Zhang, X. Brian; **Lam, Simon S.**; **Lee, Dong-Young**
Group rekeying with limited unicast recovery. (English) Zbl 1078.68007
Comput. Netw. 44, No. 6, 855-870 (2004).

Summary: In secure group communications, a key server can deliver a "group-oriented" rekey message to a large number of users efficiently using multicast. For reliable delivery, Keystone [*C. K. Wong* and *S. S. Lam*, "Keystone: A group key management system", Proc. Int. Conf. on Telecommunications, Acapulco, Mexico, May 2000] proposed the use of Forward Error Correction (FEC) in an initial multicast, followed by the use of unicast delivery for users that cannot recover their new keys from the multicast. In this paper, we investigate how to limit unicast recovery to a small fraction r of the user population. By specifying a very small r, almost all users in the group will receive their new keys within a single multicast round. We present analytic models for deriving r as a function of the amount of FEC redundant information (denoted by h) and the rekeying interval duration (denoted by T) for both Bernoulli and two-state Markov Chain loss models. From our analyses, we conclude that r decreases roughly at an exponential rate as h increases. We then present a protocol designed to adaptively adjust (h, T) to achieve a specified r. In particular, our protocol chooses from among all feasible (h, T) pairs one with h and T values close to their feasible minima. Our protocol also adapts to an increase in network traffic. Simulation results using ns-2 show that with network congestion our adaptive FEC protocol can still achieve a specified r by adjusting values of h and T.

MSC:

68M10 Network design and communication in computer systems
68M12 Network protocols

Keywords:

forward error correction; network traffic

Full Text: DOI