Key Predistribution Schemes in Distributed Wireless Sensor Network

김정태
목원대학교
분산 무선 센서 네트워크에서의 선수 키 분배 방법
Jung-Tae Kim
Mokwon University
E-mail : jtkim5068@gmail.com

요 약

A Sensor Node in Wireless Sensor Network has very limited resources such as processing capability, memory capacity, battery power, and communication capability. When the communication between any two sensor nodes are required to be secured, the symmetric key cryptography technique is used for its advantage over public key cryptography in terms of requirement of less resources. Keys are pre-distributed to each sensor node from a set of keys called key pool before deployment of sensors nodes. Combinatorial design helps in a great way to determine the way keys are drawn from the key pool for distributing to individual sensor nodes. We study various deterministic key predistribution techniques that are based on combinatorial design.

Ⅰ. Introduction

When secured communication between two sensor nodes is required, then they can follow either symmetric key cryptography or asymmetric key cryptography. Asymmetric key cryptography requires huge computing resources that a tiny sensor can't afford. So a symmetric key cryptography is preferred. But key generation and distribution using Diffie-Hellman technique or public key infrastructure is also more or less infeasible in distributed sensor network consisting of resource limited sensor nodes. Due to the wireless nature of the communication and the potential commercial sensitivity of the data they measure, there is a requirement for cryptographic techniques to provide authentication, data integrity and/or confidentiality. The limited processing power and memory of the sensors means that in many circumstances the use of symmetric cryptographic primitives may be preferred to more computationally intensive public-key operations. This creates a requirement for the sensors to share keys. A sensor node can communicate with other node if the second one is lying within the circle of radio frequency range of the first one, and if both of them share a common key. The first work related to key predistribution can be traced back in 1985, by R. Blom. The research momentum in this field gained after the seminal work by Eschenauer & Gligor. Keys of a key-chain are selected from a key pool randomly and assigned to a sensor node. This method of key predistribution is probabilistic. Key predistribution schemes based on combinatorial designs are deterministic[1]. Key establishment in

sensor networks can also be realized with protocols where the nodes set up a shared secret key after deployment, either through key transport or key agreement [2]. A key transport protocol is a protocol where one entity creates or otherwise obtains a secret key and transfers it securely to the other entity (or entities). Key agreement refers to a mechanism or protocol where all participating entities contribute a random input which is used to derive a shared secret key. The advantage of key agreement over key transport is that no entity can predetermine the resulting key as it depends on the input of all participants.

II. The Energy Cost of Cryptographic Key Establishment

The overall energy cost of a key establishment protocol is not only determined by energy required for calculating cryptographic primitives, but also by the energy cost of radio communication between the involved parties. Raghunathan et al [3] analyzed the power consumption characteristics of modern sensor nodes and found out that, depending on the operating modes of the node's components, the wireless transmission of data can account for a major portion of the total energy consumption. Ideally we would like a KPS(Key Predistribution Scheme) to provide good connectivity with strong resilience, without requiring nodes to store too many keys. As these properties are in opposition to each other, the design of a KPS involves finding an appropriate trade-off between them. Certain trivial schemes may seem obvious candidates for KPSs in grid based networks. However, they have inherent limitations that affect their applicability:

- single key scheme
- immediate neighbours scheme
- locally-complete pairwise scheme

The inflexibility of these schemes makes it impossible to vary the trade-off between storage, connectivity and resilience to suit application requirements. A key predistribution scheme (KPS) is a means of specifying which nodes store which keys. Many such schemes have been proposed for use in WSNs for surveys of this field); they essentially involve a trade-off between the competing requirements of low memory usage, high network connectivity, and resilience against adversaries who capture nodes and extract the keys that they store.

III. Key Pre-distribution Process

A secure and efficient key pre-distribution scheme for WSNs aims to provide an appropriate plan to generate and store secret keys, and compute common keys for node-to-node secure communication. The key pre-distribution scheme is the foundation to gain authenticity and confidentiality of WSNs. In EUC Workshops 2005, S. J. Choi and H. Y. Youn proposed a key pre-distribution scheme for WSNs [4]. The scheme first describes the way to form the possible keys to a symmetric matrix K, and then decompose it into the product of a lower triangle matrix L and an upper triangle matrix U. The scheme uses the L matrix for secret information of the nodes in WSNs, and the U matrix for public information exchange and building common keys. S. J. Choi and H. Y. Youn's scheme can guarantee that any pair of nodes can find a common key between them.

The key pre-distribution process contains four steps [4]:

Step 1: General a large pool of keys which are possibly to be used during the communication between nodes.

Step 2: Form a symmetric matrix K by using the keys in the pool.
Step 3: Apply LU decomposition to the symmetric key matrix K, then we get L and U.
Step 4: Assign keys to nodes: every node is randomly assigned the data of one row of the L matrix and one column
of the U matrix, where the row and the column have the same position in the matrix. For example, the data
of i_{th} row of the L matrix (denoted as Lr i) and the ith column of the U matrix (denoted as Uc i) should be assigned to a same node.

Key predistribution is one widely-studied solution to the problem of key establishment in sensor networks: keys (or other keying material) are stored in the nodes' memories prior to deployment, so that nodes that share keys can then communicate securely once deployed (provided they are within communication range). A key predistribution scheme (KPS) is a means of specifying which nodes store which keys. Many such schemes have been proposed for use in WSNs for surveys of this field); they essentially involve a trade-off between the competing requirements of low memory usage, high network connectivity, and resilience against adversaries who capture nodes and extract the keys that they store. One possible approach to key predistribution for group-deployed networks is to employ a standard-model KPS; however, we would expect their performance to be exceeded by that of schemes designed to take group deployment into account. Nevertheless, such schemes can be used as components in the construction of group-based KPSs; One possible approach to key predistribution for group-deployed networks is to employ a standard-model KPS[6].

IV. Conclusion

In this paper, we survey that key predistribution schemes a grid-based network enables an efficient trade-off between the connectivity, resilience and storage requirements of a KPS, and we discuss the balancing of these properties to suit application requirements.

References

[1] Eschenauer L. and Gligor V. D. A Key-Management Scheme for Distributed Sensor Networks. In Proceedings of the 9th ACM Conference on Computer and Communications Security 2002. 41 47.
[2] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1996.
[3] V. Raghunathan, C. Schurgers, S. Park, and M. B. Srivastava. Energy-aware wireless microsensor networks. IEEE Signal Processing Magazine, 19(2):40 50, Mar. 2002.
[4] S. J. Choi and H. Y. Youn, An Effi cient Key Pre-distribution Scheme for Secure Distributed Sensor Networks, EUC Workshops 2005, LNCS 3823, pp. 1088-1097, 2005.
[5] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, M. Yung, Perfectly-secure key distribution for dynamic conferences., in: E. F. Brickell (ed.), Advances in Cryptology -CRYPTO '92, vol. 740 of LNCS, Springer-Verlag, 1992, pp. 471 486.
[6] N. T. Canh, Y.-K. Lee, S. Lee, HGKM: A group-based key management scheme for sensor networks using deployment knowledge, in: CNSR, IEEE Computer Society, Los Alamitos, CA, USA, 2008,
pp. 544 551.