Abstract

Wireless network suffers from security threats which are of different nature. One of the most significant reasons for weak security of the wireless network is the lack of strong key exchange technique. In 802.11 adaptation of wireless protocol, generally end users selects the key for current session and exchange encrypted data with same key for extended period of time. As the basic keys are weak, it is highly vulnerable to attacks and the packets are easy to intrude/read/modify. In this work we propose a unique solution of generating a strong key fingerprint automatically from the device of the user and use the same as key. We consider file transmission security between an AP and STA where the STA is a mobile node. We demonstrate the effectiveness of the technique with the help of real time setup and by synthesizing attacks like MAC address duplicating, using duplicate SIM and packet injection. The system is tested with 800MB of data transmission under different scenario and has yielded a zero hacking success of the data. As the system does not require any special hardware or
A Unique Wireless Device Fingerprinting Technique for Secured Data Communication in Wireless Network

software for implementing the same, it is easy to adopt and is acceptably scalable.

References

- Shan Kang; Naiwen Chen; Mi Yan; Xiaoxiao Chen; "Detecting identity-spoof attack based on BP network in cognitive radio network," in: Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC), 2011.

Index Terms

Computer Science

Wireless Communications
Keywords
Packet Injection  Mac Spoofing  Wireless Device Finger Printing