" the links have been identified.

```
initialize;
while Detection is Enabled do
    if Routing table Updated then
        Calculate Link Usage;
        Identify Suspicous Links;
        if Links Identified then
            foreach one hop neighbors do
                Send 1hop Confirmation Request;
                if Reply Recieved then
                    Calculate RTT And RSSI;
                else
                    resend-request
                end
            end
            if 1hop Neighbor Confirms then
                initiate end2end confirmation;
                randomely choose nodes from other end of wormhole;
                foreach choosen node do
                    send end2end confirmation request;
                    if reply is recieved then
                        Calculate RTT And RSSI;
                        Evaluate RTT vs RSSI;
                        if RTT-RSSI Outlier then
                            Mark as wormhole;
                        else
                            False Alarm
                        end
                    else
                        Mark as wormhole
                    end
                end
            else
                False Alarm or Topology Structure
            end
        else
            Routing table is normal
        end
    else
        Do not run algorigthm
    end
end
```

FIG. 6. PSUEDOCODE OF PROPOSED ALGORITHM

Since NS2 doesn't allow nodes with different transmission ranges. We had to customize NS2(2.35) to accommodate the special type of wormhole nodes that are able communicate over a larger distance (1000m) as compared to the normal (250m) of the normal NS2 nodes.

First we conducted experiments to calculate the RTT and RSSI individually with and without wormhole attack to verify the validity of our proposal.

For the RTT we created two nodes that were directly connected to one another and calculated the RTT for a simple packet transfer. The Average RTT for normal nodes was found to be around 4.5 milliseconds. Then we introduced two hidden wormhole nodes in between them and calculated the average RTT. As expected now the average RTT was a lot higher and found to be in multiples of the average RTT of normal one hop.

In real scenarios the RSSI may not be uniform in all directions because of the differences in interferences in the different directions. However NS2 doesn't take into account these interferences and hence the RSSI part was straight forward, the RSSI received at the receiver end was of the order of the senders' transmission power and its distance. If the node was a normal NS2 node, its RSSI at the receiver was lower and was higher for the customized nodes with higher transmission power.

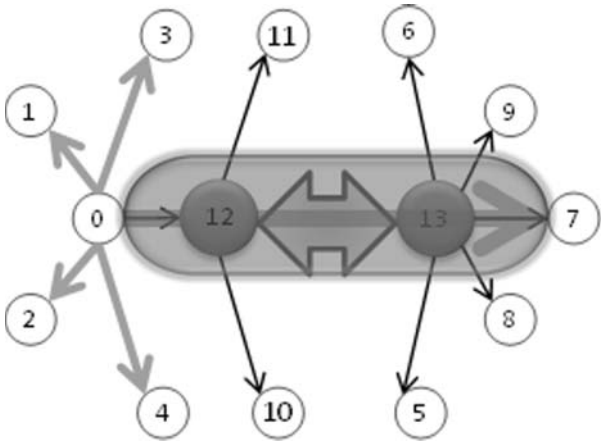

FIG. 7. HIDDEN WORMHOLE ATTACK, NODE 12 AND 13 ARE HIDDEN WORMHOLE NODES

4.1 Results

Two nodes were set up as malicious nodes by making their transmission power higher, this way they were able to communicate with one another from a longer distance. Attackers were placed at different locations making their strength and attraction different. The algorithm was able to detect the wormhole attack 99% of the time, because of the two fold detection architecture the False Alarms were reduced to almost 1% with the exceptions occurring whenever the physical location of nodes or attackers make them hard to detect. It was observed that the detection will increase with the increase in the attraction of the wormhole. PDR of the network was monitored in the following scenarios.

- Under no wormhole attack
- Under the influence of Wormhole attack
- After the Wormhole Attack mitigation

PDR was higher in case-1 since every node was acting normally and the only drops were caused by congestion or other network scenarios. Where as in case-2 PDR will drop significantly depending upon the strength/attraction of the wormhole, Table 3 and Fig. 9.

PDR as calculated by sending a fixed number of packets from source to destination. Averages were calculated and it was found that PDR was around 98% in cases where there was no wormhole present in the network, it will drop up to 50% on average once wormhole attack is introduced. After deployment of the detection algorithm the PDR will again rise up to around 90% proving the effectiveness of the proposed architecture. Table 4 and Graph in Fig. 9 shows the PDR for different cases.

4.2 Theoretical Comparison

The proposed architecture offers the following improvements over the other techniques published in literature. We have analytically compared our algorithm with some others from the literature, however a comparison of the results may not seem logical in the sense that the testing environment and scenarios are taken differently by each author. An algorithm executed in one

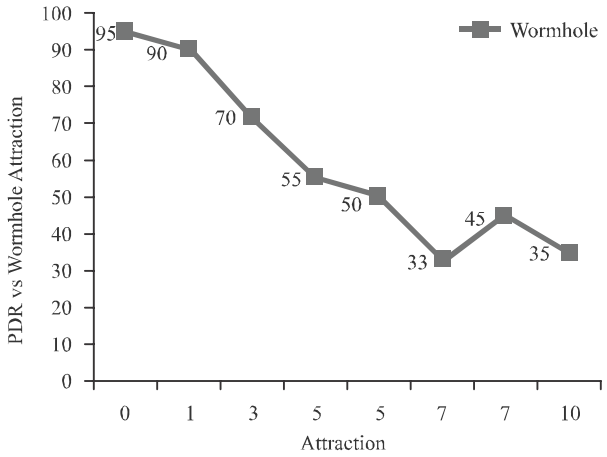

FIG. 8. SEVERITY OF WORMHOLE ATTACK ACCORDING TO ITS ATTRACTION, PACKET DELIVERY RATIO WILL DROP WITH INCREASE OF WORMHOLE ATTRACTION AND STRENGTH

TABLE 3. EFFECTIVENESS OF WORMHOLE ON PACKET DELIVERY RATIO ACCORDING TO DIFFERENT ATTRACTIONS AND STRENGTH OF THE WORMHOLE

Wormhole Path	Attraction	Sent	Received	PDR
3	7	1000	330	33
5	5	1000	500	50
8	7	1000	600	60
5	10	1000	350	35
3	5	1000	500	50
5	3	1000	720	72
	Average	1000	500	50

environment may produce completely different results in the environment built by another author. The proposed architecture has the ability of detecting both hidden and exposed wormhole as compared to single attack type detection strategy in most of the existing solutions. It has been proved [2] that our approach is better in terms of the following parameters than most of the approaches present in literature. Moreover the approach does not need any extra hardware, tightly or loosely synchronized clocks or finding location of nodes. Following are the parameters that have been taken into consideration for the analytical comparison.

- Ease of Implementation,
- Detection Accuracy
- Minimal overhead and
- Detection Speed

4.2.1 Ease of Implementation

This parameters takes into consideration the amount of effort or the Hardware required to get our technique into action. The proposed technique only requires addition of an extra column in the routing table that will contain full path from source to destination. In [12] there is a need for the GPS Hardware in order to be able to find the coordinates of each node. In [4] we may need extra hardware/software for the tightly synchronized clocks to limit the packet traveling ability for the time based leashes. In case of distance based leashes we may need GPS Hardware. In [15] the packet size may extraneously increase for lengthy paths. In [16] we need customized hardware for the processing of their challenge response detection scheme, in addition there is also a requirement of tightly synchronized clocks. From the above discussion it can be easily concluded that our proposed technique provides the most easy implementation without any extra hardware/ software or clock synchronization.

TABLE 4. COMPARISON OF PACKET DELIVERY RATIO

Attraction	Wormhole	No Wormhole	Proposed
0	95	100	100
1	90	100	95
3	72	100	90
5	55	100	90
5	50	95	85
7	33	97	85
7	45	100	90
10	35	95	85
Average	50	97.83	90

4.2.2 Detection Accuracy

The proposed technique offers the detection accuracy as compared to [4,15] which relies on the limiting the packets traveling capability and may cause legitimate packets to be dropped after the capped interval (time-based or distance-based) [15] suffers from the problem of false alarms.

4.2.3 Minimal Overhead

The proposed architecture has a minimal overhead, just the modification of routing table, the other parameters (RSSI and RTT) are already available we do not need much extra processing to calculate them. Thus we are

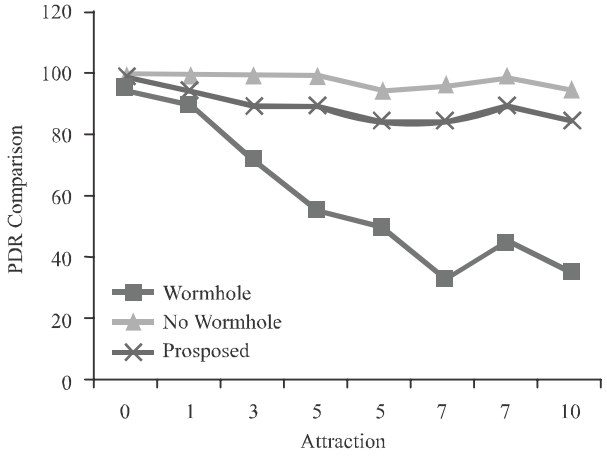

FIG. 9. COMPARISON OF PACKET DELIVERY RATIO, GREEN: THERE WAS NO WORMHOLE PRESENT IN THE NETWORK, RED: WORM ATTACK WAS LAUNCHED, BLUE: WORMHOLE ATTACK MITIGATED BY PROPOSED ALGORITHM

only increasing the size of routing table, this increased size negligible as compared to the benefit offered. The Packet Leashes suffers from the problem of increased packet overhead and extra processing requirements in terms of clock synchronization. [15] offer comparable overhead but suffers when the length of the path increases and requires overhead on all nodes along the path. [16] also has the problem of increased processing because of clock synchronization requirements.

4.2.4 Detection Speed

The proposed technique is the best of all in terms of real-time detection of the wormhole. The wormhole will be detected as soon as the attackers tries to integrate themselves into the network. on the other hand [4,15-16] are more of the type of avoidance algorithms as compared to our detection algorithm.

5. CONCLUSION

In this paper a simple and unique architecture is proposed for the detection of wormhole attack. This architecture is unique in a sense that it has the ability to detect hidden as well as exposed wormhole attack while keeping the requirements simple which does not require any extra hardware, time synchronization or any special type of nodes. The technique combines Routing Table, RTT and RSSI to make an accurate and comprehensive detection. Based upon simulations the technique has been found to be more lightweight, robust, low resource intensive and provides a real-time detection. The results obtained have also been confirmed by independent researchers who simulated our previous work in NS3 (as compared to our usage of NS2). Our algorithm achieves a high detection rate for the situations where the attackers have incorporated their entries in the routing tables of normal nodes. We are able to detect the wormhole attack as soon as the attackers try to get themselves in; long before they start to cause any damage to the system. We do not need extra hardware and neither do we need any time synchronizations; instead we are using the information that is readily available to each and every node/packet in the network. Our future work is aimed towards the monitoring of Throughput and the End-to-End delay in the network when our algorithm is in action.

ACKNOWLEDGEMENTS

Author is Ph.D. Scholar, Center for Advanced Studies in Engineering, Islamabad. This work is funded under the Indigenous 5000 Ph.D. Scholarship Programe of Higher Education Commion, Pakistan.

REFERENCES

[1] Khan, Z.A. and Islam, M.H., "Wormhole Attack: A New Detection Technique", IEEE International Conference on Emerging Technologies, pp. 1-6, 2012.

[2] Gauri, M., Singh, R.K., and Raju, M.V., "Implementation and Comparison of a New Wormhole Detection Technique with Existing Techniques", International Journal of Futuristic Science Engineering & Technology, Volume 2-4, pp. 266-273, 2013.

[3] Khan, Z.A., Rehman, S.U., and Islam, M.H., "An Analytical Survey of State of the Art Wormhole Detection and Prevention Techniques", International Journal of Science & Engineering Research, Volume 4-6, pp. 1723-1731, 2013.

[4] Hu, Y.C., Perrig, A., and Johnson, D.B., "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", IEEE 22nd Annual Joint Conference on Computer and Communications, IEEE Societies, Volume 3, pp. 1976-1986, Italy, 2013.

[5] Song, S., Wu, H., and Choi, B.Y., "Statistical Wormhole Detection for Mobile Sensor Networks", IEEE 4th International Conference on Ubiquitous and Future Networks, Volume 1, pp. 322-327, Thailand, 2012.

[6] Raju, V.K., and Kumar, K.V., "A Simple and Efficient Mechanism to Detect and Avoid Wormhole Attacks In Mobile Ad Hoc Networks", IEEE International Conference on Computing Sciences, Volume 1, pp. 271-275, Omaha, 2012.

[7] Simsek, O., and Levi, A., "A Distributed Scheme to Detect Wormhole Attacks in Mobile Wireless Sensor Networks", Computer and Information Sciences-II, pp. 157-163, Springer, 2012.

[8] Jain, S., and Baras, J.S., "Preventing Wormhole Attacks using Physical Layer Authentication", IEEE Conference on Wireless Communications and Networking, pp. 2712—2717, 2012.

[9] Upadhyay, S., and Chaurasia, B.K., "Detecting and Avoiding Wormhole Attack in MANET Using Statistical Analysis Approach", Advances in Computer Science and Information Technology, Networks and Communications, pp. 402-408, Springer, 2012.

[10] Song, S., Wu, H., and Choi, B.Y., "Statistical Wormhole Detection for Mobile Sensor Networks", IEEE 4th International Conference on Ubiquitous and Future Networks, Volume 1, pp. 322-327, Thailand, 2012.

[11] Modirkhazeni, A., Aghamahmoodi, S., and Niknejad, N., "Distributed Approach to Mitigate Wormhole Attack in Wireless Sensor Networks", IEEE 7th International Conference on Networked Computing, pp. 122-128, 2011.

[12] Vani, A., and Rao, D.S., "A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing In Ad Hoc Wireless Networks", International Journal on Computer Science & Engineering, Volume 3, No. 6, pp. 2377-2384, 2011.

[13] Vijayalakshmi, S., and Albert, R.S., "Weeding Wormhole Attack in MANET Multicast Routing Using Two Novel Techniques-LP3 and NAWA2", International Journal of Computer Applications, Volume 16, No. 7, pp. 26-33, 2011.

[14] Tran, P.V., Hung, Y.-K.L., Lee, S., and Lee, H., "Ttm: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-Hoc Networks", 4th IEEE Conference on Consumer Communications and Networking, pp. 593-598, 2007.

[15] Chiu, H.S., and Lui, K.-S. , "DELPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks", Proceeding of International Symposium on Wireless Pervasive Computing, pp. 1-1, 2006.

[16] Capkun, S., Buttyán, L., and Hubaux, J.-P. , "SECTOR: Secure Traking of Node Encouters in Multi-Hop Wireless Networks", 1st ACM Workshop on Security of Ad hoc and Sensor Networks, pp. 21-32, 2003.

[17] Masiero, R., Rossi, M., and Woods, J.C. , "RSSI Based Tracking Algorithms for Wireless Sensor Networks: Theoretical Aspects And Performance Evaluation", Ph.D. Thesis, Corso di Laurea Specialistica in Ingegneria delle Telecomunicazioni, 2007.

[18] Hussain, S., and Rahman, M.S., "Using Received Signal Strength Indicator to Detect Node Replacement and Replication Attacks in Wireless Sensor Networks", International Society for Optics and Photonics, SPIE Defense, Security, and Sensing, pp. 73440G-73440G, 2009.

[19] Papamanthou, C., Preparata, F.P., and Tamassia, R., "Algorithms for Location Estimation Based on Rssi Sampling", Algorithmic Aspects of Wireless Sensor Networks, pp. 72-86, Springer, 2008.

[20] Guoqiang, Y., Weijun, D., Chao, M., and Liang, H., "RSSI Vector Attack Detection Method for Wireless Sensor Networks", IEEE 3rd International Conference on Communication Software and Networks, pp. 229-232, 2011.

[21] Peraz, D.L., and Klepal, M., "Measuring Round Trip Times for Distance Estimation Between WLAN Nodes", , Cork Institute of technology, Ireland, Technical Report, Ireland, 2006.

[22] Xu, J., Liu, W., Lang, F., Zhang, Y., and Wang, C., "Distance Measurement Model Based on RSSI in WSN", Scientific Research Publishing, Wireless Sensor Network, Volume 2, pp. 606, 2010.