This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2011 proceedings

# Spectrum Stealing via Sybil Attacks in DSA Networks: Implementation and Defense

Yi Tan, Kai Hong
Department of ECE
Stevens Institute of Technology
Hoboken, NJ
Email: {ytan, khong@stevens.edu}

Shamik Sengupta
Department of Math. & Comp. Sci.
John Jay College of Criminal Justice
CUNY, New York, NY
Email: ssengupta@jjay.cuny.edu

K.P. Subbalakshmi
Department of ECE
Stevens Institute of Technology
Hoboken, NJ
Email: ksubbala@stevens.edu

***Abstract*—In this paper, we investigate Sybil attacks on spectrum allocation in distributed dynamic spectrum access (DSA) networks. Using IEEE 802.11 devices as secondary nodes, we demonstrate the feasibility of mounting Sybil attacks in the cognitive radio testbed, in which the malicious node poses as multiple good secondary nodes with different identities in order to steal more spectrum bands. We also show the impact of the attack through an example and simulation results. A defense strategy using the statistics of beacon intervals is also proposed. Through experimental results, we show the effectiveness of the defense mechanism when there is no interference from external sources as well as in the presence of interference.**

## I. Introduction

The conventional spectrum management policy, which results in over-utilization in some bands and under-utilization in others, has been demonstrated to be inefficient. This observation has led the Federal Communication Commission (FCC) to initiate the recent spectrum policy reform [1]. The new dynamic spectrum access (DSA) paradigm allows unlicensed secondary nodes to opportunistically use free licensed spectrum frequencies as long as causing no interference to the licensed primary users [2]. Cognitive radio (CR) [3] is expected to make DSA a reality. Unlike conventional radios, CRs can adjust transmission/reception parameters based on interaction with the environment, find the best available spectrum bands and vacate promptly upon sensing the return of primary users.

While other aspects of DSA/CR networks have received significant attention in recent years, research in the area of DSA network security is still emerging [4], [5]. Due to the lack of comprehensive security standards and specific attack prevention protocols, DSA networks are highly vulnerable to various malicious threats, e.g., denial-of-service (DoS) attacks. Particularly, due to the open paradigm, interoperability and dynamic nature of CR devices, the environment of DSA networks is continuously varying and thus, the identity authentication becomes a challenge. Hence, DSA networks are highly susceptible to identity attacks like the Sybil attack.

In a Sybil attack, originally introduced by Douceur in the context of peer-to-peer network [6], a physical malicious node takes on multiple identities and behaves as multiple distinct nodes (called Sybil nodes) in the system. In the worst case, one physical malicious node may generate an arbitrary number of additional identities. Sybil attacks in the context of sensor networks were systematically analyzed in [7], where several forms of Sybil attacks to perturb or compromise sensor network protocols were discussed and some potential defense strategies were proposed. One strategy to defend against Sybil attacks is based on localization [8], [9], where received signal strengths are used to verify the transmitting nodes' positions. However, CR secondary nodes are dynamically changing locations and thus such defense is infeasible in DSA networks. The concepts and techniques from social networks have also been applied to distinguish honest and Sybil nodes [10], [11]. However, these methods requires every node to establish a trust system for all other nodes, which leads to much overhead in computation and communication for CR devices. To the best of our knowledge, this work is the first attempt to understand Sybil attacks in DSA networks. Since there are lots of new functionalities exclusively developed for CR devices [2], investigating Sybil attack in terms of both its feasibility and impact is critical.

In this paper, we study the impact of Sybil attacks on distributed spectrum allocation and propose some defense mechanisms against it. We implement the Sybil attack using IEEE 802.11 devices in our CR testbed, SpiderRadio [12]. In our implementation, one malicious node registers itself as multiple nodes by sending beacon frames embedded with different identity information to its neighboring nodes within interference range. Through an illustrated example and simulation, we show the degradation in fairness of bandwidth allocation caused by the Sybil attack. In order to mitigate the Sybil attack, a defense strategy is proposed using anomalies in beacon transmissions of Sybil nodes. We explore the statistics of beacon intervals on the receiver's side to differentiate between the beacon frames sent from the Sybil nodes and nodes. Both hardware and software based methods for generating beacons frames with multiple identities are considered. The testbed experiments are conducted under no interference from external sources as well as in the presence of interference. Results show that the beacon frames sent from Sybil nodes can be identified with high detection probability for both the software and hardware based methods.

The rest of the paper is organized as follows. The system model is discussed in Section II. In Section III, we demonstrate the implementation feasibility of the Sybil attack and present

978-1-61284-231-8/11/$26.00 ©2011 IEEE

an illustrative example as well as simulation results to show the impact of the attack. In Section IV, a defense strategy is proposed and demonstrated effective through experimental results. The conclusions are drawn in the last section.

## II. System Model

### A. Sybil Attacks in DSA networks

Providing the security support for distributed DSA networks is particularly challenging for several reasons: (a) Distributed DSA networks are susceptible to attacks ranging from passive eavesdropping to active interfering, frequent break-ins by adversaries due to their open, ubiquitous and interoperable nature; (b) They are highly "mobile" in frequency and location [13]; (c) Due to the open source nature of DSA networks, it is practically impossible to establish a standard database to record the identity information for every CR node [4]. Thus, in a distributed DSA network without a trusted central entity, it is difficult for independent secondary nodes to verify the authenticity of identities of their neighboring nodes and so, Sybil attack is a serious security threat.

Sybil identities can be used in different types of attacks. For example, if sufficient number of Sybil identities are created in a system, they can easily "out vote" good secondary users in major decision making processes. Sybil nodes can be used to mount a Byzantine attack against collaborative spectrum sensing protocols. Sybil nodes can also be used to capture unfair spectrum shares. We study this aspect in greater details.

### B. Problem Formulation

We consider a distributed overlay DSA network within a geographical region where $N$ secondary nodes are competing for limited available spectrum bands. We follow a simple interference model wherein the transmissions between neighboring secondary nodes fail if they are within certain distance of each other and use the same frequency band or overlapping frequency bands. Thus, the spectrum allocation can be modeled as a distributed graph coloring problem.

We define an undirected graph $G = \{V, E, G\}$. $V$ represents the set of vertices denoting all secondary nodes in the network. $E$ is the set of all undirected edges and every edge denotes the interference constraint among two adjacent nodes, i.e., if any two distinct vertices have an edge in between them, they are at risk of interfering each other if using the same frequency band for transmission. $G$ represents the total number of colors filling the entire graph. The optimal graph coloring problem is known to be NP-hard in searching and NP-complete in decision. Without loss of generality, we apply the multi-coloring algorithm proposed in [14], which provides both efficient spectrum utilization and good fairness[1].

Furthermore, we assume that there exists one or more malicious nodes that want to acquire spectrum bands unfairly. These malicious nodes generate some virtual Sybil nodes, each associated with an unique counterfeit identity and capable of behaving as a normal secondary node from the perspective of other nodes. To maximize the individual spectrum occupancy, the malicious node tries to capture as much spectrum as possible using Sybil nodes. In the next section, we will discuss how the malicious node launches Sybil attacks and implement it in our CR testbed.

[1]Note that other graph coloring algorithms could also be used and are not the focus of this work.

## III. Implementation of Sybil Attacks in CR Testbed

### A. System Setup

We use Soekris Net-5501 board, shown in Fig. 1, as the motherboard in our testbed, which is equipped with AMD Geode LX CPU with X86 architecture and running Linux 2.6 operating system. We also apply a patch in the kernel to implement the watchdog protocol, which makes the system work regularly. The wireless network interface cards (WNICs) equipped with Atheros chipset[2] are provided by Ubiquiti Network Inc. The device driver for this chipset is Madwifi[3] which we modify to generate Sybil attacks. We set this board as a CR secondary node equipped with two separated WNICs. One is used for broadcasting its own service set identifiers (SSID). The other is used as a "monitor", in which we modify the Madwifi to capture all the beacon frames from the air, and also record both the timestamps from these beacon frames and local hardware timestamps in the receiver's wireless chipset.

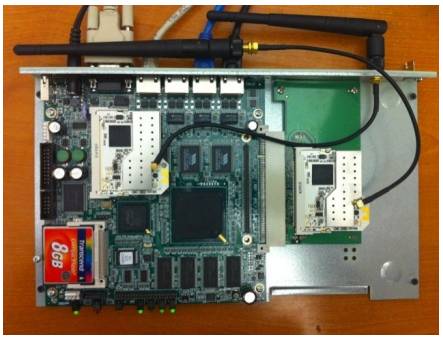

Fig. 1. The Soekris Net-5501 board.

### B. Implementation of Sybil Nodes

In the experiment, we consider that the secondary node sends beacon frames to its neighboring nodes within the interference range to claim the interference constraint. For example, if node $X$ receives a beacon frame from node $Y$, $X$ and $Y$ are connected by an edge in the graph topology. The standard 802.11 frame is composed by components tuple {Preamble, PLCP header, MAC data with CRC} [15].

In Madwifi, beacon frames transmission can be done either by hardware or by software. Both methods can be applied to create multiple SSIDs in our testbed. Our chipsets from Atheros support up to 64 SSIDs for one physical device. In our experiment, we implemented both hardware based and software based techniques for the malicious nodes to generate beacon frames with different SSIDs.

[2]Refer to: http://www.atheros.com/

[3]Refer to: http://madwifi-project.org/

In general, there are two stages to maintain a SSID, i.e., beacon frame generation stage and beacon frame transmission stage. The beacon frame generation is the same in both hardware and software based methods. To generate a beacon frame, the control field in the MAC header for the malicious node should be set properly (e.g., type field: 00; subtype field: 1000). Moreover, we set a distinct MAC address, SSID field and beacon interval field in each frame body. These fields must contain information that will be verified valid by the receiver. A set of acceptable values for these fields can be obtained by capturing SSID information from the air in other places using Wispy DBxs[4]. Then, each beacon frame is sent to the neighboring normal secondary nodes within the hearing range. At this point, the malicious node successfully generates several Sybil nodes with multiple identities.

The differences between software based and hardware based methods mainly are in the beacon frame transmission stage. In the hardware based method, three timers are used in a chipset, i.e., the target beacon transmission time (TBTT), software beacon alert (SWBA) and direct memory access (DMA) beacon alert (DBA). SWBA fires first, which generates an interrupt to notify the host to generate the beacon frame, and set this frame in pre-mapped DMA memory. DBA is fired next, which initiates the transmission of the prepared beacon frame from the host's DMA memory to chipset's hardware memory. Finally, TBTT is fired and the frame is transmitted into the air at the exact time following 802.11 timing protocol. Managed by this policy, beacon frames could be transmitted with highly accurate timing. However, not every chipset supports this policy. Hence, we also implement software based method in Madwifi, in which only one timer is used in the operating system. Every time the timer is fired, a beacon frame is attached to the queue for transmission. Hence, software based solution cannot guarantee accurate timing of transmission. In the next section, we will propose a defense mechanism via timing detection method to classify the SSIDs from normal nodes and Sybil nodes for both hardware and software based attacks.

If the transmission powers of the beacon frames from all Sybil identities are the same, it is possible for the receivers to suspect the source of these beacon frames. Hence, we apply per-packet transmission power control to send beacon frames with different power levels. This can be done in two steps. Firstly, we attach the flag "$\mathrm{hal_{tpc}}$" when we load Madwifi into memory. This flag is used to enable/disable (set to 1/0) the transmission power control function. Then, we set a different transmission power for each frame. Particularly, for Atheros chipset, a separated $tx$ descriptor in Madwifi is assigned for every frame and related parameters (i.e., transmission power and modulation mode) for this transmission are set up in this descriptor. Hence, we just need to setup power level in it and the frame will be sent with the specified power.

As a result, the neighboring secondary nodes will receive many beacon frames with different identity information and received signal strengths and erroneously think that they are from different physical nodes, whereas in reality some of these are from virtual Sybil identities.

[4]http://www.metageek.net/products/wi-spy

### C. Illustrative Example and Simulations

As an example, we set up 4 physical CR nodes in our testbed and assume that they share a certain size of spectrum bandwidth. As shown in Fig. 2, each color indicates an allocated spectrum for a particular CR node and the number of sub-bands is determined by the total number of colors used in the graph coloring process.

Firstly, we consider the case without Sybil attacks. Based on the experiment setup, the topology and graph coloring result are shown in the left hand side (LHS) figure in Fig. 2. There are totally three different colors in Fig. 2. Nodes $A$, $C$ and $D$ are assigned one color and node $B$ is assigned two colors, which indicates that $A$, $C$ and $D$ get 1/3 of the entire spectrum bands and node $B$ gets 2/3 of the entire spectrum bands. Then, we consider node $A$ as a malicious node which generates two Sybil nodes $A1$ and $A2$ following the steps described in the previous subsection. In order to maximize the spectrum occupancy, the malicious node controls nodes $A1$ and $A2$ to claim interference constraints to all other normal secondary nodes within its interference range. Thus, the topology and graph coloring result changes as shown in the right hand side (RHS) of Fig. 2. As illustrated, there are five different colors in the graph, in which the malicious node $A$ (together with two Sybil nodes) is assigned three colors and can obtain 3/5 of the entire spectrum bands. Therefore, by launching Sybil attacks, the malicious nodes can acquire more spectrum bands than other nodes, which will result in inefficient and unfair spectrum allocation.

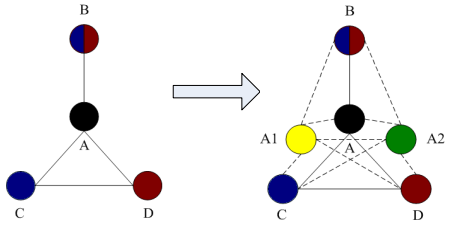


Fig. 2. The graph topology and coloring for all the secondary nodes. RHS represents a scenario with Sybil nodes and LHS represents a scenario without Sybil nodes.

To evaluate the degradation in fairness caused by Sybil attacks, we use Jain's fairness index [16] to measure the fairness of the spectrum allocation. For this problem, the fairness decreases from 0.89 without Sybil attack to 0.81 with Sybil attak.

### D. Simulation Results

We further conduct simulations in the MS Visual Studio environment to investigate the impact of Sybil attacks on graph coloring based spectrum allocation in DSA networks. In the simulation, we consider 50 physical secondary nodes sharing a total of 750 MHz available spectrum bands within a 1 km radius region. We set the interference range as 400 m for two

adjacent secondary nodes. Meanwhile, we assume that there exists one physical malicious node launching Sybil attack. To achieve a fair comparison, we use the same initial network topology without Sybil nodes, i.e., the graph containing 50 vertices and 197 edges. The simulation results are averaged over 100,000 Monte Carlo simulations.

Fig. 3 shows the impact of Sybil attack on spectrum allocation with respect to the number of Sybil nodes. It is observed from Fig. 3 (a) that the malicious nodes can obtain more spectrum by generating more Sybil nodes (e.g., approximately 85% if generating 20 Sybil nodes). Moreover, as illustrated in Fig. 3 (b), the fairness of the spectrum allocation will greatly degrade with the increase in the number of Sybil nodes existing in the network.

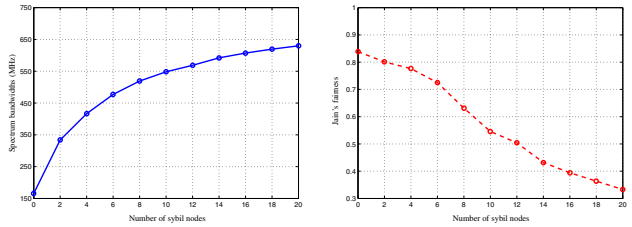


Fig. 3. The impact of Sybil attack on spectrum allocation with respect to the number of Sybil nodes. (a) The total spectrum the malicious node acquire; (b) The Jain's fairness for the network.

## IV. Defense against Sybil Attacks

In this section, we propose a defense strategy against Sybil attacks by exploring the differences between good and Sybil nodes, in statistics of time intervals between two consistent beacon frames (beacon intervals), on the receiver's side.

In practice, a normal 802.11 device uses hardware based method to send beacon frames because this achieves better accordance and accuracy with the 802.11 standard requirements than the software solution, especially in high-load cases. Hence, we adopt the hardware based method for good secondary nodes in our experiments. However, not all devices support the functionality of creating multiple different SSIDs based on the hardware solution. Hence, we consider both hardware and software techniques for the malicious node to generate different SSIDs for Sybil nodes. In the experiment, we assume that both the good secondary node and malicious node send the beacon frame to the same target receiver using burst transmission mechanism [17].

In the experiment setup, we set the beacon intervals on the sender's side as 100ms for both software and hardware based methods. As soon as the beacon frame arrives at the receiver's WNIC, a microsecond-accurate timestamp is generated based on the receiver's hardware clock. It is noted that this timestamp is generated by the WNIC, not the operating system and thus the delay between the beacon receiving and operating response could be neglected. The interference signal used in the experiment is an unlimited data rate FTP transmission between two other nodes in the communicating band with the throughput as 27Mbps.

### A. Defense against Software Based Sybil Attack

In this case, we consider that the malicious node adopts the software based method to generate beacon frames with different SSIDs, whereas the good node uses the hardware based method. Thus, if we can distinguish the beacon frames generated based on software technique, the Sybil nodes will be identified. On the receiver's side, all beacon frames are collected for 15 minutes and the beacon intervals for every source are calculated. Then, we apply a sliding window containing 10 consistent beacon intervals to compute the standard deviation for each window.

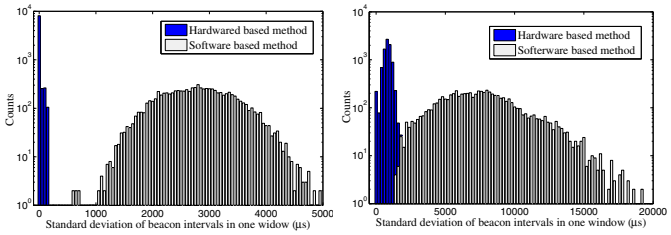


Fig. 4. The comparison of the standard deviation of beacon intervals in one window between the hardware and software based methods. (a) Without interference; (b) With interference.

Fig. 4 shows the histogram of the standard deviation of beacon intervals in one window on the receiver's side. As illustrated in Fig. 4 (a), the standard deviation values for the hardware based method are small and concentrated, whereas those for the software based method are large and scattered. Thus, if there is no interference, we can easily differentiate the hardware and software techniques based on the statistics of beacon intervals. On the other hand, when we add some interference signals, as shown in Fig. 4 (b), standard deviation values for these two techniques are closer and even overlap a bit. However, we can still differentiate them with high probability. For instance, if we set the threshold as 1600ms, the false alarm probability is 1.17%, the misdetection probability is 0.055%[5]. If the threshold is set to be 1800ms, the false alarm probability is 0.61%, the misdetection probability is 0.14%.

Therefore, if the malicious node adopts the software based method to send beacon frames with multiple SSIDs to neighbors, it is easy for the receiver to detect beacon frames from Sybil nodes based on the observation on beacon intervals.

### B. Defense against Hardware Based Sybil Attack

In this case, we assume that the malicious node is able to generate multiple SSIDs for beacons frames via hardware based method. Without loss of generality, we consider a simple scenario in our experiment: one malicious node creating two different SSIDs and two good nodes each using its own SSID send beacon frames to the same receiver. Thus, on the receiver's side, it will receive the beacon frames associated

[5]The false alarm represents the event that the good secondary node using hardware based method is mistakenly identified as the Sybil node using the software based method. The misdetection represents the event that the Sybil node is erroneously considered as the good one.

with four different SSIDs. For the purpose of analysis, we classify this scenario into two cases:

- *Case 1*: Two SSIDs from two different physical nodes.
- *Case 2*: Two SSIDs from the same physical node.

We define the time interval between two consistent beacon frames with different SSIDs as the inter SSID interval (ISI). In order to minimize the experimental errors due to the packet loss, we record the beacon intervals with different SSIDs and less than half of the prescribed beacon interval(100ms), into the ISI data set. Similarly, the sliding window is also used to calculate the distribution of ISI data.

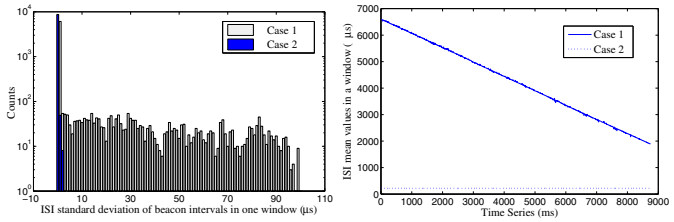


Fig. 5. The comparison of the ISI values in one window between Case 1 and Case 2 without interference. (a) Standard deviation; (b) Mean.

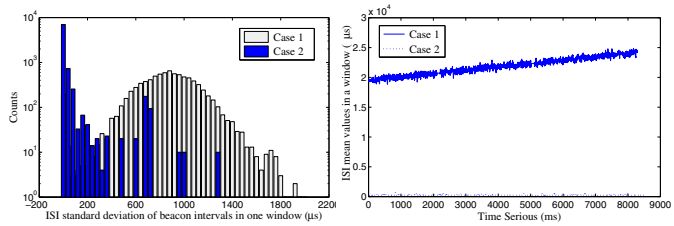


Fig. 6. The comparison of the ISI values in one window between Case 1 and Case 2 with interference. (a) Standard deviation; (b) Mean.

Fig. 5 shows (a) standard deviations and (b) means of ISI values in one window for both cases. It is observed that the ISI values for the Case 2 have much smaller standard deviations and means than Case 1, which can be considered as the criterion to differentiate the beacon frames sent by Sybil nodes. Results of the same experiment under interference are shown in Fig. 6. From Fig. 6 (a), we can see that the standard deviations of ISI values of these two cases overlap often because of interference. However, we can still identify the beacon frames sent by Sybil nodes based on the big difference in the means of the ISI values, as shown in Fig. 6 (b).

Thus, if the malicious node launch Sybil attacks using the hardware based method to send beacon frames with different SSIDs, we also can detect the Sybil nodes through exploring the differences in the statistics of beacon intervals between the Sybil nodes and good nodes.

## V. Conclusions

In this paper, we studied the Sybil attack in DSA networks. To understand the impact of this attack, we looked into a specific distributed graph coloring based spectrum allocation problem. We demonstrated that Sybil attacks are possible in DSA networks through the testbed implementation. We also showed that the fairness of spectrum allocation can deteriorate significantly, e.g., with 20 Sybil nodes in a 50 good secondary nodes system, the fairness will drop over 60%. In order to mitigate this attack, we proposed a defense strategy built on the testbed by investigating the discrepancies in statistics of beacon intervals on the receiver's side between the good nodes and Sybil nodes. The experiment results, corroborating our analysis, demonstrated the effectiveness of the proposed defense strategy.

## Acknowledgement

This research is partially funded by NIJ # 2009-92667-NJIJ, NSF # 0916180 and PSC-CUNY Award # 60079-40 41.

## References

[1] F. C. C., "In the matter of unlicensed operation in the TV broadcast bands," *Second Report and Order and Memorandum Opinion and Order*, no. FCC-08-260A1, Nov. 2008.

[2] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey," *Comput. Netw.*, vol. 50, no. 13, pp. 2127–2159, 2006.

[3] J. Mitola, "Cognitive radio: am intergrated agent architecture for software defined radio," Ph.D. dissertation, KTH Royal Institute of Technology, Stochholm, Sweden, 2000.

[4] T. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and Mitigation," *CrownCom 2008*, pp. 1–8, May 2008.

[5] Y. Tan, S. Sengupta, and K. Subbalakshmi, "Coordinated denial-of-service attacks in IEEE 802.22 networks," *IEEE International Conference on Communications (ICC), 2010*, pp. 1 –5, May. 2010.

[6] J. R. Douceur, "The sybil attack," *Proceedings of 1st Int. Workshop on Peer-to-Peer Systems (IPTPS)*, Mar. 2002.

[7] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis defenses," *Third International Symposium on Information Processing in Sensor Networks (IPSN)*, pp. 259 – 268, 2004.

[8] J. Yang, Y. Chen, and W. Trappe, "Detecting sybil attacks inwireless and sensor networks using cluster analysis," *Mobile Ad Hoc and Sensor Systems (MASS)*, pp. 834–839, Sept. 2008.

[9] B. Xiao, B. Yu, and C. Gao, "Detection and localization of sybil nodes in vanets," *Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*, pp. 1–8, 2006.

[10] H. Yu, M. Kaminsky, P. Gibbons, and A. Flaxman, "Sybilguard: Defending against sybil attacks via social networks," *IEEE/ACM Trans. Networking*, vol. 16, no. 3, pp. 576 –589, june 2008.

[11] D. Quercia and S. Hailes, "Sybil attacks against mobile users: Friends and foes to the rescue," *INFOCOM, 2010 Proceedings IEEE*, pp. 1 –5, 2010.

[12] K. Hong, S. Sengupta, and R. Chandramouli, "Spiderradio: An incumbent sensing implementation for cognitive radio networking using ieee 802.11 devices," *IEEE International Conference on Communications (ICC), 2010*, pp. 1 –5, May. 2010.

[13] T. Ulversoy, "Software defined radio: Challenges and opportunities," *IEEE Communications Surveys Tutorials*, no. 99, pp. 1–20, 2010.

[14] S. Anand, S. Sengupta, and R. Chandramouli, "Distributed opportunistic channel acquisition mechanism in dynamic spectrum access networks," Tech. Rep., 2010. [Online]. Available: http://jjcweb.jjay.cuny.edu/ssengupta/

[15] M. Ergen, "The 802.11 tutorial," Tech. Rep., 2002. [Online]. Available: http://wow.eecs.berkeley.edu/ergen/docs/ieee.pdf

[16] C. Barrett, M. Marathe, D. Engelhart, and A. Sivasubramaniam, "Analyzing the short-term fairness of ieee 802.11 in wireless multi-hop radio networks," *10th IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunications Systems, 2002. MASCOTS 2002.*, pp. 137 – 144, 2002.

[17] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.