Journal of Network and Computer Applications 34 (2011) 1160–1167

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

# Location-based authentication protocol for first cognitive radio networking standard

Hyun Sung Kim *

*Department of Computer Engineering, Kyungil University, Kyungbuk 712-701, Republic of Korea*

ARTICLE INFO

*Article history:*
Received 25 August 2010
Received in revised form
6 December 2010
Accepted 17 December 2010
Available online 30 December 2010

*Keywords:*
IEEE 802.22
Cognitive radio
Location-based authentication
Extensible authentication protocol

ABSTRACT

The developing IEEE 802.22 standard will allow broadband access to be provided in sparsely populated areas by using cognitive radio techniques with operations on a non-interfering basis over television broadcast bands. Such non-interfering basis operation will increase the efficiency of utilisation of that spectrum, and provide large economic and societal benefits. However, the security mechanisms supported by IEEE 802.22 security sub-layer are insufficient to ensure robust security due to the fact that the designers of the standard attempted to reuse the security sub-layer designed for IEEE 802.16 networks, which does not consider the unique security features from IEEE 802.22 networks. This paper proposes a location-based authentication protocol for IEEE 802.22, which can be integrated with the extensible authentication protocol. The proposed protocol uses location information as a key factor to be authenticated each other. Furthermore, it could provide the privacy and confidentiality.



## 1. Introduction

With the rapid growth of information and communication technology (ICT), people tend to more and more rely on digital communications. Cognitive radio (CR) offers the promise of intelligent radio communications that can learn from and adapt to its environment. Much research is currently underway on developing various reasoning and learning algorithms that allow CRs to operate optimally in a large variety of different situations. IEEE 802.22 is the first wireless access standard based on CR technology, which is a standard for wireless regional area network (WRAN) that utilises ultra high frequency (UHF) and very high frequency (VHF) television bands between 54 and 862 MHz. The standard mandates a centralised cognitive radio network (CRN) architecture, where the secondary IEEE 802.22 base stations (BSs) manage a unique feature of distributed sensing. To perform distributed sensing, BS instructs the secondary cognitive user devices, also called consumer premise equipments (CPEs), to synchronously sense various spectral bands for the presence of primary user activity (Mitola, 2000; IEEE 802.22, 2008; Stevenson et al., 2009). However, as with many new technologies, initial standardisation work has not focused on security aspects of CR.

Very little research has examined for the new security threats to CR due to their intelligent behaviour. Some specific works have been conducted looking at attacks in dynamic spectrum access in Chen and Park (2006) and Chen et al. (2008), and were broadened to look at a variety of denial of service attacks against policy radios in Brown and Sethi (2008) and Clancy and Goergen (2008). Quite recently, IEEE 802.22 (2009a) began to prescribe two security sub-layers that apply cryptographic transformations to media access control (MAC) data units. Most of the features of the security sub-layers are inherited from the security sub-layer in IEEE 802.16e (Johnston and Walker, 2004). IEEE 802.16e is an amendment to the base standard IEEE 802.16 and it addresses some of the base standard's security flaws by incorporating some new security mechanisms. Specifically, IEEE 802.16e incorporates the privacy key management scheme, referred to as PKMv2, as part of the standard. PKMv2 and the encapsulation protocol form the foundation of IEEE 802.22 security sub-layers. The security mechanisms supported by IEEE 802.22 security sub-layers are insufficient to ensure robust security. The standard is vulnerable against various security threats, which partly due to the fact that the designers of the standard attempted to reuse the security sub-layer designed for IEEE 802.16 networks (Bian and Park, 2008). IEEE 802.22 networks are composed of CR nodes, and thus face unique security threats not faced by the conventional networks.

Focused on a specific aspect for IEEE 802.22 draft standard, it requires all devices in the network to be installed in a fixed location and BS is required to know its location and the location of all of its associated CPEs by equipping with satellite-based geo-location technology (GPS; IEEE 802.22, 2008). It showed that location information in IEEE 802.22 system is a very important factor and the system policy should be adaptively changed by the information. Kuroda et al. (2007) proposed a radio-independent

* Tel.: +82 53 850 7288; fax: +82 53 850 7609.
*E-mail address:* kim@kiu.ac.kr

1084-8045/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.12.017