A Secure Scheme for Two-Dimension Wireless Sensor Networks Based on Symmetric Polynomials

Yuquan Zhang

Wireless Sensing Institute, College of Information Science and Engineering, Qilu Normal University, China
zyczyq@126.com

Keywords: Wireless sensor network; security; two-dimension; grids; symmetric polynomials.

Abstract. A security scheme for two-dimension wireless sensor network is presented through using the symmetric polynomials. The sensing square locates in a two-dimension coordinate system. All sensor nodes are distributed in the sensing square evenly. Each sensor node set up the common keys with its neighbor sensor nodes through utilizing the symmetric polynomials because one of its coordinates, the horizontal coordinate or the vertical coordinate, is equal to one of coordinates, the horizontal coordinate or the vertical coordinate, of the neighbor sensor nodes and the absolute value of difference between the two values, where one value is one of its coordinates, the horizontal coordinate or the vertical coordinate, and the other one value is one of coordinates, the horizontal coordinate or the vertical coordinate, of the neighbor sensor nodes, is 1 or $n$. After each sensor node set up the keys with its neighbor sensor nodes, all sensor nodes in the sensing two-dimension area set up their common keys directly or indirectly. Analysis and comparison demonstrate that this scheme improve the wireless sensor network security and the connectivity.

1. Introduction

Wireless sensor networks comprise numerous sensor nodes which are linked by a wireless medium. Those sensor nodes can sense, collect, calculate, and relay information. Wireless sensor networks have attracted considerable attention for several decades because wireless sensor networks have various applications including traffic, medical treatment, smart home, environment monitor, etc.

Wireless sensor networks have various applications, however, the sensor nodes have several disadvantages, including low computing ability, low storage, limited communication capacity, and so on. Additionally, in order to fulfil the wireless sensor network applications, wireless sensor networks sometimes are deployed in dangerous environment where the adversary launches attack to compromise the sensor nodes. Therefore, guaranteeing the wireless sensor networks secure is one of the most important issues in order to provide various services.

The key management scheme is an effective method to ensure wireless sensor network secure. Y.Zhou gave a key management scheme through using the polynomials.

This key management scheme guarantees wireless sensor network secure through using the symmetric polynomials. All sensor nodes are distributed in the whole sensing area evenly. Each sensor node set up the common keys with its neighbor sensor nodes through using the symmetric polynomials. Next, all sensor nodes establish their common keys directly or indirectly. Analysis and comparison show this scheme improves the security for wireless sensor networks. Additionally, it enhances the wireless sensor network connectivity.

The rest of this paper is arranged as follows. In section two, pairwise keys are established. Performance analysis for WSNs is presented in the section three. The conclusion of this paper is in section four.
2. Pairwise key establishment

2.1 Mathematical lemma
A symmetric polynomial\([4][5]\) is a \(t\)-degree \((K+1)\)-variate polynomial defined as follows
\[
f(x_1, x_2, \cdots, x_{K+1}) = \sum_{i_0, i_1, \cdots, i_{K+1}} a_{i_0, i_1, \cdots, i_{K+1}} x_1^{i_0} x_2^{i_1} \cdots x_{K+1}^{i_{K+1}}.
\]
All coefficients of the polynomial are chosen from a finite field \(F_q\), where \(q\) is a prime integer.

The polynomial \(f\) is a symmetric polynomial so that\([4]\)
\[
f(x_1, x_2, \cdots, x_{K+1}) = f(x_{\partial(1)}, x_{\partial(2)}, \cdots, x_{\partial(K+1)})
\]
where \(\partial\) denotes a permutation. Every node using the symmetric polynomial based protocol takes \(K\) credentials \((I_1, I_2, \cdots, I_K)\) from the key management centre, and these are stored in memory. The key management centre must also compute the polynomial shares using the node credentials and the symmetric polynomial. The coefficients \(b_i\) stored in node memory as the polynomial share are computed as follows
\[
f_b(x_{K+1}) = f(I_1, I_2, \cdots, I_K, x_{K+1}) = \sum_{i=0}^{K} b_i x_{K+1}^i.
\]

2.2 Pairwise key establishment between one sensor node and its neighbor sensor nodes
In the Fig.1, the sensing area is a square denoted as \(S\) and the sensor nodes are all the same and are distributed in \(S\) evenly. All sensor nodes, \(N_0, N_1, N_2, \cdots, N_{n-2},\) and \(N_{n-1}\), locate in the intersections of parallel lines and vertical lines respectively in the Fig.1. Let the IDs of sensor node \(N_0, N_1, N_2, \cdots, N_{n-2},\) and \(N_{n-1}\) be \(0,1,2,\cdots, n^2-2,\) and \(n^2-1\) respectively, where \(0 \leq ID \leq n^2-1\). The coordinate of the sensor node \(N_0\) is \((0,0)\), the coordinate of the sensor node \(N_1\) is \((1,0),\) the coordinate of the sensor node \(N_{ID}\) is \((c_h^{ID}, c_v^{ID}),\) the coordinate of the sensor node \(N_{n-2}\) is \((n-2, n-1)\) and the coordinate of the sensor node \(N_{n-1}\) is \((n-1, n-1)\). Clearly, \(ID = n \times c_v^{ID} + c_h^{ID}\) holds. We definite that the identity of the sensor node \(N_{ID}\) is \((c_h^{ID}, c_v^{ID}, ID)\).

In general, for a sensor node \(N_{ID}\) \((c_h^{ID}, c_v^{ID}, ID)\), where \(0 < c_h^{ID} < n-1\) and \(0 < c_v^{ID} < n-1\), it can set up common keys with its four neighbor sensor nodes respectively. Its left sensor node is \(N_{ID-1}\)

![Fig. 1. The sensing square](image-url)
\((c_h^{ID-1}, c_v^{ID-1}, ID-1)\), its right sensor node is \(N_{ID+1}(c_h^{ID+1}, c_v^{ID+1}, ID+1)\), its above sensor node is \(N_{ID+n}(c_h^{ID+n}, c_v^{ID+n}, ID+n)\), and its below sensor node is \(N_{ID-n}(c_h^{ID-n}, c_v^{ID-n}, ID-n)\). For sensor nodes \(N_{ID}\) and \(N_{ID-1}\), let \(I_1 = c_h^{ID} = c_h^{ID-1} - 1\), \(I_2 = c_v^{ID} = c_v^{ID-1}\), \(I_3^{ID} = ID\), and \(I_3^{ID-1} = ID-1\).

In this case, a \(t\)-degree \((3+1)\)-variate polynomial defined as follows
\[
f(x_1, x_2, x_3, x_4) = \sum_{i=0}^{t} \sum_{j=0}^{3} a_{i,j} x_1^i x_2^j x_3 x_4^t\]
is utilized. In order to compute a shared key, the sensor node \(N_{ID}\) takes \(ID-1\) as the input and computes \(f_{N_{ID}}(ID-1)\), and the sensor node \(N_{ID-1}\) takes \(ID\) as the input and computes \(f_{N_{ID-1}}(ID)\). Obviously, those two sensor nodes compute the same shared key because of the polynomial symmetry. Generally, the sensor nodes \(N_{ID}\) and its left neighbor node \(N_{ID-1}\) can establish shared key \(k_{N_{ID},N_{ID-1}}^L = f_{N_{ID}}(ID-1) = f_{N_{ID-1}}(ID)\). For sensor nodes \(N_{ID}\) and \(N_{ID+1}\), let \(I_1 = c_h^{ID} = c_h^{ID+1} - 1\), \(I_2 = c_v^{ID} = c_v^{ID+1}\), \(I_3^{ID} = ID\), and \(I_3^{ID+1} = ID+1\).

In this case, a \(t\)-degree \((3+1)\)-variate polynomial defined as follows
\[
f(x_1, x_2, x_3, x_4) = \sum_{i=0}^{t} \sum_{j=0}^{3} a_{i,j} x_1^i x_2^j x_3 x_4^t\]
is utilized. In order to compute a shared key, the sensor node \(N_{ID}\) takes \(ID+1\) as the input and computes \(f_{N_{ID}}(ID+1)\), and the sensor node \(N_{ID+1}\) takes \(ID\) as the input and computes \(f_{N_{ID+1}}(ID)\). Obviously, those two sensor nodes compute the same shared key because of the polynomial symmetry. Generally, the sensor nodes \(N_{ID}\) and its right neighbor node \(N_{ID+1}\) can establish shared key \(k_{N_{ID},N_{ID+1}}^R = f_{N_{ID}}(ID+1) = f_{N_{ID+1}}(ID)\).

Similarly, for sensor nodes \(N_{ID}\) and \(N_{ID-n}\), let \(I_1 = c_h^{ID} = c_h^{ID-n}, I_2 = c_v^{ID-n} = c_v^{ID-n} - 1, I_3^{ID} = ID\), and \(I_3^{ID-n} = ID-n\). We can obtain that the sensor nodes \(N_{ID}\) and its below neighbor node \(N_{ID-n}\) can establish shared key \(k_{N_{ID},N_{ID-n}}^B = f_{N_{ID}}(ID-n) = f_{N_{ID-n}}(ID)\). For sensor nodes \(N_{ID}\) and \(N_{ID+n}\), let \(I_1 = c_h^{ID} = c_h^{ID+n}, I_2 = c_v^{ID+n} - 1 = c_v^{ID+n} - 1, I_3^{ID} = ID\), and \(I_3^{ID+n} = ID+n\). We can obtain that the sensor nodes \(N_{ID}\) and its above neighbor node \(N_{ID+n}\) can establish shared key \(k_{N_{ID},N_{ID+n}}^A = f_{N_{ID}}(ID+n) = f_{N_{ID+n}}(ID)\).

For a sensor node \(N_{ID}\) \((c_h^{ID}, c_v^{ID}, ID)\), where \(0 < c_h^{ID} < n-1\) and \(c_v^{ID} = 0\), it can set up common keys with its three neighbor sensor nodes respectively. Its left sensor node is \(N_{ID-1}(c_h^{ID-1}, c_v^{ID-1}, ID-1)\), its right sensor node is \(N_{ID+1}(c_h^{ID+1}, c_v^{ID+1}, ID+1)\), its above sensor node is \(N_{ID+n}(c_h^{ID+n}, c_v^{ID+n}, ID+n)\), and it has not below neighbor sensor node. The shared key between the sensor node \(N_{ID}\) \((c_h^{ID}, c_v^{ID}, ID)\) and its left sensor node is \(k_{N_{ID},N_{ID-1}}^L = f_{N_{ID}}(ID-1) = f_{N_{ID-1}}(ID)\), the shared key between the sensor node \(N_{ID}\) \((c_h^{ID}, c_v^{ID}, ID)\) and its right sensor node is \(k_{N_{ID},N_{ID+1}}^R = f_{N_{ID}}(ID+1) = f_{N_{ID+1}}(ID)\), and the shared key between the sensor node \(N_{ID}\) \((c_h^{ID}, c_v^{ID}, ID)\) and its above sensor node is \(k_{N_{ID},N_{ID+n}}^A = f_{N_{ID}}(ID+n) = f_{N_{ID+n}}(ID)\).

Similarly, for a sensor node \(N_{ID}\) \((c_h^{ID}, c_v^{ID}, ID)\), where \(0 < c_v^{ID} < n-1\) and \(c_h^{ID} = 0\), it can set up common keys with its three neighbor sensor nodes respectively. It has not left sensor node, its right sensor node is \(N_{ID+1}(c_h^{ID+1}, c_v^{ID+1}, ID+1)\), its above sensor node is \(N_{ID+n}(c_h^{ID+n}, c_v^{ID+n}, ID+n)\), and its below neighbor sensor node is \(N_{ID-n}(c_h^{ID-n}, c_v^{ID-n}, ID-n)\). The shared key between the sensor node \(N_{ID}\) \((c_h^{ID}, c_v^{ID}, ID)\) and its right sensor node is \(k_{N_{ID},N_{ID+1}}^R = f_{N_{ID}}(ID+1) = f_{N_{ID+1}}(ID)\), the shared key between the sensor node \(N_{ID}\) \((c_h^{ID}, c_v^{ID}, ID)\) and its below sensor node is \(k_{N_{ID},N_{ID-n}}^B = f_{N_{ID}}(ID-n) = f_{N_{ID-n}}(ID)\).
\[ k_{N_{ID,n}} (ID - n) = f_{N_{ID,n}} (ID) \]

The shared key between the sensor node \( N_{ID} (c_{v}, ID) \) and its above sensor node is \( k_{N_{ID,n}} (ID + n) = f_{N_{ID,n}} (ID) \).

For a sensor node \( N_{ID} (c_{h}^{ID}, c_{v}^{ID}, ID) \), where \( 0 < c_{h}^{ID} < n - 1 \) and \( c_{h}^{ID} = n - 1 \), it can set up common keys with its three neighbor sensor nodes respectively. Its left sensor node is \( N_{ID-1} \) \( (c_{h}^{ID-1}, c_{v}^{ID-1}, ID-1) \), its above sensor node is \( N_{ID+1} (c_{h}^{ID+1}, c_{v}^{ID+1}, ID + n) \), and its below neighbor sensor node is \( (c_{h}^{ID-n}, c_{v}^{ID-n}, ID - n) \), and it has not right sensor node. We can obtain similar results.

For a sensor node \( N_{ID} (c_{h}^{ID}, c_{v}^{ID}, ID) \), where \( 0 < c_{h}^{ID} < n - 1 \) and \( c_{v}^{ID} = n - 1 \), it can set up common keys with its three neighbor sensor nodes respectively. Its right sensor node is \( N_{ID-1} \) \( (c_{h}^{ID-1}, c_{v}^{ID-1}, ID-1) \), its above sensor node is \( N_{ID+1} (c_{h}^{ID+1}, c_{v}^{ID+1}, ID + 1) \), its below neighbor sensor node is \( (c_{h}^{ID-n}, c_{v}^{ID-n}, ID - n) \), and it has not above sensor node. We can obtain similar results.

For the sensor node \( N_{0}(0,0,0) \), it can set up common keys with its two neighbor sensor nodes respectively. Its right sensor node is \( N_{1}(1,0,1) \), its above sensor node is \( N_{n}(0,n,n) \), and it has not left sensor node and below sensor node. The shared key between the sensor node and its right sensor node is \( k_{0,1} = f_{N_{0}} (1) = f_{N_{n}} (0) \), and the shared key between the sensor node and its above sensor node is \( k_{0,n} = f_{N_{0}} (n) = f_{N_{n}} (0) \).

For the sensor node \( N_{n-1}(n - 1,0,n - 1) \), it can set up common keys with its two neighbor sensor nodes respectively. Its left sensor node is \( N_{n-2}(n - 2,0,n - 2) \), its above sensor node is \( N_{n-1}(n - 1,2n - 1) \), and it has not right sensor node and below sensor node. The shared key between the sensor node and its left sensor node is \( k_{n-1,n-2} = f_{N_{n-2}} (n - 2) = f_{N_{n-2}} (n - 1) \), the shared key between the sensor node and its above sensor node is \( k_{n-1,n-2} = f_{N_{n-2}} (2n - 1) = f_{N_{n-2}} (n - 1) \).

For the sensor node \( N_{n-1}(n - 1,0,n - 2) \), it can set up common keys with its two neighbor sensor nodes respectively. Its right sensor node is \( N_{n-2}(n - 1,2n - 1) \), its above sensor node is \( N_{n-2}(n - 2,2n - 2) \), and it has not left sensor node and above sensor node. The shared key between the sensor node and its right sensor node is \( k_{n-1,n-2} = f_{N_{n-2}} (n - 2) = f_{N_{n-2}} (n - 1) \), the shared key between the sensor node and its below sensor node is \( k_{n-1,n-2} = f_{N_{n-2}} (2n - 2n) = f_{N_{n-2}} (n - 1) \).

For the sensor node \( N_{n-1}(n - 1,0,n - 1) \), it can set up common keys with its two neighbor sensor nodes respectively. Its left sensor node is \( N_{n-2}(n - 2,0,n - 2) \), its below sensor node is \( N_{n-2}(n - 2,n - 2) \), and it has not right sensor node and above sensor node. The shared key between the sensor node and its left sensor node is \( k_{n-1,n-2} = f_{N_{n-2}} (n - 2) = f_{N_{n-2}} (n - 1) \), the shared key between the sensor node and its below sensor node is \( k_{n-1,n-2} = f_{N_{n-2}} (n - 2n) = f_{N_{n-2}} (n - 1) \).

### 3. Performance analysis for WSNs

#### 3.1 Security analysis for WSNs

For those sensor nodes \( N_{ID} (c_{h}^{ID}, c_{v}^{ID}, ID) \), where \( 0 < c_{h}^{ID} < n - 1 \) and \( 0 < c_{v}^{ID} < n - 1 \), they can set up shared keys with its four sensor nodes respectively and the four keys are different each other. For those sensor nodes \( N_{ID} (c_{h}^{ID}, c_{v}^{ID}, ID) \), where \( 0 < c_{h}^{ID} < n - 1 \) and \( c_{v}^{ID} = 0 \), \( N_{ID} (c_{h}^{ID}, c_{v}^{ID}, ID) \), where \( 0 < c_{v}^{ID} < n - 1 \) and \( c_{h}^{ID} = n - 1 \), and
$N_{ID}(c^{ID}_h, c^{ID}_v, ID)$, where $0 < c^{ID}_h < n - 1$ and $c^{ID}_v = n - 1$, they can set up common keys with their three neighbor sensor nodes respectively. Those keys are different each other. For the four sensor nodes, $N_0(0, 0, 0), N_{n-1}(n-1, 0, n-1), N_{n^2-n}(0, n-1, n^2-n)$ and $N_{n^2-1}(n-1, n-1, n^2-1)$, they can set up shared keys with their two neighbor sensor nodes respectively. Those keys are different each other. In all those cases, from the symmetric polynomials employed, it is more difficult to compromise those keys in this strategy than in the paper [4]. Additionally, if a sensor node are captured, its four keys, or three keys, or two keys are exposed. Namely, its neighbor sensor nodes are attacked next by the opponent will attack its neighbor sensor nodes. However, the opponent can not attack other sensor nodes because the opponent can not obtain their keys.

3.2 Connectivity analysis for WSNs

Each sensor node of $N_{ID}(c^{ID}_h, c^{ID}_v, ID)$, where $0 < c^{ID}_h < n - 1$ and $0 < c^{ID}_v < n - 1$, set up shared keys with its four sensor nodes respectively, and each sensor node of $N_{ID}(c^{ID}_h, c^{ID}_v, ID)$, where $0 < c^{ID}_h < n - 1$ and $c^{ID}_v = 0$, $N_{ID}(c^{ID}_h, c^{ID}_v, ID)$, where $0 < c^{ID}_v < n - 1$ and $c^{ID}_h = 0$, $N_{ID}(c^{ID}_h, c^{ID}_v, ID)$, where $0 < c^{ID}_v < n - 1$ and $c^{ID}_h = n - 1$, and $N_{ID}(c^{ID}_h, c^{ID}_v, ID)$, where $0 < c^{ID}_h < n - 1$ and $c^{ID}_v = n - 1$, set up shared keys with its three sensor nodes respectively. Each sensor node of $N_0(0, 0, 0)$, $N_{n-1}(n-1, 0, n-1), N_{n^2-n}(0, n-1, n^2-n)$ and $N_{n^2-1}(n-1, n-1, n^2-1)$ set up shared keys with its two sensor nodes. Moreover, for each of sensor node $N_{ID}(c^{ID}_h, c^{ID}_v, ID)$, where $0 < c^{ID}_h < n - 1$ and $0 < c^{ID}_v < n - 1$, even if three sensor nodes of its four neighbor sensor nodes are captured, it can set up with the neighbor sensor node which is not captured. Similarly, for each of sensor node of $N_{ID}(c^{ID}_h, c^{ID}_v, ID)$, where $0 < c^{ID}_h < n - 1$ and $c^{ID}_v = 0$, $N_{ID}(c^{ID}_h, c^{ID}_v, ID)$, where $0 < c^{ID}_v < n - 1$ and $c^{ID}_h = 0$, $N_{ID}(c^{ID}_h, c^{ID}_v, ID)$, where $0 < c^{ID}_v < n - 1$ and $c^{ID}_h = n - 1$, and $N_{ID}(c^{ID}_h, c^{ID}_v, ID)$, where $0 < c^{ID}_v < n - 1$ and $c^{ID}_h = n - 1$, even if two sensor nodes of its three neighbor sensor nodes are captured, it can set up with the neighbor sensor node which is not captured. For those sensor nodes $N_0(0, 0, 0)$, $N_{n-1}(n-1, 0, n-1), N_{n^2-n}(0, n-1, n^2-n)$ and $N_{n^2-1}(n-1, n-1, n^2-1)$, we can obtain similar results. Therefore, this scheme improves the network connectivity.

3.3 Storage analysis for WSNs

For sensor node $N_{ID}(c^{ID}_h, c^{ID}_v, ID)$, where $0 < c^{ID}_h < n - 1$ and $0 < c^{ID}_v < n - 1$, we let $I_1 = c^{ID}_h = c^{ID+1}_h - 1$ to calculate the shared key beteen the sensor node and its left neighbor sensor node, we let $I_1 = c^{ID}_v = h^{ID+1}_v - 1$ to calculate the shared key beteen the sensor node and its right neighbor node, we let $I_2 = c^{ID-n}_v = c^{ID}_v - n$ to calculate the shared key beteen the sensor node and its below neighbor node, and we let $I_2 = c^{ID+n}_v = c^{ID}_v + n$ to calculate the shared key beteen the sensor node and its above above neighbor sensor node. For other sensor nodes, there are similar results. Therefore, we can save sensor node storage and reduce the computation load for the sensor nodes.

4. Conclusion

A secure strategy for wireless sensor networks which locate in two-dimension square is given through using the symmetric polynomials. The sensing square locates in a two-dimension coordinate system. All sensor nodes are dispensed in the sensing square evenly. Each sensor node set up the common keys with its neighbor sensor nodes through utilizing the symmetric polynomials because one of its coordinates, the horizontal coordinate or the vertical coordinate, is equal to one of coordinates, the horizontal coordinate or the vertical coordinate, of the neighbor sensor nodes and the absolute value of difference between the two values, where one value is one of its coordinates, the horizontal coordinate or the vertical coordinate, and the other value one of coordinates, the horizontal coordinate or the vertical coordinate, of the neighbor sensor nodes, is 1 and The difference of the ID
value of the two neighbor sensor nodes is 1 or n. After each sensor node set up the keys with its neighbor sensor nodes, all sensor nodes in the sensing two-dimension area set up their common keys directly or indirectly. Analysis and comparison show this scheme enhances the wireless sensor network security and the connectivity, saves sensor node storage and reduces the sensor node computation load.

Acknowledgements

This work was supported by the colleges and universities in Shandong province science and technology plan project number J13LN05.

References


