# An Efficient and Scalable Key Management Mechanism for Wireless Sensor Networks

Walid Abdallah*, Noureddine Boudriga*, Daehee Kim**, and Sunshin An**
(*)Communication Networks and Security research Lab, University of Carthage, Tunisia;
(**) Computer Network research Lab, Department of Electronics Engineering, Korea University, Seoul, Korea

***Abstract*—**A major issue to secure wireless sensor networks is key distribution. Current key distribution schemes are not fully adapted to the tiny, low-cost, and fragile sensors with limited computation capability, reduced memory size, and battery-based power supply. This paper investigates the design of an efficient key distribution and management scheme for wireless sensor networks. The proposed scheme can ensure the generation and distribution of different encryption keys intended to secure individual and group communications. This is performed based on elliptic curve public key encryption using Diffie-Hellman like key exchange and secret sharing techniques that are applied at different levels of the network topology. This scheme is more efficient and less complex than existing approaches, due to the reduced communication and processing overheads required to accomplish key exchange. Furthermore, little number of keys with reduced sizes are managed in sensor nodes which optimizes memory usage, and enhances scalability to large size networks.

***Index Terms*—**Wireless sensor networks, Security, Elliptic curve cryptography, Key management.

**Walid Abdallah**: is an Assistant Professor at the aviation school of Borj Elamri, Tunisia. He received his PhD in Information and communication technologies and the Diploma of engineer in telecommunications from the School of Communications engineering (Sup'Com), Tunisia. He received his Master Diploma from the National School of Engineer of Tunis (Tunisia). From 2001 to 2005 he worked for the National Digital Certification Agency (NDCA, Tunisia) and from 1997 to 2001 he worked for the national telecommunication operator (Tunisia Telecom). Currently, he is a member of the Communication Networks and Security Lab, where he is conducting research in optical networks and wireless sensor networks.

**Noureddine Boudriga** is an internationally known scientist/academic. He received his PhD in algebraic topology from University Paris XI (France) and his PhD in computer science from the University of Tunis (Tunisia). He is currently a full Professor of Telecommunications at the University of Carthage, Tunisia and the Director of the Communication Networks and Security Research Laboratory (CNAS). He has served as the General Director and founder of the Tunisian National Digital Certification Agency. He is the recipient of the Tunisian Presidential award in Science and Research (2004). He was involved in very active research and authored and co-authored many journal papers, book chapter, and books on networks and security.

**Daehee Kim** received the B.S. degree in Electronics Engineering from Yonsei University, Korea, in 2003 and M.S. degree in Electronic and Computer Engineering from Korea University, Korea, in 2006. Currently, he is working for Ph.D. degree on Electronic and Computer Engineering in Korea University, Korea. His research interests include the wireless sensor network, LTE, and security in wireless networks.

**SunshinAn** received the B.S. degree from Seoul National University, Korea in 1973, and the M.S. degree in Electrical Engineering from KAIST (Korea Advanced Institute of Science and Technology), Korea in 1975 and the Ph.D. degree in Electric and Information from ENSEEIHT, France in 1979. He joined the faculty of Korea University in 1982, where he is currently a Professor of Electronic and Computer Engineering. Prior to joining Korea University, Prof. An was Assistant Professor of Electronic Engineering in Ajou University, Suwon, Korea. He was with NIST (National Institute of Standards and Technology) in U.S.A., as a visiting scientist in 1991. His research interests include the distributed system, communication networks and protocols, information network, intelligent network, multimedia communication system, wireless sensor network and mobile RFID network