50152 Maqsood Razi

Seniority Bared Secure Distributed Authentication Service in Ad Hoc Wireless Networks.

Abstract

Mobile ad hoc networking offers convenient infrastructure less communication over the shared wireless channel. However, the nature of ad hoc networks makes them vulnerable to security attacks, and implementation of public key infrastructure in ad hoc network is also a difficult task due to lack of centralized control and fixed infrastructure. Therefore, a centralized or hierarchical network security solution does not work well.

This work proposes scalable, distributed authentication services in ad hoc networks. The proposed model provides a secure distributed authentication service in ad hoc wire less network in which multiple senior nodes belonging to a more reliable group collaboratively provide authentication services for other nodes in the network. The work first formalizes a seniority based trust model that lays the foundation for the design of a simple mechanism of authentication that is collaboratively performed by multiple senior nodes. In this seniority based trust model, an entity is trusted if any k trusted available senior entities claim so within a certain time period T. These k entities are typically among the entities of the senior group. Once a node is trusted by its senior group, it is globally accepted as a trusted node. Otherwise, if the seniors distrust an entity then it is regarded as untrustworthy in the entire network. This trusted model is an improved form of localized trust model proposed in [8]. This new model provides a more reliable group to implement Public Key Infrastructure in ad hoc wireless network and to authenticate a node as a trusted node.

I also propose a seniority based certification services by implementing the seniority based trust model, and design a Pretty Good Privacy (PGP) type security solution which is unique, simple and more reliable and secure than other similar existing solutions. The paper also presents a design of Threshold Cryptography based security solution in which I applied Seniority based Trust model instead of a localized trust model [8,23] to improve the security of authentication mechanism (Public Key Infrastructure Service) proposed in the model.

This document presents a security architecture utilizing the seniority based trust model. It contains a design of a security framework for implementing Public Key Infrastructure in ad hoc wireless network through Pretty Good Privacy type solution and Threshold Cryptography based solution. Related algorithms are also presented.