

# A Framework for Distributed Key Management Schemes in Heterogeneous Wireless Sensor Networks

Kejie Lu, Yi Qian

Department of Electrical and Computer Engineering  
University of Puerto Rico at Mayagüez  
Mayagüez, Puerto Rico 00681  
Email: {lukejie, yqian}@ece.uprm.edu

Jiankun Hu

School of Computer Science and Information Technology  
Royal Melbourne Institute of Technology  
Melbourne, VIC 3000, Australia  
Email: jiankun@cs.rmit.edu.au

**Abstract**—Key management is a major challenge in the design and deployment of secure wireless sensor networks. A common assumption in most distributed key management schemes is that all sensor nodes have the same capability. However, recent research work has shown that the connectivity and lifetime of the sensor network can be substantially improved if a small number of sensor nodes have more energy capacity and transmission capability. Therefore, how to utilize these heterogeneity features to design a good distributed key management scheme has become an important issue and needs to be explored. In this paper, we propose a framework for key management schemes in distributed wireless sensor networks with heterogeneous sensor nodes. We show by simulations analysis that, with a small number of heterogeneous nodes, the wireless sensor network can achieve higher key connectivity and higher resilience.

## I. INTRODUCTION

Wireless sensor networks have recently come into prominence because they hold the potential to revolutionize many segments of our economy and life. Wireless sensor networks are suitable for various tasks, including surveillance, widespread environmental monitoring, manufacturing and business asset management, automation in the transportation, security, and health-care industries. Compared to existing infrastructure-based networks, wireless sensor networks can be used in virtually any environment, especially those where wired connections are not possible or the terrain is inhospitable.

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 controlled environment such as factories, homes, or hospitals, or in uncontrolled environment such as disaster or hostile area, particularly battlefield, where monitoring and surveillance is crucial. Clearly, for the uncontrolled and hostile environment, security for sensor networks becomes extremely important.

Security in wireless sensor networks has many challenges, ranging from the wireless nature of communications, resource limitations on sensor nodes, very large and dense networks, and unknown network topology prior to deployment, to high risk of physical attacks to unattended sensors [1]. In some deployment scenarios, sensor nodes need to operate under adversarial condition. To provide secure communications for

the wireless sensor networks, all the messages should be encrypted and authenticated. Consequently, security solutions for such applications depend on existence of strong and efficient key distribution mechanisms for uncontrolled environments of wireless sensor networks. Obviously, using a single shared key in the whole wireless sensor network is not a good idea because an adversary can easily obtain the key. Therefore, as a fundamental security service, pair-wise key establishment shall be used, which can enable the sensor nodes to communicate securely with each other 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 can 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 past few years, different pair-wise key distribution schemes have been developed for peer-to-peer wireless sensor networks (e.g., [3]–[10]) and hierarchical wireless sensor networks (e.g., [11], [12]).

For 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.

For 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]. Base stations can be much more powerful than 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 one or more hop neighborhood of the base stations. In general, the base stations are also the key distribution centers in the sensor networks because they are assumed to be tamper-resistance.

All the above solutions for distributed wireless sensor network assume that the sensor nodes are homogeneous with the same capabilities for each sensor network. For the solutions of hierarchical wireless sensor networks, except the base

stations (or cluster supervisors), the rest of the wireless sensor nodes are homogeneous with the same capabilities within each cluster.

Recently, however, heterogeneous sensor networks are getting more attention. Particularly, with the advances in antenna technologies like multiple-input multi-out (MIMO) antenna systems [13], directional antennas [14], and cooperative communications [15], the heterogeneity in terms of transmission range for wireless sensor nodes become a practical solution. Recent studies also show that such heterogeneity can increase the network performance and network lifetime without significantly increasing the cost [16]. Although it has been proved in [16] that optimal deployment of the heterogeneity is very hard in general, it shows that only a modest number of reliable, long-range backhaul links and line-powered nodes are required to have a significant impact.

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 detailed heterogeneous sensor deployment schemes and key distribution mechanisms, we investigate the effect of heterogeneity for the key management schemes in distributed wireless sensor networks. We show by simulations and analysis that, with a small percentage of powerful nodes that have reasonable storage, processing, and communication capabilities, the wireless sensor network can achieve higher key connectivity and higher resilience.

In the remaining of the paper, we will first introduce all technical aspects of the key distribution schemes and its related research in Section II. The description of our framework for key management schemes in heterogeneous distributed wireless sensor networks is given in Section III, followed by some special cases of the framework in Section IV. The simulation analysis and discussions are presented in Section V. We draw our conclusion in Section VI.

## II. SECURITY REQUIREMENTS FOR WIRELESS SENSOR NETWORKS AND RELATED WORKS

### A. Security Requirements For Wireless Sensor Networks And Related Works

In wireless sensor networks, the 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 channel and the 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 similarities between the two types of the networks [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 wireless sensor nodes in the network. 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 the 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 random solutions, key-chains are randomly selected from a key-pool and distributed to sensor nodes. In deterministic solutions, deterministic processes are used to design the key-pool and the key-chains to provide better key connectivity. Hybrid solutions use random approaches on deterministic solutions to improve 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 a set of keys from a key pool before deployment so any pair of sensor nodes has 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 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,

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

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 have 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 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 apriori.

For hierarchical wireless sensor networks, base stations (or supervisor nodes) are 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 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 the 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) that 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 generates a secret key, and find  $m$  intermediate nodes. For the LEAP solution, security of the system depends on the master-key the nodes received in the setup phase.

All the above 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 the adversary. However, the assumption that the nodes are tamper-proof cannot be ensured in many sensor network applications 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. THE NEW FRAMEWORK FOR KEY DISTRIBUTION SCHEMES

Up to now, all the existing solutions for distributed wireless sensor networks assume that the sensor nodes are homogeneous with the same capabilities for each sensor network. Recently, however, heterogeneous sensor network architectures have become popular, particularly in real deployment because of their potential to increase network lifetime and reliability without significantly increasing the cost [16]. Therefore, it is of significance to investigate how to design a suitable key management scheme for such networks.

In the following, we propose a framework for key management schemes in distributed peer-to-peer wireless sensor networks with heterogeneous sensor nodes.

#### A. Classes of Nodes

In this framework, we consider that the sensor nodes in the network have  $I$  classes, with Class 1 the least powerful nodes, and Class  $I$  the most powerful nodes, in terms of 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  $r_j < r_k$  if  $j < k$ . Therefore, if a Class  $j$  node is within the range of direct communication link of a Class  $k$  node, the Class  $j$  node might need multiple links to reach the Class  $k$  node if  $j < k$ . The heterogeneity of the sensor nodes are distributed in the wireless sensor network, with  $p_i$  the percentage of the Class  $i$  nodes, and

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

Here it is important to notice the fundamental difference between the heterogeneous wireless sensor networks assumed in this paper and the hierarchical wireless sensor networks in [11], [12]. In the hierarchical wireless sensor networks, the base stations (or cluster supervisors) are centralized nodes, and

more importantly, they are acting 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 are still peer-to-peer and distributed.

### B. 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: 1) initialization, 2) direct key setup, and 3) (optional) path key setup. The initialization step is performed to initialize the sensors by distributing polynomial shares to them, with the consideration of the heterogeneity of the sensor nodes. The direct key setup step is for any two nodes trying to establish a pair-wise key, they always first attempt to do so through direct key establishment. 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 disable.

### C. 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 of [6]. In particular, the general 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. Thus existing distributed key management schemes can all be included in the framework. For example, if  $I = 1$ , which means that the sensor network is homogeneous, we have the following special cases:

- 1) when all the polynomials are 0-degree ones and the sensor network is homogeneous, the polynomial pool degenerates into a key pool [3], [4]; and
- 2) when the polynomial pool has only one polynomial and the sensor network is homogeneous, then general framework degenerates into the polynomial based key pre-distribution [5].

The main challenge in this framework is how to assign polynomial shares to different classes of nodes. The procedure of the assignment problem can be separated into the following steps.

In the first step, classes of sensor nodes can be further partitioned into groups, where a unique group ID  $j$  will be assigned for each group. Here we notice that different sensor node deployment options can be considered in this step, for example, the square-grid, the hexagonal-grid, or probabilistic deployment scheme with a random distribution.

In the second step, the setup server will generate a set of polynomials for each class of nodes. Specifically, for class  $i$  ( $i = 1, 2, \dots, I$ ), the setup server randomly generates a set

$F_i$  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.

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

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

where  $F_{ij}(k)$  ( $F_{ij}(k) \subseteq F_i$ ) is a subset of polynomials that are selected from  $F_i$ . 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

$$F_{i_1 j}(k) \cap F_{i_2 j}(k) \neq \emptyset. \quad (3)$$

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

$$F_{i j_1}(k) \cap F_{i j_2}(k) \neq \emptyset. \quad (4)$$

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

Clearly, 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 for each sensor node in group  $j$  with class  $i$ . During the key distribution procedure, a number of factors must be considered, include 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.

To study the behavior of the proposed scheme, in the next few sections, we will conduct case studies within the new key management framework. Our studies show that, with a small percentage of heterogeneous nodes that have reasonable storage, processing and communication capabilities, the wireless sensor network can achieve higher key connectivity and higher resilience with our proposed key management scheme.

## IV. SPECIAL CASES OF THE NEW FRAMEWORK

From the description in the previous section, we can see that the new key generation scheme in our framework is essentially different to all existing schemes. Particularly, the heterogeneity features can now be taken into account. For instance, consider a typical heterogeneous wireless sensor network that is established to collect data in a distributed scenario. In this case, a sensor node shall 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.

Since the higher class nodes have a larger transmission range, it is nature that a low class node will tend to utilize the link between itself and a high class node to submit the observations. In other words, a high class node will more likely be chosen as the next-hop neighbor of nearby low class nodes

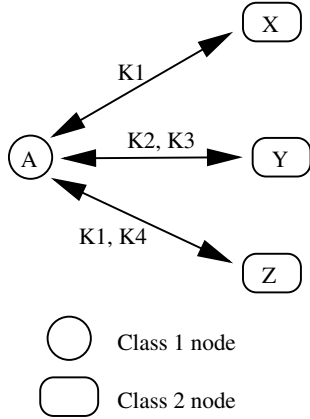


Fig. 1. An example for the proposed scheme.

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 consider two special key management schemes within the new framework for the above scenario. Specifically, we consider that there are two classes of the heterogeneous sensor nodes, i.e.  $I = 2$ . The two special cases are as the following: 1) the key-pool based key distributions; and 2) the polynomial-pool based key distributions, where the degree of polynomial is greater than 0.

When  $I = 2$ , 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 define that a  $C_1$  node is connected to the network if it shares at least  $q$  different keys with  $C_2$  nodes in its neighborhood. We then define the key connectivity as the probability that a  $C_1$  node is connected to the network. For simplicity, we only consider the direct key setup between a  $C_1$  and adjacent  $C_2$  nodes.

An example of this scheme is illustrated in Fig. 1, where node  $A$  is a  $C_1$  node and node  $X$ ,  $Y$ , and  $Z$  are  $C_2$  nodes. In this example, node  $X$ ,  $Y$ , 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 resilience, while the connectivity can also be maintained.

For the polynomial based key distributions, the main difference from the key-pool based scheme is that, a  $C_1$  node can have two different key with two  $C_2$  nodes even if they share the same polynomial, while the number of unique keys is only 1 for the key-pool based scheme.

The performance study of these two schemes will be given in the next section, where we will focus on these two special

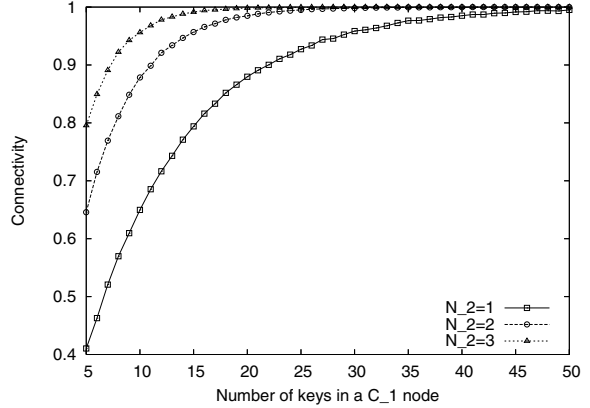


Fig. 2. Connectivity vs. the number of keys in a  $C_1$  node (key-pool based scheme,  $q = 1$ ).

cases to better understand the performances of the framework in heterogeneous wireless sensor networks.

## V. SIMULATION RESULTS AND DISCUSSIONS

In this section, we give the simulation results and the discussions for the performance of different configurations of key management schemes described in the previous section. The settings of our simulation experiments can be summarized as the following.

- There are two classes of sensor nodes, denoted as  $C_1$  and  $C_2$ , in the network.
- We consider a small cluster of a sensor network, in which the number of  $C_1$  node is 40 and the number of  $C_2$  nodes is  $N_2$ .
- Each  $C_1$  node in the cluster can directly communicate with all  $C_2$  nodes within the cluster.
- We investigate two key distribution schemes: (1) key-pool based scheme and (2) polynomial-pool based scheme.
- For the key-pool based scheme, we assume that the size of key pool is 10,000 and the number of keys in any  $C_2$  node is fixed to 1,000.
- For the polynomial-pool based scheme, we assume that the size of polynomial pool is 100 and the number of polynomials in any  $C_2$  node is fixed to 30.
- 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.

### 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 that  $q = 1$ . We can first observe 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 increase the connectivity, especially when the number of keys in  $C_1$  node is small and medium.

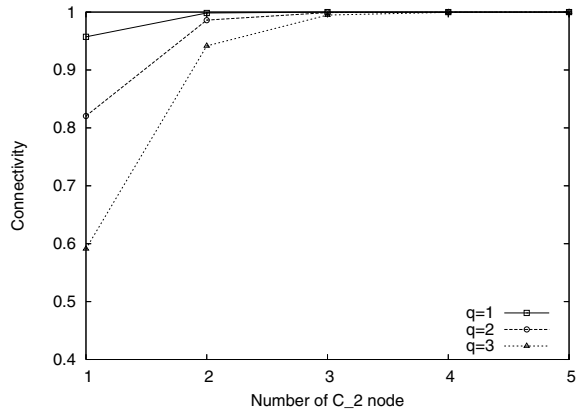


Fig. 3. Connectivity vs. the number of  $C_2$  nodes (key-pool based scheme, 30 keys per  $C_1$  node).

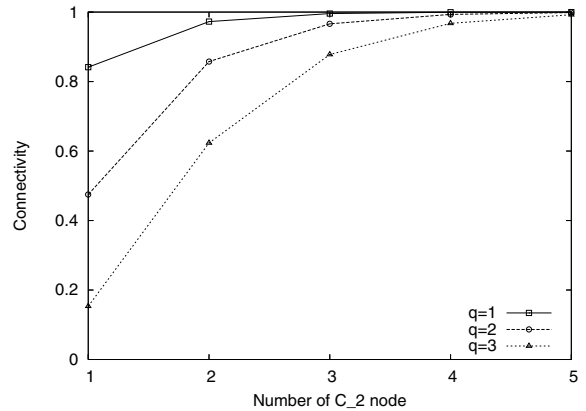


Fig. 5. Connectivity vs. the number of  $C_2$  nodes (polynomial-pool based scheme,  $P_1 = 5$ ).

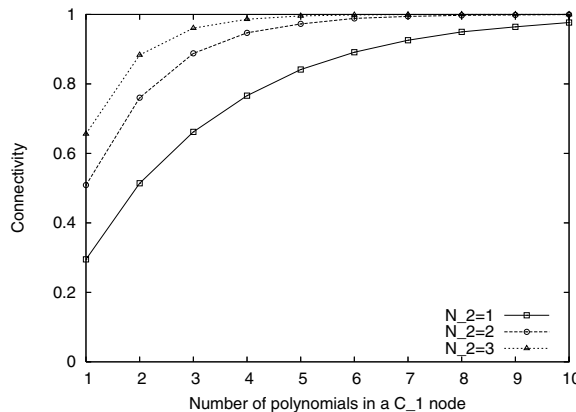


Fig. 4. Connectivity vs. the number of keys in a  $C_1$  node (polynomial-pool based scheme,  $q = 1$ ).

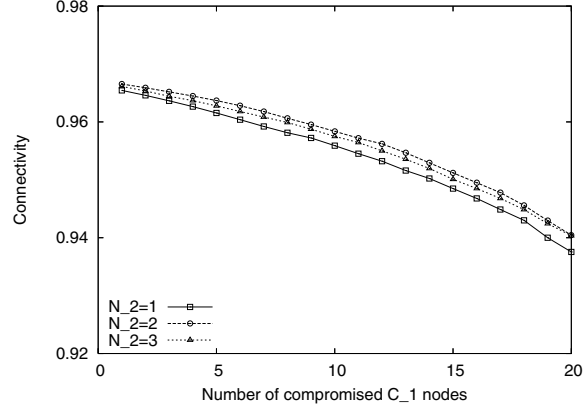


Fig. 6. Connectivity of uncompromised  $C_1$  nodes vs. the number of compromised  $C_1$  nodes (key-pool based scheme,  $q = 1$ ).

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 demonstrate in Fig. 3 the performance of connectivity versus the number of  $C_2$  nodes in the cluster with different value of  $q$ , where we let the number of keys in any  $C_1$  node be 30. It can be clearly noted that the network connectivity can be substantially improved when the number of  $C_2$  nodes increase from 1 to 3. Interestingly, the connectivity converges to 1 if  $N_2 = 3$ , which means that we do not need to deploy more  $C_2$  node if the resilience is not a concern.

In Fig. 4 and Fig. 5, we study the performance of the polynomial-pool based key management scheme. Fig. 4 shows the connectivity versus the number of keys in a  $C_1$  node with different number of  $C_2$  nodes for the polynomial-pool

based scheme, where we assume that  $q = 1$ . Fig. 5 shows the connectivity versus the number of  $C_2$  nodes with different values of  $q$ , for polynomial-pool based scheme. From Fig. 4 and Fig. 5, we can observe similar trends as those of Fig. 2 and Fig. 3, which means that a few number of  $C_2$  nodes can significantly improve the system performance for both schemes.

### B. Reliability of the New Schemes

From Fig. 3 and Fig. 5 we can also conclude 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 study the performance of the sensor network when some  $C_1$  nodes are compromised. Here we notice that it is reasonable to assume

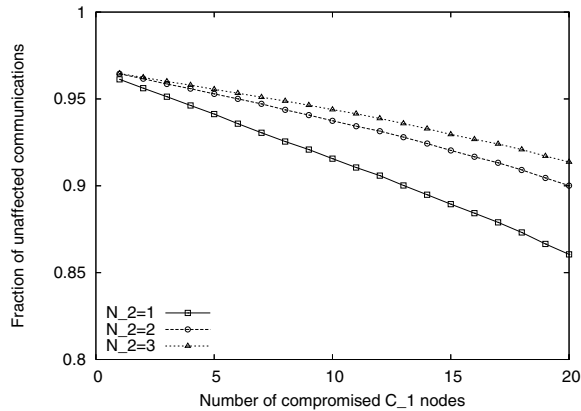


Fig. 7. Fraction of unaffected communications from uncompromised nodes vs. the number of compromised  $C_1$  nodes (key-pool based scheme,  $q = 1$ ).

that  $C_2$  nodes are more tamper resistant. In Fig. 6 and Fig. 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 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, we find that the connectivity is relatively high even if 20 nodes (amongst 40 nodes as a total) are compromised. Through 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 study the resilience of the scheme from another perspective, in which we assume 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. From Fig. 1 we can see 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, 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  $K_4$ ). This phenomenon can be clearly observed from Fig. 7, where we find that a high percentage of secured communications can still be maintained even if half of the  $C_1$  nodes are compromised. Moreover, we can see that more  $C_2$  nodes can help to increase the fraction of unaffected communications, given the same number of compromised  $C_1$  node.

## VI. CONCLUSIONS

In this paper, we proposed a general framework for key management schemes in distributed peer-to-peer wireless sensor networks with heterogeneous sensor nodes. We show by

simulations that, with a small number of powerful sensor nodes that have reasonable storage, processing and transmission capabilities, the wireless sensor network can achieve higher key connectivity and system performance. Our future work will focus on developing analytical and simulation models to analyze distributed key management schemes under the proposed framework for heterogeneous wireless sensor networks in terms of connectivity, resilience, and scalability.

## ACKNOWLEDGMENT

This work was supported in part by the US National Science Foundation (NSF) under Award Number 0424546, and in part by NSF EPSCoR start-up grant in Puerto Rico.

## REFERENCES

- [1] S. A. Camtepe and B. Yener, "Key Distribution Mechanisms for Wireless Sensor Networks: a Survey," Department of Computer Science, Rensselaer Polytechnic Institute, Technical Report TR-05-07, March 23, 2005.
- [2] W. Stallings, "Cryptography and Network Security," Pearson Education, Inc., Upper Saddle River, New Jersey, 3rd Edition, 2003.
- [3] L. Eschenauer, and V. D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," in *Proc. of 9th ACM Conference on Computer and Communication Security*, November 2002.
- [4] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," in *Proc. of IEEE Symposium on Research in Security and Privacy*, May 2003.
- [5] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-Secure Key Distribution for Dynamic Conferences," in *Proc. Advances in Cryptology - CRYPTO'92*, LNCS 740, pages 471–486, 1993.
- [6] D. Liu, and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," in *Proc. of the 10th ACM Conference on Computer and Communications Security*, October 2003.
- [7] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A Pairwise Key Predistribution Scheme for Wireless Sensor Networks," in *Proc. of the 10th ACM Conference on Computer and Communications Security*, October 2003.
- [8] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge," in *Proc. of IEEE INFOCOM'04*, March 2004.
- [9] Y. Zhou, Y. Zhang, and Y. Fang, "LLK: A Link-Layer Key establishment Scheme for Wireless sensor Networks," in *Proc. of IEEE WCNC'2005*, March 2005.
- [10] S.-P. Chan, R. Poovendran, and M. T. Sun, "A Key Management Scheme in Distributed sensor Networks Using Attack Probabilities," in *Proc. of IEEE GLOBECOM'2005*, November 2005.
- [11] Y. Law, R. Corin, S. Etalle, and P. Hartel, "A Formally Verified Decentralized Key Management for Wireless Sensor Networks," *Personal/Wireless Communications*, LNCS, Vol. 2775, pp.27–39, 2003.
- [12] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," in *Proc. of IEEE Symposium on Research in Security and Privacy*, May 2003.
- [13] D. Gesbert, M. Shaif, D. S. Shiu, P. J. 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 Antenna: A complete System Solution," *IEEE Journal on Selected Areas in Communications*, Vol. 23, No. 3, pp. 496–506, Mar. 2005.
- [15] Shuguang Cui, Andrea J. Goldsmith, and Ahmad Bahai, "Energy-efficiency of MIMO and Cooperative MIMO Techniques in Sensor Networks," *IEEE Journal on Selected Areas of Communications*, 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. of IEEE INFOCOM'05*, Mar. 2005.

