Abstract

With increasing numbers of corporate and organizations deploying wireless network and allowing the company personnel to access the internet or the wired backbone through wireless access points are increasingly getting exposed to hacking attacks. Due to easy hacking tools and less concerns about the security threats of the deployed, various crucial data of the private network is hacked. One of the important forms of a security loophole in the wireless network is accidental association. In this paper we propose a novel technique to secure the wireless signal to prevent accidental association. Layer 2 of each device is assigned with a unique time bound key and non time bound primary key. As soon as a new device is detected in the proximity by any node, it requests for the time independent primary key from the device. If the device fails to respond with the key then the network connection is withdrawn with immediate effect after the node propagates an alert message encrypted with time bound session key through which it is communicating securely with other wireless peers. A periodic search for
checking new devices which may get associated with the existing network accidently is avoided with utmost efficiency. The protocol is tested with Omnet++ simulator and results shows that the proposed technique performs much better than basic protection against such an attack offered by WEP.

References


Index Terms

Computer Science

Keywords
WEP  Accidental Association  Wireless Network Security  Dual Key Protection Scheme