C

EVALUATION AND ENHANCEMENT OF WEAKNESSES OF THE IEEE 802.11b WEP PROTOCOL WITH DYNAMIC KEY

A PROJECT REPORT PRESENTED BY

R. P. IDAMEKORALA

to the Board of Study in Statistics and Computer Science of the

POSTGRADUATE INSITUTE OF SCIENCE

in partial fulfilment of the requirement

for the award of the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

of the

UNIVERSITY OF PERADENIYA

SRI LANKA

2009

University of Peradeniya
06 NOV 2010
Library

635219

EVALUATION AND ENHANCEMENT OF WEAKNESSES OF THE IEEE 802.11b WEP PROTOCOL WITH DYNAMIC KEY

R. P. Idamekorala

Post Graduate institute of Science

University of Peradeniya

Peradeniya

Sri Lanka

Wireless technology enables one or more devices to communicate with each other without requiring cables. Wireless Local Area Networks (WLAN) are based on the IEEE 802.11 standard which is first developed in 1997. It uses radio frequency transmission where as wired technology uses cables. This air-borne nature of WLANs opens the door to intruders and hackers to attack the WLAN from any direction. Hence security is very important. This report only concern the security flaw of the IEEE 802.11b standard.

In 802.11b uses Wired Equivalence Privacy (WEP) protocol to provide the same security for WLANs as the wired networks. Unfortunately 802.11b WLAN are suffering from active and passive attacks. This is mainly due to the repetition of the key stream used for encryption. There are methods proposed by various researchers where the additional server has been introduced to stop the repetition of key stream. Some proposed methods have weakness of consuming more bandwidth.
This report tries to introduce such short comings in the WEP protocol and propose solutions to same. The proposed protocol as the solution to the problems in WEP uses a dynamic key instead of the static shared key in conventional WEP algorithm