Sudan University of Science and Technology
College of Graduate Studies
Faculty of Computer Science and Information Technology

Design of new Confident, Secure and Mutual Authentication Protocol for TV White Space Database

A thesis submitted in fulfillment of the
Requirements for the award of the degree of
Doctor of Philosophy in Computer Sciences

تصميم بروتوكول جديد آمن وموثوق للاستخدام في قاعدة بيانات الموجات التلفزيونية غيرالمستخدمة

بحث مقدم لنيل درجة الدكتوراه في علوم الحاسوب

Student
Mubark Mohamed Ahmed Elmubark

Supervision Dr. Rashid A Saed

Co- supervision Dr. Mohamed A Elshikh

October 2015

Verse

(وَقُل رَّبِّ زِدْنِي عِلْمًا)

الاية 114 - سورةـ طهـ

ABSTRACT

Due to moving from analog TV transmission to digital transmission, there will be free frequencies called TV White Space (TVWS). These frequencies can be reused in broadband communication without the interference with the incumbent and the licenses users. TVWS can be licensed by auction or freely unlicensed, which is preferred by many parties around the world. TVWS unlicensed can use cognitive radio (CR) techniques for sharing the spectrum. Many standards agreed two ways for spectrum sharing, either by spectrum sensing and/or spectrum database. Many researches and standard efforts has been given to TVWS techniques and other related issues like security, frequency allocation, interference, database management, throughput, etc. This thesis concentrated on security issues in spectrum database access specially the authentication.

To avoid the denial of service attack (DOS) and misused of the available channels like the interference, the authentication and key management had become one of the most important security issues to access the TVWS database. So, in this study a new confident and mutual authentication protocol is designed for TVWS database, which introduce new method for key generation and key distribution in a secure manner.

In general, the database security works in the application layer and IEEE802 security works on physical layer, so the user must use two protocol to authenticate themselves with the Database server. The proposed protocol takes the advantages of the available database security and the IEEE.802 security to modify IEEE802.22 Wireless Regional Area Networks (WRAN) standard protocol to generate one protocol which can authenticate the entire link between the user and the database server.

The key management is an integrated process for the authentication protocol and it includes generate and exchange a shared secrete key to encrypt and decrypt the transferring data between the database server and the users. Key management suffers from three problems, first problem is the sender and the receiver send an information (data) which the attacker can use it to

get the key, the second problem is the time to generate this key is very long, and the third one when the attackers get the key, they can generate a new key after the available key life time is expired. This protocol designs and implements a new method to generate either on key or a number of keys and exchange them to overcome these problems.

The proposed protocol has been evaluated in terms of security functionality and the performance. The simulation results show that this protocol is more secure and faster than the available protocols.

المستخلص

نظرا لانتقال البث التلفزيوني الى النظام الرقمي للبث فانه سيكون هنالك موجات/ ترددات شاغرة تسمى ترددات التلفزيون الخاية/ الغير مستخدمة. هذه الترددات يمكن اعادة استخدامها في الاتصالات. ويمكن عمل رخص لاستخدامها او استخدامها بدون تراخيص مسبقة وهذه هي الطريقة المفضلة لدي الغالبية حول العالم. ويتم استخدام هذه الترددات بالمشاركة نسبة لان كميتها ستكون محدودة مع تحقق شرط اساسي هو عدم التشويش على الاموجات الاساسية للتلفزيون وكذلك الموجات المرخص لها.

الاتجاه المتعارف عليه للحصول على هذه الترددات اما بارسال اشارة للبحث عن الموجة الخالية واستخدامها (Cognitive Radio) او عمل قاعدة بيانات للتحكم في الاستخدام الكثير من البحوث العلمية الآن اصبحت تهتم بدراسة هذه الموجات والمواضيع ذات الصلة بها مثل السرية وامكانية توفر هذه الموجات وتفادي التشويش في البث وادارة قواعد البيانات الخاصة بها وغيرها من المواضيع. وهذا البحث يهتم بدراسة السرية في قواعد البيانات وخصوصا التحقق من هوية المستخدمين.

حتى يتم تجنب الاستخدام السيء او الغير قانوني لهذه الموجات الذي قد يتسبب في عمل تشويش للموجات وايضا انكار الخدمات الموجودة (denial of service attack) فانه اصبح من الاهمية بمكان التحقق من هوية المستخدمين لهذه الموجات. ايضا يجب ان يكون هنالك مفاتيح لتشفير وفك التشفير للبيانات المرسلة اثناء الاتصال. وهذه المفاتيح يجب انشاءها وتبادلها بصورة سرية وآمنه وهو احد المواضيع التي اصبحت من مرتكزات استخدام قواعد البيانات.

للموجات الخالية/ الحرة. لنا في هنه الدراسة تم تصميم بروتكول يتم من خلاله التاكد من هوية طرفي الاتصال (المرسل/ المستقبل) وتمكينهم من انشاء وتبادل مفاتيح التشفير بصورة سرية.

بشكل عام فان السرية في قواعد البيانات يتم تطبيقها في طبقة التطبيقات العليا (Applications layer) والسرية في IEEE يتم تطبيقها في الطبقة الفيزيائية (Physical layer) وعليه فان المستخدم ومدير قاعدة البيانات يكونا بحاجة لاثنين من البروتوكولات - احدهما لقواعد البيانات والاخر للشبكات - من اجل التأكد من هوية بعضهما البعض وعليه فان البروتوكول المقترح لستفاد من وجود قواعد البيانات وقام بالتعديل على بروتوكول IEEE 802.22 لعمل بروتكول واحد يستطيع من خلاله كل من المستخدم وقاعدة البيانات التحقق من هوية الآخر.

لما مشكلة انشاء وتبادل مفاتيح التشفير فان الاساليب المستخدمة حاليا تعاني من ثلاث مشاكل. المشكلة الاولى انه يتم لرسال معلومات من خلال الشبكة هنه المعلومات لها علاقة بتوليد المفتاح. المشكلة الثانية انه اذا لستطاع المهاجمين لشتقاق المفتاح او الحصول عليه يكون باستطاعتهم انشاء مفاتيح جديدة عندما تنتهى صلاحية المفتاح المستخدم حاليا. المشكلة الثالثة والاخيرة هي ان عملية توليد المفاتيح تستغرق زمنا طويلا.

هنا البروتوكول الجديد يوفر لمكانية لتوليد مفتاح واحد او عدة مفاتيح في آن واحد وفي نفس الوقت تفادي المشاكل السابقة النكر. هنا البروتكول تم تقييمه من ناحية السرية والاداء وكانت نتائج المحاكاة تدل على ان هنا البروتوكول اكثر سرية واسرع من البروتكولات الحالية.

DEDICATION

I dedicate my dissertation work to my family and many friends. A special feeling of gratitude to my loving parents, whose words of encouragement and push for tenacity ring in my ears. My brother Mohamed and my sisters Salma, have never left my side and are very special. I also dedicate this dissertation to my many friends and my family who have supported me throughout the process. I will always appreciate all they have done, especially their advices and supports. I dedicate this work and give special thanks to my best friend Abdualrahman Abas and my wonderful kids for being there for me throughout the entire doctorate program.

Finally, this thesis is dedicated to all those who believe in the richness of learning.

ACKNLOGEMENT

First of all, I am grateful to the God for the good health and wellbeing that were necessary to complete this research.

I wish to express my sincere thanks to my supervisor Dr Rashid A Saed, for providing me with all the necessary facilities for the research.

I place on record, my sincere thank you to the Co-supervisor Dr Mohamed A Elshikh, for the continuous advices and help.

I am also grateful to my brother Mohamed, I am extremely thankful and indebted to him for sharing expertise, and sincere and valuable guidance and encouragement extended to me.

I take this opportunity to express gratitude to all of the department faculty members for their help and support. I also thank my parents for the unceasing encouragement, support and attention. I am also grateful to my colleague in group one PHD students, their supported me through this venture.

I also place on record, my sense of gratitude to one and all, who directly or indirectly, have lent their hand in this venture.

TABLE OF CONTENT

List of Tables

List of Figures

List of Abbreviations

AAA	Authentication Authorization and Accounting
AK	Authorizations Key
AP	Access Points
AH	Authentication Header
AKM	Authentication Key Management
AVISPA	**A**utomated **V**alidation of **I**nternet **S**ecurity **P**rotocols and **A**pplications.
BS	Base Station
BPSK	Binary Phase-Shift Keying
BSS	Basic Service Set
CDH	Curve Diffie-Hellman
CPE	Customer Premise Equipment
CR	Cognitive Radio
CSP	Communicating Sequential Processes
CA	Certificate Authorities
CVS	Contact Verification Signal
CPM	Channel Power Management
CAQ	Channel Availability Query
CSM	Channel Schedule Management
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CL-ATSE	Constraint Logic Attack Searcher
DAC	Discretionary Access Control
DOS	Denial of Service
DSE	Dynamic Station Enablement
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Protocol
ECA	Enhanced Certificate-based Authentication scheme
ESP	Encapsulated Security Payload
ECC	Elliptic Curve Cryptography
EMBGK	Energy and Mobility Based Group Key
EIT	Enterprise Integration Technologies
ESA	Extended Service Area
FDR	Failures-Divergences Refinement
FIA	Fast Initial Authentication
FCC	Federal Communications Commission
GDB	Geolocation Database
GDD	Geolocation Database Dependent
HIP	Host Identity Protocol

HLPSL	High-Level Protocol Specification Language
HTTP	Hypertext Transfer Protocol
IEK	Internet Key Exchange
IETF	Internet Engineering Task Force
IF	Intermediate Format
IV	Initialization Vector
KEK	Key Encryption Key
MAC	Mandatory Access Control
MAN	Metropolitan Area Network
MIC	Message Integrity Check
MMP_key	Management Message Protection Key
MN	Mobile Nodes
OFMC	On-the Fly Model Checker
PAWS	Protocol Access White Space
PDU	Protocol Data Units
PKI	Primary Key Identification
PKM	Privacy Key Management
PKM	Privacy Key Management
PS-LTL	Pure-past Security - Linear Temporal Logic
PNRG	Pseudorandom Number Generator
OFDM	Orthogonal Frequency Division Multiplexing
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase-Shift Keying
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RLSS	Registered Location Secure Server
RLQP	Registered Location Query Protocol
RSNA	Robust Security Network Associations
SA	Security Associations
SCM	Security Control Management
SET	Secure Electronic Transactions
SOM	Self-Organizing Maps
SSID	Service Set Identifier
SSL	Secure Sockets Layer
STT	Secure Transaction Technology
TA4SP	Tree Automata based automatic approximations for the analysis of Security Protocols
TEK	Traffic Encryption Key

TDM	Time Division Multiplex
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TVWSDB	TV White Space Database
WEP	Wired Equivalent Privacy
WIMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Networks
WPA	Wireless Protocol Access
WPAN	Wireless Personal Area Network
WSD	White Space Devices
WSM	White Space Map
VPN	Virtual Private Network
UE	User Equipment

List of Appendices