Design of a Secure Communication Scheme using Channel Shifting in Wireless Sensor Networks

Bin Zeng and Lu Yao
Department of Management and Economics, Naval University of Engineering, Wuhan, Hubei, China.
Email: zbrtrueice@163.com

Abstract. One of the primary challenges to wireless sensor network is to satisfy the security needs of application since it is not practical to recover quickly once the network has been compromised. In order to improve the resilience of the network against wormhole attacks, a security scheme for wireless sensor network (WSN) has been proposed. The proposed scheme hybrids polynomial pool based key pre-distribution scheme and the availability of multiple channels on every sensor node. It allows the sensor nodes not only to establish a secure link with any other sensor node using polynomial pool-based key pre-distribution scheme but also to avoid wormhole attack by shifting from the common channel to any randomly selected channel from its available channels, and hence drifting from the frequency at which adversary is assumed to be listening to launch a wormhole attack. Results show that when almost fifty percent of neighboring sensor nodes is malicious, the probability of wormhole attack is almost zero.

1. Introduction
It is critical for sensor networks to assure security for its vulnerability to all kinds of malicious attacks. For instance, an adversary operator can provide false information by pretending a legitimate link or even mixing into sensor nodes. Wormhole attack is one of severe problem carried by an adversary who poses as a legitimate channel through building a tunnel between two end points which are usually multi-hops away. By this way, the message transmitted at one end point is relayed or routed into the malicious nodes [1]. Wormhole attack is especially dangerous because it can be launched without compromising either the host or the integrity and authenticity of the sensor network. The result of this attack is that a large number of data packets are passed through the wormhole link and it may result in side effects such as congestion, packet loss, eaves-dropping, spoofing, and so on. In fact, the adversary even can improve the performance of WSN since it provides a single hop link with high bandwidth. However in most of cases, the wormhole gives the adversary a chance to do great damage to the network since the adversary can replace other legitimate sensor nodes to communicate in the network.

Traditional cryptographic algorithms like public-key cryptography cannot be adapted to WSN since battery-operated sensor nodes have low computational power and limited memory. So symmetric key algorithms have become the tools of providing a low-cost secure communication between sensor nodes. In [2], an efficient method was devised to detect and avoid wormhole attacks using Ad hoc on demand multipath distance vector protocol (AOMDV). The only problem is that the wormhole detection process is very slow and it takes too much time before declaring a part of network under wormhole attack. An anti-wormhole attack solution by detecting different route paths between nodes was proposed in [3]. Another solution was also proposed to defend wormhole attack where multiple frequencies were used [4], but in that case, static nodes do not transmit the data to the base station.
directly, rather Mobile Sink (MS) was there to collect data from sensor nodes throughout the network, and shared key was established every time a sensor node wants to send data to the base station via MS which increases the energy consumption of the sensor nodes as well.

In most of the papers intended to provide security against wormhole attack, time synchronization or location information is used as a basic parameter to eliminate wormhole attack which is not an easy task and requires complex hardware. Therefore, it is important to provide a prominent resilient secure schema against wormhole attacks. In this paper, our proposed idea is very simple and the secure switching of communication channels helps in minimizing the threat of wormhole attacks. Moreover the channel information for data communication between sensor nodes is established only once and saved for future data transmission.

2. The Proposed Scheme
A new scheme is herein proposed to minimize the threats posed by wormhole attacks in WSNs by using polynomial pool based key-predistribution scheme [5]. The main issue in this scheme is the polynomial share discovery problem, which specifies how to found a common bivariate polynomial of which both sensors have sensors have polynomial shares. Our proposed schema solves the problem by shifting to a different communication channel. We have assumed the following assumptions: (1) Each sensor node has multiple communication channels and is capable of dynamic switching between them. (2) Sensor nodes have only one radio and hence can operate at only one available channel at a time. (3) Each sensor node has a non-volatile memory to store the channel information associated with each neighbour node.

To initiate secure communication between two nodes ‘n1’ and ‘n2’, both nodes compute the key f(n1, n2); node n1 by computing f(n1,y) at point n2 and node n2 by computing f(n2,y) at point n1. Initially, all the sensor nodes have their radios tuned to a pre-selected common channel, called the initial common channel ‘C1’. The nodes will then establish pairwise keys over the common channel using polynomial pool-based key-predistribution scheme.

After key establishment, the transmitter node will select a random transmission channel ‘Ct’ from a set of n available channels {C1, C2, C3, ..., Cn} and will send the encrypted message {Ct} having the new frequency information over the common channel to receiver node n2. The sensor node n2 receives the encrypted message, decrypts it using the shared key k, and tunes its radio to the specified frequency ‘Ct’. Node n1 then uses this secret channel Ct to transmit encrypted data messages {data} to the node n2. After the data transmission, both nodes tune their radios to the common channel and start listening for any other transmission. The channel information associated with each neighbour node is also saved in a transmission channel table stored locally in a non-volatile memory, so that for any future communication between the two nodes, the nodes transmit a specific probe signal on the common channel and both nodes will tune their radios to the specific frequency by consulting the transmission channel table without having to establish the common key and sharing the transmission channel information at start of every data transmission.

Since there are thousands of nodes in a WSN and there are a limited memory size, storing the respective communication channel information of every neighbouring node along with their identifier might fill up the memory size very quickly. As a result, we have devised two approaches. First approach includes storing the entries in the transmission channel table for a limited period of time, such that after every time period ‘T’, the entry will be deleted. If the node is frequently transmitting data, the timer T gets reset and will start at the start of every data transmission. However, if the transmission is not to be required after the expiry time, they have to perform the basic process repeatedly. In the second approach, a limited number of entries are allowed in the transmission channel table. For example, if 11 entries are allowed in the transmission channel table, and the node wants to transmit data to a new neighbour (neighbour #12), after key establishment, the associated frequency information will be saved at index #1 (i.e. by deleting the previously stored entry #1) using FIFO method.

3. Threat Analysis
To launch a wormhole attack, an adversary initially establishes a direct link between two nodes in the network and this link is referred to as the wormhole link. After the establishment of wormhole link,
the adversary eavesdrops on the messages at one end of the link, known as the origin node. It then tunnels the messages via the wormhole link to the destination node (target area) and replays them there. Traditional WSN with one communication channel for transmission and reception is too vulnerable to wormhole attack because the adversary can perform tunnelling and replaying anytime and anywhere in the network. Thus, the probability of wormhole attack would be unity. Thus, we have devised the concept of channel diversity to decrease this probability of wormhole attack to a minimum possible level. In our proposed architecture, a wormhole attack launched by a single malicious node using the common channel is not considered a continuous threat, because the attacked node will use the wormhole link to switch its communication channel from the common channel to the transmission channel randomly selected by the transmitter node, which will prevent any further attacks from the malicious node, as the adversary is assumed to be possibly tuned to common channel. Even if the adversary is tuned to any of the available channel other than common channel, the threat will persist only for a limited amount of time because according to the proposed scheme mentioned in the second section, the channel-neighbour entry in transmission channel table will expire after time ‘T’ and both nodes have to repeat the key establishment process and will select another random channel for the data transmission. However, if a number of malicious nodes are tuned to different channels, then the probability of wormhole attack would increase. The relationship between malicious nodes, total available channels and probability of wormhole attack has been discussed in detail in the next section.

4. Probabilistic Analysis
In this section, we make some probabilistic analysis to examine the affect of our proposed solution and the probability of wormhole attack. We also study how different parameters can be changed in order to get better results. To find out the probability of wormhole attack, let’s consider a node ‘n’ with ‘n_l’ legitimate neighbours and ‘n_m’ malicious nodes within its transmission range. Also, each legitimate node has ‘c_a’ available channels and the malicious nodes are tuned to different channels and they have somehow acquired ‘c_b’ communication channels out of total ‘c_a’ channels.

4.1. Scenario-I
Now, we will investigate the probability of wormhole attack when ‘n_m’ malicious nodes are independently tuned to ‘c_b’ different frequencies and they do not have any information about the polynomial key shares used in the network. Since \( P(A \cap B) = P(A) P(B|A) \), if we consider \( P(A) \) to be the probability of selecting the same frequency by the malicious node at which node ‘n’ is transmitting data to one of its neighbour node and \( P(B) \) to be the probability of wormhole attack with ‘n_w’ wormhole links when ‘n_m’ malicious nodes are present, then the total probability \( P_{n_w} = P(A \cap B) \) will be:

\[
P_{n_w} = P \left( \bigcup_{i=1}^{c_b} A_j \right) e^{\frac{n_m - 1}{n_l}}
\]

On further simplification:

\[
P_{n_w} = \sum_{i=1}^{c_b} P(A) e^{\frac{n_m - 1}{n_l}}
\]

Where \( n_m < n_l \) (i.e. Ratio of malicious nodes \( \approx 1 \)).
Figure 1. Probability of wormhole attack 'versus Ratio of malicious neighbor nodes with (a) 8 available channels, (b) 16 available channels

Figure 1(a) and 1(b) shows the graphical representation of equation (2), showing the relation between probability $P_{n_w}$ and malicious node ratio $n_{m}/n_l$ with varying number of wormhole links $n_{w}$. We can see in figure 1(a) that the probability of wormhole attack increases with the increase in the ratio of malicious nodes. Figure 1(a) also shows that when number of wormhole links is increased from 4 to 8, the probability increases as well. This is because as the number of wormhole links (each with a distinct channel) increases, the probability of malicious node to select the actual communication channel as used by targeted node increases. Figure 1(b) depicts the same picture but here the available communication channels are 16 instead of 8 as in figure 1(a). When comparing figure 1(a) and 1(b), we can see that as the available communication channels are doubled, the probability of wormhole attack is decreased to half, hence probability of wormhole attack is in direct proportion to inverse of number of channels.

Also, note that, even when the ratio of malicious nodes is 0.5, the probability of wormhole attack is very much close to zero, hence our proposed solution is much resilient to wormhole attack. Even when a large number of nodes in the surrounding of transmitting nodes are malicious, the probability of a malicious node to launch a wormhole attack using the same channel as selected by the communicating nodes is very low. In figure 2, the probability of successful wormhole attack is plotted against number of communication channels. As shown in the figure, as the number of available communication channels increases, the probability of wormhole attack decreases.

Figure 2. Demonstration of the effect of multiple channels on probability of wormhole attack

4.2. Scenario-II
In the second scenario, some nodes are considered to be compromised by the adversary, hence resulting in the vulnerability caused by the polynomial shares known to the adversary. Now if the
adversary knows the key after compromising multiple nodes, it not only can decrypt every message but can also know the operating frequency at which transmission is suggested. This is basically an extension of Scenario-I, and is referred to as node collusion attack.

Assume that \( n_c \) nodes have been compromised. The probability of any polynomial \( f \) being chosen for a sensor node is \( s'/s \), and the probability of this polynomial being chosen exactly \( i \) times among \( n_c \) compromised sensor nodes is given by

\[
P_{n_c}(i) = {n_c \choose i} \left( \frac{s'}{s} \right)^i \left( 1 - \frac{s'}{s} \right)^{n_c-i}
\]

Thus, the probability of any polynomial of order \( t \) being compromised is:

\[
P_c = 1 - \sum_{i=0}^{t} P_{n_c}(i)
\]

Hence, the composite probability evaluated for Scenario II would be the product of Scenario I equation (2) and (4). Thus, the probability of a communication channel between two un-compromised communicating sensor nodes being compromised and under attack is:

\[
P_w = P_{n_c} \times \left( 1 - \sum_{i=0}^{t} P_{n_c}(i) \right)
\]

It is shown in the equation (5) that when almost 50% of sensor nodes are compromised, the probability of wormhole attack is almost zero irrespective of the malicious node ratio. But as the number of compromised nodes is increased, the probability \( P_w \) increases rapidly. This is because the polynomial pool based scheme becomes quite vulnerable at this point and since the ratio of malicious nodes is also very high, it results in a greater possibility of selecting the active communication channel by the adversary, which results in a successful wormhole attack.

Now just for comparison, we have also done the probabilistic analysis of the wormhole attack when using random key-predistribution scheme instead of polynomial pool-based key-predistribution scheme. The random pairwise keys scheme is a modification of the pairwise keys scheme based on the observation that not all keys need to be stored in the node’s key ring to have a connected random graph with high probability [6]. It assures that, even when few sensor nodes are compromised, the remainder of the network remains fully secure. Furthermore, this scheme enables node-to-node mutual authentication between neighbours without involving a base station. Also if the number of compromised nodes increases, the probability of wormhole attack increases at a drastic rate. Hence, it is clear that polynomial pool based key-predistribution scheme is way better than random generation key-predistribution scheme especially when there is a threat of nodes to be compromised.

5. Conclusions
In this paper, a new schema has been proposed using polynomial pool based key-predistribution schema, which allows any sensor node not only to establish a secure link with neighbouring sensor nodes, but also to defend against wormhole attack. Prior to network deployment, the setup server preloads every multi-channel capable sensor node with polynomial shares of a randomly selected subset of polynomials. Sensor nodes will use a common channel to establish a pairwise key and will shift to a randomly selected channel for data transmission. This channel shift will prevent wormhole attack, as the sensor node is now assumed to be operating at a channel different from that of the adversary.

6. References
[1] Chu T H, Kuo S Y, Chou Y H 2019 Using Quantum-inspired Tabu Search Algorithm with Logic Operation and Moving Average Indicator for Wormhole Attack Detection in a WSN Journal of Internet Technology 20 167-176
[2] Amish P, Vaghela V B 2016 Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol *Procedia computer science* **79** 700-707

[3] Rezaei F, Zahedi A 2017 Dealing with Wormhole Attacks in Wireless Sensor Networks Through Discovering Separate Routes Between Nodes *Engineering, Technology & Applied Science Research* **4** 1771-1774

[4] Sabri Y, El Kamoun N 2017 Attacks and Secure Geographic Routing in Wireless Sensor Networks *Indonesian Journal of Electrical Engineering and Computer Science* **5** 147-158

[5] Zhang J, Li H, Li J 2018 Key establishment scheme for wireless sensor networks based on polynomial and random key predistribution scheme *Ad Hoc Network* **71** 68-77

[6] Jamshidi M, Bazargan H, Shaltooki A A, et al. 2019 A Hybrid Key Pre-Distribution Scheme for Securing Communications in Wireless Sensor Networks *International Journal on Informatics Visualization* **3** 41-46