Abstract: Key Distribution through ECDH and subMAC for Secure ZigBee Pro

Kyung Choi[1], Mihui Kim[2], Kijoon Chae[1*]
[1]*Dept. of Computer Science and Engineering, Ewha Womans University, Seoul, Korea*
[2] *Dept. of Computer Engineering, Hankyong National University, Anseong, Korea*
*choibk@ewha.ac.kr, mhkim@hknu.ac.kr, kjchae@ewha.ac.kr**

Abstract

In this paper, we propose a secure key distribution mechanism using ECDH and subMAC for wireless sensors networks using ZigBee. ZigBee is a low-cost, low-power, wireless sensor network standard. ZigBee provides facilities for carrying out secure communications. ZigBee Pro enhances security and supports a large number of applications. Despite enhanced security, ZigBee Pro has vulnerabilities of key management, i.e., weakness of key distribution. We use ECDH for secure key distribution and subMAC to overcome the weakness of ECDH, i.e., no authentication and no prevention of man-in-the-middle-attack. Using subMAC, we provide the authentication for transmitted messages and prevent man-in-the-middle attack and replay attack. We apply our proposed key management mechanism to standard mode and high security mode in ZigBee Pro. Simulation results show our approach using ECDH and subMAC in ZigBee Pro is more efficient than existing ZigBee Pro in terms of reducing run time and energy consumption. We prove security is enhanced using BAN analysis.

Acknowledgement

The work was supported in part by the Ewha Global Top 5 Grand 2011 of Ewha Womans University, and Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology(2011-0014020).