Immediate Data Authentication for Multicast in Resource Constrained Network

C.K. Wong and Agnes Chan
Northeastern University, Boston MA 02115, USA
{ckwong,ahchan}@ccs.neu.edu

Abstract. In this paper, we consider the problem of authentication of multicast data. The TESLA scheme was introduced to provide data authentication for multicast communication over lossy channels. Later, TESLA was further improved to offer immediate authentication of packets and fortifications against denial-of-service attacks. The improved TESLA scheme is efficient and applicable to mobile resource-constrained receivers for authentication of multicast data. The resource limitation of mobile resource-constrained receivers gives additional challenges to multicast authentication. In this paper, a denial-of-service attack called the Random-Substitution attack is presented. We present a new scheme that can provide immediate packet authentication and deter the Random-Substitution attack. It is also robust against packet losses. In addition, the new scheme allows a receiver to immediately authenticate all packets upon arrival, when the receiver joins the multicast communication. Hence, the new scheme offers a practical multicast authentication solution for resource-constrained receivers.

1 Introduction

When a sender wants to simultaneously transmit a sequence of data packets to multiple receivers, multicast communication can be used. Multicast is an efficient means of communication and particularly well suited to applications such as audio and video streaming. Over the past decade, multicast communication has gained substantial attention among researchers. In an open environment such as the Internet, the communication channels generally cannot be assumed secure, and data received through insecure channels can be fabricated and altered. In unicast communication where sender and receiver share a unique secret key, message authentication code (MAC) provides an efficient means for verifying the authenticity and integrity of data. However, in multicast communication, the same common key is shared by all receivers. Any compromised receiver knowing the secret key can compute the MAC and impersonate the sender. Thus, the same approach cannot be directly applied to multicast communication.

A scheme called TESLA [3] has been proposed to provide data authentication for multicast communication over lossy channels. It is computationally efficient and is robust against packet losses. However, a drawback of TESLA is that packets cannot be immediately authenticated. Moreover, delayed packet authentication forces receivers to buffer incoming packets until they can be authenticated.
The buffering requirement introduces a vulnerability to denial-of-service attacks, as an adversary can flood bogus packets to buffer-limited receivers. An improved TESLA scheme [4] is proposed later, offering immediate packet authentication and fortifications against denial-of-service attacks.

The resource limitation of mobile resource-constrained receivers gives additional challenges to multicast authentication. In this paper, we present the Random-Substitution attack that wastes computation and storage resources of receivers. To guard against the Random-Substitution attack, we propose a new scheme that can provide immediate packet authentication and is robust against packet losses. Our new scheme is built on the improved TESLA scheme, using a different construction of hash values in order to deter the Random-Substitution attack. The design of our scheme assumes that data are stored and known to the sender in advance. Examples of such applications can be found in multimedia services for mobile users.

To provide a receiver the ability to immediately authenticate packets when the receiver joins the multicast communication, we introduce an additional hash value per packet. This additional field also provides a better sustainability of immediate authentication against packet losses.

The paper is organized as follows. In section 2, we give a review of the improved TESLA scheme. The Random-Substitution attack is presented in section 3. Next, we present the proposed scheme in section 4. The immunity of the proposed scheme to the Random-Substitution attack is discussed in section 5. Finally, we conclude the paper in section 6.

2 Review of the Improved TESLA Scheme

The original TESLA scheme [3] has drawbacks including delayed authentication of packets and vulnerabilities to denial-of-service attacks. Later, improvements to TESLA are proposed [4], offering immediate authentication of packets and fortifications against denial-of-service attacks. In this section, we review the improved TESLA scheme.

2.1 Overview

In the multicast communication model, there is a sender who multicasts messages $M_i$ to multiple receivers [3]. Each message $M_i$ is carried by a packet $P_i$. In each time interval, the sender may send zero or multiple packets. When a receiver receives a new packet $P_i$, the receiver will verify the authenticity and integrity of $P_i$. The first packet is authenticated via a digital scheme such as RSA [5] or DSA [6]. Each packet carries the hash value of the message of a future packet. Thus, if the current packet is authentic, then the hash value it carries is authentic and can be used to provide immediate authentication of a future packet.

The improved TESLA scheme can be described in four stages: sender setup, bootstrapping a new receiver, sending authenticated packets, and verifying received packets.