International Journal of Innovative Computing, Information and Control
Volume **5**, Number **8**, August **2009**

ICIC International ©2009 ISSN 1349-4198
pp. **2107–2124**

AN EFFICIENT SENSOR-TO-SENSOR AUTHENTICATED PATH-KEY ESTABLISHMENT SCHEME FOR SECURE COMMUNICATIONS IN WIRELESS SENSOR NETWORKS

Chun-Ta Li[1,2], Min-Shiang Hwang[3] and Yen-Ping Chu[4]

[1]Department of Information Management
Tainan University of Technology
529 Jhong Jheng Road, Yongkang, Tainan, 710, Taiwan
th0040@mail.tut.edu.tw

[2]Department of Computer Science and Engineering
[3]Department of Management Information Systems
National Chung Hsing University
250 Kuo Kuang Road, Taichung, 402, Taiwan
mshwang@nchu.edu.tw

[4]Department of Computer Science and Information Engineering
Tunghai University
181 Section 3, Taichung Harbor Road, Taichung, 407, Taiwan
ypchu@nchu.edu.tw

Received February 2008; revised July 2008

Abstract. *Path-key establishment has become accepted as a commonly used solution in wireless sensor networks (WSNs) for protecting node-to-node communications from malicious attacks. Unfortunately, traditional security approaches are not well suited to WSNs due to their limited computational/communication abilities and memory, and their vulnerable-to-attack structure. Moreover, to extend lifetime and usability of sensor networks, power conservation and scalability are required in the design of sensor network schemes. In this paper, we propose an efficient sensor-to-sensor authenticated path-key establishment (ES2S-APKE) scheme for wireless sensor networks. ES2S-APKE accomplishes node authentication and pairwise key establishment by applying well-known Elliptic Curve Cryptography (ECC) and using cluster-based sensor groups. In clustered sensor networks, a back-end system creates a view of the credential authority (CA) and provides credential update service for all involved nodes in the network, including sink nodes and sensor nodes. A ticket scheme is introduced to provide efficient S2S path-key establishment service. Finally, the security and performance of our proposed ES2S-APKE is compared with Lee's* [19] *and Varadharajan's* [32] *schemes.*
Keywords: Ad hoc networks, Elliptic curve cryptography, Mutual authentication, Path key establishment, Security, Wireless sensor networks

1. **Introduction.** Wireless sensor networks are formed dynamically by a number of sensor nodes. In a wireless sensor network, when sensors deploy in a designated area, they must pass an identity authentication examination by their corresponding sink nodes in order to identify both trustworthy and unreliable nodes from a security standpoint. Through this identity authentication process, the controller node (also called sink node) can determine if the sensor information can be trusted and unauthorized nodes can be isolated from networks during the identity authentication procedure. After a sensor passes the identity authentication check of a sink node, the packets transmitted between a sensor and the sink node must be kept secret while a sensor sends its data. They must establish a session key to be used between them for securing their subsequent communications.