IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 5 Issue 4, April 2018
ISSN (Online) 2348 – 7968
www.ijiset.com

High secure Mutual Authentication Protocol for TVWS Database

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

Abstract
This paper studied the authentication in the IEEE protocols (802.11-802.X1-802.11i-802.16e – 802.22) and showed the weakness and the problems that will arise when we use them and what efforts are done to overcome this problems. The finding of this paper is that IEEE 802.22 is the best protocol to use in the TVW Because of its wide area coverage. Finally the paper explained the full path authentication, and 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.

Keywords
IEEE standard, security, Geolocation database. Authentication.

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 The 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 introducing the new idea about the protocol and discusses the proposed protocol and Section IV conclude the paper.

II. Literature Review
II.1IEEE 802.11 [WEP Security]
Wired Equivalent Privacy (WEP) was an encryption algorithm designed to provide wireless security for users who implement 802.11 wireless networks . 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 and with the cipher text, is sent to the receiver. The receiver decrypts the packet using the stored WEP key and the attached IV[3]. 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.

II.2 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 [3]. 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) Figure 1 depicts a typical 802.1X message exchange with both the supplicant PAE and authenticator PAE state transitions

II.3 IEEE 802.11i

The IEEE 802.11i standard provides authentication and security at the Medium Access Control layer in wireless local area

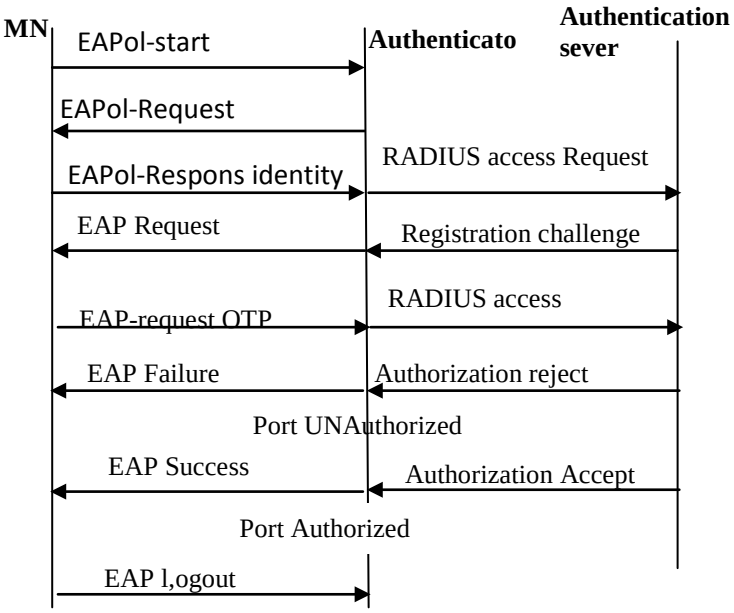

Figure 1 depicts a typical 802.1X message exchange with both the supplicant PAE and

networks (WLANs) [3]. 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 [4].

II.3 IEEE 802.16e (WiMax)

The standard IEEE 802.16e [10] use the new privacy key management protocol PKMv2 to improve the security performance, in which the EAP [11] (Extensible Authentication Protocol) are introduced into IEEE 802.16e. By combining EAP and RSA, the PKMv2 has defined different authentication modes. According to the IEEE 802.16e PKMv2 they should be 5 kinds of authentication modes, according to the 8-bit binary value of the 'Authorization policy support' domain in SBC-REQ /SBC-RSP messages. The auth modes are single RSA, single EAP_based, RSA + authenticated_EAP, EAP + authenticated_EAP mode and RSA+EAP_based mode.

There are two problems with IEEE 802.16e to use it in the TVWS first problem is the protocol distance and the second one is this type of complexity authentication will become so difficult to implement in TVWS devices because this devices suppose to be a little capabilities. Also A whole extensible authentication protocol (EAP)-based authentication scheme is time-consuming due to the operations of public key cryptography and validation of certificates which is unacceptable for the wireless regional area networks [18].

II.6 IETF PAWS Protocol

Internet Engineering Task Force (IETF) is developing a WG called Protocol to Access White Space database (PAWS) is aims to define 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 IPnetworks. 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 knows 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" [13].

As we can see in figure 2 the PAWS protocol also depend on tow layer authentication (HTTP/TLS and PAWS) this will become more complex and overhead

The protocol procedure is consisting of ten messages. Message one and tow to specify the device capability and message 3,4 for registration (if required) after the registration completed the master send message 5 asking for the available channels he can use. Then the master send message 7 asking for device validation (this is very important message to our work because we will use this message to authenticate the users mode I). And after the users select the channels that they are willing to use then the master send message 9 to notify the database about the usable channels. Figure 3 shows the protocol steps.

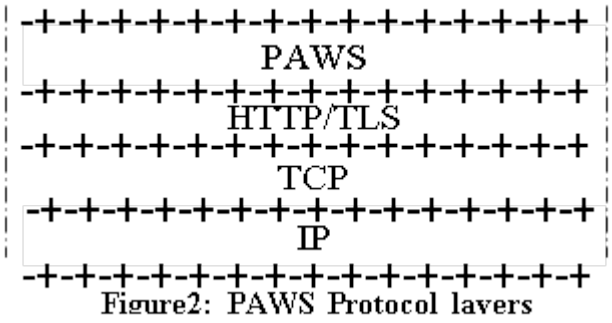

Figure2: PAWS Protocol layers

.

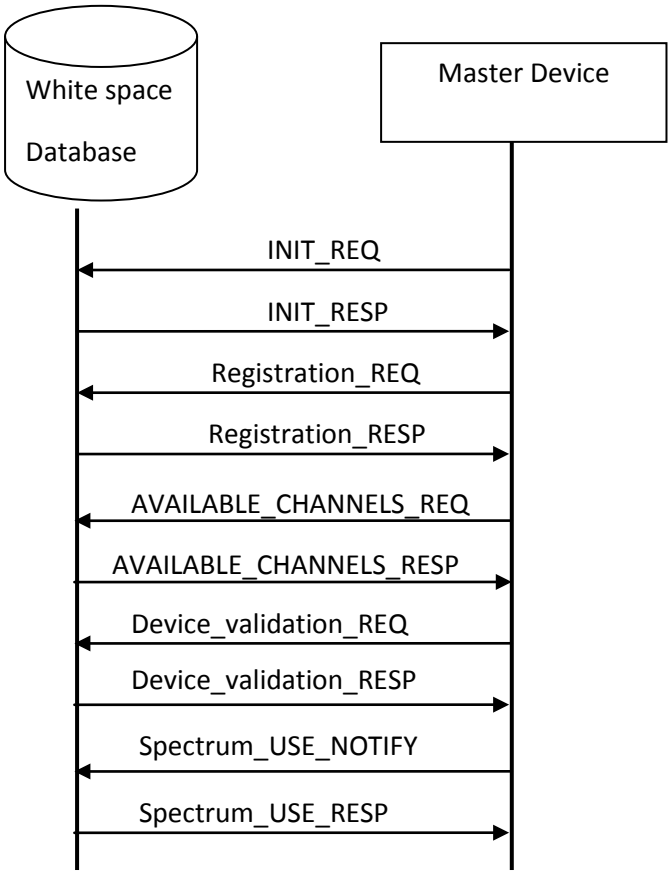

Figure 3: IETF protocol steps [2]

II.7 IEEE 802.22 (WRAN)

IEEE 802.22 is defined as the first wireless protocol for cognitive radio in wireless regional area network (WRAN) [12]. 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 [12]. The security sublayer has two components: an encapsulation protocol and a Privacy Key Management (PKM) protocol.

II.8 Master Register Protocol (MRP)

To ensure TVWS confidentiality [1] proposed a modification in WSD tables. Sketch of the WSDB is shown in Table 1. By adding a new column calls Info_Number. And a random number will be assigned for all information's that the server's need to store about the Master mode. The Info_Number is a random number could be between 0 and 1000 to make sure they have sufficient numbers; which is unique for all information exchanged between TV WSDs. In this context [1] introduced two ways, the first one is by suggest this column to be a primary key. This option prevents any repeating Info_Number values which ensure the uniqueness of this numbers. The second option is by using any random generating algorithm.

TABLE 1: THE DATABASE TABLE

Column Name	Type	Inf0_Number
DeviceType	Fixed	9658551
DeviceName	String	7435679
DeviceSerialNumber	String	62248537

III The proposed method

The Database Server (DS) has all the information about the master devices (mode 2 device) and the users device's (mode1 device) and this information is stored in the Database. So in this method the modification of the database by adding a new column and put a random number in this column Mubark el [1].
Then divided the authentication into two phases Phase1 the Master authenticates itself with the Database Server (DS), and the second phase the mdoe1 device (user device) authenticate itself with the master (mode 2 device) as depicted in figure 4,5,6.

Phase1 between the master and DS

The master sends its certificate to the Database Server and immediately sends a registrations request message (Message 1 and 2). When the database server receive this messages it verify the master certificate and if it is accepted then the server replies by sending its certificate (Message 3) and pick one of the random number from the master table as challenge question and send it back to the master as a reply message (Message 4). When the master receives the messages, first it verify the server certificate and if it has been accepted then the master replies with confirmation message (Message 5).The confirmation message is divided into two part; the first part is the answer of the server's challenge question and it represent the value of the random number from the master table, in the second part- of the message - it must pick one of the random number from the DS table as challenge question and send it back to the DS. When the DS receive this messages it first verifies the answer of the server's challenge question and if it is true then the DS replies with conf_reply message (Message 6) which answer the master's challenge question from the DS table. When the master receive this message and verifies the answer of the challenge question the master replies with Ser-Auth-success(Message 7), and the DS replies with Auth-comp-success message(Message 8). Figure3 shows the protocol steps figure 4 explained these steps.

At this point the master and DS are mutual authenticated and the master send Ava_Chanell-req message (Message 9). And also send a list of allowable user's request (the list of the users that the master is allow to authenticate). (Message 10) This message is very important to complete phase2 authentication. And the DS replies with the available channels that the master can be used in this area (Message 11) and a list of registered users which the master allows to authenticate (Message 12) Figure 5 shows this steps.

Phase2 between the master and user's

When the mobile Subscriber (MS) sends an authentication request message (Message 1) to the master then the authentication in this phase can be in two cases

Case1: If the user device mode1 is already registered in the list that the master was received in message 12, then the master replies by message 1.1 which represent the master certificate and master's challenge question to the user and the authentication process is follow the same steps in the phase1 authentication process.

But the only different is this authentication is between the master and mode1 device

Case2: if the user is not in the user's list then the master must sends user authentication request message to the DS (Message 2). And the DS replies with the challenge question and the user's data to the master (Message 3). Then master updates its database list and forward the challenge question to the user (Message 4). After this the master and the user can continue the authentication process as in phase1. Figure 6 show the cases.

IV Conclusion

This paper designed a full path authentication protocol between the user and the Database server (DS). This protocol is depend on IEEE802.22 protocol and utilize the availability of the database information to help the Mobile Subscriber (mode 1 device) to authenticate themselves with the Database Server user by using one authentication's protocol. The SPLS simulation results shows the simulation is saved as specified in figure 7.

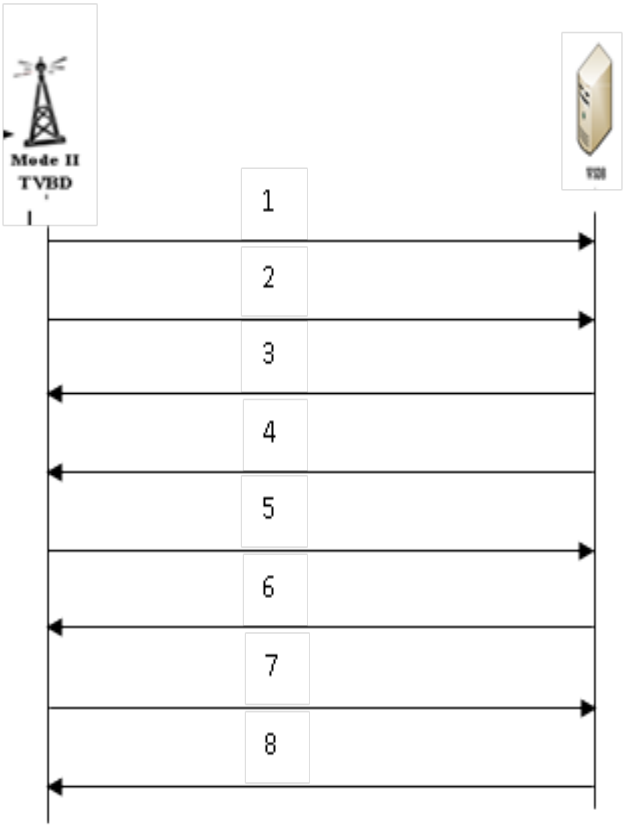

Figure 4: The protocol authentication steps

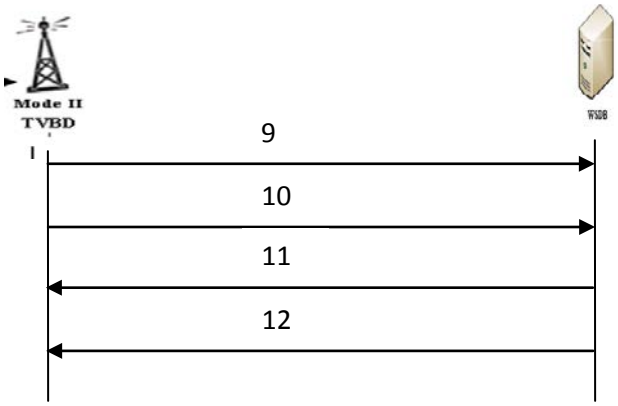

Figure 5 : list of avl_userTo Authenticat Request

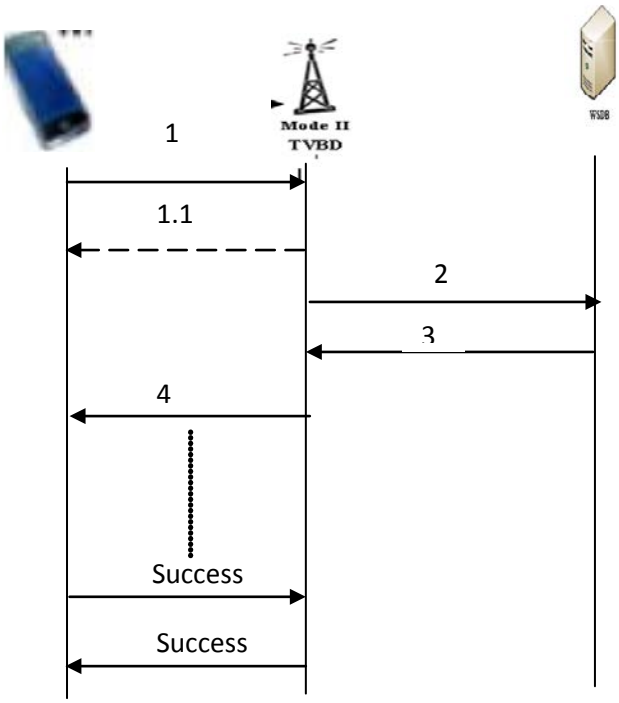

Figure 6: shows user case authentication

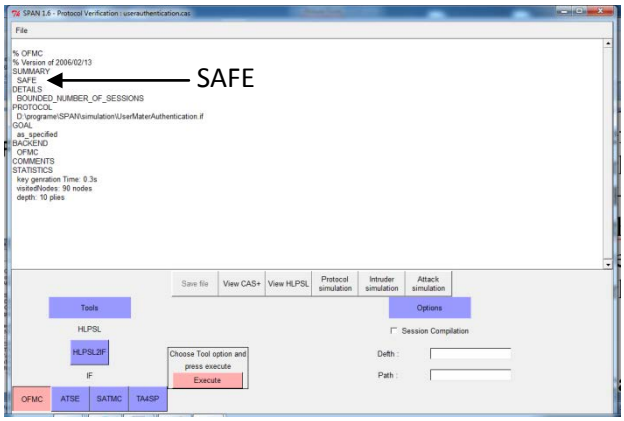

Figure 7 the HLPSL simulation result

References

1. Mubark. Rashid et "New Methods for TVWS Database Protocol" . ijcts, volume 2 issue 6. 2015.

2. ITU Regional Radio-communication seminar for Arab countries. Cognitive radio and TVWS workshop Manama Bahrain 2014.

3. JYH-CHENG CHEN and at "WIRELESS LAN SECURITY AND IEEE 802.11I" IEEE Wireless Communications , February 2005.

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

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

6. IEEE Std 802.1X-2001, "Port-Based Network Access Control," June 2001.

7. 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.

8. 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.

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

10. 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.

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

12. Kaigui Bian and et ," Security Vulnerabilities in IEEE 802.22", Digital Object Identifier: 10.4108/ICST.WICON2008.4976.

[12] I EEE Std 802.22-2011TM, Standard for Wireless Regional Area Policies and procedures for operation in the TV Bands, July 2011

[13] 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/

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

[15] 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.

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

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

[18] Cong Wang and Mode ma and Zenghua Zhao, An Efficient EAP-Based Pre-Authentication Scheme for Handovers in WRANs over TVWS, IEEE conference, Singapore, Singapore,2017.