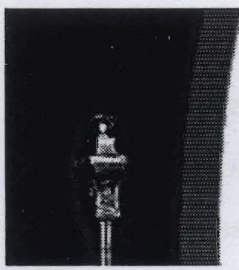


SPECIAL USE
LIBRARY USE ONLY

Abstract



National University of Science and Technology

Think in Other Terms



FACULTY OF APPLIED SCIENCES DEPARTMENT OF COMPUTER SCIENCE

ROGUE ACCESS POINT DETECTOR

BY

CHIDO MARUFU

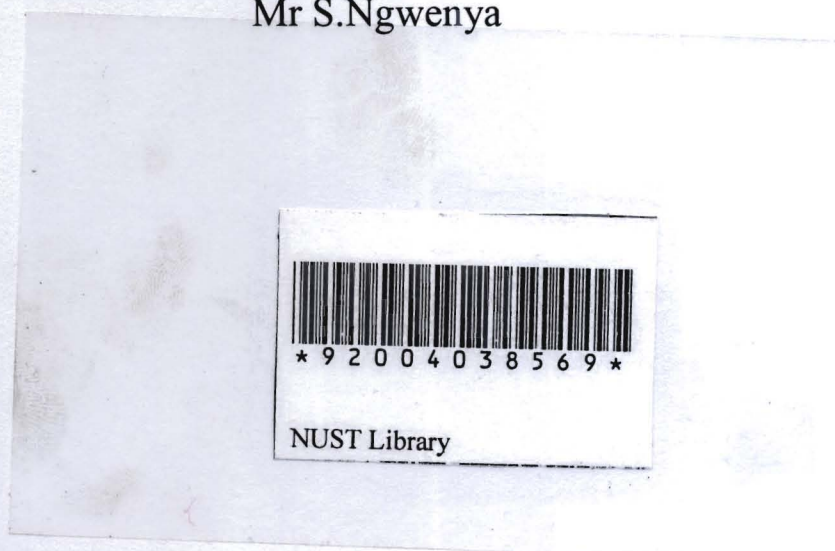
Reg.Number:

N0111207A

Supervisor:

Mr S.Ngwenya

LIBRARY NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY P.O. BOX 346 BULAWAYO ZIMBABWE		
DATE	ACCESSION	CLASS No
11/05/16	SC 15/863	



Research Project submitted to National University of Science and Technology Computer Science Department in partial fulfilment for the Bachelor of Science (Hons) Degree in Computer Science
2014-2015

Abstract

The diversity introduced by the advent of different kinds of machines has increased the need for human beings to remain connected. However, mobile connectivity has also introduced further vulnerabilities associated with the use of wireless technology. The use of wireless devices to access corporate network resources is now normal within corporate environments. The Internet is overflowing with applications that are capable of performing packet sniffing. A combination of these applications installed on a machine and the capability of the machine to be configured as an access point can present a Rogue Access Point (RAP). An intruder can sniff the Service Set Identifier (SSID) of the organisation and then deploy a RAP with the same SSID and unsuspecting employees will connect via a Rogue Access Point. Access Points advertise their availability using SSIDs. In this research we propose a solution which blocks the rogue access point. Deauthentication can be used to defend against Rogue Access Point. Methodologies used are Rational Unified Process and the build methodology. Tools used are the Netbeans IDE, connectify and My Wifi router. The results showed that this method can be used to block rogue access points in a network.