

52. IWK

Internationales Wissenschaftliches Kolloquium
International Scientific Colloquium



PROCEEDINGS

10 - 13 September 2007

FACULTY OF COMPUTER SCIENCE AND AUTOMATION



COMPUTER SCIENCE MEETS AUTOMATION

VOLUME I

Session 1 - Systems Engineering and Intelligent Systems

Session 2 - Advances in Control Theory and Control Engineering

**Session 3 - Optimisation and Management of Complex
Systems and Networked Systems**

Session 4 - Intelligent Vehicles and Mobile Systems

Session 5 - Robotics and Motion Systems



Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der deutschen
Nationalbibliografie; 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

© Technische Universität Ilmenau (Thür.) 2007

Diese Publikationen und alle in ihr enthaltenen Beiträge und Abbildungen sind urheberrechtlich geschützt. Mit Ausnahme der gesetzlich zugelassenen Fälle ist eine Verwertung ohne Einwilligung der Redaktion strafbar.

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

CONTENTS

	Page
1 Systems Engineering and Intelligent Systems	
A. Yu. Nedelina, W. Fengler DIPLAN: Distributed Planner for Decision Support Systems	3
O. Sokolov, M. Wagenknecht, U. Gocht Multiagent Intelligent Diagnostics of Arising Faults	9
V. Nissen Management Applications of Fuzzy Control	15
O. G. Rudenko, A. A. Bessonov, P. Otto A Method for Information Coding in CMAC Networks	21
Ye. Bodyanskiy, P. Otto, I. Pliss, N. Teslenko Nonlinear process identification and modeling using general regression neuro-fuzzy network	27
Ye. Bodyanskiy, Ye. Gorshkov, V. Kolodyazhniy, P. Otto Evolving Network Based on Double Neo-Fuzzy Neurons	35
Ch. Wachten, Ch. Ament, C. Müller, H. Reinecke Modeling of a Laser Tracker System with Galvanometer Scanner	41
K. Lüttkopf, M. Abel, B. Eylert Statistics of the truck activity on German Motorways	47
K. Meissner, H. Hensel A 3D process information display to visualize complex process conditions in the process industry	53
F.-F. Steege, C. Martin, H.-M. Groß Recent Advances in the Estimation of Pointing Poses on Monocular Images for Human-Robot Interaction	59
A. González, H. Fernlund, J. Ekblad After Action Review by Comparison – an Approach to Automatically Evaluating Trainee Performance in Training Exercise	65
R. Suzuki, N. Fujiki, Y. Taru, N. Kobayashi, E. P. Hofer Internal Model Control for Assistive Devices in Rehabilitation Technology	71
D. Sommer, M. Golz Feature Reduction for Microsleep Detection	77

F. Müller, A. Wenzel, J. Wernstedt A new strategy for on-line Monitoring and Competence Assignment to Driver and Vehicle	83
V. Borikov Linear Parameter-Oriented Model of Microplasma Process in Electrolyte Solutions	89
A. Avshalumov, G. Filaretov Detection and Analysis of Impulse Point Sequences on Correlated Disturbance Phone	95
H. Salzwedel Complex Systems Design Automation in the Presence of Bounded and Statistical Uncertainties	101
G. J. Nalepa, I. Wojnicki Filling the Semantic Gaps in Systems Engineering	107
R. Knauf Compiling Experience into Knowledge	113
R. Knauf, S. Tsuruta, Y. Sakurai Toward Knowledge Engineering with Didactic Knowledge	119
2 Advances in Control Theory and Control Engineering	
U. Konigorski, A. López Output Coupling by Dynamic Output Feedback	129
H. Toossian Shandiz, A. Hajipoor Chaos in the Fractional Order Chua System and its Control	135
O. Katernoga, V. Popov, A. Potapovich, G. Davydau Methods for Stability Analysis of Nonlinear Control Systems with Time Delay for Application in Automatic Devices	141
J. Zimmermann, O. Sawodny Modelling and Control of a X-Y-Fine-Positioning Table	145
A. Winkler, J. Suchý Position Based Force Control of an Industrial Manipulator	151
E. Arnold, J. Neupert, O. Sawodny, K. Schneider Trajectory Tracking for Boom Cranes Based on Nonlinear Control and Optimal Trajectory Generation	157

K. Shaposhnikov, V. Astakhov The method of ortogonal projections in problems of the stationary magnetic field computation	165
J. Naumenko The computing of sinusoidal magnetic fields in presence of the surface with bounded conductivity	167
K. Bayramkulov, V. Astakhov The method of the boundary equations in problems of computing static and stationary fields on the topological graph	169
T. Kochubey, V. Astakhov The computation of magnetic field in the presence of ideal conductors using the Integral-differential equation of the first kind	171
M. Schneider, U. Lehmann, J. Krone, P. Langbein, Ch. Ament, P. Otto, U. Stark, J. Schrickel Artificial neural network for product-accompanied analysis and control	173
I. Jawish The Improvement of Traveling Responses of a Subway Train using Fuzzy Logic Techniques	179
Y. Gu, H. Su, J. Chu An Approach for Transforming Nonlinear System Modeled by the Feedforward Neural Networks to Discrete Uncertain Linear System	185
 3 Optimisation and Management of Complex Systems and Networked Systems	
R. Franke, J. Doppelhammer Advanced model based control in the Industrial IT System 800xA	193
H. Gerbracht, P. Li, W. Hong An efficient optimization approach to optimal control of large-scale processes	199
T. N. Pham, B. Wutke Modifying the Bellman's dynamic programming to the solution of the discrete multi-criteria optimization problem under fuzziness in long-term planning	205
S. Ritter, P. Bretschneider Optimale Planung und Betriebsführung der Energieversorgung im liberalisierten Energiemarkt	211
P. Bretschneider, D. Westermann Intelligente Energiesysteme: Chancen und Potentiale von IuK-Technologien	217

Z. Lu, Y. Zhong, Yu. Wu, J. Wu WSReMS: A Novel WSDM-based System Resource Management Scheme	223
M. Heit, E. Jennenchen, V. Kruglyak, D. Westermann Simulation des Strommarktes unter Verwendung von Petrinetzen	229
O. Sauer, M. Ebel Engineering of production monitoring & control systems	237
C. Behn, K. Zimmermann Biologically inspired Locomotion Systems and Adaptive Control	245
J. W. Vervoorst, T. Kopfstedt Mission Planning for UAV Swarms	251
M. Kaufmann, G. Bretthauer Development and composition of control logic networks for distributed mechatronic systems in a heterogeneous architecture	257
T. Kopfstedt, J. W. Vervoorst Formation Control for Groups of Mobile Robots Using a Hierarchical Controller Structure	263
M. Abel, Th. Lohfelder Simulation of the Communication Behaviour of the German Toll System	269
P. Hilgers, Ch. Ament Control in Digital Sensor-Actuator-Networks	275
C. Saul, A. Mitschele-Thiel, A. Diab, M. Abd rabou Kalil A Survey of MAC Protocols in Wireless Sensor Networks	281
T. Rossbach, M. Götze, A. Schreiber, M. Eifart, W. Kattanek Wireless Sensor Networks at their Limits – Design Considerations and Prototype Experiments	287
Y. Zhong, J. Ma Ring Domain-Based Key Management in Wireless Sensor Network	293
V. Nissen Automatic Forecast Model Selection in SAP Business Information Warehouse under Noise Conditions	299
M. Kühn, F. Richter, H. Salzwedel Process simulation for significant efficiency gains in clinical departments – practical example of a cancer clinic	305

D. Westermann, M. Kratz, St. Kümmerling, P. Meyer Architektur eines Simulators für Energie-, Informations- und Kommunikationstechnologien	311
P. Moreno, D. Westermann, P. Müller, F. Büchner Einsatzoptimierung von dezentralen netzgekoppelten Stromerzeugungsanlagen (DEA) in Verteilnetzen durch Erhöhung des Automatisierungsgrades	317
M. Heit, S. Rozhenko, M. Kryvenka, D. Westermann Mathematische Bewertung von Engpass-Situationen in Transportnetzen elektrischer Energie mittels lastflussbasierter Auktion	331
M. Lemmel, M. Schnatmeyer RFID-Technology in Warehouse Logistics	339
V. Krugljak, M. Heit, D. Westermann Approaches for modelling power market: A Comparison.	345
St. Kümmerling, N. Döring, A. Friedemann, M. Kratz, D. Westermann Demand-Side-Management in Privathaushalten – Der eBox-Ansatz	351
4 Intelligent Vehicles and Mobile Systems	
A. P. Aguiar, R. Ghabchelloo, A. Pascoal, C. Silvestre , F. Vanni Coordinated Path following of Multiple Marine Vehicles: Theoretical Issues and Practical Constraints	359
R. Engel, J. Kalwa Robust Relative Positioning of Multiple Underwater Vehicles	365
M. Jacobi, T. Pfützenreuter, T. Glotzbach, M. Schneider A 3D Simulation and Visualisation Environment for Unmanned Vehicles in Underwater Scenarios	371
M. Schneider, M. Eichhorn, T. Glotzbach, P. Otto A High-Level Simulator for heterogeneous marine vehicle teams under real constraints	377
A. Zangrilli, A. Picini Unmanned Marine Vehicles working in cooperation: market trends and technological requirements	383
T. Glotzbach, P. Otto, M. Schneider, M. Marinov A Concept for Team-Orientated Mission Planning and Formal Language Verification for Heterogeneous Unmanned Vehicles	389

M. A. Arredondo, A. Cormack SeeTrack: Situation Awareness Tool for Heterogeneous Vehicles	395
J. C. Ferreira, P. B. Maia, A. Lucia, A. I. Zapaniotis Virtual Prototyping of an Innovative Urban Vehicle	401
A. Wenzel, A. Gehr, T. Glotzbach, F. Müller Superfour-in: An all-terrain wheelchair with monitoring possibilities to enhance the life quality of people with walking disability	407
Th. Krause, P. Protzel Verteiltes, dynamisches Antriebssystem zur Steuerung eines Luftschiffes	413
T. Behrmann, M. Lemmel Vehicle with pure electric hybrid energy storage system	419
Ch. Schröter, M. Höchemer, H.-M. Groß A Particle Filter for the Dynamic Window Approach to Mobile Robot Control	425
M. Schenderlein, K. Debes, A. Koenig, H.-M. Groß Appearance-based Visual Localisation in Outdoor Environments with an Omnidirectional Camera	431
G. Al Zeer, A. Nabout, B. Tibken Hindernsvermeidung für Mobile Roboter mittels Ausweichecken	437
5 Robotics and Motion Systems	
Ch. Schröter, H.-M. Groß Efficient Gridmaps for SLAM with Rao-Blackwellized Particle Filters	445
St. Müller, A. Scheidig, A. Ober, H.-M. Groß Making Mobile Robots Smarter by Probabilistic User Modeling and Tracking	451
A. Swerdlow, T. Machmer, K. Kroschel, A. Laubenheimer, S. Richter Opto-acoustical Scene Analysis for a Humanoid Robot	457
A. Ahranovich, S. Karpovich, K. Zimmermann Multicoordinate Positioning System Design and Simulation	463
A. Balkovoy, V. Cacenkin, G. Slivinskaia Statical and dynamical accuracy of direct drive servo systems	469
Y. Litvinov, S. Karpovich, A. Ahranovich The 6-DOF Spatial Parallel Mechanism Control System Computer Simulation	477

V. Lysenko, W. Mintchenya, K. Zimmermann 483
Minimization of the number of actuators in legged robots using biological objects

J. Kroneis, T. Gastauer, S. Liu, B. Sauer 489
Flexible modeling and vibration analysis of a parallel robot with numerical and analytical methods for the purpose of active vibration damping

A. Amthor, T. Hausotte, G. Jäger, P. Li 495
Friction Modeling on Nanometerscale and Experimental Verification

Paper submitted after copy deadline

2 Advances in Control Theory and Control Engineering

V. Piwek, B. Kuhfuss, S. Allers 503
Feed drivers – Synchronized Motion is leading to a process optimization

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 ($i=1, 2, \dots, P$), and generate random number keys- Rnd_j ($j=1,2\dots M$) 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 $R(R\leq P)$, 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- $Rnd_1, Rnd_2, \dots, Rnd_k$ ($K\leq M$) 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. $Rnd_j, Rnd_{j+1}, \dots, Rnd_{j+r}$) and then verify them by $Rnd_j=H(Rnd_{j+1}), Rnd_{j+2}=H(Rnd_{j+1}), \dots, Rnd_{j+r}=H(Rnd_{j+r-1})$.

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

Where L is the number of power level which the base station can adjust to broadcast message.

$p=1,2,\dots,L$;

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

After verified these keys, sensor nodes derive the keys $K_d^i, K_d^{i+1}, \dots, K_d^{i+r-1}$ 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 $K_d^i=H(Rnd_j, K_o^i), K_d^{i+1}=H(Rnd_{j+1}, K_o^i), \dots, K_d^{i+r-1}=H(Rnd_{j+r-1}, K_o^i)$ 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 $r \cdot R$ 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].

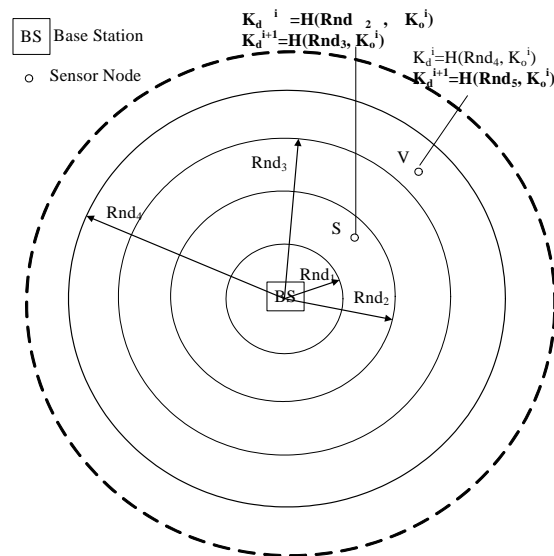


Fig1. Illustration of Derived Key Generation

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 $H(K_d^{c1}, K_d^{c2}, \dots, K_d^{cq'})$, 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 units. 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 pairwise key. Therefore, we assume that the adversary have the ability to get the Hash function and therefore construct the pairwise 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

