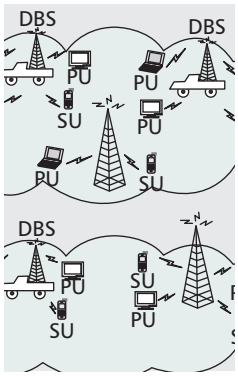
ACCEPTED FROM OPEN CALL

TOWARD SECURE COGNITIVE COMMUNICATIONS IN WIRELESS NETWORKS

TINGTING JIANG, VIRGINIA TECH
TONGTONG LI AND JIAN REN, MICHIGAN STATE UNIVERSITY



Wireless networks are challenged in efficiency and security. The authors present a fundamental study of cognitive communications in wireless networks after analyzing the limitations in today's cognitive radios.

ABSTRACT

Wireless networks are challenged in efficiency and security. This article is devoted to the fundamental study of cognitive communications in wireless networks after analyzing the limitations in today's cognitive radios. The research scope includes architecture design, resource management, anti-interference/interception system design through multi-layer diversity, routing anonymity, and security analysis.

OVERVIEW

Cognitive radio has been proposed as a promising technique to promote efficient wireless spectrum allocation [1]. The idea of cognitive radio is motivated by the observation that lots of licensed frequency bands in the spectrum are largely unoccupied or only partially occupied most of the time [2]. This under-utilization of the electromagnetic spectrum leads to the thought that: spectrum utilization can be improved significantly by making it possible for a secondary user (SU) to access a spectrum hole unoccupied by the licensed primary user (PU). In other words, the cognitive radio technique enables an SU to sense for spectral holes, and to transmit on the bands where the PU is idle or not fully active. Based on real-time spectrum sensing, cognitive radios are expected to "learn" about the surrounding environment and make self-adjustments to achieve dynamic spectrum access.

As an exciting concept, cognitive radio emphasizes the power or capability of the *individual* radio devices. While each individual cognitive radio can make flexible decisions, the lack of user coordination and network control raises serious issues in *security* and *efficiency*.

MAJOR CHALLENGES IN COGNITIVE RADIO

The major challenges in cognitive radio can be described from three aspects.

This work was partially supported by the U.S. National Science Foundation under grants CNS-0845812, CNS-1050326 and CND-1117831.

Serious Security Fragility — The essence of cognitive radio is real-time sensing and reuse of the PU's under-utilized spectrum on a non-interference basis. To do so, the SUs have to continuously monitor the spectrum usage of the PUs for spectrum utilization, which requires SUs to get full knowledge of the spectrum usage and behavior of the PUs. Spectrum sensing enables the SU to perform legitimate traffic analysis of the PU, including spectrum occupation, traffic volume, traffic pattern, and even traffic routing path. This is, in fact, a *security compromise* of the PUs on their spectrum utilization.

The idea of cognitive radio *violates* the fundamental security requirements of the PUs. The cognitive radio nature of the system introduces an entirely new suite of threats and tactics that are very challenging and not easily mitigated. Providing strong security may prove to be the most difficult aspect of making cognitive radio a long-term commercially-viable concept [3]. Unfortunately, the security of cognitive radio has received attention far less than is adequate. Malicious eavesdroppers or adversaries can invoke hostile jamming attacks, also known as Denial-of-Service (DoS) attacks, of the ongoing transmissions and paralyze effective communications. There are also new unique opportunities presented to the malicious attackers, leading to potentially devastating spoofing and integrity attacks that can influence both spatial and temporal behavior of the network. Unfortunately, these attacks are very difficult to prevent in the current cognitive radio network. There is an urgent need to restrain spectrum sensing and software driven mobile reconfiguration as network controlled operations.

Spectrum Manipulation — In cognitive radio, the locally observed information is used to construct a perceived environment. The information will impact both current and future behaviors of spectrum utilization. It requires the spectrum allocation of the PUs to be relatively static and predictable for the SUs. Therefore, no spectrum protection or unanticipated secure dynamic spectrum allocation would be possible. The unprotected spectrum utilization of the PUs allows the SUs as well as the attackers to manipulate the spectrum utilization of any PU and

1536-1284/12/$25.00 © 2012 IEEE

conduct spoofing attacks. In addition, both the attackers and the legitimate users can also manipulate the spectrum so that the malicious activities can be justified as erroneous due to inaccurate spectrum analyzing, and therefore, will not be punished.

Denial-of-Service (DoS) Attack — The unprotected spectrum utilization allows the SUs and the attackers to be able to distinguish the spectrum usage of each individual user. The attackers can jam any PU and perform DoS attacks due to the lack of authentication and access control mechanisms of local observers. It is true that virtually any wireless system is vulnerable to brute force DoS attacks through jamming. However, without protective spectrum allocation mechanisms in place, in cognitive radio, it can be trivial and extremely easy to jam any PU. The attacker can also adaptively occupy all the white spectrum based on spectrum analysis so that no other SUs can be accommodated.

Security and Privacy Compromise of the PUs — The requirement for cognitive radio to work is based on knowledge of the spectrum utilization of the PUs and also the SUs. This requires the spectrum usage of the PUs and SUs to be unprotected so that other SUs can perform spectrum sensing and analysis. In addition, to improve the spectrum usage efficiency, the spectrum allocation should follow a model that can be easy for the SUs to reuse the spectrum holes. These requirements are against the fundamental security principles and constitute a major privacy violation of the PUs in particular. In a cognitive radio environment, it is very challenging to regulate the identities of the SUs while enforcing spectrum security, and therefore, the PU privacy.

Spectral Inefficiency Due to Traffic Collisions — The current cognitive radio is analogous to flying an aircraft without relying on the air traffic controllers. Traffic collisions can happen between a PU and an SU, or between the SUs, regardless of the technology of spectrum analysis and sensor technologies, including, for example, some recently proposed spectrum sensing technologies [4]. In cognitive radio, ideally, when the frequency band is reclaimed by a PU, the SU(s) should evacuate immediately and move to other available spectrum holes for further transmission. However, without effective network control, the return of the PU cannot be fully predicted by the SU, and traffic collisions between the PU and the SU are therefore inevitable.

For the SU, there is no guarantee that another spectrum hole can be accessed by the SU for smooth transmission. When there are multiple active SUs in the system, the contention among the SUs also leads to traffic collisions. *Traffic collisions can cause transmission failures for both PUs and SUs, limit the spectral efficiency, and formulate a bottleneck for system capacity improvement*.

High Cost of Terminals — In cognitive radio, every individual terminal needs to perform continuous spectrum sensing, and be able to adapt to the unpredictable, ever changing environment. These operations require expensive hardware and software, which implies that the cost of each radio terminal will be high. Furthermore, continuous spectrum sensing and real-time decision making at every terminal cause significant resource waste, which is against the fundamental design criterion of modern wireless networks.

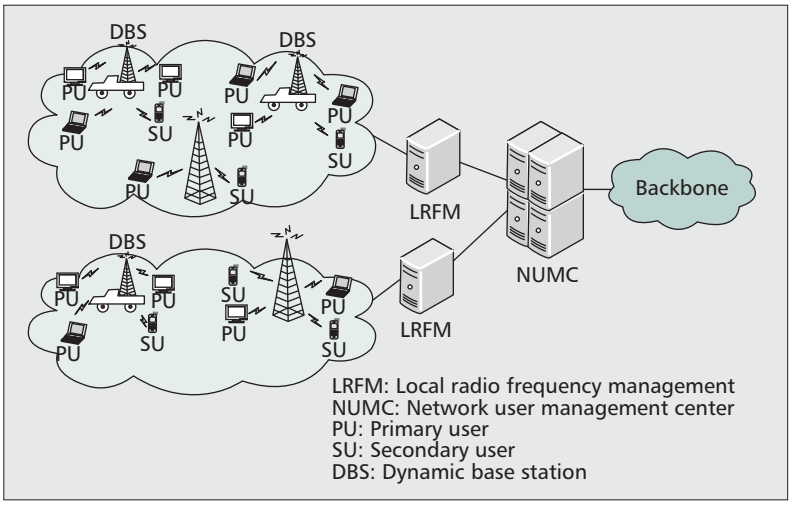


Figure 1. *Architecture of the proposed cognitive networks.*

Our Proposed Approach: Cognitive Networks

Based on the discussions above, we can see that even with empowered cognitive radios, there is still an obliged and urgent need for centralized network management. Allowing the radio devices to modify user services and reconfigure RF parameters can raise serious efficiency and security concerns for PUs, operators, and regulators. Therefore, mandatory network control has to be enforced. Motivated by these observations, in this research, we introduce the concept and architecture of *cognitive networks*.

By cognitive network, we mean an intelligent wireless system that can collect and analyze the current network conditions, and then make real-time changes to network operating parameters (e.g., modulation scheme, carrier frequencies, coding schemes, and security mechanisms) for optimal network performance. The overall goal is to ensure spectrally efficient and secure information exchange among versatile wireless devices, including both the legacy devices and the powerful software-defined radios (SDRs).

System Architecture

The proposed system architecture of a cognitive network is shown in Fig. 1. The main objectives of the proposed architecture are:

- To increase spectral efficiency and system reliability through collision-free spectrum sharing.
- To reconcile the conflict between spectrum reuse and communication security in wireless networks.
- To reinforce the system flexibility and scalability through dynamic BS deployment.

In the new architecture, we allow coexistence of fixed and dynamic BSs and introduce the con-

Dynamic BSs, such as vehicle mounted BSs, are connected with the LRFM through the airlink, and can easily be relocated based on the change of user population or traffic distribution. This architecture can be particularly useful in emerging scenarios.

cepts of Local Radio Frequency Management (LRFM) center and Network User Management Center (NUMC). All the users, both PUs and SUs, register with the NUMC to become authorized users. In wireless systems, one spectrum reuse region may contain one or more cells, and is generally referred to as a cluster. An LRFM is attached to each cluster. The LRFM is responsible for continuous spectrum sensing, and dynamic resource allocation for collision-free spectrum sharing among all the users within the cluster. Network management tasks, such as user authentication, access control, handover and accounting, are conducted by the NUMC, with assistance of the LRFM. While increasing spectrum efficiency and protecting the privacy of the PUs, this architecture also allows the SUs to use more feasible and cost efficient devices since they are no longer required to perform continuous spectrum-sensing. Moreover, the system flexibility and scalability are increased significantly by introducing vehicle mounted dynamic BSs into the fixed infrastructure.

In the following, we will explain how the system works within each cluster, and how the clusters are connected into a network.

- First, the subscribers register with the system through the NUMC. In reality, the system generally has some fixed PUs, like those involved in TV/radio broadcasting and public safety systems. All the other users access the network in a random manner. An authorized user can request PU service or SU service based on the user's need and resource availability at each communication event. PUs will be granted higher priority and higher Quality of Service (QoS), at a higher service cost. For a time sensitive signal, like a phone conversation, the user can claim itself as a PU. While for a less time sensitive and short delay tolerable signal, like transmitting a short message or email, the user can claim itself as an SU to get a better price deal.
- QoS for PUs will be divided into different levels, with a minimum information rate guarantee for all the PUs. PUs have higher priority for all the unassigned frequency bands. At the same time, the system can still support a considerable number of SUs due to the wide existence of spectrum holes or under-utilization.
- Spectrum allocation for all the users (including both PUs and SUs) within a cluster is managed by the LRFM attached to the BSs. Spectrum sensing of the PUs will be performed by the LRFM, and the detected spectrum holes are distributed among the SUs. Note that the LRFM can be equipped with advanced receivers and strong data processor and controller, and it also has the real-time information of the frequency band occupied by each PU. The LRFM can perform much more accurate spectrum sensing and highly efficient dynamic resource allocation. As a result, *transmission collisions can be completely resolved*, and each user terminal no longer suffers from the burden of continuous spectrum sensing and access frequency selection.
- When the user is moving from one cluster to another cluster, it will be handed over to the LRFM in the new cluster through the NUMC. The NUMC is also responsible for other network management tasks, including user authentication, access control, and accounting (for billing and record tracking purpose) etc.

Finally, we would like to point out that in addition to supporting dynamic resource management through network centric spectrum sensing and heterogeneous radio transmission, a major difference between the proposed architecture and the conventional centralized network is the coexistence of fixed BSs and dynamic BSs. Dynamic BSs, such as vehicle mounted BSs, are connected with the LRFM through the airlink, and can easily be relocated based on the change of user population or traffic distribution. This architecture can be particularly useful in emerging scenarios.

Dynamic Resource Management

Dynamic resource management for heterogeneous cognitive networks faces the coexistence of PUs and SUs, legacy mobiles and SDRs, fixed BSs and dynamic BSs, and various interferences, including hostile interference. In this article, we focus on spectrum management other than computing resource management.

Major Challenges

The study of cognitive radios has been focused on cooperative resource management through information exchange between the neighboring nodes. Due to the lack of network control, resource management tends to be difficult, complex, and inefficient. Moreover, the system efficiency and security may be further threatened because of selfish or hostile behaviors from malicious users. For a centralized network, the common radio resource management (CRRM) problem has been proposed under the 3GPP framework, and studied as a platform for coordination between heterogeneous components. The problem has also been studied based on the Fractional Brownian Motion [5], the Fractional Stable Motion, the theory of effective bandwidth, as well as traffic prediction techniques.

For dynamic resource management based on the proposed architecture, *the major challenges* lie in that:

- In addition to handling the coordination between PUs and SUs, legacy mobiles and SDRs, we have to cope with the coexistence of both fixed and dynamic BSs. While dynamic BSs introduce more flexibility into system design, they also raise significant challenges in resource management.
- We take both system induced interference and hostile jamming interference into consideration. When diversity based anti-interference/interception techniques are involved, resource management becomes much more difficult due to the requirement on frequency diversity and routing diversity.

In addition, practical parameters like service level, security requirement, operable frequency range, and data rate, etc., should also be taken into account through analytical modeling and analysis.

General Protocols

Note that each cluster has a LRFM, which is responsible for spectrum allocation of all the PUs and SUs in the cluster. Within each cluster,

the total available spectrum generally contains numerous frequency bands and services. For maximum spectral efficiency, we will rely on network-controlled software-defined radio (NC-SDR). The frequency shift and transmission rate variation of the mobile set are invoked or controlled by the LRFM. For a rather long period, there will be coexistence of NC-SDRs and legacy devices that can only be used at a fixed frequency band. Generally, legacy devices can only be registered as PUs due to the lack of flexibility, since SUs must be able to shift from band to band and allow variable transmission rates. The NC-SDRs are coordinated with the legacy devices for maximum frequency utilization according to the following rules:

NC-SDRs versus legacy devices: When a new user enters the system, the LRFM will first determine whether it is an NC-SDR or a legacy device. If it is an NC-SDR, the LFRM will assign it to the band with the lightest traffic load. If it is a legacy device, the LFRM has to assign it to its designed working band, and move the NC-SDRs to other bands if necessary. In practice, for maximum system capacity, telecommunication carriers often provide free upgraded mobile devices to the users to get rid of legacy mobiles.

PUs versus SUs: PUs have higher priority on unassigned bands over the SUs. Partially assigned bands are mainly assigned to SUs; a PU will be put on partially assigned bands only if the minimum required transmission rate can be guaranteed for the PU. Except for the fixed group of PUs (like TV and radio stations), a primary service request would be accepted only when the requested transmission rate can be ensured by the system; otherwise the user must be registered as an SU.

Network Capacity Evaluation and Cluster Size Control

We first estimate the network capacity from an information theoretic point of view, and then convert it to the capacity in terms of the number of users that can be supported by the system under a required QoS.

Based on Shannon's channel capacity theory, for an ideal additive white Gaussian noise (AWGN) channel (that is, a flat fading channel) of bandwidth B Hz, the channel capacity can be calculated as:

$$C = B\log_2(1 + SNR)\ bits/\text{sec},$$

where SNR is the signal-to-noise ratio. In wireless communications, due to the effect of multipath propagation, different frequency components of the transmitted signal generally experience different fading effects. In other words, we have to deal with non-ideal frequency selective channels, and we need to extend the results for the ideal channel to frequency selective channels. To do this, we divide the bandwidth into small bins of width Δf, where Δf is small enough that the channel transfer function is approximately constant over a range of Δf (see Fig. 2).

Let $H(2\pi f)$ denote the channel transfer function. Consider one of these subbands centered at frequency f_0; this subband is characterized with a flat gain of $H(2\pi f_0)$. At the same time, the additive noise can be considered to be white over the subband, assuming the noise power spectral density is $S_N(2\pi f_0)$. Suppose that there is a constraint on the average transmit power $E[X^2(t)] = P_s$, and let $S_X(2\pi f)$ be an appropriate input power spectrum that meets this constraint, then the capacity of this subchannel is given by

$$C(2\pi f_0) = \Delta f \log_2\left(\frac{S_X(2\pi f_0)\left|H(2\pi f_0)\right|^2}{S_N(2\pi f_0)}\right) \text{b/s}.$$

The total capacity is then the sum of the subchannel capacities, which becomes an integral in the limit of $\Delta f \to 0$,

$$C = \int_0^\infty \log_2\left(1+\frac{S_X(2\pi f)\left|H(2\pi f)\right|^2}{S_N(2\pi f)}\right) df \text{ b/s}.$$

Based on this result, we can evaluate the network capacity for various multiple access systems, including hybrid TD-FDMA, CDMA, and OFDMA. The underlying argument is based on the trunking theory: the spectral efficiency of the network will be increased significantly as the number of available channels increases. The capacity region needs to be further examined by taking packet transmission into consideration, since every time a transmission failed, the whole packet will be retransmitted. The position of the users in the cell should also be considered for capacity evaluation, as the signal power fades significantly as the mobile travels farther from the BS.

Once the network capacity is evaluated, the total number of users that can be supported will be estimated under the required QoS, including data rate, the probability that a call is blocked, and the average delay for queued calls. With these results, cluster size control or the frequency reuse spectrum management plan can be carried out through appropriate transmit power adjustment.

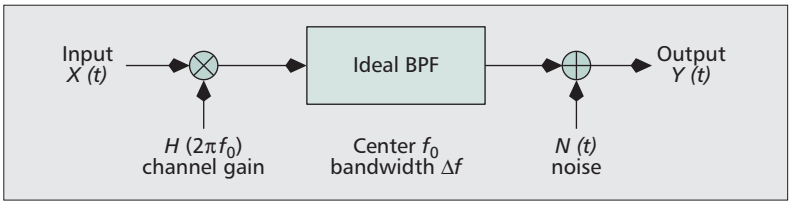


Figure 2. *Channel model for capacity calculation.*

Equal Average Load Criterion

In the proposed cognitive network architecture, the LRFM is spectrum aware. It maintains a real-time spectrum usage distribution for all the frequency bands (an example is shown in Fig. 3). The spectrum is divided into three categories: white spectrum, gray spectrum, and black spectrum. White spectrum denotes the spectrum that is unassigned, or not allocated to any users; gray

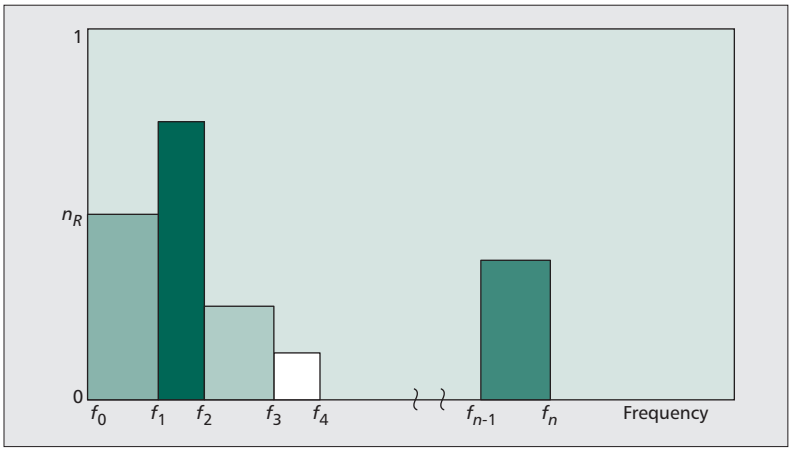


Figure 3. *Relative traffic load.*

spectrum denotes the spectrum that is assigned to a user (generally a PU), but is not fully utilized; black spectrum denotes the spectrum that is fully occupied and utilized by a PU. For numerical characterization, we introduce the concept of *relative traffic load*, which is defined as:

$$\eta_R = \frac{\text{Active traffic over the band}}{\text{Total band capacity}}.$$

Clearly, $0 \le \eta_R \le 1$, $\eta_R = 0$ for white spectrum, $\eta_R = 1$ for black spectrum. η_R is measured in Erlangs. In order to optimize the system performance, we propose to distribute the traffic uniformly among all the available bands based on the water-pouring criterion, so that a constant average load is maintained over different bands. We name it as the *equal average load criterion*. The realization of this criterion needs to be investigated jointly with dynamic user assignment based on the corresponding multiple access schemes and channel state information.

Dynamic User Assignment Based on Channel State Information

For a passband channel centered at f_0 with bandwidth BHz, if the channel transfer function is $H(2\pi f)$, then the channel capacity is given by

$$C = \int_{-B/2}^{B/2} \log_2 \left(1 + \frac{S_X(2\pi(f+f_0)\left|H(2\pi f + f_0)\right|^2}{S_N(2\pi(f+f_0))}\right) df \text{ b/s}.$$

We can see that if the signal power spectral density $S_X(2\pi f)$ and noise power spectral density $S_N(2\pi f)$ are fixed, a larger $H(2\pi f)$ will result in a larger capacity. That is, when more than one user (assuming the same priority) are considered for a particular band, the user with the strongest channel gain should be chosen for transmission. This problem becomes NP-complete when there are numerous users and a large amount of available channels. Some interesting research issues include:

- Design of suboptimal but less complex solutions for a fixed system with M users and N channels.
- Study the scenario that the users in the system come and go following a Poisson distribution and explore how the system should react to the changes in the user population.

Dynamic Base Station Deployment

In emergency scenarios, the user population and the traffic flow in a particular area can change dramatically. Communications based on fixed infrastructure may become invalid due to severe traffic congestion and possible damage or disability of fixed BSs; in this case, dynamic BS deployment is particularly important.

The dispatch or deployment of dynamic BSs can be studied from the following research aspects:

- Dynamic cluster size control: Once the traffic request in a cluster is beyond the network capacity, new BSs should be deployed to split the original cluster into subclusters.
- Maximum coverage: When the number of dynamic BSs is fixed, optimum organization and relocation of the BSs should maximize the coverage and overall network throughput.
- Anti-interference and anti-interception: In the case when hostile interference is a threat, the careful deployment of dynamic BSs can provide sufficient routing diversity to ensure robust communication under hostile environment. Moreover, it also allows anonymous routing and protects the identities of source destination pairs.

Anti-Interference/Interception System Design through Multi-layer Diversity

Two major threats to reliable transmission in cognitive networks are interference and unauthorized interception/detection. There are two kinds of interference in wireless networks: self interference caused by the system, and hostile intentional jamming interference launched by adversaries. Existing anti-interference and anti-interception systems, including CDMA systems and frequency hopping systems, rely heavily on rich time-frequency diversity over large spectrum. Mainly limited by multiuser interference and/or collision effects, the spectral efficiency of existing anti-interference and anti-interception systems are very low due to inefficient use of the large bandwidth. In conventional FH systems, for example, each user hops independently based on its own PN sequence; a collision occurs whenever two users transmit over the same frequency band. When there is a collision, it is reasonable to assume that the bit-error-rate becomes 50 percent. Mainly limited by the collision effect, the spectral efficiency of conventional FH systems is very low.

While existing systems work reasonably well for voice centric communications, which only requires relatively narrow bandwidth, their low spectral efficiency can no longer provide sufficient capacity for today's high speed multimedia wireless services, and the problem becomes even more complex when multi-hop is involved in the transmission process. The major challenges here are:

- How to design cognitive systems that are highly efficient and at the same time have excellent anti-interference/interception features?
- How to ensure robust multi-hop communication under a hostile environment?

Anti-Interference System Design with Routing Diversity

FH achieves jamming resistance through frequency diversity. Motivated by the observation that the efficiency of conventional FH is mainly limited by the collision effect, we propose a network centric collision-free frequency hopping scheme based on the secure carrier assignment algorithm. The proposed secure subcarrier assignment algorithm is based on the advanced encryption standard (AES) [6] to ensure that:

- Each user hops to a different set of subcarriers in a pseudo-random manner at the beginning of each hopping period.
- At each hopping period, different users always transmit on non-overlapping sets of subcarriers and hence are collision-free.

To further improve the spectral efficiency and enhance the anti-interference property, we considered space-time coded collision-free frequency hopping based on the orthogonal frequency division multiple access (OFDMA) framework. We have shown that for frequency selective fading channels, *the efficiency of the proposed CFFH system can be more than 10 times higher than that of the conventional FH* [7]. In addition to PHY jamming resistance techniques, we now propose to combat random jamming through routing diversity.

Consider an example where a message needs to be sent from node S to node D through three hops (see Fig. 4). If there are only two nodes, A1 and B1, between S and D, then there is only one routing path. If we add two more relay nodes, say A2 and B2, there will be four paths if the message has to be sent in three hops, six paths for the message to be sent in four hops, and two more paths for the message to be sent in five hops. Altogether, there are 12 different routing paths if the message is allowed to be sent in up to five hops.

Anti-Interference/Interception through Routing Anonymity

While routing diversity can maximize the possibility for successful message transmission, it also induces high overhead and may not be feasible for resource constrained environments. An alternative approach is to maximize the probability of successful message transmission, while minimizing the communication overhead through routing anonymity based anti-interference/interception techniques. This is achieved by making the active routing path indistinguishable from all the possible routing paths to the adversary. When multiple routing paths are available, the adversary is unable to determine the active routing path and the active message packets. In this case, unless the adversary launches interference or jamming over all the routing paths, communications may still be conducted free of interference. As an example, in Fig. 4, between node S and node D, there are many possible routing paths. If the adversary tries to intercept in the route $S \leftrightarrow A_2 \leftrightarrow B_2 \leftrightarrow D$, the communications between S and D can still be continued through one of the routing paths from $S \leftrightarrow A_1 \leftrightarrow B_1 \leftrightarrow D$, $S \leftrightarrow A_1 \leftrightarrow B_2 \leftrightarrow D$, and $S \leftrightarrow A_2 \leftrightarrow B_1 \leftrightarrow D$.

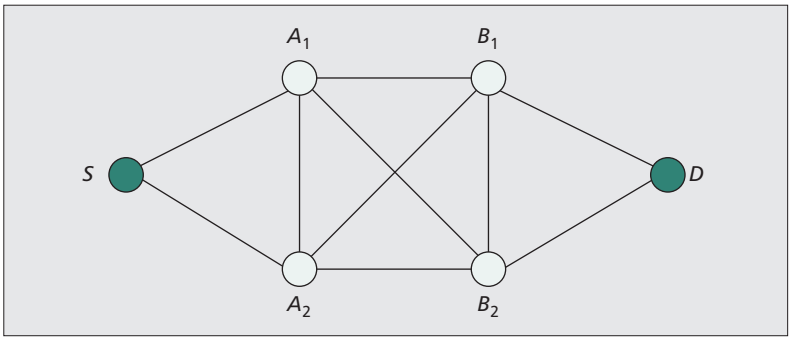


Figure 4. *Routing diversity.*

Anonymous communication can also be achieved through anonymous authentication [8] between two parties in the sense that each party only reveals its group membership to the other party in the same group, while no other parties are able to recognize information about the communications between these two parties.

We assume there is an administrator who assigns each party A a set of pseudonyms $\mathcal{N}_A = \{\mathrm{id}_1^A, \cdots, \mathrm{id}_\tau^A\}$, and a corresponding *secret set* $S_s = \{g^{sG^h}(\mathrm{id}_1^A), \cdots, g^{sG^h}(\mathrm{id}_\tau^A)\}$, where τ is a large security parameter, s_G is the group's secret and h is a collision-resistant cryptographic hash function, mapping arbitrary inputs to fixed-length outputs on $\mathbb{Z}_p$, e.g., SHA-1. The pseudonyms will be dynamically selected and used to substitute the real IDs in each communications. The anonymous authentication between A and B can be perform through three steps:

- A randomly selects an unused pseudonym id_i^A and a random nonce N_1, then sends id_i^A and N_1 to user B.
- B randomly selects an unused pseudonym id_j^B and a random nonce N_2, then sends id_j^B, N_2, and $V_0 = h(K_{BA} \| \mathrm{id}_i^A \| \mathrm{id}_j^B \| N_1 \| N_2 \| 0)$ to user A, where $K_{BA} = g^{sG^h(\mathrm{id}_i^A)\cdot h(\mathrm{id}_j^B)} \bmod p$.
- A sends $V_1 = h(K_{AB} \| \mathrm{id}_i^A \| \mathrm{id}_j^B \| N_1 \| N_2 \| 1)$ to user B, where $K_{AB} = g^{sG^h(\mathrm{id}_j^B)\cdot h(\mathrm{id}_i^A)} \bmod p$.

Since $K_{BA} = g^{sG^h(\mathrm{id}_i^A)\cdot h(\mathrm{id}_j^B)} \bmod p = g^{sG^h(\mathrm{id}_j^B)\cdot h(\mathrm{id}_i^A)} \bmod p = K_{AB}$, A can verify V_0 by checking whether $V_0 \stackrel{?}{=} h(K_{AB} \| \mathrm{id}_i^A \| \mathrm{id}_j^B \| N_1 \| N_2 \| 0)$. If the verification succeeds, then A knows that B is an authentic group peer. Similarly, B can verify A by checking whether $V_1 = h(K_{BA} \| \mathrm{id}_i^A \| \mathrm{id}_j^B \| N_1 \| N_2 \| 1)$. This means that party A and party B can know each other's group membership only if they both belong to the same group.

Security of the Proposed Cognitive Networks

The security of the cognitive networks become very typical and much easier to address. Many existing security techniques can be easily adapted. The multiple access techniques, such as

In addition to dynamic spectrum assignment, the combination of multi-layer diversity, routing diversity, and anonymity make it very difficult for adversaries to link spectrum allocations of each end user based on the intercepted information over the air.

TD-FDMA, CDMA, and OFDMA [9], can be used in the network for spectrum allocation. Each multiple access technique will result in a different spectrum sharing algorithm and protocol. When the frequency-hopping (FH) technique is involved for security purposes, spectrum allocation will be more dynamic and challenging. In fact, in a FH system, each user will hop to a different frequency band(s) after a hopping period. The hopping period is comparable with the symbol period in slow hopping systems, and it is smaller than the symbol period in fast hopping systems.

While eliminating communication collision and increasing spectrum efficiency, dynamic spectrum allocation can also effectively prevent the adversaries from tracking the spectral usage and perform traffic analysis of each individual user. In this way, the spectral usage information of both the PUs and SUs can be entirely controlled by the LRFM; therefore, the communication privacy of both the PUs and the SUs can be guaranteed. The spectrum privacy of each end user can also prevent DoS attacks and spectrum manipulation of any users since the end user spectrum will no longer be available to the adversaries.

In addition to dynamic spectrum assignment, the combination of the aforementioned multi-layer diversity, routing diversity, and anonymity make it very difficult for adversaries to link spectrum allocations of each end user based on the intercepted information over the air. Through efficient anonymous authentication schemes, the recovery of the end user information from the intercepted communication over the air can be made computationally infeasible.

Conclusion

In this article, we first analyzed the limitations of the current cognitive radio networks. We then delineated the open issues that cannot be easily resolved in the cognitive radios. These issues include serious security fragility, inevitable traffic collision, low spectrum efficiency, and expensive individual user cost, etc. Next, we proposed a system architecture of cognitive networks, which is an intelligent wireless system that can collect and analyze the current network conditions and then make real time changes to network operating parameters for optimal network performance. We described the anti-interference/ interception system design techniques through multi-layer diversity to increase security and prevent DoS attacks of the individual users. We also presented dynamic resource management techniques to increase the network performance of the proposed architecture. We hope this article will open up an alternative approach to tackle the spectrum shortage problem and find the silver lining of the cloud.

References

[1] S. Haykin, "Cognitive Radio: Brain-Empowered Wireless Communications," *IEEE JSAC*, vol. 23, no. 2, Feb. 2005, pp. 201–20.

[2] T. Hou, Y. Shi, and H. Sherali, "Spectrum Sharing for Multi-Hop Networking With Cognitive Radio," *IEEE JSAC*, vol. 26, no. 1, Jan. 2008, pp. 146–55.

[3] J. Burbank, "Security in Cognitive Radio Networks: the Required Evolution in Approaches to Wireless Network Security," *CrownCom*, 2008, pp. 1 – 7.

[4] R. Chen and J. Park, "Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks," *IEEE SECON*, Reston, VA, USA, Sept. 25–28, 2006.

[5] I. Norros, "A Storage Model with Self-Similar Input," *Queueing Syst.*, vol. 16, no. 3–4, 1994, pp. 387–96.

[6] L. Lightfoot *et al.*, "Secure Collision-Free Frequency Hopping for OFDMA based Wireless Networks," *EURASIP J. Advances in Signal Processing*, 2009, DOI: 0.1155/2009/361063, 2009.

[7] T. Li, Q. Ling, and J. Ren, "A Spectrally Efficient Frequency Hopping System," *2007 IEEE Global Telecommun. Conf.*, Washington D.C., Nov. 2007.

[8] J. Ren, T. Li, and K. Han, "Anonymous Communication Protocol in Overlay Networks," *Proc. IEEE Int'l. Conf. Commun. (ICC)*, 2008.

[9] D. Kivanc, G. Li, and H. Liu, "Computationally Efficient Bandwidth Allocation and Power Control for OFDMA," *IEEE Trans. Wireless Commun.*, vol. 2, no. 11, Nov. 2003, pp. 1150–58.

Biographies

TINGTING JIANG [S'11] received her B.S. degree (Summa Cum Laude) in Computer Science from Virginia Tech, Blacksburg, VA, in 2007. During 2007-2009, she was a Software Engineer at Intrexon Corp., Blacksburg, VA. Currently, she is pursuing a Ph.D. degree in Computer Science at Virginia Tech, Blacksburg, VA. She is a recipient of NSF Graduate Research Fellowship (2011–2014) and a Microsoft Research Graduate Women's Scholarship (2011). Her research area is in wireless security, with a current focus on security in cognitive radio networks.

TONGTONG LI [SM'08] (tongli@egr.msu.edu) received her Ph.D. degree in Electrical Engineering in 2000 from Auburn University. From 2000 to 2002, she was with Bell Labs, and had been working on the design and implementation of 3G and 4G systems. Since 2002, she has been with Michigan State University, where she is now an Associate Professor. Her research interests fall into the areas of wireless and wired communications, wireless security, information theory and statistical signal processing. She is a recipient of a National Science Foundation (NSF) CAREER Award (2008) for her research on efficient and reliable wireless communications. She served as an Associate Editor for IEEE Signal Processing Letters from 2007–2009, and as an Editorial Board Member for EURASIP Journal Wireless Communications and Networking from 2004-2011. Since 2012, she has been serving as an Associate Editor for IEEE Transactions on Signal Processing.

JIAN REN [M'98, SM'09] (renjian@egr.msu.edu) received his Ph.D. degree from the Xidian University in 1994. Currently, he is an Associate Professor in the Department of Electrical and Computer Engineering at Michigan State University. Prior to joining MSU, he was the Leading Secure Architect at Avaya Lab, Bell Lab and Racal Datacom in security architecture and solution development. His research interests include network security, wireless security, secure and energy efficient wireless sensor network protocols, cryptographic primitives, information forensics, network management, error-control coding and digital copyright protection. He received the National Science Foundation (NSF) CAREER award in 2009.