ISSN 2047-3338

New Methods for TVWS Database Protocol

Mubark A. Elmubark, Rashid A. Saeed, Mohamed Awad Elshikh and Rania A. Mokhtar
Blue Nile University and Sudan University of Science and Technology (SUST), Sudan
mubarkElmubark@gmail.com

Abstract– **In this paper, we study the authentication in the IEEE protocols (802.11-802.X1-802.11i- 802.16e – 802.22) and show the weakness and the problems that will arise when we use them and what efforts are done to overcome these problems. And also we analyze the database authentication. We find that IEEE 802.22 is the best protocol to use in the TVWS, because it is defined as the first wireless protocol for cognitive radio in WRAN. Finally, we explain the new idea to enhance this protocol to be more suitable in TVWS database authentication. This paper introduces new integrated security framework that ensures closing the gap between security sublayer at lower layers and upper layers at session layer and above. The new protocol is supported with all recommended functions from various standards.**

Index Terms– **IEEE Standard, Security, Protocol and Geolocation Database**

I. INTRODUCTION

THERE are two types of TVWS access, sensing by using cognitive radio and geolocation database. Wireless technology is nowadays on high demand and this makes it hard to secure the communications, and so the geolocation database has become the best way of accessing the free channels. The database is used to store user's data and all the available channels and the information related to these channels such as frequencies, interference and authorizations. The database security is becoming an increasingly important especially the authentication and the authorization to protect the data against so many types of attackers, like spoofing and Denial of Service (DOS) attackers.

The rest of the paper is organized as follows: Section II literature review specifies the security uses in the IEEE standards such as (802.11, 802.x1, 802.16e, 802.22), IETF and PAW protocol. Section III discusses the problems which arise when using these protocols in TVWS and explain why IEEE 802.22 is the best one explains our new idea and the proposed protocol for TVWS. In Section IV, we conclude by introducing our new idea about the protocol we need to design and use in TVWS database.

II. LITERATURE REVIEW

A) IEEE 802.11 [WEP Security]

Wired Equivalent Privacy (WEP) was an encryption algorithm designed to provide wireless security for users implementing 802.11 wireless networks. WEP was developed by a group of volunteer IEEE members. The intention was to offer security through an 802.11 wireless network while the wireless data was transmitted from one end point to another over radio waves. WEP was used to protect wireless communication from eavesdropping (confidentiality), prevent unauthorized access to a wireless network (access control) and prevent tampering with transmitted messages (data integrity) WEP uses the RC4 stream cipher, combining a 40-bit WEP key with a 24-bit random number known as an Initialization Vector (IV) to encrypt the data. The sender XORs the stream ciphers with the actual data to produce cipher text. The packet, combined with the IV with the cipher text, is sent to the receiver. The receiver decrypts the packet using the stored WEP key and the attached IV [1]. Unfortunately, the encryption protocol had not been subjected to a significant amount of peer review before release. Serious security flaws were present in the protocol. Although the application of WEP may stop casual sniffers, experienced hackers can crack the WEP keys in a busy network within 15 minutes. In general, WEP was considered as a broken protocol. The vulnerability of WEP can be attributed to the following:

i). *WEP key recovery*– WEP uses the same WEP key and a different IV to encrypt data. The IV has only a limited range (0 to 16777215) to choose from. Eventually, the same IVs may be used over and over again. By picking the repeating IVs out of the data stream, an attacker can ultimately have enough collection of data to crack the WEP key.

ii). *Unauthorized decryption and the violation of data integrit* – Once the WEP key is revealed, a hacker may transform the ciphertext into its original form and understand the meaning of the data. Based on the understanding of the algorithm, a hacker may use the cracked WEP key to modify the ciphertext and forward the changed message to the receiver.

iii). *Poor key management*– A proper WEP key is typed into a wireless device associated in a wireless network to enable the WEP. Unfortunately, there are no mechanisms to renew the stored WEP key. Once the WEP key is compromised, for example, an employee leaves a company; the key has to be changed in order to remain the security. The change of keys may be applicable in a home or small business environment. However, in an enterprise environment with thousands wireless mobile devices associated with the wireless network, the use of this method is almost impossible.

iv). *No access point authentication*– WEP only provides a method for network interface cards (NICs) to authenticate access points. There is no way for access points to authenticate the NICs. As a result, it is possible for a hacker to reroute the data to access points through an alternate unauthorized path.

B) Custom solutions to WEP

The customer solutions were in three ways. Firstly by extended extend the WEP key from 40-bit to 104-bit so the attackers might take longer amount of time to break the key. Secondly by using dynamic WEP key to prevented attackers from eavesdropping the communications. Lastly by The implementation of VPNs and enable remote devices to establish a secure connection to access points.

P. Bachan and Brahmjit Singh [16] investigated a physical layer technique for enhancing authentication in a time-variant wireless environment. And using EAP-TLS protocol instead of WEP.

C) Responses from the 802.11 working group

In order to address WEP security issues, the 802.11 working group adopted the 802.1X standard for authentication, authorization and key management. At the same time, IEEE formed a Task Group “I” to develop 802.11i standard, with a purpose to produce a detailed specification to enhance the security features for wireless LANs dramatically.

D) Wi-Fi Protected Access (WPA)

The Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of wireless local area network products based on IEEE 802.11 specification [1].

The Wi-Fi Protected Access (WPA) is a standards-based interoperable security specification. Its purpose is to increase the level of security for existing and future wireless LANs in three manners. The first way by implements 802.1X EAP based authentication to enforce mutual authentication. Secondly by Apply Temporal Key Integrity Protocol (TKIP) on existing RC4 WEP to impose strong data encryption. And the last way by Use Michael Message Integrity Check for message integrity WPA is an interim security solution that targets on all known WEP vulnerabilities.

IEEE 802.1X [PNAC]

The IEEE 802.1X standard defines a mechanism for port-based network access control to provide compatible authentication and authorization mechanisms for devices interconnected by various 802 LANs. It could also be used to distribute security keys for 802.11 WLANs by enabling public key authentication and encryption between access points (APs) and mobile nodes (MNs). In 802.1X, the *port* represents the association between MN and AP. There are three main components in the 802.1X authentication system: *supplicant*, *authenticator*, and *authentication server* (AS). A supplicant is usually an MN requesting WLAN access. An authenticator represents the network access server (NAS). In 802.11 networks it is normally an AP. A RADIUS server is commonly used as the authentication server, although other types of AAA servers such as Diameter could also serve as the authentication server. In 802.11, the authentication server might be physically integrated into an AP.

IEEE 802.1X Framework

As indicated in Fig. 1 [3], both supplicant and authenticator have a port access entity (PAE) that operates the algorithms and protocols associated with the authentication mechanisms. The authenticator PAE controls the authorized/unauthorized state of its controlled port depending on the outcome of the authentication processes.

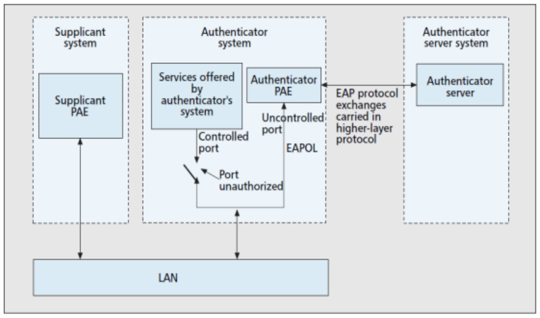


Fig. 1: IEEE 802.1X framework

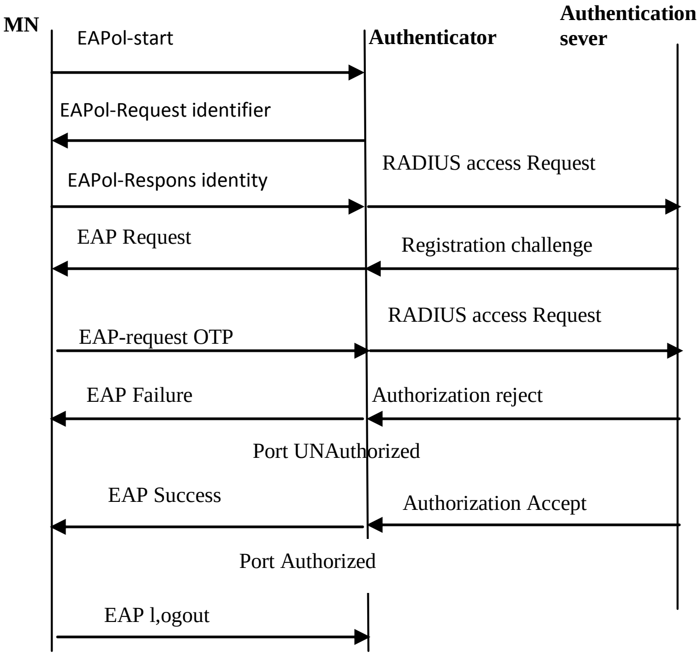


Fig. 2: Depicts a typical 802.1X message exchange with both the supplicant PAE and authenticator PAE state transitions

Before the supplicant is authenticated, the authenticator uses an uncontrolled port to communicate with the supplicant PAE. The authenticator will block all traffic except 802.1X messages before the supplicant is authenticated. The 802.1X standard leverages Extensible Authentication Protocol (EAP, IETF RFC 2284) to provide a number of authentication schemes, including (MD5, TLS, TTLS) [4], (PEAP) [5], EAP SIMs [6]. 802.1X also defines EAP over LANs (EAPOL) that encapsulates EAP messages between the supplicant and authenticator. EAP messages from the supplicant are relayed to the authentication server by the authenticator PAE. In order to let the RADIUS server authenticate users using EAP, the authenticator PAE encapsulates the same EAP messages in RADIUS packet format and sends them to the RADIUS server, assuming it has been adopted as the authentication server. The encapsulation is known as RADIUS-encapsulated EAP with the EAP-Message attribute, which is defined in RADIUS Extensions (IETF RFC 2869) for supporting EAP within RADIUS. If the authentication is failed the port will stay unauthorized. Once the supplicant is authenticated successfully, the controlled port in the authenticator is authorized. Packets from the supplicant will now go through the controlled port of the authenticator to backend networks to acquire the necessary services. Fig. 2 depicts a typical 802.1X message exchange with both the supplicant PAE and authenticator PAE state transitions. It also displays the authentication process.

The controlled port is thus still unauthorized. If the MN is authenticated and wants to perform a logoff procedure from the current AP, the MN originates an EAPOL-Logoff packet to the AP. After that, the controlled port of the current AP transits to unauthorized state immediately. The supplicant and authenticator will transit to the LOGOFF state and DISCONNECTED state, respectively.

IEEE 802.1X with Diameter

Usage of Diameter in an 802.1X system is similar to that of RADIUS. The major difference is in the replacement of RADIUS messages with Diameter messages. For intersubnet roaming, Diameter also specifies a Mobile IPv4 application [8].

IEEE 802.11i-2004 [WPA2]

The IEEE 802.11 Working Group has been working on MAC enhancement for several years. In May 2001, the MAC enhancement was split into different task groups. Task Group E (TGe) is responsible for quality of service (QoS). Task Group I (TGi) is working on security.

One of the major missions of 802.11 TGi is to define a robust security network (RSN). The definition of an RSN according to IEEE 802.11i draft [2] is *a security network that only allows the creation of robust security network associations* (RSNAs). That is, in an RSN the associations between all stations including APs are built on a strong association/authentication called an RSNA, which is also defined by the 802.11 TGi as: *an RSNA depends on 802.1X to transport its authentication services and deliver key management services*. A security association is defined as *the context providing the state (cryptographic keys, counters, sequence spaces, etc.) needed for correct operation of the IEEE 802.11 cipher suites*. RSNA includes a novel *four-way handshake* mechanism to provide robust session key management. By leveraging IEEE 802.1X, the four-way handshake, and the enhanced cryptographic algorithms, communication links in 802.11 wireless are securely protected.

THE IEEE 802.11i FRAMEWORK

The IEEE 802.11i standard provides authentication and security at the Medium Access Control layer in wireless local area networks (WLANs). It involves an authentication process followed by a four-way handshake to evolve a key for securing data sessions. The standard suffers under denial-of-service (DoS) attacks. These attacks often block the ongoing communication process and deprive services to the legitimate users. These are easy to conduct while maintaining anonymity of the attackers.

It hence becomes imperative to learn about the attacks and their solutions in IEEE 802.11i-protected WLANs so that future research proposals and solutions to mitigate the attack may develop [15].

Authentication Enhancement

In the original 802.11 standard, a station should first associate with an 802.11 AP. It then is able to access the WLAN service. An example of the process is shown by flows 1–6 in Fig. 3. After finding an AP by receiving the Probe Response, the mobile station needs to proceed to the following two steps: 802.11 entity authentication and association. Before associating with an AP, the station needs to accomplish 802.11 entity authentications [1].

As discussed earlier, there are two authentication schemes: open system and shared key authentication. Open system authentication allows a station to be authenticated without having a correct WEP key. There are two message exchanges. The first message sending from supplicant (mobile station) to authenticator (AP) is used to expose the identity of the station. Based on the identity, the authentication result is sent from the authenticator back to the station. There is no authentication algorithm.

In shared key authentication, there are four message exchanges. The first message containing the identity of the station is delivered from the station to the AP. The AP will then send a challenge packet to the mobile station. The mobile station is required to encrypt the challenge packet using the shared WEP key and send the encrypted result back to the AP. If the challenge packet is encrypted correctly, the supplicant is authenticated successfully. The authentication result is sent to the station in the fourth message.

If the station is authenticated successfully, it proceeds to the 802.11 association. The mobile station should transmit an Association Request to the AP. The AP then sends back an Association Response to the station.

Shared key authentication in 802.11 is not adopted by 802.11i. Instead, it incorporates 802.1X as the authentication solution for the RSN. As depicted in Fig. 3, 802.1X is performed after 802.11 open system authentication and association. IEEE 802.1X provides a port-based network access control mechanism to protect against unauthorized access. Details of 802.1X have been discussed.

Please note that Fig. 3 depicts the establishment of an RSN. The two message exchanges of flows 3 and 4 for open system authentication should not be replaced by the four message exchanges of shared key authentication.

IEEE 802.11i also specifies a more robust security framework utilizing 802.1X, a four-way handshake, and a group key handshake to authenticate and authorize stations. The fourway and group key handshakes are described in the next section. After the station is authenticated successfully, the cryptographic keys are configured as well. The station is thus able to send and receive unicast and broadcast frames in a secure manner. Moreover, IEEE 802.11i also supports pre-authentication.

A station could preauthenticate with an AP before roaming. A station could initiate an EAPOL-Start message through the serving AP to inform the new AP to start the IEEE 802.1X authentication, thus reducing handoff latency the four way handshake

Group key handshake (is optional): The RSNA also defines a group key handshake that enables the authenticator to deliver the group transient key (GTK) to the supplicant so that the supplicant can receive roadcast messages. Like the fourway handshake, the messages exchanged in the group *four-way handshake*, the key handshake also use the EAPOL-Key format. Figure 3 depicts the message flows of the group key handshake. As indicated in Fig. 3, the group key handshake is performed after the four-way handshake. In Fig. 4 we showed the flow chart of the improved 8021.11i which presented in 6 stages. Fig. 4 shows these stages.

IEEE 802.16- IEEE 802.16e (WIMAX)

IEEE 802.16, [1] the standard for constructing Wireless Metropolitan Area Networks (WMANs), was originally developed to address the "last mile" problem. Until recently, most of the wireless industry and its users mistakenly believed that the standard's major security weakness was its use of 56-bit Data Encryption Standard (DES). In fact, the key size is one of the standard's most insignificant security weaknesses [2].

Media access control and physical layers

Each of the four main modes of the IEEE 802.16 physical layer (PHY) offers significant flexibility. This flexibility allows operation across a wide range of spectrum allocations, including variations in channel bandwidth, frequency division duplex, and time division duplex. However, all modes support a common feature set, including initial ranging, registration, bandwidth requests, and connection-oriented channels for management and user data. IEEE 802.16 security protocols are the same, regardless of PHY type [2]. And also uses the same sequences in authentication procedure.

Network entry

Each SS want to enter the network it must precede with a sequence of actions:

1. The SS scans for a suitable BS downlink signal, which it uses to establish channel parameters.
2. Initial ranging allows the SS to set PHY Parameters correctly and establish the primary management channel with the BS. This channel is used for capability negotiation, authorization, and key management.
3. The privacy and key management (PKM) protocol authorizes the SS to the BS.
4. The SS registers by sending a request message to the BS. The BS's response assigns a connection ID for a secondary management connection.
5. The SS and BS create transport connections using a MAC_create_connection request. A request to create a dynamic transport connection indicates whether MAC-level encryption is required [2].

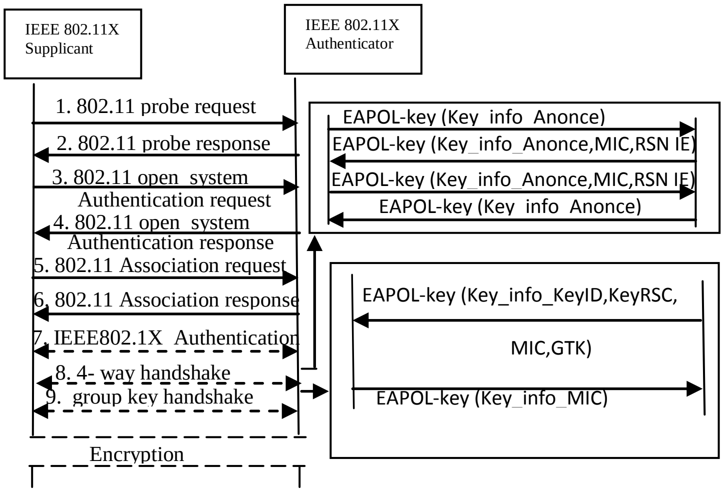

IEEE 802.11X Supplicant
IEEE 802.11X Authenticator
1. 802.11 probe request
2. 802.11 probe response
3. 802.11 open system Authentication request
4. 802.11 open system Authentication response
5. 802.11 Association request
6. 802.11 Association response
7. IEEE802.1X Authentication
8. 4- way handshake
9. group key handshake
Encryption
EAPOL-key (Key info Anonce)
EAPOL-key (Key_info_Anonce,MIC,RSN IE)
EAPOL-key (Key_info_Anonce,MIC,RSN IE)
EAPOL-key (Key info Anonce)
EAPOL-key (Key_info_KeyID,KeyRSC,
MIC,GTK)
EAPOL-key (Key_info_MIC)

Fig. 3: IEEE 802.11i enhancement

Security Algorithms

IEEE 802.16 security is implemented as a privacy sublayer at the bottom of the MAC protocol's internal layering. Its goal is to provide access control and confidentiality of the data link. The IEEE 802.16 security architecture uses five components, described in the following subsections.

Security associations: Security associations (SAs) maintain the security state relevant to connection. IEEE 802.16 uses two SA types but explicitly defines only the data SA, which protects transport connections between one or more SSs and a BS [2].

X.509 certificate profile: X.509 certificates identify communicating parties.

PKM authorization: The PKM authorization protocol distributes an authorization token to an authorized SS. The authorization protocol consists of a three-message exchange between a subscriber station SS and a base station BS. SS initiates the protocol by sending the first two messages, and BS responds with the third message.

Privacy and key management: A PKM protocol instance establishes a data SA between BS and SS.

The PKM protocol consists of a two- or three-message exchange between SS and BS to handle the key management.

Encryption: DES-CBC encryption, operating over the payload field, enciphers a plaintext MPDU, but not the MPDU GMH or the CRC.

The most striking thing about the IEEE 802.16 design is its failure to explicitly define the authorization SA, meaning it never receives the same attention data SAs receive.

Threats against data SAs apply directly to the authorization SA, so this failure will likely lead to problems.

The other problem is this authorization protocol subjects the SS to replay attacks, because it is single way authentication protocol (SS cannot authorize BS) and this will led to so many problems like reply attack and DOS problems. The solution was to design the mutual authentication protocol which was IEEE 802.16e. (WIMAX) to allow the SS to authenticate the BS by using any types of EAP protocol.

EAP Authentication

Task group e considered two options for the EAP-based authentication method. The first uses IEEE 802.1X to transport EAP messages. The task group rejected this option because IEEE 802.1X encodes EAP messages as data frames, which assumes that a fully operational data link exists– an untrue assumption for any wireless medium prior to link establishment. The second approach encodes EAP messages directly into IEEE 802.16 management frames. This approach permits authentication during link establishment. IEEE 802.16e introduces two additional PKM messages to transport EAP: PKM-EAPREQ and PKM-EAP-RSP.

IEEE 802.16e does not define the authentication method used, and EAP methods to support the needs of wireless networking security are still a research area. However, designers are beginning to articulate generally accepted requirements.

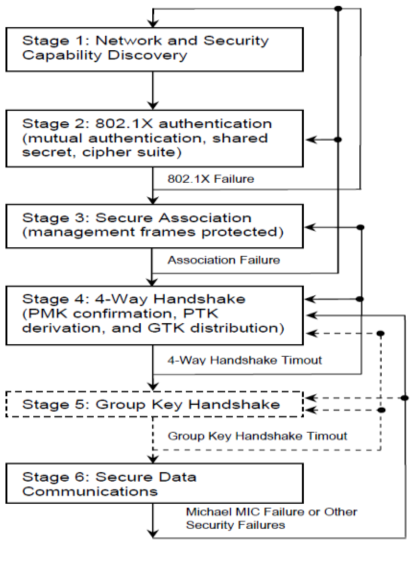

Stage 1: Network and Security Capability Discovery
Stage 2: 802.1X authentication (mutual authentication, shared secret, cipher suite)
802.1X Failure
Stage 3: Secure Association (management frames protected)
Association Failure
Stage 4: 4-Way Handshake (PMK confirmation, PTK derivation, and GTK distribution)
4-Way Handshake Timout
Stage 5: Group Key Handshake
Group Key Handshake Timout
Stage 6: Secure Data Communications
Michael MIC Failure or Other Security Failures

Fig. 4: A flow chart of the improved 8021.11i

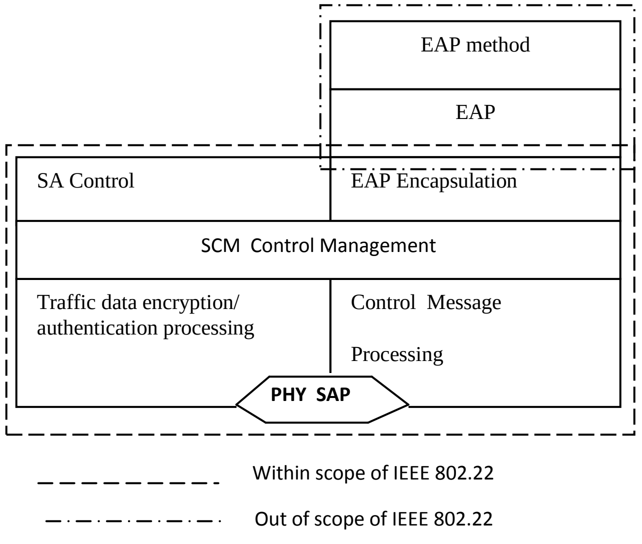
IETF PAWS Protocol

Internet Engineering Task Force (IETF) is developing a WG called Protocol to Access White Space database (PAWS) with the goal of defining the device-database interface for TVWS database systems. Devices may be able to connect to the database directly or indirectly via the Internet or private IP networks. This interface needs to be: radio/air interface agnostic (802.11af, 802.16, 802.22, LTE etc) PAWS pretends to specify both a database identification mechanism (how can a device know what database it has to connect to) and contents of the queries and responses (XML is an option). This protocol did not state any type of authentication procedure but just state that "This messaging between the device and the database needs to be secure (authentication, integrity of the content, prevent from man-in-the-middle attacks etc.), requiring some authentication and security measures" [3].

IEEE 802.22 (WRAN)

IEEE 802.22 is defined as the first wireless protocol for cognitive radio in wireless regional area network (WRAN). The security sublayer defined in 802.22 provides confidentiality, authentication, and data integrity services by applying cryptographic transformations to MAC data units carried across connections between CPEs and the BS. The security sublayer has two components: an encapsulation protocol and a Privacy Key Management (PKM) protocol. The encapsulation protocol defines a set of supported cryptographic suites (i.e., pairings of data encryption and authentication algorithms) and the rules for applying those algorithms to a MPDU payload. The PKM protocol ensures the secure distribution of keying material from the BS to the CPEs. The security sublayer protects network control information by attaching message authentication codes to CMAC management messages [5].

All CPEs attempting access to the network shall be authenticated. If the authentication exchange is successfully completed, the BS shall consider the CPE to be authenticated, and proceed to authorize the CPE to access the network. If the authentication exchange is not successfully completed, the BS


EAP method
EAP
SA Control
EAP Encapsulation
SCM Control Management
Traffic data encryption/ authentication processing
Control Message Processing
PHY SAP
Within scope of IEEE 802.22
Out of scope of IEEE 802.22

— SCM Control Management: This stack controls all security components. Various keys are derived and generated in this stack.
— Traffic Data Processing: This stack encrypts or decrypts the traffic data and executes the authentication function for the traffic data.
— Control Message Processing: This stack processes the various SCM-related MAC messages, and provides either authentication and/or encryption of such messages

Fig. 5: The security components of the components of the IEEE 802.22

shall deny the CPE access to the network. In this case, the CPE may attempt access on one of the other WRAN services it detected during initialization. If during authentication exchange, the CPE specifies that it does not support IEEE 802.22 security for protection of user data, then after successful completion of authentication, the key exchange used to setup protection of user data shall be skipped [1].

Security Architecture for the Data/Control and Management Planes

Privacy has two component protocols as follows:

i) An encapsulation protocol for securing packet data over the air. This protocol defines a set of supported *cryptographic suites*, i.e., pairings of data encryption and authentication algorithms, and the rules for applying those algorithms to a MAC PDU payload.

ii) A Security for Control and Management (SCM) protocol providing the secure distribution of keying data from the BS to the CPE. Through this key management protocol, the CPE and the BS synchronize keying data; in addition, the BS uses the protocol to enforce conditional access to network services. The protocol stack for the security components of the system are shown in Fig. [5].

Authentication state machine: The Authentication state machine (ASM) Fig. 6 adopts an authentication framework similar to the model specified in IEEE Std. 802.16-2009. The ASM incorporates EAP authentication and is made up of four states and thirteen events and messages that are used to communicate with other aspects of the SCM framework. The ASM has to interoperate with the TEK state machine and the EAP Process [1].

Start Authentication: This event is generated to start the ASM after the conclusion of the basic capabilities exchange (CBC-REQ/RSP) during network entry.

EAP Timeout: ASM generates this event when 'EAP Authentication Timer' has expired prior to reception of SCM EAP-Start/Transfer messages during initial authentication or re-authentication. When this happens, the 'Current # of Authentication Attempts' is incremented and the 'EAP Authentication Timer' is restarted.

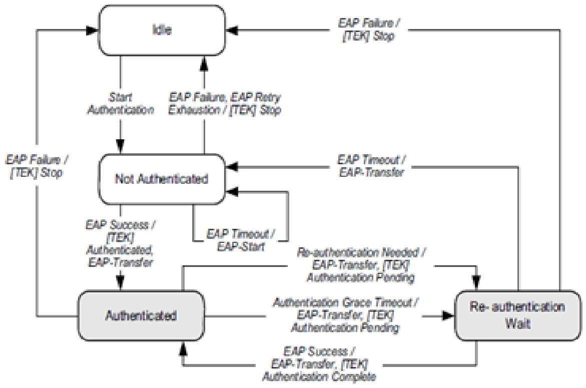

Idle
EAP Failure / [TEK] Stop
Start Authentication
EAP Failure, EAP Retry Exhaustion / [TEK] Stop
EAP Failure / [TEK] Stop
Not Authenticated
EAP Timeout / EAP-Transfer
EAP Success / [TEK] Authenticated, EAP-Transfer
EAP Timeout / EAP-Start
Re-authentication Needed / EAP-Transfer, [TEK] Authentication Pending
Authenticated
Authentication Grace Timeout / EAP-Transfer, [TEK] Authentication Pending
Re- authentication Wait
EAP Success / EAP-Transfer, [TEK] Authentication Complete

Fig. 6: Authentication State Machine

EAP Failure: The EAP Process generates this message to tell the ASM that the EAP Process has not resulted in successful authentication being verified.

EAP Failure: The EAP Process generates this message to tell the ASM that the EAP Process has not resulted in successful authentication being verified.

EAP Retry Exhaustion: This event is generated by the ASM when the 'Max # EAP Authentication Attempts' has been reached without successful completion of authentication or re-authentication.

EAP Success: The EAP Process generates this even to tell ASM that EAP Process, during initial authentication or re-authentication, has completed successfully. The 'Current # of authentication attempts' is set to zero upon indication of this event.

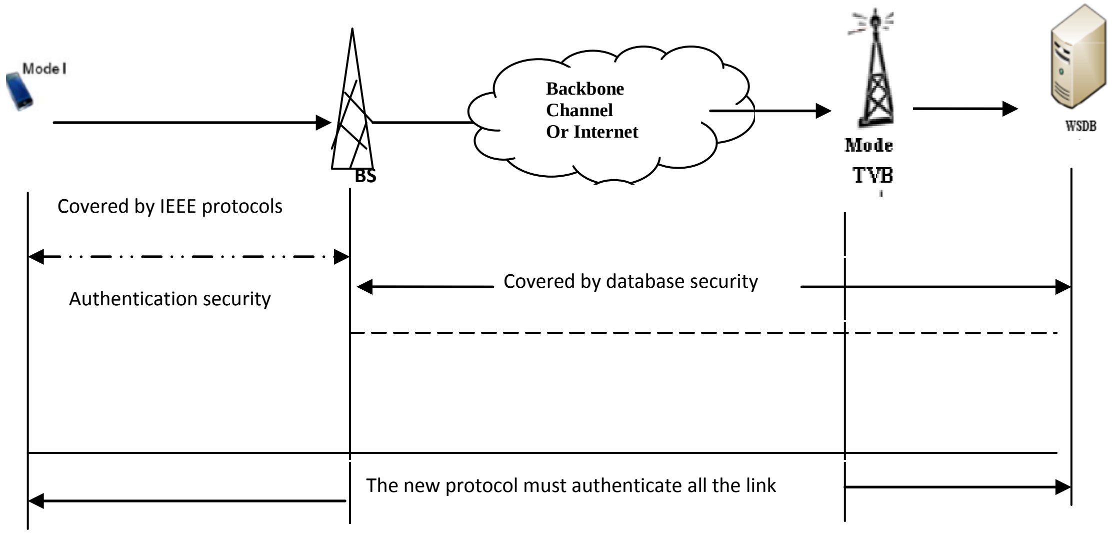

Mode l
BS
Backbone Channel Or Internet
Mode TVB
WSDB
Covered by IEEE protocols
Authentication security
Covered by database security
The new protocol must authenticate all the link

Fig. 7: A protocol to authenticate all the link between CPE and BS

Re-authentication Needed: Generated when the network operator or AAA service decides to force reauthentication prior to expiration of current AK or to update successive/concurrent AK contexts that are operating on the CPE. Reception of an (unsolicited) SCM EAP-Start/Transfer message prior to expiration of current AK, while in the authenticated state can trigger this event.

Authentication Grace Timeout: When 'Authentication Grace Timer' expires, reauthentication process is automatically restarted. The authentication process is specified in five way hand shaking f. The first and second message as the same as specified in WIMAX protocol, but the different is the second message here is registration request message REG-REQ, and also after BS check the CPE certificate and authenticate it then the BS must send Registration response message which include its certificate and the authentication of the CPE. When CPE receive this message it verifies the BS certificate and if it's true the CPE authenticate the BS by sending ACK message to the BS. Fig. 6 shows the authentication state machine.

III. THE PROTOCOL FOR TVWS DATABASE AND NEW IDEA

TV white spaces (TVWS) exist in the broadcast TV operating frequencies known as the VHF/UHF band, specifically ranging from 470 MHz - 790 MHz in Europe [1], [2] and non-continuous 54 MHz - 698 MHz in the United States [3]. We found that there are so many reasons why IEEE 802.22 is the best protocol for TVWS.

Firstly its broadband access in remote and rural areas. Its frequency allows for wider coverage and more services and users hence provide a suitable business case. Secondly it has been realized that many TV channels are largely unoccupied in many parts of the US [17], given that most households and businesses rely on cable and satellite TV services. Finally the 802.22 is the only protocol which has the ability to work with incumbent channels.

The problem with the IEEE 802.22 and all other IEEE protocols is that these protocols work in the physical layer which means it will be used to authenticate only the CPE with the BS and the data

between BS and Master Mode2, as depicted in Fig. 7, also the Database security (work in application layer) is covering the range between the BS and Master Mode2. The new idea which we want to apply is "to *design a new protocol for TVWS to authenticate the CPE with the Master Mode2 and the database"*. In the other word we need one protocol to authenticate the entire link (between the CPE and the Database) directly and apply this protocol in MAC Sublayer.

IV. CONCLUSION

In this paper, we review the IEEE protocols security and the database security particular the authentication, in order to design a new protocol more suitable for the TVWS database. We found that there are so many reasons why IEEE 802.22 is the best protocol for TVWS. And we explain our needs to enhance the protocol to be used in the TVWS and how we can enhance it.

REFERENCES

[1]. JYH-CHENG CHEN, "Wireless LAN Security and IEEE 802.11I**",** IEEE Wireless Communications, Feb 2005.

[2]. P. Bachan and Brahmjit Singh, "Performance Evaluation of Authentication Protocols for IEEE 802.11 Standard", 978-1-4244-9034-/10/$26.00©2010.

[3]. Stanley Wong, "The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards", SANS Institute 2003.

[4]. IEEE Std 802.1X-2001, "Port-Based Network Access Control," June 2001.

[5]. P. Funk and S. Blake-Wilson, "EAP Tunneled TLS Authentication Protocol (EAP-TTLS)," IETF Internet draft, draftietf-pppext-eap-ttls-03.txt, Aug. 2003, work in progress.

[6]. A. Palekar et al., "Protected EAP Protocol (PEAP) Version 2", IETF Internet draft, draft-josefsson-pppext-eap-tlseap-07.txt, Oct. 2003, work in progress.

[7]. H. Haverinen and J. Salowey, "EAP SIM Authentication", IETF Internet draft, draft-haverinen-pppext-eap-sim-12.txt, Oct. 2003, work in progress.

[8]. IEEE Std. 802.16-2001, IEEE Standard for Local and Metropolitan Area Networks, part 16, "Air Interface for Fixed Broadband Wireless Access Systems," IEEE Press, 2001.

[9]. DAVID, JOHNSTON AND, JESSE WALKER, "Overview of IEEE 802.16 Security", IEEE COMPUTER SOCIETY 1540-7993/04/$20.00 © 2004 IEEE.

[10]. Kaigui Bian, "Security Vulnerabilities in IEEE 802.22", Digital Object Identifier: 10.4108/ICST.WICON2008.4976.

[11]. IEEE Std 802.22-2011TM, Standard for Wireless Regional Area Policies and procedures for operation in the TV Bands, July 2011.

[12]. Ofcom (2012, July 4), Regulatory requirements for white space devices in the UHF TV band [Online]. Retrieved April 2013, from:http://www.cept.org/Documents/se-43/6161/

[13]. ETSI, "EN 301 598 White Space Devices (WSD): Wireless Access Systems operating in the 470 MHz to 790 MHz frequency band," Oct 2012.

[14]. Electronic Code of Federal Regulations (2013, April), Title 47, part 15, subpart H Television Band Devices [Online]. Retrieved April 2013, from GPO: http://www.ecfr.gov.

[15]. Wi-Fi Alliance. "What is Wi-Fi?", URL: http://www.wi-fi.com/OpenSection/index.asp

[16]. P. Rastegari, "An overview of the IEEE 802.22 Standard", 2012.