Ad Hoc Networks 24 (2015) 288–316

Contents lists available at ScienceDirect

Ad Hoc Networks

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

Survey Paper

A survey of broadcast authentication schemes for wireless networks

Kanika Grover *, Alvin Lim

Computer Science and Software Engineering, Auburn University, Auburn, AL 36849, United States

ARTICLE INFO

Article history:
Received 30 August 2013
Received in revised form 24 March 2014
Accepted 28 June 2014
Available online 23 August 2014

Keywords:
Broadcast
Authentication
TESLA
Digital signatures
Wireless networks

ABSTRACT

With the increase in the usage of wireless networks and their applications where broadcast transmission is widely used, it has become critical to authenticate broadcast messages. Several broadcast authentication techniques are currently available. However, no scheme is ideal for all broadcast transmission applications. Our goal is to classify, compare and analyze existing broadcast authentication techniques to enable designers to select an appropriate technique that suits their system, computation, communication and application requirements. Furthermore, this study provides better understanding of the research challenges that are still not addressed or only partially addressed.

1. Introduction

There has been a massive increase in the variation of wireless applications that require broadcast transmission of messages. For example, in vehicular networks, broadcast can serve as a means to alert other vehicles about an accident or congestion further on down the road, using intersection collision warnings (ICW) and road congestion notification (RCN). Other examples include broadcast of emergency calls for staff in hotels and hospitals, broadcast of a location change information for a session in conferences, and broadcast of new offers and deals in supermarkets and shopping stores. Moreover, there is an immense variation in the kind of wireless devices that will be receiving the wireless broadcast transmission, an instance is depicted in Fig. 1.

The increase in the use of broadcast transmission brings along with it an increase in threats and attacks, thus demanding security alternatives for all types of circumstances. The issue that life and safety are involved in some of these applications makes authentication of broadcast messages much more important. Hence, it has become critical to discuss available broadcast authentication schemes, including their advantages, shortcomings and requirements, in order to improve broadcast authentication schemes.

Various types of authentication schemes have been proposed in wireless network security, but as new threats and attack models are introduced, more need to be developed. Authentication schemes can be distinguished based on the following two basic criteria and an optional third criterion. Firstly, authentication schemes can be differentiated according to the purpose they accomplish, i.e., authenticating unicast, multicast or broadcast messages. Secondly, authentication schemes can be characterized by the cryptographic method used. It can be either a symmetric (shared-key) method or an asymmetric (public-key) method. Thirdly, authentication schemes targeting static, mobile or both aspects of the wireless networks are of importance in Mobile Ad hoc Networks (MANETs) and Vehicular Ad hoc Networks (VANETs).

* Corresponding author.
E-mail addresses: kanika@auburn.edu (K. Grover), limalvi@auburn.edu (A. Lim).

http://dx.doi.org/10.1016/j.adhoc.2014.06.008
1570-8705/© 2014 Elsevier B.V. All rights reserved.

Fig. 1. Wireless broadcast transmission.

Numerous high quality research papers have focused on point-to-point authentication schemes for wireless networks that validate unicast messages [1–11]. Despite being provably secure, unicast schemes cannot be applied directly to multicast or broadcast authentication messages; hence, the need for dedicated broadcast authentication mechanisms. A broadcast authentication scheme must make sure that broadcast messages are received directly from reliable sources, without being modified in transit. Therefore, the basic and most essential component of a broadcast authentication process is confirming the identity of the source from which the message originates (non-repudiation) as well as the integrity of the message to ensure the originality of the message. In addition, providing precaution against impersonation, forgery and replay attacks are important features of authentication schemes.

As discussed above, authentication schemes can be studied on the basis of cryptographic methods, which can either be symmetric or asymmetric. Symmetric methods use shared-key cryptography while asymmetric methods use public-key cryptography. In shared-key methods, both the sender and receiver use the same key in their authentication and verification processes. On the other hand, in public-key methods, a pair of keys is used, such that a sender signs a message with the private key and receiver(s) verify it using the corresponding public key. Shared-key methods are used in schemes such as Message Authentication Codes (MAC) whereas public-key cryptography is used in digital signatures techniques.

In our survey, we focus on asymmetric broadcast authentication schemes because symmetric key schemes are less secure. Therefore, in our study we classify the asymmetric broadcast authentication schemes on the basis of the cryptographic building block used in the technique. The building blocks under which we classify broadcast authentication schemes are MACs (operating asymmetrically), one-time signatures and digital signatures using public key.

In brief, this work discusses existing broadcast authentication schemes for wireless networks, classified according to their cryptographic building blocks. Further, we compare and analyze the schemes to generate a list of important issues and open research challenges. Therefore, we provide an exhaustive study on the available schemes for broadcast authentication in wireless networks and their applications. Our study includes an important aspect of examining the schemes on the basis of properties that we perceive as necessary for broadcast authentication, such as non-repudiation, immediate or delayed authentication, and Denial-of-Service (DoS) attack resilience. These are studied for various application scenarios. Our comparison table(s) are useful for decision-making on the most appropriate schemes that best satisfy specific application scenario requirements.

We came across the following two limited surveys on authentication mechanisms. The first is a survey on authentication mechanisms for wireless sensor networks [12] which mentions only five pre-shared key authentication and/or encryption schemes, but they neither consider authentication using digital signatures nor broadcast authentication. The second is a survey on vehicular authentication [13] which focused on IEEE 1609.2. They mainly discuss the security framework of vehicular adhoc networks (VANETs) using peer-to-peer schemes. Since the above papers discussed only a limited number of protocols and have not discussed broadcast authentication specifically, therefore, this is the first paper to have extensively surveyed broadcast authentication protocols for wireless networks.

The main contributions of this work are:

- Classification of broadcast authentication protocols based on their cryptographic building block.
- Comparison of broadcast authentication protocols.
- Analyses of current broadcast authentication schemes in different scenarios.
- Open research challenges or important issues in broadcast authentication.

The rest of the paper is organized in the following manner. Section 2 introduces the types of authentication in wireless networks and highlights the challenges of