Available online at www.sciencedirect.com
SCIENCE DIRECT
Computer Communications 28 (2005) 726–740
computer communications
www.elsevier.com/locate/comcom

RLH: receiver driven layered hash-chaining for multicast data origin authentication

Yacine Challal*, Abdelmadjid Bouabdallah, Yoann Hinard

Computer Science Department, Heudiasyc Lab., Compiegne University of Technology, BP. 20529, Compiegne-Cedex 60205, France

Received 7 June 2004; revised 17 October 2004; accepted 26 October 2004
Available online 20 November 2004

Abstract

Securing the multicast communication model is a strategic requirement for effective deployment of large scale business multi-party applications (TV over Internet, Video-on-Demand (VoD), video-conferencing, interactive group games, …). One of the main issues in securing multicast communication is the *authentication service*; a keystone of every secure architecture. Even though several authentication mechanisms have existed so far, data origin authentication in multi-party communications remains a challenging problem in terms of scalability, efficiency and performance.

In this paper, we propose an efficient multicast data origin authentication protocol based on a novel layered hash-chaining scheme. Our protocol tolerates packet loss and guarantees non-repudiation of media-streaming origin. Furthermore, our protocol allows receivers to make the decision regarding the authentication information redundancy degree depending on the quality of reception in term of packet loss ratio. This novel technique allows to save bandwidth since the packet loss distribution over a large scale network is likely to be not uniform. We have simulated our protocol using NS-2, and the simulation results show that the protocol has remarkable features and efficiency compared to other recent data origin authentication protocols.

Keywords: Data origin authentication; Non-repudiation; Layered hash-chaining; Multicast streaming

1. Introduction

The lack of security obstructs the large scale deployment of multicast [10] communication applications, such as: TV over Internet, Video-on-Demand (VoD), video-conferencing, e-learning, database replication and interactive group games. One of the main issues in securing multicast communication is the *authentication service*; a keystone of every secure architecture. Even though several authentication mechanisms have existed so far, data origin authentication in multi-party communications remains a challenging problem in terms of scalability, efficiency and performance. Indeed, hashes [12,22,40], MACs [23], and digital signatures [37,41] are the cryptographic answers to integrity, authentication, and non-repudiation in data transmission. However, these mechanisms have been designed typically for point-to-point transmissions, and using them in multicasting yields inefficient and non-adequate solutions. This non-suitability of existing authentication mechanisms is mainly due to the number of group members which may be high in multi-party applications, and to the type of transmitted data which consists generally in continuous streaming of multicast messages with real-time transmission requirement.

In order to assure that a message originates from a valid group member, generally group members use a shared key. This key is commonly called, *group key*. Indeed, applying a MAC to a message with the *group key* assures that the message originates from a valid group member, since only valid group members are supposed to know the *group key*. Hence, the *group authentication* problem is reduced to the *group key management* and essentially to its scalability to large groups [8,19,20,38]. In contrast, *data origin*

* Corresponding author. Tel.: +33 3 44 23 44 23; fax: +33 3 44 23 44 77.
E-mail addresses: ychallal@hds.utc.fr (Y. Challal), bouabdal@hds.utc.fr (A. Bouabdallah), yhinard@hds.utc.fr (Y. Hinard).

0140-3664/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2004.10.009

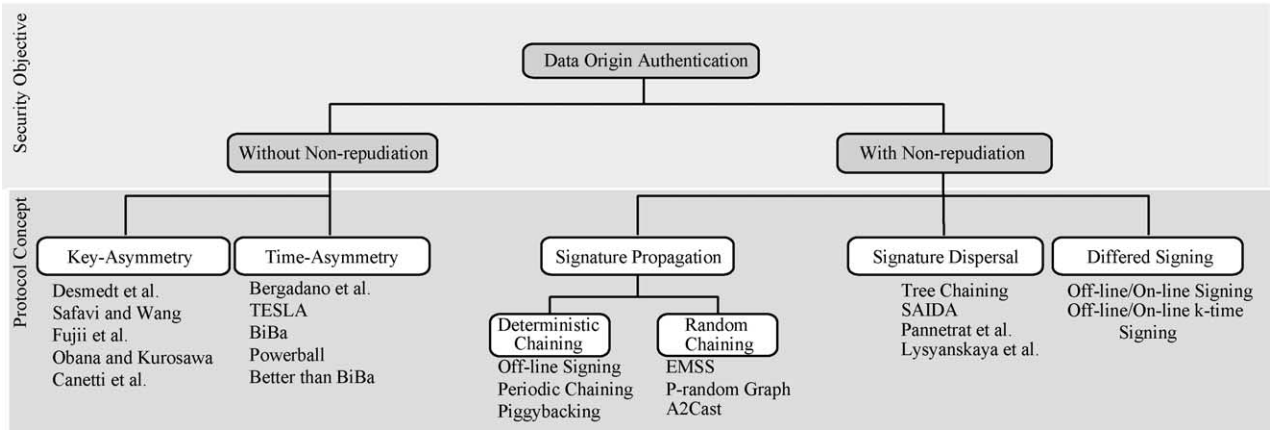

Fig. 1. Taxonomy of data origin authentication protocols in group communication.

authentication in multicasting is more complicated because the *group key* which is known by all group members cannot be used to identify a specific sender. Furthermore, to guarantee *non-repudiation* of the multicast data origin, the stream has to be *signed*. In order to avoid signing each packet of the multicast data stream, proposed solutions rely on the concept of *amortizing a single digital signature over multiple packets*. The signature and its amortization induces some *extra-information* called the *authentication information*. Besides, most of multicast media streaming applications do not use reliable transport layer. Hence, some packets may be lost in course of transmission. Therefore, the proposed solutions introduce *redundancy* in the *authentication information*, in a way that even if some packets are lost, the required authentication information can be recovered in order to verify received packets' authenticity. In this case, the *bandwidth overhead*, induced by the redundant authentication information, increases. Proposed solutions deal with how to trade bandwidth for tolerance to packet loss.

One problem with existing solutions is that they do not take into consideration the distribution of packet loss throughout a large scale network [49]. Indeed, in existing solutions, the source considers the *worst packet loss ratio* that receivers may encounter in the network and introduces the required authentication information redundancy degree to tolerate this *worst case*. This approach assures a high tolerance to packet loss but introduces extra authentication information overhead since it considers the worst case which is likely to appear only at some parts of the network.

In this paper, we propose an efficient multicast data origin authentication protocol based on a novel layered hash-chaining scheme. We called this protocol: *Receiver driven Layered Hash-chaining for multicast data origin authentication (RLH)*. This protocol tolerates packet loss and guarantees non-repudiation of media-streaming origin. Furthermore, *RLH* allows receivers to make the decision regarding the authentication information redundancy degree depending on the quality of reception in term of packet loss ratio. This novel technique allows to save bandwidth since the packet loss distribution over a large scale network is likely to be not uniform [49]. We have simulated our protocol using NS-2, and the simulation results show that the protocol has remarkable features and efficiency compared to other recent data origin authentication protocols.

In the following section, we give an overview of existing data origin authentication protocols for group communication, then we present some related works that use hash-chaining techniques to amortize signatures over a sequence of packets of a data-stream. In Section 4, we describe our protocol: *RLH*, then we evaluate and compare it with other protocols using NS-2 simulations.

2. Data origin authentication in group communication

Fig. 1 illustrates a classification of existing solutions for data origin authentication in group communication. In a first stage we classify them according to the security goal. Namely, we distinguish two sets of protocols: the protocols that aim to assure data origin authentication, and the protocols that aim to assure non-repudiation of the data origin. Then, we refine the classification depending on the technical concept underlying each subset of those protocols.

In what follows, we present briefly each category of the protocols depicted in Fig. 1.[1] In Section 3, we present with some details the protocols that fit into the same category of *RLH* protocol in order to ease its presentation in the subsequent sections.

2.1. Multicast data origin authentication

This security level guarantees *only* data origin authentication of the multicast source. In this case, a sender needs to

[1] Detailed descriptions of the protocols as well as comparisons and discussions can be found in [6].