A Framework for a Distributed Key Management Scheme in Heterogeneous Wireless Sensor Networks

Kejie Lu, Yi Qian, Mohsen Guizani, and Hsiao-Hwa Chen

Abstract— **Key management has become a challenging issue in the design and deployment of secure wireless sensor networks. A common assumption in most existing distributed key management schemes is that all sensor nodes have the same capability. However, recent research works have suggested that connectivity and lifetime of a sensor network can be substantially improved if some nodes are given greater power and transmission capability. Therefore, how to exploit those heterogeneity features in design of a good distributed key management scheme has become an important issue. This paper proposes a unified framework for distributed key management schemes in heterogeneous wireless sensor networks. Analytical models are developed to evaluate its performance in terms of connectivity, reliability, and resilience. Extensive simulation results show that, even with a small number of heterogeneous nodes, the performance of a wireless sensor network can be improved substantially. It is also shown that our analytical models can be used to accurately predict the performance of wireless sensor networks under varying conditions.**

Index Terms— **Wireless sensor networks, heterogeneous, key management.**

I. Introduction

RECENTLY wireless sensor networks have attracted much attention due to its great potential to be used in various applications, including surveillance, widespread environmental monitoring, manufacturing and business asset management, automation in the transportation, security, and health-care industries. If compared to existing infrastructure-based networks, wireless sensor networks can virtually work in any environment, especially those where wired connections are not possible.

In general, wireless sensor networks consist of battery-operated sensor devices with computing, data processing, and communicating components. The ways the sensors are deployed can either be in a controlled environment such as factories, homes, or hospitals, or in an uncontrolled environment such as disaster or hostile area, particularly battlefield, where monitoring and surveillance is crucial. Clearly, in the uncontrolled and hostile environments, security for sensor networks becomes extremely important.

It is a great challenge to implement security in wireless sensor networks because of the nature of wireless communications, resource limitation on sensor nodes, size and density of the networks, unknown topology prior to deployment, and high risk of physical attacks to unattended sensors [1]. In some deployment scenarios, sensor nodes need to operate under adversarial conditions. To provide secure communications for the wireless sensor networks, all messages have to be encrypted and authenticated. Consequently, security solutions for such applications depend very much on the use of strong and efficient key distribution mechanisms in uncontrolled environments. Obviously, using a single shared key for the whole wireless sensor network is not a good idea because an adversary can easily obtain the key. Therefore, to implement a fundamental security service, pair-wise key establishment should be used, enabling secure communication among the sensor nodes using cryptographic techniques.

However, due to resource constraints on sensor nodes, it is not feasible for sensors to use traditional pair-wise key establishment techniques such as public key cryptography and key distribution center [2]. Instead, sensor nodes should use pre-distributed keys directly, or use keying materials to dynamically generate pair-wise keys. In such a case, the main challenge is to find an efficient way of distributing keys and keying materials to sensor nodes prior to deployment. In the last few years, different pair-wise key distribution schemes have been developed for peer-to-peer wireless sensor networks [3]–[10] and hierarchical wireless sensor networks [11] [12].

In peer-to-peer wireless sensor networks, there is no fixed infrastructure, and network topology is not known prior to deployment. Sensor nodes are usually randomly scattered all over the target area. Once they are deployed, each sensor node scans its radio coverage area to figure out its neighbors. In hierarchical wireless sensor networks, there is a hierarchy among the nodes based on their capabilities: base stations (or cluster supervisors) and sensor nodes [11] [12]. The base stations can be much more powerful than the sensor nodes in terms of transmission range, data processing capability, storage capacity, and tamper-resistance. Base stations can form the backbone of the sensor network and sensor nodes can be deployed around single- or multi-hop neighborhood of the

Manuscript received August 18, 2006; accepted November 7, 2006. The associate editor coordinating the review of this paper and approving it for publication was R. Fantacci.

K. Lu is with the Department of Electrical and Computer Engineering, University of Puerto Rico at Mayagüez, Mayagüez, Puerto Rico 00681 (e-mail: lukejie@ece.uprm.edu).

Y. Qian is with the Advanced Network Technologies Division, National Institute of Standards and Technology, Gaithersburg, MD 20899 (e-mail: yqian@nist.gov).

M. Guizani is with the Department of Computer Science, Western Michigan University, Kalamazoo MI (e-mail: mguizani@ieee.org).

H.-H. Chen (the corresponding author) is with the Institute of Communications Engineering, National Sun Yat-Sen University, Kaohsiung, Taiwan (e-mail: hshwchen@ieee.org).

Digital Object Identifier 10.1109/TWC.2008.060603.

base stations. In general, the base stations are also the key distribution centers in the sensor networks because they are assumed to be tamper-resistant.

All aforementioned solutions for a distributed wireless sensor network assumed that the sensor nodes are homogeneous with the same capabilities. For the solutions of hierarchical wireless sensor networks, except the base stations (or cluster supervisors), the rest of the sensor nodes are homogeneous with the same capabilities within each cluster.

However, heterogeneous sensor networks are given more attention recently. Particularly, with the advances in antenna technologies like multiple-input-multi-output (MIMO) systems [13], directional antennas [14], and cooperative communications [15], the heterogeneity in terms of transmission range in wireless sensor nodes has become a reality. Recent studies also showed that such heterogeneity can improve network performance and network lifetime without significantly increasing the cost [16]. Although it has been proven in [16] that optimal deployment of the heterogeneity is very hard in general, it showed that only a modest number of reliable, long-range backhaul links and line-powered nodes are enough to exert a significant impact on the overall performance.

In this paper, we propose a framework for key management schemes in distributed peer-to-peer wireless sensor networks with heterogeneous sensor nodes. With the heterogeneous sensor deployment schemes and key distribution mechanisms, we will investigate the effect of heterogeneity for different key management schemes on distributed wireless sensor networks. We will show using simulations as well as analysis that, with a small percentage of powerful nodes that have reasonable storage, processing, and communication capabilities, a wireless sensor network can achieve higher key connectivity and higher resilience.

The paper can be outlined as follows. We first introduce the major technical aspects of all key distribution schemes in Section II. The description of the framework for key management schemes in heterogeneous distributed wireless sensor networks is given in Section III, in which some special cases are also discussed. We then develop analytical models for these schemes in Section IV. The numerical results and discussions are presented in Section V. Finally, the conclusion of the paper is drawn in Section VI.

II. Security Requirements and Related Works

A. Security Requirements

In a wireless sensor network, physical security of wireless links is virtually impossible because of the broadcast nature and resource limitation on sensor nodes and uncontrolled environments where they are left unattended. Consequently, security attacks on information flow can be widespread, e.g., passive interception of data transmission, active injection of traffic, and overloading the network with garbage packets. Modification of information is possible because of the nature of the wireless channels and uncontrolled node environments. An opponent can make use of these natural impairments to modify information and also render the information unavailable. Security requirements in wireless sensor networks are similar to those of wireless ad-hoc networks due to their similarities [1]. Thus, wireless sensor networks also have the general security requirements of availability, integrity, authentication, confidentiality and non-repudiation. These security requirements can be provided by a key distribution mechanism with the requirements of scalability, efficiency, key connectivity, and resilience. Scalability is the ability to support large sensor nodes in the networks. Key distribution mechanism must support large network, and must be flexible against substantial increase in the size of the network even after deployment. Efficiency is the consideration of storage, processing and communication limitations on sensor nodes. Key connectivity is the probability that two or more sensor nodes store the same key or keying material. Enough key connectivity must be provided for a wireless sensor network to perform its intended functionality. Resilience is about the resistance against node capture. Compromise of security credentials, which are stored on a sensor node or exchanged over radio links, should not reveal information about security of any other links in a wireless sensor network. Higher resilience means lower number of compromised links.

B. Related Works

In the last few years, many pair-wise key distribution schemes have been developed for peer-to-peer wireless sensor networks [3]–[10] and hierarchical wireless sensor networks [11] [12]. Solutions to key distribution problem in wireless sensor networks can use one of the three approaches: random, deterministic, or hybrid [1]. In the random solutions, key-chains are randomly selected from a key-pool and distributed to sensor nodes. In the deterministic solutions, deterministic processes are used to design the key-pool and the key-chains to provide better key connectivity. The hybrid solutions use random approaches on deterministic solutions to improve the scalability and resilience.

Eschenauer and Gligor [3] proposed a random key pre-distribution scheme for pair-wise key establishment in peer-to-peer wireless sensor networks. The main idea in [3] is to let each sensor node randomly pick up a set of keys from a key pool before deployment so any pair of sensor nodes have a certain probability of sharing at least one common key. Chan *et al.* [4] further extended this idea and developed two key pre-distribution techniques: q-composite key pre-distribution and random pair-wise keys scheme. The q-composite key pre-distribution also uses a key pool but requires two sensors to compute a pair-wise key from at least q pre-distributed keys they share. The random pair-wise keys scheme randomly picks pairs of sensors and assigns each pair a unique random key.

In [5], Blundo *et al.* proposed to use bivariate polynomials to achieve key distribution for dynamic conferences. To establish a pair-wise key between two nodes, the key setup server randomly generates a t-degree bivariate polynomial as

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

over a finite field F_q, where q is a predetermined prime number that is large enough to accommodate a cryptographic key. By choosing appropriate coefficients $a_{ij} = a_{ji}$, we can have the desired symmetric property, $f(x,y) = f(y,x)$. Assume that

each sensor node has a unique non-zero integer ID. For a pair of sensor nodes n_i and n_j (n_i and n_j are unique sensor node IDs), we can assign a polynomial share $f(n_i, y)$ to n_i and another share $f(n_j, y)$ to n_j. After deployment, both nodes need to broadcast their IDs to establish a pair-wise key. Then node n_i can compute $f(n_i, n_j)$ by evaluating $f(n_i, y)$ at point $y = n_j$, and node n_j can compute $f(n_j, n_i)$ by evaluating $f(n_j, y)$ at point $y = n_i$. Due to the symmetry of the bivariate polynomial, the secure pair-wise key between nodes n_i and n_j is established as $K_{ij} = f(n_i, n_j) = f(n_j, n_i)$. The security proof in [5] ensures that this scheme is unconditionally secure and t-collusion resistant. That is, the coalition of no more than t compromised sensor nodes knows nothing about the pair-wise key between any two non-compromised nodes.

The polynomial based key pre-distribution scheme in [5] has some limitations. In particular, it can only tolerate no more than t compromised nodes, where the value of t is limited by the memory available in sensor nodes. The larger a sensor network is, the more likely an adversary compromises more than t sensor nodes and then the entire network. To improve this, Liu and Ning [6] developed a framework for pair-wise key establishment based on the polynomial-based key pre-distribution protocol in [5] and random key distribution in [3], [4]. They further developed two pair-wise key pre-distribution schemes: a random subset assignment scheme and a grid-based key pre-distribution scheme.

Du *et al.* [7] proposed a key pre-distribution scheme with the objective to improve the resilience of the network if compared to the previous schemes. In [8], Du *et al.* proposed another scheme to utilize node deployment knowledge to improve the Eschenauer-Gligor scheme in [3] in terms of network connectivity, memory usage, and network resilience against node compromise. Their scheme assumes a group-based deployment model, in which sensor nodes are deployed in groups around their deployment points and the distribution of deployment points follows a rectangular grid model. In each group, the Eschenauer-Gligor scheme is applied. Zhou *et al.* [9] presented a location-based key establishment scheme, which is a hexagonal-grid-based deployment model combined with a polynomial-based key establishment model to establish a key between two neighboring nodes. In [10], the authors considered the problem of designing a clustered distributed sensor network when the probability of node compromise in different deployment regions is known a prior.

For hierarchical wireless sensor networks, base stations (or supervisor nodes) act like key distribution centers. Initially, base stations may share a distinct pair-wise master-key with each sensor nodes within a cluster. These master-keys can then be used to establish other secure keys. In hierarchical wireless sensor networks, pair-wise keys are required for the communications between a base station and sensor node, and between two sensor nodes. The requirement can be easily resolved if a base station shares a distinct pair-wise master-key with each sensor node [1]. In such a scenario, the base station can intermediate the establishment of a pair-wise key between any pair of sensor nodes. Law *et al.* [11] used a similar approach where sensor nodes are separated into domains that are supervised by cluster supervisors. Zhu *et al.* [12] proposed localized encryption and authentication protocol (LEAP), where each sensor node can establish pair-wise keys with its one-hop neighbor. Multi-hop pair-wise keys may be required to reach cluster heads, and it can be done by each node generating a secret key and finding m intermediate nodes. For the LEAP solution, security of the system depends on the master-key the nodes received in the setup phase.

All aforementioned key management schemes for hierarchical wireless sensor networks have the underlying assumption that the sensor nodes are tamper proof and the master-key which is stored inside each node cannot be retrieved by an adversary. However, the assumption that the nodes are tamper-proof cannot be ensured in many sensor networks because sensor nodes are usually left unattended in a hostile environment. Once the master-key has been hacked, the adversary can use it to break the security of the entire network.

III. Distributed Key Management Schemes

A. The Framework

In this paper, we propose a general framework for key management schemes in distributed peer-to-peer wireless sensor networks that consist of heterogeneous sensor nodes. The framework can be described in terms of the following factors.

1) Classes of Nodes: In this framework, we consider that there are I classes of sensor nodes in the network, with Class 1 being the least powerful nodes, and Class I the most powerful nodes, in terms of their communication range, node processing capability, and energy level. Particularly, in terms of communication range, we assume bi-directional link between any two nodes. Let r_i denote the communication range of Class i nodes, we always have $r_m < r_n$ if $m < n$. Therefore, if a Class m node is within the range of direct communication link of a Class n node, Class m node might need multiple links to reach Class n node if $m < n$. The sensor nodes are distributed heterogeneously in the wireless sensor network, with p_i being the percentage of Class i nodes, and thus

$$p_1 + p_2 + \cdots + p_I = 1.$$

Here, it is important to note the fundamental difference between the heterogeneous wireless sensor networks assumed in this paper and the hierarchical wireless sensor networks considered in [11] [12]. In the hierarchical wireless sensor networks, the base stations (or cluster supervisors) are centralized nodes, and more importantly, they act like key distribution centers. By contrast, in the heterogeneous wireless sensor networks, except that the higher class nodes are more powerful in terms of communication range, node capability, and energy level, the communications between all different classes of nodes is still on peer-to-peer basis and distributed.

2) Pair-Wise Key Establishment: Similar to previous studies [3], we also consider that there are three steps in the framework to establish pair-wise keys between the sensor nodes: (a) initialization, (b) direct key setup, and (c) (optional) path key setup. The initialization step is performed in a key setup center before the deployment of all the sensor nodes. In this step, the setup server is responsible for distributing polynomial shares to different sensor nodes; and the heterogeneity will be taken into account in this process. The direct key setup step is for any two nodes trying to establish a pair-wise key; and they

always first attempt to do so through direct key establishment in a peer-to-peer manner. If the second step is successful, there is no need to start the third step. Otherwise, these sensor nodes may start path key setup step, trying to establish a pair-wise key with the help of other sensors. Depending on the heterogeneity, the third step can be disabled.

3) Key Generation: The general framework for key generation in heterogeneous distributed wireless sensor networks is based on the random key distribution [3] [4] and the polynomial based key pre-distribution protocol [5], and is inspired by the approaches found in [6]. In particular, our framework uses a pool of randomly generated bivariate polynomials to establish pair-wise keys between sensor nodes, with the consideration of I Classes of heterogeneity among the wireless sensor nodes.

In this manner, existing distributed key management schemes can all be included in the framework. To better understand the possible schemes, we let S be the total number of polynomials in the pool. Consequently, existing and potential schemes can be listed as the following:

- Category 1: $I = 1, S > 1$, the degree of every polynomial share is 0. In this case, the network is homogeneous and the key distribution scheme degenerates to the traditional key-pool based scheme [3], [4].
- Category 2: $I = 1$, $S = 1$, the degree of the polynomial share is larger than 0. In this case, the network is homogeneous and the key distribution scheme becomes a polynomial based scheme [5].
- Category 3: $I = 1, S > 1$, the degree of every polynomial share is larger than 0. In this case, the network is still homogeneous and the key distribution scheme is the polynomial-pool based scheme [6].
- Category 4: $I > 1, S > 1$, the degree of every polynomial share is 0. In this case, the network is heterogeneous and the key distribution scheme is a key-pool based scheme.
- Category 5: $I > 1$, $S > 1$, the degree of all polynomial shares are larger than 0. In this case, the network is heterogeneous and the key distribution scheme is a polynomial-pool based scheme.

Clearly, both Category 4 and Category 5 have there pros and cons. In particular, compared to the key-pool based scheme, the polynomial-pool based scheme may be more resilient and require less memory storage as well as communication overhead, it does require additional computational capability in the sensor nodes to calculate polynomials and thus may increase the energy consumption of the operation. Nevertheless, we notice that both of these two schemes can be included in our framework.

B. The Main Challenge

The main challenge in this framework is how to assign polynomial shares to different classes of nodes. To address this issue, we first formulate the problem as described in the following procedures.

1) In the first step, classes of sensor nodes can be further partitioned into J groups, where a unique group ID j will be assigned to each group. With the definition of group, our framework becomes more general, or in other words can include existing or potential location-based key distribution schemes [8]–[10]. In this step, different sensor node deployment options can be considered, such as square-grid [8], hexagonal-grid [9], or probabilistic deployment scheme with a random distribution [10].
2) In the second step, the setup server will generate a set of polynomials for each class of nodes. Specifically, for class i ($i = 1, 2, \cdots, I$), the setup server randomly generates a set, denoted as F_i, of bivariate t_i-degree polynomials over the finite field F_{q_i}, where q_i is a large prime number. In this procedure, the setup server can assign each polynomial a unique ID.
3) In the third step, a set of polynomials, denoted as F_{ij}, can be created for nodes in class i and group j. Particularly, we let

$$F_{ij} = \bigcup_{k=1}^{i} F_{ij}(k), \tag{2}$$

where $F_{ij}(k)$ ($F_{ij}(k) \subseteq F_k$) is a subset of polynomials that are selected from F_k. We can see from Eq. (2) that, within group j, two classes i_1 and i_2 ($i_1 < i_2$) will be able to share some common polynomials if there exists a k ($k \leq i_1 < i_2$) such that

$$F_{i_1 j}(k) \bigcap F_{i_2 j}(k) \neq \emptyset. \tag{3}$$

Similarly, for the same class i, nodes in two different groups $j_1 \neq j_2$ will be able to share common polynomials if there exists a k ($k \leq i$) such that

$$F_{i j_1}(k) \bigcap F_{i j_2}(k) \neq \emptyset. \tag{4}$$

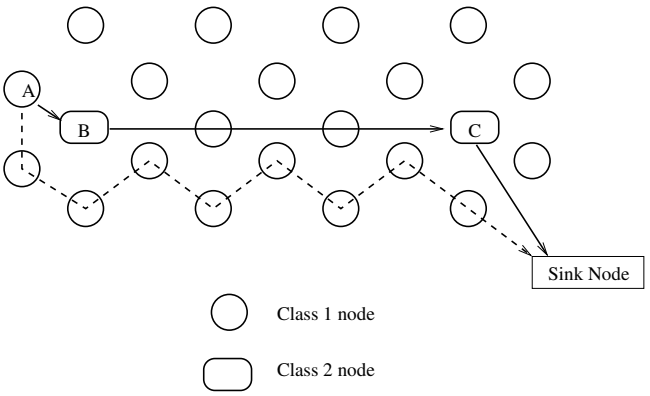
4) In the fourth step, the setup server picks up a subset of polynomials, denoted as Φ_{ij}^n ($\Phi_{ij}^n \subseteq F_{ij}$) for a node n in class i and group j, and assigns the polynomial shares of these polynomials to the node.

From the above discussion, we can clearly observe that the major issue in our framework is the subset assignment problem, which specifies how to determine the set of polynomials F_{ij} and how to assign the polynomial shared by sensor nodes in group j with class i. During the key distribution procedure, some factors must be considered, including the probability that adjacent nodes can share a common key, the resilience of the network when it is under attack, and importantly, the nature of the heterogeneity.

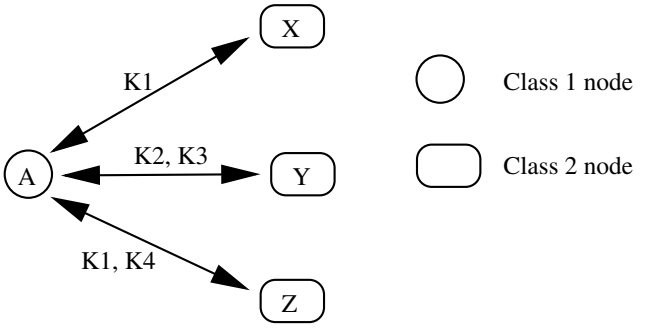
C. Key Distribution Schemes

From the description above, we observe that the new key generation scheme in our framework is essentially different to all existing schemes. Particularly that in our proposed scheme, heterogeneity features can be taken into account. Let us consider a typical heterogeneous wireless sensor network that is established to collect data in a distributed scenario. In this case, a sensor node should submit its observation to a sink node (or sink nodes, depending on the configuration of the network) through the network in a hop-by-hop manner, as shown in Fig. 1 (a), where there are two types of sensor nodes.

Since the higher class nodes have a larger transmission range, it is natural that a low class node will tend to utilize



(a) An example for wireless sensor network



(b) An example for the proposed scheme

Fig. 1. Examples of wireless sensor networks and the proposed key management scheme.

the link between itself and a high class node to submit the observations. For example, in Fig. 1 (a), Class 1 node A will tend to use the path "A-B-C-Sink" to submit its report, instead of passing the message by Class 1 nodes (the dash line). Evidently, a high class node will more likely be chosen as the next-hop neighbor of nearby low class nodes to forward data. Consequently, in this heterogeneous sensor network, the connectivity between a low class node and a high class node will be more important than the connectivity between two low class nodes.

We now design two special key distribution schemes within the new framework for the above scenario. Specifically, we consider that there are only two classes of the heterogeneous sensor nodes, i.e., $I = 2$. To simplify the illustration, we also assume that there is only one group, denoted as group 0, in the network.

The first scheme is a key-pool based key distribution scheme that belongs to Category 4 in Section III.A.3 and the second one is a polynomial-pool based scheme that belongs to Category 5 in Section III.A.3. For both schemes, we denote C_1 as the class of the less powerful sensor nodes, and denote C_2 the class of the more powerful sensor nodes. For both cases, we first define that a C_2 node is in the *neighborhood* of a C_1 node if this C_1 node can directly receive a broadcast message from the C_2 node. In other words, the C_1 node can receive the key (polynomial) pool information of the C_2 node without the relay of other sensor nodes. To simplify the discussion, we assume that a C_1 node can transmit messages to any C_2 nodes in its neighborhood, either through a one-hop link if the distance between them is small enough, or through a multi-hop path if the distance is larger than a threshold. In the latter case, the message from one C_1 node can still be secure if the C_1 node and the C_2 node share at least one key, and all other nodes in the path are not compromised.

An example of this scheme is illustrated in Fig. 1 (b), where node A is a C_1 node and nodes X, Y, and Z are C_2 nodes. In this example, nodes X, Y, and Z are the only C_2 neighbor nodes of node A. In addition, node A shares key K_1 with node X, K_2 and K_3 with node Y, and K_1 and K_4 with node Z, respectively. In this example, node A is connected if $q \leq 4$. In such a case, if node A wants to submit new information to the sink node, it can first randomly select a key from K_1 to K_4, then it can randomly select a neighbor node that shares the same key with it. In this manner, we can see that the communication is more resilient, while maintaining the connectivity.

IV. Analytical Model

In this section, we develop analytical models to evaluate the performance of the key management schemes within the framework. Similar to the previous studies, probability theoretical approach will be applied because the keys in each node are randomly selected or randomly generated.

A. Connectivity for Polynomial-Pool Based Scheme

In this case, we consider the polynomial-pool based key management scheme discussed in the previous section. It is noted that the degree of polynomial in general is greater than one, and thus the same polynomial can generate multiple keys at different nodes. Therefore, the total number of keys that a C_1 node can share with all C_2 nodes is the summation of the number of shared polynomials between the C_1 node and each of the C_2 nodes.

Based on this observation, we can first calculate the probability that a C_1 node shares i polynomials with a C_2 node, denoted as $p(i)$. Let S be the size of the polynomial pool, and let P_1 and P_2 be the number of polynomials that can be stored in a C_1 node and in a C_2 node, respectively. We can directly derive $p(i)$ as follows

$$p(i) = \frac{\binom{S}{i}\binom{S-i}{P_1-i}\binom{S-P_1}{P_2-i}}{\binom{S}{P_1}\binom{S}{P_2}} \tag{5}$$

With $p(i)$, we can derive the distribution that the total number of shared keys between a C_1 node and n_2 C_2 nodes as

$$p_{n_2}(i) = \underbrace{p(i) \otimes p(i) \otimes \cdots \otimes p(i)}_{n_2}, \tag{6}$$

where $\otimes$ denotes convolution operation. Finally, the connectivity for the polynomial-pool based key management scheme can be achieved by

$$C_p(q) = 1 - \sum_{i=0}^{q-1} p_{n_2}(i). \tag{7}$$

B. Connectivity for Key-Pool Based Scheme

In this case, a key that is shared by one C_1 node and multiple C_2 nodes will be considered as one key. To take such effect into account, we first let $v_n(i)$ be the probability that a C_1 node shares i different keys with n C_2 nodes. Now let K_1 and K_2 be the number of keys that can be stored in a C_1 node and in a C_2 node, respectively. Similar to Eq. (5), we have

$$v_1(i) = \frac{\binom{S}{i}\binom{S-i}{K_1-i}\binom{S-K_1}{K_2-i}}{\binom{S}{K_1}\binom{S}{K_2}} \tag{8}$$

To calculate $v_n(i)$ ($n > 1$), we can utilize the following recursive algorithm

$$v_n(i) = \sum_{j=0}^{i} v_{n-1}(j)h(i-j|j), n > 0 \tag{9}$$

where $h_{n-1}(i-j|j)$ is the conditional probability that a C_1 node can share $(i-j)$ keys with a C_2 node, given that it shares j keys (different from the $i-j$ keys) with other C_2 nodes.

Clearly, $h(i-j|j)$ does not depend on the number of C_2 nodes, and it can be calculated by

$$h(i-j|j) = \frac{\binom{S-j}{i-j}\binom{S-i}{K_1-i}\binom{S-K_1+j}{K_2-i+j}}{\binom{S-j}{K_1-j}\binom{S}{K_2}} \tag{10}$$

Finally, the connectivity for the key-pool based key management scheme can be obtained by

$$C_k(q) = 1 - \sum_{i=0}^{q-1} v_{n_2}(i), \tag{11}$$

where n_2 is the total number of C_2 nodes in the neighborhood of a C_1 node.

C. Resilience of the Key-Pool Based Scheme

In this case, we consider the performance of the key-pool based scheme when some C_1 nodes are compromised. We consider two scenarios: 1) the compromised nodes can be identified; and 2) the compromised nodes cannot be detected.

In the first scenario, we analyze the connectivity of the normal nodes after some C_1 nodes are compromised and all other nodes in the network recognize these compromised nodes. Here, it is reasonable to assume that C_2 nodes are tamper-resistant. To conduct the analysis, we define $q_n(i)$ as the probability that a C_1 node shares i different keys with neighboring C_2 nodes, given that n C_1 nodes in the same region have been captured. Let $g(j-i|i)$ be the probability that $(j-i)$ keys are compromised when a C_1 node is compromised, given that j keys are available before the attack. We can then derive a recursive algorithm to calculate $q_n(i)$ as follows.

$$q_0(i) = v_{n_2}(i), \forall 0 \le i \le K_1 \tag{12}$$

$$q_n(i) = \sum_{j=i}^{K_1} q_{n-1}(j)g(j-i|j) \tag{13}$$

where $g(j-i|i)$ can be calculated by

$$g(j-i|j) = \frac{\binom{j}{j-i}\binom{S-j}{K_1+i-j}}{\binom{S}{K_1}} \tag{14}$$

In the second scenario, normal nodes in the network do not notice that some C_1 nodes have been compromised. Therefore, a certain number of sessions will be eavesdropped. To evaluate the performance, we use the ratio of unaffected traffic to describe the resilience behavior in such a scenario. Here, it is important to note that, with the new schemes, a C_1 node can still transmit data securely to C_2 nodes even if some of the keys are compromised. For example, in Fig. 1, if K_1 is the only key that is compromised, then we can see that node A still has 75% chance to forward the data to any one of the C_2 nodes (with K_2, K_3, or K_4).

To analyze the unaffected ratio, denoted as $\rho(n)$, where n is the number of compromised C_1 nodes, we define $r(i,j,n)$ as the probability that j keys of a C_1 node are not compromised, given that in total i keys are shared by the C_1 node and neighboring C_2 nodes and that n other C_1 nodes have been compromised. Clearly, we have

$$\rho(n) = \sum_{i=1}^{K_1}\sum_{j=1}^{i}\left[v_{n_2}(i) \times r(i,j,n) \times \frac{j}{i}\right] \tag{15}$$

In Eq. (15), $v_{n_2}(i)$ can be calculated by Eq. (9) and $r(i,j,n)$ can be calculated recursively.

$$r(i,j,1) = \frac{\binom{i}{i-j}\binom{S-i}{K_1-i+j}}{\binom{S}{K_1}} \tag{16}$$

$$r(i,j,n) = \sum_{k=j}^{i} r(i,k,n-1)\frac{\binom{k}{k-j}\binom{S-k}{K_1-k+j}}{\binom{S}{K_1}}. \tag{17}$$

V. Numerical Results

In this section, we present the analytical and simulation results to compare the performance of different configurations of key management schemes discussed in the previous sections. The settings of our experiments can be summarized as follows.

- There are two classes of sensor nodes, denoted as C_1 and C_2, in the network.
- We consider a small area of a sensor network, in which the number of C_1 nodes is 40 and the number of C_2 nodes is N_2.
- Each C_1 node in the area can directly communicate with all C_2 nodes within the area.
- We investigate two key distribution schemes: (1) key-pool based scheme, and (2) polynomial-pool based scheme.
- For each of the simulation runs, we test 1,000 small sensor networks. Since each network has 40 C_1 nodes, the connectivity of 40,000 C_1 nodes will be measured.

Other simulation settings can be found in Table. I.

TABLE I
SIMULATION SETTINGS

Parameters	Key-pool based scheme	Polynomial-pool based scheme
Pool size	$S = 10000$	$S = 1000$
N_1	40	40
N_2	To be investigated	To be investigated
For C_1 nodes	K_1: to be investigated	P_1: to be investigated
For C_2 nodes	$K_2 = 1000$	$P_2 = 100$

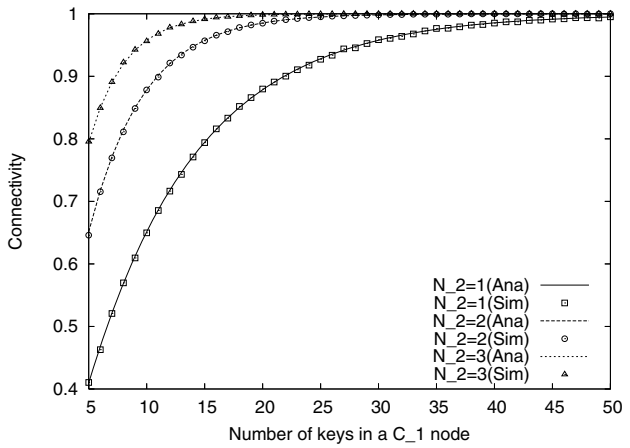


Fig. 2. Connectivity vs. the number of keys in a C_1 node (key-pool based scheme, $q = 1$).

A. Key Connectivity of the New Schemes in Normal Conditions

Fig. 2 shows the connectivity versus the number of keys in a C_1 node with different number of C_2 nodes for the key-pool based scheme, where we assume $q = 1$. It can be observed that, the connectivity can increase with the increase of the number of keys. For a fixed number of keys in each C_1 node, we can see that a small increase of the number of C_2 nodes can significantly improve the connectivity, especially when the number of keys in C_1 node is small and medium. From another perspective, we can see that, to achieve a specific connectivity, the number of keys that must be stored in each C_1 node can be decreased with the increase of N_2. For instance, if the connectivity is 0.99, then about 45 keys are required for N_2 = 1, about 23 keys are required for $N_2 = 2$, and about 15 keys are needed for $N_2 = 3$.

To highlight the impact of C_2 nodes, we illustrate in Fig. 3 the performance of connectivity versus the number of C_2 nodes in the cluster with different values of q, where the number of keys in any C_1 node is 30. It can be clearly seen that the network connectivity can be substantially improved when the number of C_2 nodes increases from 1 to 3. Interestingly, the connectivity converges to 1 if $N_2 = 3$, meaning that we do not need to deploy more C_2 nodes if the resilience is not a concern.

In Figs. 4 and 5, the performance of the polynomial-pool based key management scheme is illustrated. Fig. 4 shows the connectivity versus the number of keys in a C_1 node with different numbers of C_2 nodes for the polynomial-pool based scheme, where we assume $q = 1$. Fig. 5 shows the connectivity versus the number of C_2 nodes with different values of q for polynomial-pool based scheme. From Figs. 4 and 5, similar trends can be observed as those of Figs. 2 and 3, meaning that only very few number of C_2 nodes can significantly improve the system performance in both schemes.

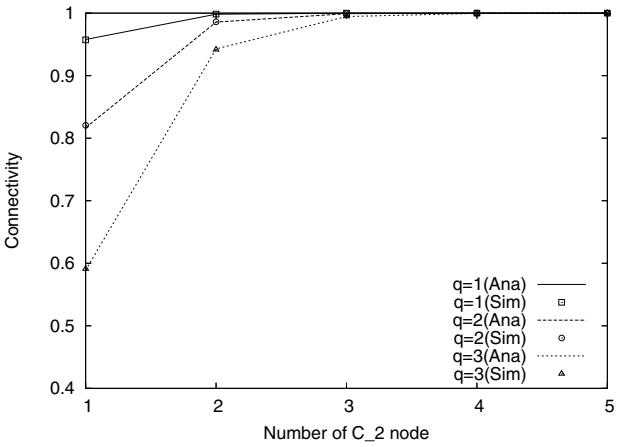


Fig. 3. Connectivity vs. the number of C_2 nodes (key-pool based scheme, 30 keys per C_1 node).

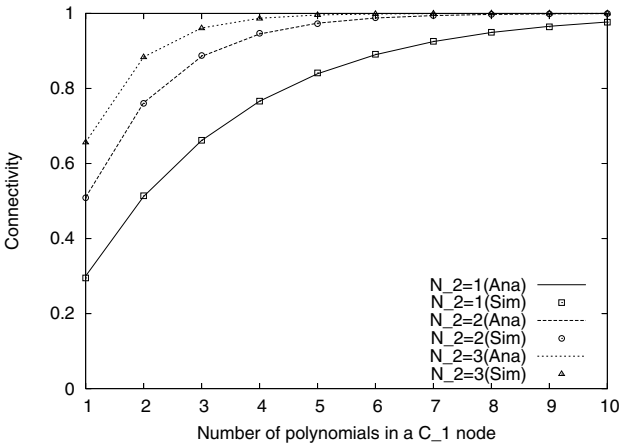


Fig. 4. Connectivity vs. the number of polynomials in a C_1 node (polynomial-pool based scheme, $q = 1$).

B. Reliability of the New Schemes

From Figs. 3 and 5 it can also be concluded that the increase of the number of C_2 nodes can substantially improve the reliability of the network. In particular, if we deploy 5 C_2 nodes in the key-pool based scheme, the connectivity of the C_1 nodes can be maintained even if any two C_2 nodes are broken.

C. Resilience of the New Schemes

To evaluate the resilience of the new schemes, we evaluated performance of a sensor network when some C_1 nodes are compromised. Here, it has to be noted that C_2 nodes are assumed to be more tamper-resistant. In Figs. 6 and 7, we consider the key-pool based scheme, in which we let $q = 1$ and the keys per C_1 node will be selected such that the network connectivity is 99% under normal conditions.

We first investigate the connectivity of the remaining uncompromised nodes, if the compromised nodes and the corresponding keys can be identified after the capture of

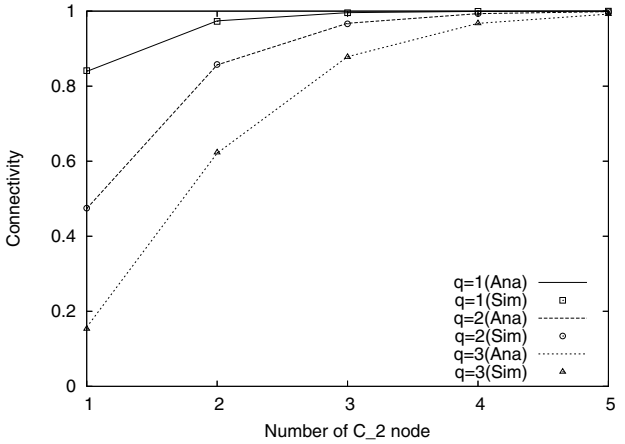


Fig. 5. Connectivity vs. the number of C_2 nodes (polynomial-pool based scheme, $P_1 = 5$).

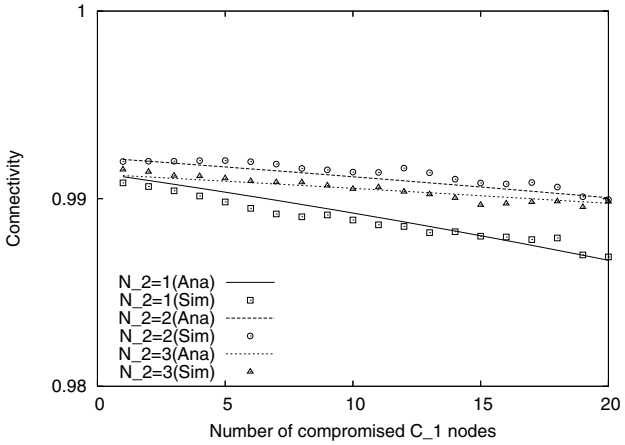


Fig. 6. Connectivity of uncompromised C_1 nodes vs. the number of compromised C_1 nodes (key-pool based scheme, $q = 1$).

any C_1 nodes. From Fig. 6 we can clearly observe that the connectivity of the remaining nodes decreases with the increasing number of compromised nodes. Nevertheless, it is seen that the connectivity is relatively high even if 20 nodes (amongst 40 nodes in total) are compromised. From Fig. 6 we can also observe that the connectivity can be improved slightly if more than one C_2 nodes are deployed.

In Fig. 7, we show the resilience of the scheme from another perspective, in which it is assumed that the compromised C_1 nodes cannot be detected. In such a scenario, the data transmission from an unaffected C_1 node may be eavesdropped by a nearby compromised node. Therefore, it is important to study the percentage of communications that are not affected. In the previous discussion, we have seen that with the new schemes a C_1 node can still transmit data securely to C_2 nodes even if some of the keys are compromised. This phenomenon can be clearly observed in Fig. 7, where a high percentage of secured communications can still be maintained even if half of the C_1 nodes are compromised. Moreover, it is seen that more C_2 nodes can help to increase the fraction of unaffected communications, given the same number of compromised C_1 nodes.

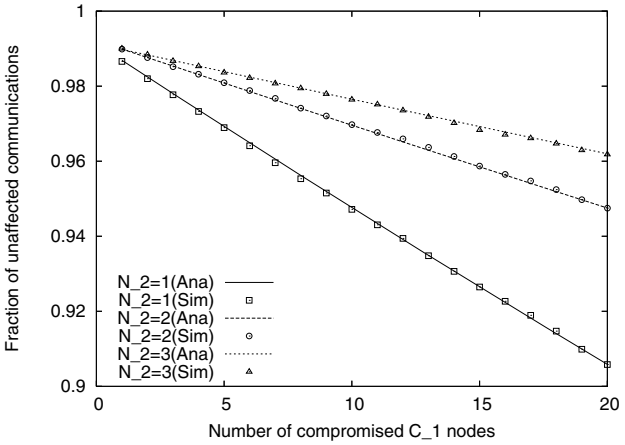


Fig. 7. Fraction of unaffected communications from uncompromised nodes vs. the number of compromised C_1 nodes (key-pool based scheme, $q = 1$).

VI. Conclusion

In this paper, we design a distributed key management scheme for heterogeneous wireless sensor networks. Analytical models are developed to evaluate the performance of the scheme in terms of connectivity, reliability, and resilience. Extensive simulation results have shown that, even with a small number of heterogeneous nodes, the key connectivity, reliability, and resilience of a wireless sensor network can be improved effectively. It is also shown that the proposed analytical models can be used to predict the performance accurately under varying operational conditions.

Acknowledgment

This work was supported partially by the US National Science Foundation (NSF) under Award Number 0424546, NSF EPSCoR start-up grant in Puerto Rico, and the research grants NSC96-2221-E-110-035 and NSC96-2221-E-110-050 from National Science Council, Taiwan.

References

[1] S. A. Camtepe and B. Yener, "Key distribution mechanisms for wireless sensor networks: a survey," Department of Computer Science, Rensselaer Polytechnic Institute, Tech. Rep. TR-05-07, March 23 2005.

[2] W. Stallings, *Cryptography and Network Security: Principles and Practices*, 4th ed. Upper Saddle River, NJ: Prentice Hall, 2005.

[3] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. CCS '02: 9th ACM Conference on Computer and Communications Security*. New York: ACM Press, Nov. 2002, pp. 41–47.

[4] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. IEEE Symposium on Research in Security and Privacy*, May 2003.

[5] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," in *Proc. CRYPTO '92: 12th Annual International Cryptology Conference on Advances in Cryptology*. London: Springer-Verlag, 1992, pp. 471–486.

[6] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in *Proc. CCS '03: 10th ACM Conference on Computer and Communications Security*. New York: ACM Press, 2003, pp. 52–61.

[7] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key predistribution scheme for wireless sensor networks," in *Proc. 10th ACM Conference on Computer and Communications Security*, Oct. 2003.

[8] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in *Proc. IEEE INFOCOM*, vol. 1, March 2004, pp. 586–597.

[9] Y. Zhou, Y. Zhang, and Y. Fang, "LLK: a link-layer key establishment scheme for wireless sensor networks," in *Proc. IEEE WCNC*, vol. 4, March 2005, pp. 1921–1926.
[10] S.-P. Chan, R. Poovendran, and M.-T. Sun, "A key management scheme in distributed sensor networks using attack probabilities," in *Proc. IEEE GLOBECOM*, vol. 2, Nov. 2005, pp. 1007–1011.
[11] Y. W. Law, R. Corin, S. Etalle, and P. H. Hartel, "A formally verified decentralized key management for wireless sensor networks," in *PersonalWireless Communications*, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, Sept. 2003, vol. 2775/2003, pp. 27–39.
[12] S. Zhu, S. Setia, and S. Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks," in *Proc. CCS '03: 10th ACM conference on Computer and communications security*. New York: ACM Press, 2003, pp. 62–72.
[13] D. Gesbert, M. Shafi, D. shan Shiu, P. Smith, and A. Naguib, "From theory to practice: an overview of MIMO space-time coded wireless systems," *IEEE J. Select. Areas Commun.*, vol. 21, no. 3, pp. 281–302, Apr. 2003.
[14] R. Ramanathan, J. Redi, C. Santivanez, D. Wiggins, and S. Polit, "Ad hoc networking with directional antennas: a complete system solution," *IEEE J. Select. Areas Commun.*, vol. 23, no. 3, pp. 496–506, Mar. 2005.
[15] S. Cui, A. Goldsmith, and A. Bahai, "Energy-efficiency of MIMO and cooperative MIMO techniques in sensor networks," *IEEE J. Select. Areas Commun.*, vol. 22, no. 6, pp. 1089–1098, Aug. 2004.
[16] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh, "Exploiting heterogeneity in sensor networks," in *Proc. IEEE INFOCOM*, vol. 2, March 2005, pp. 878–890.

Kejie Lu (S'01, M'04, SM'07) received the B.S. and M.S. degrees in Telecommunications Engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 1994 and 1997, respectively. He received the Ph.D. degree in Electrical Engineering from the University of Texas at Dallas in 2003. In 2004 and 2005, he was a postdoctoral research associate in the Department of Electrical and Computer Engineering, University of Florida. Currently, he is an assitant professor in the Department of Electrical and Computer Engineering, University of Puerto Rico at Mayagüez. His research interests include architecture and protocols design for computer and communication networks, performance analysis, network security, and wireless communications.

Yi Qian (M'96, SM'07) has been with National Institute of Standards and Technology since August 2007. He was an Assistant Professor in the Department of Electrical and Computer Engineering, University of Puerto Rico at Mayagüez. Prior to joining UPRM in July 2003, he worked for several start-up companies, consulting firms, and a large telecommunication equipment manufacture company, in the areas of voice over IP, fiber optical switching, Internet packet video, network optimizations and network planning for wireless and satellite networks, as a Technical Advisor, a Sr. Consultant, and a Sr. Member of Scientific Staff. He received a Ph.D. degree in Electrical Engineering with focus on Telecommunication Networks from Clemson University. His current research interests include network security, network management, network modeling, simulation, and performance analysis for next generation wireless networks, wireless sensor networks, broadband satellite networks, optical networks, high-speed networks and internet. He has publications and patents in all these areas.

He has been on numerous conference technical committees including serving as the General Chair of the International Symposium on Wireless Pervasive Computing 2007, the Technical Program Co-Chair of the IEEE GLOBECOM 2006 - Symposium on Wireless Communications and Networking, and the Technical Program Co-Chair of the Workshop on Information Assurance 2006 and 2007. Dr. Yi Qian is a member of Sigma Xi, ACM, IEICE, IEEE Communications Society, Computer Society, and Vehicular Technology Society.

Mohsen Guizani is currently a Professor and the Chair of the Computer Science Department at Western Michigan University. He received his B.S. (with distinction) and M.S. degrees in Electrical Engineering; M.S. and Ph.D. degrees in Computer Engineering in 1984, 1986, 1987, and 1990, respectively, from Syracuse University, Syracuse, New York. His research interests include Computer Networks, Wireless Communications and Mobile Computing, and Optical Networking. He currently serves on the editorial boards of six technical Journals and the Founder and EIC of *Wireless Communications and Mobile Computing Journal*, published by John Wiley (http://www.interscience.wiley.com/jpages/1530-8669/). He is also the Founder and General Chair of the IEEE International Conference of Wireless Networks, Communications, and Mobile Computing (IEEE WirelessCom 2005). He is the author of four books. He guest edited a number of special issues in Journal and Magazines. He also served as member, Chair, and General Chair of a number of conferences. He has more than 140 publications in refereed journals and conferences. Dr. Guizani received both the Best Teaching Award and the Excellence in Research Award from the University of Missouri-Columbia in 1999 (a college wide competition). He won the best Research Award from KFUPM in 1995 (a university wide competition). He was selected as the Best Teaching Assistant for two consecutive years at Syracuse University, 1988 and 1989. He is the Chair of TAOS and Vice-Chair of TCPC IEEE Technical Committees. Dr. Guizani is an active senior member of IEEE, member of IEEE Communication Society, IEEE Computer Society, ASEE, ACM, OSA, SCS, and Tau Beta Pi.

Hsiao-Hwa Chen (S'89-M'91-SM'01) is currently a full Professor and was the founding Director of the Institute of Communications Engineering of the National Sun Yat-Sen University, Taiwan. He received BSc and MSc degrees from Zhejiang University, China, and PhD degree from University of Oulu, Finland, in 1982, 1985 and 1990, respectively, all in Electrical Engineering. He has authored or co-authored over 200 technical papers in major international journals and conferences, five books and several book chapters in the areas of communications, including the books titled "Next Generation Wireless Systems and Networks" (512 pages) and "The Next Generation CDMA Technologies" (468 pages), both published by John Wiley and Sons in 2005 and 2007, respectively. He has been an active volunteer for IEEE various technical activities for over 20 years. Currently, he is serving as the Chair of IEEE Communications Society Radio Communications Committee. He served or is serving as symposium chair/co-chair of many major IEEE conferences, including VTC, ICC, Globecom and WCNC, etc. He served or is serving as Associate Editor or/and Guest Editor of numerous important technical journals in communications. He is serving as the Chief Editor (Asia and Pacific) for Wiley's *Wireless Communications and Mobile Computing (WCMC) Journal*, and Wiley's *International Journal of Communication Systems*, etc. He is the Editor-in-Chief of Wiley' *Security and Communication Networks Journal* (www.interscience.wiley.com/journal/security). He is also an adjunct Professor of Zhejiang University, China, and Shanghai Jiao Tung University, China.