Scalable rekeying algorithm in IEEE 802.16e

Mohammad Mehdi Gilanian Sadeghi[a]; Borhanuddin Mohd Ali[a]; Maode Ma[b]; Jamalul-lail Ab Manan[c]; Nor Kamariah Noordin[a]; Sabira Khatun[d]

[a] Department of Computer and Communication Systems Engineering, Universiti Putra Malaysia, Malaysia msadeghi@ieee.org,{borhan, nknordin@eng.upm.edu.my} * Institute of Advanced Technology, Universiti Putra Malaysia, Malaysia

[b] School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore

[c] Advanced Analysis and Modeling (ADAM) Cluster, MIMOS Berhad, Malaysia, jamalul.lail@mimos.my

[d] Faculty of Computer Systems and Software Engineering, Universiti Malaysia Pahang, Malaysia, sabira@ump.edu.my

ABSTRACT

IEEE 802.16e standard provides wide coverage and high bandwidth for subscribers in a metropolitan area network. It introduces Multicast and Broadcast Rekeying Algorithm (MBRA) which is a multicasting scheme to communicate with many users concurrently. Although ELAPSE (for Efficient sub-Linear rekeying Algorithm with Perfect SEcrecy) improves on the deficiencies of MBRA, the algorithm poorly responds to scalability issue. This paper proposes a Scalable Rekeying Algorithm (SRA) based on a complete binary tree structure. SRA is introduced with linear linked list structure in order to make the system more scalable. Evaluation analysis shows that SRA manages to improve the scalability issue in MBRA for Mobile WiMAX.

KEYWORDS:

Rekeying algorithm; scalability; unicast; group key managemet

REFERENCES

1. "IEEE Std 802.16, IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Broadband Wireless Access Systems ", ed: IEEE Press, February 2004.

2. "IEEE Std 802.16, IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Broadband Wireless Access Systems and Revision of IEEE Std 802.16-2004," ed: IEEE Press, May 2009.

3. "IEEE Std 802.16e, IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Amendment and Corrigendum to IEEE Std 802.16-2004," ed: IEEE Press, February 2006

4. D. Johnston and J. Walker, "Overview of IEEE 802.16 Security," IEEE Security and Privacy, vol. 2, pp. 40-48, 2004.

5. S. Xu, C.-T. Huang, and M. M. Matthews, "Secure Multicast in WiMAX," Journal of Networks, vol. 3, pp. 48-57, 2008.