Key Management in Wireless Sensor Networks Extended Abstract

Wenliang Du Jing Deng Yunghsiang S. Han Pramod K. Varshney
Department of Electrical Engineering and Computer Science,
Syracuse University, Syracuse, NY 13244-1240, USA
Email: {wedu,jdeng01,yshan,varshney}@ecs.syr.edu

I. Introduction

Recent advances in electronic and computer technologies have paved the way for the proliferation of wireless sensor networks (WSN). Sensor networks usually consist of a large number of ultra-small autonomous devices. Each device, called a sensor node, is battery powered and equipped with integrated sensors, data processing capabilities, and short-range radio communications. In typical application scenarios, sensor nodes are spread randomly over the deployment region under scrutiny and collect sensor data. Examples of sensor network projects include SmartDust [1] and WINS [2].

Sensor networks are being deployed for a wide variety of applications [3], including military sensing and tracking, environment monitoring, patient monitoring and tracking, smart environments, etc. When sensor networks are deployed in a hostile environment, security becomes extremely important, as they are prone to different types of malicious attacks. For example, an adversary can easily listen to the traffic, impersonate one of the network nodes, or intentionally provide misleading information to other nodes. To provide security, communication should be encrypted and authenticated. An open research problem is how to bootstrap secure communications among sensor nodes, i.e. how to set up secret keys among communicating nodes?

This key agreement problem is a part of the *key management* problem, which has been widely studied in general network environments. There are three types of general key agreement schemes: trusted-server scheme, self-enforcing scheme, and key pre-distribution scheme. The *trusted-server* scheme depends on a trusted server for key agreement between nodes, e.g., Kerberos [4]. This type of scheme is not suitable for sensor networks because there is usually no trusted infrastructure in sensor networks. The *self-enforcing* scheme depends on asymmetric cryptography, such as key agreement using public key certificates. However, limited computation and energy resources of sensor nodes often make it undesirable to use public key algorithms, such as Diffie-Hellman key agreement [5] or RSA [6], as pointed out in [7]. The third type of key agreement scheme is key *pre-distribution*, where key information is distributed among all sensor nodes prior to deployment. If we know which nodes are more likely to stay in the same neighborhood before deployment, keys can be decided *a priori*. However, because of the randomness of the deployment, knowing the set of neighbors deterministically might not be feasible.

There exist a number of key pre-distribution schemes. A naive solution is to let all the nodes carry a *master* secret key. Any pair of nodes can use this global master secret key to achieve key agreement and obtain a new pairwise key. This scheme does not exhibit desirable network resilience: if one node is compromised, the security of the entire sensor network will be compromised. Some existing studies suggest storing the master key in tamper-resistant hardware to reduce the risk, but this increases the cost and energy consumption of each sensor. Furthermore, tamper-resistant hardware might not always be safe [8]. Another key pre-distribution scheme is to let each sensor carry $N-1$ secret pairwise keys, each of which is known only to this sensor and one of the other $N-1$ sensors (assuming N is the total number of sensors). The resilience of this scheme is perfect because compromising one node does not affect the security of communications among other nodes; however, this scheme is impractical for sensors with an extremely limited amount of memory because N could be large. Moreover, adding new nodes to a pre-existing sensor network is difficult because the existing nodes do not have the new nodes' keys.

II. A Pairwise Key Pre-Distribution Scheme

We propose a new key pre-distribution scheme [9]. Our scheme builds on Blom's key pre-distribution scheme [10] and combines the random key pre-distribution method with it. Our results show that the resilience of our scheme is substantially better than Blom's scheme as well as other random key pre-distribution

schemes. In [10], Blom proposed a key pre-distribution scheme that allows *any* pair of nodes to find a secret pairwise key between them. Compared to the $(N-1)$-pairwise-key pre-distribution scheme, Blom's scheme only uses $\lambda+1$ memory spaces with λ much smaller than N. The tradeoff is that, unlike the $(N-1)$-pairwise-key scheme, Blom's scheme is not perfectly resilient against node capture. Instead it has the following λ-secure property: *as long as an adversary compromises less than or equal to λ nodes, uncompromised nodes are perfectly secure; when an adversary compromises more than λ nodes, all pairwise keys of the entire network are compromised.*

The threshold λ can be treated as a security parameter in that selection of a larger λ leads to a more secure network. This threshold property of Blom's scheme is a desirable feature because an adversary needs to attack a significant fraction of the network in order to achieve high payoff. However, λ also determines the amount of memory to store key information, as increasing λ leads to higher memory usage. **The goal of our scheme** is to increase network's resilience against node capture without using more memory.

Blom's scheme uses *one* key space for all nodes to make sure that any pair can compute its pairwise key in this key space. Motivated by the random key pre-distribution schemes presented in [11], [12], we propose a new scheme using *multiple* key spaces: we first construct ω spaces using Blom's scheme, and each sensor node carries key information from τ ($2 \leq \tau < \omega$) randomly selected key spaces. According to Blom's scheme, if two nodes carry key information from a common space, they can compute their pairwise key from the information; when two nodes do not carry key information from a common space, they can conduct key agreement via other nodes which share pairwise keys with them. Our analysis has shown that using the same amount of memory, our new scheme is substantially more resilient than Blom's scheme and other key pre-distribution schemes.

To further improve the resilience, we also develop a two-hop-neighbor key pre-distribution scheme. The idea is to let the direct neighbor forward the message from a sender, such that nodes that are two hops away from the sender can also receive the message. The nodes that are two hops away are known as two-hop neighbors. Treating two-hop neighbors as "direct" neighbors, the number of neighbors of each sender increases fourfold. The consequence is that the resilience threshold can be improved as well. Our results show that under certain conditions, the threshold can be improved to four times as much as that of our first scheme.

A. Main Results

The main contributions of this work are summarized as follows:

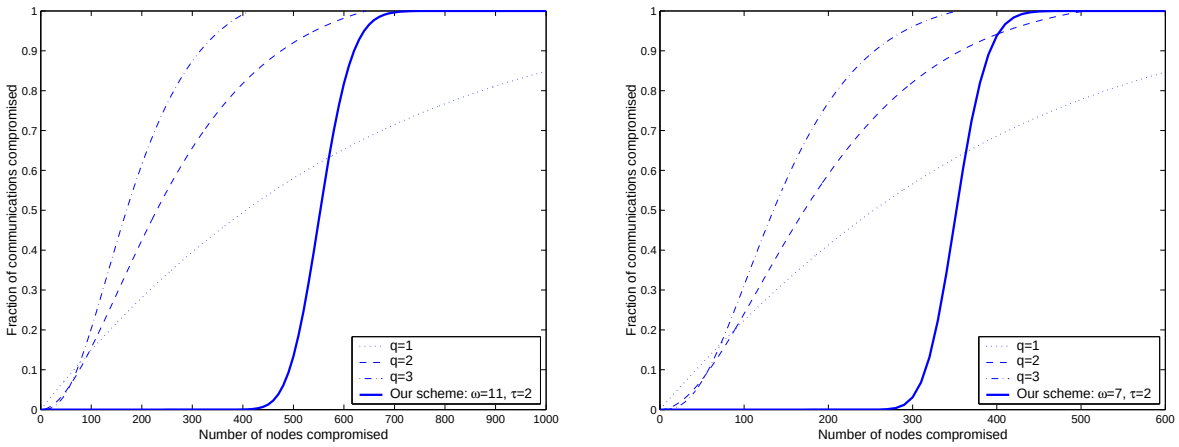
1) Our scheme substantially improved network resilience against node capture over existing schemes.
2) We have conducted a thorough theoretical analysis of security, and communication and computation overhead analysis.

Our scheme has a number of appealing properties. First, our scheme is scalable and flexible. For a network that uses 64-bit secret keys, our scheme allows up to $N = 2^{64}$ sensor nodes. These nodes do not need to be deployed at the same time; they can be added later, and still be able to establish secret keys with existing nodes. Second, compared to existing key pre-distribution schemes, our scheme is substantially more resilient against node capture. Our analysis and simulation results have shown, for example, that to compromise 10% of the secure links in the network secured using our scheme, an adversary has to compromise 5 times as many nodes as he/she has to compromise in a network secured by Chan-Perrig-Song scheme [12] or Eschenauer-Gligor scheme [11]. The comparison with these two schemes are depicted in Fig. 1. In the figure, $q = 1$ refers to the Eschenauer-Gligor scheme and $= 2, 3$ refers to the Chan-Perrig-Song scheme, p represents the probability of any two neighboring nodes sharing at least one space (we also call p the local connectivity).

In addition to the security analysis, we have conducted a thorough overhead analysis to show the efficiency of our scheme. The communication overhead analysis has shown that when the local connectivity is greater than 0.33, a node can almost (with very high probability) reach its neighbor within at most 3 hops. For the computation overhead, although our scheme involves modular multiplications, we have shown that the energy cost is about the same as encrypting a message of length 3200 bits using AES.

III. Key Management Scheme Using Deployment Knowledge

None of the key pre-distribution schemes exploits the *node deployment knowledge*, which, in practice, can be derived from the way that nodes are deployed. Let us look at a deployment method that uses an airplane to deploy sensor nodes. The sensors are first pre-arranged in a sequence of smaller groups. These groups are dropped out of the airplane sequentially as the plane flies forward. This is analogous to parachuting troops or dropping cargo in a sequence. The sensor groups that are dropped next to each other have a better chance to be close to



(a) $p = 0.33$ (b) $p = 0.5$

Fig. 1. The Pairwise Key Pre-Distribution Scheme

each other on the ground. This spatial relation between sensors derived prior to deployment can be useful for key pre-distribution. The goal of this paper is to show that knowledge regarding the actual non-uniform sensor deployment can help us improve the performance of a key pre-distribution scheme.

Knowing which sensors are close to each other is important to key pre-distribution. In sensor networks, long distance peer-to-peer secure communication between sensor nodes is rare and unnecessary in many applications. The primary goal of secure communication in wireless sensor networks is to provide such communications among neighboring nodes. Therefore, the most important knowledge that can benefit a key-predistribution scheme is the knowledge about *who can be the neighbors of each sensor node*. When we know deterministically the neighbors of each node in the network, the key pre-distribution becomes trivial: for each node n, we just need to generate a pairwise key between n and each of its neighboring nodes, and save these keys in n's memory. This guarantees that each node can establish a secure channel with each of its neighbors after deployment.

However, because of the randomness of deployment, it is unrealistic to know the exact set of neighbors of each node, but knowing the set of *possible* neighbors for each node is much more realistic. However, the number of possible neighbors can be very large and it may not be feasible for a sensor to store the secret keys for each potential neighbor due to memory limitations. This problem can be solved using the random key pre-distribution scheme [11], i.e., instead of guaranteeing that any two neighboring nodes can find a common secret key with 100% certainty, we only guarantee that any two neighboring nodes can find a common secret key with a certain probability p. In this paper, we exploit deployment knowledge in the random key pre-distribution scheme [11], such that the probability p can be maximized while the other performance metrics (such as security and memory usage) are not degraded.

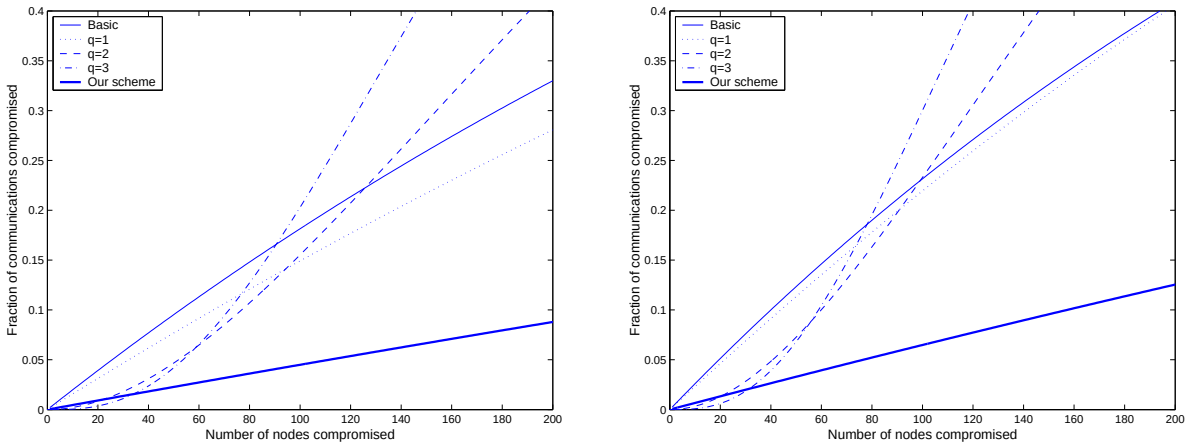
Deployment knowledge can be modeled using probability density functions (pdfs). When the pdf is uniform, no information can be gained on where a node is more likely to reside. All the existing key pre-distribution schemes assume such a uniform distribution. In this paper, we look at a non-uniform pdf, the Normal (Gaussian) distribution. Since this distribution is different from uniform distribution, it is equivalent to saying that we know that a sensor is more likely to be deployed in certain areas. We show how this knowledge can help improve the random key pre-distribution scheme proposed by Eschenauer and Gligor in [11].

A. Main Results

The main contributions of this work are summarized in the following:

1) We model node deployment knowledge in a wireless sensor network, and develop a key pre-distribution scheme based on this model. This is the first attempt at the use of deployment knowledge while developing a key pre-distribution scheme.
2) We show that key pre-distribution with deployment knowledge can substantially improve a network's connectivity and resilience against node capture, and reduce the amount of memory required.

The results and comparison with existing key pre-distribution schemes are depicted in Fig. 2 ("Basic"



(a) $p = 0.33$ (b) $p = 0.50$

Fig. 2. Key Pre-distribution Using Deployment Knowledge

refers to the Eschenauer-Gligor scheme; "$q = 1, 2, 3$" refers to the Chan-Perrig-Song scheme). The figures show that our scheme substantially lowers the fraction of compromised communication after x nodes are compromised. Such an improvement is attributed to the deployment knowledge, which enables us to reduce the number of unnecessary keys carried by each sensor node.

IV. Future Work

In our future work, we will focus on the following:

1) we will investigate how much the deployment knowledge can improve the q-composite random key pre-distribution scheme, the pairwise key pre-distribution scheme proposed by Chan, Perrig, and Song [12], and our Blom scheme-based key pre-distribution scheme [9].
2) We will study the resilience situation when the adversaries are limited in a local area.
3) Other deployment strategies and associated distributions will also be considered.

References

[1] J. M. Kahn, R. H. Katz, and K. S. J. Pister, "Next century challenges: Mobile networking for smart dust," in *Proceedings of the 5th Annual ACM/IEEE Internation Conference on Mobile Computing and Networking (MobiCom)*, 1999, pp. 483–492.

[2] Wireless Integrated Network Sensors, University of California, Available: http://www.janet.ucla.edu/WINS.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, August 2002.

[4] B. C. Neuman and T. Tso, "Kerberos: An authentication service for computer networks," *IEEE Communications*, vol. 32, no. 9, pp. 33–38, September 1994.

[5] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, pp. 644–654, November 1976.

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

[7] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar, "Spins: Security protocols for sensor networks," in *Proceedings of the 7th Annual ACM/IEEE Internation Conference on Mobile Computing and Networking (MobiCom)*, Rome, Italy, July 2001, pp. 189–199.

[8] R. Anderson and M. Kuhn, "Tamper resistance - a cautionary note," in *Proceedings of the Second Usenix Workshop on Electronic Commerce*, November 1996, pp. 1–11.

[9] W. Du, J. Deng, Y. S. Han, and 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*, October 2003.

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

[11] L. Eschenauer and 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.

[12] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *IEEE Symposium on Security and Privacy*, Berkeley, California, May 11-14 2003, pp. 197–213.