A wireless network is a type of network where various physical devices (e.g., computer, laptops, PDAs etc) are interconnected with each other using network infrastructure. Owing to wireless medium of data communication, the security risk is potentially high for unauthorized access and intrusion of various malicious programs. The security protocols of wireless network are governed by family of IEEE 802.11 standards. Wireless Network is studied in research with respect to wireless LAN (Local Area Network), wireless mesh network, wireless sensor network, mobile adhoc network, etc. In recent times, wireless sensor network was on constant focus among the research community owing to its potential advantage of data collection in remote areas as well as security problems associated with it. Wireless Sensor Network (WSN) consists of various sensor motes that form a cluster and perform data aggregation. Usually, the aggregated data is forwarded from the sensor nodes to the base station, which then reaches to user for analysis. The security problems is a matter of concern even for wireless sensor network that aims for either compromising the routing protocols or invoke illegitimate access to resources by bypassing the security protocols. In a wireless sensor network, the communication takes place by group based, where sensor nodes are deployed in groups and each group performs communication using keys. Therefore this paper reviews some of the potential key-management techniques in past for maintaining group based communication and
extracts the research gap.

References

Communications and Networking

Index Terms

Computer Science

Wireless

Keywords

Application Dependent Sensor Network, Key Management, Security, WSN