Accepted Manuscript

Title: Secure data aggregation using access control and authentication for wireless sensor networks

Author: Abdul Razaque, Syed S. Rizvi

PII: S0167-4048(17)30140-2
DOI: http://dx.doi.org/doi: 10.1016/j.cose.2017.07.001
Reference: COSE 1167

To appear in: *Computers & Security*

Received date: 20-1-2017
Revised date: 24-5-2017
Accepted date: 3-7-2017

Please cite this article as: Abdul Razaque, Syed S. Rizvi, Secure data aggregation using access control and authentication for wireless sensor networks, *Computers & Security* (2017), http://dx.doi.org/doi: 10.1016/j.cose.2017.07.001.

Secure Data Aggregation Using Access Control and Authentication for Wireless Sensor Networks

[1]Abdul Razaque and [2]Syed S. Rizvi
[1]Department of Computer Science, New York Institute of Technology, USA
[2]Department of Information Sciences and Technology, Pennsylvania State University, Altoona, PA 16601
[1]arazaque@nyit.edu and [2]srizvi@psu.edu

Abstract

The existing secure data aggregation approaches for wireless sensor networks were not designed for authorization, energy efficiency and proper security, leaving them prone to attacks. In this paper, we introduce the secure data aggregation using the access control and authentication (SDAACA) protocol. Using this protocol, we aim to detect two severe types of attacks: sinkhole and Sybil attacks that are difficult to detect by existing cryptographic approaches. The proposed SDAACA protocol consists of two novel algorithms: the secure data fragmentation (SDF) and the node joining authorization (NJA). The SDF algorithm hides the data from the adversary by fragmenting it into small pieces. In the NJA algorithm, an authorization process is initiated before allowing any new node to join the network. Both algorithms help improve the Quality of Service (QoS) parameters. Moreover, we propose an access control scheme that supports accuracy, energy efficiency, freshness and authentication by reducing the communication overhead and guaranteeing the communication authenticity process. Furthermore, the proposed protocol is mapped on the oil-refinery plant to prevent and detect both sinkhole and Sybil attacks in presence of static and mobile sensor nodes. Finally, we show the effectiveness of our proposed protocol through extensive simulations and a comparative study of other known secure data aggregation protocols.

Keywords: Secure Data Aggregation; Access Control; Authentication; Wireless Sensor Network Security; Sinkhole attack; Sybil attack; energy efficiency