Enhancing the Scalability of Secure Wireless Multicast

V. Vasudevan[1] and R. Sukumar[2,*]

[1] Department of Information Technology
Arulmigu Kalasalingam College of Engineering
Krishnankovil, Virudhunagar District, Tamilnadu, India
[2]Sethu Institute of Technology,
Pulloor, Kariapatti – 626 106. Virudhunagar District, Tamil Nadu, India.
rsugum@yahoo.co.in

Received 13 July 2009; Revised 19 August 2009; Accepted 1 September 2009

Abstract. In this paper, we propose a multi server architecture that uses LKH and dynamic split and merge for group key management to improve the packet delivery ratio. The proposed system utilizes the dynamic split and merge with low overhead where a physical server adaptively splits and merges its traffic into multiple groups each served by a dedicated server so as to improve the packet delivery ratio. We compare the performance of this proposed approach with that of the single server case. Our results show that multi server architecture scales well as compared with the traditional approaches.

Keywords: Key management, logical key hierarchy, multicast bandwidth, scalability, wireless networks, group key controller.

References

[1] G. Chaddoud, I. Chrisment, A. Schaff, "Dynamic Group Communication Security," *Proceedings of Sixth IEEE Symposium on Computers and Communications (ISCC'01)*, pp. 49-56, 2001.

[2] H. Lu,"A Novel High-Order Tree for Secure Multicast Key Management," *IEEE Transactions on Computers*, Vol. 54, No. 2, pp. 214–224, 2005.

[3] R.D. Pietro, A. Durante, L.V. Mancini, "A Reliable Key Authentication Schema for Secure Multicast Communications," *IEEE Symposium on Security and Privacy*, pp. 56–73, 2003.

[4] H. Zhao and K.J. R. Liu, "A Secure Multicast Scheme for Anti-Collusion Fingerprinted Video," *Proceedings of IEEE Globecom*, Vol. 2, pp. 571-575, 2004.

[5] Mingyan Li, R. Poovendran, C. Berenstein, "Design of Secure Multicast Key Management Schemes with Communication Budget Constraint," *IEEE Communications Letters*, Vol. 6, No. 3, pp. 108-110, 2002.

[6] K.C. Chan and S.H.G. Chan, "Distributed Servers Approach for Large-Scale Secure Multicast," *IEEE Journal on Selected Areas in Communications*, Vol. 20, No. 8, pp. 1500-1510, 2002.

[7] L. R. Dondeti, A. Samal, S. Mukherjee, "A Dual Encryption Protocol for Scalable Secure Multicasting," *Proceedings of IEEE International Symposium on Computer and Communications*, pp. 2-8, 1999.

[8] W. Aye and M.U. Siddiqi, "A Key Distribution Scheme for Secure Multicast Over IPv6 Wireless Networks," *Proceedings of 6th Asia-Pacific Symposium on Information and Telecommunication Technologies*, *APSITT*, pp. 322–327, 2005.

* Correspondence author

[9] J. Zhang, V. Varadharajan, Y. Mu "A Novel Dynamic Key Management Scheme for Secure Multicasting," *Proceedings of ICON 2003*, Vol. 1, No. 28, pp. 391-395, 2003.

[10] B.H. Li, Y.B. Liou, Y.L. Zhao, "A Scalable Key Distribution Scheme for Secure Multicast," *Proceedings of 2004 International Conference on Machine Learning and Cybernetics,* Vol. 4, pp. 2532-2536, 2004.

[11] R. Shankaran, V. Varadharajan, M.Hitchens "A Secure Multicast Support Framework for Mobile IP," *Proceedings of Wireless Communications and Networking,* pp. 2114–2119, 2003.

[12] G. Kenny and U.K. Logicacmg, "A Demonstration of a Secure Multicast System for the Distribution of Video Content," *IEEE Seminar on IP over Satellite – The Next Generation: MPLS, VPN, and DRM Delivered Services*, pp. 63-83, 2003.

[13] I.Y.K. Pang and H.C.B. Chan, "A Hybrid Re-keying Mechanism for Supporting Secure Multicast of Multimedia Data over the Internet," *Proceedings of IEEE International Conference on Systems, Man, and Cybernetics*, Vol. 4, pp. 3110 – 3114, 2003.

[14] A Y. R. Yang, X. S. Li, X. B. Zhang, S. S. Lam, "Reliable Group Rekeying: A Performance Analysis," *Proceedings of the 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, pp. 27–38, 2001.

[15] K.C. Chan and S.H.G. Chan, "Distributed Server Networks for Secure Multicast," *Proceedings of IEEE Globecom '01*, San Antonio, TX, Vol. 3, pp. 1974-1978, 2001.