A Review of Pairwise Key Establishment Techniques for Wireless Sensor Networks

Shishir Sharma[1], Gajendra Singh Chandel[2]

PG Student, Department of CSE, SSSIST, Sehore (M.P), India

Associate Professor, Department of CSE, SSSIST, Sehore (M.P), India

Abstract: ***To achieve security in wireless sensor networks, it is important tobe able to encrypt and authenticate messages sent among sensornodes. Keys for encryption and authentication purposes must beagreed 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 keysfor 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 approacheshave 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 targettracking, 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 thecommunication between sensor nodes in hostile environments. As one of the most fundamental security services, pairwise 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 pairwisekey establishment techniques such as public key cryptography and key distribution center(KDC).

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

Eschenauer and Gligor proposed a probabilistic key predistribution scheme recently forpairwise key establishment [Eschenauer and Gligor 2002]. The main idea is to let eachsensor node randomly pick a set of keys from a key pool before the deployment so that anytwo 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 –compositekey predistribution scheme and a random pairwise keys scheme [Chan et al. 2003]. Theq -composite key predistribution also uses a key pool but requires two nodes compute apairwise key from at least q predistributed keys that they share. The random pairwise keysscheme 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 pairwise key establishment problem is still not fully solved. For the basicprobabilistic and the q -composite key predistribution schemes, as the number of compromised nodes increases, the fraction of affected pairwise keys increases quickly. As a result,a small number of compromised nodes may affect a large fraction of pairwise keys. Thoughthe random pairwise keys scheme does not suffer from the above security problem, given amemory constraint, the network size is strictly limited by the desired probability that twosensor nodes share a pairwise key, the memory available for keys on sensor nodes, and thenumber of neighbor nodes that a sensor node can communicate with.
In this paper, we develop a number of key predistribution techniques to deal with theabove problems. We first develop a general framework for pairwise key establishmentbased on the polynomial-based key predistribution protocol in [Blundo et al. 1993] andthe probabilistic key distribution in [Eschenauer and Gligor 2002; Chan et al. 2003]. Thisframework is called polynomial pool-based key predistribution, which uses a polynomialpool instead of a key pool in [Eschenauer and Gligor 2002; Chan et al. 2003]. The secretson each sensor node are generated from a subset of polynomials in the pool. If two sensornodes have the secrets generated from the same polynomial, they can establish a pairwisekey based on the polynomial-based key predistribution scheme. All the previous schemesin [Blundo et al. 1993; Eschenauer and Gligor 2002; Chan et al. 2003] can be consideredas special instances in this framework.

By instantiating the components in this framework, we further develop two novel 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 secretsgenerated 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 aunique 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 nodecan then identify whether it can directly establish a pairwise key with another node, and ifnot, what intermediate nodes it can contact to indirectly establish the pairwise key.Our analysis indicates that our new schemes have some nice features compared withthe previous methods. In particular, when the fraction of compromised secure links isless than 60%, given the same storage constraint, the random subset assignment schemeprovides a significantly higher probability of establishing secure communication betweennon-compromised nodes than the previous methods. Moreover, unless the number of com-promised nodes sharing a common polynomial exceeds a threshold, compromise of sensornodes does not lead to the disclosure of keys established between non-compromised nodesusing this polynomial.

Similarly, the hypercube-based scheme also has a number of attractive properties. First, it guarantees that any two nodes can establish a pairwise key when there are no compromised nodes, provided that the sensor nodes can communicate with each other. Second, itis resilient to node compromise. Even if some sensor nodes are compromised, there is stilla high probability to re-establish a pairwise key between non-compromised nodes. Third,a sensor node can directly determine whether it can establish a pairwise key with anothernode and how to compute the pairwise key if it can. As a result, there is no communicationoverhead during the discovery of directly shared keys.Evaluation of polynomials is essential to the proposed schemes, since it affects the performance of computing a pairwise key. To reduce the computation at sensor nodes, weprovide an optimization technique for polynomial evaluation. The basic idea is to computemultiple 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 finitefields is that no division is necessary for modular multiplication. As a result, evaluationof polynomials can be performed efficiently on low cost processors on sensor nodes thatdo not have division instructions. Our analysis indicates that such a method only slightlydecreases the uncertainty of the keys.

2. Related Work

The Eschenauer-Gligor scheme [11] and the Chan-Perrig-Songscheme [7] have been reviewed earlier in this section. Detailedcomparisons 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-Gligorscheme using a priori deployment knowledge [9]. This method canalso be used to further improve other random key pre-distributionschemes, such as the Chan-Perrig-Song scheme and the schemepresented in this paper.Blundo et al. proposed several schemes which allow any groupof t parties to compute a common key while being secure againstcollusion between some of them [5]. These schemes focus on saving communication costs while memory constraints are not placedon group members. When t = 2 , one of these schemes is actually a special case of Blom’s scheme [4]. A modified version ofBlom’s scheme will be reviewed in Section 2. Compared to Blom’sscheme, our scheme is more resilient and more memory-efficient.Perrig et al. proposed SPINS, a security architecture specificallydesigned for sensor networks [16]. In SPINS, each sensor nodeshares a secret key with the base station. Two sensor nodes can-not directly establish a secret key. However, they can use the basestation 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 proposea new key pre-distribution scheme that uses Blom’s method as abuilding block. Our idea is based on the following observations:Blom’s method guarantees that any pair of nodes can find a secretkey between themselves. To represent this we use concepts fromgraph theory and draw an edge between two nodes if and only ifthey can find a secret key between themselves. We will get a complete graph (i.e., an edge exists between all node pairs). Althoughfull connectivity is desirable, it is not necessary. To achieve ourgoal of key agreement, all we need is a connected graph, rather thana complete graph. Our hypothesis is that by requiring the graph tobe only connected, each sensor node needs to carry less key information.Before we describe our proposed scheme, we define a key space (orspace in short) as a tuple (D , G), where matrices D and G are asdefined 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 pairwise keyif they have picked a common key space.

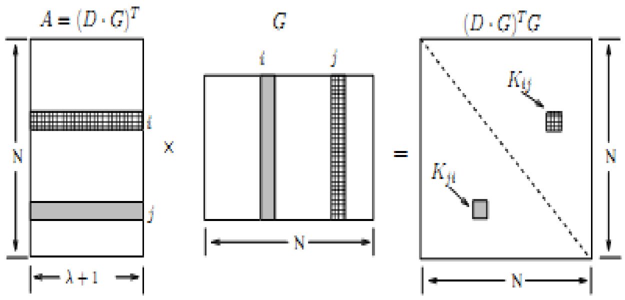

Figure 1: Generating Keys in Blom’s Scheme

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’ locationsHowever, 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 pairwise 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 pairwise 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 pairwise 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 pairwise key pre-distribution schemefor wireless sensor networks. Pairwise key distribution has a number of appealing properties. First, this scheme is scalable and flexible. Fora network that uses 64-bit secret keys, our scheme allows up to$N = 2^{64}$ sensor nodes. These nodes do not need to be deployedat the same time; they can be added later, and still be able to establish secret keys with existing nodes. Second, compared to existingkey pre-distribution schemes, our scheme is substantially more resilient against node capture. Our analysis and simulation resultshave shown, for example, that to compromise 10% of the securelinks in the network secured using our scheme, an adversary has tocompromise 5 times as many nodes as he/she has to compromisein a network secured by Chan-Perrig-Song scheme or Eschenauer-Gligor scheme. Furthermore, we have also shown that networkresilience can be further improved if we use multi-hop neighbors.

References

[1] Wireless Integrated Network Sensors, University ofCalifornia, Available: http://www.janet.ucla.edu/WINS.
[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, andE. Cayirci. A survey on sensor networks. IEEE
[3] Communications Magazine, 40(8):102–114, August 2002[3] R. Anderson and M. Kuhn. Tamper resistance - a cautionarynote. In Proceedings of the Second Usenix Workshop onElectronic Commerce, pages 1–11, November 1996.
[4] R. Blom. An optimal class of symmetric key generationsystems. Advances in Cryptology: Proceedings ofEUROCRYPT 84 (Thomas Beth, Norbert Cot, and IngemarIngemarsson, 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 dynamicconferences. Lecture Notes in Computer Science,740:471–486, 1993.
[6] D. W. Carman, P. S. Kruus, and B. J. Matt. Constraints andapproaches for distributed sensor network security. NAI LabsTechnical 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 keypredistribution schemes for sensor networks. In IEEESymposium on Security and Privacy, pages 197–213,Berkeley, California, May 11-14 2003.
[8] W. Diffie and M. E. Hellman.New directions incryptography. 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 usingdeployment knowledge. Technical Report, SyracuseUniversity, 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 schemefor distributed sensor networks.In Proceedings of the 9th ACM conference on Computer and communications security,November 2002.
[12] J. M. Kahn, R. H. Katz, and K. S. J. Pister. Next centurychallenges: Mobile networking for smart dust. InProceedings of the 5th Annual ACM/IEEE InternationConference on Mobile Computing and Networking(MobiCom), pages 483–492, 1999.
[13] F. J. MacWilliams and N. J. A. Sloane.The Theory ofError-Correcting Codes. New York, NY: Elsevier SciencePublishing Company, Inc., 1977.
[14] D. Malkhi, M. Reiter, A. Wool, and R. N. Wright.Probabilistic quorum systems. Information andComputation, (2):184–206, November 2001.
[15] B. C. Neuman and T. Tso. Kerberos: An authenticationservice 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. InProceedings of the 7th Annual ACM/IEEE InternationConference 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 forobtaining digital signatures and public-key cryptosystems.Communications of the ACM, 21(2):120–126, 1978.