ACCESS CONTROL MODELS FOR MOBILE AD HOC NETWORKS

Soumya Maity

Abstract

Restricting unauthorized accesses on the network resources is a major concern for the enterprises that employ mobile ad hoc networks (MANET) for their operations. The deployment of mobile ad hoc networks (MANETs) in several security-critical organizations (such as, military and defence networks) emphasizes a need for enforcing appropriate security policies to control unauthorized accesses on the network resources. Policy-based security infrastructure is more complex in MANET due to uncontrolled media access and absence of network perimeters, mobility of the nodes and their varying trustworthiness. Thus the security technologies (firewall, IDS etc.) which are used in traditional networks are unable to meet the security requirements of MANET. Moreover, absence of any network perimeter in MANET demands the policies to be applied in a distributed manner, taking into account the mobility of nodes. This work presents a security access control mechanism that can handle the need for enforcing appropriate security policies to control the unauthorized accesses of the network resources and ensures proper and secure forwarding of data. Attribute based access control modelling of the policies, specifications and implementations of policy rules and a proper trust-based model for distribution and enforcement of the policy rules are the research challenges that have been addressed in the work. The effectiveness, robustness and scalability of the proposed framework has been demonstrated through experimental studies and formal verification. The conciliation of the policy rules for heterogeneous MANET has been also presented in this work. The access control framework is extended for heterogeneous MANET resulting it to be a viable solution for any type of MANET that is used in practice.