Computers and Electrical Engineering 59 (2017) 242–249

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

A two way authentication using bilinear mapping function for wireless sensor networks[☆]

Shyamala Ramachandran[a,*], Valli Shanmugam[b]

[a] Department of Information Technology, University College of Engineering, Tindivanam, 600401 India
[b] Department of Computer Science and Engineering, Anna University, Chennai 600025, India

ARTICLE INFO

Article history:
Received 23 June 2016
Revised 9 November 2016
Accepted 11 December 2016
Available online 27 February 2017

Keywords:
Two-way authentication
MAP function
Computation cost
Wireless Sensor Network
Secure group leader selection
Bilinear MAP function

ABSTRACT

The deployment of sensor networks for security and safety related environments requires securing communication primitives such as broadcast, multicast, and point to point communication. Security services are vital for ensuring the integrity, authenticity, and confidentiality of the critical information. Therefore, the authentication mechanisms are required to support these security services and to be resilient to distinct attacks. Recent research shows that two-way authentication provides better security and high energy saving for wireless sensor networks (WSN). In this work, we investigate a shared authentication protocol for WSNs using bilinear mapping function. Many one-way broadcast authentication protocol proposed such as Timed Efficient Stream Loss-Tolerant Authentication (TESLA), Bin and Balls Authentication (BiBA), etc., which cannot provide energy efficient authentication. Here, we propose a two-way authentication based on bilinear map function and used in secure group formation algorithm. The performance metrics such as message cost, computation and communication overhead are calculated.

1. Introduction

Wireless sensor network (WSN) consists of million/billion of sensor node deployed in the target field [1]. The target area may be an environment monitoring, habitat monitoring, healthcare, home automation, traffic control and industrial system automation. In the application area, the sensor nodes are deployed from truck or airplane. The deployed nodes form the adhoc infrastructure-less wireless network. Each sensor node senses a data such as pressure, temperature, etc., and routes the data to the base stations through the multi-hop communication path. The advantages of the wireless sensor networks are, it requires less power, easy to deploy and low maintenance. The communication between sensor nodes and the base station is either broadcast or multicast. In hierarchical sensor networks, the three kinds of nodes are used for communication. They are the base station, group leader and the sensor node. In this type of network multicast communication saves more power. Due to the fact, sensor nodes have limited capabilities like low power battery, small memory, less data processing capability and short communication range. Multicast group communication is well suited. The sensor nodes deployed in hostile environment security and piracy are highly important. Authentication is one of the essential requirements for secure communication. The best authentication scheme is a public key authentication which uses large key size for digital certificates [2,3]. Because of this property public key cryptography is not suited for WSN. Therefore, previous works [4–6] such as BiBa,

[☆] Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. A. Parakh.

[*] Corresponding author.
E-mail addresses: vasuchaaru@gmail.com, shyashyala@gmail.com (S. Ramachandran), valli@annauniv.edu (V. Shanmugam).

http://dx.doi.org/10.1016/j.compeleceng.2016.12.009
0045-7906/© 2016 Published by Elsevier Ltd.

TESLA etc. use one-way hash functions which use SHA/MD5. In our work we consider map to hash function and device identification number as a key for two-way authentication. This authentication method was implemented in group based WSN and the results were obtained.

The rest of this paper is organized as follows. Section 2 explains the related work and Section 3 describes the proposed system architecture. Section 4 explains the Working of the two-way authentication protocol. Section 5 analyzes the performance and Section 6 concludes the work.

2. Related work

Ren et al. [5] described Markel hash tree based broadcast authentication scheme for WSN and proved that communication delay is less but it fails to provide less computation time with an increase in group size. Das and Hsieh et al. [7,8] provided two-factor authentication protocol which gives strong authentication and session key establishment. Jokhio et al. [9] developed a secure localization schema which uses SHA. Li et al. [10] proposed the secure method for integrating WSN in Internet of Things (IoT) based on bilinear Diffie Hellman and signcryption schema. Rasheed et al. [11] proposed a three-tier security scheme for WSN. It uses q – composite key per distribution scheme and compared the performance with another pairwise key distribution scheme. Alagheband et al. [12] suggested dynamic and secure key management for hierarchical WSN using elliptic curve cryptography (ECC). Zhu et al. [13] proposed a trust management system for cloud-based sensor networks. Saewoon et al. [14] used pattern based key renewal scheme for WSN and guaranteed long lifetime. Jian Li et al. [15] presented an authentication system for hop by hop message using ECC. It uses polynomial based function to preserve privacy. Abdallah et al. [16] described a key management function using ECC and requires less key exchange and less processing overhead. Alshinina et al. [17] proposed an authentication system using ECC and compared with traditional RSA public key algorithm. Jilna et al. [18] proposed an optimized hardware design which implemented ECC-based key management scheme.

Choi et al. [19] described a location based key management to solve interference problem and resist insider attacks. Saleh et al. [20] suggested an authentication method for routing using shared key in which each node authenticates itself. This method needs more energy. Zhang et al. [21] proposed a key management scheme for hierarchical sensor networks and gave key establishment, key transportation, and dynamic key revocation algorithms and proved that method has high security with less communication computation and storage. Singh et al. [22] described insider intruder detection scheme for WSN and proved this visual cryptography taken less time and energy. Bhaskar et al. [23] discussed a genetic algorithm to secure data aggregation in hierarchical WSN. By this work, he proved that genetic algorithm highly reduced transmission overhead in WSN. Sarvabhatha et al. [24–26] discussed a mutual authentication method using biometric system. The biometric authentication is used for IoT and proved that it resisted all major cryptography attack with less computation cost. Banaie et al. [27] unified WSN and cloud and proposed secure data processing framework for sensor cloud infrastructure using the hash function. Ahmed et al. [28] suggested polynomial bivariate key and ID secure communication between the mobile sink and sensor nodes and stated that this method required less energy and is inexpensive. He et al. [29] described a dos attack resistant distributed code dissemination technique for WSN. The authors [30–32] suggested a method secure routing using TESLA based certificates. Therefore, it is observed that one-way authentication had a limitation of one key/one message. Only one message is sent from sender to receiver using a key in which the sender was authenticated. For the communication from the receiver, another key is used. So, key renewal is often and key computation time is longer. The PKI is extremely powerful but it is not simplified for WSN. Hence, it is necessary to improve the designed two-way authentication protocol in which both sender and receiver authenticate each other assures the identity of both the parties. This work attempts a two-way authentication protocol using the map to a hash function for three-tier hierarchical WSN and studied the performance such as computation time, overhead and energy consumption.

3. Proposed architecture and assumptions

In this section, we discuss the proposed network architecture of two-way authentication protocol. In our protocol, we have identified four types of nodes such as base station, the gateway node, group leader and sensor nodes. These four types of nodes are given in Fig. 1 and all four nodes are used in implementation are explained in the further section.

3.1. Preliminaries and assumptions

The Weil pairing was introduced by Andre Weil in 1940 has proven to be a useful tool in the study of elliptic curves. There are several definitions of the Weil pairing which are all closely related but not exactly equivalent. We will not focus on these differences here and stick to the definition that allows for straightforward extraction of an algorithm to compute it. The Weil pairing is a function that maps a pair of points in an n-torsion group of an elliptic curve to an nth root of unity in some extension field of the field the curve was defined over. Let ‘n’ be a prime number. Let $G = <P>$ be an additively-written group of order n with identity ∞, and let G_T be a multiplicatively-written group of order n with identity 1. A bilinear pairing on (G, G_T) is a map e: $G \times G \rightarrow G_T$ that satisfies the following conditions [33]:

- Bilinearity: For all $R, S, T \in G_1$, $e(R+S, T)=e(R, T)\, e(S, T)$ and $e(R, S+T)=e(R, S)\, e(R, T)$.