

2010

Security in Ad Hoc Networks and Pervasive Computing


Isaac Z. Wu

X.-Y. Li

M. Song
Old Dominion University

C.-M. Liu

Follow this and additional works at: https://digitalcommons.odu.edu/ece_fac_pubs

 Part of the [Digital Communications and Networking Commons](#), and the [Information Security Commons](#)

Repository Citation

Wu, Isaac Z.; Li, X.-Y.; Song, M.; and Liu, C.-M., "Security in Ad Hoc Networks and Pervasive Computing" (2010). *Electrical & Computer Engineering Faculty Publications*. 152.
https://digitalcommons.odu.edu/ece_fac_pubs/152

Original Publication Citation

Wu, I. Z., Li, X. Y., Song, M., & Liu, C. M. (2010). Security in *ad hoc* networks and pervasive computing. *Security and Communication Networks*, 3(5), 359-361. doi:10.1002/sec.202

Guest Editorial

Security in *ad hoc* networks and pervasive computing

By Isaac Z. Wu, X.-Y. Li, M. Song and C.-M. Liu

Pervasive computing is an exciting and blooming research field, in which innovative techniques and applications are continuously emerging and aim to provide ambient and personalized services to users with high quality. *Ad hoc* networks are wireless, self-organizing systems formed by cooperating nodes within communication range of each other that form temporary networks. Their topology is dynamic, decentralized, ever changing and the nodes may move around arbitrarily. The last few years have witnessed a wealth of research ideas on *ad hoc* networking that are moving rapidly into implemented standards. Technology under development for *ad hoc* networks and pervasive computing is making important steps toward this end goal possible.

However, the security concerns remain a serious impediment to widespread adoption. The underlying radio communication medium for wireless network provides serious exposure to attacks against wireless networks. Wireless *ad hoc* networks usually cannot depend on traditional infrastructure found in enterprise environments such as dependable power sources, high bandwidth, continuous connectivity, common network services, well-known membership, static configuration, system administration, and physical security. Finally, throw in malicious adversaries with Byzantine collusion threats and you have a very interesting and challenging problem. Without adequate security, enterprises will not be able to profit from the use of wireless *ad hoc* networks and pervasive computing environment, defense organizations might be unable to guarantee the safety of their personnel in battlefield scenarios, and wireless *ad hoc* networks and pervasive computing will remain on the drawing board even if the other problems associated with

them are solved. This special issue is focused on various aspects of security in *ad hoc* networks and pervasive computing research and development to report both in-depth research and applications-oriented works.

The special issue is intended to foster state-of-the-art research in the area of security in *ad hoc* networks and pervasive computing.

The aim of this special issue is to present a collection of high quality research papers that report the latest research advances in security of *ad hoc*. In this special issue, we selected seven papers, which can demonstrate advanced works in this field. A detailed overview of the selected works is given below.

The first paper, *A Lightweight Secure Data Transmission Protocol for Resource Constrained Devices*, presents a simple, lightweight, but robust security protocol based on the backward property of RC4 stream cipher. The proposed protocol provides data confidentiality, data authentication, data integrity, and data freshness with low overhead and simple operation, allows packets be received in an arbitrary order, achieves semantic security, and does not require frequent key renew.

The second paper, *PAPA-UIC: A Design Approach and a Framework for Secure Mobile Ad-hoc Networks*, proposes a new design approach and a framework for securing a practical type of MANETs. The framework is named PAPA-UIC. The paper proposes a secure routing protocol and solutions to general problems of identity-based cryptography. The routing protocol has several improvements over existing ones.

The third paper, *RFIDGuard: A Lightweight Privacy and Authentication Protocol for Passive RFID Tags*, introduces a protocol which requires little computation and achieves both privacy and authentication

simultaneously. The lightweight and secure nature of the RFIDGuard protocol make it particularly suitable for supply chain management.

The fourth paper, *Using Hidden Markov Model to Detect Rogue Access Points*, proposes a statistical based approach to detect rogue access points using a Hidden Markov Model, which is applied to passively measure packet-header data collected at a gateway router. The main idea is to process the sequence of packet traces in order to distinguish the normal packets from the abnormal ones. The approach is scalable and non-intrusive, requiring little deployment cost and effort, and is easy to manage and maintain.

The fifth paper, *Defending Sybil Attacks Based on Neighboring Relations in Wireless Sensor Networks*, develops a mechanism to protect a WSN from Sybil attacks without using any authentication-based method. Furthermore, the detection approach requires no specialized hardware or support devices. The feature that a malicious node creates many fake identities is exploited to distinguish legitimate nodes from Sybil/malicious nodes. Since all of the fake identities forged by the same malicious node are associated with the same physical device, they will have the same legitimate neighbors. Therefore, by collecting the neighboring information of the suspected victim of the Sybil attacks, the legitimate nodes which are the neighbors of the malicious nodes can be determined. In contrast to existing protection schemes, this approach has no requirement for shared keys, secret information, or special hardware support.

The sixth paper, *An Autonomous Attestation Token to Secure Mobile Agents in Disaster Response*, introduces the Autonomous Attestation Token (AAT), a hardware token for mobile computing devices that is capable of guaranteeing the trusted state of a limited set of devices without relying on a networked service. The paper proposes a Local Attestation protocol with user interaction that in conjunction with the AAT prevents unauthorized access to an emergency mobile agent platform. In addition, the paper sketches a possible solution which integrates trusted computing to leverage *ad hoc* networks and peer-to-peer systems to provide a robust communication platform.

The seventh paper, *Building Advanced Applications with the Belgian eID*, introduces the Belgian Electronic Identity Card. The card enables Belgian citizens to digitally prove their identity and to sign electronic documents. This paper presents two reusable extensions to the Belgian eID technology that opens up new opportunities for application developers. First, a secure and ubiquitously accessible remote storage service is

presented. Second, it is shown how the eID card can be used to issue new certificates. The feasibility and reusability of both extensions are validated through the development of several applications in different domains.

In conclusion, this issue of Security in *Ad hoc* offers a groundbreaking view into the recent advances in secure *ad hoc* networks. This issue offers both academic and industry appeal the former as a basis toward future research directions, and the latter toward viable commercial applications.

Finally, we would like to express our gratitude to the Editor-in-Chief, Professor Hsiao-Hwa Chen for his advice, patience, and encouragements since the beginning until the final stage. Special thanks go to Michelle in Wiley during the production. We thank all anonymous reviewers who spent much of their precious time reviewing all the papers. Their timely reviews and comments greatly helped us select the best papers in this special issue. We also thank all authors who have submitted their papers for consideration for this issue.

We hope you will enjoy reading the great selection of papers in this issue.

Isaac Z. Wu

Information Department
Beijing Forest University, China
E-mail: iszzwu@gmail.com

X.-Y. Li

Computer Science Department
Illinois Institute of Technology, USA

M. Song

Electrical and Computer Engineering Department
Old Dominion University, USA

C.-M. Liu

Computer Science and Information Engineering
Department, National Taipei University of
Technology, Taiwan

Authors' Biographies



Dr. Isaac Z. Wu received his PhD degree in computer science from Beijing Inst. of Tech, China, in 2006. He is a lecturer of Department of Information Science and Technology at the Beijing Forestry University. His current research interests include embedded systems, computer network security, and algorithm design. He serves as reviewer for several conferences.



Prof. X-Y. Li received two BS degrees from Tsinghua University, China, in 1995 and the MS and PhD degrees in computer science from the University of Illinois at Urbana-Champaign in 2000 and 2001, respectively. He has been an associate professor since 2006 in the Department of Computer Science, Illinois Institute of Technology. He is

also a visiting professor of Microsoft Research Asia from May, 2007 to August 2008. His research interests span wireless ad hoc networks, game theory, computational geometry, and cryptography and network security. He has published approximately 80 conference papers in top-quality conferences such as ACM MobiCom, ACM MobiHoc, ACM SODA, ACM STOC, IEEE INFOCOM, etc. He has more than 50 journal papers published or accepted for publication. In 2008, he published a monograph "Wireless Ad Hoc and Sensor Networks: Theory and Applications". He is an editor of Ad Hoc & Sensor Wireless Networks: An International Journal, and Networks: An International Journal. He served in various positions (such as the conference chair, local arrangement chair, financial chair, session chair, or TPC member) at a number of international conferences such as AAIM, IEEE INFOCOM, ACM MobiHoc, ACM STOC, and ACM MobiCom. He is a senior member of the IEEE.



Dr. M. Song is an Associate Professor in the Department of Electrical and Computer Engineering at Old Dominion University. He received his PhD in Computer Science from the University of Toledo in 2001. His research interests include protocols design and performance analysis of mobile ad hoc networks and wireless sensor networks,

computer networks security, cognitive networking, wireless communications, and packet switch architectures. Dr. Song is the recipient of NSF CAREER award. He received early tenure and promotion in June of 2007. He is the founder and director of the Wireless Communications and Networking Laboratory. Dr. Song is an IEEE Senior member. He is the Editor-in-Chief of International Journal on Computer Networks and the Editor/Guest Editor of 10 international journals.



Prof. C-M. Liu received his PhD in Computer Sciences from Purdue University in 2002. He is an associate professor in the Department of Computer Science and Information Engineering, National Taipei University of Technology, TAIWAN. He is a member of Upsilon Pi Epsilon Honor Society in Computer Science since

1998. His research interests include parallel and distributed computation, data management and data dissemination in different wireless environments, ad hoc and sensor networks, and analysis and design of algorithms.