Computer Communications 98 (2017) 43–51

Contents lists available at ScienceDirect

Computer Communications

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

Lightweight and escrow-less authenticated key agreement for the internet of things

Marcos A. Simplicio Jr., Marcos V.M. Silva, Renan C.A. Alves*, Tiago K.C. Shibata

Escola Politécnica, Universidade de São Paulo, São Paulo/SP, Brazil

ARTICLE INFO

Article history:
Received 16 September 2015
Revised 14 March 2016
Accepted 8 May 2016
Available online 20 May 2016

Keywords:
Security
Authenticated key agreement
Sensor networks
Internet of things

ABSTRACT

Security is essential for wide wireless sensor network (WSN) deployments, such as the Internet of Things (IoT). However, the resource-constrained nature of sensors severely restricts the cryptographic algorithms and protocols that can be used in such platforms. Such restrictions apply especially to authenticated key agreement (AKA) protocols for bootstrapping keys between authorized nodes: in traditional networks, such schemes involve the transmission of quite large certificates and the execution of memory- and processing-intensive cryptographic algorithms, which are not suitable for WSNs. Whereas lightweight WSN-oriented schemes also exist, most of them focus on small deployments where key-escrow is possible (i.e., a fully trusted authority knows the private keys of all nodes). Aiming to identify AKA solutions suitable for the IoT scenario, in this article we assess lightweight and escrow-free schemes, evaluating their security and performance in terms of processing time and energy consumption in the TelosB platform. Besides proving that some very efficient schemes are actually flawed, we show that the combination of SMQV (strengthened-Menezes-Qu-Vanstone) with implicit certificates leads to a secure and lightweight AKA scheme.

1. Introduction

Wireless Sensor Networks (WSNs) are a especial type of ad-hoc network comprising several autonomous sensor nodes, known as motes [1]. The interest of WSNs is that they can be deployed in the area of interest for gathering and processing data from their surroundings (e.g., mechanical, thermal, biological, chemical, and optical readings). Hence, they enable several applications, including environment and habitat monitoring, support for logistics, health care, and emergency response [1]. Sensors are also an integral part of the Internet of Things (IoT), in which they interact with actuators for building a pervasive smart network [2].

Motes usually have a limited amount of resources such as storage, memory, processing power, bandwidth and, especially, energy [3,4]. Therefore, one of the main design goals of WSN-oriented security protocols is to optimize processing and network usage, allowing sensors to preserve energy and, thus, extend the network's lifetime [5,6]. While many studies show the feasibility of symmetric cryptography for encryption [7,8] and authentication [6] in WSNs, the task of bootstrapping the required keys for using those algorithms is a more controversial issue. Preliminary schemes relied almost exclusively on key pre-distribution (for a survey, see [9]), avoiding the costs involved in asymmetric protocols for dynamic key generation and distribution at the cost of higher susceptibility to node capture and lower scalability. More recently, however, the development of highly efficient cryptographic libraries [10–12] with support to Elliptic Curve Cryptography (ECC) [13,14] and bilinear pairings [15] renewed the interest of asymmetric primitives for WSNs [16–18]. Especial attention was dedicated to authenticated key agreement (AKA) solutions following the ID-based paradigm [19], which uses identities (e.g., a label or network address) instead of random strings as public keys. The reason is that this allows keys to be dynamically generated with fewer and smaller messages than solutions relying on Public Key Infrastructure (PKI) certificates for public key validation [16,18], thus saving energy.

Unfortunately, however, recent cryptanalytic results [20,21] have shown the low security of the "pairing-friendly" elliptic curves in characteristic 2 that enable the processing and memory optimizations found in ID-based AKA schemes such as [10,11]. In addition, since the ID-based approach requires a trusted authority (TA) that issues (and, hence, knows) all private keys in the network, it is probably not be the best choice in the context of IoT. Actually, this key escrow property of the ID-based approach may be acceptable in small deployments, since in such scenarios the TA

* Corresponding author.
E-mail addresses: mjunior@larc.usp.br (M.A. Simplicio Jr.), mvsilva@larc.usp.br (M.V.M. Silva), ralves@larc.usp.br (R.C.A. Alves), tshibata@larc.usp.br (T.K.C. Shibata).

http://dx.doi.org/10.1016/j.comcom.2016.05.002
0140-3664/© 2016 Elsevier B.V. All rights reserved.

can simply be a computer controlled by the motes' owner [16,17]. However, in the large scale scenario of IoT, it is reasonable to consider that the TA would actually be a (federated) remote server. This server could then be accessed (e.g., via a domestic gateway) by multiple motes, owned by different users, for bootstrapping the keys that allow those sensors to engage in secure communications. In this context, it is not reasonable to assume that all users will fully trust the server with the private keys of their sensors.

Aiming to tackle the above-mentioned issues of existing protocols, in this manuscript we evaluate lightweight pairing- and escrow-free authenticated key agreement (AKA) schemes for use in WSNs. Our research shows that, unfortunately, there are only a few schemes in the literature with such characteristics, many of which actually suffer from security or performance issues. To address this lack of suitable candidates, we describe a combination of an elliptic curve variant of MQV [22] (in this article, we focus on the strengthened MQV, also called SMQV [23]) and public keys generated from implicit certificates [24,25], which can fulfill these requirements in an efficient manner. The advantage of implicit certificates is that they can be much shorter than traditional PKI-based certificates, saving memory for its storage and bandwidth (and, thus, energy) for its transmission. We also compare the resulting implicitly-certified AKA (iSMQV) protocol with existing solutions, showing that it is better adapted for use in the context of IoT and other constrained scenarios in which key escrow must be avoided. As an extra contribution, we also show that two highly efficient escrow-free AKA schemes recently proposed for use in WSNs are actually prone to impersonation attacks.

The remainder of the article is organized as follows. Section 2 discusses the recent advances in the area of WSN-oriented escrow-free AKA schemes, as well as their limitations. Section 3 then describes SMQV when employed under the implicit certification paradigm. The security of the resulting scheme is discussed in Section 4, while its performance in terms of processing and energy costs is experimentally evaluated in Section 5. Finally, Section 6 presents our concluding remarks.

2. Related work

Since the appearance of highly efficient ECC and bilinear pairings libraries such as MIRACL [26] and RELIC [12], the ID-based approach for key management in WSNs gained considerable attention from the research community. This interest led to many ID-based AKA schemes that rely on bilinear-pairings over elliptic curves as a way to reduce the amount of information exchanged between nodes in a WSN (e.g., [10,17,27–29], to cite a few). While the above-mentioned schemes do not tackle the key escrow issue, there are also a few pairing-based schemes [30–32] that do so by adopting the certificate-less paradigm [33]. In this case, the key escrow problem is avoided by partitioning the private key into two components: a partial identity-based key, generated by the TA and, thus, subject to escrow; and one conventional non-certified partial key, unknown to the TA. All those advances, however, were severely affected by recent attacks against the pairing-friendly curves [20,21] that would allow them to achieve a reasonably good performance. Therefore, the results obtained with such solutions and their corresponding suitability for use in WSNs need to be reconsidered with caution. Partially due to this reason, but also aiming at better efficiency, part of the WSN-oriented literature on AKA protocols has shifted to pairing-free, albeit still escrowed, schemes, such as those described in [34–37].

Finally, with a growing interest in bringing efficient and escrowless AKA solutions to the context of WSNs, a few pairing-free schemes based on the certificate-less paradigm appeared in the literature in the last few years [38–43]. Most of them involve more computation than traditional and well analyzed AKA protocols, such as MQV [22] and its variants (e.g., HMQV [44] and SMQV [23]). This happens because, as shown in Table 1, they involve a higher number of point multiplications, usually much more costly than point additions and hash computations. Nevertheless, these solutions remain potentially more energy-efficient than traditional MQV-like schemes due the reduced size of the messages exchanged between nodes, which is a direct advantage of the certificate-less paradigm over PKI-based solutions. Unfortunately, however, our analysis of the most efficient solutions among them (namely, [39], [43] and [40]) shows that they are actually flawed (see Appendix A), allowing attackers to impersonate any user in the network.

Table 1
Computational cost of different AKA schemes, in terms of point multiplications/additions (PM/PA) and hashes (H).

Protocol	PM	PA	H
Ni et al.[38]	6	3	2
Tu et al.[42]	5	3	3
Tong et al.[41]	5	1	3
Islam et al. [43] (flawed)	4	0	3
Yong-Jin et al. [39] (flawed)	4	3	2
Farouk et al. [40] (flawed)	3	5	2
(S)MQV [22,23]	4	2	4

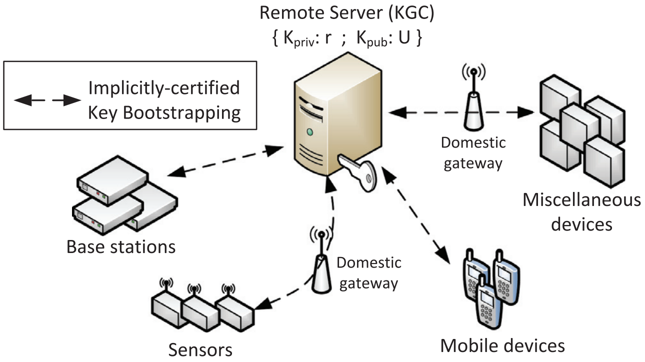

Fig. 1. Key bootstrapping using a key distribution center (KGC).

As it turns out, however, a highly energy efficient and escrow-free AKA protocol can be obtained by combining the security and performance of the (S)MQV protocol with implicit certificates [25], instead of relying on the certificate-less paradigm. To the best of our knowledge, the combination of the low-communication overhead provided by implicit certificates and the high security obtained with (S)MQV has not been explored in the WSN-specialized literature. Hence, even though in Section 5 we experimentally evaluate all non-broken schemes listed in Table 1, in what follows we describe how SMQV can be coupled with implicit certificates.

3. Implicitly-certified authenticated key agreement (iSMQV)

In this section, we describe an efficient WSN-oriented AKA scheme that is both pairing-free and escrow-less. The target IoT scenario is depicted in Fig. 1, which shows a number of different devices that, with the help of a common Key Generation Center (KGC), are able to bootstrap public/private key pairs $\{K_{pub}, K_{priv}\}$ and their corresponding implicit certificates. Leveraging on this implicit public key validation, any pair of nodes can then use an elliptic curve implementation of SMQV [23] for establishing symmetric keys among themselves, as depicted in Fig. 2.