Predistribution Scheme for Establishing Group Keys in Wireless Sensor Networks

Lein Harn and Ching-Fang Hsu

***Abstract*—Special designs are needed for cryptographic schemes in wireless sensor networks (WSNs). This is because sensor nodes are limited in memory storage and computational power. In 1992, Blundo *et al.* proposed a noninteractive group key establishment scheme using a multivariate polynomial. Their scheme can establish a group key of m sensors. Since each share is a polynomial involving $m-1$ variables and having degree k, each sensor needs to store $(k+1)^{m-1}$ coefficients from GF(p), which is exponentially proportional to the size of group. This makes their scheme only practical when $m=2$ for peer-to-peer communication. So far, most existing predistribution schemes in WSNs establish pairwise keys for sensor nodes. In this paper, we propose a novel design to propose a predistribution scheme for establishing group keys in WSNs. Our design uses a special-type multivariate polynomial in Z_N, where N is a RSA modulus. The advantage of using this type of multivariate polynomial can limit the storage space of each sensor to be $m(k+1)$, which is linearly proportional to the size of group communication. In addition, we prove the security of the proposed scheme and show that the computational complexity of the proposed scheme is efficient.**

***Index Terms*—Wireless sensor networks, group keys, pre-distribution keys, multi-variate polynomials, RSA.**

I. INTRODUCTION

WIRELESS sensor networks (WSNs) have been developed in wide range of data acquisitions in battle fields, human body [1], [2], hazardous environments, etc. Most sensor nodes are small, low-cost, and low-power devices [3]. Sensors are randomly deployed without knowing their locations in prior of the deployment. Since sensors are low-cost, limited in both memory storage and computational power, it is a challenging research problem to develop cryptographic schemes suitable for WSNs.

Most research papers in WSNs propose schemes establish pairwise keys for sensors. We can classify key establishment schemes in WSNs into two types, the *probabilistic schemes* and the *deterministic schemes*. The probabilistic scheme do not guarantee connectivity in WSNs. Eschenauer and Gligor proposed [4] the first *Random Key Pre-distribution scheme*. In their scheme, each sensor is pre-loaded with a key ring of k keys randomly selected from a large pool S of keys. After the deployment, if two neighbors share at least one key, they establish a secure link and compute their session secret key which is one of the common keys. Otherwise, they should determine a secure path which is composed by successive secure links. The values of the key ring size k and the key pool size $|S|$ are chosen in such a way that the intersection of two key rings is not empty with a high probability. However, if the sensors are progressively corrupted, the attacker may discover a large part or the whole global key pool. Hence, a great number of links will be compromised. Chan et al. [5] proposed a protocol called *Q-composite scheme* that enhances the resilience of the random key scheme. In this solution, two neighboring nodes can establish a secure link only if they share at least Q keys. This approach enhances the resilience against node capture attacks because the attacker needs more overlap keys to break a secure link. However, this approach degrades the network secure connectivity coverage because neighboring nodes must have at least Q common keys to establish a secure link. Chan et al. [5] proposed a pairwise key pre-distribution scheme to protect the resiliency against node capture and each captured node does not reveal any information about external links. The main drawback of their scheme is the non-scalability because the number of the stored keys depends linearly on the network size. This property will cause implementation issue of the scheme if the number of sensors in network is very large. In this paper, we propose a scheme that the storage size of each sensor is independent of the network size. Du et al. [6] proposed an enhanced random scheme assuming the node deployment knowledge. However, the application of this scheme is restrictive if the deployment knowledge is not possible. Rasheed and Mahapatra [7] proposes two key pre-distribution schemes based on the polynomial pool-based key pre-distribution scheme, the probabilistic generation key pre-distribution scheme, and the Q-composite scheme. Their schemes perform better in terms of network resilience to node capture than existing schemes if used in WSNs with mobile sinks. In 2013, Ruj et al. [8] proposed the first triple key establishment in WSNs. Any three sensors can establish unique triple keys among them. Recently, Li and Xiong [9] proposed a heterogeneous online and offline signcryption scheme to secure communication between a sensor node and an Internet host. Their scheme is based on the bilinear pairing.

Manuscript received January 23, 2015; revised April 24, 2015; accepted April 30, 2015. Date of publication May 4, 2015; date of current version July 21, 2015. This work was supported by the Self-Determined Research Funds of Central China Normal University through the Colleges Basic Research and Operation within the Ministry of Education under Grant CCNU15A02018. The associate editor coordinating the review of this paper and approving it for publication was Prof. Okyay Kaynak. *(Corresponding author: Ching-Fang Hsu.)*

L. Harn is with the Department of Computer Science and Electrical Engineering, University of Missouri–Kansas City, Kansas City, MO 64110 USA (e-mail: harnl@umkc.edu).

C.-F. Hsu is with the Department of Computer Science, Central China Normal University, Wuhan 430079, China (e-mail: cherryjingfang@gmail.com).

Digital Object Identifier 10.1109/JSEN.2015.2429582

The deterministic schemes do guarantee the connectivity in WSNs. Most deterministic schemes are based on threshold cryptography. Blom [10] proposed the first pairwise key establishment scheme based on threshold cryptography and Blundo et al. [11] further investigated the key establishment using polynomials. In Blum's scheme, every sensor node is preloaded with coefficients of a symmetric bivariate polynomial evaluated at one of its variables using its identification value. The symmetry property of a polynomial allows every node to establish a pairwise key with every neighbor node. For an adversary to compromise a communication link between two non-compromised nodes, it must capture at least a certain number of sensors (i.e, the threshold) to reconstruct the bivariate polynomial from its shares stored in the nodes and then break the system. For a polynomial of degree t, the scheme provides unconditionally secure if no more than $t-1$ sensors collude. Liu et al. [12] developed a general framework for pairwise key establishment based on the polynomial-based key pre-distribution protocol [11] and the probabilistic key distribution in [4] and [5]. Their scheme provided a higher probability for non-compromised sensors to establish secure communication links than that demonstrated in previous schemes. Khan et al. [13] proposed a pre-distribution scheme using a symmetric matrix and a generator matrix of maximum rank distance to establish pairwise keys for sensor nodes.

In this paper, we propose a novel pre-distribution scheme for establishing group keys in WSNs. Our scheme uses a special type of multi-variate polynomial to minimize the storage requirement of sensors. In addition, an adversary trying to compromise a communication link between two non-compromised nodes must capture at least a certain number of sensors to reconstruct the polynomial from its shares stored in the nodes. Since polynomial computations are very efficient, our proposed scheme is especially suitable for key establishment in WSNs.

Here, we summarize contributions of our paper.

- A pre-distribution scheme of group keys in WSNs is proposed.
- The scheme is based on a special type of multi-variate polynomial with minimum amount of memory storage and low computations.
- An adversary must capture at least a certain number of sensors in order to place a successful attack in WSNs.

The rest of paper is organized as follows. In Section 2, we review Blundo et al. scheme [11] based on multi-variate polynomials. The model of our proposed scheme is introduced in Section 3, including scheme description, type of adversaries and security features of proposed scheme. The scheme is presented in Section 4. The conclusion is given in Section 5.

II. Review of Blundo et al. Scheme [11]

In 1992, Blundo et al. [11] proposed a non-interactive k-secure m-member group key establishment scheme using a multi-variate polynomial. Their scheme can establish a group key of $m$sensors. A scheme is said to be k-secure if any $k$sensors have been captured and compromised their shares, the adversary has no information on shares stored in other sensors. The key distribution center (KDC) is responsible to pick a symmetric m-variate polynomial having degree k, $F(x_1, x_2, ..., x_m) = \sum_{0 \le j_1, ... j_m \le k} a_{j_1, ... j_m}(x_1)^{j_1}(x_2)^{j_2}...(x_m)^{j_m}$. and generates shares, $f_i(x_2, ..., x_m) = F(i, x_2, ..., x_m) = \sum_{0 \le j_2, ... j_m \le k} b_{j_2, ... j_m}(x_2)^{j_2}...(x_m)^{j_m}, i = 1, 2, ..., n$, for sensors. Later, each sensor can use its share to establish a group communication involving m sensors. In [11], it has shown that the k-secure 2- member scheme is a special case of Blom's scheme [10]. Since each share is a polynomial involving *m-1* variables and having degree k, each sensor needs to store $(k+1)^{m-1}$ coefficients from $GF(p)$, where $GF(p)$ is the finite field with p elements (also called the ***Galois Field***). The storage space of each sensor is exponentially proportional to the size of group. For example, to establish a group communication involving 10 sensors (*m=10*), the KDC picks a symmetric *10*-variate polynomial having degree *5 (k=5)*, which can resist attacks up to *5* sensors been captured. The storage of each sensor is $(6)^9$ integers from $GF(p)$, where p is at least a 100-bit prime. This makes their scheme only practical when $m = 2$ for peer-to-peer communication.

However, the k-secure 2-member protocol is a special case of Blundo et al. scheme and this scheme is based on a symmetric bivariate polynomial. A bivariate polynomial with degree k is defined as $F(x, y) = a_{0,0}+a_{1,0}x+a_{0,1}y+a_{2,0}x^2+a_{1,1}xy+a_{0,2}y^2+...++a_{t-1,0}x^{t-1}+a_{t-2,1}x^{t-2}y+...+a_{k,k}x^k y^k \bmod p$, where $a_{i,j} \in GF(p)$. If the coefficients satisfy $a_{i,j} = a_{j,i}, \forall i, j$, it is a symmetric bivariate polynomial. The KDC generates shares, $F(x_i, y), i = 1, 2, ..., n$, for sensors, where x_i is the public information associated with each sensor, U_i. Each share, $F(x_i, y)$, is a univariate polynomial with degree k. Note that shares generated in this way, since $F(x_i, x_j) = F(x_j, x_j)$, a pairwise secret key can be established between any pair of sensors U_i and U_j. The storage space of each sensor is to store $k+1$ coefficients from $GF(p)$. This special case can significantly limit the size of stored information for each sensor. Since then, key distribution schemes [12], [14]–[17] using symmetric bivariate polynomial has been widely adopted in WSNs. There are some key establishment schemes that use polynomials other than a bivariate polynomial. For example, the key establishment scheme proposed by Zhou and Fang [18] is based on a *tri*-variate polynomial and the scheme proposed by Fanian et al. [19] is based on an m-variate polynomial. However, both schemes can only establish a secret key for two sensors.

III. Model of Proposed Group Key Establishment Scheme

In this section, we describe the model of our proposed group key establishment scheme including the scheme description, the adversary and security properties of our proposed scheme. Figure 1 illustrates a sensor networks consisting multiple secure group communications.

A. Scheme Description

Number In our proposed scheme, there has a mutually trusted KDC and there are n sensors, $\{U_1, U_2, ..., U_n\}$. Each sensor is to pre-load shares by a KDC initially. The KDC

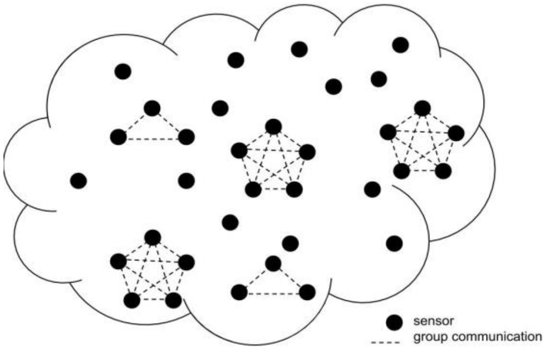

Fig. 1. Sensor network.

selects a special type of m-variate polynomial and generates shares. Shares of each sensor are $m-1$ univariate polynomials. In order to establish a secure group communication involving m (i.e., $2 \leq m \leq n$) sensors, the group key is computed by each sensor in the group communication using its shares. There is no interaction with other sensors to compute the group key. Thus, our proposed scheme is very efficient in group key establishment since there is no additional communication. Furthermore, the group key computation of each sensor needs only polynomial computations which are much faster than public-key computations. We will give detail discussion in performance evaluation of the proposed scheme.

B. Type of Adversaries

We consider two types of attacks: inside and outside attacks. The inside attack is implemented by an adversary who has captured sensors and recovered their stored shares. From the inside attack, the adversary may try to recover other sensors' shares and then use these recovered shares to obtain other group keys. On the other hand, the outside attack is implemented by an adversary who has no knowledge of any valid shares. An adversary may try to recover shares of sensors or the group keys. This attack is related to the secrecy of group keys. In security analysis, we will show that none of these attacks can work properly against our scheme.

C. Security Features of Proposed Scheme

We consider the following security features of group keys.

(a) *Correctness:* The group key can be computed by each sensor in a group communication involving m (i.e., $2 \leq m \leq n$) sensors.

(b) *k-Secure:* If any k sensors are captured, there has no information on shares of other sensors.

(c) *Key Confidentiality:* It is computationally infeasible for any outside attacker to discover any group key.

(d) *Key Independence:* Knowing a subset of group keys, $K' \subset K$, where k is the complete set of group keys, the adversary cannot discover any other group keys, $K''=K-K'$.

IV. Proposed Scheme

In this paper, we propose a group key establishment scheme using a multi-variate polynomial in Z_N, where N is a RSA modulus [20]. The advantage of using this type of multi-variate polynomial can limit the storage space of each sensor to be $m(k+1)$ coefficients which is linearly proportional to the size of group.

Scheme 1

Shares generation

Step 1. The KDC selects a random polynomial having degree k as $f(x) = a_k x^k + \ldots + a_1 x + a_0 \bmod N$, where $a_i \in (0, N)$. The *tri*-variate polynomial is $F(x_1, x_2, x_3) = \prod_{i=1}^{3} f(x_i) \bmod N$.

Step 2. For each sensor $P_{i,}$ KDC first computes $f(i)$ mod N, where i is a public information associated with the sensor, P_i. Then KDC randomly selects an integer, $f_{i,1}(i)$, in Z_N and solves $f_{i,2}(i)$ satisfying $f_{i,1}(i) \cdot f_{i,2}(i) = f(i) \bmod N$. KDC computes shares, $s_{i,1}(x) = f_{i,1}(i) f(x) \bmod N$ and $s_{i,2}(x) = f_{i,2}(i) f(x) \bmod N$. Shares are stored in sensor P_i secretly.

Group key establishment

We assume that three sensors, $\{P_1, P_2, P_3\}$, want to establish a secret group key among them. Each sensor P_j, where $j \in \{1, 2, 3\}$, uses its shares, $\{s_{j,1}(x), s_{j,2}(x)\}$, to compute $K = s_{j,1}(i_1) \cdot s_{j,2}(i_2) \bmod N$, where $i_1, i_2 \in \{1, 2, 3\} - \{j\}$ and $i_1 \neq i_2$.

The KDC picks a RSA modulus N, where N is the product of two large safe primes, p and q, i.e., $p=2p'+1$ and $q=2q'+1$, where p' and q' are also primes. p and q are KDC's secrets, N is made publicly known. The following RSA assumption assumes that it is computationally infeasible to factor the product of two large primes.

Definition 1 (RSA Assumption [20]): It is computationally infeasible to compute M given only the cipher text $C = M^e \, mod N$ and RSA public key (N, e).

A. Group Key Establishment Scheme for 3 Sensors

In the following discussion, we assume that the size of a group communication is limited to be three so a *tri*-variate polynomial is used by the KDC to generate shares of sensors. This scheme, *Scheme 1*, can be generalized in the next sub-section to a group communication involving m sensors by using a m-variate polynomial, *Scheme 2*.

Note that the shares, $(s_{j,1}(x), s_{j,2}(x))$, of each sensor are two univariate polynomials. Each sensor needs to store $2(k+1)$ coefficients from Z_N. In the following sub-section, we generalize this group key establishment scheme involving three sensors to m sensors.

B. Group Key Establishment Scheme for m Sensors

In the following discussion, we assume that the size of a group is limited to be m sensors so a m-variate polynomial is used by the KDC to generate shares of sensors.

Note that the shares, $\{s_{j,1}(x), s_{j,2}(x), \ldots, s_{j,m-1}(x)\}$, of each sensor are $m-1$ univariate polynomials. Thus, each sensor needs to store $(m-1)(k+1)$ coefficients from Z_N.

Scheme 2

Shares generation

Step 1. The KDC selects a random polynomial having degree k as $f(x) = a_k x^k + ... + a_1 x + a_0 \bmod N$, where $a_i \in (0, N)$. The m-variate polynomial is $F(x_1, x_2, ..., x_m) = \prod_{i=1}^{m} f(x_i) \bmod N$.

Step 2. For each sensor $P_{i,}$ KDC first computes $f(i) \bmod N$, where i is a public information associated with the sensor P_i. Then KDC randomly selects integers, $\{f_{i,1}(i), f_{i,2}(i), ..., f_{i,m-2}(i)\}$, where each integer is in Z_N, and solves $f_{i,m-1}(i)$ satisfying $f_{i,1}(i) \cdot f_{i,2}(i) \cdot ... \cdot f_{i,m-1}(i) = f(i) \bmod N$. KDC computes shares, $\{s_{i,1}(x), s_{i,2}(x), ..., s_{i,m-1}(x)\}$, where $s_{i,j}(x) = f_{i,l}(i) f(x) \bmod N$, for $l = 1, 2, ..., m-1$. Shares are stored in sensor P_i secretly.

Group key establishment

We assume that m sensors, $\{P_1, P_2, ..., P_m\}$, want to establish a secret group key among them. Each sensor P_j, where $j \in \{1, 2, ..., m\}$, uses its shares, $\{s_{j,1}(x), s_{j,2}(x), ..., s_{i,m-1}(x)\}$, to compute $K = s_{j,1}(i_l) \cdot s_{j,2}(i_2) \cdot ... \cdot s_{j,m-1}(i_{m-1}) \bmod N$, where $i_1, i_2, ...i_{m-1} \in \{1, 2, ..., m\} - \{j\}$ and $i_{\mathrm{r}} \neq i_s, \forall r, s$.

Remark 1: If there are any r (i.e., $2 \leq r \leq m \leq n$) sensors, $\{P_1, P_2, ..., P_r\}$, want to establish a secure group key, each sensor P_j, where $j \in \{1, 2, ..., r\}$, uses its shares, $\{s_{j,1}(x), s_{j,2}(x), ..., s_{i,m-1}(x)\}$, to compute $K = s_{j,1}(i_l) \cdot s_{j,2}(i_2) \cdot ... \cdot s_{j,r-1}(i_r) \cdot s_{j,r}(0) \cdot s_{j,r+1}(0) \cdot ... \cdot s_{j,m-1}(0) \bmod N$, where $i_1, i_2, ...i_{r-1} \in \{1, 2, ..., r\} - \{j\}$ and $i_{\mathrm{r}} \neq i_s, \forall r, s$.

C. Security Analysis

In this sub-section, we discuss security features as described in Section 3.3.

(a) *Correctness:* The group key is $K = f(1) \cdot f(2) \cdot ... \cdot f(m) \bmod N$. It is obvious that this group key can only be computed by sensors in the set, $\{P_1, P_2, ..., P_m\}$.

(b) *k-Secure:* In the following theorem, we prove that an adversary cannot recover the secret polynomial $f(x)$ from a captured sensor.

Theorem 1: Under the RSA assumption, the proposed scheme is secure against the attack to recover the secret polynomial $f(x)$ from a captured sensor.

Proof: It is obvious that an adversary cannot obtain $f(x)$ from each individual share, $s_{i,j}(x) = f_{i,l}(i) f(x) \bmod N$, since $f_{i,l}(i)$ is a random integer selected by the KDC. We use the technique of *proof by contradiction* to prove the rest of this theorem. Suppose to the contrary that without knowing the factoring of the RSA modulus N, given the product of shares, $g(x) = s_{i,1}(x) \cdot s_{i,2}(x) \cdot ... \cdot s_{i,m-1}(x) = f(i) f(x)^{m-1} \bmod N$, there exists an algorithm, *Algorithm A*, which can factor the product polynomial, $g(x)$, to obtain the secret polynomial, $f(x)^{m-1}$ and the integer, $f(i)$. In the following discussion, we want to show that the adversary can use *Algorithm A* to decrypt the RSA cipher text, $C = M^e \bmod N$, knowing only RSA public key, (N, e). Given any cipher text, $C = M^e \bmod N$, where $C = (c_k, c_{k-1}, ..., c_0)_{10} \in Z_N$, the cipher text can be represented as a polynomial, $g(x) = c_k x^k + c_{k-1} x^{k-1} + \cdots + c_0 \bmod N$, such that $C = g(10)$. The adversary can model the RSA encryption in terms of polynomials as $g(x) = f(i) \cdot f(x)^{e-1} \bmod N$, such that if $x = i = 10$, we have $g(10) = f(10)^e \bmod N \Rightarrow C = M^e \bmod N$. This implies that $M = f(10) mod N$. Thus, *Algorithm A* can be used to factor $g(x)$ to obtain the polynomial, $f(x)^{e-1}$ and the integer, $f(10) = M$. This result contradicts the RSA assumption. We conclude that *Algorithm A* does not exist.

In the following theorem, we prove that our scheme is *k-secure.*

Theorem 2: If any k sensors are captured, there has no information on shares of other sensors.

Proof: From each captured sensor, the adversary cannot obtain $f(x)$ from each share, $s_{i,j}(x) = f_{i,l}(i) f(x) \bmod N$, since $f_{i,l}(i)$ is a random integer selected by the KDC. On the other hand, from each captured sensor, the adversary can obtain $g(x) = s_{i,1}(x) \cdot s_{i,2}(x) \cdot ... \cdot s_{i,m-1}(x) = f(i) f(x)^{m-1} \bmod N$. Since the polynomial, $F(x_1, x_2, ..., x_m) = \prod_{i=1}^{m} f(x_i) \bmod N$ has degree k, according to the Lagrange interpolation formula, it needs at least $k + 1$or more than $k + 1$ points, for example, if $(i, f(i)^m)$, $i = 1, 2, ..., k+1$, are known, to solve the polynomial by computing $\sum_{i=1}^{k+1} f(i)^m \prod_{l=1}^{m} \prod_{j=1, j \neq i}^{k+1} \frac{(x_l - j)}{(i - j)} mod N = \prod_{i=1}^{m} f(x_i) mod N$. Thus, from k sensors, there has no information on the polynomial, $F(x_1, x_2, ..., x_m)$. The adversary cannot obtain shares of other sensors.

(c) *Key Confidentiality:* The group key, $K = f(x_{i_1}) \cdot f(x_{i_2}) \cdot ... \cdot f(x_{i_m}) \bmod N$, can only be obtained by any sensor participated in the group communication. It is computationally infeasible for an adversary to discover any group key.

(d) *Key Independence:* Knowing $k + 1$ or more than $k + 1$ group keys, for example knowing $k + 1$ keys, $\{f(1) f(2) ... f(m-1) f(m), f(1) f(2) ... f(m-1) f(m+1), , ..., f(1) f(2) ... f(m-1) f(m+k)\}$, according to the Lagrange interpolation formula, an adversary can obtain the interpolation polynomial, $\sum_{i=m}^{m+k} f(1) f(2), f(m-1) f(i) \prod_{j=m, j \neq i}^{m+k} \frac{(x-j)}{(i-j)} \bmod N == f(1) \cdot f(2) \cdot ... \cdot f(m-1) f(x)$. From this polynomial, the adversary can obtain other group keys, for example, the group key, $f(1) f(2) ... f(m-1) f(m+2k)$, can be computed from the polynomial. Thus, the key independence is preserved if knowing fewer than $k + 1$ group keys.

D. Performance Evaluation and Comparison

Each sensor needs to store the shares, $\{s_{j,1}(x), s_{j,2}(x), ..., s_{j,m-1}(x)\}$, which are $m - 1$ univariate polynomials. Thus, the memory cost of each sensor is to store $(m - 1)(k + 1)$ coefficients from Z_N. There is no communication overhead to establish a group key. ■

Horner's rule [21] can be used to evaluate polynomials. In the following discussion, we show the cost for computing a group key involving m (i.e., $2 \leq m \leq n$) sensors. From Horner's rule, evaluating a polynomial of degree k needs k multiplications and $k + 1$ additions. The computational cost

TABLE I
COMPARISONS

	Probabilistic (P) /Deterministic (D) scheme	**Interactive (I)/Non-interactive (N) scheme**	**Group(G)/Pairwise key (P)**	**Storage requirement of each sensor**	**Operation of each sensor**
Our scheme	D	N	G	$(m-1)(k+1)$ integers from Z_N	Polynomial evaluation
Blundo et al. [11]	D	N	G	$(k+1)^{m-1}$ integers from $GF(p)$	Polynomial evaluation
Khan et al. [13]	D	I	P	k integers	Matrix operation
Gligor [4]	P	I	P	k integers	none

to establish a group key with size m consists of the cost of evaluating $m-1$ polynomials. Overall, the computational cost to establish a group key involving m sensors, each sensor needs to evaluate $(m-1)k$ multiplications and $(m-1)(k+1)$ additions. Since the time of addition can almost be ignored in comparing with the time of multiplication, the computational cost to establish a group key of our proposed scheme is to evaluate $(m-1)k$ multiplications.

The computation of our proposed scheme is much simpler than schemes use public-key cryptography. For example, a RSA public-key operation is a modular exponentiation which requires approximately $1.5log_2N$ multiplications (i.e., in RSA, N is at least 1024 bits). In other words, a 1024-bit RSA operation requires approximately 1536 multiplications, Moreover, all existing public-key based group key establishment schemes require at least $(m-1)$ public-key operations of each sensor to establish connections with other sensor. Thus, public-key based group key establishment becomes infeasible in wireless sensor networks. ■

In Table I, we compare our proposed scheme with three other pre-distribution schemes of sensor networks. Our proposed scheme is a deterministic, non-interactive scheme which can establish a group key among m sensors with storage requirement of $(m-1)(k+1)$ integers from Z_N and polynomial operation needed of each sensor. Theoretically, Blundo et al. [11] is also a deterministic, non-interactive scheme which can establish a group key among m sensors. However, the storage requirement of $(k+1)^{m-1}$ integers from $GF(p)$ of each sensor makes this scheme to become impractical for establishing a group key but only suitable for establishing pair-wise keys. Khan et al. [13] is a deterministic, interactive scheme that can only establish a pair-wise keys between 2 sensors. Matrix operation is needed for establishing a pair-wise key. Gligor scheme [4] is a probabilistic, interactive pair-wise key establishment scheme with storage requirement of a key ring of k keys randomly selected from a large pool S of keys. After the deployment, if two neighbors share at least one key, they establish a secure link and compute their session secret key which is one of the common keys.

V. CONCLUSION

We have proposed a novel group key establishment scheme using a special type of multi-variate polynomial. The storage space of each sensor is linearly proportional to the size of group communication. Since there is no information exchange in determining the group key, the scheme has no communication overhead in group key establishment. In addition, only polynomial computations are needed to compute the group key. The proposed scheme is especially suitable in WSNs.

REFERENCES

[1] T. Gao, D. Greenspan, M. Welsh, R. Juang, and A. Alm, "Vital signs monitoring and patient tracking over a wireless network," in *Proc. 27th Annu. Int. Conf. Eng. Med. Biol. Soc. (IEEE-EMBS)*, Jan. 2006, pp. 102–105.

[2] L. Gu *et al.*, "Lightweight detection and classification for wireless sensor networks in realistic environments," in *Proc. 3rd ACM Conf. Embedded Netw. Sensor Syst.*, Nov. 2005, pp. 205–217.

[3] G. J. Pottie and W. J. Kaiser, "Wireless integrated network sensors," *Commun. ACM*, vol. 43, no. 5, pp. 51–58, May 2000.

[4] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. ACM CCS*, 2002, pp. 41–47.

[5] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2003, pp. 197–213.

[6] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in *Proc. IEEE INFOCOM*, Mar. 2004, pp. 586–597.

[7] A. Rasheed and R. N. Mahapatra, "Key predistribution schemes for establishing pairwise keys with a mobile sink in sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 1, pp. 176–184, Jan. 2011.

[8] S. Ruj, A. Nayak, and I. Stojmenovic, "Pairwise and triple key distribution in wireless sensor networks with applications," *IEEE Trans. Comput.*, vol. 62, no. 11, pp. 2224–2237, Nov. 2013.

[9] F. Li and P. Xiong, "Practical secure communication for integrating wireless sensor networks into the Internet of Things," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3677–3684, Oct. 2013.

[10] R. Blom, "Non-public key distribution," in *Advances in Cryptology—CRYPTO*, D. Chaum, R. L. Rivest, and A. T. Sherman, Eds. New York, NY, USA: Plenum, 1982, pp. 231–236.

[11] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," in *Advances in Cryptology—CRYPTO*, E. F. Brickell, Ed. Berlin, Germany: Springer-Verlag, 1992, pp. 471–486.

[12] D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," in *Proc. 10th ACM Conf. Comput. Commun. Secur. (CCS)*, Oct. 2003, pp. 52–61.

[13] E. Khan, E. Gabidulin, B. Honary, and H. Ahmed, "Matrix-based memory efficient symmetric key generation and pre-distribution scheme for wireless sensor networks," *IET Wireless Sensor Syst.*, vol. 2, no. 2, pp. 108–114, Jun. 2012.

[14] Y. Cheng and D. P. Agrawal, "An improved key distribution mechanism for large-scale hierarchical wireless sensor networks," *Ad Hoc Netw.*, vol. 5, no. 1, pp. 35–48, Jan. 2007.

[15] S. Guo and V. Leung, "A compromise-resilient group rekeying scheme for hierarchical wireless sensor networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2010, pp. 1–6.

[16] H. Liang and C. Wang, "An energy efficient dynamic key management scheme based on polynomial and cluster in wireless sensor netwoks," *J. Converg. Inf. Technol.*, vol. 6, no. 5, pp. 321–328, 2011.

[17] N. Saxena, G. Tsudik, and J. H. Yi, "Efficient node admission and certificateless secure communication in short-lived MANETs," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 2, pp. 158–170, Feb. 2009.

[18] Y. Zhou and Y. Fang, "A two-layer key establishment scheme for wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 6, no. 9, pp. 1009–1020, Sep. 2007.

[19] A. Fanian, M. Berenjkoub, H. Saidi, and T. A. Gulliver, "An efficient symmetric polynomial-based key establishment protocol for wireless sensor networks," *ISC Int. J. Inf. Secur.*, vol. 2, no. 2, pp. 89–105, 2010.

[20] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[21] D. E. Knuth, *The Art of Computer Programming, Seminumerical Algorithms*, vol. 2. Reading, MA, USA: Addison-Wesley, 1981.

Lein Harn received the B.S. degree in electrical engineering from National Taiwan University, in 1977, the M.S. degree in electrical engineering from the State University of New York–Stony Brook, in 1980, and the Ph.D. degree in electrical engineering from the University of Minnesota, in 1984. He is currently a Professor with the Department of Electrical and Computer Engineering, University of Missouri–Kansas City, Kansas City. He is currently investigating new ways of using secret sharing in various applications.

Ching-Fang Hsu received the M.Eng. and Ph.D. degrees in information security from the Huazhong University of Science and Technology, Wuhan, China, in 2006 and 2010, respectively. From 2010 to 2013, she was a Research Fellow with the Huazhong University of Science and Technology. She is currently an Assistant Professor with Central China Normal University, Wuhan. Her research interests are cryptography and network security, especially secret sharing and its applications.