Abstract

Key management is equally important as compared to any other security measure such as encryption and authentication. With the growing usage of mobile devices and the advent of multicast communication, there has been a significant amount of work carried out in developing an optimum group key management protocol for mobile multicast systems. Key management is widely being adopted in securing group communication for both wired and wireless networks. Securing group communication over wired networks is fairly well established; however, wireless networks bring additional challenges due to member mobility and increase in the number of members. This paper presents a comprehensive survey of group key management protocols in wireless mobile environments that employ multicast communication. They are classified into network dependent and independent protocols and further categorized into tree-based and cluster-based key management protocols. The survey clearly outlines the characteristics of each protocol along with highlighting their advantages and limitations with respect to real-world systems. The paper is concluded with a taxonomy of the individual protocols with respect to the defined requirements which provides a strong source of literature reference for researchers in this field.
Group Key Management Protocols for Secure Mobile Multicast Communication: A Comprehensive Survey

- S. Gharout, A. Bouabdallah, M. Kellil, and Y. Challal, "Key management with host mobility in dynamic groups," presented at the Proceedings of the 3rd international conference on Security of information and networks, Taganrog, Rostov-on-Don, Russian

Index Terms

Computer Science  Communications

Keywords

Mobile multicast  security  group key management  wireless network