Jordan University of Science and Technology

Signing the First Packet in Amortization Scheme for Multicast Stream Authentication

Authors: Mohammed Shatnawi, Qusai Abuein, and Susumu Shibusawa

Abstract: Signature amortization schemes have been introduced for authenticating multicast streams, in which, a single signature is amortized over several packets. The hash value of each packet is computed, some hash values are appended to other packets, forming what is known as hash chain. These schemes divide the stream into blocks, each block is a number of packets, the signature packet in these schemes is either the first or the last packet of the block. Amortization schemes are efficient solutions in terms of computation and communication overhead, specially in real-time environment. The main effective factor of amortization schemes is it?s hash chain construction. Some studies show that signing the first packet of each block reduces the receiver?s delay and prevents DoS attacks, other studies show that signing the last packet reduces the sender?s delay. To our knowledge, there is no studies that show which is better, to sign the first or the last packet in terms of authentication probability and resistance to packet loss. In this paper we will introduce another scheme for authenticating multicast streams that is robust against packet loss, reduces the overhead, and prevents the DoS attacks experienced by the receiver in the same time. Our scheme-The Multiple Connected Chain signing the First packet (MCF) is to append the hash values of specific packets to other packets, then append some hashes to the signature packet which is sent as the first packet in the block. This scheme is especially efficient in terms of receiver?s delay. We discuss and evaluate the performance of our proposed scheme against those that sign the last packet of the block.