Detection and Defense Strategy of Wormhole Attack in WSN

Jin Guo\(^1\,2\)\*  
1 School of Computing, Northwestern Polytechnical University, Xi’an 710072, China  
2 School of Electronic and Information Engineering, Xi’an Technological University, Xi’an 710032, Shaanxi, China  
\*Corresponding author (E-mail: guojin00881@sina.com)

Shengbing Zhang  
School of Computing, Northwestern Polytechnical University, Xi’an 710072, China

Zheng Qiu  
AeronauticalComputingTechnique Research Institute, 15th Lab, Xi’an710000, Shaanxi, China

Abstract  
Due to the limited resource of sensors and distributed network architecture, Wireless Sensor Network (WSN) is more vulnerable to wormhole attacks, which is one of the vital attacks on availability in WSN. To address this problem, a new wormhole attack defense strategy is designed via neighbor node verification and the difference value of RREQ arriving times. Under this strategy, when each normal node receives a control packet, it will monitor the packet and determine whether it comes from its normal neighbor nodes to effectively defend against the Wormhole attack. Simulation of WSN based on OMNeT++ shows that the new method can implement effective defense.

Key words: Defense Strategy, Wireless Sensor Network, Wormhole, Neighbor Node.

1. INTRODUCTION  
Wireless Sensor Network is a kind of wireless network, which is composed of numerous sensor nodes through Ad Hoc (Tilak, AbuGhazaleh and Heinzelman, 2002). At the same time, sensor nodes, perceptible objects and observers are the three basic elements of WSN. With the development of the wireless and manufacturing technology, wireless sensor networks can be applied in many fields to monitor and control the physical world (Gajbhiye and Mahajan, 2008). In other words, WSN is becoming more and more necessary, while the reality is that WSN normally is deployed with-little maintenance under uncontrollable circumstance, which will unavoidably pose more security challenges to WSN, such as information disclosure, DOS, information tampering, black hole attack, wormhole attack, etc. Making sure the authenticity and the reliability of data has become a very important research subject in WSN area. Due to the limited resource of sensors and distributed network architecture, WSN is more vulnerable to wormhole attacks. Wormhole is one of the vital attacks on availability in WSN (Triki, Rekhis and Boudriga, 2009; Li and Zeng, 2008). The wormhole attack is a really serious control attack. In the Wireless Sensor Network (WSN), malicious nodes may capture the packets and send them to other malicious nodes through special tunnels, which will damage normal functions of WSN. While mature security protocol in traditional wired and wireless ad hoc networks can’t be copied to WSN, various kinds of unique potential security attack form in WSN and their defense strategies need to be studied. It also needs to research on key technologies as encryption, authentication and security management and development security platform adapt to characteristics of WSN to further from effective security defense system (Xun, Sriram and Wen, 2010; Taejoon and Kang, 2005). This paper presents a wormhole attack defense strategy of WSN based on neighbor nodes verification and the difference value of RREQ arriving times. Simulation of WSN based on OMNeT++ shows that the new strategy can implement effective defense. The paper includes 3 sections: Section 1 is the introduction; Section 2 presents principle and damage of wormhole attack; Section 3 performs simulation analysis on the proposed strategy based on OMNeT++; Section 4 concludes the work.

2. WORMHOLE ATTACK IN WIRELESS SENSOR NETWORK

2.1. Principle of Wormhole Attack
Wormhole attack usually takes the network with defensive routing protocol as attacking object, and it is a kind of serious attack. It establishes a private tunnel between two malicious nodes. Meanwhile, attacker somewhere of the network records data packet and location information. As a consequence, through this private
tunnel theft information is transmitted to another location of network. Because malicious nodes are usually connected through private tunnel, wormhole attack also called tunnel attack.

Figure 1 shows the simple model of wormhole attack. Nodes A and B are normal nodes, M1 and M2 are malicious nodes. Malicious node M1 intercepts packet from normal node A and sends it to another malicious node M2 through a special tunnel, and then M2 replays this packet in the WSN. This will lead normal node A and normal node B to believe that there is a short route between M1 and M2, even though it is only an illusion that malicious nodes M1 and M2 want to create. As a result of this illusion, node M1 and M2 will collect a great number of data flowing through the network to the tunnel.

![Simple model of wormhole attack](image)

**Figure 1.** Simple model of wormhole attack

### 2.2. Damage of Wormhole Attack

Wormhole attack is usually connected with high-speed communication tunnels, so superficially if the special tunnel can be used properly it will be a very efficient network connection, rather than only damages for the network. However, damaging the data of network, such as information tampering and selective transferring, is no exceptional the final goal of wormhole attacks. At the same time, illusional short route through private tunnel will disturb routing scheme and possibly lead to the failure of route discovery. It is not allowed to ignore all of these damages caused by wormhole attack. It should be noted that Wormhole attack does not need to crack encryption key of the network or capturing legal node, so it has more damage.

### 3. Defense Wormhole Attack

#### 3.1. Basic Idea of Defense Wormhole Attack

Aiming at characteristics of Wormhole attack, the paper presents a new wormhole attack defense strategy of WSN, and takes AODV protocol as an example to illustrate the new strategy.

Figure 2 and Figure 3 show the principles of RREQ broadcast and RREP single cast respectively. In AODV protocol, we are well known that as long as there is RREQ from sending node A arriving at the receiving node B, node B will send the RREP data packet in a completely opposite routing path compared with RREQ coming. At the same time, receiving node B will discard all of following RREQ (Li, 2015). However, the first arriving RREQ possibly is managed by malicious node. The reason is that wormhole attack usually through establishing a shortcut routing path, named tunnel, to attract a great number of data flowing through the network to the tunnel. So the first arriving RREQ may possibly be transmitted through tunnel, while we know that all nodes in AODV protocol do not specify whether control packets come from their normal neighbor nodes in case of processing routing request RREQ, routing response RREP, routing acknowledgement RREP ACK and routing error RERR (Wen, Ke and Wade, 2006; AlSakib and Hyung, 2006). Suppose all normal nodes firstly do verify these receiving packets, they can determine whether packets come from their normal neighbors to avoid adverse effect of Wormhole replayed routing control packets from nodes outside hops on AODV routing selection, so as to avoid Wormhole effectively.

#### 3.2. Defense Strategy of This Paper

On the basis of above analysis, we should make the following assumptions to effectively conduct the defense strategy based on neighbor node verification:

Firstly, All normal nodes need to record their neighbor nodes in the early period of network deployment; Secondly, in the network deployment process, before each normal node finds and records all its normal neighbor
nodes through broadcasting HELLO routing control packets, Wormhole node has not complete deployment; Thirdly, in the early period of network deployment, each normal node needs to record its neighbor nodes; In the network deployment process, before each normal node finds and records all its normal neighbor nodes through broadcasting HELLO routing control packets, Wormhole node has not complete deployment; Finally, the strategy is just designed to apply in static WSN, which means there are no mobile nodes in the network.

![Figure 2. RREQ broadcast](image1)

![Figure 3. RREP single cast](image2)

Each normal node broadcasts HELLO message in the early period of network deployment. After each node received HELLO message from neighbor nodes, it will establish neighbor node table. Each item records related information of this neighbor node, such as MAC and build routing table. Each routing table item takes neighbor node as a target node. It also records other routing information as Sequence Number, hop count and others. In the routing query phase, when each node sends or forwards control packets as RREQ, RREP, RREP_ACK and RERR as well as DATA, it needs to add information into the packet that can characterize its identity, such as MAC.

After each node received control packets and data packets from normal nodes or malicious nodes, it firstly extracts characterization information carried in the packet to determine where these packets come from. At the same time, it compares the characterization information with record information in the neighbor nodes table to determine whether these packets come from its neighbor node. If so, conduct appropriate processing, otherwise discard these packets(Li, 2016).

Obviously, above defense strategy based on neighbor node verification can only be applied in static WSN, which means mobile nodes are not permitted in the network. As a result, defense strategy based on neighbor node verification can’t run well alone. Aiming at this problem the paper also introduces the improving strategy into AODV protocol to adapt dynamic WSN. The improving strategy includes:

Above all, When the first RREQ packet from sending node A arriving at the receiving node B, record the first RREQ relative arriving time and hop number and save the RREQ data packet directly; Furthermore, when the second RREQ from sending node A arriving at the receiving node B, do not discard the second RREQ immediately but record the second RREQ arriving time and hop number; Last but not least, compare the arriving time and hop number of first RREQ and second RREQ then choose one routing path to transmit RREP data packet.

Figure 4 shows the main routing process described above.
It is well known that wormhole attack attracts more and more data flowing through powerful ability of computation and long distance communication. As a result, when transmitting same data packet malicious nodes will take much less time than normal nodes. On this basis, we mainly use the virtue of parameters T and t to choose the routing path, following is the detailed description of how to get the value of parameters T and t, also how to choose the routing path according to T and t.

\[ \theta = \theta_2 - \theta_1 \] (1)

\[ \eta \approx \frac{1}{n} \sum_{i=1}^{n} \sum_{j=0}^{m} \delta_{ij} \] (2)

Where \( \theta \) is the hop difference of two routing path, RREQ1 and RREQ2, \( \theta_1 \) is the hop number of RREQ1, \( \theta_2 \) is the hop number of RREQ2, \( n \) is the total number of sensor node in WSN, \( i \) is the node number, \( j \) is the difference of hop, \( \delta_{ij} \) is the possibility of node i when the hop difference is j. Because when the hop of first arriving RREQ packet is obviously smaller than the second arriving RREQ packet’s, we believe that the first RREQ packet has been transferred by malicious nodes, so from equation (1) and (2) we can conclude that when \( \theta \geq \eta \) routing path of RREQ2 will be chosen to transmit data packet.

\[ T = \frac{T_2 - T_1}{\theta} \] (3)

\[ t = \frac{\sum_{k=1}^{r} T_k}{\sum_{k=1}^{r} S_k} \] (4)

Where \( T_1 \) is the arriving time of RREQ1, \( T_2 \) is the arriving time of RREQ2, \( T_k \) is the time of one requesting link, \( S_k \) is the hop number of the requesting link. When \( T \) is obviously larger than t, we believe that the first RREQ (named RREQ1) packet has been transferred through malicious nodes.
4. SIMULATION AND EVALUATION

4.1. Topology of WSN in This Paper

With NED language of OMNeT++, we can build each node in WSN. Organize all nodes to form the topology of WSN such as Fig. 4 showed. Among them, node1 is the base station of WSN, which is responsible for connecting WSN and internet to achieve communication protocol transformation among two protocols. It releases listening task of management node and forward data from inside WSN to external network. Node1to node7 are ordinary sensor node, which is responsible for collecting environment data and forwarding various control information as well as data information. Data collected by each node was gathered to node1 through certain routing. The node wormhole A and wormhole B are two malicious nodes deployed in the WSN topology. The node wormhole A was deployed near node2 to listen and forward control packets as RREQ, RREP and data packets. The node wormhole B was deployed near node7 to listen and forward control packets as RREQ, RREP and data packets.

![Figure 5. Malicious nodes in WSN topology](image)

4.2. Simulation and Performance Analysis

Modifying AODV protocol according to above defense algorithm and conducting simulation in OMNeT++, we can clearly see the defense effect from Table.1 and Table.2.

In the simulation process, the data sent by node1 and received by node7 were recorded as shown in Table.1 and Table.2. Through the comparison of these two tables, we conclude that node7 can accurately receive all integers sent by node1. That is the designed attack on DATA packet in wormhole node fails to work. That is to say, the new wormhole attack defense strategy of WSN based on neighbor nodes verification and the difference value of RREQ arriving times presented in this paper implement effective defense.

**Table 1. Data Sent of Node1**

<table>
<thead>
<tr>
<th>Sent Time (s)</th>
<th>Data (integer value)</th>
<th>Sent Time (s)</th>
<th>Data (integer value)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.184236</td>
<td>0</td>
<td>5.549536</td>
<td>8</td>
</tr>
<tr>
<td>3.305467</td>
<td>1</td>
<td>5.736784</td>
<td>9</td>
</tr>
<tr>
<td>3.659432</td>
<td>2</td>
<td>5.898798</td>
<td>10</td>
</tr>
<tr>
<td>4.082735</td>
<td>3</td>
<td>6.017586</td>
<td>11</td>
</tr>
<tr>
<td>4.316977</td>
<td>4</td>
<td>6.199878</td>
<td>12</td>
</tr>
<tr>
<td>4.567945</td>
<td>5</td>
<td>6.312463</td>
<td>13</td>
</tr>
<tr>
<td>4.976982</td>
<td>6</td>
<td>6.625893</td>
<td>14</td>
</tr>
<tr>
<td>5.217985</td>
<td>7</td>
<td>6.847684</td>
<td>15</td>
</tr>
</tbody>
</table>
Table 2. Data Received of Node7

<table>
<thead>
<tr>
<th>Sent Time (s)</th>
<th>Received Time (s)</th>
<th>Data (integer value)</th>
<th>Sent Time (s)</th>
<th>Received Time (s)</th>
<th>Data (integer value)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.184236</td>
<td>3.255214</td>
<td>0</td>
<td>5.549536</td>
<td>5.642984</td>
<td>8</td>
</tr>
<tr>
<td>3.305467</td>
<td>3.371403</td>
<td>1</td>
<td>5.736784</td>
<td>5.824582</td>
<td>9</td>
</tr>
<tr>
<td>3.659432</td>
<td>3.725368</td>
<td>2</td>
<td>5.898798</td>
<td>5.966782</td>
<td>10</td>
</tr>
<tr>
<td>4.082735</td>
<td>4.148671</td>
<td>3</td>
<td>6.017586</td>
<td>6.110676</td>
<td>11</td>
</tr>
<tr>
<td>4.316977</td>
<td>4.382913</td>
<td>4</td>
<td>6.199878</td>
<td>6.290241</td>
<td>12</td>
</tr>
<tr>
<td>4.567945</td>
<td>4.633881</td>
<td>5</td>
<td>6.312463</td>
<td>6.380447</td>
<td>13</td>
</tr>
<tr>
<td>4.976982</td>
<td>5.057313</td>
<td>6</td>
<td>6.625893</td>
<td>6.706449</td>
<td>14</td>
</tr>
<tr>
<td>5.217985</td>
<td>5.285969</td>
<td>7</td>
<td>6.847684</td>
<td>6.915668</td>
<td>15</td>
</tr>
</tbody>
</table>

Figure 6 shows the ratio of successful detection under different hop difference value (θ). From Figure 5, we find that when the difference value of hop (θ) is much smaller, such as 3 showed in Figure 6, the ratio of successful detection is not so good. The reason is that when θ is much smaller, parameters of T and t will be much similar according to equation (3) and (4), which leads to wormhole detection more difficult. As a result, we can conclude that the new strategy presented in this paper can achieve a better detection performance when the hop difference θ is much higher.

Figure 6. Malicious nodes in WSN topology

5. CONCLUSIONS

Due to the limited resource of sensors and distributed network architecture, WSN is more vulnerable to wormhole attacks. Wormhole is one of the vital attacks on availability in WSN. In the Wireless Sensor Network (WSN), malicious nodes may capture the packets and send them to other malicious nodes through special tunnels, which will damage normal functions of WSN. Aiming at characteristics of Wormhole attack, the paper presented a novel wormhole attack defense strategy of WSN based on neighbor nodes verification and the difference value of RREQ arriving times. Simulation of WSN based on OMNeT++ shows that the new method can achieve effective wormhole defense.

REFERENCES


