Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 109C (2017) 553–559

Procedia Computer Science

www.elsevier.com/locate/procedia

The 8th International Conference on Ambient Systems, Networks and Technologies (ANT 2017)

An Efficient Broadcast Authentication Scheme in Wireless Sensor Networks

Bacem Mbarek[a], *Aref Meddeb*[b], *Wafa Ben Jaballah*[c] *and Mohamed Mosbah*[d]

a National Engineering School of Tunis, University of Tunis El Manar, Tunis, Tunisia, Email:bacem.mbarek1@gmail.com
b National Engineering School of Sousse, NOCCS Laboratory, University of Sousse, Tunis, Tunisia
c Orange, France
d LaBRI, Bordeaux INP, University of Bordeaux, CNRS, France

Abstract

Broadcast source authentication is a challenging topic in wireless sensor networks. This security service allows senders to broadcast messages to multiple receivers in a secure way. Although several authentication mechanisms have been proposed to address the need for security in WSNs, most of them are resource consuming and are inadequate for constrained environments. In this paper, we shed the light to the security vulnerabilities of symmetric key based authentication mechanisms, and their inability to tackle memory DoS attacks. Moreover, we provide a new efficient broadcast authentication scheme based on a Bloom filter data structure in order to reduce the communication overhead. Finally, we run a thorough set of simulations to assess the efficiency of our approach compared to some state of the art solutions in terms of energy consumption, communication and computation overhead. Our results provide insight into the suitability of our approach for use in WSNs.

Peer-review under responsibility of the Conference Program Chairs.

Keywords:
Source Authentication, Broadcast authentication, Wireless Sensor Networks, Bloom filter

1. Introduction

Wireless sensor networks (WSNs) are frequently used for data gathering applications, such as military sensing and tracking, environment monitoring, patient monitoring, etc. WSN is in general, more vulnerable to attacks and unauthorized access than traditional (wired) networks. The sensor nodes are often deployed in hostile environments where they can be easily captured, compromised, or manipulated by an adversary. Therefore, the security becomes extremely important that provide confidentiality and authentication are critical for the operation of many sensor ap-

* B.Mbarek, National Engineering School of Tunis, University of Tunis El Manar, Tunis, Tunisia, Email: bacem.mbarek1@gmail.com
E-mail address: author@institute.xxx

Peer-review under responsibility of the Conference Program Chairs.
10.1016/j.procs.2017.05.340

plications. For this reason, the implementation of secure techniques in WSN are an important research topic[1,2]. Networks should collect data from the sensors for long periods of time without requiring human intervention. In addition, it could be impossible or inconvenient to recharge the battery, because nodes may be deployed in a hostile or unpractical environment. The sensors must be low in cost, thus will have constrained battery power, limited storage and low computational capacity[3]. Due to these constraints it is difficult to directly employ the existing security approaches to the area of WSNs. Therefore, security protocols for WSNs are focused on conquest of these constraints. In this work, we focus on broadcast authentication as it is a fundamental security service that enables a sender to broadcast critical data to receiver nodes in an authenticated way such that an attacker is unable to forge broadcasted messages.

Due to their inherent limitations, WSNs are especially sensitive to severe Denial of Service (DoS) attacks[3,4,5]. Compared to traditional networks, a WSN is more resource constrained, subject to open wireless communication, and prone to the physical risks of in-situ deployment. These factors increase the susceptibility of WSNs to DoS attacks. An adversary could either execute signal jamming attack; or overwhelm nodes to quickly exhaust their energy, communication bandwidth, memory and CPU of sensor nodes. In this paper, we address the vulnerability of WSNs to DoS attacks when providing authentication mechanisms. We propose a novel bloom filter scheme, for broadcast authentication protocols in wireless sensor networks. The novel bloom sheme reduce the hash function colLision by using a collision resolution scheme for the values stored in the filte, and have a very hight resistant against collision attaks that the attacker could muster. These protocol implementations are evaluated and validated in terms of authentication delay, authentication probability, resilience against DoS attacks, memory and energy consumption overhead.

The remainder of this paper is organized as follows. Section 2 describes work related to broadcast authentication and presents various authentication protocols used for WSN. In Section 3, we present our solution, and Section 4 provides a thorough performance evaluation. Finally, Section 5 concludes the paper.

2. RELATED WORK

Many secure broadcast authentication based schemes have been proposed for resource constrained networks[6,3,7,4,8,9]. Broadcast authentication schemes could be classified into three groups based on the main cryptographic primitive employed: (1) Message Authentication Code (MAC), (2) signature amortization and (3) one-time signature.

Protocols in the first group are symmetric authentication schemes such as TESLA[10], its simplified version for resource limited networks μTESLA[11], and the enhancements of μTESLA such as[7]. These schemes provide broadcast authentication by using MACs and require time synchronization between the nodes and the sink. Moreover, these schemes are vulnerable to DoS attack. Another shortcoming of μTESLA is the difficulty of establishing the initial trust between the nodes and the sink.

Schemes in the second group of broadcast authentication protocols employ signature amortization. One of the first protocols in this group is SAIDA [12]. This protocol is not robust against false packet injection and packet modification attacks. The designers of SAIDA have proposed Reed Solomon codes to handle the packet modification attack. However, this kind of coding is too complex for the low-power processor of the nodes. The one-time signature BiBa[13] and an improvement of BiBa, called HORS[14], are among the schemes in the second group. The major drawback of using one-time signature schemes in wireless networks is that the public key has to be frequently updated to maintain security. This requirement significantly adds to the communication overhead of the protocol. Moreover, broadcast authentication schemes based on one-time signatures are not suitable for designing node-to network multihop broadcast protocols. Broadcast communications of any node has to be handled by the sink as an intermediary.

The third category employs symmetric keys[4,8,15], however it implements time asymmetry to tackle the source authentication problem. An efficient time asymmetry scheme based on key disclosure is μTESLA[11], a simplified version of TESLA[10]. The main idea is to use key disclosure delay to keep the authentication key secret until the expiration of a given time interval, and then it will be disclosed. This approach is referred to as temporal asymmetry authentication TESLA[7]. Such approaches are adequate for non real time applications in which the actual reception of the packet and its verification depend on key disclosure delay. All these schemes use MACs and require time synchronization between the nodes and the sink. These schemes are vulnerable to DoS attack and exhibit some difficulties to establish initial trust between the nodes and the sink.