ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Novel Encryption Standard Against User Emulation Attacks

Bingi Uma Maheswari
MTech Student
Department of ECE
AnuBose Institute Of Technology(ABIT)
Paloncha, Khammam, India

K.Vasavi
Associate Professor
Department of ECE
AnuBose Institute Of Technology(ABIT)
Paloncha, Khammam, India

ABSTRACT: ***Cognitive radio, the recent emerging software enabled radio system, which is capable of self-turning frequency band and setting suitable parameters for utilizing a channel freed or unused by licensed primary user . The cognitive radio which utilize unused channel, are called secondary user. The Secondary User detect whether a Primary User's channel is free or occupied at the time using spectrum sensing techniques. It is proved that single Secondary User free channel detection success ratio is comparatively low than cooperative sensing with other secondary user because of noisy wireless channel. The security concern arises when any of the cognitive radio selfish nodes is transmitting false detection report to fusion center which taken decision would be wrong and result of low free channel utilization. We propose model detect wrong information sent by cognitive radio and misbehaving cognitive radio in cognitive radio network. By using the advanced encryption standard find the authorized primary user. Keywords: Cognitive Radio Network, Primary User Emulation Attack, DTV, AES-Encrypted, DSA, CR Networks***

Index Terms—Neighbor position verification, mobile ad hoc networks, vehicular networks.

INTRODUCTION:

Cognitive radio can be described as an intelligent and dynamically reconfigurable radio that can adaptively regulate its internal parameters as a response to the changes in the surrounding environment. Namely, its parameters can be reconfigured in order to accommodate the current needs of either the network operator, spectrum lessor, or the enduser. Although this doesn't necessarily need to be the case, Cognitive Radio (CR) is usually being defined as an upgraded and enhanced Software Defined Radio (SDR). Typically, full Cognitive Radios will have learning mechanisms based on some of the deployed machine learning techniques, and may potentially also be equipped with smart antennas, geolocation capabilities, biometrical identification, etc.However, the newly-introduced cognitive capabilities are exactly what make Cognitive Radios susceptible to a whole new set of possible security issues and breaches. Furthermore, the threats characteristic to Software Defined Radios, as well as those characteristic to ―traditional‖ wireless networks also need to be taken into account.Cognitive Radio Network can be described as a network in which one or more users are Cognitive Radios. With the assumption of the potential attacker, as well as legitimate Secondary Users (SUs) always being CRs, the taxonomy of the threats within CRNs can be done with respect to the type of the Primary Users (PUs) considered.

Existing System:

In this Project, It is desired to minimize spectrumsensing error that means sum of false alarm and missdetectionprobabilities since minimizing spectrum sensing error bothreduces collision probability with primary user and enhancesusage level of vacant spectrum. To provide reliable spectrumsensing performance (i.e., minimize spectrum sensing error),one of the great challenges is determining threshold levelsince spectrum sensing performance depends on thethreshold level. When determining threshold level, besidesspectrum sensing error, spectrum sensing constraint whichrequires false alarm and miss detection probabilities to bebelow target level should also be considered since

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

itguarantees minimum required protection level of primaryuser and usage level of vacant spectrum.

Proposed System:

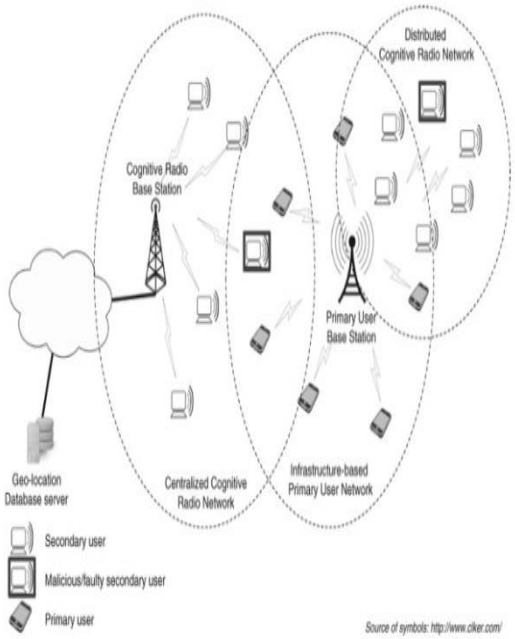
In this paper the proposed system an Advanced Encryption Standardfor DTV is robust and reliable primary and secondary systemoperations. In the proposed system, At the Sending end primary user generatesa pseudo-random number AES-encrypted reference signal that is usedas the segment sync bits. The sync bits in the field sync segmentsremain unchanged for the channel estimation purposes at the receiving end, the reference signal is regenerated forthe detection of the primary user and malicious user. It shouldbe emphasized that synchronization is still guaranteed in theproposed scheme since the reference bits are also used forsynchronization purposes. For each Slot period check the correlation and the threshold value it will detect the Primary user emulation attack.

Securely determining own location.

In mobile environments,self-localization is mainly achieved through GlobalNavigation Satellite Systems, e.g., GPS, whose security canbe provided by cryptographic and noncryptographicdefense mechanisms. Alternatively, terrestrial specialpurposeinfrastructure could be used along withtechniques to deal with nonhonest beacons. We remarkthat this problem is orthogonal to the problem of NPV. Inthe rest of this paper, we will assume that devices employone of the techniques above to securely determine their ownposition and time reference.

Cognitive radio networks

A network employing CR technology may adopt a centralized or distributed architecture, as illustrated in Figure 1. With a centralized approach or infrastructure-based CR network, spectrum decisions are performed and coordinated by a central entity (e.g., a base station) based on the fusion of sensing results collected from several SUs or dedicated sensors. This approach therefore enables a centralized cooperative sensing scheme. The central entity can additionally rely on geo-location databases providing the coordinates of known primary transmitters (e.g., television transmitter towers) and their respective regions of potential interference. This is the approach adopted in the recent IEEE 802.22 standard [12], which targets CR operations over television frequency bands (54 to 862 MHz) in order to enable the deployment of wireless regional networks. IEEE 802.22 uses both spectrum sensing and geo-location databases for the detection of spectrum holes, with regulatory bodies being responsible for the maintenance of the information describing the locations of the primary systems. When this information is not available, all the television channels are considered potential opportunities and only sensing is used.



Cognitive radio security threats

Security threats against CR networks may be motivated not only by the wireless nature of such communication environments (and that are in fact inherent of any wireless communications technology) but also by the employment of specific cognitive operations. In Figure 2, we illustrate a taxonomy of the

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

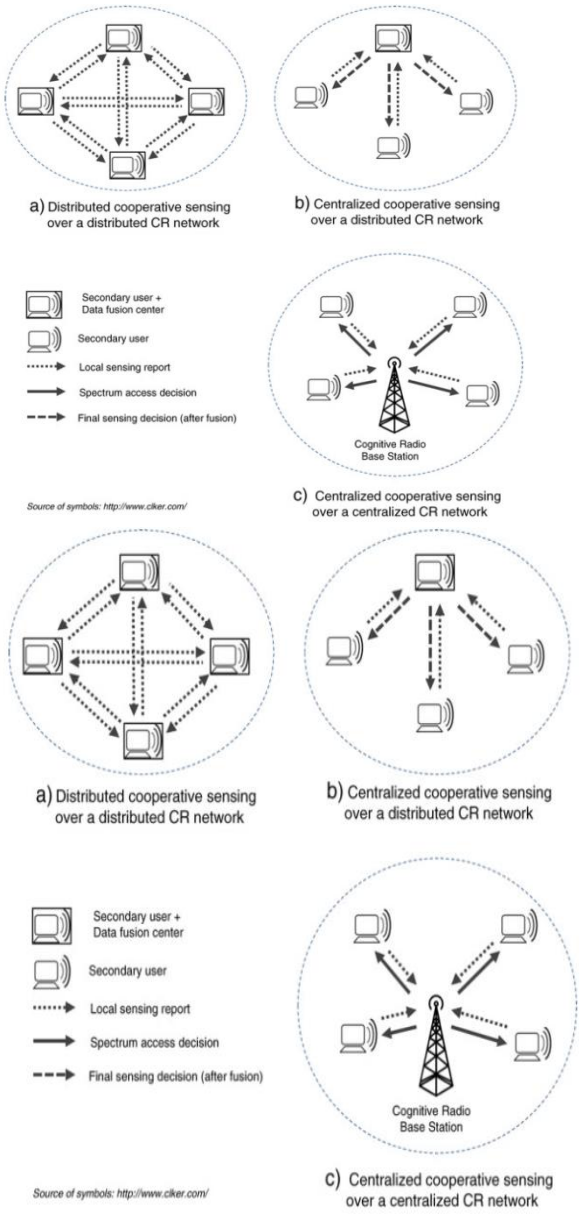
security threats against CR environments, considering such two different and complementary perspectives.

Approaches to attack-tolerant primary user detection on CR environments

Various security threats are transversal to wireless environments and may consequently also affect CR applications and communication mechanisms. For example, a beacon falsification attack in IEEE 802.22 environments may allow the transmission of false spectrum or geo-location information to users, allowing the subversion of normal spectrum space access and usage rules. As in most wireless environments, well-known security solutions may be of help in circumventing many of such attacks in CR networks. In this context, the security layer 1 as defined in IEEE 802.22 defines encryption and authentication mechanisms offering protection for geo-location information as reported by the SUs using the co-existence beacon protocol (CBP).

Attacks against cooperative sensing

Spectrum sensing is a fundamental mechanism of CR networks and, in this context, one major problem to avoid is the designated hidden PU problem. This problem occurs when a SU cannot sense the activity of a PU it interferes with, i.e., when it is out of the coverage area of the PU or when sensing is affected by well-known adverse effects in wireless communications, in particular multipath fading and shadowing. For instance, in Figure 1 the PU base station is a hidden PU, in the perspective of the three nodes of the distributed CR network that are out of its coverage area, while having transmission ranges that overlap it. In practice, we must consider that sensing can also be erroneous due to inherent hardware imperfections, and consequently the usage of spectrum occupancy information obtained exclusively from local sensing might not achieve satisfactory results. In this context, cooperative or collaborative sensing is considered an effective means to increase the efficiency of PU detection in CR environments. However, it also creates new security vulnerabilities, as we proceed to discuss in greater detail.



Primary user emulation in CRenvironments

Primary user emulation attacks in CR environments aim at forcing SUs to avoid using specific frequency bands and, therefore, may cause the same adverse effect as always reporting a channel to be busy with cooperative sensing schemes, as described in Table 2. This threat is materialized through the transmission of fake PU signals and does not necessarily require the attackers to participate in any underlying cooperative scheme. Thus, a PU emulation attacker does not aim at causing interference to PUs and, according to Araujo

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

et al., PU emulation is the most studied attack against CR.

CONCLUSION:

Cognitive radio is a highly multidisciplinary area currently attracting numerous research efforts, which provides a large number of challenges regarding security and accurate sensing. As previously discussed, this survey is focused particularly on security in the context of primary user detection, particularly in what concerns two major types of attacks: primary user emulation and spectrum sensing data falsification. The importance of such attacks is also related to the fact that they may in fact compromise the feasibility of CR solutions and applications. As in other communication approaches, we may expect security to represent a fundamental enabling factor of future CR applications

REFERENCES:

[1] 1609.2-2006: IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE, 2006.

[2] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure Vehicular Communications: Design and Architecture," IEEE Comm. Magazine, vol. 46, no. 11, pp. 100-109, Nov. 2008.

[3] P. Papadimitratos and A. Jovanovic, "GNSS-Based Positioning:Attacks and Countermeasures," Proc. IEEE Military Comm. Conf.(MILCOM), Nov. 2008.

[4] L. Lazos and R. Poovendran, "HiRLoc: High-Resolution Robust Localization for Wireless Sensor Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 233-246, Feb. 2006.

[5] R. Poovendran and L. Lazos, "A Graph Theoretic Framework for Preventing the Wormhole Attack," Wireless Networks, vol. 13, pp. 27-59, 2007.

[6] S. Zhong, M. Jadliwala, S. Upadhyaya, and C. Qiao, "Towards a Theory of Robust Localization against Malicious Beacon Nodes," Proc. IEEE INFOCOM, Apr. 2008.

[7] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, and J.-P.Hubaux, "Secure Neighborhood Discovery:AFundamental Element for Mobile Ad Hoc Networks," IEEE Comm. Magazine, vol. 46, no. 2, pp. 132-139, Feb. 2008.

[8] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," Proc. IEEE INFOCOM, Apr. 2003.