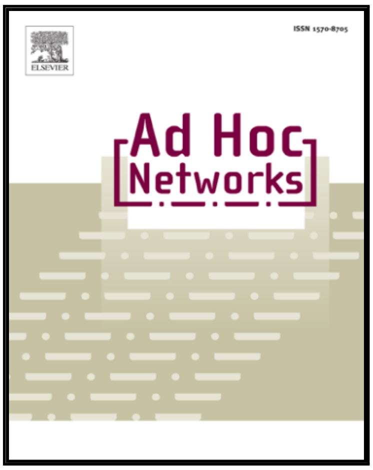

Continuous Leakage-Resilient Access Control for Wireless Sensor Networks

Yanwei Zhou, Bo Yang, Yi Mu, Zhe Xia

PII: S1570-8705(18)30432-3
DOI: 10.1016/j.adhoc.2018.07.001
Reference: ADHOC 1701

To appear in: *Ad Hoc Networks*

Received date: 6 February 2018
Revised date: 27 June 2018
Accepted date: 1 July 2018

Please cite this article as: Yanwei Zhou, Bo Yang, Yi Mu, Zhe Xia, Continuous Leakage-Resilient Access Control for Wireless Sensor Networks, *Ad Hoc Networks* (2018), doi: 10.1016/j.adhoc.2018.07.001

Continuous Leakage-Resilient Access Control for Wireless Sensor Networks

Yanwei Zhou[1,2,3], Bo Yang[1,3]*, Yi Mu[2], and Zhe Xia[4]

[1] *School of Computer Science, Shaanxi Normal University, Xi'an, China.*
[2] *School of Computing and Information Technology, University of Wollongong, Wollongong, Australia.*
[3] *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China.*
[4] *School of Computer Science and Technology, Wuhan University of Technology, Wuhan, China.*

Abstract

An important objective of cryptographic schemes is to withstand various attacks, including leakage attacks. Otherwise, leakage of the secret key may cause serious threats to the security of computer systems. However, leakage attacks have not received adequate attention in the literature. For example, most of the existing security protocols in the wireless sensor networks (WSNs) lack the consideration of leakage attacks. Instead, they are only designed in the traditional security model, in which an adversary is assumed not to obtain any information of the internal secret states. Obviously, this is not ideal because partial information of the secret key may be leaked in practice due to side channel attacks or fault injection attack. In this paper, we propose a new construction of secure continuous leakage-resilient certificate-based signcryption (CBS) scheme with access control without using bilinear pairings, and its security can be proved based on the assumptions that solving the classical decisional Diffie-Hellman problem and discrete logarithm problem is infeasible. We then propose a novel certificate-based access control scheme for the WSNs. The analysis shows that our construction not only achieves high computational efficiency in the continuous leakage setting, but also has superior performance regarding communication efficiency and storage requirement.

Keywords: Access Control Scheme, Certificate-based Signcryption, Continuous Leakage Resilience, Wireless Sensor Networks, Provable Security.

1. Introduction

Traditional wireless sensor networks (WSNs) consist many tiny sensor nodes with the capabilities of computing, sensing and communication. Hence, they have many useful applications in target tracking, military sensing, environment monitoring, etc. Moreover, they are useful techniques to build industrial Internet, such as Internet of things (IoT) and Internet of Vehicles (IoV). In IoT and IoV, many tiny sensor nodes are deployed on a smart equipment. These sensor nodes continuously monitor the efficiency of the smart equipment by measuring its vibration, pressure, temperature, humidity, power quality, etc. This helps to gather more comprehensive information so that the control centre can make better management control and decision making.

In Fig.1, we show an overview of the network framework in WSNs that is consisted of four different entities: a service provider (SP), the sensor nodes, a gateway and some users. The SP is in charge of deploying the wireless sensor network (WSN), including the registration of users and sensor nodes. The users who want to access the WSN will be authorized by the SP. The sensor nodes have limited computation and storage resources, while the gateway has much higher storage and processing capability. It is assumed that the SP is always trusted and it can never be compromised. However, the gateway is honest but curious. When a user wants to access the monitoring data of the WSN, she first sends a query message to a sensor node. Then, the sensor node checks if the user is authorized to access the WSN. If yes, the sensor node sends the collected data to the user through a secure channel. Otherwise, the sensor node rejects the query request.

*Corresponding author: Bo YANG, E-Mail: byang@snnu.edu.cn