52. IWK

Internationales Wissenschaftliches Kolloquium
International Scientific Colloquium

PROCCEDINGS | **10 - 13 September 2007**

FACULTY OF COMPUTER SCIENCE AND AUTOMATION

COMPUTER SCIENCE MEETS AUTOMATION

VOLUME I

TECHNISCHE UNIVERSITÄT
ILMENAU

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der deutschen Nationalbiografie; detaillierte bibliografische Daten sind im Internet über **http://dnb.ddb.de** abrufbar.

ISBN 978-3-939473-17-6

Impressum

Herausgeber:	Der Rektor der Technischen Universität Ilmenau Univ.-Prof. Dr. rer. nat. habil. Peter Scharff
Redaktion:	Referat Marketing und Studentische Angelegenheiten Kongressorganisation Andrea Schneider Tel.: +49 3677 69-2520 Fax: +49 3677 69-1743 e-mail: kongressorganisation@tu-ilmenau.de
Redaktionsschluss:	Juli 2007
Verlag:	 Technische Universität Ilmenau/Universitätsbibliothek Universitätsverlag Ilmenau Postfach 10 05 65 98684 Ilmenau www.tu-ilmenau.de/universitaetsverlag
Herstellung und Auslieferung:	Verlagshaus Monsenstein und Vannerdat OHG Am Hawerkamp 31 48155 Münster www.mv-verlag.de
Layout Cover:	www.cey-x.de
Bezugsmöglichkeiten:	Universitätsbibliothek der TU Ilmenau Tel.: +49 3677 69-4615 Fax: +49 3677 69-4602

Preface

Dear Participants,

Confronted with the ever-increasing complexity of technical processes and the growing demands on their efficiency, security and flexibility, the scientific world needs to establish new methods of engineering design and new methods of systems operation. The factors likely to affect the design of the smart systems of the future will doubtless include the following:

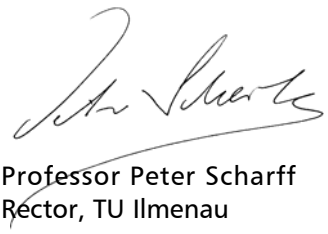
- As computational costs decrease, it will be possible to apply more complex algorithms, even in real time. These algorithms will take into account system nonlinearities or provide online optimisation of the system's performance.
- New fields of application will be addressed. Interest is now being expressed, beyond that in "classical" technical systems and processes, in environmental systems or medical and bioengineering applications.
- The boundaries between software and hardware design are being eroded. New design methods will include co-design of software and hardware and even of sensor and actuator components.
- Automation will not only replace human operators but will assist, support and supervise humans so that their work is safe and even more effective.
- Networked systems or swarms will be crucial, requiring improvement of the communication within them and study of how their behaviour can be made globally consistent.
- The issues of security and safety, not only during the operation of systems but also in the course of their design, will continue to increase in importance.

The title "Computer Science meets Automation", borne by the 52nd International Scientific Colloquium (IWK) at the Technische Universität Ilmenau, Germany, expresses the desire of scientists and engineers to rise to these challenges, cooperating closely on innovative methods in the two disciplines of computer science and automation.

The IWK has a long tradition going back as far as 1953. In the years before 1989, a major function of the colloquium was to bring together scientists from both sides of the Iron Curtain. Naturally, bonds were also deepened between the countries from the East. Today, the objective of the colloquium is still to bring researchers together. They come from the eastern and western member states of the European Union, and, indeed, from all over the world. All who wish to share their ideas on the points where "Computer Science meets Automation" are addressed by this colloquium at the Technische Universität Ilmenau.

All the University's Faculties have joined forces to ensure that nothing is left out. Control engineering, information science, cybernetics, communication technology and systems engineering – for all of these and their applications (ranging from biological systems to heavy engineering), the issues are being covered.

Together with all the organizers I should like to thank you for your contributions to the conference, ensuring, as they do, a most interesting colloquium programme of an interdisciplinary nature.
I am looking forward to an inspiring colloquium. It promises to be a fine platform for you to present your research, to address new concepts and to meet colleagues in Ilmenau.



Professor Peter Scharff
Rector, TU Ilmenau

Professor Christoph Ament
Head of Organisation

Table of Contents

C O N T E N T S

Paper submitted after copy deadline

2 Advances in Control Theory and Control Engineering

52nd Internationales Wissenschaftliches Kolloquium
Technische Universität Ilmenau
10 – 13 September 2007

Yiping Zhong / Jianqing Ma

Ring Domain-Based Key Management in Wireless Sensor Network

ABSTRACT

Wireless sensor networks (WSNs) are Ad hoc networks that include sensor nodes with limited computation, memory, energy and communication capabilities. When WSNs are deployed in unprotected/hostile areas, Wireless sensor networks (WSNs) are known to be particularly vulnerable to all kind of attacks like eavesdropping communication, node capture attacks, etc. Hence WSNs require cryptographic protection of communications, sensor capture resistance, key distribution and key revocation. In this paper, we present a key management schemes based on location-aware and random key predistribution model. The schemes propose to generate the pairwise keys by union of diversity of random keys and spatial diversity, and therefore improve network resistance on compromised nodes. Comparing with these random key predistribution based models (e.g. q-composite schemes), our scheme can improve the performances both on secure link connection ratio and security for resistance on compromised node. Comparing with these location-aware key management schemes, the scheme has no assumption about preknowledge of deployment or aid of distributive key configuration servers, which the major location-based key management schemes usually need. The analysis indicate that this scheme have nice properties like high secure connection ratio, security, resource-saving, resilience of network, etc.

Key words: wireless sensor network; security; key management;

1. INTRODUCTION

In future, wireless sensor networks (WSN) are expected to have wide applications both in military and civil fields. These applications include battlefield surveillance, target detection and tracking by the military, microclimate control in buildings, nuclear, biological and chemical attack detection, home automation, environmental monitoring, etc. When WSNs are deployed in unattended/hostile environments such as building guard, battlefield, etc, the adversary may launch various attacks such as eavesdropping, falsifying legitimate nodes to disturb network's objective, etc. To prevent these attacks, communication should be encrypted and authenticated for the

sake of security. Secure communication is made possible through the use of keys which are themselves managed using the techniques of key management.

Unlike the traditional network, WSN have several factors (e.g. vagaries of wireless links; Ad hoc communication; vulnerability of nodes to physical capture; resource constraints such as limited memory, communication and computation capability, etc) which make the key management of WSN very different and difficult, especially on using public key schemes. Traditional techniques of key management like certification authority (CA) and key distribution center (KDC) cannot be applied in the WSN because of the following reasons: 1) single point of failure and incurring to denial of service (DOS) attack; 2) lowering service success ratio and prolonging service time because of the high bit error ratio in wireless ad hoc communication; 3) network congestion because of high communication overhead of node authentication. Symmetric key schemes have nice properties like simple and rapid encryption algorithms, short key bit, etc. Therefore, symmetric key schemes have been widely proposed to address the problem of key management in WSNs on account of the resource constraints associated with their features mentioned above[1][2].

Key management in WSNs require all nodes that need secure communication to share key for building secure links; support to securely distribute keys to additional nodes for secure communication with other nodes; support to renew older key, revoke compromised key effectively and efficiently, etc; Therefore, the main factors of key management scheme in WSNs include: 1) securely distributing keys to each sensor nodes; 2) securely discovering the shared key of sensor nodes and can prevent these attacks like eavesdrop, falsified nodes, etc ; 3) network resilience against node capture; 4) less influence on network performance, especially for connectivity, resource consumption and scalability 5)being convenient to renew or revoke the keys.

The sensor nodes of WSNs are collected, secure and trust each other before deployment, Therefore, the popular key management schemes using symmetric key in WSNs are random key predistribution schemes[4][5][6][7], in which a subset of a key pool are predistributed to each sensor node before deployment. These schemes keep a certain secure connectivity probability of any pairwise nodes because these nodes share at least one common key with probability. There are two main merits in these key predistribution schemes. 1) The major work of key management has been finished before deployment and the schemes only need run the key agreement after deployment, hence it can save communication overhead and energy consumption besides security risk for WSNs. 2) They trade off these network performances (e.g. resource consumption, network connectivity, network security, etc).

In this paper, we propose a novel location-based key management-RDBK by using random key predistribution. The RDBK scheme randomly distributes original key set to every sensor; then the sensor nodes generate derived key set by using their original keys and the broadcasted random number keys of base station after deployment; and last, RDBK builds the pairwise key of node to ensure secure link by hashing their common derived keys.

2. RDPK SCHEME

In this section, we will introduce details of RDBK scheme in three sequent phases: key predistribution before deployment, key distribution in initial phase of network deployment; building secure links before secure communication.

2.1 Key predistribution phase

In the phase of key predistribution, the base station store a key pool which composes of original keys K_o^i (i=1, 2, …, P), and generate random number keys-Rnd_j (j=1,2…M) by using random number Rnd_M and one-way hash function, where $Rnd_j=Hash(Rnd_{j+1})$. And then, The base station randomly predistributes each sensor node a key subset of key pool, which compose of different original keys K_o^i with number of R(R≤P), and a common one-way hash function H().

2.2 Initial phase of network deployment

In the initial phase of network deployment, the base station broadcast the sequent random number keys-Rnd_1, Rnd_2, ..., Rnd_k (K≤M) by increasing power level p (see formula 1). Thus, the sensor nodes in different ring domains receive different random number keys (See Fig1). Each sensor stores the first received r+1 random number keys (e.g. Rnd_j, Rn d_{j+1} ， … ， Rnd_{j+r}) and then verify them by $Rnd_j=H(Rnd_{j+1})$, $Rnd_{j+2}=H(Rnd_{j+1})$,…, $Rnd_{j+r}=H(Rnd_{j+r-1})$.

$$P_{out}= P_{max}/L * p \quad (1)$$

Where L is the number of power level which the base station can adjust to broadcast message. p=1,2,…,L;

P_{max} is the maximum power of base station can launch.

After verified these keys, sensor nodes derive the keys K_d^i , K_d^{i+1} …,K_d^{i+r-1} by using their original keys (e.g. K_o^i), verified random number keys (e.g. Rnd_j , Rnd_{j+1})and hash function H(). The derive key set can be generated by the formula like $K_d^i=H(Rnd_j, K_o^i)$, $K_d^{i+1}=H(Rnd_{j+1}, K_o^i)$, …, $K_d^{i+r-1}=H(Rnd_{j+r-1}, K_o^i)$ where the K_o^i is the original key and Rnd_j is the random number key (for example, see Figure 1). It can deduce that the number of derived keys is r·R where r is the number of stored random number keys and R is the number of stored original keys in each sensor node. It should point out that RDBK can increase the number of common derive keys and therefore improve the probability to build the pairwise keys comparing with q-composite scheme [3].

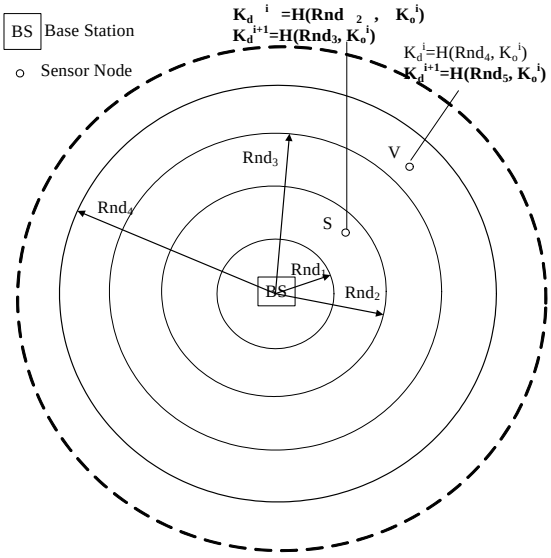


Fig1. Illustration of Derived Key Generation

2.3 Building secure links phase

In the phase of building secure links, the RDBK scheme is similar as q-composite scheme. When the number of common derived keys (denote as q') surpass the threshold number q, we build the pairwise key by function $H(K_d^{c1}, K_d^{c2}, \ldots, K_d^{cq'})$, where H is the one-way hash function and K_d^{ci} is one of common derived keys between a pair of nodes. According to the approach mentioned above, we can deduce that the threshold of common original keys decreases to number q/r for successfully building secure link in RDBK. Therefore, RDBK have better performance both on security and connectivity, comparing with q-composite scheme [3].

3. ANALYSIS

In this section, we will compare RPBK scheme with q-composite scheme and other location-based key management scheme. Before comparison, we define the secure connectivity ratio and compromise ratio like [8]:

Secure connectivity ratio: For a given node, it is defined as the ratio of the number of neighbors of the node with which it can form secure links (since it shares keys with those neighbors) to the total number of neighbors of the node. The Secure connectivity ratio for the network is then the average of the connectivity values for each of the nodes in the network.

Compromise ratio: The compromise ratio is defined as the ratio of the number of secure links formed by the non-compromised nodes that have become vulnerable to the total number of secure links formed by non-compromised nodes in the network. The secure links become vulnerable on account of the leakage of keying material on the compromised nodes.

We use Matlab to simulate a network of sensors. In the simulations reported here, we assume that the sensors nodes with number of 600 are deployed randomly over an area of size 800x800 units. The default values for the transmission radius of sensor node is 30 unites. The default threshold values of sharing key number is 3 (q=3). The default storing random key number of each node is 3 (r=3). Because the Hash function that derive the derived key is deleted after the initial phase of network

deployment, the adversary even capture all keys in pool, it still cannot construct the pairewise key. Therefore, we assume that the adversary have the ability to get the Hash function and therefore construct the pairewise key in experiment. Thus, when the ratio of compromised nodes is less than 30%, (the number of ring L= 10 or 20, the key number of pool P=1000 or 5000, the number of original key R=75, the number of shared derived key q=3, the compromise ratio is less than 0.01% and the secure connectivity ratio are larger than 99%. At the same condition, the compromise ratio of q-composite is about 45% and its secure connectivity is 92%. In a word, the main performance of RPBK scheme is better than q-composite. Comparing with other location-based schemes, RPBK scheme have no assumption that the sensor node location can be predicted before deployment and therefore can deploy WSN more conveniently and expand the application scenario of WSN.

4. CONCLUSION

In this paper, we propose a key management scheme named RPBK, which is suitable to static WSN. The RPBK scheme unites the diversity of node deployment location with the diversity of random predistribution keys. Thus, on the one hand, the RPBK scheme can expand the size of key pool and reduce the probability of shared key of sensor nodes in different ring area to improve the performance of compromise resistance. On the other hand, RPBK scheme can improve the number of shared pairwise key of neighbor nodes and therefore improve the security connection ratio of network. Comparing with other location-based schemes, RPBK need not deployment preknowledge and therefore improve the convenience of WSN deployment and application scenario. In a word, RPBK scheme have nice performance like network security, connectivity and scalability.

References:

[1] S. Basagni, K. Herrin, D. Bruschi, , and E. Rosti. Secure pebblenet. Proceedings of the 2001 ACM
[2] Laurent Eschenauer, Virgil D. Gligor, A Key-Management Scheme for Distributed Sensor, NetworksCCS'02, ACM, November 18–22, 2002
[3] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks,"Proceedings of 2003 Symposium on Security and Privacy. Los Alamitos, CA: IEEE Computer May 11–14 2003, pp. 197–215
[4]Laurent Eschenauer, Virgil D. Gligor, A Key-Management Scheme for Distributed Sensor, NetworksCCS'02, ACM, November 18–22, 2002
[5]H. Chan, A. Perrig, and D. Song, " Random key predistribution schemes for sensor networks, " Proceedings of 2003 Symposium on Security and Privacy. Los Alamitos, CA: IEEE Computer May 11 – 14 2003, pp. 197 – 215.
[6]Wenliang Du, Jing Deng, Yunghsiang S. Han, and Pramod K. Varshney. A pairwise key pre-distribution scheme for wireless sensor networks. In ACM CCS 2003, pages 42–51, October 2003.
[7]Wenliang Du,Jiang Deng.A key management scheme for wireless sensor networks using deployment knowledge[C].In:Proceedings of the IEEE INFOCOM'04,2004
[8]Farooq Anjum, Location dependent key management using random key-predistribution In Sensor Networks. WiSe'06 September 29, 2006

Authors:

Prof. Yiping Zhong
Ph.D Jianqing Ma
Department of Computing and Information Technology, Fudan University,
No.220 Handan Rd, 200433, Shanghai, P.R.China
Phone: 86-21-65643189
Fax: 86-21-65647894
E-mail: ypzhong@fudan.edu.cn; jqma_edu@yahoo.com.cn