Computer Networks 73 (2014) 41–57

Contents lists available at ScienceDirect

Computer Networks

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

On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions

Ding Wang [a,b,*], Ping Wang [b,c]

[a] School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China
[b] National Engineering Research Center for Software Engineering, Beijing 100871, China
[c] School of Software and Microelectronics, Peking University, Beijing 100260, China

ARTICLE INFO

Article history:
Received 2 April 2014
Received in revised form 27 June 2014
Accepted 27 July 2014
Available online 11 August 2014

Keywords:
Two-factor authentication
Wireless sensor networks
User anonymity
Smart card
Non-tamper resistant

ABSTRACT

Anonymity is among the important properties of two-factor authentication schemes for wireless sensor networks (WSNs) to preserve user privacy. Though impressive efforts have been devoted to designing schemes with user anonymity by only using lightweight symmetric-key primitives such as hash functions and block ciphers, to the best of our knowledge none has succeeded so far. In this work, we take an initial step to shed light on the rationale underlying this prominent issue. Firstly, we scrutinize two previously-thought sound schemes, namely Fan et al.'s scheme and Xue et al.'s scheme, and demonstrate the major challenges in designing a scheme with user anonymity.

Secondly, using these two foremost schemes as case studies and on the basis of the work of Halevi–Krawczyk (1999) [44] and Impagliazzo–Rudich (1989) [43], we put forward a general principle: Public-key techniques are intrinsically indispensable to construct a two-factor authentication scheme that can support user anonymity. Furthermore, we discuss the practical solutions to realize user anonymity. Remarkably, our principle can be applied to two-factor schemes for universal environments besides WSNs, such as the Internet, global mobility networks and mobile clouds. We believe that our work contributes to a better understanding of the inherent complexity in achieving user privacy, and will establish a groundwork for developing more secure and efficient privacy-preserving two-factor authentication schemes.

1. Introduction

With the rapid development of micro-electromechanical systems and wireless network technologies, wireless sensor networks (WSNs) have attracted increasing attention due to its wide range of applications from battlefield surveillance to civilian applications, e.g., environmental monitoring, real-time traffic control, industrial process control and home automation. As is well known, most large-scale WSNs [1–3] follow a tiered architecture due to its superiority in increasing the network capacity and scalability, accommodating the node mobility, reducing the management complexity and prolonging the network lifetime. Thus, in this work we mainly focus on the tiered WSNs as well. In many critical applications, external users are generally interested in accessing real-time information from sensor nodes, yet if the data queries are issued by the base station, efficiency, scalability and security may not be ensured over the long communication path between the base station and the sensor nodes [4,5].

* Corresponding author at: Room 560, 2#, Changchunxinyuan, University, No. 5 Yiheyuan Road, Haidian District, Beijing 100871, China. Tel.: +86 185 1134 5776; fax: +86 010 6276 5808.
E-mail addresses: wangdingg@mail.nankai.edu.cn (D. Wang), pwang@pku.edu.cn (P. Wang).

http://dx.doi.org/10.1016/j.comnet.2014.07.010
1389-1286/

To enable external users to access the real-time data directly from the desired sensor nodes without involving the gateway node (or base station) as demanded, it is of great concern that such critical data is well protected from eavesdropping, malicious modification, unauthorized access, and so on. Accordingly, user authentication constitutes an essential security mechanism for the user to be first authenticated by the sensor nodes before being granted the right to access data. Owing to its simplicity, portability, efficiency and high level of security, smart-card-based password authentication (or the so-called two-factor authentication [6]), as depicted in Fig. 1, has become one of the most promising authentication mechanisms for real-time data access in WSNs.

The past twenty years of research on two-factor authentication has proved that, it is incredibly difficult to get a general-purpose two-factor scheme right [7–9]. The design of a secure and efficient scheme for WSNs can only be harder. Crucially, the designers are confronted with a paradoxical challenge—"providing lightweight cryptographic algorithms for strong authentication, privacy and other cryptographic services on a speck of dust" [10]. On the one hand, sensor nodes and smart cards are small devices with low computation capability, limited memory capacity and scarce energy resources, it is more desirable to only employ symmetric-key techniques (e.g., hash functions, symmetric encryptions and XOR operations) rather than to use comparatively expensive asymmetric cryptographic operations (e.g., modular exponentiation and Pairing).

On the other hand, WSNs are generally deployed in unattended environments and often perform extremely sensitive tasks (e.g., health-care and battlefield surveillance) and thus, in addition to the traditional security threats, they exhibit a larger attack surface and are prone to more serious (even life-threatening) attacks. Consequently, an admired two-factor authentication scheme for WSNs should be able to guard against various known attacks including these general attacks such as impersonation, replay and offline password guessing, as well as some special attacks in WSNs environments like gateway bypassing and node capture [11]. Besides security, user privacy is also of particular interest. For example, some current projects including GEOSS [12] and NOPP [13] are developing large-scale WSNs to adaptively monitor the earth–ocean–atmosphere system. The sensed data may be of interest to various types of users ranging from individual users to universities, government research centers, and business companies (e.g., GEOSS [12] involves 61 countries, NOPP [13] involves the DARPA, the Department of Homeland Security among others). The activities of these users may be of great sensitiveness to the outsiders and even the users themselves cannot fully trust each other due to diversified interests. Consequently, there is an urgent need for protecting user's data access privacy, e.g., when she accessed the sensor data, which data types she was interested in, or from which nodes she obtained the data, since the leakage of such information could be exploited against her interest. Generally, there is a growing requirement for protecting user privacy information (e.g., preferences, login history, location, physical condition, personal data [14,15]) from being leaked and abused, which outlines the needs for designing schemes that can attain user anonymity.

It is worth mentioning that, in the context of user authentication, user anonymity is defined against the public rather than the server, because it is necessary for the latter to be aware of the real identity of each user in order to detect, record and remove the malicious users. Moreover, in many cases the server needs to learn the user identity for accounting, auditing, and/or billing purposes [16]. It also should be noted that, instead of a unique "user anonymity" property, different application scenarios may implement quite varied notions of what it means to be user anonymity [17,18], such as user identity protection, user un-traceability, anonymous user linkability, k-anonymity and blender anonymity. Interested readers are referred to [19] for more details. As for user authentication, this notion basically means user identity-protection, which ensures

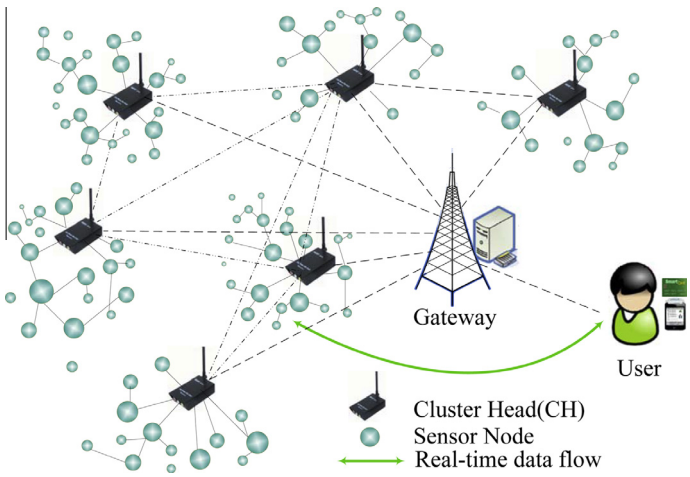

Fig. 1. Direct real-time application data access in WSNs.