Abstract

Existing group key management scheme may not be applied effectively in Delay tolerant network where transmission between nodes (users) has the characteristics of irregular connectivity and long communication delay. In Previous proposed schemes, Group key is regenerated every time whenever new user joins or leave form the existing group, in order to maintain backward secrecy and forward secrecy and therefore the overhead to broadcast new group key to all member of group increases. In this proposed scheme which is based on Chinese remainder theorem constraint to broadcast new group key generated by server in case of user join as well as user leave is removed thus making the complexity constant in both scenario. Simulation is done in Opportunistic Networking Environment(ONE) Simulator and the result shows that Key update, Receiving success rate and key update success rate is better than Logical key Hierarchy LKH as well as Chinese remainder group key (CRGK) schemes.

References
1. R. S. Mangrulkar "Design and Development of Delay Tolerant Network: A Case Study" Nirma University International Conference on Engineering (NUiCONE) IEEE 2012
3. Sofia Anna Menesidou and Vasilios Katos "Authenticated Key Exchange (AKE) in Delay Tolerant Networks" Springer Berlin Heidelberg 2012
9. Xinliang Zheng, Chin-tser Huang "Chinese Remainder Theorem Based Group Key Management" citeseer 2007

Index Terms

Computer Science
Networks

Keywords

Delay tolerant network; Group key management; Chinese Remainder Theorem; Logical Key Hierarchy; Opportunistic Networking Environment; Modified Chinese remainder group key.