SCHOOL OF ENGINEERING

WIRELESS LOCAL AREA NETWORK SECURITY

FINAL REPORT

STUDENT'S NAME	: NEELESHWAREN CHANDIRAN
STUDENT'S ID	: 99207886
MAJOR	: B. ENG. (HONS) COMMUNICATION & ELECTRONICS ENGINEERING
FIRST SUPERVISOR	: MS. RUZITA BINTI ABU BAKAR
SECOND SUPERVISOR	: ASSOCIATE PROF. LACHMAN TARACHAND
PROJECT'S COORDINATOR	: DR . KHEDR M . M . ABOHASSAN

JANUARY – AUGUST 2005

Abstract

Wireless networking technology is quickly changing the way networked computers communicate. The convenience offered by the ability to connect to networks using mobile computing devices has also introduced many security issues that do not exist in the wired world. The security measures we have relied on in the past to secure our networks are now obsolete with this new technology. Wireless Local Area Network (WLAN) are indeed very useful, but the encryption and authentication methods specified in the 802.11 standard are flawed, leading to serious security issues.

This report introduces the 802.11 standard and the security issues surrounding it. As an alternative solution, the commonly used WLAN antennas are studied and simulated using SUPERNEC (electromagnetic simulation software). Based on the results, a secured network can be designed by selecting appropriate antenna and positioning in such a way that signal access is minimised towards the user working area only, thus avoiding unauthorised interception of signal. Modelling of coverage in WLAN is done based on few models to estimate the range of the antenna theoretically.