Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 15 (2011) 1481 – 1486

Procedia Engineering

www.elsevier.com/locate/procedia

Advanced in Control Engineeringand Information Science

An Improved Direct Anonymous Attestation Scheme for M2M Networks

Yingying He[a],Liquan Chen[a]*, Lingling Wang[a]

a. Research Center of Information Security, Southeast University, Nanjing, 210096，China

Abstract

The remote anonymous trusted authentication of M2M equipments is a key problem in Internet of Things system. The Direct Anonymous Attestation (DAA) protocol had been adopted by TCG to implement the attestation of the trusted platform. Limited by the deficient computing and storing resources of most embedded devices, a new improved DAA (I-DAA) scheme is proposed to be applied in M2M networks. The proposed I-DAA scheme not only retains the security of the legacy DAA, but also greatly reduces the computational complexity, which makes it more suitable for M2M networks.

© 2011 Published by Elsevier Ltd. Selection and/or peer-review under responsibility of [CEIS 2011]

Key words: M2M; TPM; DAA; bilinear pairing; ECC

1. Introduction

M2M (Machine to Machine) networks are new research hotspot in Internet of Things system [1]. The security requirements in M2M systems are urgent to be solved. Thus, it is important to introduce the trusted computing framework into M2M networks. The core part of a trusted computing system is Trusted Platform Module (TPM).which is a security chip with physical tamper preventing, encryption, decryption, and other functions. One of the basic questions related to TPM is the attestation of TPM. In order to protect the privacy of TPM and the information integrity, TCG proposed a solution called Privacy CA

* Corresponding author. Tel.:13813852253.
E-mail address: Lqchen@seu.edu.cn.

1877-7058 © 2011 Published by Elsevier Ltd.
doi:10.1016/j.proeng.2011.08.275

scheme [2] in TPM standard v1.1 and DAA (Direct Anonymous Attestation) scheme [3] in TPM standard v1.2.

Although the Privacy CA scheme is simple, it has two apparent weaknesses [4]. To solve these two problems, the DAA scheme is proposed. But the traditional DAA scheme includes lots of zero-knowledge proof and complex calculation, which make it not suitable for embedded devices, such as M2M equipment, cell phones, etc. A lot of research has been done to improve the DAA schemes [5], [6], [7]. [8], [9]. We propose a new Improved DAA (I-DAA) scheme in this paper.

This paper is organized as follows. In Section 2, we give a brief analysis of these existing schemes. We describe the related mathematical fundamentals needed in Section 3 and the I-DAA scheme will be described in Section 4. In Section 5, security proofs are presented. Efficiency analysis and comparisons are described in Section 6 and conclusions are given in Section 7.

2 Existing ECC-DAA schemes

The existing schemes are as follows:

1) The BCL-DAA scheme [7], [8], a DAA scheme that introduced bilinear map into the basic DAA scheme to replace the RSA mechanism.

2) The CMS-DAA [9] scheme that uses asymmetric bilinear map instead of symmetric bilinear.

3) The ABP-DAA scheme [4]. It pointed out that if DDH problem in is easy, we can protect the privacy of TPM through blinding fP_1 .

4) The C-DAA scheme [5], which is by far the most efficient scheme. This scheme benefits from an efficient batch proof.

The ABP-DAA scheme simplifies much computational complexity, but it still has several deficiencies to be fixed.

- After receiving the credential (A, B, C), TPM or Host does not check whether it is legal, which reduces the computing complexity at the cost of decreasing the security level.
- The ABP-DAA scheme considers that DDH assumption in G_{1+} is easy, so TPM participates in computing C in the credential, $C = k^{-1}\tilde{C} = k^{-1}(x + fxy)K = (x + fxy)P_1$, But we generally consider the assumption is difficult.
- At the end of the ABP-DAA scheme, it points out that Issuer and Verifier may collude. If TPM provides fP_1 to Issuer, then Issuer can obtain privacy information by computing equation $e(B_i, fP_1) = e(B_i^f, P_1)$. Thus, in the ABP-DAA scheme, TPM provides kfP_1 instead of fP_1, but Issuer can obtain the privacy information by computing the equation $e(B_i, fkP_1) = e(B_i^f, kP_1)$, which means collusion can still succeed.
- In the whole scheme, no random number is added, which can not prevent replay attack.
- Since Base name is not used, it has no property of user-controlled-traceability, which decreases the flexibility of the scheme.

3 Pre-knowledge

3.1 Bilinear mapping [4]

G_{1+} , G_{2+} are two additive cyclic groups. $G_{3\times}$ is a multiplicative cyclic group, and order of the three groups is q . A map $e: G_{1+} \times G_{2+} \rightarrow G_{3\times}$, is called bilinear map if it meets the following conditions:

- **Bilinear:** For any $P_1, P_2, P \in G_{1+}$, $Q \in G_{2+}$, the two equations $e(P_1 + P_2, Q) = e(P_1, Q)e(P_2, Q)$ $e(aP, bQ) = e(P, Q)^{ab}$ hold, where $a, b \in Z_q$.

دریافت فوری ← متن کامل مقاله

ISIArticles
مرجع مقالات تخصصی ایران

- ✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
- ✓ امکان دانلود نسخه ترجمه شده مقالات
- ✓ پذیرش سفارش ترجمه تخصصی
- ✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
- ✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
- ✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
- ✓ دانلود فوری مقاله پس از پرداخت آنلاین
- ✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات