

الآية

بسم الله الرحمن الرحيم

((وما أوتيتم من العلم إلا قليلا))

صدق الله العظيم

سورة الإسراء- الآية (85)

الإهداء

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

شكر وتقدير

من حق النعمة الذكر وأقل جزاء للمعروف الشكر

ل جدر بي أن أتقدم ببالغ الإمتنان وجزئوجل ي 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 results 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.

المسـ تخلص

جـيال الحديثـة من الشبـكة الراديوية المعرفية هي تقنية نامية ومتقدمة وتعتبر تقنية واعدة للأسي وتلبية الشبكات اللاسلكية من أجل تحقيق إستخدام كفؤ لموارد الطيف الكهرومغناطيسي . الإحتياج المتنامي للتطبيقات اللاسلكية والخدمات

الشبكات إنتشار هذه الشبكات يواجه معوقات نتيجة لنقاط الضعف التي تؤثر على هذه،
 يقة محاكاة التي تنشأ نتيجة مهاجمة الشبكة بطر هذا 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
 .ة المستخدم الرئيسي بطريقة محاك

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

CONTENTS

SUBJECT	PAGE NO
الآية	1
الإهداء	11
الشكر والتقدير	111
ABSTRACT	IV
المستخلص	V
Contents	VI
List of Table	VIII
List of Figures	IX

Abbreviation	X
Chapter One	1
Introduction	1
1.1 Preface	1
1.2 Problem Statement	1
1.3 Objectives	2
1.4 Methodology	2
1.5 Thesis Scope	3
1.6 Thesis Outline	3
Chapter Two	4
Literature Review	4
2.1 Introduction	4
2.2 Cognitive Radio technology	5
2,3 TV White Space	18
2.4 Security Issues in Cognitive Radio	18
2.5 Security at Different Layer	21
2.6 Primary User Emulation (PUE) Attack	25
2.7 Related Works	30
Chapter Three	50
System Model	50
3.1 Model Description	50
3.2 Model Analysis	52
Chapter Four	55
Results and Analysis	55

4.1 Introduction	55
4.2 System Parameters for Simulation	55
4.3 Probability Density Function Using Simulation and Mathematically	56
4.4 Case One of System Design	57
4.5 Case Two of System Design	60
Chapter Five	65
Conclusion and Future Work	65
5.1 Conclusion	65
5.2 Future Work	65
5.3 References	66
Appendix A	70
Appendix B	72
Appendix C	75

LIST of TABLES

TABLE NO	PAGE NO
Table (4-1) : System Parameters	55-56
Table (4-2) : Case one probabilities values	59-60
Table (4-3) : Case tow probabilities values	61-62

LIST of FIGURES

FIGURE NO	PAGE NO
Figure (2-1) : Radio Frequency Allocation in US	5
Figure (2-2) : Spectrum Utilization	5
Figure (2-3) : Architecture for CR Network	9
Figure (2-4) : A power spectral density snapshot	9
Figure (2-5) : Classification of Spectrum Sensing Techniques	13
Figure (2-6) : Classification of spectrum sharing in xG networks	16
Figure (2-7) : Inter-network Spectrum Sharing	17
Figure (2-8) : White Spaces in the Spectrum	18

Figure (2-9) : PUE Attack	25
Figure (3-1) : Cognitive Radio Network Model	50
Figure (4-1) : PDF of the received power due to the primary transmitter	56
Figure (4-2) : PDF of the received power due to the malicious users	57
Figure (4-3) : Probability of false alarm (successful PUE attack)	58
Figure (4-4) : Probability of miss detection	59
Figure (4-5) : probability of false alarm (successful PUE attack)	60
Figure (4-6) : Probability of miss detection	61
Figure (4-7) : False alarm Probability Vs. network radius R	63
Figure (4-8) : CDF of False alarm and miss detection probabilities	64

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