Abstract

Mobile Ad hoc Networks (MANETs) are subject to various kinds of attacks. Deploying security mechanisms is difficult due to inherent properties of ad hoc networks, such as the high dynamics of their topology, restricted bandwidth, and limited resources in end devices. With such dynamism in connectivity and limited resources it is not possible to deploy centralized security solution. Like many distributed systems, security in ad hoc networks widely relies on the use of key management mechanisms. However, traditional key management systems are not appropriate for them. This work aims at providing a secure and distributed authentication service in ad hoc networks. A trusted and secured clustered protocol in MANET, where clusters are formed based on highly-trusted nodes having sufficient energy is proposed. Secured communication with public key authentication service based on trust model and network model to prevent nodes from obtaining false public keys of the others when there are malicious nodes in the network is organized. Efforts to present energy efficient, secure and trusted clustering to enhance the security assurance and significant adaptation of trustworthy communication is
presented. Simulation results demonstrate that proposed routing protocols can improve the energy efficiency, packet delivery ratio and route stability.

References


15. T. Ghosh, N. Pissinou, and K. Makki, “Collaborative trust-based secure routing in


Index Terms

Computer Science Networks

Keywords

MANET, Trust, Key management, Cluster