A Group-Based Deployment for Wormhole Prevention in Sensor Networks

GU-HSIN LAI*, CHEN-SEN OUYANG* AND CHIA-MEI CHEN*

*Department of Information Management
National Sun Yat-sen University
Kaohsiung, 804 Taiwan

*Department of Information Engineering
I-Shou University
Kaohsiung, 840 Taiwan

Wireless sensor networks consist of many tiny sensors with sensing and communication ability. The applications of wireless sensor networks are widely used today in battlefield guard, circumstance monitor, and traffic analysis. Sensor network often carries on mission-critical tasks. Thus, security in sensor network is vital. Wormhole attack may threaten the availability of networks by dropping data randomly or disturbing routing path. In this paper, a group-based deployment is proposed to prevent wormhole attack. Sensors are deployed by groups and are aware of their own group location where the group of sensors will be located and no exact location is known in advance. Group location will be exchanged among sensors during routing path establishment and a link between two sensors will be built only when the distance of two sensor's group location is close enough. The proposed approach to prevent wormhole is novel and efficient, using only the group location information and no any special hardware is needed.

Keywords: sensor network, wormhole attack, network security, sensor deployment, attack prevention

1. INTRODUCTION

Because sensor network often carries on mission-critical task, loss of availability may have serious impacts (e.g. fail to detect a potential accident and result in financial loss in plant monitor or environmental surveillance). One of the vital attacks on availability in wireless networks is wormhole and sensor network is more vulnerable to wormhole attacks due to the special features of sensor network: distributed network architecture and limited resources of sensors. Two malicious sensor nodes may construct a wormhole tunnel through a low-latency communication link, replaying messages from neighbors and dropping messages to disturb the normal function of the network. The sensors would think the routing path through the tunnel is shorter than the normal multi-hop route, as the wormhole tunnel reaches further than the normal wireless transmission range of a single hop [5]. Wormhole threats will be described below.

In Fig. 1 (a), two malicious nodes, M1 and M2 replay the messages received from their neighbors where a dash circle centered by node A represents the wireless transmission range of the node. Its messages will be replayed by M1 and M2 as M1 is in its transmission range; hence, M2, D, and E are A’s neighbors. Consequently, A will send message “directly” to node D, the one which A thinks it is a neighbor, as shown in Fig. 1

Received October 30, 2009; accepted June 24, 2010.
Communicated by Ren-Hung Hwang, Chung-Ming Huang, Cho-Li Wang, and Sheng-Tzong Cheng.
However, A to D indeed is long-distance communication, not one-hop communication. The messages from A will be lost and resent until A exhausts its battery power. Another possible attack is illustrated in Fig. 1 (c) where the wormhole tunnel randomly drops the messages sent from the endpoint’s neighbors, A, B, and C. Wormhole disturbs the establishment of routing path, exhausting sensor’s battery power. It seems that wormhole might cause great damage to sensor networks but it can be launched easily even without compromising any legitimate sensor nodes.

Some researches on wormhole detection need special hardware like GPS or directed antenna [2, 7]. Some use centralized approaches to detect wormhole attack. However, special hardware and centralized approaches are not suitable for sensor networks [7, 9].

In this paper, we propose a deployment scheme based on group deployment to prevent wormhole attacks. In the proposed approach, sensors can be divided by groups and deployed in an area of their own group. Group locations can be determined in advance. On the other hand, deploying sensors one by one in a hostile area is costly and impractical. Thus, we assume that group locations are predetermined and sensors only have the knowledge of their group location, no exact location. Sensors of the same group have the same group location. If two sensors are close to each other topologically, the chance that the two group locations are near is high. By means of group location, a sensor can check if its neighbor exceeds the communication range, no additional hardware is needed to prevent wormhole attacks.
2. RELATED WORKS

Wormhole attack in wireless ad-hoc networks was first independently introduced by Hu [3], Dahill [1], and Papadimitratos [3]. Dahill [1] and Papadimitratos [6] used secure modulation over the wireless channel which can be demodulated only by authorized nodes. Such approach defends against outside attackers without the possession of cryptographic keys.

Hu et al. proposed packet leash mechanism against wormhole attacks [3-5]. A leash in a packet is information designed to restrict the packet’s maximum allowed transmission distance. It assumes that all nodes are time synchronized and are aware of their location information.

Sanzgiri and Dahill proposed Authenticated Routing for Ad-hoc networks (ARAN) to prevent wormhole attack [8]. ARAN enforces authentication, message integrity, and non-repudiation as a minimal security policy. Furthermore, ARAN requires a certificate server and PKI to realize the above security services.

Poovendran and Lazos characterized worm attack, in wireless sensor networks, by a graph theoretic framework [7]. The authors proposed a cryptography based solution to the wormhole attack. A set of special nodes called guards are deployed over the network for establishing local broadcast keys. However, in some situations, deploying a set of powerful guards is impractical. Hu and Evans [2] used directional antennas to prevent wormhole attack. By means of shared secret keys and directional antennas, each node can discover its neighbors and avoid the development of wormhole. Most sensors are compact and primitive, equipped with directional antenna might be rare.

Wang and Bhargava developed a mechanism, MDS-VOW (Multi-Dimensional Scaling-Visualization of Wormhole), reconstructing the network using multi-dimensional scaling and detecting a wormhole attack by visualization the anomalies resulted from the attack [10]. When multiple wormholes form gradually, the reconstructed surface will be distorted far from the original layout and the detection may not be able to locate all fake connections. MDS-VOW is a centralized approach. Decentralized approach in timely manner is more desired and practical in sensor networks. Another centralized mechanism based on statistical decision theory, SAM (Statistical Analysis of Multi-path) [9], identifies a wormhole attack by analyzing the information collected from multi-path routing.

Most researchers studied wormhole attack on ad-hoc networks, not sensor networks. Some use centralized schemes and others may require additional hardware. Most approaches are not suitable for distributed sensor network environments. Therefore, a novel decentralized solution is needed to solve the wormhole problem in sensor networks.

3. PROPOSED APPROACH

In this paper, we assume that the topology of the sensor network is static, that the links between sensors are bidirectional, and that secure communication between two sensors exists in the network. Each sensor is equipped with its group location before deployment and the deployment distribution of the sensors in one group follows Gaussian distribution. All the group locations are pre-determined and standard deviation is assumed to be able to be estimated in advance.
The following notations are required to describe the proposed system.

- \( S_i \) represents a sensor ID.
- \( G_i \) represents a group ID.
- \( L_k(x_i, y_i) \) is the pre-determined group location of group \( k \).
- \( B \): The upper bound of the distance of two sensors in the direct communication range.

The sensors of group \( G_i \) with the knowledge of their group location \((x_i, y_i)\) are denoted as black dots in Fig. 2. The mean of the Gaussian distribution \( \mu \) is \((x_i, y_i)\) and the probability distribution function of a node in a group is

\[
f(x, y) = \frac{1}{2\pi\sigma^2} e^{-(x-x_1)^2+(y-y_1)^2/2\sigma^2}
\]

where \( \sigma \) is the standard deviation. Based on Gaussian distribution, about 95\% of sensors will locate within \( 2\sigma \) as illustrated in Fig. 2. Based on the proposed group-based deployment, two sensors are close to each other topologically, the chance that the two group locations are near is high. Based on our observation illustrated in Fig. 3 that the distance between two sensors belonged to the same group or the neighbor groups, \( G_i \) and \( G_j \), is less than \( 4\sigma \). Such bound is still too loose for wormhole prevention. Therefore, we will develop an upper bound of the distance between two group locations, \( B \), to determine if two nodes are close to each other and a direct link may exist.

Fig. 2. Group-based deployment.                      Fig. 3. Distance bound of two sensors.

To build a one-hop link between two endpoints, there are two cases: the two endpoints are belonged to the same group or different groups. As illustrated in Fig. 3, sensors R and Q are within the communication range of sensor P. As sensors P and R belongs to same group G1, the routing path between these two nodes can be established easily. As for nodes P and Q, if the distance of the two group locations is smaller than the upper bound, \( (x_1-x_2)^2+(y_1-y_2)^2 < B \) they are considered as closed to each other and the routing path is established.

Fig. 4 illustrates the impact of the bound. Suppose that the bound \( B \) is set to \( \sigma \), sensor P can establish a direct communication link to A, B, C, and F, respectively. However, P cannot establish a direct communication link to D, because the distance of the two group
location is more than \( B \), \( \sqrt{\left(x_1 - x_4\right)^2 + \left(y_1 - y_4\right)^2} \approx 1.4\sigma > B \). Let the bound \( B \) set to \( 1.5\sigma \). P can establish a direct communication link to D as well. \( \sqrt{\left(x_1 - x_4\right)^2 + \left(y_1 - y_4\right)^2} \approx 1.4\sigma < B \). Larger bound can cover more neighbor groups, but cannot affect the wormhole prevention. Therefore, we suggest the bound is set to \( 1.4\sigma \) to \( 1.5\sigma \). As the wormhole endpoints normally are away from each other and are belonged to different groups, the distance of the group locations of the wormhole endpoints mostly likely is large. \( \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2} > B \), as shown in Fig. 5. Therefore, the proposed solution disallows such path and hence avoids the wormhole.

4. ANALYTIC MODEL

A mathematical model is proposed to analyze the performance of our proposed method. Based on the distribution function of the group deployment, Gaussian distribution, the probability that two sensors in the neighboring groups are located at opposite sites and far from their group location is low. Therefore, the probability that a wormhole link whose endpoints are located at the neighboring groups is longer than \( 4\sigma + B \) is lower than 5%, as illustrated in Fig. 6. A wormhole link in two different, non-neighboring groups will exceed the distance bound specified above. Hence, we can conclude that the wormhole attack can be avoided based on the bound.

Furthermore, we show the connectivity analysis of our approach below. Given a group
Fig. 6. A wormhole link located at neighboring group.

$G_{(1)}$ and a set of its corresponding neighboring groups, \{\(G_{(m)}\) | \(m = 2, 3, \ldots, M\)\}. Each group \(G_{(m)}\) contains \(N\) sensors with group location \((x_m, y_m)\). For a sensor \(S_{(j)}\) belonged to the group \(G_{(1)}\) and located at \((x, y)\), the probability that it can communicate with at least one other sensor can be derived as follows.

Without loss of generality, the generation of each sensor in each group is assumed to be independent of the others; the generation of each group is assumed to be independent of the others. Let \(C\) be the event that \(S_{(j)}\) can communicate with at least one other sensor, \(A_m\) be the event that no sensor in \(G_{(m)}\) can communicate with \(S_{(j)}\), and \(B_{mn}\) be the event that the sensor \(S_{(mn)}\) (located at \((x_{mn}, y_{mn})\)) in \(G_{(m)}\) can communicate with \(S_{(j)}\). The probability of event \(A_m\) can be calculated by the following equation:

\[
P(A) = P(B_{11} \cap B_{12} \cap \ldots \cap B_{1M}) = \prod_{n=1, n \neq 1}^N p(B_{1n}) = [1 - p(B_{1n})]^{N-1}
\]

and

\[
P(A_m) = P(B_{m1} \cap B_{m2} \cap \ldots \cap B_{mn}) = \prod_{n=1}^N P(B_{mn}) = [1 - P(B_{mn})]^N, \quad m = 2, 3, \ldots, M,
\]

where

\[
P(B_{mn}) = P((x_m - x)^2 + (y_m - y)^2 \leq R^2) = \int_{x_{mn}-R}^{x_{mn}+R} \int_{y_{mn}-R}^{y_{mn}+R} f_{mn}(x, y)dydx.
\]

\(f_{mn}(x, y)\) is the probability density function of group \(G_{(m)}\). Therefore, the probability that no sensor in the network can communicate with \(S_{(j)}\), \(P(A_1 \cap A_2 \cap \ldots \cap A_M)\) is calculated as follows,

\[
P(A_1 \cap A_2 \cap \ldots \cap A_M) = \prod_{m=1}^M P(A_m) = [1 - P(B_{1n})]^{N-1} \prod_{m=2}^M [1 - P(B_{mn})]^N.
\]

Finally, we have

\[
P(C) = 1 - P(A_1 \cap A_2 \cap \ldots \cap A_M) = 1 - [1 - p(B_{1n})]^{N-1} \prod_{m=2}^M [1 - p(B_{mn})]^N.
\]

To ensure that a sensor can communicate with at least one sensor in the network, we want to develop a lower bound for the number of sensors in a group such that the whole network will not be too sparse to communicate with other sensors and hence can avoid
wormhole by the proposed solution. For a given lower bound $\alpha$ for $P(C)$, the probability that a sensor can communicate with at least one sensor, we can derive the lower bound $\alpha_N$ for the number of sensors, $N$, in each group.

$$P(C) \geq \alpha \Rightarrow 1 - \left(1 - p(B_{1s})\right)^{N-1} \prod_{m=2}^{M} \left[1 - p(B_{ms})\right]^N \geq \alpha \Rightarrow$$

$$\left[1 - p(B_{1s})\right]^{N-1} \prod_{m=2}^{M} \left[1 - p(B_{ms})\right]^N \leq 1 - \alpha \Rightarrow$$

$$\log \{\left[1 - p(B_{1s})\right]^{N-1} \prod_{m=2}^{M} \left[1 - p(B_{ms})\right]^N\} \leq \log \{1 - \alpha\} \Rightarrow$$

$$(N - 1) \log \{1 - p(B_{1s})\} + N \sum_{m=2}^{M} \log \{1 - p(B_{ms})\} \leq \log \{1 - \alpha\} \Rightarrow$$

$$N \geq \frac{(N - 1) \log \{1 - \alpha\} + N \sum_{m=2}^{M} \log \{1 - p(B_{ms})\}}{\sum_{n=1}^{M} \log \{1 - p(B_{ns})\}}$$

Therefore, we obtain the lower bound for $N$, $\alpha_N$, as below.

$$\alpha_N = \frac{(N - 1) \log \{1 - \alpha\} + N \sum_{m=2}^{M} \log \{1 - p(B_{ms})\}}{\sum_{n=1}^{M} \log \{1 - p(B_{ns})\}}$$

Based on the analysis above, we can know that the maxima distance of wormhole link and the connectivity can be estimated, if the standard deviation can be estimated in advance and group location can be pre-determined.

### 5. SIMULATION AND RESULT

In the previous section, we evaluated our algorithms through theoretical analysis. In this section, we present the simulation environment and results for the proposed approach. The goal of this simulation is to evaluate the performance of the proposed method. The system performance is measured by the connectivity of sensors and the security of our approach. We compare our approach with uniform distribution approach. Uniform deployment approaches were widely used in sensor networks. Fig. 7 illustrates the topology of group-based deployment and Fig. 8 illustrates the topology of uniform deployment.

In Fig. 7, the “×” means group location and “o” means sensor location. We deploy 81 groups and each group contains seven sensors (576 sensors). Sensors are deployed by group and grid in 550m × 550m area. In Fig. 7, the distance between groups is 50m and the standard deviation is also 50m. We can see only some isolated sensors fall in the border of the area in Fig. 7. Though we deploy sensors by grid, we can deploy sensors in different ways based on different geography in real world application.

In Fig. 8, sensors are deployed randomly, and each can communicate others directly. Many researchers used such approach for sensor deployment. Therefore, we compare group-based deployment approach with the uniform one using connectivity as measure-


ment. Let \( N \) be the total number of sensors and \( I \) be the total number of isolated sensors. In uniform deployment approach, an isolated sensor is one which has no any other sensors within its communication range. In our approach, an isolated sensor has no any sensors which belong to its neighbor groups within its communication range. The connectivity in our simulation is \( 1/N \).

In this section, we first evaluate the connectivity of our approach and we evaluate the security of our approach later. In experiment 1, we observe the relation between density of sensor and connectivity. In group-based approach, sensors are deployed by group and grid. We deploy sensors on 550m \( \times \) 550m area in both approaches. Each experiment runs 100 times and the experiment results are in the average. Table 1 illustrates the fixed parameters of experiment 1 and Fig. 9 illustrates the result of experiment 1.
Table 1. The fixed parameters of experiment 1.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of groups in group-based approach</td>
<td>81 (9 x 9) groups</td>
</tr>
<tr>
<td>The distance of groups n group-based approach</td>
<td>50m</td>
</tr>
<tr>
<td>Communication ranges of sensors</td>
<td>50m</td>
</tr>
<tr>
<td>Bound of group-based approach</td>
<td>75m</td>
</tr>
<tr>
<td>Standard deviation of group-based approach</td>
<td>40m</td>
</tr>
</tbody>
</table>

The result of experiment 1 illustrates that the uniform deployment approach has better connectivity but the connectivity of group-based approach is also acceptable. Once the density of sensors is high, the connectivity will become high. But in our simulation, even the density is low, the system still keeps an acceptable connectivity (96.77%). Fig. 10 illustrates the network topology which each group has only three sensors.

In Fig. 10, we can see many isolated sensors in the border of the environment, this is because there are fewer groups in the border of environment and the standard deviation is high (40m). If we deploy more sensors in border group, the connectivity might improve. Experiment 2 evaluates the connectivity if we deploy one more sensors on the border group. Table 2 illustrates the fixed parameters of experiment 2 and Fig. 11 illustrates the result of experiment 2.

Table 2. The fixed parameters of experiment 2.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of groups in group-based approach</td>
<td>81 (9 x 9) groups</td>
</tr>
<tr>
<td>The distance of groups n group-based approach</td>
<td>50m</td>
</tr>
<tr>
<td>Communication ranges of sensors</td>
<td>50m</td>
</tr>
<tr>
<td>Bound of group-based approach</td>
<td>75m</td>
</tr>
<tr>
<td>Standard deviation of group-based approach</td>
<td>40m</td>
</tr>
</tbody>
</table>

Experiment 2 illustrates that if we deploy more sensors on border group, the connectivity is better when the density is low. However, the improvement is not significant.
when the density is high.

We observe that the relation between density of sensors and connectivity when deviation is high (40m) in experiment 1 and that when standard deviation is low (20m) in experiment 3. Table 3 shows the fixed parameters of experiment 3 and Fig. 12 illustrates its result. The proposed approach has better connectivity than uniform deployment approach, when the standard deviation is low. If standard deviation is low, the location of sensors which belong to the same group will close to their group location. Thus we can get higher connectivity. Experiment 3 also shows that if the standard deviation is low, the connectivity of our approach reaches to almost 100% even in low density of sensors. If standard deviation is low and density is high, the connectivity of two approaches has no significant difference.

Table 3. The fixed parameters of experiment 3.

<table>
<thead>
<tr>
<th>Number of groups in group-based approach</th>
<th>81 (9 × 9) groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>The distance of groups n group-based approach</td>
<td>50m</td>
</tr>
<tr>
<td>Communication ranges of sensors</td>
<td>50m</td>
</tr>
<tr>
<td>Bound of group-based approach</td>
<td>75m</td>
</tr>
<tr>
<td>standard deviation of group-based approach</td>
<td>20m</td>
</tr>
</tbody>
</table>

In our approach, we assume that the standard deviation could be estimated in advance. According to experiment 3, we know that the standard deviation will influence the connectivity. Fig. 13 illustrates the topology with different standard deviation.

In Fig. 13, we can see that if the standard deviation is high (60m), there are many isolated sensors in the border of the area. But if the standard deviation is low (20m), there are almost no any isolated sensors in the border of the area. In addition, if the standard deviation is high, more sensors might be deployed far from group locations. Thus even there are some sensors within their communication range, they cannot communicate to another.

Since standard deviation is an important parameter in our approach, we observe the relation between connectivity and different standard deviation in experiment 4. Table 4 illustrates the fixed parameters of experiment 4 and Fig. 14 illustrates its result. We can see that the lower the standard deviation is, the better the connectivity of our approach is. The connectivity is also acceptable (97.819%), even when the standard deviation is high.
A GROUP-BASED DEPLOYMENT FOR WORMHOLE PREVENTION IN SENSOR NETWORKS

(a) $\sigma = 20$. 
(b) $\sigma = 60$. 
Fig. 13. The topology with different standard deviation.

Table 4. The fixed parameters of experiment 4.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of groups in group-based approach</td>
<td>81 (9 x 9)</td>
</tr>
<tr>
<td>The distance of groups n group-based approach</td>
<td>50m</td>
</tr>
<tr>
<td>Communication ranges of sensors</td>
<td>50m</td>
</tr>
<tr>
<td>Bound of group-based approach</td>
<td>75m</td>
</tr>
<tr>
<td>Number of sensors in one group</td>
<td>8</td>
</tr>
</tbody>
</table>

Fig. 14. The result of experiment 4.

The simulation result in experiments 1 to 4 shows the connectivity of our approach is high. In experiments 5 to 7, we will evaluate the performance of our approach against wormhole attacks. In the proposed approach, we assume that the distance of wormhole is always long and our approach can prevent wormhole attacks rather than detect them. Therefore, we do not compare our approach with others because the proposed approach is quite different than previous and the performance is incomparable.
In experiment 5, we evaluate the relation between the distance of wormhole tunnel and the performance of our approach. 100 times of attacks are simulated with different distance of wormhole tunnel. Table 5 shows the fixed parameters and Fig. 15 the result. The result indicates that the proposed approach performs better when the distance of wormhole tunnel is long and worse when that becomes short.

<table>
<thead>
<tr>
<th>Table 5. The fixed parameters of experiment 5.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of groups</td>
</tr>
<tr>
<td>The distance of groups</td>
</tr>
<tr>
<td>Communication ranges</td>
</tr>
<tr>
<td>Bound</td>
</tr>
<tr>
<td>Number of sensors in one group</td>
</tr>
<tr>
<td>standard deviation</td>
</tr>
</tbody>
</table>

In practical, the distance of wormhole tunnel usually is long; the proposed approach is useful for wormhole attack prevention. In section 4, we proved the distance of wormhole tunnel is bounded by bound and standard deviation. There are two ways to shorten the distance of wormhole tunnel: one is to decrease the standard deviation and the other is to decrease the bound. If we have a better deployment approach to decrease the standard deviation, the distance could be reduced. Therefore, in experiment 6, we set standard deviation as 20m and observe our performance in low deviation. Table 6 states the fixed parameters and Fig. 16 the result. We can see our approach performs well in low standard deviation.

<table>
<thead>
<tr>
<th>Table 6. The fixed parameters of experiment 6.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of groups</td>
</tr>
<tr>
<td>The distance of groups</td>
</tr>
<tr>
<td>Communication ranges</td>
</tr>
<tr>
<td>Bound</td>
</tr>
<tr>
<td>Number of sensors in one group</td>
</tr>
<tr>
<td>standard deviation</td>
</tr>
</tbody>
</table>
As mentioned above, the second approach to improve the performance is to shorten the bound. We can get a shorter bound by increasing the number of groups. Fewer sensors are deployed in each group to keep the density of sensors for increasing the group numbers. Experiment 2 illustrates if the standard deviation is low, the connectivity can reach to 99.79% even we only deploy three sensors on each group. Therefore, if we can deploy sensors with lower standard deviation, we can increase the number of groups and get shorter bound. Fig. 17 illustrates the topology with more groups for experiment 7.

Table 7. The fixed parameters of experiment 7.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of groups</td>
<td>196 (14 × 14) groups</td>
</tr>
<tr>
<td>The distance of groups</td>
<td>40m</td>
</tr>
<tr>
<td>Communication ranges</td>
<td>50m</td>
</tr>
<tr>
<td>Bound</td>
<td>60m</td>
</tr>
<tr>
<td>Number of sensors in border group</td>
<td>3</td>
</tr>
<tr>
<td>standard deviation</td>
<td>20m</td>
</tr>
</tbody>
</table>
196 groups are deployed; each has three sensors only; the group distance is 40m. Table 7 shows the fixed parameters of experiment 7 and Fig. 18 the result.

The result proves that the proposed approach performs well even when group number increases. In experiments 4 to 7, we can see our approach can prevent wormhole attack. In wormhole attack, the distance between attacks is always long. Thus the simulation result shows that our approach can prevent wormhole well. In addition, in our approach, only few sensors which are deployed far from their group location might be affected even wormhole attack occurs. All of the experiments show that the performance of our system is good. Our approach can prevent wormhole attack with high connectivity and without additional hardware or global information.

6. CONCLUSION

In this paper, a group-based deployment is proposed to prevent wormhole attacks in sensor networks. Unlike previous approaches, the proposed decentralized, group-base deployment does not require any hardware support. Only predetermined group location is needed for each sensor to prevent the construction of wormhole tunnel. The proposed approach also minimized the damage caused by wormhole. In our approach, wormhole attacks occur only when the distance of tunnel is short. If the distance of tunnel is short, the damage of wormhole also decreases. Even though the wormhole tunnel is built successfully, only few sensors which deployed far from the group location could be influenced.

The analytic model shows that the chance that the proposed solution will misjudge a wormhole is very small. Hence, this is an efficient and practical solution against wormhole attacks.

In our approach, we assume that secure communication between two sensors is established by other mechanism. In our future work, we plan to develop an efficient pairwise key distribution based on such group deployment and can future reduce the chance of wormhole attacks.

REFERENCES


Gu-Hsin Lai (賴谷鑫) received the M.S. degree in Information Management from the National Chi Nan University, Taiwan, in 2002, the Ph.D. degrees in Information Management from National Sun Yat-sen university, Taiwan, in 2009. He is a principal engineer of Taiwan Semiconductor Manufacturing Company. His research focus on spam mail filter, wireless sensor network and system security.

Chen-Sen Ouyang (歐陽振森) received the B.S. and Ph.D. degrees from the National Sun Yat-sen University, Kaohsiung, Taiwan, in 1998 and 2004, respectively. He joined the faculty of the Department of Information Engineering, I-Shou University, Kaohsiung, Taiwan, in 2005. His research interests include machine learning, data mining, cloud computing, computer vision, and biometrics. Dr. Ouyang is a member of the IEEE and the Taiwanese Association of Artificial Intelligence.

Chia-Mei Chen (陳嘉玟) joined in the National Sun Yat-sen University as an associate professor in 1996 and became a full professor in 2004. In addition, she is Section Chef of Network Division, Office of Library and Information Services. She received B.S. in Computer Science and Information Engineering from National Chiao Tung University, and Ph.D. in Computer Science from the University of Maryland, College Park. She serves as a coordinator of TWCERT/CC (Taiwan Computer Emergency Response Team/Coordination Center) since 1998 and continues working for the network security society. Her current research interests include mobile networks, multimedia systems, and network security.