Secure Techniques to Support Cognitive Access in Spectrum Bands

Emmanouil A. Panaousis and Christos Politis
Wireless Multimedia and Networking (WMN) Research Group, Kingston University London
United Kingdom, e-mail: {e.panaousis,c.politis}@kingston.ac.uk

Abstract

Cognitive radio (CR) is a promising technology for efficient spectrum utilisation in the future wireless communication systems. The main idea behind the use of CR is to achieve greater utilisation of the spectrum by allowing license-exempt users to coexist with the incumbent licensed primary users provided that they do not cause harmful interference to the latter. Thus, CR systems used by license-exempt users must be able to sense and learn the radio environment and finally adapt their parameters to avoid interfering with incumbent users. The CR field has introduces several challenging problems including security. Namely, malicious entities have the potential to corrupt the appropriate functionality of CR systems by disrupting the spectrum sensing protocol, change the sensing reports, which are used in the spectrum sharing protocol. Needless to say, there is an apparent need to secure the aforementioned protocols along with establishing trust among the licensed-exempt users towards authenticated and integrity validated sensing data sharing. In this paper we discuss our envision for the future where secure cognitive radio communications will be proven critical in many scenarios such as emergency cases where telecommunications infrastructures have failed or are not available.

Keywords

Cognitive radio, spectrum sensing, clustering, common control channel, security

1. Introduction

The inherent demand for wireless services has led to an increased demand for radio spectrum. The necessary sharing of this finite resource has traditionally been regulated by governmental agencies. Spectrum is divided into fixed size portions that can be licensed or license exempt. In the UK around five per cent of the spectrum is used for license exempt technologies and 95% for licensed use at present. License exempt spectrum is the spectrum that may be used freely without the need for a specific license from the regulator or an authorised spectrum manager.

Spectrum efficiency can be significantly increased by allowing a group of potential users to opportunistically access licensed bands of the spectrum. To overcome the challenge of interference and to improve the spectrum efficiency by exploiting the unused spectrum in dynamically changing environments, the technology of Cognitive Radios (CR) (Mitola, 2000) has the potential to be utilised in the future. The IEEE 802.22 Working Group (WG) has defined the term of cognitive radio as following: "A cognitive radio is a radio frequency transmitter/receiver that is designed to intelligently detect whether a particular segment of the radio spectrum is currently in use, and to jump into (and out of, as necessary) the temporarily-unused spectrum very rapidly, without interfering with the transmissions of other authorised users".

According to (Srinivasa & Jafar, 2009) it may be feasible to find non-utilised portions of spectrum through the exploitation of new technologies that allow cognitive radio users to operate in the same spectrum with legacy users of traditional radio technology, without interfering with them. In other words, a cognitive radio system enables devices to operate efficiently in multiple different frequency bands of the radio spectrum, including those with legacy users.

The concept of cognitive radio can be applied in contexts such as disaster recovery, military applications and health monitoring. It is worth mentioning that within the context of cognitive networking, mesh networking (Akyildiz et al, 2009) can be utilised to support emergency or military applications (Younis et al, 2009). For instance, in many extreme emergency scenarios such as natural or manmade disasters, the rescuers may face difficulty using traditional legacy networks due to destruction or collapse of the telecommunications infrastructure. The mesh nature along with cognitive radio capabilities can be utilised in the context of an emergency for all the involved emergency rescue teams.

Within the realm of cognitive radios, security becomes an emerging area of research that is attracting interest among scientists. Although the amount of research carried out in the security domain for cognitive radios is not significant, few papers such as (Chen et al, 2008) have highlighted the most critical security considerations. In summary, all of the supported approaches mention that compared to traditional radio networks, cognitive networks are intelligent and flexible and thus more exposed to malicious users that can jeopardise a user's functionality by disrupting e.g. the appropriate operation of spectrum sharing.

2. Motivation

Spectrum sensing (Hwang et al, 2010) is one of the most challenging issues in next generation wireless communication systems. Spectrum sensing is the task of obtaining awareness about the spectrum usage and existence of different users in a geographical area. According to (Kaligineedi et al, 2008) the most important challenge for a cognitive radio system is to determine the presence of legacy users. Consequently, one of the primary requirements of cognitive networks is their ability to scan the spectral band and identify vacant channels available for opportunistic transmission. The secondary users have to depend on their own individual or cooperative sensing ability to detect primary user transmissions. In fact, spectrum sensing determines a list of spectrum bands that are available within a geographical boundary. Then the participating nodes have to share their sensing data. Within this context, two cooperative approaches can be currently utilised; the distributed and the centralised. In the centralised approach, the various cognitive radio devices sent the sensing data to a data aggregator that is responsible apart from collecting the data, to decide on the spectrum sharing among cognitive radio users. In the latter case, each node has either a direct link to the data aggregator or he sends its message through intermediate nodes constituting in this way a cognitive mesh network. On the other hand, distributed approaches assume that the cognitive radio devices exchange information about the spectrum sensing in a distributed manner.

Some researchers argue that the performance of cooperative and distributed sensing can be improved by clustering (Sun et al, 2007). Additionally, in (Van and Koo, 2009) cognitive radio users within the same location are grouped into a cluster. According to these approaches, clustering of the cognitive devices can make the secondary network scalable in collecting measurements for data fusion by authorising cluster-heads to make local (intra-cluster) decisions. The role of optimal data fusion rule within a cluster has the imperative purpose to reduce the rate of reporting errors therefore increases the spectrum sensing accuracy. Within a cluster the cluster-head has to collect the data from each cognitive radio user and transfer them to the data aggregator or fusion centre that has to take the final decision on the spectrum access namely to fulfil the spectrum sharing command. Most of the existing Medium Access Control (MAC) protocols for cognitive radio networks, such as the one proposed in (Timmers et al, 2010) require a dedicated global control channel named *Common Control Channel* (CCC). In fact, cooperative schemes envisage a CCC that creates a data bus to distribute sensing data reports among the various cognitive radio users. Cognitive radio users make use of a CCC to complete channel negotiations before any actual data transmission. Cooperation among spectrum sensing devices (Zhang et al, 2009) has been shown to offer various benefits including decrease in sensitivity requirements of the individual sensing devices. To stimulate cooperation among cognitive radio users, a CCC is needed to share spectrum information and coordinate the spectrum access.

However, according to (Kaligineedi et al, 2008) the performance of cooperative sensing schemes can be severely degraded if malicious users send false sensing data. Furthermore, spectrum sensing and data reports introduce vulnerabilities that malicious nodes can exploit to harm the cognitive radio network by preventing cognitive radio users from successfully accessing the spectrum band. For instance adversaries may emulate a primary user (Chen & Reed, 2008). Depending on the type the adversary we can categorise the different attacks into the following types: (i) malicious attacks where adversaries deter cognitive radio users from using the spectrum (Denial of Service attacks). Therefore the available bandwidth is affected and the scheduled services are disrupted, (ii) selfish attacks, i.e. when a cognitive radio user attempts to acquire access to spectrum with higher priority by deceiving other users. A selfish node can occupy the spectrum as long as he chooses. It is worth noting that a malfunctioning node could cause the same damage with a selfish or a malicious node.

According to the bibliography, a limited number of papers examine the case of secure spectrum sensing (Kaligineedi et al, 2008), (Chen et al, 2008). In the latter, authors discuss that when we defend spectrum-sensing protocols it will be reasonable to devise a robust method for validating the authenticity of a licensed signal. For example for verifying incumbent signals is simple to embed a signature in the signal. However, no alterations of the incumbent signals must be required to allow opportunistic spectrum access. The same authors explain methods of verifying an incumbent signal using the location of the transmitter and the received signal power level. In fact, they propose a transmitter verification method called *Localisation-based Defence* (LocDef) that verifies the authenticity of an incumbent signal by estimating its location and comparing it with the location of known incumbents. Although, authors highlight that their method is inefficient in a network where the nodes are mobile and lightweight.

According to the same work, dynamic spectrum sharing techniques treat all the cognitive sensing devices indiscriminatingly regardless of their sensing report. For example if a node transmits all the time false data, it would have been effective to detect the malfunction of that node than to accept its report. In (Kaligineedi et al, 2008) authors propose a methodology to detect and nullify the effect of malicious nodes when energy detection method is used by the spectrum sensing devices. Their methodology is limited to detect malicious devices which distribution differs from the underlying distribution of legitimate nodes. As the authors highlight, their simulation results do not consider very complex or intelligent malicious users. To the best of our knowledge the only work that proposes a framework that protects the CCC has been proposed in (Safdar & O'Neill, 2009). The authors propose a secure MAC protocol that guarantees authentication, integrity and confidentiality of the messages transmitted over a CCC. However, they do not assume clustering, their solution protects only MAC layer attacks and they assume that the participated nodes are not compromised.

3. Security Framework

We envisage to design and evaluate a security framework for cognitive radio users who opportunistically access spectrum bands. Solutions for secure spectrum sensing, secure communication with fusion centres and secure communications within a cognitive cluster will be proposed towards a unified security model for cognitive radio networks. In the following sections, we discuss a research case study, which clearly depicts how the security model can be applied in cognitive radio networks. Additionally, we describe in detail the specific parts of the aforementioned security framework.

3.1 Research Case Study

Our research case examines a scenario where a number of cognitive users (CU) intend to communicate using any available technology such as those depicted in Figure 1. In our devised scenario, the CU may seek services such as mobile multimedia download, wireless broadband access, online gaming, emergency support (which are in agreement with Ofcom's CR study (Ofcom, 2007) and (Politis, 2009), or to access the digital dividend bands, which will be freed up after the digital switchover (DSO) (Ofcom, 2009). These users are equipped with portable devices that support cognitive radio techniques such as spectrum sensing and are able to access a wealth of wireless interfaces opportunistically. By employing such functionality CUs are capable of detecting white spaces or spectrum holes. We have adopted the concept of clustering in order to group a set of cognitive users together that will cooperatively distribute the acquired spectrum sensing data over a common control channel (CCC). Each cluster is spearheaded by a cluster-head, which is a super node with high computational capabilities and high Quality-of-Service profile. To initiate the spectrum sensing phase, the cluster-head node communicates with the spectrum database of each technology's fusion centre to determine which frequencies, if any, are available in its location. Then, it notifies the CUs about the bands they have to sense in order to confirm their spectral availability. The reason of this procedure is twofold. First, the cluster-head should inform the CUs about which spectrum band might be available before the start of spectrum sensing and second each fusion centre could update its spectrum database with new results from the spectrum sensing at a later stage.

On the other hand, the communication of cognitive users with the cluster-head takes place over a common control channel (CCC). After the spectrum sensing phase, the CUs send their sensing data to the cluster-head. The latter contacts the fusion centre of each technology, which is responsible to receive all the sensing transactions and decides on the spectrum availability depending on the collected data. Each fusion centre is collocated or integrated with the AAA server and they are connected typically via a logical link in order to validate all the sensing data information sent by the cluster-head. It is worth noting that the cluster-head to any fusion centre communication is considered to be transparent to the whole operation of the cognitive architecture as is supported by seamless mobility among various heterogeneous infrastructures. We also need to stress here that seamless mobility among these infrastructures is considered technically viable in our study and will not be investigated further. Finally, it is worth stressing here that the cluster-head queries the AAA servers/ fusion centres of the different technologies to find the different values of QoS and pricing for the requested service and provides CUs with this information over the CCC. It is worth mentioning that each cluster head supports up to a certain number of CUs, depending on its processing power and availability.

3.2 Main functionalities

The aim of our security framework is to develop protocols that will allow secure spectrum sensing and secure exchange of data within a cognitive users cluster. Particular emphasis will be given on the following two objectives:

- To develop a secure methodology for spectrum sensing and communication with each spectrum database based on but not limited to cryptographic and hash algorithms and intrusion detection techniques.

- To define a reliable communication paradigm within a cognitive cluster by securing the common control channel (CCC) namely the path between the cluster-head and cognitive users.

The result of the above objectives will be a framework that will enable cognitive radio users to access safely and reliably any spectrum band in an opportunistic manner.

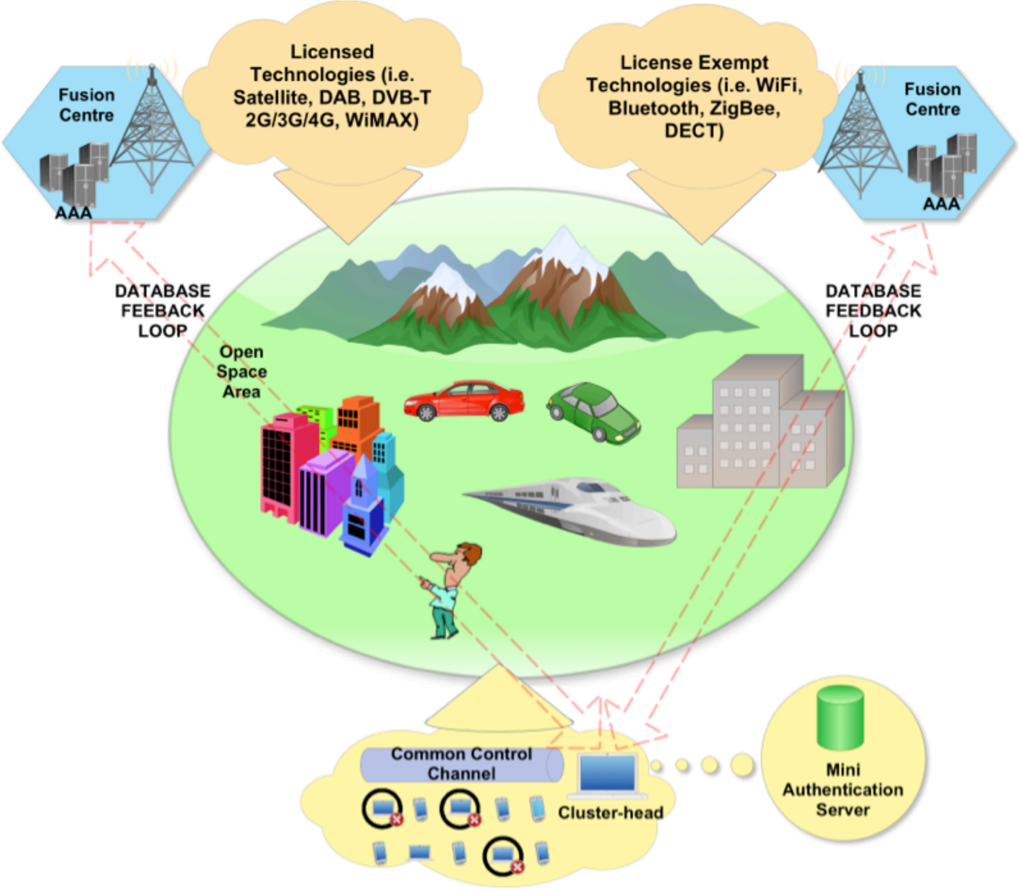
Fusion Centre
AAA
Licensed Technologies (i.e. Satellite, DAB, DVB-T 2G/3G/4G, WiMAX)
License Exempt Technologies (i.e. WiFi, Bluetooth, ZigBee, DECT)
Fusion Centre
AAA
DATABASE FEEBACK LOOP
DATABASE FEEDBACK LOOP
Open Space Area
Common Control Channel
Cluster-head
Mini Authentication Server

Fig 1. The research case scenario.

3.2.1 Secure spectrum sensing with spectrum database feedback

The initial objective towards the development of our security model is to select an “appropriate” spectrum sensing technique. The most crucial considerations when we select a spectrum sensing technique in our research hypothesis are the following. Cognitive devices are lightweight so they are designed to implement energy efficient and computationally simple methods. Needless to say, the power limitations of the sensing devices play a significant role for the spectrum sensing because each device has its own critical sensing data to report back to the fusion centre. For example if a sensing device runs out of power and this device was the only one that could sense the existence of a particular incumbent transmitter then the cluster-head may not have accurate information regarding the occupancy of the spectrum. This has the potential to happen due to the hidden node problem that has been studied extensively in the international bibliography (e.g. an accurate summary of the problem appears in (Politis, 2009)).

In fact, our goal is to secure the communication between the cluster-head and the spectrum databases and to secure a selected spectrum sensing technique used by the cognitive users within a licensed or license-exempt radio network. Before commencing spectrum sensing by the CU devices, the cluster-head has to contact the spectrum database of each technology and retrieve information about spectrum occupancy (temporal and spatial) within the geographical area of its cluster. Thus, the secure communication of the cluster-head with each fusion centre, which is included within the AAA architecture, is critical. Within this context a cluster-head is concerned about malicious nodes that can capture part of the transmitted information and alter it, or they can masquerade as a fusion centre or

AAA server. Our methodology will include but not limited to mutually authenticating the cluster head to a fusion centre and visa-versa and provide encryption, integrity and authentication for the communication between cluster-head and any fusion centre. However, the main objective is to explore the various potential vulnerabilities and attacks that may be launched against the spectrum sensing technique that the cognitive devices of our scenario use. We envisage that our methodology will guarantee that an adversary outsider and a limited number of compromised insiders cannot mislead cognitive users into using a non-vacant channel and interfere with a primary user or not using a vacant channel (Denial-of-Service attack). Our methodology will use a set of techniques that we call intrusion detection techniques, which will recognise the existence of one or more malicious activities within the licensed and/ or LE bands. The intrusion detection will be based either on the detection of a specific attacker's pattern (misuse or signature-based intrusion detection system) or on normal network traffic evaluations (statistical anomaly-based intrusion detection system).

3.2.2 Secure intra-cluster communication

After the spectrum sensing phase of our scenario, the cognitive users (CU) have to transmit their sensing data to a cluster-head node. By seeing that a cluster-head utilises the observations by all the CUs, there is an apparent need to authenticate the shared observations given the distributed and ever-changing nature of the network. Malicious nodes can impersonate legitimate nodes and report wrong information. In this case, a spectrum sharing technique will not make correct spectrum decisions disrupting in this way the accurate operation of the cognitive radio network. For example, it could modify the source IP address (IP spoofing) to pretend another node and thus could appear as part of the cluster. Then, it can advertise its spectrum sensing results claiming that it has sensed the existence of one or more incumbent nodes within the given licensed band. Goal of the malicious node is a denial-of-service attack and if it is successful the cognitive license-exempt (CU) nodes will not be granted with access to the licensed spectrum and communication with any other destination outside a cluster will be impossible.

The first thing we will guarantee is to establish trust among the cognitive users of a cluster and the cluster-head. In other words, the CUs will be authenticated, before they send the sensing data reports, by the cluster-head. In this way, their identity will be validated and the cluster-head plays the role of a 'mini' authentication server (let's call it authenticator). Obviously, a challenging issue that is emerging is the key management within a cluster. In the beginning of the network's life the different nodes will safely generate and securely exchange one or more cryptographic keys based on group key agreement algorithms. A key refresh mechanism must be provided to guarantee a safe long-term operation of the network using dynamic cryptographic keys. Once the authentication of a CU by the cluster-head has been accomplished the cluster-head will be able to realise whether the spectrum sensing information is originated from an authenticated node or not. In this context, the propagation of an attack's effect within the cognitive radio network is prevented. In addition, we will define a reliable communication paradigm for cognitive users by securing the common control channel. Our method will provide confidentiality, integrity and availability for the participated CU devices. According to our scenario, a malicious device has the potential to acquire important and confidential information about the spectrum sensing strategy of the cognitive users. If CUs effectively encrypt their data, any potential malicious node will have to apply specific techniques to break the security of the communication channel. This will cost him in energy consumption, which might be critical for its operation. Both symmetric (e.g. AES –Advanced Encryption Standard) and public-key cryptography algorithms (e.g. RSA – Rivest, Shamir and Adleman) will be used to encrypt transmitted data over a common control channel (CCC) towards a final comparison between the two types of cryptographic solutions in terms of energy consumption and security strength in the presence of adversaries. Apart from overhearing the communications, due to the broadcast nature of radio transmissions in our case, CCC is more susceptible to malicious traffic analysis. For this reason, we will include in our security model, an anonymity method to enable anonymous communications thus tackling the threat of traffic analysis. Likewise, malicious nodes may capture packets transmitted over the CCC and deliberately change the spectrum sensing information. They can also modify the source IP address (IP spoofing) to pretend another node thus the originator of a report can wrongly appear as malfunction. To avoid the stated above threats, integrity checksums will be used based on Hash Message Authentication Codes (HMAC). Within this context, the cluster-head will be able to realise if the received data is changed or it is exactly the same with the one that an originator transmitted. Generally speaking, we will investigate and design protocols that will be able to tackle different types of attacks launched against the CCC.

4. Conclusions

In this paper, we discuss our plans for a security model that will allow secure cognitive access in different spectrum bands (e.g. 2/3/4G, satellite, TV band, WiMAX, etc). We propose our envision for the future, which includes (i) secure spectrum sensing with spectrum database feedback and (ii) secure intra-cluster communication. We strongly believe that this discussion will stimulate thoughts about the aforementioned security model, which has the potential to be applied in many cases or real life scenarios such as extreme emergencies.

5. Future Work

Our plans for future work include but are not limited to developing the counterparts of the discussed security model and to test its security performance against well-known attacker models. The implementation it will be done by using programming tools such as NS/2-3, Matlab and C/C++ based simulators. We envisage that the security model or else toolkit will be proper to be adopted by the majority of CR devices that will be deployed when the era of cognitive radio networking arises.

5. References

Akyildiz, I., Lee W.Y. and Chowdhury, K., (2009), "*Spectrum management in cognitive radio mesh networks*", IEEE Network Magazine, Vol. 23, No. (4), pp6-12.

Chen, R., Park, J.M., Hou, Y.T. and Reed, J. H., (2008), "*Toward secure distributed spectrum sensing in cognitive radio networks*", IEEE Communications Magazine, Vol. 46, No. (4), pp50-55.

Chen, R., Park, J.M. and Reed, J.H., (2008), "*Defense Against Primary User Emulation Attacks in Cognitive Radio Networks*", IEEE Journal Selected Areas in Communications, Vol. 26, No. (1), pp25-37.

Hwang, C.H., Lai G.L. and Chen, S.C., (2010), "*Spectrum Sensing in Wideband OFDM Cognitive Radios*", IEEE Transactions on Signal Processing, Vol. 58, No. (2), pp709-719.

Kaligineedi, P., Khabbazian, M. and Bhargava, V.K., (2008), "*Secure Cooperative Sensing Techniques for Cognitive Radio Systems*", In Proceedings of the IEEE International Conference on Communications (ICC), pp3406-3410.

Mitola, J., (2000), "*Cognitive radio: an integrated agent architecture for software-defined radio*", PhD Dissertation, Royal Institute of Technology (KTH), Stockholm, Sweden.

Ofcom "Cognitive Radio Technology," A Spectrum Framework Review Study by QinetiQ Ltd, http://www.ofcom.org.uk/research/technology/research/emer_tech/cograd/cograd_main.pdf, February 2007.

Ofcom "Digital dividend: cognitive access," Consultation on licence-exempting cognitive devices using interleaved spectrum, http://www.ofcom.org.uk/consult/condocs/cognitive/cognitive.pdf, February 2009.

C. Politis, “Managing the radio spectrum,” Vehicular Technology Magazine, IEEE, vol. 4, no.1, pp. 20-26, March 2009.

Safdar, G.A. and O'Neill, M., (2009), “*Common Control Channel Security Framework for Cognitive Radio Networks*”, In Proceedings of the IEEE 69th Vehicular Technology Conference (VTC), pp1-5.

Srinivasa, S. and Jafar, S.A., (2007), “*Cognitive radios for dynamic spectrum access - the throughput potential of cognitive radio: A theoretical perspective*”, IEEE Communications Magazine, Vol. 45, No. (5), pp73–79.

Sun, C., Zhang, W. and Ben, K., (2007), “*Cluster-Based Cooperative Spectrum Sensing in Cognitive Radio Systems*”, In Proceedings of the IEEE International Conference on Communications (ICC), pp2511-2515.

Timmers, M., Pollin, S., Dejonghe, A., Van der Perre, L. and Catthoor, F., (2010), “*A Distributed Multichannel MAC Protocol for Multihop Cognitive Radio Networks*”, IEEE Transactions on Vehicular Technology, Vol. 59, No. (1), pp446-459.

Van, H. and Koo, I., (2009), “*An Optimal Data Fusion Rule in Cluster-Based Cooperative Spectrum Sensing*”, An Intelligent Computing Technology and Applications With Aspects of Artificial Intelligence, Vol. 5755/2009, ISBN: 978-3-642-04019-1, Springer Berlin / Heidelberg, pp708-717.

Younis, O., Kant, L., Chang, K., Young, K. and Graff, C., (2009), “*Cognitive MANET design for mission-critical networks*”, IEEE Communications Magazine, Vol. 47, No. (10), pp64-71.

Zhang, W., Mallik, R. and Letaief, K., (2009), “*Optimization of cooperative spectrum sensing with energy detection in cognitive radio networks*”, IEEE Transactions on Wireless Communications, Vol. 8, No. (12), pp5761-5766.