Abstract

The 802.11 standard defines the Wired Equivalent Privacy (WEP) and encapsulation of data frames. It is intended to provide data privacy to the level of a wired network. WEP suffered threat of attacks from hackers owing to certain security shortcomings in the WEP protocol. Lately, many new protocols like WiFi Protected Access (WPA), WPA2, Robust Secure Network (RSN) and 802.11i have come into being, yet their implementation is fairly limited. Despite its shortcomings one cannot undermine the importance of WEP as it still remains the most widely used system and we chose to address certain security issues and propose some modifications to make it more secure. In this paper we have proposed a modification to the existing WEP protocol to make it more secure. We achieve Message Privacy by ensuring that the encryption is not breached. The proposed enhancements attempt to rectify the vulnerabilities to enhance the WEP with Private IV and Session Time for improved authentication process. In the proposed algorithm we can use all possible 224 different IVs without making them predictable for an attacker, eliminates the IV collision ensuring Message Privacy that further strengthens security of the existing WEP.
Design of Multithreaded Security Algorithm using Session Keys to Secure Initialization Vector(IV) for Enhancing the Wireless Protocol WEP

- “An Examination of Security Algorithm flaws in Wireless Networks”, University of Maryland,, OCT 2004
- J. Edney and W.A. Arbaugh, “Real 802.11 Security Wi-Fi Protected Access and 802.11i”, 2004, Pearson Education Inc.

Index Terms

Computer Science Network Security

Key words

Wireless networks security Session Time
Design of Multithreaded Security Algorithm using Session Keys to Secure Initialization Vector (IV) for Enhancing the Wireless Protocol WEP

IV

WEP