Abstract

Wireless LAN is one of the cost effective way to establish local networking as compared to wired network. Although the last decade has seen various sophisticated WLAN routers and devices, but few of them are actually found to be highly resilient against potential attacks on WLAN. Literatures also share evidence that such issues are yet unsolved and call for a serious modeling of issues and testing the security efficiencies. The prime reason behind this is the incapability of the existing security protocols to ensure reliable authentication system. Hence, this study presents a technique that uses the most recent versions of cryptographic hash functions to ensure the bidirectional authentication between the nodes and WLAN router. Finally, the paper discusses about mathematical modeling of the presented security protocol as well as accomplished results are compared with the existing system.

References

SAKGP: Secure Authentication Key Generation Protocol in WLAN

- N. Phil, A. P. Horrocks, "Vulnerability of IEEE802.11 WLANs to MAC layer DoS attacks", pp. 14-14, 2004
- http://keccak noekeon.org/
- X. Zheng, C. Chen, C-T Huang, A Dual Authentication Protocol for IEEE 802.11 Wireless LANs, pp. 565-569, IEEE, 2005

Index Terms

Computer Science Wireless

Keywords

Wireless LAN Cryptographic Hash Security Authentication IEEE 802.11