John A. Clark
Richard F. Paige
Fiona A.C. Polack
Phillip J. Brooke (Eds.)

LNCS 3934

Security in Pervasive Computing

Third International Conference, SPC 2006
York, UK, April 2006
Proceedings

Springer

John A. Clark Richard F. Paige
Fiona A.C. Polack Phillip J. Brooke (Eds.)

Security in Pervasive Computing

Third International Conference, SPC 2006
York, UK, April 18-21, 2006
Proceedings

Springer

Volume Editors

John A. Clark
Richard F. Paige
Fiona A.C. Polack
University of York
Department of Computer Science
Heslington, York, YO10 5DD, UK
E-mail: {jac,paige,fiona}@cs.york.ac.uk

Phillip J. Brooke
University of Teesside
School of Computing
Middlesbrough, TS1 3BA, UK
E-mail: p.j.brooke@tees.ac.uk

Library of Congress Control Number: 2006923045

CR Subject Classification (1998): C.2, D.2, D.4.6, H.5, K.4.1, K.4.4, K.6.5, H.4

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN	0302-9743
ISBN-10	3-540-33376-2 Springer Berlin Heidelberg New York
ISBN-13	978-3-540-33376-0 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11734666 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3934

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Preface

This volume contains the papers presented at the Third International Conference on Security in Pervasive Computing (SPC 2006), held April 19–21, 2006 in York, UK. The conference focused on methods, tools, principles, and practices for assessing and achieving security in a pervasive environment. New security concepts were discussed, in domains and applications such as handheld devices, mobile phones, smartcards, RFID chips, and smart labels, as well as new, emerging technological spaces. The conference also presented work on fundamental themes such as risk identification and mitigation, security policies for pervasive environments, privacy measures (especially cryptographic protocols), and mobility and location-aware services. Submissions included work on biometrics, ambient intelligence, Web services, security requirements, and many other topics.

We received 56 submissions, and accepted 16 full papers for presentation. Each submission was reviewed by the international Programme Committee. We are grateful to the Programme Committee members, and the additional reviewers, for their timely completion of the reviewing process, and for the quality and detail of their reviews and discussion.

Our thanks go to all members of the Programme Committee for their efforts; the additional reviewers; the authors, for submitting their papers; the keynote speaker, Frank Stajano; the invited speaker, Howard Chivers; and the Department of Computer Science, University of York, for supporting the event.

April 2006

John A. Clark (Program Chair)
Richard F. Paige
Fiona A.C. Polack
Phillip J. Brooke

Organization

SPC 2006 was organized by the Department of Computer Science, University of York.

Executive Committee

Program Chair	John A. Clark (Univ. of York, UK)
Organizing Co-chairs	Richard F. Paige and Fiona A.C. Polack (Univ. of York, UK)
Publicity Chair	Phillip J. Brooke (Univ. of Teesside, UK)

Programme Committee

Anos Anastassiadis	Cyveillance, USA
N. Asokan	Nokia, Finland
Phil Brooke	Univ. of Teesside, UK
Howard Chivers	Cranfield University, UK
Stephen J. Crane	HP, UK
Sadie Creese	QinetiQ, UK
Michael Goldsmith	Formal Systems Europe, UK
Stefanos Gritzalis	Univ. of the Aegean, Greece
Jochen Haller	SAP, Germany
Dieter Hutter	DFKI, Germany
Paul Karger	IBM, USA
Dennis Kuegler	BSI, Germany
Marc Langheinrich	ETH Zurich, Switzerland
Cetin Kaya Koc	Oregon State, USA
Cathy Meadows	NRL, USA
Takashi Moriyasu	National Information Security Center, Japan
Guenter Mueller	Univ. of Freiburg, Germany
Richard Paige	Univ. of York, UK
Panos Papadimitratos	Virginia Tech, USA
Fiona Polack	Univ. of York, UK
Yves Roudier	Eurecom, France
Peter Ryan	Univ. of Newcastle, UK
Andrei Serjantov	Free Haven Project, UK
Werner Stephan	DFKI, Germany
Markus Ullman	BSI, Germany
Irfan Zakuiddin	QinetiQ, UK

Additional Referees

F. Aivaloglou
J. Bryans
L. Gymnopoulos
C. Kalloniatis
G. Kambourakis
Y. Karabulut
F. Kerschbaum
R. Monroy
T. Peacock
P. Robinson
M. Volkamer

Lecture Notes in Computer Science

For information about Vols. 1–3835

please contact your bookseller or Springer

Vol. 3939: C. Priami, L. Cardelli, S. Emmott (Eds.), Transactions on Computational Systems Biology IV. VII, 141 pages. 2006. (Sublibrary LNBI).

Vol. 3934: J.A. Clark, R.F. Paige, F.A. C. Polack, P.J. Brooke (Eds.), Security in Pervasive Computing. X, 243 pages. 2006.

Vol. 3933: F. Bonchi, J.-F. Boulicaut (Eds.), Knowledge Discovery in Inductive Databases. VIII, 251 pages. 2006.

Vol. 3931: B. Apolloni, M. Marinaro, G. Nicosia, R. Tagliaferri (Eds.), Neural Nets. XIII, 370 pages. 2006.

Vol. 3928: J. Domingo-Ferrer, J. Posegga, D. Schreckling (Eds.), Smart Card Research and Advanced Applications. XI, 359 pages. 2006.

Vol. 3927: J. Hespanha, A. Tiwari (Eds.), Hybrid Systems: Computation and Control. XII, 584 pages. 2006.

Vol. 3925: A. Valmari (Ed.), Model Checking Software. X, 307 pages. 2006.

Vol. 3924: P. Sestoft (Ed.), Programming Languages and Systems. XII, 343 pages. 2006.

Vol. 3923: A. Mycroft, A. Zeller (Eds.), Compiler Construction. XIII, 277 pages. 2006.

Vol. 3922: L. Baresi, R. Heckel (Eds.), Fundamental Approaches to Software Engineering. XIII, 427 pages. 2006.

Vol. 3921: L. Aceto, A. Ingólfsdóttir (Eds.), Foundations of Software Science and Computation Structures. XV, 447 pages. 2006.

Vol. 3920: H. Hermanns, J. Palsberg (Eds.), Tools and Algorithms for the Construction and Analysis of Systems. XIV, 506 pages. 2006.

Vol. 3918: W.K. Ng, M. Kitsuregawa, J. Li, K. Chang (Eds.), Advances in Knowledge Discovery and Data Mining. XXIV, 879 pages. 2006. (Sublibrary LNAI).

Vol. 3917: H. Chen, F.Y. Wang, C.C. Yang, D. Zeng, M. Chau, K. Chang (Eds.), Intelligence and Security Informatics. XII, 186 pages. 2006.

Vol. 3916: J. Li, Q. Yang, A.-H. Tan (Eds.), Data Mining for Biomedical Applications. VIII, 155 pages. 2006. (Sublibrary LNBI).

Vol. 3915: R. Nayak, M.J. Zaki (Eds.), Knowledge Discovery from XML Documents. VIII, 105 pages. 2006.

Vol. 3910: S.A. Brueckner, G.D.M. Serugendo, D. Hales, F. Zambonelli (Eds.), Engineering Self-Organising Systems. XII, 245 pages. 2006. (Sublibrary LNAI).

Vol. 3909: A. Apostolico, C. Guerra, S. Istrail, P. Pevzner, M. Waterman (Eds.), Research in Computational Molecular Biology. XVII, 612 pages. 2006. (Sublibrary LNBI).

Vol. 3907: F. Rothlauf, J. Branke, S. Cagnoni, E. Costa, C. Cotta, R. Drechsler, E. Lutton, P. Machado, J.H. Moore, J. Romero, G.D. Smith, G. Squillero, H. Takagi (Eds.), Applications of Evolutionary Computing. XXIV, 813 pages. 2006.

Vol. 3906: J. Gottlieb, G.R. Raidl (Eds.), Evolutionary Computation in Combinatorial Optimization. XI, 293 pages. 2006.

Vol. 3905: P. Collet, M. Tomassini, M. Ebner, S. Gustafson, A. Ekárt (Eds.), Genetic Programming. XI, 361 pages. 2006.

Vol. 3904: M. Baldoni, U. Endriss, A. Omicini, P. Torroni (Eds.), Declarative Agent Languages and Technologies III. XII, 245 pages. 2006. (Sublibrary LNAI).

Vol. 3903: K. Chen, R. Deng, X. Lai, J. Zhou (Eds.), Information Security Practice and Experience. XIV, 392 pages. 2006.

Vol. 3901: P.M. Hill (Ed.), Logic Based Program Synthesis and Transformation. X, 179 pages. 2006.

Vol. 3899: S. Frintrop, VOCUS: A Visual Attention System for Object Detection and Goal-Directed Search. XIV, 216 pages. 2006. (Sublibrary LNAI).

Vol. 3897: B. Preneel, S. Tavares (Eds.), Selected Areas in Cryptography. XI, 371 pages. 2006.

Vol. 3896: Y. Ioannidis, M.H. Scholl, J.W. Schmidt, F. Matthes, M. Hatzopoulos, K. Boehm, A. Kemper, T. Grust, C. Boehm (Eds.), Advances in Database Technology - EDBT 2006. XIV, 1208 pages. 2006.

Vol. 3895: O. Goldreich, A.L. Rosenberg, A.L. Selman (Eds.), Theoretical Computer Science. XII, 399 pages. 2006.

Vol. 3894: W. Grass, B. Sick, K. Waldschmidt (Eds.), Architecture of Computing Systems - ARCS 2006. XII, 496 pages. 2006.

Vol. 3891: J.S. Sichman, L. Antunes (Eds.), Multi-Agent-Based Simulation VI. X, 191 pages. 2006. (Sublibrary LNAI).

Vol. 3890: S.G. Thompson, R. Ghanea-Hercock (Eds.), Defence Applications of Multi-Agent Systems. XII, 141 pages. 2006. (Sublibrary LNAI).

Vol. 3889: J. Rosca, D. Erdogmus, J.C. Príncipe, S. Haykin (Eds.), Independent Component Analysis and Blind Signal Separation. XXI, 980 pages. 2006.

Vol. 3888: D. Draheim, G. Weber (Eds.), Trends in Enterprise Application Architecture. IX, 145 pages. 2006.

Vol. 3887: J.R. Correa, A. Hevia, M. Kiwi (Eds.), LATIN 2006: Theoretical Informatics. XVI, 814 pages. 2006.

Vol. 3886: E.G. Bremer, J. Hakenberg, E.-H.(S.) Han, D. Berrar, W. Dubitzky (Eds.), Knowledge Discovery in Life Science Literature. XIV, 147 pages. 2006. (Sublibrary LNBI).

Vol. 3885: V. Torra, Y. Narukawa, A. Valls, J. Domingo-Ferrer (Eds.), Modeling Decisions for Artificial Intelligence. XII, 374 pages. 2006. (Sublibrary LNAI).

Vol. 3884: B. Durand, W. Thomas (Eds.), STACS 2006. XIV, 714 pages. 2006.

Vol. 3882: M.L. Lee, K.L. Tan, V. Wuwongse (Eds.), Database Systems for Advanced Applications. XXI, 923 pages. 2006.

Vol. 3881: S. Gibet, N. Courty, J.-F. Kamp (Eds.), Gesture in Human-Computer Interaction and Simulation. XIII, 344 pages. 2006. (Sublibrary LNAI).

Vol. 3880: A. Rashid, M. Aksit (Eds.), Transactions on Aspect-Oriented Software Development I. IX, 335 pages. 2006.

Vol. 3879: T. Erlebach, G. Persinao (Eds.), Approximation and Online Algorithms. X, 349 pages. 2006.

Vol. 3878: A. Gelbukh (Ed.), Computational Linguistics and Intelligent Text Processing. XVII, 589 pages. 2006.

Vol. 3877: M. Detyniecki, J.M. Jose, A. Nürnberger, C. J. '. van Rijsbergen (Eds.), Adaptive Multimedia Retrieval: User, Context, and Feedback. XI, 279 pages. 2006.

Vol. 3876: S. Halevi, T. Rabin (Eds.), Theory of Cryptography. XI, 617 pages. 2006.

Vol. 3875: S. Ur, E. Bin, Y. Wolfsthal (Eds.), Hardware and Software, Verification and Testing. X, 265 pages. 2006.

Vol. 3874: R. Missaoui, J. Schmidt (Eds.), Formal Concept Analysis. X, 309 pages. 2006. (Sublibrary LNAI).

Vol. 3873: L. Maicher, J. Park (Eds.), Charting the Topic Maps Research and Applications Landscape. VIII, 281 pages. 2006. (Sublibrary LNAI).

Vol. 3872: H. Bunke, A. L. Spitz (Eds.), Document Analysis Systems VII. XIII, 630 pages. 2006.

Vol. 3870: S. Spaccapietra, P. Atzeni, W.W. Chu, T. Catarci, K.P. Sycara (Eds.), Journal on Data Semantics V. XIII, 237 pages. 2006.

Vol. 3869: S. Renals, S. Bengio (Eds.), Machine Learning for Multimodal Interaction. XIII, 490 pages. 2006.

Vol. 3868: K. Römer, H. Karl, F. Mattern (Eds.), Wireless Sensor Networks. XI, 342 pages. 2006.

Vol. 3866: T. Dimitrakos, F. Martinelli, P.Y.A. Ryan, S. Schneider (Eds.), Formal Aspects in Security and Trust. X, 259 pages. 2006.

Vol. 3865: W. Shen, K.-M. Chao, Z. Lin, J.-P.A. Barthès, A. James (Eds.), Computer Supported Cooperative Work in Design II. XII, 659 pages. 2006.

Vol. 3863: M. Kohlhase (Ed.), Mathematical Knowledge Management. XI, 405 pages. 2006. (Sublibrary LNAI).

Vol. 3862: R.H. Bordini, M. Dastani, J. Dix, A.E.F. Seghrouchni (Eds.), Programming Multi-Agent Systems. XIV, 267 pages. 2006. (Sublibrary LNAI).

Vol. 3861: J. Dix, S.J. Hegner (Eds.), Foundations of Information and Knowledge Systems. X, 331 pages. 2006.

Vol. 3860: D. Pointcheval (Ed.), Topics in Cryptology – CT-RSA 2006. XI, 365 pages. 2006.

Vol. 3858: A. Valdes, D. Zamboni (Eds.), Recent Advances in Intrusion Detection. X, 351 pages. 2006.

Vol. 3857: M.P.C. Fossorier, H. Imai, S. Lin, A. Poli (Eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. XI, 350 pages. 2006.

Vol. 3855: E. A. Emerson, K.S. Namjoshi (Eds.), Verification, Model Checking, and Abstract Interpretation. XI, 443 pages. 2005.

Vol. 3854: I. Stavrakakis, M. Smirnov (Eds.), Autonomic Communication. XIII, 303 pages. 2006.

Vol. 3853: A.J. Ijspeert, T. Masuzawa, S. Kusumoto (Eds.), Biologically Inspired Approaches to Advanced Information Technology. XIV, 388 pages. 2006.

Vol. 3852: P.J. Narayanan, S.K. Nayar, H.-Y. Shum (Eds.), Computer Vision – ACCV 2006, Part II. XXXI, 977 pages. 2006.

Vol. 3851: P.J. Narayanan, S.K. Nayar, H.-Y. Shum (Eds.), Computer Vision – ACCV 2006, Part I. XXXI, 973 pages. 2006.

Vol. 3850: R. Freund, G. Păun, G. Rozenberg, A. Salomaa (Eds.), Membrane Computing. IX, 371 pages. 2006.

Vol. 3849: I. Bloch, A. Petrosino, A.G.B. Tettamanzi (Eds.), Fuzzy Logic and Applications. XIV, 438 pages. 2006. (Sublibrary LNAI).

Vol. 3848: J.-F. Boulicaut, L. De Raedt, H. Mannila (Eds.), Constraint-Based Mining and Inductive Databases. X, 401 pages. 2006. (Sublibrary LNAI).

Vol. 3847: K.P. Jantke, A. Lunzer, N. Spyratos, Y. Tanaka (Eds.), Federation over the Web. X, 215 pages. 2006. (Sublibrary LNAI).

Vol. 3846: H. J. van den Herik, Y. Björnsson, N.S. Netanyahu (Eds.), Computers and Games. XIV, 333 pages. 2006.

Vol. 3845: J. Farré, I. Litovsky, S. Schmitz (Eds.), Implementation and Application of Automata. XIII, 360 pages. 2006.

Vol. 3844: J.-M. Bruel (Ed.), Satellite Events at the MoDELS 2005 Conference. XIII, 360 pages. 2006.

Vol. 3843: P. Healy, N.S. Nikolov (Eds.), Graph Drawing. XVII, 536 pages. 2006.

Vol. 3842: H.T. Shen, J. Li, M. Li, J. Ni, W. Wang (Eds.), Advanced Web and Network Technologies, and Applications. XXVII, 1057 pages. 2006.

Vol. 3841: X. Zhou, J. Li, H.T. Shen, M. Kitsuregawa, Y. Zhang (Eds.), Frontiers of WWW Research and Development - APWeb 2006. XXIV, 1223 pages. 2006.

Vol. 3840: M. Li, B. Boehm, L.J. Osterweil (Eds.), Unifying the Software Process Spectrum. XVI, 522 pages. 2006.

Vol. 3839: J.-C. Filliâtre, C. Paulin-Mohring, B. Werner (Eds.), Types for Proofs and Programs. VIII, 275 pages. 2006.

Vol. 3838: A. Middeldorp, V. van Oostrom, F. van Raamsdonk, R. de Vrijer (Eds.), Processes, Terms and Cycles: Steps on the Road to Infinity. XVIII, 639 pages. 2005.

Vol. 3837: K. Cho, P. Jacquet (Eds.), Technologies for Advanced Heterogeneous Networks. IX, 307 pages. 2005.

Vol. 3836: J.-M. Pierson (Ed.), Data Management in Grids. X, 143 pages. 2006.

¥385.00元

Table of Contents

Invited Talk

Protocols

Mechanisms

Integrity

Privacy and Security

Information Flow and Access Control

Authentication

Trust Without Identification

Howard Chivers

Department of Information Systems, Cranfield University, DCMT Shrivenham,
Swindon SN6 8LA, UK
hrchivers@iee.org

Abstract. This extended abstract describes an alternative to trusting individual nodes in pervasive systems, which is to exploit the diversity of nodes in such systems to build application ensembles that are collectively trustworthy. These configurations are resilient to high levels of attack, and are not dependent on large pre-distribution key-spaces.

1 Background

Trust is a measure of belief in expected behaviour, in particular the likelihood of a particular outcome of a transaction; inevitably such estimates underpin security decision-making. Trust reputation systems estimate the likely behaviour of a node from the history of its interactions, which include recommendations obtained from other nodes. However, the nodes in such systems must be individually identifiable, otherwise they are vulnerable to an attacker who simply creates multiple electronic persona: the Sybil attack [1]. Such attacks can exploit start-up credits in reputation schemes, or fake many low-value recommendations to build an undeserved reputation.

Establishing a reliable identity in a pervasive system is problematic because nodes may have limited long-term storage and intermittent connectivity. Conventional public key systems require certificate validation and revocation, which may be difficult to achieve. An alternative is to extend key pre-distribution schemes to support identity [2]; a node can be identified by a number of keyspaces, which are probed as other network nodes establish connections.

The identity problem occurs because of the assumption that trust is a property of an individual node; however, in pervasive systems this may be questionable. Pervasive applications exploit the redundancy provided by a large number of nodes to achieve an adequate level of robustness, reliability, and performance. An important question is the extent that this approach can also be used to support security.

The real objective is to trust the outcome of an application, and there are many cases where appropriate outcomes can be achieved even if some of the contributions are in doubt; examples range from simple voting schemes to the sophisticated signal processing of sensor information. Of course, voting would be vulnerable to Sybil, but there are ways of improving the situation without resorting to individual identities.

2 Configuration Trust

A possible approach is to simply ensure that the nodes in an application are different; such an application may include malicious nodes, but up to a threshold they will be

J.A. Clark et al. (Eds.): SPC 2006, LNCS 3934, pp. 1 – 2, 2006.

unable to overwhelm the application and corrupt its results. This can be achieved by pre-distribution of authentication tokens or *diversity keys*; the application configuration is assembled using nodes that hold different keys.

These ideas can be extended further; in the process of configuring an application, nodes with identical diversity keys may be encountered. The nodes may be legitimate; alternatively, the particular key may be over-represented, indicating an attacker who is replicating nodes to improve their likelihood of use. The more aggressive the attack, the easier it can be rejected. In contrast, conventional trust recommendation schemes are unlikely to converge given a high proportion of malicious nodes.

Related security problems can also be addressed by managing trust at the level of the application configuration, rather than the individual. Location verification can be used to defend against Sybil attacks, but accurately locating individual nodes is an open research question [2]. In many applications, it may be sufficient to ensure that nodes are in a consistent location, rather than measure their actual position. For example, batch identifiers could be implanted in sensors nodes; nodes from the same batch are distributed in a similar way and are likely to be co-located.

These security concepts have been applied to the concrete example of a sensor network [3]. A significant result is that the security of an application is not strongly related to the size of the diversity keyspace. A diversity keyspace equal to the number of network nodes would amount to individual identities, so this result confirms that identity is not an essential precursor to trust in an application.

3 Conclusion

An alternative to trusting individual nodes in a pervasive system, is to focus on the need to trust the outcome of an application, by exploiting diversity. This viewpoint suggests alternative trust protocols that reject very high levels of attack, and are not dependent on large pre-distribution key-spaces. The fact that such protocols can be designed suggests that there is scope for further work in this field, and that it may not be necessary to be able to prove the identity of every node in a pervasive system.

References

1. Douceur, J. R. The Sybil Attack, *Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS02)*, Cambridge, MA (USA). (*Lecture Notes in Computer Science, vol. 2429/2002*). Springer-Verlag, 2002; 251-260.
2. Newsome, J., Shi, E., Song, D., and Perrig, A. The Sybil Attack in Sensor Networks: Analysis & Defenses, *Proceedings of the Third International Symposium on Information Processing in Sensor Networks (IPSN'04)*, Berkley California. ACM Press, 2004; 259-268.
3. Chivers, H. and Clark, J. A., Smart dust, friend or foe?—Replacing identity with configuration trust. *Computer Networks Special Issue: Military Communications Systems and Technologies*, 2004. **46**(5). 723-740.

Constant-Round Password-Based Group Key Generation for Multi-layer Ad-Hoc Networks*

Jin Wook Byun[1], Su-Mi Lee[1], Dong Hoon Lee[1], and Dowon Hong[2]

[1] Center for Information Security Technologies (CIST), Korea University, Anam Dong, Sungbuk Gu, Seoul, Korea
{byunstar, donghlee, smlee}@korea.ac.kr

[2] Electronics and Telecommunications Research Institute (ETRI), Gajeong-dong, Yuseong-gu, Daejeon, Korea
dwhong@etri.re.kr

Abstract. In this paper, we consider a multi-layer mobile ad-hoc network (MANET) composed of several kinds of networking units (such as ground soldiers, tanks, and unmanned aerial vehicles) with heterogeneous resources to communicate and compute. In this multi-layer MANET, we first propose a password-based authenticated group key exchange scheme with members' different passwords. The proposed scheme only requires constant-round to generate a group session key under the dynamic scenario, hence it is scalable, i.e., the overhead of key generation is independent of the size of a total group. We support the proposed scheme with formal security proof. Namely, our proposed scheme is the first constant-round password-based group key exchange with different passwords for the dynamic setting of MANET.

Keywords: Password authentication, key agreement, authenticated key exchange, heterogeneous, pervasive computing, multi-layer ad-hoc network.

1 Introduction

A mobile ad-hoc network (MANET) is a wireless network composed of mobile nodes that require little or no fixed infrastructure to communicate, and it has dynamic property itself because any mobile node may join and also leave the network at any given time. Thus, to protect communication between mobile nodes, it is desirable to use efficient and scalable cryptographic solutions with dynamic configuration. To communicate securely over an insecure wireless MANET it is essential that secret keys (encryption and decryption keys) are exchanged securely. A password-based authenticated group key exchange protocol allows mobile nodes holding passwords to agree on a common secret key over an insecure ad-hoc network in a secure and authenticated manner.

* This work was supported by grant No. R01-2004-000-10704-0 from the Basic Research Program of the Korea Science & Engineering Foundation.

J.A. Clark et al. (Eds.): SPC 2006, LNCS 3934, pp. 3–17, 2006.

1.1 Related Works

In this paper, we first consider the problem of a password-based group *Diffie-Hellman* key exchange in a dynamic scenario using *different* passwords. Most password-based authenticated key exchange schemes in the literature have focused on an authenticated key exchange using a *shared* password between clients or between a client and a server [1, 4, 5, 8, 20, 21, 24, 29, 15, 19]. However, the setting such that all clients have a same password is not practical since a password is not a common secret but a secret depending on an individual. For example, in mission-critical MANET such as emergency rescue and military operations, the setting in which group mobile nodes have different passwords is more suitable.

In recent years, a lot of password-based key exchange using different passwords have been presented. Byun *et al.* first proposed a secure *Client-to-Client Password-Authenticated Key Agreement* (C2C-PAKA) in the cross-realm setting where two clients were in two different realms and hence there existed two servers involved [10]. They have heuristically proved that the schemes were secure against all attacks considered. Unfortunately, the scheme was found to be flawed. Chen first pointed out that in the scheme with the cross-realm setting one malicious server can mount a dictionary attack to obtain the password of client who belongs to the other realm [13]. In [9], Wang *et al.* showed three dictionary attacks on the same protocol, and Kim *et al.* pointed out that the protocol was susceptible to Dening-Sacco attack in [23]. Kim *et al.* also proposed a improved C2C-PAKA protocol. However, very recently, Phan and Goi suggested two unknown key share attacks on the improved C2C-PAKA protocol in [25]. Several countermeasures to protect the attacks on C2C-PAKA protocol have been presented in [13, 9, 23, 25], but without any formal treatment. Very recently, Byun *et al.* efficiently and securely modified the original C2C-PAKA protocol with formal security model and proof, and presented EC2C-PAKA protocol [12].

In the group setting, Byun and Lee first suggested a password-based group key exchange protocols using group members' different passwords [9], but the schemes also had security holes such that a malicious insider can get information of other valid users' passwords [28]. Very recently, Byun *et al.* revised the schemes of [9], and presented password-based group key exchange schemes secure against insider guessing attacks [11]. However, these protocols do not consider dynamic scenario in which a group member is not known in advance but any member may join and also leave the group at any time, which is one of the most important properties in MANET.

1.2 Our Contributions

In this paper, we study a password-based group key exchange for the dynamic MANET. In particular, we focus on a heterogeneous multi-layer MANET with mobile backbone and unmanned aerial vehicles, which have been studied in [16, 17, 18, 26]. Consequently, we first design a constant-round password-based group key exchange protocol (namely, N-party EKE-D) using different passwords for a multi-layer MANET setting. As illustrated in Figure 1, the multi-layer

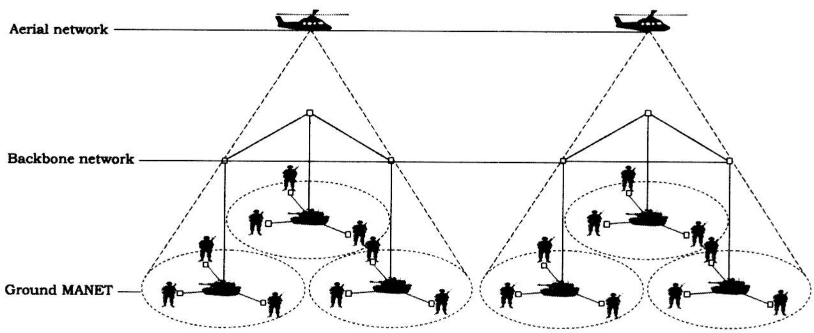

Fig. 1. The framework of Multi-layer Mobile Ad-hoc Network

MANET is composed of three kinds of networking units with heterogeneous communication capabilities and computation powers: the regular ground mobile nodes, the ground mobile backbone nodes, and the unmanned aerial vehicle nodes. Their capabilities and characteristics are summarized as follows [16, 17, 18, 26].

- Ground MANET (first layer) : This network includes regular ground mobile (GN) nodes and a ground mobile backbone (MBN) node. For instance, GN nodes can be soldiers equipped with limited communication and computation devices. They have the constrained transmission capabilities and use the short range channel access.
- Ground mobile backbone network (second layer) : This network includes MBN nodes which are special fighting units like trucks and tanks. These MBN nodes may carry a lot more equipment than individual soldiers.
- Unmanned aerial vehicles (third layer) : The unmanned aerial vehicles (UAV) maintain a station at an altitude of 10 to 20 thousands feets by flying in a circle. With the help of phased array antennas, it can provide the shared beam to the ground to keep line-of-sight connectivity for one area of operation down below.

The multi-layer MANET assumes that the second and third layers have well established infrastructures equipped with more communication and computation powers than the ones of the first layer. That is, highly cost cryptographic solutions can be used to protect communication between MBN nodes (tanks and trucks) and UAV nodes (such as airlines). Thus, we may employ wireless PKI-based group key exchange and tree-based group key exchange protocols [6, 22] as a security module for the second and third layer networks. However, in the first ground MANET, there are various physical attacks and bombs with dynamic changing network configuration, hence quick and secure cryptographic solutions should be applied to protect communication of GN nodes such as soldiers. Since our scheme only uses human memorable passwords to generate a group session key without any public key infrastructure (PKI) requiring tedious and expensive certificate management, it is well suitable for making a secure channel between soldiers in the first layer ground MANET. In addition, our proposed N-party EKE-D protocol requires only a constant number of rounds to establish a group session key. Accurately, one round is demanded by nodes, and two rounds are demanded by a central MBN node.[1] Furthermore only 2 modular exponentiations are required by each GN node. Our proposed N-party EKE-D protocol is the first constant-round and provably secure scheme in the dynamic scenario. We show that our proposed scheme is secure under the assumption that computational *Diffie-Hellman* problem is intractable.

2 Security Model and Definition

In this section we briefly review communication model and security definition for designing a secure password-based group key exchange protocol. Our model do not include the general security model for the multi-layer MANET, but just only security model for the ground MANET. Our communication model are based on the works of [1, 5].

2.1 Communication Model

Participants. We have two types of protocol participants, *GNs* and *MBNs*. Let $ID = GNs \cup MBNs$ be a non-empty set of protocol participants. We assume that *MBNs* consists of a single central node MBN, and $GNs = \{\mathsf{GN}_1, ..., \mathsf{GN}_n\}$ consists of identities of n GN nodes. Each node $\mathsf{GN}_i \in GNs$ has a secret password pw_i, and central MBN keeps password verifiers in its database. A node $\mathsf{GN}_i \in GNs$ may execute a key exchange protocol multiple times with different partners, and we denote the t-th instance of the protocol executed by entity GN_i (MBN) as oracle GN_i^t (MBN_i^t, respectively).

Algorithm. An N-party EKE-D protocol P requires the following four algorithms.

- **Password Generation Algorithm** $\mathsf{PGA}(1^k)$: Given an input of 1^k, where k is a security parameter, and then provides each node $\mathsf{GN}_i \in GNs$ with password pw_i.
- **Setup Algorithm** $\mathsf{Setup}(\mathcal{C})$: Takes input as a set of $\mathcal{C}$ and starts the protocol P. A new set $\mathcal{I}$ is created and set by $\mathcal{I} = \mathcal{C}$.
- **Join Algorithm** $\mathsf{Join}(\mathcal{I}, \mathcal{J})$: $\mathcal{J}$ is a set of newly joining group members. Takes inputs as sets $\mathcal{I}$ and $\mathcal{J}$, updates $\mathcal{I} = \mathcal{I} \cup \mathcal{J}$. Output is a new group session key shared between nodes of $\mathcal{I}$ including newly joining group members.

[1] We assume that ground MANET is the multicast network, hence any node can send messages to multiple recipients only in one round. One round includes all the messages that can be sent in parallel during the protocol.