Ad Hoc Networks 20 (2014) 1–15

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks

Ding Wang *, Ping Wang

College of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China
National Engineering Research Center for Software Engineering, Beijing 100871, China

ARTICLE INFO

Article history:
Received 19 June 2013
Received in revised form 10 January 2014
Accepted 11 March 2014
Available online 21 March 2014

Keywords:
Password authentication
Hierarchical wireless sensor networks
User anonymity
Smart card
Non-tamper resistant

ABSTRACT

Understanding security failures of cryptographic protocols is the key to both patching existing protocols and designing future schemes. In this work, we investigate two recent proposals in the area of smart-card-based password authentication for security-critical real-time data access applications in hierarchical wireless sensor networks (HWSN). Firstly, we analyze an efficient and DoS-resistant user authentication scheme introduced by Fan et al. in 2011. This protocol is the first attempt to address the problems of user authentication in HWSN and only involves lightweight cryptographic primitives, such as one-way hash function and XOR operations, and thus it is claimed to be suitable for the resource-constrained HWSN environments. However, it actually has several security loopholes being overlooked, and we show it is vulnerable to user anonymity violation attack, smart card security breach attack, sensor node capture attack and privileged insider attack, as well as its other practical pitfalls. Then, A.K. Das et al.'s protocol is scrutinized, and we point out that it cannot achieve the claimed security goals: (1) It is prone to smart card security breach attack; (2) it fails to withstand privileged insider attack; and (3) it suffers from the defect of server master key disclosure. Our cryptanalysis results discourage any practical use of these two schemes and reveal some subtleties and challenges in designing this type of schemes. Furthermore, using the above two foremost schemes as case studies, we take a first step towards investigating the underlying rationale of the identified security failures, putting forward three basic principles which we believe will be valuable to protocol designers for advancing more robust two-factor authentication schemes for HWSN in the future.

1. Introduction

With the rapid development of micro-electromechanical systems and wireless network technologies, wireless sensor networks (WSNs) have drawn increasing interest from both academic and industrial areas due to its easy deployment, ubiquitous nature and wide range of applications. Generally speaking, there are two architectures available for WSNs: the distributed flat architecture and the hierarchical architecture. Most large-scale WSNs prefer to follow the latter, for it is more energy-efficient and has more operational advantages than its flat counterpart [1]. In hierarchical wireless sensor networks (HWSN), there is a hierarchy among the nodes based on their capabilities: base station, cluster heads and sensor nodes. The HWSN is divided into a number of clusters to enhance its flexibility and to save energy consumption. Each cluster

* Corresponding author at: College of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China. Tel.: +86 185 1134 5776; fax: +86 010 6275 4993.
E-mail address: wangdingg@mail.nankai.edu.cn (D. Wang).

http://dx.doi.org/10.1016/j.adhoc.2014.03.003
1570-8705/

is administered by a cluster head. Sensor nodes communicate with each other in the same cluster and finally communicate with the cluster head via one-hop or multi-hop transmission(s). The base station is typically a gateway to another network, a powerful data processing and storage center, or also an access point for human interface. In this study, we focus mainly on HWSN, and more details about HWSN can be found in [2,3].

In many security-critical applications, such as real-time traffic control, industrial process control, healthcare monitoring and military surveillance, external users are generally interested in accessing real-time information from sensor nodes. To facilitate the external users to access the real-time data directly from the desired sensor nodes inside HWSN without involving the base station or gateway node as and when demanded (as illustrated in Fig.1), it is of utter importance to protect the users and systems' security and privacy from malicious adversaries because of the broadcast nature of wireless communications. Accordingly, user authentication becomes an essential security mechanism for the external user to be first authorized to the base station (or the gateway node) as well as the sensor nodes before granting his/her access to the real-time data. However, given the stringent constraints on memory capacity, computation capability, bandwidth and energy consumption of sensor nodes, it still remains quite a challenging problem to design an efficient and secure remote user authentication scheme for real-time data access directly from the desired sensor nodes inside HWSN.

To address the above issues, in 2011, Fan et al. [4] proposed the first smart-card-based password authentication scheme for HWSN. This proposal involves only lightweight operations, such as one-way hash function and exclusive-OR operations, which is well-suited to the large-scale resource-limited sensor networks. The authors claimed that their scheme is free from various related cryptographic attacks, such as smart card security breach attack, offline password guessing attack, replay attack and impersonation attack. Although their scheme is efficient and has been equipped with a formal security proof, we find it actually cannot achieve the claimed security goals: (1) it cannot preserve user anonymity and (2) it is vulnerable to smart card security breach attack. The authors also overlook dimensions on which their scheme fares poorly, such as the feature of local password change, resistance to node capture attack and insider-attack.

More recently, A.K. Das et al. [5] proposed a novel user authentication scheme based on traditional password and smart card to provide user access to real-time data by authorizing her directly at node level for HWSN. As with Fan et al.'s scheme [4], this protocol also only involves hash and XOR operations, with no additional symmetric encryption or asymmetric computations, and thus it is very efficient. This scheme also possesses many attractive features, such as dynamic node addition, local password change and session key establishment. Therefore, it exhibits great potential for practical applications. The authors claimed that their scheme provides better security as compared with the other related works, such as mutual authentication between the user and the cluster heads, resistance to privileged-insider attack, denial-of-service attack, node capture attack and smart card security breach attack. However, in this study, we demonstrate that it still cannot achieve the claimed security goals: (1) It is vulnerable to smart card security breach attack; (2) it fails to withstand privileged-insider attack; and (3) it suffers from the problem of server master key disclosure.

There have been a number of papers [6–13] dealing with security vulnerabilities in smart-card-based password authentication (i.e., two-factor authentication [14]) schemes for WSNs. In these studies, the authors only focus on presenting attacks on target protocols and proposing 'enhanced schemes', nevertheless, little (to the best of our knowledge, actually no) attention is paid to the underlying rationales of the identified security failures, and to the design principles of a sound proposal. Unsurprisingly, the same mistakes are repeated over and over again. For example, many schemes using non-tamper resistant smart

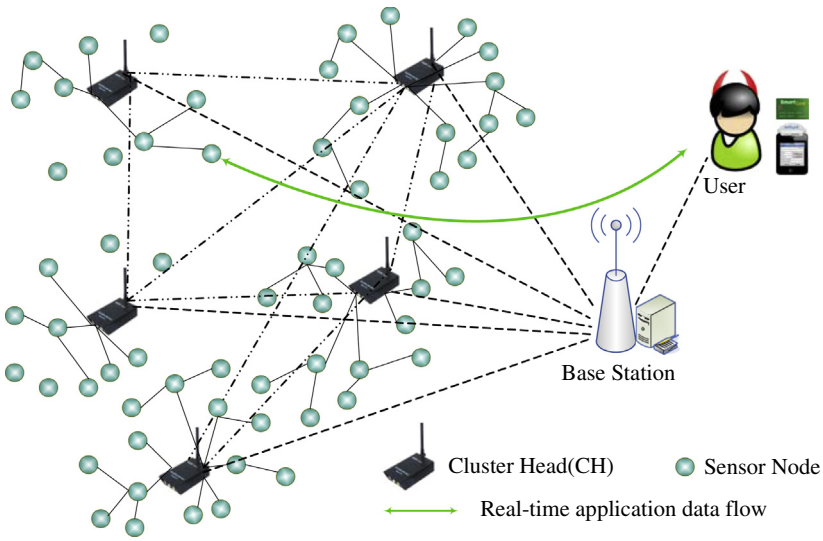

Fig. 1. Direct data access in hierarchical wireless sensor networks (HWSN).