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 High School of Communications (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.