International Journal of Innovative Computing, Information and Control
Volume **5**, Number **10(A)**, October **2009**

ICIC International ©2009 ISSN 1349-4198
pp. **3085–3097**

AN EFFICIENT CONCEALED DATA AGGREGATION SCHEME FOR SENSOR NETWORKS BASED ON SECRET SHARING

Gwoboa Horng[1], Chien-Lung Wang[1] and Tzung-Her Chen[2]

[1]Department of Computer Science and Engineering
National Chung-Hsing University
250 Kuo-Kuang Road, Taichung 402, Taiwan
{ gbhorng; phd9004 }@cs.nchu.edu.tw

[2]Department of Computer Science and Information Engineering
National Chiayi University
300 University Rd., Chiayi City, 600, Taiwan
thchen@mail.ncyu.edu.tw

Received April 2008; revised September 2008

Abstract. *Soon after wireless sensor networks (WSNs) attracted attention in both industry and academia, to maintain the security of WSNs, especially in end-to-end encryption, has become a challenging research issue. A sensor device has limited computation capability, low battery power, and small memory size. To save the overall energy resources and maintain the security, we need to reduce the computation cost as well as the amount of encrypted data transmitting through the WSN. One plausible approach is to consolidate the encrypted data along the routing path. This is called concealed data aggregation (CDA). This paper proposes a novel end-to-end CDA scheme based on the concept of secret sharing. It has the following characteristics: 1) It provides efficient end-to-end encryption on the sensed data between the sensor node and the sink node so that the sensed data remains confidential during transmission. 2) It is secure up to some fixed number of compromised nodes. 3) The size of the aggregated ciphertext is constant throughout the network. 4) It extends to aggregate two or more pieces of data separately in one round of transmission. 5) It is good for key update and routing flexibility.*
Keywords: Concealed data aggregation (CDA), Wireless sensor network (WSN), End-to-end encryption, Secret sharing, Security

1. **Introduction.** As applications of wireless sensor networks (WSNs) growing in industry and academia, the demand of keeping the sensed data secret from malicious outsiders will increase. WSNs can quickly gain popularity due to their potentiality of becoming low cost solutions to a variety of real-world challenges [1]. They are widely used in environment monitors (such as seismaesthesia, barometric pressure, temperature and humidity) as well as other ecological distribution monitors or location of a moving sensor [14] or control system [5, 18], especially, in hostile environments (such as military sensing and tracking).

A wireless sensor network usually consists of a huge number of tiny autonomous devices called sensor nodes. A typical sensor node is equipped with a MHz processor rather than a GHz processor. It has limited memory size, short-range radio communication capability, and is powered by battery/solar energy, e.g., the MICA2 [7] is composed of an 8 MHz processor, 128 KB(Kilobyte) of instruction memory, 4 KB of RAM for data, 512 KB of flash memory, 19.2 Kbps (kilobit per second) bandwidth, and 10-20 meters communication range. In practice, the MICA2 with full energy can run about 2 weeks in the work mode, and one year in its sleep mode. However, sensor nodes have severe resource constraints