Future Generation Computer Systems 55 (2016) 362–375

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Fast authentication in wireless sensor networks

Chafika Benzaid [a,*], Karim Lounis [a], Ameer Al-Nemrat [b], Nadjib Badache [a], Mamoun Alazab [c]

[a] Laboratoire des Systèmes Informatique, USTHB, Algérie

[b] Architecture, Computing, and Engineering School, UEL, UK

[c] Australian National University, Australia

HIGHLIGHTS

- Exploit the cooperation between nodes to accelerate the signature verification.
- The accelerated scheme allows a longer network lifetime.
- The new scheme saves up to 45% of the energy drained during the verification.
- The accelerated scheme runs 66% faster than the traditional signature verification.
- Theoretical analysis, simulation, and real-world experimentation were conducted.

ARTICLE INFO

Article history:
Received 2 December 2013
Received in revised form
13 June 2014
Accepted 29 July 2014
Available online 16 August 2014

Keywords:
Broadcast authentication
ID-based cryptography
Digital signature
Accelerated verification
Wireless sensor networks

ABSTRACT

Broadcast authentication is a fundamental security service in wireless sensor networks (WSNs). Although symmetric-key-based μTESLA-like schemes were employed due to their energy efficiency, they all suffer from DoS attacks resulting from the nature of delayed message authentication. Recently, several public-key-based schemes were proposed to achieve immediate broadcast authentication that may significantly improve security strength. However, while the public-key-based schemes obviate the security vulnerability inherent to symmetric-key-based μTESLA-like schemes, their signature verification is time-consuming. Thus, speeding up signature verification is a problem of considerable practical importance, especially in resource-constrained environments. This paper exploits the cooperation among sensor nodes to accelerate the signature verification of vBNN-IBS, a pairing-free identity-based signature with reduced signature size. We demonstrate through on extensive performance evaluation study that the accelerated vBNN-IBS achieves the longest network lifetime compared to both the traditional vBNN-IBS and the accelerated ECDSA schemes. The accelerated vBNN-IBS runs 66% faster than the traditional signature verification method. Results from theoretical analysis, simulation, and real-world experimentation on a MICAz platform are provided to validate our claims.

1. Introduction

In wireless sensor networks, message broadcast is an efficient and a common communication paradigm that allows a multitude of users to join in and disseminate messages into the network dynamically in order to obtain information of their interest. Unfortunately, sensor networks are very susceptible for attacks. Due to the nature of wireless communication in sensor networks, adversaries can easily eavesdrop on the traffic, inject bogus data messages or alter the contents of legitimate messages during multihop forwarding. Hence, authentication mechanisms must be provided to ensure that communication at all times is performed between the correct entities.

When the issue of broadcast authentication first appeared, symmetric key cryptography-based μTESLA-like schemes [1,2] were employed due to their energy efficiency. μTESLA-like schemes provide source authentication and message integrity by using one-way hash chains and delayed disclosure of authentication keys. By using Message Authentication Code (MAC) and one-way hash functions, μTESLA is able to take low computation effort to broadcast. Nevertheless, the μTESLA induces cache delays for broadcast packets which could be exploited by an attacker to launch DoS attacks [3]. The lack of immediate authentication makes μ-TESLA and its variations unsuitable for applications with real-time

* Corresponding author. Tel.: +213 21247917.
E-mail addresses: w_benzaid@yahoo.fr, cbenzaid@usthb.dz (C. Benzaid).

http://dx.doi.org/10.1016/j.future.2014.07.006
0167-739X/

requirements. In addition, they also require some level of synchronization between all nodes in the network which must be achieved by periodic broadcasting [4]. All these shortcomings make such schemes unsuitable for broadcast authentication.

Public key cryptography (PKC), on the other hand, is desirable for broadcast authentication. Employing PKC for implementing broadcast authentication in WSNs provides simple solutions, strong security resilience, good scalability and immediate message authentication, when compared to symmetric-key based solutions [5]. Although there is a prejudice against the feasibility of PKC in WSN, recent studies [6,7] have reported that PKC is possible in WSNs. For instance, Elliptic Curve Cryptography (ECC) signature verification takes 1.61 s, with 160-bit keys on an ATmega128 8-MHz processor [6]. Thus, several PKC-based broadcast authentication protocols have been proposed [8,7,9,10]. These protocols are based on several cryptographic techniques, including Merkle Hash Tree [11], public-key ECC-based signature scheme such as ECDSA [12], and ID-based signature scheme [13] with either pairing-free or optimal-pairing. While the PKC-based schemes avoid the security vulnerability intrinsic to μTESLA-like schemes, the relatively slow signature verification in public-key cryptosystems causes high energy consumption and long verification delay for broadcast authentication in WSNs. Thus, speeding up signature verification is a problem of considerable practical importance, especially in resource-constrained environments. Fan and Gong [5] proposed a method to accelerate ECDSA signature verification in WSNs by exploiting the cooperation among sensor nodes. The speedup results from each node probabilistically forwarding a partially-calculated signature to its neighbors. Then many sensor nodes can use the received intermediate computation results to accelerate their signature verifications. Unlike public-key ECC-based authenticated systems, ID-based authenticated systems do not require the transmission of public-key certificates which reduces the certificate overhead and improves computational efficiency. This makes them especially attractive for use in WSNs. However, the verification of ID-based signatures is still slow and computationally expensive for WSNs.

Inspired by the acceleration technique of Fan and Gong [5], we propose in this paper an accelerated verification of digital signatures generated by vBNN-IBS [9], a pairing-free identity-based signature with reduced signature size. However, unlike the original technique and in order to harden the attacker's task, the proposed technique releases the sum of two intermediate computation results rather than releasing them separately. By doing so, it becomes more difficult for an attacker to forge the two intermediate results. It also allows to reduce the message overhead while more intermediate results are released. Another important contribution of our work consists in the extensive performance evaluation through theoretical, simulation and real-world experimental studies. Through this evaluation, we:

- carefully chose the optimization methods used for a scalar point multiplication based on ensuring a satisfactory compromise between the execution time and the required memory size.
- emphasized the impact of energy consumed by the different node's states on the protocol performances; something that was neglected in similar works. We found out that node's states constitutes an important fraction (more than 92%) of the total energy dissipated within the network. Therefore, neglecting this important fraction can lead to erroneous conclusions about the protocol performances.
- demonstrated that the scheme's performances are not only affected by the number of nodes releasing intermediate results, but also by the deployment topology of nodes and the diffusion pattern followed to broadcast the user packet in the entire network.

The rest of the paper is organized as follows. In Section 3, we give a brief introduction to elliptic curve cryptography and vBNN-IBS [9]. Section 4 describes the proposed acceleration technique for signature verification in WSNs. In Section 5, we improve the scheme and we discuss the selection of system parameters. The security strengths of the proposed scheme are discussed in Section 6. Section 7 presents theoretical, simulation, and real-world experimentation performance results that demonstrate the effectiveness of the proposed acceleration technique. The impact of the network topology on the performance achieved is assessed in Section 8. Finally, Section 9 outlines our concluding remarks and future work directions.

2. Related work

When the issue of broadcast authentication first appeared, symmetric key cryptography-based μTESLA-like schemes [1,2,14] were employed due to their energy efficiency. μTESLA-like schemes provide source authentication and message integrity by using one-way hash chains and delayed disclosure of authentication keys. μTESLA [1] is an extension of the TESLA [15] authentication scheme adapted for WSNs to reduce the computation overhead. The μTESLA scheme employs a chain of authentication keys linked to each other by a one-way hash function; each key in the chain is the hash value of the next key computed using the one-way hash function. The first key of the chain, called the *key-chain commitment*, is securely sent to all the receiving nodes. A sender broadcasts a packet along with a Message Authentication Code (MAC) generated using the current key from the one-way chain, that key will be disclosed after a pre-defined period of time. Upon receiving this packet, each receiver checks if the packet was sent before the disclosure of the key used to calculate the attached MAC. If so, the receiver buffers the packet which will be authenticated when the corresponding disclosed key is received. μTESLA faces a scalability problem because the key-chain commitment has to be unicasted to each node which incurs high communication overhead limiting the network scale. Moreover, the key chain length is limited, and thus cannot support broadcast for a long time.

To address the two aforementioned problems, the multi-level μTESLA [2] technique was proposed. The unicast-based distribution of key chain commitments is bypassed by predetermining and broadcasting the commitments. To extend the lifetime of authenticated broadcast without requiring a very long key chain, a multi-level key chains are used. The keys in the lowest level key chains are used for authenticating data packets and usually lasts for a relatively short period. Each higher-level key chain is used to distribute the commitments of the immediately lower-level key chains. However, multi-level μTESLA scheme as well as the original μTESLA protocol are not scalable in terms of the number of senders. Subsequently, the tree-based μTESLA [14] scheme was proposed to support a large number of senders over a long period of time by using Merkle hash tree [11]. The basic idea consists first in defining multiple μTESLA instances which may be used by different senders during different periods of time. Then, a Merkle hash tree is built to authenticate and distribute the initial parameters (i.e., the key chain commitment, starting time, duration of each μTESLA interval, etc.) for μTESLA instances. The ith leaf corresponds to the hash value of the initial parameters for the ith μTESLA instances. Unfortunately, the tree-based μTESLA scheme supports the multisender scenario at the cost of higher communication overhead per message, limiting thus the number of senders.

By using MAC codes and one-way hash functions, μTESLA-like schemes are able to take low computation effort to broadcast. Nevertheless, those schemes induce cache delays for broadcast packets which could be exploited by an attacker to launch DoS attacks [3]. The lack of immediate authentication makes μTESLA