Abstract

Many issues concern with secure multicasting are confidentiality, authentication, non-repudiation and data integrity including access control. Group-oriented applications such as video-conferencing, broadcasting stock quotes, software distribution or audio/video transmission are made possible through multicasting as an efficient communication mechanism. The deployment of these kinds of efficient communication mechanism is hindered because of lack of security. These limitations kindle the research minds to contribute towards secure multicasting. Hash Tree Signature Scheme (HTSS) is a newly proposed mechanism for multicast authentication that aims at providing packet authentication along with data integrity, non-repudiation and protection against key exposure. The scheme follows asymmetric cryptographic approach using tree-chaining technique that implements the tree construction for key generation and signature amortization for secure packet transmission. Performance
evaluation is based on signing rate, providing non-repudiation and protection against key exposure. The HTSS is proposed in four different modes and its compatibility with the different issues in multicasting is discussed. The different modes discussed are sign-each, fixed delay, continuous and dynamic mode.

References

- B. Weis, "The use of RSA/SHA-1 signatures within encapsulating security payload (ESP) and authentication header (AH)," RFC 4359, Jan. 2006.
- Secure Hash Standard (SHS), NIST FIPS 180-2, 2004

**Index Terms**

Computer Science  
Emerging Trends in Technology

**Keywords**

Forward Security  Hash-tree  Multicast Authentication  Network Security  Signature  Amortization