Unconditionally Secure Fully Connected Key Establishment Using Deployment Knowledge

Sarbari Mitra, Sourav Mukhopadhyay, Ratna Dutta

Unconditionally Secure Fully Connected Key Establishment using Deployment Knowledge

Sarbari Mitra, Sourav Mukhopadhyay and Ratna Dutta
{sarbari,sourav,ratna}@maths.iitkgp.ernet.in

Department of Mathematics
IIT Kharagpur, India

Abstract. We propose a key pre-distribution scheme to develop a well-connected network using deployment knowledge where the physical location of the nodes are pre-determined. Any node in the network can communicate with any other node by establishing a pairwise key when the nodes lie within each other's communication range. Our proposed scheme is unconditionally secure against adversarial attack in the sense that no matter how many nodes are compromised by the adversary, the rest of the network remains perfectly unaffected. On a more positive note, our design is scalable and provides full connectivity.
Keywords : sensor network, bivariate symmetric polynomial.

1 Introduction

Wireless Sensor Networks (WSN) are built up of resource-constrained, battery powered, small devices, known as sensors, which have capability of wireless communication over a restricted target field. Due to its immense application from home front to battle field, environment monitoring such as water quality control, landslide detection, air pollution monitoring etc., key distribution in sensor network has become an active area of research over the past decade. Usually sensor networks are meant to withstand harsh environments and thus secret communication is very essential. The secret keys are assigned to the nodes before their deployment in a Key Pre-distribution Scheme (KPS) to enable secure communication.

The bivariate symmetric polynomials were first used in key distribution by Blundo et al. [1]. The scheme is t-secure, i.e., the adversary cannot gain any information about the keys of the remaining uncompromised nodes if the number of compromised nodes does not exceed t. However, if more than t nodes are captured by the adversary, the security of the whole network is destroyed. Blundo's scheme is used as the basic building block in the key pre-distribution schemes proposed in [5, 6].

We present a deployment knowledge based KPS in a rectangular grid network by dividing the network in subgrids and applying Blundo's polynomial based KPS in each subgrid in such a way that nodes within communication range of each other can establish pairwise key. The induced network is fully connected – any two nodes, lying within communication range of each other, are able

to communicate privately by establishing a secret pairwise key. The t-secure property of Blundo's scheme is utilized. A t-degree polynomial is assigned to at most $(t-1)$ nodes, where at least $(t+1)$ shares are required to determine the polynomial. This results in an unconditionally secure network, i.e., the network is completely resilient against node capture and this is independent of the number of nodes compromised. The nodes need to store at least $(t+1)\log q$ bits (where q is large prime) and a fraction of the total nodes needs to store at most $4(t+1)\log q$ bits. The storage requirement decreases with decreased radio frequency radius of the nodes. Comparison of the proposed scheme with existing schemes indicates that our network provides better connectivity, resilience and sustains scalability, with reasonable computation and communication overheads and slightly large storage for few nodes.

2 Our Scheme

Subgrid Formation : The target region is an $r \times c$ rectangular grid with r rows and c columns i.e., there are c cells in each row and r cells in each column of the grid. Each side of a cell is of unit length. A node is placed in each cell of the grid. Thus the network can accommodate at most rc nodes. Each of the $N(\leq rc)$ nodes are assigned a unique node identifier. All the nodes have equal communication range. Let ρ be the radius of communication range and d be the density of the nodes per unit length. Then $m = \rho d$ is the number of nodes lying within the communication radius of each node. We divide this network into a set of overlapping rectangular subgrids $SG_{i,j}$, for $i, j \geq 1$, of size $(2m+1) \times (2m+1)$ each. Each subgrid contains $(2m+1)^2$ cells and two adjacent subgrids overlap either in m rows or in m columns. By $N_{x,y}$ we denote the node at row x and column y in our rectangular grid. Deployment knowledge is used to get the idea about the location of the nodes after their deployment in the target field. We have designed the network to enable any pair of nodes lying in the radio frequency range of each other to be in at least one common subgrid. From the construction, t , according to our assumption. Let us assume that $R_i,\ 1 \leq i \leq r$ is the i^{th} row and $C_j,\ 1 \leq j \leq c$ is the j^{th} column of the rectangular grid. We refer a node to be *covered*, if it shares at least one common subgrid with each node within its communication range. Note that the nodes that lie at the intersection of the rows $R_i (1 \leq i \leq m)$ and columns C_j $(1 \leq i \leq m)$ are covered by subgrid $SG_{1,1}$. We consider sub-grid $SG_{1,2}$ and $SG_{2,1}$ overlap with $SG_{1,1}$ in m columns and m rows respectively, so that the nodes at the intersection of R_i and C_j, for $\{1 \leq i, j \leq 2m+1\} \setminus \{1 \leq i, j \leq m\}$, are made covered. Similarly, $SG_{2,2}$ intersects $SG_{1,2}$ and $SG_{2,1}$ in m rows and m columns respectively. This automatically covers all the nodes $N_{x,y}$ for $1 \leq x, y \leq 2m+2$. The overlapping of subgrids are repeated as described above to make all the nodes in the network covered.

Polynomial Share Distribution : Now, we apply Blundo's KPS in each subgrid. We choose randomly a bivariate symmetric polynomial $f_{ij}(x, y)$ of

degree $t > (2m+1)^2$ for subgrid $SG_{i,j}$, $i, j \geq 1$ and distribute univariate polynomial shares of the polynomial $f_{ij}(x, y)$ to each of the $(2m+1)^2$ nodes. Thus any node with identifier ID in subgrid $SG_{i,j}$ receives its polynomial share $P_{\mathsf{ID}}(y) = f_{ij}(\mathsf{ID}, y)$ and is able to establish pairwise keys with the remaining nodes in $SG_{i,j}$ following Blundo's scheme.
Now, let us discuss the scheme in detail for $m = 1$ in the following example.
Example: when $m = 1$

Lemma 21 The subgrid $SG_{i,j}$ consists of $(2m+1)^2 = 9$ nodes $N_{x,y}$, where $2i-1 \leq x \leq 2i+1$ and $2j-1 \leq y \leq 2j+1$.

Proof. From Figure 1, it follows that the result holds for $SG_{1,1}$. Without loss of generality, let us assume that the result is true for $i = i_1$ and $j = j_i$, i.e., the nine nodes of the subgrid SG_{i_1,j_1} are given by $N_{x,y}$, where $2i_1-1 \leq x \leq 2i_1+1$ and $2j_1-1 \leq y \leq 2j_1+1$.

Now we consider the subgrid SG_{i_1+1,j_1}. Each of the sub-grid are in the form of a 3×3 grid. From the construction it follows that the columns of SG_{i_1,j_1} and SG_{i_1+1,j_1} are identical, and they overlap in only one row (since $m = 1$), i.e., R_{2i_1+1}, which can also be written as $R_{2(i_1+1)-1}$. Therefore, SG_{i_1+1,j_1} consists of the nine nodes lying at the intersection of the rows $R_{2(i_1+1)-1}$, $R_{2(i_1+1)}$ and $R_{2(i_1+1)+1}$; and the columns C_{2j_1-1}, C_{2j_1} and C_{2j_1+1}. Thus the nodes of SG_{i_1+1,j_1} are given by $N_{x,y}$, where $2(i_1+1)-1 \leq x \leq 2(i_1+1)+1$ and $2j_1-1 \leq y \leq 2j_1+1$. Similarly, it can be shown that the rows of SG_{i_1,j_1} and SG_{i_1,j_1+1} are identical and they overlap in the column C_{2j_1+1}, which can also be represented as $C_{2(j_1+1)-1}$. Proceeding in the similar manner the nine nodes of the subgrid SG_{i_1,j_1+1} are $N_{x,y}$, where $2i_1-1 \leq x \leq 2i_1+1$ and $2(j_1+1)-1 \leq y \leq 2(j_1+1)+1$.
Thus the result holds for the subgrid SG_{i_1+1,j_1} and SG_{i_1,j_1+1}, whenever it is true for the subgrid SG_{i_1,j_1}. Also the result holds for $SG_{1,1}$. Hence, by the principle of mathematical induction, the result holds for subgrid $SG_{i,j}$, for all values of i, j. □

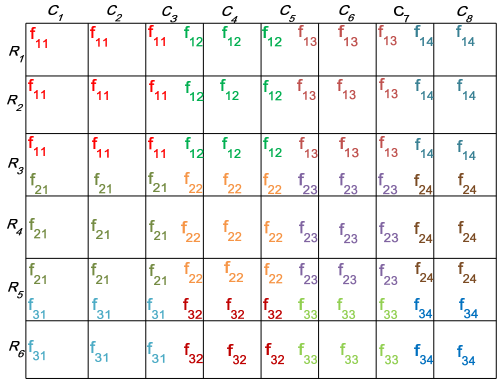

Fig. 1. Polynomial assignment to 3×3 overlapping sub-grid in a network, where $m = 1$

Lemma 22 Let univariate share of the bivariate symmetric polynomial f_{ij} be assigned to the node $N_{x,y}$.

(i) Let both x and y be even. Then $i = \frac{x}{2}, j = \frac{y}{2}$.

(ii) Let x be even and y be odd. Then $i = \frac{x}{2}$ and $j = \begin{cases} 1, & \text{if } y = 1; \\ \frac{y-1}{2}, \frac{y+1}{2}, & \text{otherwise .} \end{cases}$

(iii) Let x be odd and y be even. Then $j = \frac{y}{2}$ and $i = \begin{cases} 1, & \text{if } x = 1; \\ \frac{x-1}{2}, \frac{x+1}{2}, & \text{otherwise .} \end{cases}$

(iv) Let both x and y be odd. Then $\begin{cases} i = 1, j = 1, & \text{if } x = 1, y = 1; \\ i = 1, j = \frac{y-1}{2}, \frac{y+1}{2}, & \text{if } x = 1, y \neq 1; \\ i = \frac{x-1}{2}, \frac{x+1}{2}, j = 1, & \text{if } x \neq 1, y = 1; \\ i = \frac{x-1}{2}, \frac{x+1}{2}, j = \frac{y-1}{2}, \frac{y+1}{2}, & \text{otherwise .} \end{cases}$

Proof. From the construction of the scheme, it follows that univariate shares of the bivariate symmetric polynomial f_{ij} are distributed to each of the nine nodes of the subgrid $SG_{i,j}$. Thus our target is to find the coordinates of the subgrid $SG_{i,j}$ to which a node $N_{x,y}$ belong. Lemma 21 suggests that sub-grid $SG_{i,j}$ consists of the nodes $N_{x,y}$, for $2i - 1 \leq x \leq 2i + 1$ and $2j - 1 \leq y \leq 2j + 1$. Hence possible values of i are $\frac{x-1}{2}$, $\frac{x}{2}$ and $\frac{x+1}{2}$. Since i is an integer we must have $i = \frac{x}{2}$, when x is even and $i = \frac{x-1}{2}$ and $\frac{x+1}{2}$ when x odd. We further observe from Figure 1 that the first coordinate of all the subgrids and hence that of the corresponding bivariate polynomials assigned to the nodes lying in the first row is always 1. Similarly, possible values of j are $\frac{y-1}{2}$, $\frac{y}{2}$ and $\frac{y+1}{2}$, follows from Lemma 21. As j is also an integer we have $j = \frac{y}{2}$, when y is even and $j = \frac{y-1}{2}$ and $\frac{y+1}{2}$ when y is odd. We also observe from the Figure 1 that the second coordinate of all the subgrids and hence that of the corresponding bivariate polynomials assigned to the nodes lying in the first column is always 1, according to the construction of our design. Hence,

$$i = \begin{cases} 1, & \text{if } x = 1; \\ \frac{x}{2}, & \text{if } x \text{ is even;} \\ \frac{x-1}{2} \text{ and } \frac{x+1}{2}, & \text{otherwise,} \end{cases} \quad \text{and} \quad j = \begin{cases} 1, & \text{if } y = 1; \\ \frac{y}{2}, & \text{if } y \text{ is even;} \\ \frac{y-1}{2} \text{ and } \frac{y+1}{2}, & \text{otherwise .} \end{cases}$$

Hence, combining all the possible cases for the combination of the values of x and y we obtain the expression given in the statement of the Lemma. □

Theorem 23 We define the following variables for our $r \times c$ rectangular grid structure where K is the total number of symmetric bivariate polynomial required, M_1, M_2 and M_3 denote the total number of nodes containing only one, two or four polynomial shares respectively. We further identify the following cases as : *Case I* : – r and c both are odd; *Case II* : – r is odd and c is even; *Case III* : – r is even and c is odd and *Case IV* : – r and c both are even. Then

	K	M_1	M_2	M_3
Case I	$\frac{1}{4}(r-1)(c-1)$	$\frac{1}{4}(r+3)(c+3)$	$\frac{1}{4}(r-3)(c-3)$	$\frac{1}{2}(rc-9)$
Case II	$\frac{1}{4}(r-1)c$	$\frac{1}{4}(r+3)(c+2)$	$\frac{1}{4}(r-3)(c-2)$	$\frac{1}{2}(rc-6)$
Case III	$\frac{1}{4}r(c-1)$	$\frac{1}{4}(r+2)(c+3)$	$\frac{1}{4}(r-2)(c-3)$	$\frac{1}{2}(rc-6)$
Case IV	$\frac{1}{4}rc$	$\frac{1}{4}(r+2)(c+2)$	$\frac{1}{4}(r-2)(c-2)$	$\frac{1}{2}(rc-4)$

Proof. We provide the proofs in (a) and (b) for the expressions of K and M_1 respectively given in the table and leave the other two for page restrictions.

(a) According to the description of the scheme, each subgrid corresponds to a distinct bivariate polynomial, hence, the total number of polynomials required is equal to the total number of sub-grid present in the network. Let us assume that the sub-grid form a matrix consisting of r_1 rows and c_1 columns. Thus, we must have $K = r_1 c_1$.
This also follows from the construction that the subgrids are numbered in such a way that the coordinates of the k^{th} node of the subgrid $SG_{i,j}$ is less than or equal to the coordinates of the k^{th} node of the subgrid $SG_{i',j'}$, for $1 \leq k \leq 9$, whenever $1 \leq i \leq i' \leq r_1$ and $1 \leq j \leq j' \leq c_1$. According to the assumption, $N_{r,c} \in SG_{r_1,c_1}$. From Lemma 21 it follows that $2r_1 - 1 \leq r \leq 2r_1 + 1$ and $2c_1 - 1 \leq c \leq 2c_1 + 1$. Hence we must have $r_1 \geq \frac{r-1}{2}$ and $c_1 \geq \frac{c-1}{2}$. Since, r_1 and c_1 are integers (according to the assumption), we have

$$r_1 = \begin{cases} \frac{r-1}{2}, & \text{when } r \text{ is odd;} \\ \frac{r}{2}, & \text{when } r \text{ is even .} \end{cases} \text{ and } c_1 = \begin{cases} \frac{c-1}{2}, & \text{when } c \text{ is odd;} \\ \frac{c}{2}, & \text{when } c \text{ is even .} \end{cases}$$

Hence, considering the possible combinations from the above cases and substituting the values in the equation $K = r_1 c_1$, we obtain the expression given in the first column of the table given in the statement of the theorem.

(b) Let the node $N_{x,y}$ for $1 \leq x \leq r$, $1 \leq y \leq c$, stores exactly one univariate polynomial share. The possible values of x and y depends respectively on the number of rows r and number of columns c in the rectangular grid. Then it follows from the construction and can be verified from Figure 1 that

$$x \in \begin{cases} \{1, 2, \ldots, r\} \setminus \{2k+1 : 1 \leq k \leq \frac{r-3}{2}\}, & \text{when } r \text{ is odd;} \\ \{1, 2, \ldots, r\} \setminus \{2k+1 : 1 \leq k \leq \frac{r}{2} - 1\}, & \text{when } r \text{ is even .} \end{cases}$$

Hence, we get $\frac{r+3}{3}$ and $\frac{r+2}{3}$ possible cases for r being odd and even respectively. Similarly, we get $\frac{c+3}{3}$ cases when c is odd and $\frac{c+2}{3}$ cases when c is even. Hence, considering the possible combinations from the above cases and multiplying the corresponding values, we obtain the expression given in the second column of the table given in the statement of the theorem.

□

Resilience quantifies the robustness of the entwork against node capture. We consider the attack model as the random node capture, where the adversary captures nodes randomly, extracts the keys stored at them. Blundo's scheme has the t-secure property, as the adversary will not be able to gain any information if less than t nodes are compromised when univariate shares from a t-degree bivariate polynomial are assigned to the nodes. Here, we have assigned univariate shares of a t-degree bivariate polynomial where $t > (2m+1)^2$, to at most $(2m+1)^2$ nodes in a subgrid. Hence, even if upto $(2m+1)^2 - 2 = 4m^2 + 4m - 1$ nodes are captured by the adversary, the remaining two nodes will still be able to establish a pairwise key, which is still unknown to the adversary. This happens to all the pairwise independent bivariate polynomials. Hence, the network is unconditionally secure, i.e., no matter how many nodes are captured by the adversary, remaining network will remain unaffected.

Comparison : In Table 1, we provide the comparison of our scheme with the existing schemes proposed by Blundo et al. [1], Liu and Ning [6], Das and Sengupta [3] and Sridhar et al. [7]. Here, t denotes degree of the bivariate polynomial;

q stands for the order of the underlying finite field $\mathbb{F}_q$; N is the total number of nodes in the network; s denotes the number of nodes compromised by the adversary and t in [3] is assumed to be sufficiently larger than $\sqrt{N}$, $c^{'}$ is a constant and $\mathcal{F}$ is the total number of polynomials in [6].

Schemes	Deployment Knowledge	Storage	Comm. Cost	Comp. Cost	Full Connectivity	Resilience	Scalable
[1]	No	$(t+1)\log q$	$O(\log N)$	$t+1$	Yes, 1-hop	t-secure	No
[6]	Yes	$c^{'}(t+2)\log q$	$c^{'}\log \lvert\mathcal{F}\rvert$	$t+1$	No	t-secure	No
[3]	No	$(t+2)\log q$	$O(\log N)$	$t+1$	Yes, 2-hop	secure	To some extent
[7]	No	$4(t+1)\log q$	$O(\log N)$	$O(t\log^2 N)$	No	depends on s	Yes
Ours	Yes	$\leq 4(t+1)\log q$	$O(\log N)$	$t+1$	Yes, 1-hop	secure	Yes

Table 1. Comparison with existing schemes

3 Conclusion

Utilizing the advantage of deployment knowledge and t-secure property of Blundo's polynomial based scheme, we design a network, which requires reasonable storage to establish a pairwise key between any two nodes within radio frequency range. The network is unconditionally secure under adversarial attack and can be scaled to a larger network without any disturbance to the existing nodes in the network.

References

1. Blundo C., Santis A. D., Herzberg A., Kutten S., Vaccaro U., Yung M. : Perfectly-secure Key distribution for Dynamic Conferences. *Advances in Cryptology-CRYPTO'92*, LNCS 740, pp: 471-486,(1993).
2. Chan H., Perrig A., and Song D. X.: Random Key Predistribution Schemes for Sensor Network. *In IEEE Symposium on Security and Privacy*, pp: 197-213, (2003).
3. Das A. K. and Sengupta I.: An Effective Group-Based Key Establishment Scheme for Large-Scale Wireless Sensor Networks using Bivariate Polynomials. *COMSWARE 2008* pp:9-16, (2008).
4. Das A. K.: An Unconditionally Secure Key Management Scheme for Large-Scale Heterogeneous Wireless Sensor Networks. *CoRR abs/1103.4678* (2011).
5. Li G., He J., and Fu W. Y. : A Hexagon-Based Key Predistribution Scheme in Sensor Networks. *International Conference on Parallel Processing Workshops (ICPPW'06)* ,pp.175-180, (2006).
6. Liu D., and Ning P. : Improving Key Pre-Distribution with Deployment Knowledge in Static Sensor Networks. *ACM Transactions on Sensor Networks*, vol. 1, no. 2, pp. 204-239, (2005).
7. Sridhar V., Raghavendar V. : Key Predistribution Scheme for Grid Based Wireless Sensor Networks using Quadruplex Polynomial Shares per Node. *Procedia Computer Science* 5, pp. 132-140, (2011).