行政院國家科學委員會專題研究計畫　期中進度報告

安全與可信賴之微型監測器系統網路設計與實作(1/3)

計畫類別：個別型計畫
計畫編號：NSC92-2213-E-009-122-
執行期間：92 年 08 月 01 日至 93 年 07 月 31 日
執行單位：國立交通大學資訊工程學系

計畫主持人：謝續平
共同主持人：楊明豪

報告類型：精簡報告
報告附件：出席國際會議研究心得報告及發表論文
國際合作計畫研究心得報告
處理方式：本計畫可公開查詢

中　華　民　國 93 年 6 月 1 日

行政院國家科學委員會專題研究計畫期中報告

安全與可信賴之微型監測器系統網路設計與實作

計畫編號：92-2213-E-009-122-
執行期間：92 年 08 月 01 日至　93 年 07 月 31 日
主持人：謝續平
執行單位：國立交通大學資訊工程學系

Abstract

Wireless Sensor Networks (WSNs) are formed by a set of small devices, called nodes, with limited computing power, storage space, and wireless communication capabilities. Most of these sensor nodes are deployed within a specific area to collect data or monitor a physical phenomenon. Data collected by each sensor node needs to be delivered and integrated to derive the whole picture of sensing phenomenon. To deliver data without being compromised, WSN services rely on secure communication and efficient key distribution.

In this project, we present some protocols for WSNs to improve the memory storage requirement. We also discuss the characteristics of node-to-node authentication and necessary resistance against node capture.

1. Introduction

Wireless Sensor Network (WSN) is a kind of network composed of nodes associated with sensors. Each node has the characteristics of small size, limited power, low computation and wireless access. The sensor node is responsible for collecting and delivering data over wireless network, and it is desirable to keep the delivered data confidential along the wireless transmission path from one node to another.

To ensure secure peer-to-peer wireless communication, the shared session key between any two nodes must be derived. Some protocols use a trusted third party to deliver keys to every node, while other protocols pre-distribute communication keys to all nodes. Since WSNs are self-organized and trusted third party may not be available, key pre-distribution protocols are often adopted in such networks. However, key pre-distribution protocols need to store session keys in every node. This may be difficult in a sensor network where thousands of nodes are deployed with limited storage space only enough to store a small number of session keys. It is desirable to design a new key pre-distribution protocol, which can reduce the storage space of session keys for a large WSN without degrading its security..

1.1. Wireless Sensor Network

With the increasing advances in hardware and wireless network technologies, the small wireless devices will be able to provide access to information anytime, anywhere. The WSN is a kind of application that is formed with a set of small untethered sensor devices that are

deployed in an ad hoc fashion and cooperate on sensing a physical phenomenon.

The differences between WSNs and other wireless networks, such as *Mobile Ad-hoc Networks* (*MANETs*) and cellular networks, are [1, 12, 24, 26]:

- The large scale of deployment: A WSN consists of hundreds even thousands of small wireless sensor nodes. Those sensor nodes are deployed in a large wide area for sensing a physical phenomenon.
- Low communication bandwidth: The bandwidth of WSNs is about 1 – 100kb/s. It is relative low to the traditional wireless networks.
- Limited memory space and computing power: Due to the small volume and low cost of each sensor node, the memory space and computing power are critically limited. The memory space ranges from several kilo bytes to hundreds kilo bytes. The computing power ranges from 4MHz to 100MHz.
- Critical of energy consumption: The small volume of sensor node causes the critical battery capacity. The energy consumption becomes the most critical issue of the design of sensor node. The energy consumption is often less than 1 μW.
- High node failure rate: The terrible deployed environment may make sensor nodes easy to be broken, and there may be some obstacles blocked the communication signal and made sensor nodes temporary unavailable.

There are lots of applications for sensor networks. In military applications, they can be used for command, control, and communication. In health applications, they can be deployed on patients to monitor and assist the disabled patients. In commercial applications, they can be used for managing inventory, and product quality monitoring. There are other applications such as disaster area monitoring, traffic monitoring…etc.

1.2. Constraints of Providing Key Distribution in WSNs

Much work has been done for wireless sensor network, such as network protocols, energy efficiency [16], real-time communication [13], deployment issues, and data dissemination [14, 15, 18]. The security services on wireless sensor network have become more and more important. As to provide security services on the WSN, key distribution has been regarded as the fundamental and critical issue.

The constraints of providing key distribution in WSNs are the ad hoc nature, and resource limitations of the WSN environment. The traditional key exchange and key distribution protocols are based on infrastructures and relying on trusted third parties. The ad hoc nature makes these protocols impractical for large scale of WSNs. The limitation of computing power and energy restricts the sensor node to use the public key-based key distribution scheme. According to the experimental result in [16], the total energy cost of processing the Diffie-Hellman key exchange protocol with Elliptic Curve point-multiplication enhanced is about ten to

hundreds times larger than the cost of processing key exchange protocol based on the AES secret-key algorithm. The energy efficiency problem makes the public key-based system hard to be implemented on the sensor network.

Besides the constraints of providing key distribution in WSNs, the high channel error rate, high latency, high node failure rate, and unreliable communications also increase the difficulty to provide the key distribution. Moreover, it is not easy to provide a tamper-resistant protection on each sensor node, but the sensor nodes are easy to be compromised. Therefore the keys stored in the compromised nodes will be extracted by the adversaries. Thus, the key distribution scheme must be robust with the node compromise.

2. Related Work

We firstly review related works of key distribution for traditional ad-hoc networks in Section 2.1. After that, we review the key distribution solutions proposed for wireless sensor networks in Section 2.2. Finally we present a more detailed review for the Random Key based schemes in Section 2.3.

2.1 Key Distribution Schemes for Ad-Hoc Networks

Zhou and Haas [30] proposed a solution to secure ad hoc networks by using an asymmetric cryptography and threshold scheme to distribute the services of certificate authority to a set of server nodes. The asymmetric cryptography is considered not suitable for the resource limited sensor networks.

Luo et al [19, 21] proposed a fully distributed certificate authority scheme for ad hoc networks. It distributes a RSA certificate signing key to all nodes in the network by using a threshold scheme. RSA is considered too expensive for sensor networks due to the limited computing power.

Hubaux et al [17] proposed a public key management solution for ad hoc network by using a PGP-like scheme in terms of the certificates are issued by the users themselves without the involvement of any certificate authority. In this scheme, each node has to maintain a large certificate cache and generates public/private key pairs. Those requirements are not suitable for the sensor networks.

Asokan and Ginzboorg [2] proposed a key agreement scheme for ad-hoc networks. They extend the generic two-party encrypted key exchange protocol to the multi-party case. The key exchange protocols they enhanced are based on the public cryptography, and are not suitable for sensor network due to the limited computing power.

Yi and Kravets [28, 29] proposed a key management scheme for heterogeneous wireless ad-hoc networks. It uses threshold cryptography to distribute the functions of certificate authority into specially selected nodes which are based on the security and physical characteristics of the nodes. Those selected nodes must have greater computing power and battery capacity. Otherwise they would be the bottlenecks of the network.

Basagni et al [4] proposed a distributed key management system named “Secure Pebblenets”, which provides group authentication, message

integrity and confidentiality. It is based on symmetric cryptography and uses the cluster architecture. This scheme needs tamper-resistant devices to protect the network nodes from captured and retrieved secret information inside. It is not suitable for the sensor networks environment due to the low cost property makes it difficult to provide tamper-resistant devices on each sensor node.

2.2 Key Distribution Schemes for WSNs

Carman et al [6] have analyzed variety of traditional approaches for the key establishment and key distribution in WSN. They have evaluated those schemes on different hardware platform, and they analyzed the overheads and energy consumption of each scheme. In [5] they proposed a key management for sensor networks which is based on group key agreement protocols and identity-based cryptography. It is based on the Diffie-Hellman operation to perform group key agreement. The Diffie-Hellman operation is not suitable for sensor networks due to the limited computing power.

Perrig et al. [22] proposed a security protocol for sensor networks named SPINS. It is based on a base station involved into the network as a trusted third party to set up the new keys between sensor nodes. Liu and Ning [20] extended the above scheme and proposed an efficient broadcast authentication method for sensor network. It uses multi-level key chains to distribute the key chain commitments for the broadcast authentication. Those schemes are not suitable for the sensor networks without base stations involved.

Undercoffer et al [27] proposed a security protocol for sensor networks. It is resource driven and factors in the trade off between levels of security and the requisite power and computational resources. It is not suitable for sensor networks without base stations involved.

Eschenauer and Gligor [10] proposed a key management scheme for sensor network, which is based on Random Graph Theory. Therefore Chan et al [8] extends Eschenauer and Gligor's scheme and proposed three new schemes. The memory space requirements for the above scheme are critical for the large network size. The detail of their schemes will be introduced in Section 2.3.

2.3 Random Key Based Schemes

The random key predistributed scheme was first proposed by L. Eschenauer and V. D. Gligor in [10]. We named their approach as the *basic scheme* in the remainder of this paper. Afterward, in [8], H. Chan, A. Perrig, and D. Song extended the basic scheme and proposed three mechanisms: *q-composite scheme*, *multipath key reinforcement scheme*, and *random-pairwise keys scheme*. We will introduce above schemes in this section.

2.3.1 Random Graph Theory

A random graph *G(n, p)* is a graph with n nodes, and the probability that a link exists between any two nodes in the graph is *p*. When *p* is zero, the graph *G* has no edges, whereas when *p* is one, the graph *G* is fully connected. In [9], Erdős and Rényi showed the monotone properties of a random graph *G(n, p)* that there exists a threshold value of *p*, over which value the property exhibits a "phase transition", i.e. the probability for *G* to have that property will transit from "likely false" to "likely true". The

threshold probability is defined by:

$$p = \frac{\ln(n) - \ln(-\ln(P_c))}{n} \qquad (1)$$

where P_c stands for desired probability of the property.

We present a simple example. The property we want to observe is the connectivity of this graph. We define the P_c as the probability to form a connected graph, i.e. while the P_c equals to one, there is no isolated node in this graph. Let us assume there are n = 10,000 nodes in the network, and the P_c = 0.99999, therefore the threshold probability p = 0.002.

Furthermore, we can calculate the expected degree of a node, where

$$d = p*(n-1) = \frac{(n-1)(\ln(n) - \ln(-\ln(P_c)))}{n} \qquad (2)$$

2.3.2 Basic Scheme

The basic scheme consists of three phases, named *key pre-distribution phase*, *shared-key discovery phase*, and *path-key establishment phase*.

In the key pre-distribution phase, each node randomly picks up r keys from a large key pool of S keys. In the shared-key discovery phase, every node tries to discover its neighbors that share the common keys with itself in wireless communication range. In addition, the network topology is progressively to form a connected graph. Finally in the path-key establishment phase, each node tries to establish a path-key with other nodes which are in the wireless communication range but do not share a common key.

2.3.3 *q*-composite Scheme

In this q-composite scheme, they try to enhance the security strength by using all common shared key between two nodes to establish the link key. They modified the basic scheme to let each pair of nodes in neighborhood at least share q common keys, and a new communication link key K is generated as the hash of all common shared keys, e.g., $K=hash(k_1||k_2||...||k_{q'})$, where q' is the number of actual keys shared by two nodes and $q' \geq q$. Therefore, the link key will be secured by q' keys instead of a single key.

2.3.4 Multipath Key Reinforcement Scheme

This scheme assume that initial key-setup has been completed (they can use the basic scheme to perform the initial key-setup), and there are now many secure links established through the common keys in the various nodes' key rings. Suppose A has a secure link to B after key-setup and this link is protected by a single common key k from the key pool S. They try to coordinate the key-update over multiple independent paths between A and B. Assume there is enough routing information supported, A knows all disjoint paths to B. Let j be the number of the disjoint paths. Then A generate j random number $v_1, v_2, ..., v_j$, and send each number through a disjoint path to B. When B has received all j numbers, the new link key k' can be calculated by both A and B where

$$k' = k \oplus v_1 \oplus v_2 \oplus \Lambda \oplus v_j$$

In this scheme, unless the adversary can eavesdrop on all j paths, otherwise they will not be able to compromise the new link key. In the other words, the security strength of a link is enhanced by the reinforcing neighbors.

2.3.5 Random-pairwise Keys Scheme

This scheme provides node-to-node authentication for wireless sensor network. The basic idea is that if each key in the key pool is just allow two sensor nodes to select it into their key rings, and these two nodes will know each other who has selected the same key with itself. Therefore they can authenticate each other by this unique pair-wised key.

3. Conclusion

In our project, we are now working on more progressive study about security issues in Wireless Sensor Network and identify the security challenges in WSN. Key distribution is the critical and fundamental issue for the security service in wireless sensor networks. The pre-distributed and symmetric cryptography based key management system would be well suitable for the resource limited sensor network. We want to propose efficient schemes based on the Random Graph theory to provide key distribution services for the secure sensor network services and improve the memory storage requirement by better performance in memory space under a given level of security strength. We also want to propose other scheme to possess the characteristics of node-to-node authentication and the great resistance against node capture. As well as it achieves better performance in maximum supported network size.

Reference

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," *IEEE Communications Magazine*, pages 102-114, August, 2002.

[2] N. Asokan and P. Ginzborg, "Key Agreement in Ad Hoc Networks," *Computer Communications Volume 23*, 2000.

[3] D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong, "Talking to Strangers: Authentication in Ad-Hoc Wireless Networks," *Internet Society, Conference Proceeding of NDSS Conference 2002*.

[4] S. Basagni, K. Herrin, E. Rosti, D. Bruschi, and E. Rosti, "Secure Pebblenets," *In Proceedings of the 2001 ACM International Symposium on Mobile ad hoc networking & computing*, pp. 156 - 163, 2001.

[5] D. W. Carman, B. J. Matt and G. H. Cirincione, "Energy-efficient and Low-latency Key Management for Sensor Networks," *In Proceedings of 23rd Army Science Conference*. Dec 2-5 2002 Orlando Florida.

[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*, September 2000.

[7] S. Capkun, L. Buttyán, and J-P Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," *IEEE Transactions on Mobile Computing, VOL. 2, NO. 1*, January-March 2003 Page(s): 52 -64.

[8] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," *IEEE Symposium on Security and Privacy*, May 2003.

[9] P. Erdős and A. Rényi, "On the Evolution

of Random Graphs," *Publ. Math. Inst. Hungat. Acad. Sci. 5* (1960) 17-61.

[10] L. Eschenauer and V. D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," *In Proceedings of the 9th ACM Conference on Computer and Communication Security*, pages 41-47, November 2002.

[11] N. Asokan and P. Ginzboorg, "Key Agreement in Ad Hoc Networks," *Computer Communications, Vol. 23*, pp. 1627-1637, 2000.

[12] D. Estrin, R. Govindan, J. Heidemann and S. Kumar, "Next Century Challenges: Scalable Coordination in Sensor Networks," *In Proceedings of the Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking*, August 1999

[13] T. He, J. A. Stankovic, C. Lu, and T. F. Abdelzaher, "SPEED: A Stateless Protocol for Real-Time Communication in Sensor Networks," *In International Conference on Distributed Computing Systems (ICDCS 2003)*, Providence, RI, May 2003.

[14] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-Efficient Communication Protocols for Wireless Microsensor Networks," *Proc. Hawaaian Int'l Conf. on Systems Science*, January 2000.

[15] W. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive Protocols for Information Dissemination in Wireless Sensor Networks," *In Proceedings of the fifth annual ACM/IEEE international conference on Mobile computing and networking*, August 1999.

[16] A. Hodjat and I. Verbauwhede, "The Energy Cost of Secrets in Ad-hoc Networks," *IEEE CAS Workshop on Wireless Communications and Networking*, September 2002.

[17] J-P. Hubaux, L.Buttyán, and S. Capkun, "The Quest for Security in Mobile Ad Hoc Networks," *In Proceedings of the 2001 ACM International Symposium on Mobile ad hoc networking & computing*, October 2001.

[18] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks," In *Proceedings of the Sixth Annual International Conference on Mobile Computing and Networks (MobiCOM '00)*, August 2000.

[19] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing Robust and Ubiquitous Security Support for Mobil Ad-Hoc Network," *Network Protocols Ninth International Conference on ICNP 2001*, 2001.

[20] D. Liu and P. Ning, "Efficient Distribution of Key Chain Commitments for Broadcast Authentication in Distributed Sensor Networks," *the 10th Annual Network and Distributed System Security Symposium,* San Diego, California. February 2003.

[21] H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang, "Self-securing Ad Hoc Wireless Networks," *In Proceedings of Seventh International Symposium on Computers and Communications (ISCC 2002)*, pp. 567 -574, 2002.

[22] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: Security

Protocols for Sensor Networks," *In Proceedings of the seventh annual international conference on Mobile computing and networking*, July 2001.

[23] P. Santi and D. M. Blough, "The Critical Transmitting Range for Connectivity in Sparse Wireless Ad Hoc Networks," *IEEE Transactions on Mobile Computing, VOL. 2, NO. 1*, January-March 2003. Page(s): 25 -39.

[24] S. Slijepcevic, M. Potkonjak,V. Tsiatsis, S. Zimbeck, M. B. Srivastava, "On communication Security in Wireless Ad-Hoc Sensor Network," *Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02)*, June 10 - 12, 2002 Pittsburgh, Pennsylvania, USA.

[25] J. Spencer. *The Strange Logic of Random Graphs*, Algorithms and Combinatorics 22, Springer-Verlag 2000, ISBN 3-540-41654-4.

[26] S. Tilak, N. Abu-Ghazaleh, and W. Heinzelman, "A Taxonomy of Wireless Microsensor Network Models," *ACM Mobile Computing and Communications Review (MC2R 2002)*, 2002.

[27] J. Undercoffer, S. Avancha, A. Joshi, and J. Pinkston, "Security for Sensor Networks," *2002 CADIP Research Symposium*.

[28] S. Yi and R. Kravets, "MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks," *2nd Annual PKI Research Workshop Program (PKI 03)*, Gaithersburg, Maryland, April, 2003.

[29] S. Yi and R. Kravets, "Key Management for Heterogeneous Ad Hoc Wireless Networks," *the 10th IEEE International Conference on Network Protocols (ICNP 2002)*.

L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," *IEEE Networks Magazine, Volume 13, Issue 6*, Pages 24-30, November/December 1999.