الآيـــــة

بسم الله الرحمن الرحيم

((وما أوتيتم من العلم إلا قليلا))

صدق الله العظيم

سورة الإسراء-الآية(85)

الإهـــداء

إلى أسرتي التي كانت عوناً وسنداً لي دائماً

لم حفظهم الله إلى كل من علمني حرفاً وأنار لي الطريق إلى الع والمعرفة

إليهم جميعاً أهدي هذا الجهد المتواضع

شكـــر وتقديـــر

من حق النعمة الذكر وأقل جزاء للمعروف الشكر

ل جدر بي أن أتقدم ببالغ الإمتنان وجزيوجل يـ فبعد حممد الله عز العرفان إلى كل من وجهني وعلمني وأخص بذلك المشرف على هذا تابع البحث الأستاذ الدكتور / إبراهيم خضر الطاهر الذي قوم وصوب و بحسن إرشاده في كل مراحل البحث فله كل التقدير والعرفان

ABSTRACT

Cognitive Radio (CR) Network is an advanced growing technique and promising technology for the upcoming generation of the wireless networks in order to efficiently utilize the limited spectrum resources and satisfy the rapidly increasing demand for wireless applications and services. Deployment of such networks is hindered by the vulnerabilities that these network are

exposed to , this thesis focus on security problems arising from Primary User Emulation (PUE) attack in CR network . The thesis presents a comprehensive introduction to cognitive radio network and the primary user emulation attacks and its impact on CR network. The thesis focus on design a security model using Matlab software and use the Neyman-Pearson Composite Hypothesis Test NPCHT to obtain the hypothesis test and detect the PUE attack . In order to secure CR networks against PUE attacks , the system considered the power received at the secondary receiver. Simulation resulte proved that using the NPCHT it is possible to keep the probability of success of PUE attack low depends on the threshold value. The number of malicious users in the system can significantly increase the probability of false alarm (successful PUE attack) in the network.

المســـــتخلص

جيال الحديثة من الشبكة الراديوية المعرفية هي تقنية نامية ومتقدمة وتعتبر تقنية واعدة للأ سي وتلبية الشبكات اللاسلكية من أجل تحقيق إستخدام كفؤ لموارد الطيف الكهرومغناطي الإحتياج المتنامي للتطبيقات اللاسلكية والخدمات .

الشبكات إنتشار هذه الشبكات يواجه معوقات نتيجة لنقاط الضعف التي تؤثر على هذه، يقة محاكاة ة التي تنشأ نتيجة مهاجمة الشبكة بطرهذا البحث يركز على المشكلات الأمني المستخدم الرئيسي في الشبكات الراديوية المعرفية .

م إختيار يركز هذا البحث على تصميم نموذج أمني بإستخدام برنامج المات لاب وإستخدا لمهاجمة نايمن بيرسون الإفتراضي المركب للحصول على إفتراضات ومن ثم كشف ا اة المستخدم الرئيسيبطريقة محاك .

ي المركب فاءنه نتائج برنامج المحاكاة أثبتت أنه بإستخدام إختبار نايمن بيرسون الإفتراض مة عتبه من الممكن المحافظة على إحتمالية أقل لنجاح حدوث مهاجمة لشبكات بناء على قي المهاجمة ةمعينة وأن عدد المهاجمين في النظام يزيد بصورة كبيرة إحتمالية حدوث عملي للشبكة بطريقة محاكاه المستخدم الرئيسي في الشبكة.

CONTENTS

LIST of TABLES

LIST of FIGURES

ABBREVIATION

CR	Cognitive Radio
PUE	Primary User Emulation
QoS	Quality of Service
DoS	Denial of Service
WRAN	Wireless Regional Area Network
TV	Television
PHY	Physical Layer
MAC	Medium Access Control
FCC	Federal Communication Commission
TVWS	Television White Space

SNR	Signal to Noise Ratio
SSL	Secure Socket Layer
TLS	Transport Layer Security
IEEE	Institute of Electrical and Electronics Engineers
DRT	Distance Ratio Test
RSS	Received Signal Strength
DDT	Distance Difference Test
LV	Location Verifiers
PU	Primary User
SU	Secondary User
EMS	Electromagnetic Signature
RF	Radio Frequency
Pdf	Probability Density Function
NPCHT	Neyman Composite Hypothesis Test