Available online at www.sciencedirect.com

ScienceDirect

Ad Hoc Networks 5 (2007) 35–48

Ad Hoc Networks

www.elsevier.com/locate/adhoc

An improved key distribution mechanism for large-scale hierarchical wireless sensor networks

Yi Cheng, Dharma P. Agrawal *

Center for Distributed and Mobile Computing, Department of Electrical and Computer Engineering and Computer Science, University of Cincinnati, 816 Engineering Research Center Building, P.O. Box 210030, Cincinnati, OH 45221-0030, United States

Available online 27 June 2006

Abstract

Wireless sensor networks are often deployed in hostile environments and operated on an unattended mode. In order to protect the sensitive data and the sensor readings, secret keys should be used to encrypt the exchanged messages between communicating nodes. Due to their expensive energy consumption and hardware requirements, asymmetric key based cryptographies are not suitable for resource-constrained wireless sensors. Several symmetric-key pre-distribution protocols have been investigated recently to establish secure links between sensor nodes, but most of them are not scalable due to their linearly increased communication and key storage overheads. Furthermore, existing protocols cannot provide sufficient security when the number of compromised nodes exceeds a critical value. To address these limitations, we propose an improved key distribution mechanism for large-scale wireless sensor networks. Based on a hierarchical network model and bivariate polynomial-key generation mechanism, our scheme guarantees that two communicating parties can establish a unique pairwise key between them. Compared with existing protocols, our scheme can provide sufficient security no matter how many sensors are compromised. Fixed key storage overhead, full network connectivity, and low communication overhead can also be achieved by the proposed scheme.

Keywords: Wireless sensor network; Security; Key management; Polynomial-key distribution; Large-scale hierarchical networks

1. Introduction

With the recent technology improvement of micro-electro-mechanical systems (MEMS), large-scale wireless sensor networks are envisioned to be widely applied in various applications such as object tracking, environment monitoring and data gathering in the near future. Typically, a wireless sensor network is composed of a large number of sensor nodes; each sensor node is a small, inexpensive wireless device with limited battery power, memory storage, data processing capacity and short radio transmission range. Depending on the equipped sensing units, wireless sensor nodes can measure various physical characteristics, such as sound, temperature, pressure, etc. A number of wireless sensor nodes can be organized into clusters to track a particular object or monitor the surrounding environment in an interested area [1,2,22,26].

* Corresponding author. Tel.: +1 513 556 4756; fax: +1 513 556 7326.

E-mail addresses: chengyg@ececs.uc.edu (Y. Cheng), dpa@ececs.uc.edu (D.P. Agrawal).

1570-8705/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.adhoc.2006.05.011

In many applications, such as target tracking, battlefield surveillance and intruder detection, wireless sensor networks are often deployed in hostile environments, therefore, the sensitive data and sensor readings should be protected properly [4,14,21,24,25]. In wireless communication environments an adversary not only can eavesdrop the radio traffic in a network, but also can intercept or interrupt the exchanged messages. To prevent the malicious node impersonating good nodes for spreading misleading information intentionally, secret keys should be used to achieve data confidentiality, integrity and authentication between communicating parties. Additionally, wireless sensor networks are often operated on an unattended mode. An adversary may physically capture some sensors to compromise their stored sensitive data and communication keys. In most applications, wireless sensors are not tamper resistant due to their low cost. Therefore, any adversary that gets hold of a sensor can easily extract its stored cryptographic information. This serious attack is defined as node capture attack, which makes wireless sensor networks more vulnerable than traditional wireless networks. Key protection and revocation issues must be considered with special attention in wireless sensor networks.

In traditional wired networks and infrastructure-supported wireless networks, communication security is achieved by data encryption and mutual authentication between communicating parties. Public-key based asymmetric cryptographic algorithms and trusted third-party authentication schemes are used frequently to achieve communication security. Due to the resource constraints of wireless sensors, public-key based security protocols (e.g., Rivest et al. [28], Diffie and Hellman [29]) are too complicated and energy-consuming for large-scale wireless sensor networks. Furthermore, the unpredictable network topology, short radio transmission range and the intermittence operations of wireless sensors make the trusted third-party authentication protocols also infeasible for wireless sensor networks.

Specifics of wireless sensor networks, such as strict resource constraints and large network scalability, require a proposed security protocol to be not only secure but also efficient. Recent research shows that pre-loading symmetric keys into sensors before they are deployed is a practical method to deal with the key distribution and management problem in wireless sensor networking environments [3]. After the deployment, if two neighboring nodes have some common keys, they can setup a secure link by the shared keys.

Two straightforward strategies exist to pre-load symmetric keys into sensors. The first one is called master-key approach, in which all the sensors are pre-loaded a unique symmetric key in its memory. After the deployment, every two nodes in the network use the same symmetric key to encrypt/decrypt the exchanged data between them. This approach is extremely efficient since there is no communication overhead for key establishment and only one key is required to be stored in sensors, but it cannot provide sufficient security for wireless sensor networks. As we mentioned previously, node capture attack is the most serious threat for wireless sensor networks. In master-key approach, even one single node's capture could compromise the entire network, which is unacceptable for large-scale wireless sensor networks.

Another method is pairwise-key based approach. In this approach, a set of symmetric keys are pre-loaded into each sensor node to make sure any two nodes have a unique key between them. This approach can provide sufficient security since any node's capture cannot compromise the secure communication between non-captured nodes, but it is not scalable due to its extremely large key storage overhead. For a network composed of n nodes, this approach requires each node stores at least $(n-1)$ keys to ensure any two sensors can establish a secure link. The limited memory size of wireless sensors makes this approach infeasible for real deployments.

Above two straightforward approaches show that key pre-distribution schemes have a tradeoff between the security and the key storage overhead. To achieve sufficient security, a certain number of keys should be pre-loaded in each node; but the limited memory size of tiny sensors, on the other hand, decides that sensors cannot store too many keys as they want. Key distribution problem has been a hot research topic recently. Several enhanced key pre-distribution schemes have been proposed in literature [3,4,11,12,21,23,27,30,31], and attempt to achieve both security and efficiency for large-scale wireless sensor networks.

Briefly, existing schemes can be classified into three categories: random key pre-distribution schemes [3,4], polynomial-key pre-distribution schemes [10,11,21], and location based key pre-distribution schemes [27,30,31]. Each of them has its advantages and limitations, the main differences are follows.

In random key pre-distribution schemes, there is no computational overhead to generate pairwise keys between sensor nodes; but the communication overhead for shared key discovery phase is proportional to the number of the keys stored in each sensor. A tradeoff between network connectivity and key storage overhead exists in random key schemes; a certain number of keys have to be preloaded into each sensor node to achieve a high network connectivity probability.

Polynomial-key pre-distribution schemes have lower communication overhead than random key approaches, but they cannot provide sufficient security for large-scale networks to against the node capture attack. Only if the number of compromised sensors is less than a critical value (the degree of the corresponding polynomial), the communication between non-compromised nodes can keep secure; once the critical value is exceeded, the adversary would crack all the pairwise keys in the network by calculations.

Actually, location based key pre-distribution schemes are nothing different than the two previous approaches, except that they take advantage of the sensor deployment information to improve the network performance. Assuming sensors' expected location can be predicted before the deployment, location based schemes can reach the same network connectivity with fewer keys stored in each sensor node than previous schemes. Considering that in most applications wireless sensors are randomly dropped by a vehicle or airplane, it is impossible to predict each sensor's location beforehand. We argue that location based schemes only can be applied for some specific situations (such as a small-size, manually deployed network), which narrows their contributions significantly.

Most of the existing key distribution schemes consider wireless sensor networks have a highly distributed, flat architecture, which is easy to implement but not applicable for large-scale sensor networks, specifically for data-driven monitoring applications. Research shows that the hierarchical network architecture has better throughput and scalability than the flat structure for a large-scale wireless sensor network, since the redundant sensing data can be aggregated in the relay nodes and the destination node can be reached in fewer hops [5–9]. In this paper, we develop a new key pre-distribution mechanism for large-scale wireless sensor networks to improve both security and performance. Based on a three-tier hierarchical network model, an enhanced polynomial key distribution and management mechanism is proposed to establish pairwise keys between any pair of communicating parties. Compared with existing key pre-distribution schemes, our approach not only achieves better network security, but also has improved the network performance in terms of network connectivity, communication overhead and key storage overhead.

The rest of this paper is organized as follows. Section 2 presents some related work. Section 3 describes our proposed scheme in detail. Section 4 gives the security analysis and performance evaluation. The conclusion is summarized in Section 5.

2. Related work

Due to the severe resource constraints, the extremely large network size and the lack of the infrastructure support, key distribution and management is much harder in wireless sensor networks than traditional wired and wireless counterparts. Public-key based asymmetric cryptographic algorithms and traditional trusted third-party authentication mechanisms are not suitable for large-scale sensor networks, new security protocols or mechanisms need to be proposed to deal with the new emerging security requirements for wireless sensor networks. Symmetric key approach is an appropriate cryptography for wireless sensors due to its low energy consumption and simple hardware requirement, but how to distribute symmetric keys into sensor nodes is not just a trivial problem [3]. Many researchers have focused on this area recently and proposed several key pre-distribution schemes to establish pairwise key between sensor nodes [3,4,11,12,21,23,27,30,31].

The first key pre-distribution scheme was investigated by Eschenauer and Gligor [3]. Based on the probability and random graph theories, they proposed a random key pre-distribution scheme for wireless sensor networks. In this approach, a large size symmetric key pool P is generated first. Before deployment, each sensor node's memory is preloaded a set of randomly selected keys from the key pool P. After randomly deployed in the sensing area, each sensor node exchanges its stored keys information with its neighbors. Since all the keys are randomly selected from the same key pool, two sensor nodes may have some overlapped keys in their memories. In network initialization phase, a key discovery procedure is executed by sensors to find the common keys between neighbors. If two sensors have some keys in common, they can setup a secure link directly. Otherwise, a path-key establishment procedure needs to be triggered to setup a secure link between two neighbors. According to the probability and random graph theories, Eschenauer et al. showed that if the probability that any two nodes share at least one common key satisfies a critical value, the connectivity of the entire network can be obtained with high probability.

Eschenauer et al.'s work is the first attempt to deal with the key distribution problem in wireless sensor networks; it is more efficient than public-key based security schemes. The main problem of this scheme is it cannot provide sufficient security when the number of compromised nodes increases. Because of the low-cost hardware, wireless sensors are not tamper resistant devices. If a sensor node is captured, all its stored cryptographic information can be easily extracted by the adversary. In [3] a same key may be used by different pairs of sensors in a network, therefore each sensor's capture may compromise the communication between non-captured nodes. This problem is defined as network resilience in wireless sensor networks, which is used to evaluate how much fraction of the communication between non-captured nodes will be compromised when a certain number of sensors are captured by the adversary.

To improve the network resilience against node capture attacks, Chan et al. [4] proposed a "*q-composite*" scheme based on Eschenauer et al.'s work. In their approach, any two nodes need share at least $q(q \geqslant 2)$ common keys to establish a secure link between them. Chan et al. showed that when the number of the compromised nodes is less than some critical value, the network resilience against node capture attack can be improved when the value of q is increased. This is, the adversary needs to compromise more sensor nodes in [4] to crack the same fraction of the secure communication between non-captured nodes in [3].

Both [3,4] cannot guarantee the entire network's connectivity with one-hop neighboring nodes' key information exchange. To achieve the required network connectivity, a complicated path-key establishment procedure needs to be involved to setup a secure link between two neighboring nodes through some intermediate node, which not only degrades the network security, but also produces additional communication overhead in the network. For large-scale wireless sensor networks, the above two random key pre-distribution schemes need store many keys in each sensor node to achieve the required network connectivity. The approach in [4] can only improve the network resilience when the number of the captured nodes is low; once the number of the captured nodes exceeds a critical value, its performance degrades dramatically.

Blom [10] proposed a method to ensure any two members in a group to generate a common key between them in 1985. In their scheme, a $(\lambda - 1) \times n$ matrix G and a $(\lambda - 1) \times (\lambda - 1)$ symmetric matrix D are constructed first, where n is the group size and λ is the expected threshold of how many members can compromise the secret collusively. In the group initialization phase, each member randomly selects a row vector from matrix A, where $A = (G^{\mathrm{T}} \cdot D)$, and a corresponding column vector form matrix G. Suppose member a selects the ith row from A and ith column from G, and member b selects the jth row from A and the jth column from G, respectively. Once a and b want to communicate each other, they exchange their stored column vectors first, then multiply their stored row vector with the partner's column vector. After the calculations, a gets the (ith, jth) entry of matrix K ($K = G^T DG$), b gets the (jth, ith) entry of the same matrix. Since K is a symmetric matrix, the two entries have the same value which can be worked as the unique pairwise key between a and b. Blom's scheme can provide sufficient security when compromised members is less than λ. Once more than λ nodes are compromised, all the secret information of the group would be broken. This issue is called "λ-*security*", which is the main limitation of this kind of approaches.

Initially, Blom's scheme was not developed for wireless sensor networks. Du et al. proposed a pairwise key pre-distribution scheme for wireless sensor networks in [11] by combining [10] with the random key pre-distribution approaches. Multiple key generating spaces are used in [11] to improve the network resilience against node capture attack. In Du et al.'s scheme, if two sensor nodes share a common key generating space, they can use Blom's method to calculate a pairwise key between them. Otherwise, they need to establish a path-key using the same procedure in [3]. Although Du et al.'s scheme can improve the network resilience against node capture attack; it cannot guarantee any two neighboring nodes establish a secure link directly. The path-key generation procedure may increase the network connectivity, but additional communication and computational overheads are involved.

Cheng et al. proposed an efficient pairwise key establishment and management scheme in [12]. In this approach, a two-dimensional key matrix is generated to distribute symmetric keys into sensor nodes. Each sensor randomly stores a row and a column from the matrix before the deployment. Since each row has an intersection entry with each column in the matrix, every pair of sensors would share at least two common keys between them. After the deployment, two neighboring nodes combine their shared common keys and their node identities to generate a pairwise key between them. Because all the established pairwise keys are distinct to each other, any sensor's compromise cannot affect the secure communication between non-compromised nodes. Although Cheng et al.'s scheme can provide better network performance and security than previous schemes; it has some limitations when used for large-scale sensor networks. The communication overhead is still too high for large-scale dense networks, too many keys need to be pre-loaded into sensor nodes, node addition is a complicated and energy consuming procedure.

All the above schemes assume that wireless sensor networks are distributed flat networks and attempt to establish pairwise keys between any two sensor nodes. Because of the high density and large size of wireless sensor networks, these key pre-distribution schemes need consume a large amount of energy and produce huge communication overheads in a network. Another weakness of above schemes is their security property degrades dramatically when the number of compromised sensors increases or exceeds a threshold.

As we know, wireless sensors only have short transmission range. Therefore, it is not necessary to setup a pairwise key for any two nodes in a network, only neighboring nodes need to secure their communications. Furthermore, if a wireless sensor network has a hierarchical architecture, only the cluster head (CH) and its cluster members need to establish a pairwise key between them, which will significantly reducing the communication overhead in the network initialization phase. Since the hierarchical network architecture has the better network performance than the flat network structure [5–9], we believe that key distribution and management schemes could be simplified and more efficient if the hierarchical network architecture is adopted. (In fact for most data-driven monitoring applications, especially in military area, wireless sensor networks are usually organized as a hierarchical structure where people belong to different groups based on their ranks and each group is led by a higher commander.)

Gaurav et al. proposed a low-energy key management protocol for hierarchical wireless sensor networks in [13]. In their scheme, a wireless sensor network is partitioned into several distinct clusters by some gateway nodes. Each cluster is composed of a gateway node (as the cluster head) and a set of sensors. Senor node only communicates with its cluster head, no communication between sensors exists. Gateway nodes can communicate each other, and relay the information received from its members to the sink node.

Before deployment, each gateway node stores a set of keys in its memory; each sensor randomly selects a key from a gateway node and stores it with the gateway node's id in its memory. After the deployment, each sensor exchanges its key information with its cluster head, if the cluster head has the key in its memory, they can establish a secure link directly. Otherwise, the cluster head request the intended key from the corresponding gateway node. Once the key information exchange phase is finished, every cluster head can establish a secure link with its members.

Gaurav et al.'s scheme provides better network performance than previous key pre-distribution schemes since a hierarchical network model is used, but it does not address the node capture attack problem which is the major threat in wireless sensor networks. In [13], any gateway node's capture in the network initialization phase would compromise a large number of secret keys. Also in Gaurav et al.'s scheme, to improve the network performance, a group key is used to encrypt the communication among gateway nodes, which is extremely dangerous for a wireless sensor network. If a gateway node is compromised, the adversary could track all the communications between gateway nodes. Since all the communications in the hierarchical network are relayed by the gateway nodes, the whole network would be crashed by a single gateway node's failure.

To address the limitations of current key distribution schemes, we present an improved key distribution mechanism (IKDM) for large-scale hierarchical wireless sensor networks. Based on the same network model in [13] and the polynomial key calculation mechanism, our scheme enables any pair of communicating parties (cluster head to sensor, cluster head to cluster head, cluster head to sink, sensor to sink) to establish a unique pairwise key between them. Our proposed scheme can provide sufficient security for large-scale sensor networks against node capture attack and each node has fixed key storage overhead regardless of the network size and density. Security analysis and performance evaluation illustrate that IKDM has better performance then existing protocols, in terms of network connectivity, communication overhead, key storage overhead, and network resilience.

3. Improved key distribution mechanism (IKDM)

3.1. Network model

Basically, two architectures are available for wireless networks. One is the distributed flat architecture, and the other is hierarchical architecture. The former is easier for deployment, the latter provides simpler network management, and can help further reduce transmissions. As we know, wireless sensor networks are distributed event-driven systems that differ from traditional wireless networks in several ways: extremely large network size, severe energy constraints, redundant low-rate data, and many-to-one flows. It is clear that in many sensing applications, connectivity between all sensors is not necessary; wireless sensors merely observe and transmit data to those nodes with better routing and processing capabilities, and do not share data amongst themselves. Data centric mechanisms should be performed to aggregate redundant data in order to reduce the energy consumption and traffic load in wireless sensor networks. Therefore, hierarchical heterogeneous network model has more operational advantages than flat homogeneous model for wireless sensors their inherent limitations on power and processing capabilities [5–9].

In this work, we focus on large-scale wireless sensor networks with the same three-tier hierarchical architecture in [14,15]. Illustrated by Fig. 1, our network model has three different kinds of wireless devices; sink node/base station (BS), cluster head node (CH) and sensor node (S).

Sensor node (S): Sensor nodes are inexpensive, limited-capability, generic wireless devices in this paper. Each sensor has limited battery power, memory size, data processing capability and short radio transmission range. Sensor only communicates with its cluster head (CH) directly; no communication between sensors exists in our model. After deployment, sensor nodes keep stationary during the network operation period.

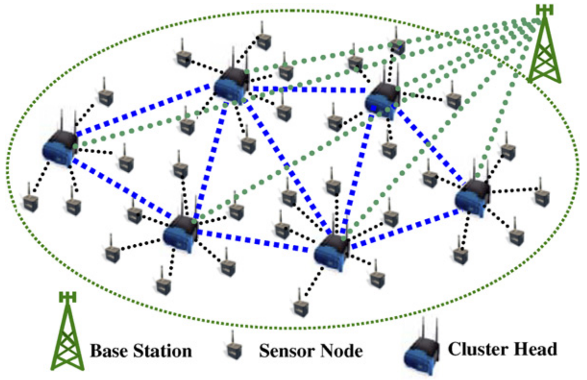

Fig. 1. A three-tier hierarchical wireless sensor network architecture.

Cluster head node (CH): Cluster heads have considerably more resources than sensors. Equipped with high power batteries, large memory storages, powerful antenna and data processing capacities, cluster heads can execute relatively complicated numerical operations and has much longer radio transmission range than sensor nodes. Cluster heads can communicate with each other directly and relay data between its cluster members and the sink node (base station).

Sink node/Base station (BS): Sink node is the most powerful node in a wireless sensor network, it has virtually unlimited computational and communication power, unlimited memory storage capacity, and very large radio transmission range which can reach all the nodes in a network. Sink node can be located either in the center or at a corner of the network based on the application.

In our network model, a large number of wireless sensors are randomly distributed in an area. A sink node/base station (BS) is located in a well-protected place and takes charge of the whole network's operation. As shown in Fig. 1, after the deployment, cluster heads (CHs) partition a network into several distinct clusters by some existing clustering algorithms [16–20]. In our network model, each cluster is composed of a cluster head (CH) and a set of sensor nodes (distinct from other sets). Wireless sensors monitor the surrounding environment and transmit the sensed readings to their cluster head. Cluster heads aggregate their received data, perform some mission-related data processing and send the aggregated and filtered data result to the sink node.

3.2. Background of polynomial key pre-distribution scheme

To improve the network security against the node capture attack, a polynomial-key pre-distribution mechanism is used in our scheme. Polynomial key pre-distribution scheme was first developed by Blundo et al. in [21]. An off-line key distribution server (KDS) distributes some t-degree polynomial shares into a set of users in such a way that any t users can compute a common key among them without any interaction. By evaluating its stored polynomials with the ids of the other $(t-1)$ users, each user can calculate a common key shared with others independently. The original protocol was developed to generate a group key for a set of users. Since our goal in this paper is to establish a unique pairwise key between two communicating nodes, we only discuss the bivariate polynomial key establishment approach here.

3.2.1. Procedure of bivariate polynomial key pre-distribution scheme

In this subsection, we briefly introduce the bivariate polynomial key pre-distribution scheme which was first proposed in [21]. Consider a k-degree bivariate polynomial $f(x, y)$, defined as

$$f(x,y) = \sum_{i,j=0}^{k} a_{ij}x^i y^j, \tag{1}$$

where the coefficients a_{ij} $(0 \leqslant i, j \leqslant k)$ are randomly chosen from a finite field $GF(Q)$, Q is a prime number that is large enough to accommodate a cryptographic key.

The bivariate polynomial above has a symmetric property such that

$$f(x,y) = f(y,x). \tag{2}$$

Each sensor has a unique id in a network. Before deployment, an offline key distribution server (KDS) first initializes sensors by giving each sensor p a polynomial share $g_p(y)$, which is obtained by evaluating $f(x, y)$ at $x = p$.

$$g_p(y) = f(p,y). \tag{3}$$

In other words, each sensor node p stores k number of coefficients g_j, $(0 \leqslant j \leqslant k)$ in its memory.

$$g_j = \sum_{i=0}^{k} a_{ij}(p)^i, \quad (0 \leqslant j \leqslant k), \tag{4}$$

where p is the node id of the intended sensor, and g_j is the coefficient of y^j in the polynomial $f(p, y)$.

In order to setup a pairwise key between sensors p and q, they exchange their node ids first, than node p evaluates $f(p, y)$ at $y = q$, and node q evaluates its stored polynomial $f(q, y)$ at $y = p$. Since $f(p, q) = f(q, p)$, sensors p and q can obtain a same value from the two distinct calculations, which can be used as their pairwise communication key.

3.2.2. Property of polynomial key pre-distribution scheme

The advantage of the bivariate polynomial key pre-distribution scheme is there is no communication overhead during the pairwise key establishment process. The main drawback of this scheme is the "*K-security*" property. According to the security proof in [21], a k-degree bivariate polynomial key scheme can keep secure against coalitions of up to k compromised sensors. When the number of compromised nodes is less than k, even all the compromised nodes put their stored information together, the coefficients of the polynomial cannot be derived. But once more than k nodes are compromised, the adversary may put the compromised information together and crack the coefficients of the polynomial. In this case, all the pairwise keys in the entire group would be cracked. Although increasing the value of k can improve the security property of bivariate polynomial key scheme, it is not suitable for wireless sensor networks due to the limited memory size of sensors.

3.3. Our improved approach

Based on a three-tier hierarchal network model, we propose an improved key distribution mechanism (IKDM) for large-scale wireless sensor networks. Our approach has three phases, key pre-distribution phase, inter-cluster pairwise establishment phase and inter-cluster pairwise key establishment phase. The notations used in this paper are listed in Table 1.

3.3.1. Key pre-distribution phase

Due to the resource constraints of wireless sensors, the best key distribution method is pre-loading the secret keys into sensors before they are deployed [3,4,11,21,27]. Similarly, some secret information needs to be pre-loaded into sensor nodes and cluster heads before they are deployed in our proposed scheme.

Table 1
Notations

Notation	Description
BS	Sink node (base station)
CH_i	Cluster head i
S_i	Sensor node i
CH	Set of cluster heads in a network
S	Set of sensor nodes in a network
K_{A-B}	Symmetric key between A and B (A, B can be sink node, cluster head or sensor node)
E_K(data)	Encrypted message by key K
$f_{\mathrm{CH}}(x, y)$	t-degree bivariate symmetric polynomial (used for key calculation between cluster heads)
$f_{\mathrm{CH}_i}(x,y)$ $(1 \leqslant i \leqslant m)$	t-degree bivariate symmetric polynomial (used for key calculation between cluster head i and sensors)

For convenience, we assume there are n sensor nodes and m cluster heads in our investigated network, each cluster has a cluster head and $\lceil n/m \rceil$ sensors inside. Two different bivariate symmetric polynomials are used in our approach, one is $f_{\mathrm{CH}}(x, y)$ which is used to establish pairwise keys between cluster heads. The other is $f_{\mathrm{CH}_i}(x,y)$ $(0 \leqslant i \leqslant m)$, which is used by cluster head CH_i to calculate a secret share for an intended sensor node.

To achieve data confidentiality, authentication and integrity in our proposed scheme, different secret information is pre-loaded into different level of nodes.

Sink node: To authenticate and secure the communication between sink node and other nodes in a network, sink node needs to store $(n + m)$ keys in its memory, each key is shared with a particular sensor node or cluster head. In this paper, we use $K_{\mathrm{CH}_i-\mathrm{BS}}$, $(1 \leqslant i \leqslant m)$ to represent the shared pairwise key between cluster head CH_i and sink node, and $K_{S_i-\mathrm{BS}}$, $(1 \leqslant i \leqslant n)$ to represent the shared pairwise key between sensor S_i and sink node.

Cluster head: Each cluster head CH_i stores a symmetric key $K_{\mathrm{CH}_i-\mathrm{BS}}$, and two polynomial shares $g_{\mathrm{CH}}(y)$ and $g_{\mathrm{CH}_i}(y)$ in its memory. $K_{\mathrm{CH}_i-\mathrm{BS}}$ is used to authenticate and secure the communication between CH_i and sink node. $g_{\mathrm{CH}}(y)$ and $g_{\mathrm{CH}_i}(y)$ can be obtained by Eqs. (5) and (6), respectively.

$$g_{\mathrm{CH}}(y) = f_{\mathrm{CH}}(\mathrm{CH}_i, y), \tag{5}$$

$$g_{\mathrm{CH}_i}(y) = f_{\mathrm{CH}_i}(\mathrm{CH}_i, y). \tag{6}$$

Sensor node: To reduce the key storage overhead of wireless sensors, only two keys are pre-loaded in each sensor node in our scheme. For sensor node S_i, the two pre-loaded keys are $K_{S_i-\mathrm{BS}}$ and $K_{S_i-\mathrm{CH}}$. As we mentioned before, $K_{S_i-\mathrm{BS}}$ is randomly generated by an offline key distribution server (KDS) and used to authenticate and secure the communication between sink node and sensor S_i. $K_{S_i-\mathrm{CH}}$ is used for S_i to authenticate and communicate with its intended cluster head. $K_{S_i-\mathrm{CH}}$ is generated complicatedly to achieve a high level security. The procedure is illustrated as follows:

i. KDS randomly selects l $(l \geqslant 1)$ polynomials from the m polynomials $f_{\mathrm{CH}_i}(x,y)$, $(1 \leqslant i \leqslant m)$. To achieve sufficient security, large l is desired. For convenience, we assume $l = 2$ in this example and polynomials $f_{\mathrm{CH}_a}(x,y)$ and $f_{\mathrm{CH}_b}(x,y)$ are randomly selected.

ii. KDS evaluates $f_{\mathrm{CH}_a}(x,y)$ at $(x = \mathrm{CH}_a, y = S_i)$ and $f_{\mathrm{CH}_b}(x,y)$ at $(x = \mathrm{CH}_b, y = S_i)$ respectively to get the two secret shares k_1 and k_2 of $K_{S_i-\mathrm{CH}}$.

$$k_1 = f_{\mathrm{CH}_a}(\mathrm{CH}_a, S_i), \tag{7}$$

$$k_2 = f_{\mathrm{CH}_b}(\mathrm{CH}_b, S_i). \tag{8}$$

iii. KDS calculates key $K_{S_i-\mathrm{CH}}$ by exclusive-or k_1 and k_2 under Eq. (9).

$$K_{S_i-\mathrm{CH}} = k_1 \oplus k_2, \tag{9}$$

iv. KDS pre-loads key $K_{S_i-\mathrm{CH}}$ with the two cluster head id CH_a and CH_b into sensor node S_i. $K_{S_i-\mathrm{CH}}$ will be the pairwise key between node S_i and its intended cluster head after the deployment.

After the key pre-distribution phase, each node in the network stores different keys in its memory. The powerful sink node stores $(m + n)$ pairwise keys in its memory. For the resource-constrained sensors, each node only needs to store two pairwise keys in its memory, which extremely reduces the key storage overhead for large-scale sensor networks. Each cluster head stores one pairwise key and two polynomial shares in its memory; after the deployment, each cluster head needs to establish pairwise keys with its cluster members and other cluster heads by its pre-loaded polynomial shares.

In our scheme, a wireless sensor network is partitioned into m distinct clusters after the deployment. Each cluster has a cluster head and a set of sensor nodes. To reduce the energy consumption and the redundant traffic loads in a network, sensor nodes only communicate with its cluster head, no communication between sensors exist. Sensor nodes gather environment data and transmit them to the cluster heads. Cluster heads can communicate with each other directly and send the aggregated sensing data to the sink node via long-haul transmission.

3.3.2. Inter-cluster pairwise key establishment

After the deployment, each cluster head needs to establish pairwise keys with other cluster heads first to secure the communication between them. Suppose cluster heads CH_a and CH_b need to establish a secure link between them, the procedure is as follows:

i. First, cluster heads CH_a and CH_b exchange their node id each other.

ii. CH_a evaluates its stored polynomial $f_{\mathrm{CH}}(\mathrm{CH}_a, y)$ at $(y = \mathrm{CH}_b)$ to get $K_{\mathrm{CH}_a-\mathrm{CH}_b}$:

$$K_{\mathrm{CH}_a-\mathrm{CH}_b} = f_{\mathrm{CH}}(\mathrm{CH}_a, \mathrm{CH}_b), \qquad (10)$$

iii. Similarly, CH_b evaluates its stored polynomial $f_{\mathrm{CH}}(\mathrm{CH}_b,y)$ at $(y = \mathrm{CH}_a)$ to get $K_{\mathrm{CH}_b-\mathrm{CH}_a}$:

$$K_{\mathrm{CH}_b-\mathrm{CH}_a} = f_{\mathrm{CH}}(\mathrm{CH}_b, \mathrm{CH}_a). \qquad (11)$$

Since $f_{\mathrm{CH}}(\mathrm{CH}_a, \mathrm{CH}_b) = f_{\mathrm{CH}}(\mathrm{CH}_b, \mathrm{CH}_a)$, cluster heads CH_a and CH_b establish a unique pairwise key $K_{\mathrm{CH}_b-\mathrm{CH}_a}$ between them. This pairwise key is used to authenticate the corresponding two cluster heads and secure the communication data between them.

In our scheme, each pair of cluster heads have a distinct pairwise key between them after the inter-cluster pairwise key establishment phase. All the communication between cluster heads is encrypted by the corresponding pairwise key during the network operation time, which means our approach can achieve data confidentiality, authentication and integrity for the inter-cluster communication in a wireless sensor network.

3.3.3. Intra-cluster pairwise key establishment

After the inter-cluster pairwise key establishment phase, each cluster head need to establish pairwise keys with its cluster members to secure the intra-cluster communication. The procedure of the intra-cluster pairwsie key establishment phase can be briefly described as follows.

First, a sensor node sends its node id and its stored cluster heads' ids to its physical cluster head. The physical cluster head sends the sensor's id to the intended cluster heads to require the corresponding key shares. Any cluster head received the key share request message will evaluate its stored polynomial with the intended sensor's id and send back the calculated key share to the physical cluster head. Once the physical cluster head receives all the key shares of the intended sensor node, it can calculate the corresponding pairwise key by the received key shares.

A detailed procedure is illustrated below. Suppose sensor node S_i is a member of cluster head CH_j, and the pairwise key $K_{S_i-\mathrm{CH}}$ pre-loaded in S_i is obtained by Eq. (9) in the previous key pre-distribution phase, where $K_{S_i-\mathrm{CH}} = f_{\mathrm{CH}_a}(\mathrm{CH}_a, S_i) \oplus f_{\mathrm{CH}_b}(\mathrm{CH}_b, S_i)$.

i. First, sensor node S_i sends its id S_i and its stored cluster head ids CH_a and CH_b to its physical cluster head CH_j.

ii. CH_j sends S_i to CH_a and CH_b respectively to request the corresponding key shares.

iii. Once receives the request message, CH_a evaluates its stored polynomial $f_{\mathrm{CH}_a}(\mathrm{CH}_a, y)$ at $(y = S_i)$. Suppose $k_1 = f_{\mathrm{CH}_a}(\mathrm{CH}_a, S_i)$, CH_a sends back $E_{K_{\mathrm{CH}_a-\mathrm{CH}_j}}(k_1)$ to CH_j, where $K_{\mathrm{CH}_a-\mathrm{CH}_j}$ is the pairwise key between CH_a and CH_j.

iv. CH_j decrypts $E_{K_{\mathrm{CH}_a-\mathrm{CH}_j}}(k_1)$ by $K_{\mathrm{CH}_j-\mathrm{CH}_a}$ to get k_1.

v. Similarly, CH_j can get k_2 from CH_b in the same way.

vi. CH_j calculates $K_{S_i-\mathrm{CH}}$ by exclusive-or k_1 and k_2 under Eq. (9).

Now, cluster head CH_j establishes a pairwise key with its cluster member S_i. All the communication between CH_j and S_i are encrypted by the established pairwise key $K_{\mathrm{CH}_j-S_i}$ to achieve communication security.

Once the intra-cluster pairwise key establishment phase is finished, a secure hierarchical wireless sensor network has been established. In this network, each sensor node stores two pairwise keys in its memory, one is shared with its cluster head, the other is shared with the sink node. These pairwise keys are used to authenticate and secure the communication between sensor nodes and cluster heads or sink node. Any pair of cluster heads also has a unique pairwise key to secure the communication between them. In other words, our proposed scheme guarantees any two communicating parties have a unique pairwise key between them. Since all the communication in the network is encrypted by a certain pairwise key shared between the communicating parties, our proposed scheme can provide sufficient security for the information authenticity, confidentiality and integrity in wireless sensor networks.

4. Security analysis and performance analysis

In this section, we evaluate the security property and network performance of our proposed scheme (IKDM). We will compare our scheme with the random key based pre-distribution schemes in [3,4], efficient pairwire key establishment and management scheme (EPKEM) in [12] and low-energy key management protocol (LEKM) in [13].

4.1. Security analysis

Node capture attack is a serious threat in wireless sensor networks; an adversary may physically capture sensor nodes to compromise the stored secret information since wireless sensors are not tamper resistant due to their low cost. In random key pre-distribution schemes [3,4], the same keys may be used by different pairs of sensors, some sensor nodes' capture may compromise the communication between other non-captured nodes. In LEKM [13] and our proposed IKDM, no communication between sensor nodes exists; each sensor only stores two pairwise keys in its memory, which not only reduces the key storage overhead for sensor nodes but also increases the network resilience against sensor node capture attack.

In our proposed scheme, since each pair of two communicating parties has a unique pairwise key, any sensor node's compromising cannot compromise the secure communication between non-compromised nodes. Fig. 2 compares the resilience against sensor node capture attack for different schemes. IKDM, EPKEM and LEKM can prevent the key compromising for non-captured sensor nodes no matter how many sensors are captured in a network.

In LEKM all the secret keys are pre-loaded in the cluster heads during the network initialization phase, each cluster head stores (n/m) secret keys in its memory. Once a cluster head is captured in this period, all its stored keys could be compromised by the adversary.

Fig. 3 shows the network resilience against cluster head node capture attack in the network initialization phase. Suppose there are 10,000 sensors and 100 cluster heads in a network. In LEKM, each cluster head stores 100 sensor's secret keys in its memory. Therefore, any single cluster head's capture could compromise the 100 sensors' secret keys. When the number of captured cluster heads increases, the number of compromised sensors increases dramatically. In our proposed IKDM scheme, only two 128-degree bivariate polynomial shares are stored in each cluster head during the network initialization phase, cluster heads have no idea about the sensors' secret keys. Even all the 100 cluster heads are compromised, none of the keys preloaded in sensor nodes could be compromised in the network.

Furthermore, in LEKM group keys are used to secure the inter-cluster communication among cluster heads, which could lead to the single-point failure attack in wireless sensor network environment. Once a cluster head is captured and compromised its stored key information, the adversary can used the compromised group key to crack the communi-

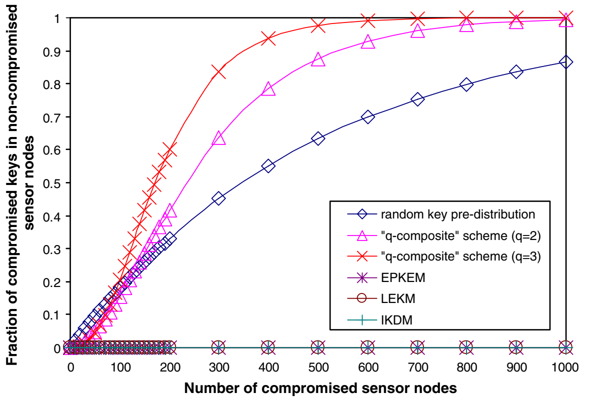

Fig. 2. Fraction of compromised keys in non-captured sensor nodes vs. number of compromised sensor nodes.

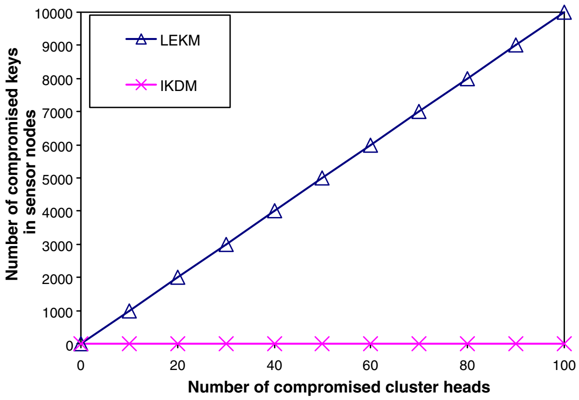

Fig. 3. Number of compromised sensor keys vs. number of the compromised cluster heads in the network initialization phase.

cations between other non-compromised cluster heads. Since all the communication in the hierarchal sensor network should go through the cluster heads, this single-point failure attack could break the entire network's security.

In IKDM, only polynomial shares are pre-loaded in cluster heads. Two cluster heads need to establish a unique pairwise key between them before they exchange the sensitive information. There is no group key involved in IKDM, any communication between cluster heads need to be encrypted by the intended pairwise key. Therefore, any single cluster head's compromising does not affect the secure communication between non-compromised cluster heads, the single-point failure attack is prevented in our scheme. According to security property of t-degree bivariate polynomial, IKDM can guarantee the network's security when there is no more than t cluster heads are compromised. Furthermore, in our network model, cluster heads have considerably high battery power and large memory storage size. We can select a relatively large degree polynomial to generate the pairwise keys between cluster heads. If $t > m$ is satisfied (where m is the number of cluster heads in the network), even all the cluster heads are compromised, the coefficients of the selected polynomial still cannot be derived by the adversary.

4.2. Performance evaluation

4.2.1. Maximum supported network size

Since wireless sensor networks are usually composed of a large number of sensors, proposed key distribution scheme should be scalable when the number of sensor nodes increases. In random key pre-distribution schemes [3,4], when the network size linearly increases, to achieve the required network connectivity, the number of keys stored in each sensor also need to increase linearly. Due the limited physical memory size of sensor nodes, each sensor can not store the pre-loaded keys as many as it wants. Therefore, the maximum supported network size is limited in [3,4]. Although EPKEM [12] has better performance than random key approaches, its key storage overhead is still sub-linearly increased when the network size is linearly increases. Based on the three-tier hierarchical network model, our proposed IKDM has better scalability than previous schemes. In IKDM, each sensor node stores two keys in its memory no matter how large the network size is, therefore, the network size is only decided by the cluster heads. In our proposed network model, cluster heads have relatively large memory size and sufficient power and data processing capacity. Theoretically, IKDM can be applied for any size of wireless sensor networks if the suitable polynomials and clustering algorithms are properly selected.

4.2.2. Key storage overhead

In [3,4], to achieve the required network connectivity, each sensor needs to store a certain number of keys in its memory. Although [12] has a smaller key ring size than [3,4] for the same network size, its key storage overhead is still sub-linearly with the network size. In our proposed IKDM scheme, each sensor only needs to store two keys in its memory no matter how many nodes in the network, which is extremely memory efficient for the large-scale wireless sensor networks.

Fig. 4 compares the number of keys stored in each sensor node for different schemes. When the network size is linearly increased, the number of keys stored in each sensor node also linearly increases in [3,4]. EPKEM has lower key storage overhead than random key pre-distribution schemes and its key storage overhead increases sub-linearly when the network size is linearly increased. IKDM has the lowest key storage overhead for sensor nodes, only two keys need to be stored in each sensor node no matter how large the network size is.

4.2.3. Communication overhead

In wireless sensor networks, radio communications consume much more energies than the code execution or calculations. To save the energy consumption, proposed security schemes should have low communication overhead. Compared with

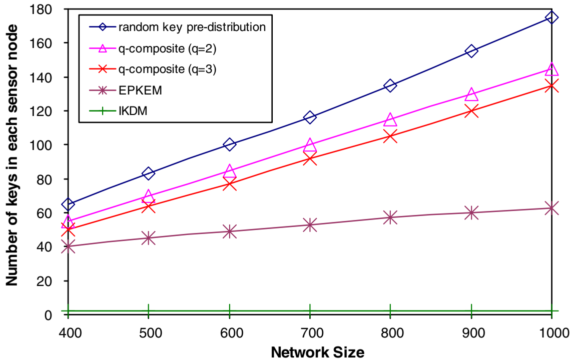

Fig. 4. Key storage overhead vs. network size.

existing schemes, our proposed scheme is more energy efficient due to the lower communication overhead for sensor nodes.

For key pre-distribution schemes, the communication overhead mainly occurs in the network initialization phase, since each sensor needs to exchange key information with its neighbors. In IKDM each sensor only stores two keys in its memory and its handshaking message is much shorter than previous schemes, which reduces the communication overhead significantly in the network initialization phase.

Additionally, in many applications fresh sensors need to be added into an existing network to replace the power exhausted nodes, which is another main energy-consuming procedure in wireless sensor networks. In [3,4], a fresh node needs to exchange its stored key information with the existing nodes after it is deployed into the network. This fresh node addition procedure produces lots of additional communication overheads in a network. In [13], fresh node addition is also a complicated energy-consuming procedure. Sink node needs to assign new keys into sensors and a particular cluster head, cluster heads need to exchange the new keys between them in order to establish a secure link with its new members. This procedure is extremely time and energy consuming, especially for a large-scale wireless sensor network.

Our proposed IKDM scheme is based on the polynomial share calculation; there is no additional key re-assignment and re-distribution operations needed when new sensors are joined into an existing network. By just pre-loading two keys into the new sensors with the same procedure in the key pre-distribution phase, fresh nodes can be easily deployed into an existing network to join a particular cluster. Sink node does not need to re-exchange key information with cluster heads, which extremely reduces the communication overhead in the network.

To compare the communication overhead for different schemes, we assume all the node identifiers are 16 bits, the established pairwise keys and polynomial-shares are 128 bits, there are 10,000 sensors and 100 cluster heads in the evaluation model, each cluster has 100 members inside, the average degree of sensor node is 60.

Fig. 5 shows that EPKEM has the lowest communication overhead since new nodes only need to exchange two identifiers with their neighbors. Random key pre-distribution schemes have the highest communication overhead. IKDM and LEKM have lower communication overhead than random key pre-distribution schemes since new sensors only need to send three identifiers to their cluster heads. Additionally, our IKDM scheme can reduce 25% communication overhead than LEKM since there is no key re-broadcast procedure involved.

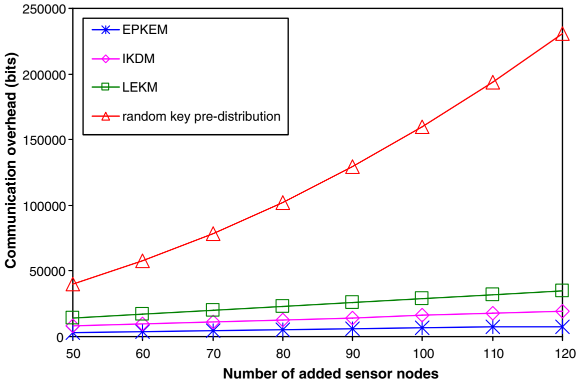

Fig. 5. Communication overhead vs. Sensor node addition.

5. Conclusion

Based on a three-tier hierarchical network architecture and bivariate polynomial-key pre-distribution mechanism, we present an improved key distribution mechanism for large-scale hierarchical wireless sensor networks in this paper. We show that hierarchical network architecture is more suitable for large-scale wireless senor network with its better scalability and network throughput. Compared with the existing key pre-distribution schemes, our proposed IKDM scheme can achieve better network resilience against node capture attack. The communication overhead of our scheme is much lower than the LEKM protocol and random key pre-distribution schemes. In our scheme, each sensor node only needs to store two keys in its memory regardless of the network size and density, which extremely reduces the key storage overhead for tiny sensors and makes our scheme suitable for large-scale wireless sensor networks.

Acknowledgement

This work has been supported by the Ohio Board of Regents Doctoral Enhancement Funds.

References

[1] D.P. Agrawal, Q-A. Zeng, Introduction to Wireless and Mobile Systems, Brooks/Cole Publishing, 2003.

[2] Neha Jain, D.P. Agrawal, Current trends in wireless sensor network design, International Journal of Distributed Sensor Networks 1 (1) (2005) 101–122.

[3] L. Eschenauer, V.D. Gligor, A key-management scheme for distributed sensor networks, in: Proceedings of the 9th ACM Conference on Computer and Communications Security, November 2002.

[4] H. Chan, A. Perrig, D. Song, Random key pre-distribution schemes for sensor networks, in: Proceedings of IEEE Symposium on Security and Privacy, Berkeley, California, May 11–14 2003, pp. 197–213.

[5] P. Gupta, P. Kumar, Internets in the sky: The capacity of three dimensional wireless networks, Communications in Information Systems 1 (1) (2001) 33–50.

[6] S. Zhao, K. Tepe, I. Seskar, D. Raychaudhuri, Routing protocols for self-organizing hierarchical ad hoc wireless networks, in: Proceedings of IEEE Sarnoff 2003 Symposium, 2003.

[7] P. Gupta, P.R. Kumar, The capacity of wireless networks, IEEE Transactions on Information Theory 46 (2) (2000) 388–404.

[8] B. Liu, Z. Liu, D. Towsley, On the capacity of hybrid wireless networks, in: Proceedings of IEEE Infocom 2003, San Francisco, CA, April 2003.

[9] S. Zhao, K. Tepe, I. Seskar, D. Raychaudhuri, Routing protocols for self organizing ad hoc wireless networks, in: IEEE Sarnoff Symposium 2003, Princeton, NJ, April 2003.

[10] R. Blom, An optimal class of symmetric key generation systems, in: Thomas Beth, Norbert Cot, Ingemar Ingemarsson (Eds.), Advances in Cryptology: Proceedings of EUROCRYPT 84, Lecture Notes in Computer Science, vol. 209, Springer-Verlag, 1985, pp. 335–338.

[11] W. Du, J. Deng, Y.S. Han, P.K. Varshney, A pairwise key pre-distribution scheme for wireless sensor networks, in: Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), Washington, DC, USA, October 27–31, 2003, pp. 42–51.

[12] Y. Cheng, D.P. Agrawal, Efficient pairwise key establishment and management in static wireless sensor networks, in: Proceedings of the Second IEEE International Conference on Mobile ad hoc and Sensor Systems, Washington, DC, November 7–10, 2005.

[13] G. Jolly, M.C. Kuscu, P. Kokate, M. Yuonis, A low-energy management protocol for wireless sensor networks, in: Proceedings of the Eighth IEEE International Symposium on Computers and Communication (ISCC'03), Kemer-Antalya, Turkey, June 30–July 3, 2003.

[14] M. Younis, M. Youssef, K. Arisha, Energy-aware routing in cluster-based sensor networks, in: Proceedings of the 10th IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS2002), (Forth Worth, TX), October 2002.

[15] K. Arisha, M. Youssef, M. Younis, Energy-Aware TDMA-Based MAC for Sensor Networks, in: Proceedings of the IEEE Workshop on Integrated Management of Power Aware Communications, Computing and Networking (IMPACCT 2002), May 2002.

[16] G. Gupta, M. Younis, Performance Evaluation of Load-Balanced Clustering of Wireless Sensor Networks, in: Proceedings of the 10th International Conference on Telecommunications (ICT'2003), Tahiti, Papeete – French Polynesia, February 2003.

[17] Jason Li, R. Levy, Fair and Secure Clustering Scheme (FSCS) clustering protocol, Technical report, Intelligent Automation Inc. 2005.

[18] S. Banerjee, S. Khuller, A Clustering Scheme for Hierarchical Control in Multi-hop Wireless Networks, in: Proceedings of IEEE INFOCOM, April 2001.

[19] D. Estrin, R. Govindan, J. Heidemann, S. Kumar, Next Century Challenges: Scalable Coordination in Sensor Networks, in: Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM), August 1999.

[20] S. Basagni, Distributed clustering algorithm for ad- hoc networks, in: Proceedings of International Symposium on Parallel Architectures, Algorithms, and Networks (I-SPAN), 1999.

[21] C. Blundo, A.D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, M. Yung, Perfectly-secure key distribution for dynamic conferences, Lecture Notes in Computer Science 740 (1993) 471–486.

[22] David W. Carman, Peter S. Kruus, Brian J. Matt, Constraints and approaches for distributed sensor network security, NAI Labs Technical Report #00-010, September 2000.

[23] Sencun Zhu, Sanjeev Setia, Sushil Jajodia, LEAP: Efficient security mechanisms for large-scale distributed sensor networks, in: Proceedings ACM CCS 2003, pages 62–72, October 2003.

[24] J.M. Kahn, R.H. Katz, K.S.J. Pister, Next century challenges: Mobile networking for smart dust, in: Proceedings of the fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), pages 483–492, 1999.

[25] C. Karlof, D. Wagner, Secure routing in wireless sensor networks: Attacks and countermeasures, in: Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.

[26] I. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, A survey on sensor networks, IEEE Communication Magazine 40 (8) (2002) 102–116.

[27] D. Liu, P. Ning, Location-based pairwise key establishments for relatively static sensor networks, in: Proceedings of 2003 ACM Workshop on Security of Ad hoc and Sensor Networks (SASN'03), October 31, 2003. George W. Johnson Center at George Mason University, Fairfax, VA, USA.

[28] Ronald L. Rivest, Adi Shamir, Leonard M. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21 (2) (1978) 120–126.

[29] W. Diffie, M.E. Hellman, New directions in cryptography, IEEE Transactions on Information Theory IT-22 (November) (1976) 644–654.

[30] D. Liu, P. Ning, Improving key pre-distribution with deployment knowledge in static sensor networks, in: ACM Transactions on Sensor Networks (TOSN), 2005.

[31] D. Liu, P. Ning, W. Du, Group-based key pre-distribution in wireless sensor networks, in: Proceedings of 2005 ACM Workshop on Wireless Security (WiSe 2005), September 2005.

Yi Cheng is currently a Ph.D., student at the Department of ECECS, University of Cincinnati. His main research interest is the security of wireless ad hoc and sensor networks. He received BS from the Tianjin University, China in 1997, majoring in Electrical Engineering. He also received MS from the University of Cincinnati, in 2003, majoring in Mathematics.

Dharma P. Agrawal is the Ohio Board of Regents Distinguished Professor of Computer Science and Engineering and the founding director for the Center for Distributed and Mobile Computing in the Department of ECECS, University of Cincinnati, OH. He has been a faculty member at the N.C. State University, Raleigh, NC (1982–1998) and the Wayne State University, Detroit (1977–1982). His current research interest includes energy efficient routing and information retrieval in mesh, ad hoc and sensor networks, QoS in integrated wireless networks, use of smart multi-beam directional antennas for enhanced QoS, and secured communication in mesh, ad hoc and sensor networks. His co-authored textbook on *Introduction to Wireless and Mobile Systems*, published by Thomson has been adopted throughout the world and revolutionized the way the course is taught and the second edition has been published recently. His latest co-authored book *Ad hoc and Sensor Networks – Theory and Applications* has been published in March 2006 by the World Scientific Publishing. He is an editor for the *Journal of Parallel and Distributed Systems*, *International Journal on Distributed Sensor Networks, International Journal of Ad hoc and Ubiquitous Computing (IJAHUC)*, *International Journal of Ad hoc and Sensor Wireless Networks, and the Journal of Information Assurance and Security (JIAS)*. He has served as an editor of the IEEE *Computer magazine*, the *IEEE Transactions on Computers* and the *International Journal of High Speed Computing*. He has been the Program Chair and General Chair for numerous international conferences and meetings. He has received numerous certificates and awards from the IEEE Computer Society. He was awarded a "*Third Millennium Medal*," by the IEEE for his outstanding contributions. He has also delivered keynote speech for five international conferences. He also has four patents and 18 patent disclosures in wireless networking area. He has been selected as a Fulbright Senior Specialist for duration of five years. He is a Fellow of the IEEE, the ACM, the AAAS, and WIF.