International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Review of Pairwise Key Establishment Techniques for Wireless Sensor Networks

Dinesh Dhakar[1], Ravi Khatri[2]

[1]PG Student, Dep't. Of CSE, VITM, Indore, M.P, India
[2]Assoc. Professor, Dep't. Of CSE, VITM, Indore, M.P, India

Abstract: ***To achieve security in wireless sensor networks, it is important to be able to encrypt and authenticate messages sent among sensor nodes. Keys for encryption and authentication purposes must be agreed upon by communicating nodes. Due to resource constraints, achieving such key agreement in wireless sensor networks is non-trivial. Many key agreement schemes used in general networks, such as Diffie-Hellman and public-key based schemes, are not suit-able for wireless sensor networks. Pre-distribution of secret keys for all pairs of nodes is not viable due to the large amount of memory used when the network size is large. To solve the key pre-distribution problem, two elegant key pre-distribution approaches have been proposed recently [11, 7].***

Keywords: Security, Key establishment, Mobile sensor networks, Key prioritization, Post-deployment knowledge

1. Introduction

Distributed sensor networks have received a lot of attention recently due to its wide applications in military as well as civilian operations. Example applications include target tracking, scientific exploration, and data acquisition in hazardous environments. The sensor nodes are typically small, low-cost, battery powered, and highly resource constrained. They usually communicate with each other through wireless links. Security services such as authentication and key management are critical to secure the communication between sensor nodes in hostile environments. As one of the most fundamental security services, pair wise key establishment enables the sensor nodes to communicate securely with each other using cryptographic techniques. However, due to the resource constraints on sensor nodes, it is not feasible for them to use traditional pairwise key establishment techniques such as public key cryptography and key distribution center (KDC).

Instead of the above two techniques, sensor nodes may establish keys between each other through key predistribution, where keying materials are predistributed to sensor nodes before deployment. As two extreme cases, one may setup a global key among the network so that two sensor nodes can establish a key based on this global key, or assign each sensor node a unique random key with each of the other nodes. However, the former is vulnerable to the compromise of a single node, and the latter introduces huge storage overhead on sensor nodes.

Eschenauer and Gligor proposed a probabilistic key predistribution scheme recently for pairwise key establishment [Eschenauer and Gligor 2002]. The main idea is to let each sensor node randomly pick a set of keys from a key pool before the deployment so that any two sensor nodes have a certain probability to share at least one common key. Chan et al. further extended this idea and developed two key predistribution techniques: a q – composite key predistribution scheme and a random pair wise keys scheme [Chan et al. 2003]. The q -composite key predistribution also uses a key pool but requires two nodes compute a pairwise key from at least q predistributed keys that they share. The random pair wise keys scheme randomly picks pairs of sensor nodes and assigns each pair a unique random key. Both schemes improve the security over the basic probabilistic key predistribution scheme. However, the pair wise key establishment problem is still not fully solved. For the basic probabilistic and the q -composite key predistribution schemes, as the number of compromised nodes increases, the fraction of affected pair wise keys increases quickly. As a result, a small number of compromised nodes may affect a large fraction of pair wise keys. Though the random pair wise keys scheme does not suffer from the above security problem, given a memory constraint, the network size is strictly limited by the desired probability that two sensor nodes share a pair wise key, the memory available for keys on sensor nodes, and the number of neighbor nodes that a sensor node can communicate with.

In this paper, we develop a number of key predistribution techniques to deal with the above problems. We first develop a general framework for pair wise key establishment based on the polynomial-based key predistribution protocol in [Blundo et al. 1993] and the probabilistic key distribution in [Eschenauer and Gligor 2002; Chan et al. 2003]. This framework is called polynomial pool-based key predistribution, which uses a polynomial pool instead of a key pool in [Eschenauer and Gligor 2002; Chan et al. 2003]. The secrets on each sensor node are generated from a subset of polynomials in the pool. If two sensor nodes have the secrets generated from the same polynomial, they can establish a pairwise key based on the polynomial-based key predistribution scheme. All the previous schemes in [Blundo et al. 1993; Eschenauer and Gligor 2002; Chan et al. 2003] can be considered as special instances in this framework.

By instantiating the components in this framework, we further develop two novels pair-wise key predistribution schemes: a random subset assignment scheme and a hypercube-based scheme. The random subset assignment scheme assigns each sensor node the secrets generated

from a random subset of polynomials in the polynomial pool. The hypercube-based scheme arranges polynomials in a hypercube space, assigns each sensor node to a unique coordinate in the space, and gives the node the secrets generated from the polynomials related to the corresponding coordinate. Based on this hypercube, each sensor node can then identify whether it can directly establish a pair wise key with another node, and if not, what intermediate nodes it can contact to indirectly establish the pair wise key. Our analysis indicates that our new schemes have some nice features compared with the previous methods. In particular, when the fraction of compromised secure links is less than 60%, given the same storage constraint, the random subset assignment scheme provides a significantly higher probability of establishing secure communication between non-compromised nodes than the previous methods. Moreover, unless the number of com-promised nodes sharing a common polynomial exceeds a threshold, compromise of sensor nodes does not lead to the disclosure of keys established between non-compromised nodes using this polynomial.

Similarly, the hypercube-based scheme also has a number of attractive properties. First, it guarantees that any two nodes can establish a pair wise key when there are no compromised nodes, provided that the sensor nodes can communicate with each other. Second, it is resilient to node compromise. Even if some sensor nodes are compromised, there is still a high probability to re-establish a pair wise key between non-compromised nodes. Third, a sensor node can directly determine whether it can establish a pair wise key with another node and how to compute the pair wise key if it can. As a result, there is no communication overhead during the discovery of directly shared keys. Evaluation of polynomials is essential to the proposed schemes, since it affects the performance of computing a pair wise key. To reduce the computation at sensor nodes, we provide an optimization technique for polynomial evaluation. The basic idea is to compute multiple pieces of key fragments over some special finite fields such as F28 + 1 and F216 + 1 and concatenate these fragments into a regular key. A nice property provided by such finite fields is that no division is necessary for modular multiplication. As a result, evaluation of polynomials can be performed efficiently on low cost processors on sensor nodes that do not have division instructions. Our analysis indicates that such a method only slightly decreases the uncertainty of the keys.

2. Related Work

The Eschenauer-Gligor scheme [11] and the Chan-Perrig-Song scheme [7] have been reviewed earlier in this section. Detailed comparisons with these two schemes will be given in Section 4.Some other related work is discussed next. Du et al. proposed a method to improve the Eschenauer-Gligor scheme using a priori deployment knowledge [9]. This method can also be used to further improve other random key pre-distribution schemes, such as the Chan-Perrig-Song scheme and the scheme presented in this paper. Blundo et al. proposed several schemes which allow any group of t parties to compute a common key while being secure against collusion between some of them [5]. These schemes focus on saving communication costs while memory constraints are not placed on group members. When t = 2, one of these schemes is actually a special case of Blom's scheme [4]. A modified version of Blom's scheme will be reviewed in Section 2. Compared to Blom's scheme, our scheme is more resilient and more memory-efficient. Perrig et al. proposed SPINS, a security architecture specifically designed for sensor networks [16]. In SPINS, each sensor node shares a secret key with the base station. Two sensor nodes can-not directly establish a secret key. However, they can use the base station as a trusted third party to set up the secret key.

3. Multiple - Space Keypre - Distribution Scheme

To achieve better resilience against node capture, we propose a new key pre-distribution scheme that uses Blom's method as a building block. Our idea is based on the following observations: Blom's method guarantees that any pair of nodes can find a secret key between themselves. To represent this we use concepts from graph theory and draw an edge between two nodes if and only if they can find a secret key between themselves. We will get a complete graph (i.e., an edge exists between all node pairs). Although full connectivity is desirable, it is not necessary. To achieve our goal of key agreement, all we need is a connected graph, rather than a complete graph. Our hypothesis is that by requiring the graph to be only connected, each sensor node needs to carry less key information. Before we describe our proposed scheme, we define a key space (or space in short) as a tuple (D, G), where matrices D and G are as defined in Blom's scheme. We say a node picks a key space (D, G) if the node carries the secret information generated from (D, G) using Blom's scheme. Two nodes can calculate their pair wise key if they have picked a common key space.

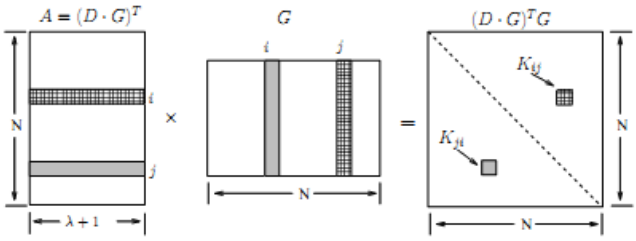

Figure 1: Generating Keys in Blom's Scheme

4. Issues in Mobile Sensor Networks

To design a key pre-distribution scheme in mobile sensor networks, we may consider the following issues. The first issue is that we should not assume any prior knowledge of sensors' locations However; we can assume the post-deployment knowledge of sensors' locations. This assumption becomes practical due to the following researches. Akyildiz et al. [1] pointed out that "most of the sensing tasks require knowledge of positions" and also "location finding systems are required by many of the proposed sensor network routing protocols". There are several recent advances in determining individual sensor nodes' positions either with a global positioning system (GPS) or local references [12, 19]. Sastry et al. [22], Lazos

et al. [11], Du et al. [7] and Liu et al. [16, 17] describe the methods of determining secure locations. Thus, in a mobile sensor network, it is a possible task for sensor nodes to determine their deployment locations securely after deployment. Hence, we can use advantage of post-deployment knowledge in mobile sensor networks. The second issue is to use extra memory for applications to store an excessive amount of pre-distributed keys as well as the direct pair wise keys between neighbor sensors. Crossbow Technology Inc. [10] develops a typical MICA2 mote sensor device which has 512 EEPROM, but only 4KB RAM. Thus, it is practical to store more pre-distributed keying information in a sensor device.

5. Key Prioritization Technique Using Post-Deployment Knowledge

We describe briefly the concept of the key prioritization technique proposed by Liu and Ning [15]. Their scheme takes the advantage of the post-deployment knowledge of sensor nodes to improve the pair wise key pre-distribution in static sensor networks. This scheme assigns each sensor node an excessive amount of pre-distributed keys in key pre-distribution phase by using the memory for sensing applications. Then, depending on the post-deployment knowledge, it prioritizes the pre-distributed keys in key prioritization phase, and discard the low priority keys in order to thwart against node capture attack. Since the low priority keys are deleted from the memory, so the returned memory is used for the application part.

In direct key establishment (i.e., shared key discovery) phase, two neighbor nodes establish a pair wise key by exchanging the IDs of the higher priority keys. Liu and Ning then applied it to the polynomial pool-based scheme [13] and its analysis shows that it significantly improves the security and performance than the previous key pre-distribution schemes.

6. Conclusion

We have presented in this paper several pair wise key pre-distribution scheme for wireless sensor networks. Pair wise key distribution has a number of appealing properties. First, this 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 or Eschenauer-Gligor scheme. Furthermore, we have also shown that network resilience can be further improved if we use multi-hop neighbors.

References

[1] Wireless Integrated Network Sensors, University of California, Available: http://www.janet.ucla.edu/WINS.
[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. IEEE Communications Magazine, 40(8):102–114, August 2002
[3] R. Anderson and M. Kuhn. Tamper resistance - a cautionary note. In Proceedings of the Second Usenix Workshop on Electronic Commerce, pages 1–11, November 1996.
[4] 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, 209:335–338, 1985.
[5] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. Perfectly-secure key distribution for dynamic conferences. Lecture Notes in Computer Science,740:471–486, 1993.
[6] D. W. Carman, P. S. Kruus, and B. J. Matt. Constraints and approaches for distributed sensor network security. NAI Labs Technical Report #00-010, available athttp://download.nai.com/products/media/nai/zip/nailabs-report-00-010-final.zip,2000.
[7] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In IEEE Symposium on Security and Privacy, pages 197–213, Berkeley, California, May 11-14 2003.
[8] W. Diffie and M. E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, 22:644–654, November 1976.
[9] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney. Akey management scheme for wireless sensor networks using deployment knowledge. Technical Report, Syracuse University, July 2003. Available fromhttp://www.cis.syr.edu/~wedu/Research/paper/ddhcv03.pdf.
[10] Erd˝os and R´enyi. On random graphs I. Publ. Math. Debrecen, 6:290–297, 1959.
[11] L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In Proceedings of the 9thACM conference on Computer and communications security, November 2002.
[12] 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 International Conference on Mobile Computing and Networking (MobiCom), pages 483–492, 1999.
[13] F. J. Mac Williams and N. J. A. Sloane. The Theory ofError-Correcting Codes. New York, NY: Elsevier Science Publishing Company, Inc., 1977.
[14] D. Malkhi, M. Reiter, A. Wool, and R. N. Wright. Probabilistic quorum systems. Information and Computation, (2):184–206, November 2001.
[15] B. C. Neuman and T. Tso. Kerberos: An authentication service for computer networks. IEEE Communications,32(9):33–38, September 1994.
[16] 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 International Conference on Mobile Computing and Networking (MobiCom), pages 189–199, Rome, Italy, July 2001.
[17] W. W. Peterson. Error-Correcting Codes. Cambridge, MA: Mass. Inst. Tech., second edition, 1972.
[18] R. L. Rivest, A. Shamir, and L. M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2):120–126, 1978