Journal of Information Security and Applications 40 (2018) 9–19

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

# Design of an enhanced message authentication scheme for smart grid and its performance analysis on an ARM Cortex-M3 microcontroller

Dariush Abbasinezhad-Mood, Morteza Nikooghadam*

*Department of Computer Engineering and Information Technology, Imam Reza International University, Mashhad, Iran*

ARTICLE INFO

*Article history:*
Available online 5 March 2018

*Keywords:*
ARM Cortex-M3
Key agreement
Elliptic curve cryptography
Smart grid
Smart meter security

ABSTRACT

Shared key generation between different entities of smart grid is so important because it can provide the possibility of subsequent fast and secure communications by means of symmetric key algorithms. Since the smart meters are some computationally-constrained electronic devices, this shared key generation process must put the least possible burden on the smart meters' resources. To this end, several lightweight authentication and key agreement schemes have been proposed during the last decade to be employed in the context of smart grid. Nevertheless, after careful consideration, we found that the efficiency and security of these schemes can still be improved. As a result, in this paper, we propose an enhanced elliptic curve cryptography based authentication and key agreement scheme that not only is secure against the well-known attacks and provides the perfect forward secrecy, but also is more efficient than similar recently published schemes in terms of both computational and communication costs. More significantly, our formal verification using the commonly-accepted ProVerif tool and implementation on a state-of-the-art Atmel 32-bit ARM Cortex-M3 microcontroller, as a suitable chip for the smart meters, confirm our claim.



## 1. Introduction

Smart Grid (*SG*), the next generation of power grid, is an intelligent electrical grid that benefits from features like digital structure, distributed generation, self-healing capabilities, and pervasive control and brings us more efficiency, flexibility, and reliability [1,2]. Due to the rapid decrease in fossil fuels and hence increase in the electricity production costs, and also the emission of greenhouse gases [1,3], upgrading the traditional electrical grid to a modern grid that can meet the actual requirements of today's modern societies [4] becomes a vital necessity. As a result, many countries intend to implement *SG* to not only take its many advantages, but also to overcome the cons of traditional power system. Nevertheless, there are many challenges in the adoption of *SG* that must be fully considered. The challenges of *SG* have been discussed by so many papers [1,5–11]. The authors of these papers, have mentioned the challenges, which exist in sensing and measurement [1], architecture [5], information and communication technologies [1,6,7,10], networking and routing [8], load-balancing [9], and security. Security is a very important and challenging requirement [12,13] that must be taken into account in all parts of *SG*. Hence, to achieve the security requirements, scholars have proposed numerous security schemes [14–28] from different aspects and they have applied miscellaneous security mechanisms, such as different flavors of encryption and access control. Among these papers, there are some works, which have paid attention to key generation and distribution [15–17], some papers have proposed solutions for the false data injection attack [18–20], many of these papers [21–25] have presented privacy-preserving methods, and some works like [26–28] have proposed lightweight schemes for communications of smart meters and neighborhood gateways in *SG*.

In *SG*, the advanced communication technologies have been integrated into the current power grid making management of the electrical grid infrastructure more affordable [2]. As opposed to the existing electrical grid, which has one-way communication, in *SG*, the communication is bidirectional. This two-way communication is an important concept [4,8], which facilitates the real-time monitoring and control of the electricity consumptions. In *SG*, the smart meters (*SMs*) collect the usage reports and send them to control center, and the control center also sends some control messages to the *SMs*. In between, there exist some gateways, such as Building Area Network (*BAN*) gateways and Neighborhood Area Network (*NAN*) gateways, which aggregate the sent usage reports of *SMs* and forward them to the control center [26]. Each *SM* must be able to communicate securely with a *BAN* gateway and this would be possible by first, the mutual authentication of the *SM* and *BAN* gate-

* Corresponding author.
*E-mail addresses:* dariush.abbasinezhad@imamreza.ac.ir (D. Abbasinezhad-Mood), m.nikooghadam@imamreza.ac.ir (M. Nikooghadam).

https://doi.org/10.1016/j.jisa.2018.02.007
2214-2126/

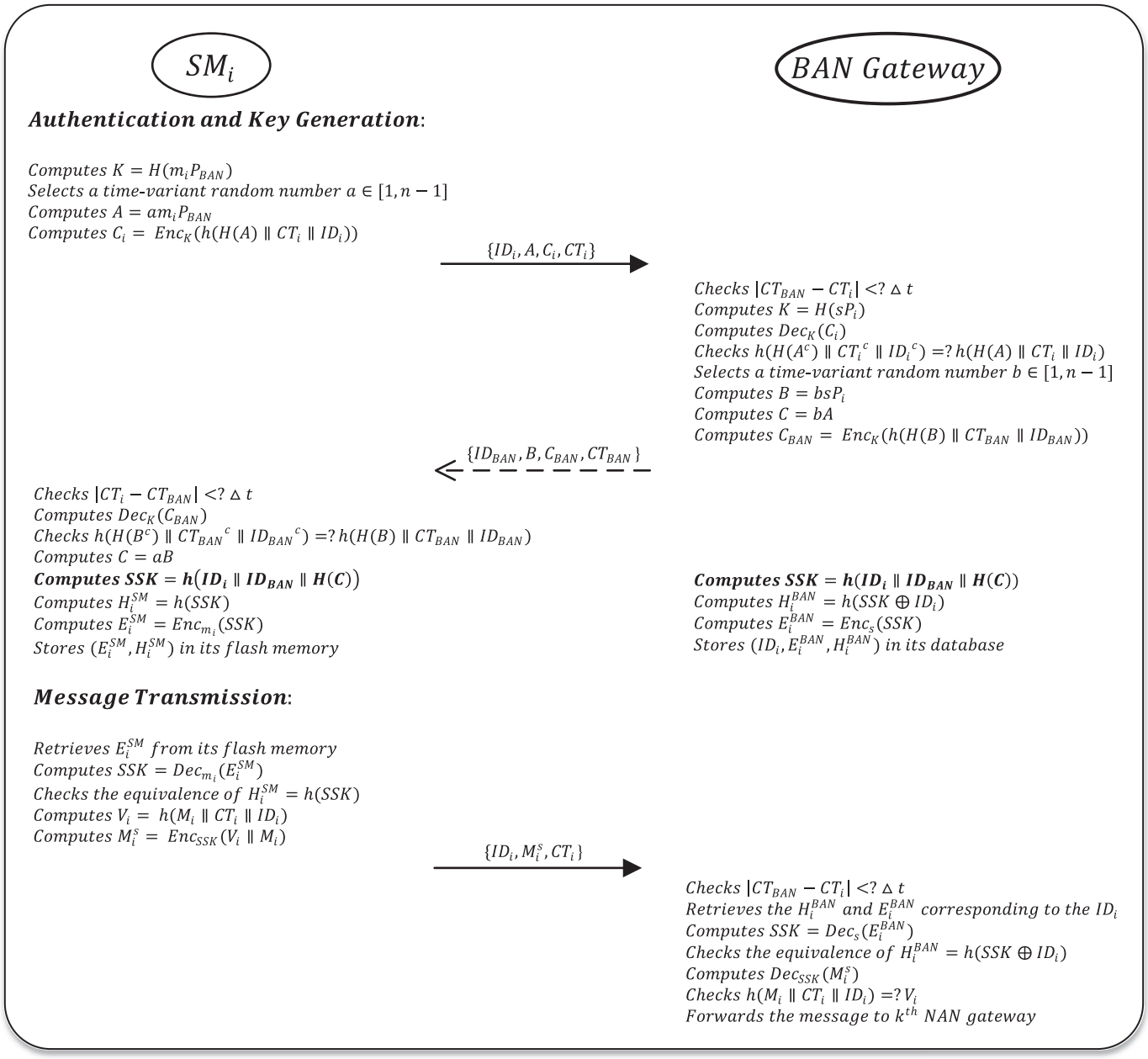


**Fig. 1.** The "mutual authentication and key agreement" and "message transmission" phases of the proposed scheme.

way and second, the generation of a shared common key. Afterwards, the *SM* and *BAN* gateway can communicate securely by applying the generated shared key and utilizing a symmetric encryption/decryption algorithm.

Since the *SMs* have limited storage space and computational capability, every proper authentication and key agreement scheme must not only consider the security requirements, but also must take the *SMs*' constraints into account. Therefore, presenting lightweight authentication and communication schemes is an interesting topic that has taken much attention from scholars. Li et al. [27] proposed an Authenticated Communication scheme (*AC*), which can be used for the secure communications of each *SM* and the neighborhood gateway. They employed the Merkle hash tree to construct a tree that can be applied for the message source authentication. They assumed a general Diffie-Hellman key exchange protocol for the common key generation and they also compared their scheme with the *RSA*-based authentication scheme. Recently, Liu et al. [28] have proposed an enhanced Lightweight Authenticated Communication scheme (*LAC*), which as opposed to the *AC* scheme uses the bitwise *Exclusive-OR* operation and the Lagrange interpolation formula for encrypting the collected usage reports and the sender authentication, respectively. These two schemes [27,28] and the presented scheme in [26] mainly focus on details of the communication phase and they just adopt a known protocol for the key agreement phase. Contrary to these three schemes, there are some schemes that mainly concentrated on the authentication and key agreement phase. In 2011, Fouda et al. [29] proposed a lightweight authentication scheme for the secure communications of the *SMs* that are used in the Home Area Network (*HAN*) and the *SMs* used in the *BAN*. Recently, Mahmood et al. [30] have proposed an improved lightweight message authentication scheme, which is more efficient than both Fouda et al.'s scheme [29] and Sule et al.'s scheme [31] in terms of computational cost. In order for the mutual authentication and key agree-