Wired equivalent privacy reinvestigated

Amar Kumar Mohapatra [*]
IGIT, GGSIP University
Kashmere Gate, Delhi 110 006
India

Nupur Prakash [†]
USIT, GGSIP University
Kashmere Gate, Delhi 110 006
India

Abstract

Security is a strong requirement for effective deployment of business wireless communication applications. Therefore, many proposals dealt with security holes in *Wired Equivalent Privacy protocol* (WEP). In this paper, we analyze WEP security holes and we propose an improvement over WEP which achieves its security goals. Our premise is to permit deploying an efficient security mechanism on wireless networks. We introduce an efficient way by using shared session keys as the seed to the RC4 stream cipher. The shared session key can be calculated at the sender's and the receiver's end simultaneously by using the Triple Formula. The solution calculates the key without transmitting any part of it in open air unlike IV vector which eliminates the possibility of a key leak. Security analysis shows that the proposed scheme is strong against some well known attacks like Key Reuse, Authentication forging, Denial of Service, Brute force and Known plain text attack.

Keywords : *IV vector, pythagorean triple, WEP, RC4.*

I. Introduction

With the rapid adoption of WLANs in enterprises and personal networks, securing WLAN, shielding them from intruders, is the need of the time. Most secure technologies have been breached and hackers have wreaked havoc over the entire networks [1]. Essentially, it is required to protect and fortify the Wi-Fi systems in order to use wireless technology as

[*] *E-mail*: `mohapatra.amar@gmail.com`

[†] *E-mail*: `nupurprakash@rediffmail.com`

Journal of Discrete Mathematical Sciences & Cryptography
Vol. 13 (2010), No. 2, pp. 141–151