Addressing a Secure Session-Key Scheme for Mobility Supported e-Healthcare Systems

Pardeep Kumar[1], Pawani Porambage[1], Mika Ylianttila[1], Andrei Gurtov[2], Hoon-Jae Lee[3], and Mangal Sain[3]

[1] Centre for Wireless Communication, University of Oulu, Finland

[2] Aalto University, Finland

[3] Dongseo Univesity, Busan, South Korea

(Pt9)pradeepkhl@gmail.com, pporamba@ee.oulu.fi, mika.ylianttila@ee.oulu.fi, gurtov@hiit.fi, hjlee@dongseo.ac.kr, mangalsain1@gmail.com

(Pt9)Abstract—**Wireless medical sensor networks, also called e-Healthcare systems, provide mobility to the patients for making life easier and comfortable. However, a secure mobility support is highly desirable to a patient while he/she is moving. In this paper, we discuss security issues facing mobility supported e-Healthcare applications, and propose a secure session-key scheme for addressing security issues. The proposed scheme is suitable for the e-Healthcare systems where a patient is allowed to move and stay connected, securely. The proposed scheme not only establishes a session-key but according to HIPAA acts it also performs robust authenticity for the (mobile) medical sensor, the fixed access point, and the base-station. Our preliminary evaluation shows that the proposed scheme is feasible in-hospital, in-clinic, and homecare environments.**

(Pt9)Keyword—**Authentication, e-healthcare, medical sensor network, mobility, session-key, security.**

Pardeep Kumar received the Master of Technology in Computer Science and Engineering from Chaudhary Devilal University, Sirsa (Hr.), India in 2006, and Ph.D. in Computer Science from Dongseo University, South Korea in 2012. Since April 2012, he has been working with the Centre for Wireless Communications and Department of Communication Engineering, University of Oulu, Finland. His current research interests include secure wireless communication, security in sensor network, body area network, secure routing protocols, Internet of Things, and computer network.

Pawani Porambage is currently a PhD student in Department of Communications Engineering at University of Oulu, Finland. She obtained her Bachelor Degree in Electronics and Telecommunication Engineering in 2010 from University of Moratuwa, Sri Lanka and her Master's Degree in Ubiquitous Networking and Computer Networking in 2012 from University of Nice Sophia-Anipolis, France. Her main research interests include lightweight security protocols, security and privacy on Internet of Things, and Wireless Sensor Networks.

Mika Ylianttila received his Doctoral Degree on Communication Engineering at the University of Oulu in 2005. He has worked as a researcher and professor at the Department of Electrical and Information Engineering. He is the director of the Center for Internet Excellence (CIE) research and innovation unit. He is a pert-time professor at the Department of Communications Engineering in the field of broadband communications networks and systems, especially wireless Internet technologies. His research interests include Future Internet, mobile Networking and applications, Internet of Things, 3D Internet, M2M and P2P networking. He is a Senior Member of IEEE.

Andrei Gurtov received his M.Sc. (2000) and Ph.D. (2004) degrees in Computer Science from the University of Helsinki, Finland. He is presently a visiting scholar at the International Computer Science Institute (ICSI), Berkeley. He was a Professor at University of Oulu in the area of Wireless Internet in 2010-12. He is also a Principal Scientist leading the Networking Research group at the Helsinki Institute for Information Technology HIIT. Previously, he worked at TeliaSonera, Ericsson NomadicLab, and University of Helsinki. Dr. Gurtov is a co-author of over 130 publications including two books, research papers, patents, and IETF RFCs. He is a senior member of IEEE.

Hoon-Jae Lee received his BS, MS, and PhD degrees in Electronic Engineering from Kyungpook National University, Daegu, Korea, in 1985, 1987, and 1998, respectively. He is currently a professor in the Department of Information Communication Engineering at Dongseo University. From 1987 to 1998, he was a research associate at the Agency for Defense Development (ADD). His current research interests include developing secure communication system, side-channel attack, and ubiquitous sensor network/radio frequency identification security.

Mangal Sain is an assistant professor in Department of Information Engineering at Dongseo University, Busan Republic of Korea. He received his Ph.D. majoring in Ubiquitous Information technology from Dongseo University, Busan, Korea in 2011. He finishes his master in 2003 from India. During 2003-2007, he joined BSES Ltd and Altivolus InfoTech as a software engineer and Sr. Software Engineer respectively. His research interests are Wireless Sensor Networks, Ubiquitous Healthcare, Embedded Systems, Middleware, Cloud Computing and Cloud Middleware. He published more than 30 publications (Book Chapter, Journals, and Conference papers) in aforementioned areas. Over the years, he has served as a member of technical program committee, Editor, Reviewer, Guest Editor of more than 20 international conferences in the wireless communications area. He is a member of IEEE and TIIS. He was involved in research projects, BK21 in Ubiquitous Healthcare, Obstacle detection in smart car, Regional Innovation Project: Secure and Authentic RFID Reader/Writer etc. During 2007-2011, he was a Member of the 2nd Stage BK21 (Brain Korea 21) research team for Ubiquitous healthcare Technology Development using Wireless Sensor Network. His current research interests are in the fields of middleware, specially related with Cloud Computing.