Abstract

Wireless LAN, in the current state of the world, has become ubiquitous. Therefore it is imperative to safeguard this technology, which otherwise could prove disastrous. Compromised WLANs, have the potential to leave the user susceptible to a plethora of unfavorable situations. In the following paper it is attempted to make wireless networks more easily secure by addressing one of the more commonly exploited technique of Rogue Access Points. This problem is tackled by articulating a method by which clients can recognize Access points to which they have previously connected. After a standard authentication procedure a packet exchange mechanism is used buttressed by a host of algorithms, selected randomly from an algorithm pool, which are run on selected packages on the client as well as the Access Point in order to completely obviate the possibility of a client connecting to a Rogue Access Point.

Index Terms

Computer Science
Networks

Keywords