LIGHTWEIGHT TRUSTED ID-BASED SIGNCRYPTION SCHEME FOR WIRELESS SENSOR NETWORKS

Zhimin Li, Xin Xu, Zexiang Fan
School of Computer Engineering
Huaihai Institute of Technology, Canwu Road 59
Lianyungang, China, 222005
Emails: {lizhimin1981, xinxu, zx.fan}@gmail.com

Submitted: Aug.3, 2012 ***Accepted: Sep.3, 2012*** ***Published: Dec.1, 2012***

Abstract - Wireless sensor networks (WSN) are usually deployed in hostile environments, which having a wide variety of malicious attacks. As various applications of WSN have been proposed, security has become one of the big research challenges dan is receiving increasing attention. In order to insure the security of communication in wireless sensor networks, we proposed a new ID-based signcryption scheme using bilinear pairing. Under the computational Diffie-Hellman assumption, the security of the scheme is proved under the Random Oracle Model. This scheme can be used by the sensor nodes that with low power, less storage space and low computation ability. It is concluded that the proposed lightweight scheme satisfies the security requirements of WSN.

Index terms*:* WSN, ID-based signcryption, provably secure, bilinear pairing.