行政院國家科學委員會專題研究計畫　成果報告

適用於無線感測網路的密鑰管理技術之研究

計畫類別：個別型計畫
計畫編號：NSC94-2213-E-032-015-
執行期間：94 年 08 月 01 日至 95 年 07 月 31 日
執行單位：淡江大學資訊工程學系

計畫主持人：黃仁俊

計畫參與人員：蘇豐富、蔡宜君、蕭宇凱

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
處理方式：本計畫可公開查詢

中　華　民　國 95 年 10 月 24 日

行政院國家科學委員會補助專題研究計畫☑ 成 果 報 告 □期中進度報告

適用於無線感測網路的密鑰管理技術之研究

計畫類別：☑ 個別型計畫　　□ 整合型計畫

計畫編號：NSC 94-2213-E-032 -015 -

執行期間：　　94年　8　月　1　日至　　95年　　7月　　31日

計畫主持人：黃仁俊
共同主持人：
計畫參與人員： 蘇豐富、蔡宜君、蕭宇凱

成果報告類型(依經費核定清單規定繳交)：☑精簡報告　□完整報告

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
☑出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、列管計畫及下列情形者外，得立即公開查詢
□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位：淡江大學資訊工程系
中　華　民　國　　95 年　　10　月　　12　日

中文摘要

無線感測網路是軍事和民間相關應用的一項重要新技術。感測節點可能獨自並且部署在公開或者敵人的區域。它的通信可能受到監控並且感測節點也易受到敵對者取得和操縱。因此安全技術是發展與應用無線感測網路一項很重要的議題。發展無線感測網路的安全機制和技術，密鑰管理是一極為重要主題。無線感測網路 Ad Hoc 本質和其計算能力、儲存空間、頻寬和電力等資源限制使傳統密鑰管理技術在無線感測網路環境中無法切實可行。也由於無線感測網路的這些特殊本質，提高了密鑰管理設計的挑戰與難度。本專案計畫研發設計一適用於具大量感測節點的無線感測網路中感測節點間安全通信所需密鑰管理技術。本專案計畫研發設計的技術提供鑑別和祕密性功能且不需要密鑰配發中心的協助。我們的技術有良好的擴充性，因為每個感測節點都僅僅需持有數量不多的密鑰且其數量不受網路節點數量的影響。本專案計畫研發設計的技術的另一種重要性質是它提供兼具安全與高效率的資訊廣播功能；每一個感測節點都與它所有的直接相鄰感測節點共有一份密鑰，所以僅僅一次廣播資訊就能將資料安全地透過所有可能的管道傳遞出去。另外我們所研發設計的技術也提供許多重要性質例如抵抗節點複製攻擊、廣播效率、感測節點擴充性和感測撤消與新增等。比起過去的研究成果，本專案計畫研究成果是更有效率且安全。因此本專案計畫研究成果有符合並達到計畫的目標。我們將投稿本專案計畫研究成果到國際學術期刊。

Abstract

Wireless sensor networks (WSNs) is an important new technique for military and civilian applications. WSN nodes may be left unattended and the WSN may be formed in public or hostile areas. Its communication is monitored and sensor nodes are subject to capture and manipulation by an adversary. Security is a very important issue of WSN. To develop security mechanisms and protocols for sensor networks, key management is a paramount issue. The special nature of MSNs imposes challenging requirements on key management design. The traditional key management schemes are not feasible in WSN because of its ad hoc nature and the limited processing power, storage, bandwidth and energy resources. This project devises a distributed, deterministic key management protocol for securing communication between sensor nodes in large-scale sensor networks. The proposed protocol provides authentication and confidentiality functionality, without the need of a key distribution center. It is scalable since every node only needs to hold a small number of keys independent of the network size. Another important property of the proposed protocol is that it is optimized for message broadcast; each node shares one pairwise key with all of its immediate neighbors, so only one transition is necessary to broadcast a message. The proposed scheme provides many important properties such as resiliency against node replication, efficient broadcasting of encrypted messages, intermediate node accessibility of data, scalability, and revocation of compromised nodes and addition of new ones. The proposed scheme is more efficient and secure than the previous research results. Thus, this result achieves the subject of this project. We will submit this research result to an international journal.

一、前言與目的

Advances in micro-electro-mechanical systems (MEMS) and evolution in wireless communication, the application domains of wireless sensor network (WSN) are more and more

wide. They include military, environmental science, medical health, spatial research and other business applications [7]. WSN is constructed over the randomly distributed sensor nodes through self-organization protocol. The nodes utilize their sensor to sense peripheral signals then send these signals to data collector or base station through radio wave. The data collector or base station receive and process these data and do some applications. WSN nodes may be left unattended and the WSN may be formed in public or hostile areas. Its communication is monitored and sensor nodes are subject to capture and manipulation by an adversary. Security is a very important issue of WSN. To prevent attackers from subverting the wireless sensor network, wireless sensor network must include the following security functions: availability, authentication, confidentiality and integrity. There are many well-know security schemes or protocols have been proposed for wired network. However, these network security mechanisms are not feasible in WSN because of the limited processing power, storage, bandwidth and energy resources. Public-key cryptographic techniques, such as RSA are undesirable, since they are computationally expensive. Instead, symmetric cryptographic techniques and hashing functions are between two to four orders of magnitude faster [2]. They are the basic tools for securing sensor networks communications. To develop security mechanisms and protocols for sensor networks, key management is a paramount issue. The special nature of MSNs imposes challenging requirements on key management design. Most of cryptographic techniques are reliant on the use of secret key. Unless the secure key is used, a security system may be exposed to attack. The purposes of key management system are to: generate, distribute, authenticate, use, rekey, store, backup, valid period, revoke… and so on. However, it is difficult to devise a practical key management for the wireless sensor network because of its ad hoc nature, intermittent connectivity, and resource limitations. The key management of traditional wired network cannot be applied to the wireless sensor network directly. Since there is no prior knowledge of which nodes will be neighboring before deployment, a simple solution would be for every pair of sensor nodes in the network to share a unique key. However this solution is not feasible due to memory constraints. A more scalable solution is the use of a key common to all sensor nodes in the network [1]. The drawback with this approach is that if a single node is compromised then the security of the whole network is disrupted. Furthermore, renewing the common key is too expensive due to communication overhead. Besides scalability, there are also some other requirements that need to be considered while using a key sharing approach. A desirable feature is rebellion again node capture. An adversary should not be able to gain control of other parts of the network by using the revealed material, even if a node is compromised and its key material is revealed. Therefore the compromise of nodes should result in a breach of security that is constrained within a small, localized part of WSN. Another problem that must be handled well by key management schemes is the efficiency of message broadcasting. Since nodes communicate with their immediate neighbors in WSN applications, they should establish pairwise keys with their one-hop neighbors. If a node shares a different key (or set of keys) with each of its neighbors, then it is inefficient because it has to make multiple transmissions of messages, encrypted each time with a different key, in order to broadcast a

message to all of its neighbors. In these cases, we believe that transmissions must be kept as low as possible because of their high energy consumption rate. This project devises a security protocol that has the following properties: resilience to node replication, energy efficiency, scalability, easy deployment and node addition.

二、文獻探討

Basagni et al.'s key management scheme [1] uses a global common key shared by all nodes. In terms of storage requirements and energy efficiency, their solution is good. However, it is obvious that its disadvantage is the compromise of even a single node will reveal the universal key. There exist several schemes [3, 5, 6, 9] suggest random key pre-distribution: Before deployment each sensor node is preloaded with a set of symmetric keys that have been randomly chosen from a key pool. Then nodes can communicate with each other by using one or more of the keys they share according to the model of random key pre-distribution used. It is not scalable, although these schemes offer network resilience against node capture. The number of symmetric keys stored in sensor nodes must be increased in order to provide sufficient security of links when the size of the sensor network increases. However, in case of node capture, the more keys are stored in a node, the more links become compromised (even not neighboring ones). In LEAP [11], starting from a master key, each node creates a cluster key that distributes to its immediate neighbors using pair-wise keys that shares with each one of them. In this case, each node has to apply a different cryptographic key before forwarding the message because clusters highly overlap. This scheme has a more expensive bootstrapping phase and increased storage requirements, while it offers deterministic security and broadcast of encrypted messages. Dimitriou and Krontiris [4] discovered that even if the master key is deleted, the LEAP protocol can be attacked. More specifically an attacker may force a sensor node to compute pairwise keys with other nodes in WSN. Slijepcevic *et al.* [10] proposed dividing the network into hexagonal cells, each having a unique key shared between its members. Nodes belonging to the bordering region between neighboring cells store the keys of those cells, so that perform message exchange. All sensor nodes of their scheme can discover their exact location. It is an important assumption for Slijepcevic et al.'s scheme, because nodes can organize into cells and produce a location based key. Moreover, they assume that sensor nodes are tamper resistant. However, these assumptions are usually too demanding for sensor networks.

三、研究方法與成果

In this section, we introduce the research results of this project briefly. We divide our protocol into three phases: the initial phase, cluster key setup phase and Secure message forwarding phase.

Initialization phase:

Loading 4 keys: Node key K_i, Cluster Key K^c_i, Master Key K_m, Commitment key K_0 to each sensor Node i before distributing it.

Cluster key setup phase:

In this phase, all nodes will be either cluster heads or cluster members, depending on whether they sent a HELLO message or received one. Each Node i broadcastes a HELLO message "$E_{Km}(ID_i|K^c_i|H(K_m,ID_i|K^c_i)$" to its neighbors claiming its decision to become a cluster head at a random time according to a suitable probability distribution. The ID of this cluster $CID=ID_i$. When receiving a HELLO message, each Node j decrypts and authenticates it. If Node j does not declare its decision, it joins the cluster which Node i is the cluster head. Node j keeps K^c_i as the cluster key K^c. If Node j has already joined another cluster, or it has sent a HELLO message being a cluster head itself, it discards this message. All nodes in a cluster share a common key K^c. The whole sensor network is divided into clusters whose nodes share a common key.

After jointing one cluster, each node broadcasts the message "$E_{Km}(CID_i|K^c|H(K_m,CID|K^c)$" to its neighboring clusters. Nodes of the same cluster simply ignore the message. Any nodes in neighboring clusters store (CID_i, K^c_i) and use it to decrypt secret information coming from that cluster.

Secure message forwarding phase:

There are two cases for the secure message forwarding: one is a source node would like to send a message to the base station, the other one is a node would like to forward a received message to the base station. L records the cluster ID of the path from the source node to the base station step by step and is empty initially.

Case 1. a source node i (belong to CID_i cluster) would like to send a message M to the base station.

Step 1: If Node i is the cluster head, add ID_i to L.

Step 2: If it is necessary to provide confidentiality for M, perform the following substeps; otherwise T=M and go to Step 3.

Step 2.1: $K^0_e=F_{K_i}(0)$.

Step 2.2: $T=E_{K^0_e}(M)$.

Step 3: Generate a corresponding C for M.

Step 3.1: $K^0_H=F_{K_i}(1)$, τ= Time().

Step 3.2: $t_1 = H(K^0_H, T, \tau)$.

Step 3.4: $K'_M=F_{K^c_i}(1)$.

Step 3.5: $CID_s=CID_d=CID_i$.

Step 3.6: $t_2 = H(K'_M, CID_s, ID_i | T | t_1 | \tau)$.

Step 3.7: Broadcast $C=\{ID_i | CID_s | CID_d | T | t_1 | t_2 |\tau| L\}$

Step 5: If Node i is the cluster head, it generates and broadcasts another C to its each neighbor cluster CID_j (its cluster key is K^c_j) as the following substeps.

Step 5.1: $K'_M=F_{K^c_j}(1)$.

Step 5.2: $CID_s=CID_i$; $CID_d=CID_j$.

Step 5.3: $t_2 = H(K'_M, CID_s, ID_i | T | t_1 | \tau)$.

Step 5.4: Broadcast $C=\{ID_i | CID_s | CID_d | T | t_1 | t_2 | \tau | L\}$.

Case 2. Node i (belong to CID_i cluster with a cluster key K^c_i) would like to forward a received message C(={$ID_o|CID_s|CID_d|T|t_1|t_2|\tau|L$}) to the base station.

Step 1: If $CID_d \neq CID_i$ terminate this protocol.

Step 2: Verify "$ID_o|T|t_1|\tau$" by t_2, if it is false terminate this protocol.

Step 3: If Node i is not the cluster head go to Step 7.

Step 4: If L includes CID_i or (T, τ) has been forward terminate this protocol; otherwise, add CID_i to L.

Step 5: Perform the following substeps to generate and broadcast new C to cluster member.

Step 5.1: $K'_M = F_{K^c_i}(1)$.

Step 5.2: $CID_s = CID_d = CID_i$.

Step 5.3: $t_2 = H(K'_M, CID_s, ID_o|T|t_1|\tau)$.

Step 5.4: Broadcast C={$ID_o|CID_s|CID_d|T|t_1|t_2|\tau|L$}.

Step 5.5 Record (T, τ) has been forward.

Step 6: Generates and broadcasts new C to each neighbor cluster CID_j (whose cluster key is K^c_j) except the neighbor cluster CID_s as the following substeps.

Step 6.1: $K'_M = F_{K^c_j}(1)$.

Step 6.2: $CID_s = CID_i$; $CID_d = CID_j$.

Step 6.3: $t_2 = H(K'_M, CID_s, ID_o| T | t_1 | \tau)$.

Step 6.4: Broadcast C={$ID_o | CID_s | CID_d | T | t_1 | t_2 | \tau | L$}.

Step 6.5: Terminate this protocol.

Step 7:If $CID_s \neq CID_i$ go to Step 10.

Step 8:If $CID_s \neq ID_o$ terminate this protocol.

Step 9:Perform the following substeps to generate and broadcast new C to its each neighbor cluster CID_j (whose cluster key is K^c_j)

Step 9.1: $K'_M = F_{K^c_j}(1)$.

Step 9.2: $CID_s = CID_i$; $CID_d = CID_j$.

Step 9.3: $t_2 = H(K'_M, CID_s, ID_o| T | t_1 | \tau)$.

Step 9.4: Broadcast C={$ID_o | CID_s | CID_d | T | t_1 | t_2 | \tau | L$}.

Step 9.5: Terminate this protocol.

Step 10:If L includes CID_i or (T, τ) has been forward terminate this protocol.

Step 11:Generate and broadcast new C to the cluster head as the following substeps.

Step 11.1: $K'_M = F_{K^c_i}(1)$.

Step 11.2: $CID_s = CID_d = CID_i$.

Step 11.3: $t_2 = H(K'_M, CID_s, ID_o | T | t_1 | \tau)$.

Step 11.4 Broadcsat C={$ID_o | CID_s | CID_d | T | t_1 | t_2 |\tau| L$}.

Step 11.5 Record (T, τ) has been forward.

四、結論與成果自評

This project devises a key establishment protocol for sensor network deployment. The

number of secret information kept for each sensor nodes is independent of the number of sensor nodes of the network. It is scalable. The proposed protocol resists a large number of security attacks. It also guarantees that data securely reaches the base station in an energy efficient manner. No time synchronization or location knowledge is needed for the proposed protocol. It provides many important properties such as resiliency against node replication, efficient broadcasting of encrypted messages, intermediate node accessibility of data, scalability, and revocation of compromised nodes and addition of new ones. The proposed scheme is more efficient and secure than the previous research results. It achieves the objects of this project. The results will submit to the international journal for possible publication.

參考文獻

[1] S. Basagni, K. Herrin, D. Bruschi, and E. Rosti, "Secure pebblenet," *Proceedings of the 2001 ACM Iternational Symposium on Mobile Ad Hoc Networking & Computing, MobiHoc 2001*, pp. 156–163, October2001.

[2] D. Carman, P. Kruus, and B.J.Matt, "Constraints and approaches for distributed sensor network security," *Tech. Rep. 00-010*, NAI Labs, June, 2000.

[3] H.Chan, A.Perrig, and D.Song, "Random key predistribution schemes for sensor networks," *proceedings of IEEE Symposium on Security and Privacy*, pp. 197–213, May 2003.

[4] T. Dimitriou and I. Krontiris, "A Localized, Distributed Protocol for Secure Information Exchange in Sensor Networks," *Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium* (IPDPS'05), 2005

[5] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key predistribution scheme for wireless sensor networks," in *Proceedings of the 10th ACM conference on Computer and communication security*, pp. 42–51, October 2003.

[6] 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*, pp. 41–47, 2002.

[7] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in *Proceedings of the 10th ACM conference on Computer and communication security*, pp. 52–61, October 2003.

[8] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva,"Directed diffusion for wireless sensor networking," *ACM/IEEE Transactions on Networking*, vol. 11, February 2002.

[9] K. Romer and F. "Mattern: The design space of wireless sensor networks," *IEEE Wireless Communications*, Vol. 11, Issue 6.pp. 54–61, 2004.

[10] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, and M. Srivastava, "On communication security in wireless ad-hoc sensor networks," in *11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, pp. 139–144, June 2002.

[11] S. Zhu, S. Setia, and S. Jajodia, “LEAP: effi cient security mechanisms for large-scale distributed sensor networks,” in *Proceedings of the 10th ACM conference on Computer and communication security*, pp. 62–72, October 2003.