An Hybrid Approach for Efficient Multicast Stream Authentication over Unsecured Channels

Christophe Tartary[1,2], Huaxiong Wang[1,3], and Josef Pieprzyk[3]

[1] Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University
Singapore
[2] Institute for Theoretical Computer Science
Tsinghua University
Beijing, 100084
P.R. China
[3] Centre for Advanced Computing - Algorithms and Cryptography
Department of Computing
Macquarie University
NSW 2109 Australia
{ctartary,josef}@ics.mq.edu.au,
HXWang@ntu.edu.sg

Abstract. We study the multicast stream authentication problem when an opponent can drop, reorder and inject data packets into the communication channel. In this context, bandwidth limitation and fast authentication are the core concerns. Therefore any authentication scheme is to reduce as much as possible the packet overhead and the time spent at the receiver to check the authenticity of collected elements. Recently, Tartary and Wang developed a provably secure protocol with small packet overhead and a reduced number of signature verifications to be performed at the receiver.

In this paper, we propose an hybrid scheme based on Tartary and Wang's approach and Merkle hash trees. Our construction will exhibit a smaller overhead and a much faster processing at the receiver making it even more suitable for multicast than the earlier approach. As Tartary and Wang's protocol, our construction is provably secure and allows the total recovery of the data stream despite erasures and injections occurred during transmission.

Keywords: Stream Authentication, Polynomial Reconstruction, Unsecured Channel, Merkle Hash Tree, Erasure Code.

1 Introduction

With the expansion of communication networks, broadcasting has become a major technology to distribute digital content from a single user to a large audience via a public communication channel such as the Internet for instance. Online games, military defense systems, satellite television and financial quotes are a few examples of multicast distribution of information. Nevertheless, in large-scale broadcasts, a lost piece of a data stream[1] could generate a flood of retransmission requests from the receivers that

[1] In broadcasting, the sequence of information sent into the network is called *stream*.

W. Susilo, J.K. Liu, and Y. Mu. (Eds.): ProvSec 2007, LNCS 4784, pp. 17–34, 2007.

congregate at the sender's side. Furthermore the network can be under the influence of malicious users performing illegal and damaging operations on the stream. As a consequence, the security of a multicast authentication protocol relies on the network properties and the opponents' computational power. Several unconditionally secure schemes have been developed [5, 9, 36] but either these are one-time protocols or they require too large storage capacities. In this work, we consider that adversaries have polynomially bounded computational abilities.

An application like a pay-TV channel broadcasting programs 24 hours a day and seven a week suggests that the stream can be considered as infinite. Nevertheless the receivers must be able to authenticate data within a short period of time upon reception. Since many protocols will distribute private or sensitive content, non-repudiation of the sender is required for most of them as using data from an uncertain origin can have disastrous consequences during military operations for instance. Unfortunately signing each data packet[2] is impractical as digital signatures are generally very expensive to generate and/or verify. Furthermore bandwidth limitations prevent one-time and k-time signatures [11, 35] from being used due to their large size. Boneh et al. constructed short signatures in [6] but their verification time is prohibitive to be a practical solution for authenticated broadcast [3, 37]. Thus a general approach is to generate a single signature and to amortize its computational cost and overhead over several data packets using a chain of hash functions for instance.

Several constructions relying on hash functions have been developed to deal with packet loss [12, 21, 31, 32]. A signature is generated from time to time and is always assumed to be received correctly. This provides authentication and non-repudiation of the sender and allows new receivers to join the communication group at any block[3] boundary. Using Markov chains [10, 30, 42] to model the network packet loss, the authors of the previous constructions determined bounds on the packet authentication probability. Unfortunately, the main issue in those schemes is the fact that they rely on the reliable reception of signature packets. Since networks like the Internet only provide a best effort delivery of data, the reliability requirement limits the area of applications of those constructions.

In order to overcome this issue, a general solution is to split the signature into k parts where only ℓ of them ($\ell < k$) are enough to guarantee the recovery of the whole signature. Many schemes have been developed using this idea [1, 26, 27, 28, 29] but none of them tolerates a single packet injection. Using a Merkle hash tree [20], Wong and Lam developed a construction dealing with both erasures and injections [41]. Nevertheless, it is vulnerable to denial of service attacks (DoS) against the computational resources of the receiver as each packet carries the block signature. Thus, in the worst case, the number of signature verifications to be performed per block of n packets is $\Theta(n)$. In [15], Karlof et al. overcame this problem by using Merkle hash trees as one-way accumulators [2, 4, 24, 25]. Their approach requires $O(1)$ signature verifications per block in any case and each augmented packet[4] has to carry $\lceil \log_2 n \rceil$ hashes which may be too

[2] Since the data stream is large, it is divided into fixed-size chunks called *packets*.

[3] In order to be processed, packets are gathered into fixed-size sets called *blocks*.

[4] We call *augmented packets* the elements sent into the network. They generally consist of the original data packets with some redundancy used to prove the authenticity of the element.