Security Analysis of Secure Data Aggregation Protocols in Wireless Sensor Networks

Triana Mugia Rahayu, Sang-Gon Lee*, Hoon-Jae Lee

Departement of Ubiquitous IT
Division of Computer and Information Engineering
Dongseo University
Busan, Korea

gia.sutriadi@gmail.com, nok60@dongseo.ac.kr, hjlee@dongseo.ac.kr
*Corresponding author

***Abstract*— In order to conserve wireless sensor network (WSN) lifetime, data aggregation is applied. Some researchers consider the importance of security and propose secure data aggregation protocols. The essential of those secure approaches is to make sure that the aggregators aggregate the data in appropriate and secure way. In this paper we give the description of ESPDA (Energy-efficient and Secure Pattern-based Data Aggregation) and SRDA (Secure Reference-Based Data Aggregation) protocol that work on cluster-based WSN and the deep security analysis that are different from the previously presented one.**

***Keyword*— Data aggregation protocol, secure data aggregation protocol, ESPDA, SRDA, WSN.**

Triana Mugia Rahayu received her B. Eng. degree in Electrical Engineering from Petra Christian University, Indonesia, in 2011. She is now pursuing her master degree in Department of Ubiquitous IT, Division of Computer and Information Engineering, Dongseo University. Her current research area includes security for wireless sensor network.

Sang-Gon Lee received his B. Eng., M. Eng., and Ph.D degrees in Electronics Engineering from Kyungpook National University, Daegu, Rep. of Korea, in 1986, 1988 and 1993, respectively. He is a professor in Division of Computer & Information Engineering, Dongseo University. He was a visiting scholar at QUT, Australia, from August 2003 to July 2004 and at the University of Alabama at Huntsville, USA, from July 2012 to June 2013. His research areas include information security, network security, wireless mesh/sensor networks, and future Internet.

Hoon-Jae Lee received the B.S., M.S. and Ph.D. degree in Electrical Engineering from Kyungpook National University, Daegu, Rep. of Korea, in 1985, 1987 and 1998, respectively. He had been engaged in the research on cryptography and network security at Agency for Defense Development from 1987 to 1998. Since 2002 he has been working for Department of Computer Engineering of Dongseo University as an associate professor, and now he is a full professor. His current research interests are security communication system, side-channel attack, USN & RFID security. He is a member of the Korea Institute of Information Security and Cryptology, IEEE Computer Society, IEEE Information Theory Society and etc.