CHAPTER 5

DESIGNING OF DISTRIBUTED TECHNIQUES FOR DETECTING THE WORMHOLE ATTACKS

In this chapter, two techniques for the detection of wormhole attacks are proposed. In the first stage, wormholes can be prevented by measuring round-trip travel time of a message and its acknowledgement. In the second stage, by comparing the average number of neighbors with the neighboring number of nodes, the wormhole can be detected. Simulation results shows that the proposed detection techniques can provide improved packet delivery ratio with less packet drops.

5.1 Introduction

In wireless LAN networks, a wormhole attack causes two or more malicious nodes to collide and creates a higher level virtual tunnel in the network, which is employed to transport packets between the tunnel end points. A wormhole attack is considered dangerous as it is independent of MAC layer protocols and immune to cryptographic techniques. Wireless local area networks (WLANs) have many possible disturbing threats. The security issues which affect the WLAN are misconfigured wireless access points (WAPs) to session hijacking in Denial of Service (DoS). Other than the TCP/IP based attacks which are related to the wired networks, a few particular threats in the wide array of 802.11 affect the wireless networks. For protecting and detecting these possible threats, an
An intrusion detection system (IDS) must be used by the WLANs. IDS solution is also important for the organizations which do not have a WLAN due to the dangerous wireless threats [54].

A misbehaving WAP is introduced into the WLAN coverage area which attacks and collects the sensitive data from the WLAN. Even the users introduce the misbehaving nodes. WLANs can be improved well on combining the advantages of the low cost and easy implementation along with the flexibility. A backdoor can be created into the network by installing a WAP on a recognized LAN undermining all the hardwired security solutions and give the network open to the hackers [95]. Many ad hoc network routing protocols and location-based wireless security systems are affected by the wormhole attack. The existing ad hoc network routing protocols can’t be able to find routes longer than one or two hops if there is no mechanism for defending wormhole attacks which disrupts communication severely [66].

Wormhole helps in the networking services, as it simply presents a long network path to the link layer and upper layer, the attacker may use this link for attacking. The data flow is disrupted by selectively dropping or modifying data packets, generating unnecessary routing activities by turning off the wormhole link periodically, when the attacker attracts a lot of data traffic through the wormhole. The attacker records the traffic for later analysis. An attacker can also break any protocol which relies on geographic proximity directly or indirectly, with the use of wormholes [92, 99].
5.2 Wormhole attack

Wormhole attacker designs a tunnel which makes use of the encapsulation and de-capsulation to create a false route between illegal nodes [92]. Wormhole is created in the following three ways in the ad hoc networks: Tunneling of packets above the network layer, Long-range tunnel using high power transmitters, Tunnel creation via external wired infrastructure [99]. Attacker with limited resources and no cryptographic material is enabled by the wormhole attack to disrupt wireless networks. In wormhole attack, packets are recorded at one location in the network by an attacker; they are tunneled into another location, and retransmitted into the network. Also, many vicious nodes create higher level virtual tunnel in the network which are used for transporting packets between the tunnel end points. These tunnels try to appear like the shorter links in the network. Even though there is authenticated communication and also if the attacker has not compromised any hosts, there is a possibility of the wormhole attack. Wormhole attack is not affected by cryptographic techniques and doesn’t depend upon the MAC layer protocols and so it is considered hazardous.

A distributed wormhole detection technique can provide the approximate location of a wormhole and gives useful information about the defense techniques. The packets do not travel above the radio transmission range due to the ‘Packet leashes’ technique [31]. First we have to find out the round-trip travel time of a message and its acknowledgement, the distance between the nodes based on this
travel time is estimated. We need to verify whether the calculated distance is within the maximum possible communication range.

5.3. Related work

The numbers of researcher have worked on wormhole detection and prevention. Some of the researchers have designed defence architecture based on physical and MAC layer, some on routing.

5.4.1 Physical and MAC layer based:

Wassim Znaidi, Marine Minier and Jean-Philippe Babau [104] have proposed an algorithm for detecting and thus defending against wormhole attacks in wireless multihop networks. This algorithm uses only local and neighborhood information without requiring clock synchronization, location information or dedicated hardware. Moreover, the algorithm is independent of wireless communication models. Note that a wormhole link could only be detected if the real distance between the two wormhole nodes is greater than 4-hop due to the computed coefficients. This does not represent a real restriction because the longer the wormhole link is the more efficient it is.

5.4.2 MAC layer based:

Yurong Xu, Guanling Chen, James Ford, Fillia Makedon [110 ] have proposed a distributed wormhole detection algorithm called Wormhole Geographic Distributed Detection (WGDD) that is based on detecting network disorder caused by the existence of a wormhole. Since wormhole attacks are passive, this
algorithm uses a hop-counting technique as a probe procedure to detect wormhole attacks, then reconstructs local maps in each node. After that, it uses a feature called “diameter” to detect abnormalities caused by wormholes. The main advantage of using a distributed wormhole detection algorithm is that such an algorithm can provide the approximate location of a wormhole, which may be useful information for further defense mechanisms.

Khin Sandar Win [63] had addressed the various solutions available for wormhole attack in wireless Ad hoc and sensor networks. More specifically, they addressed algorithms used in the DaW security model that incorporates a detection and defense mechanism against the wormhole attack. The performance of DaW in terms of precision of alarms, amount of false positive has been found to be good. The alarms were found to be more precise than LF analysis. The performance of secure in multi hop wireless systems with the help of ns-2 simulations and our routing protocol can efficiently defend against the wormhole attack and achieve low delay. The links which are close to the wormhole tend to have high link frequencies. All these links also become suspicious. Suppose these links contain the wormhole node in them, SaW might falsely detect these links as a wormhole connection as the wormhole will have a low trust value.

Yih-Chun Hu, Adrian Perrig, David B. Johnson, [106] have proposed a particularly challenging attack to defend against, which is called a wormhole attack, and we present a new, general mechanism for detecting and thus defending against wormhole attacks. In this attack, an attacker records a packets, or individual bits from a packet, at one location in the network, tunnels the packet
(possibly selectively) to another location, and replays it there. We introduce the
general mechanism of packet leashes to detect wormhole attacks, and we present
two types of leashes: geographic leashes and temporal leashes. Finally, we
design an efficient authentication protocol, called TIK, for use with temporal leashes
[35].

Geographic leashes are less efficient than temporal leashes, since they require
broadcast authentication, but they can be used in networks where precise time
synchronization is not easily achievable.

He Ronghui, Ma Guoqing, Wang Chunlei, and Fang Lan [42] have introduced an
easy and effective method to detect and locate wormholes. The basic idea is to
take advantage of the known locations of beacon nodes which originally are used
in location discovery in WSNs. A hop counting technique is employed to make
every beacon node know its hop distance to the other beacon nodes as well as the
coordinates of them. Since some hop distances may be remarkably decreased by a
wormhole link, while the corresponding straight line distances calculated by the
coordinates are unaffected. The algorithm also provides an approximate location
of a wormhole, which can assist in implementing defense mechanisms. Another
advantage of our algorithm is that it can deal with multiple wormholes.

5.4.3 Routing tree Based:

Rouba El Kaissi, Ayman Kayssi, Ali Chehab and Zaher Dawy [92] have
presented a new protocol called DAWWSEN that incorporates a detection and
defense mechanism against the wormhole attack, a powerful attack that has
serious consequences on sensor routing protocols. A great advantage of DAWSEN is that it doesn’t require any geographical information about the sensor nodes, and doesn’t take the time stamp of the packet as an approach for detecting a wormhole attack, which is very important for the resource constrained nature of the sensor nodes. In future work, some modifications can be introduced to our routing protocol in order to get a balanced tree where the load would be fairly distributed among the nodes since this will considerably help in reducing the value of Trefresh.

V.S. Shankar [101] have developed an effective method called Wormhole Attack Prevention (WAP) without using specialized hardware. The WAP not only detects the fake route but also adopts preventive measures against action wormhole nodes from reappearing during the route discovery phase. They proposed an efficient algorithm based on Dynamic Source Routing (DSR) protocol. The advantage of this algorithm is that it does not require the location information of time synchronization. Their future work is to study false positive problems with regard to the detection of wormholes and a mechanism to solve such problems and also to apply the WAP algorithm to other on-demand routing protocols.

Tran Van Phuong et al [103] have proposed a transmission time based mechanism (TTM) to detect wormhole attacks – one of the most popular and serious attacks in Wireless Ad Hoc Networks. TTM detects wormhole attacks during route setup procedure by computing transmission time between every two successive nodes along the established path. Wormhole is identified base on the
fact that transmission time between two fake neighbors created by wormhole is considerably higher than that between two real neighbors which are within radio range of each other. Their future work is to extend the mechanism to work in other routing protocols such as DSDV and DSR.

V.S. Shankar Sriram et al [101] have presented taxonomy for possible wormhole attack using an Infrastructure based wireless Architecture. They had presented a mechanism that incorporates a detection strategy. The fundamental mechanism used is Neighbor Discovery and Link Verification that monitors traffic in and out of its neighboring AP and uses a data structure of first and second-hop neighbors. Their mechanism reduces the threat of wormhole attacks and requires no clock synchronization and location information. Their future work is to overcome some more sophisticated wormholes using Mobile agents.

5.4. Proposed Distributed Defense Techniques

Here two techniques for defending the wormhole attack between the nodes has been proposed (figure 5.1).

5.4.1 Technique 1: Based on RTT

The round-trip travel time i.e. RTT of a message and the distance between the nodes based on this travel time is calculated. The packets do not travel above the radio transmission range due to the ‘Packet leashes’ technique. We need to verify whether the calculated distance is within the maximum possible communication range (figure 5.2).
To calculate RTT, every node will have two time stamps values which store

- Forwarding time of the request from source to destination (RREQ) i.e. the Route request.
- Receiving time of the reply to source back i.e. Route reply (RREP).
Given all RTT values between nodes in the route and the destination, RTT between two successive nodes, say A and B, can be calculated as follows:

\[ RTT_{A,B} = RTT_A - RTT_B \]  \hspace{1cm} .................................. (1)

Consider Figure 1.

- The route path from source to destination includes S \(\rightarrow\) N1 \(\rightarrow\) N2 \(\rightarrow\) D.
- \(TS_{REQ}(S), TS_{REQ}(N1), TS_{REQ}(N2)\) are the time stamps which denote the time taken by the nodes S, N1, and N2 to forward RREQ to D. And \(TS_{REP}(D), TS_{REP}(N2), TS_{REP}(N1)\) are the time stamps which denote the time taken by the nodes D, N2, and N1 to forward RREP to S (Refer Figure 5.2).
- The RTT between S, N1, N2, and D can be calculated using the formulas:
  \[ RTTS = TS_{REP}(S) - TS_{REQ}(S) \]
  \[ RTTN1 = TS_{REP}(N1) - TS_{REQ}(N1) \]
  \[ RTTN2 = TS_{REP}(N2) - TS_{REQ}(N2) \]
  \[ RTTD = TS_{REP}(D) - TS_{REQ}(D) \]  \hspace{1cm} ..................(2)
- The calculation of RTT between two successive nodes is given by,
  \[ RTT_{S,N1} = RTT_S - RTT_{N1} \]
  \[ RTT_{N1,N2} = RTT_{N1} - RTT_{N2} \]
  \[ RTT_{N2,D} = RTT_{N2} - RTT_D \]  \hspace{1cm} ..................(3)
After calculating the values, if there is a wormhole line between two nodes, the RTT value may considerably higher than other successive RTT values and suspected that there may be a wormhole link between these two nodes.

\[ \text{RTT}_{N1,N2} > \text{RTT}_{S,N1} \text{ and } \text{RTT}_{N2,D} \]

Then, we can assume that there is a wormhole link between N1 and N2.

5.4.2. Technique -2: Based on Neighbors

In this stage, detection of wormhole is based on the fact that by introducing new links into the network, the attacker increases the number of neighbors (nn) of the nodes within its radius. So it needs to check the neighboring number of these two nodes to estimate average number of neighbors NOnh, which is given as

\[ N_{Onh} = \frac{(n-1)\pi r^2}{P} \]  

(4)

where,

- P is the area of the region,
- n is the number of nodes in that region
- r is the common transmission radius.

If the RTT value between two nodes is considerably greater than for other links, it needs to check the value of nn for those two nodes. If also the nn value for the nodes is higher than the average neighbor number NOnh, there is a suspect that a wormhole link is between the two nodes.
(ie) If \( nn > NO_{nh} \), we can say that wormhole is detected between the two nodes.

By combining these two techniques, we can pinpoint the location of the wormhole attack.

5.5. Simulation Results

In order to test the protocol, the NS2 simulator is used. The proposed distributed detection technique is compared with the normal wormhole attack scenario without applying any detection techniques in terms of different performance metrics like received bandwidth, packets dropped, packets received and packet delivery ratio.

5.5.1 Simulation results of Technique -1

In the first experiment, the performance of first technique is tested and measure by the above metrics.

![Figure 5.3: Attack Rate vs Delivery Ratio of Technique- 1](image)
Figure 5.4: Attack Period vs Packets Dropped of Technique-1

Figure 5.5: Attack Period vs Packets Received of Technique-1

Figure 5.6: Attack Period vs Bandwidth Received of Technique-1
The Figure 5.3 shows the rate vs delivery ratio of Technique 1. Figure 5.4 shows the packets dropped in the both cases. As it can be observed from the figure, the packet drop is significantly reduced in case of our distributed defense technique. Since the packet drop is less, the packets received and bandwidth received both are high in proposed technique when compared to the normal case, which can be seen from figure 5.5 and figure 5.6, respectively. As it can be seen from the figure 5.3, the packet delivery ratio is also high in the proposed technique.

5.5.2 Simulated results of Technique-2

In this experiment, the performance of the second stage is tested and measures on the basis of different metrics (figure 5.7 to5.9).

![Figure 5.7: Attack Rate vs Delivery Ratio of Technique- 2](image-url)
Figure 5.8: Attack Period vs Packets Dropped of Technique- 2

Figure 5.9: Attack Period vs Bandwidth Received of Technique- 2

Figure 5.8 shows the packets dropped in the both cases. As the figure revealed that the packet drop is significantly reduced in case of the distributed defense technique. Since the packet drop is less, the bandwidth received is high in the distributed technique when compared to the normal case, which can be seen from figure 5.9. As it can be seen from the figure 5.7, the packet delivery ratio is also high in the proposed technique.
5.7 Chapter Summary

In this chapter, two distributed wormhole detection techniques for detecting the wormhole attacks were developed. The detection is done using two techniques. In the first technique, RTT value is calculated which is considered as the time difference between the node sending Route Request, RREQ, to the acknowledgement as Route Reply, RREP, from the destination). The RTT value may considerably higher than other successive RTT values, if there is a wormhole line between two nodes. In the second technique, wormhole is detected based on the fact that by introducing new links into the network graph, the opponent increases the number of neighbors of the nodes within its radius. If the neighboring number value for the nodes is higher than the average neighbor number, there is a suspect that a wormhole link exists between the two nodes. The proposed Distributed detection techniques are compared with the normal wormhole attack scenario without applying any detection technique. The simulation results show (see appendix A-1) that the Distributed Techniques are much more effective than the normal attacks scenario for detecting the Wormhole attacks in WLAN in terms of different performance metrics like received bandwidth, packets dropped, packets received and packet delivery ratio. The detection efficiency is quite high even in elongated attacks of periods up to 25 seconds and high rate up to 500kb. The investigation shows that the proposed detection techniques can provide improved packet delivery ratio with less packet drops.