# Detecting and mitigating the impact of wideband jammers in IEEE 802.11 WLANs

Eduard Garcia-Villegas  Moisés Gómez  Elena López-Aguilera  Jordi Casademont

Wireless Networks Group – Telematics Engineering Dept. Technical University of Catalonia (UPC)
Avda. del Canal Olímpic, sn, 08860 Castelldefels, Barcelona

eduardg@entel.upc.edu  moises.gomez@estudiant.upc.edu  elopez@entel.upc.edu  teljcs@entel.upc.edu

## ABSTRACT

IEEE 802.11 Wireless LANs (WLANs) are highly sensitive to Denial of Service (DoS) attacks carried out with jamming devices. In this paper we focus on 2.4GHz wideband constant jammers. The interest in the wideband jammer lies in the fact that it beats all possible channels at the same time, leaving no possible escape following traditional channel-switching defenses. After studying and developing an effective detection mechanism, we propose the implementation of a load balancing technique based on cell breathing for mitigating the harmful effects of the jammer over an IEEE 802.11 WLAN. Cell breathing is achieved by dynamically tuning the transmission power to adjust the size of a WLAN cell.

## Categories and Subject Descriptors

C.2.3 [Network Operations]: Network Monitoring; C.4 [Performance of Systems]: Fault Tolerance; C.2.4 [Distributed Systems]: Distributed applications.

## General Terms

Algorithms, Management, Performance, Security.

## Keywords

IEEE 802.11 WLANs, Resource Management, Jamming.

## 1. INTRODUCTION

IEEE WLANs have gone through a big evolution since their first steps. Victims of their own success, due to the permanent growth in the number of Wi-Fi users along with an increase on their traffic demands, the IEEE 802.11 working group is unceasingly studying new amendments to such an extent that they have used up the whole (occidental) alphabet. One of the key issues that required an in-depth revision was security. As a consequence, the IEEE 802.11i amendment was released to add the levels of privacy that Wi-Fi users demanded. Nevertheless, security is not only about privacy and authentication; there are other threats that should be taken into account. A natural objective of an attacker is to drastically reduce the throughput of the network. This can be achieved by jamming the channel with simple and cheap devices that are within the reach of the non-expert public. From [1], *a jammer is an entity who is purposely trying to interfere with the physical transmission and reception of wireless communications*.

After experiencing the impact of a wideband wireless jammer, in section 2 we define a jammer detector mechanism that runs in an IEEE 802.11 access point (AP). In section 3 we discuss possible defenses against a jamming attack and propose the utilization of a load balancing technique based on cell breathing in order to reduce the impact of the jammer. In section 4 we evaluate the effectiveness of our approach. Finally, conclusions are given in section 5.

### 1.1 The Jammer

For our study we used the CVSAL-3405, a portable wireless jammer that interferes with communications in the following bands: 895 to 1000 MHz, 1195 to 1300 MHz and 2395 to 2500 MHz. The total output power on its three omni-directional antennas is 450mW.

Following the taxonomy established in [2], this device could be considered a *channel-oblivious memoryless* jammer. That is, in contrast to other smart jammers (e.g see [3]) this jammer ignores the IEEE 802.11 MAC procedures and constantly transmits energy to the channel regardless of its state and independently from its past actions. Even though this jamming mechanism is not particularly efficient in terms of energy, according to our tests its battery life spans up to two hours, although it starts losing effectiveness after 90 minutes.

The impact of this jammer on an IEEE 802.11 transmission was measured in an indoor environment where a semi-open office propagation model is applicable [4]. In this scenario, and as shown in Fig. 1, the jammer is able to completely block communications within a radius of 5m, although its impact is still noticeable when the jammer is 60m away. Obviously, the grade of the impact depends on the distance between the jammer and its victims, and also on the modulation used in the communication. For example, when the most robust modulation available is used (1 Mbps DBPSK), the jammer has no effect if it is more than 20m away. In contrast, a faster but less robust modulation (e.g. 11 Mbps CCK) is affected even though the jammer is at a distance of 45m or less.

The interest in this simple yet effective jammer lies in the fact that it beats the entire spectrum available for 2.4GHz ISM applications. Unlike “smart” or MAC-aware jammers, which can be avoided by switching the frequency channel in use, there is no possible escape from a wideband jammer.

### 1.2 Attacking an 802.11 transmitter/receiver

The IEEE 802.11 MAC procedure [5] provides two operating modes: Distributed Coordination Function (DCF) and Point Coordination Function (PCF). However, only DCF devices can be found on the market today.

The DCF uses the CSMA/CA algorithm: before initiating a transmission, a station’s clear channel assessment mechanism (CCA) senses the channel to determine whether it is idle or busy. If the medium is sensed idle, the station is allowed to transmit. If

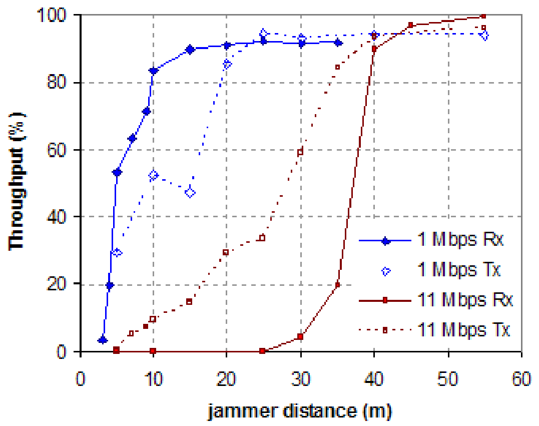

**Figure 1. Normalized throughput measured under jamming**

the medium is sensed busy, the transmission is delayed. Basically, the physical layer provides a busy/idle medium recognition based on the detection of any energy above a given threshold. In consequence, a jammer could completely block a transmitter by sending energy above the carrier sense threshold. This is also known as the exposed node problem.

After a successful reception, the receiving station must send an acknowledgement frame (ACK) back to the transmitter. If the sending station does not receive an ACK after a specified period of time, it will assume that the frame was received in error and will retransmit the frame after a randomly chosen backoff time.

Similarly to the hidden node problem, if the jammer is far from the transmitter, but close to the receiver, the transmitter may infer that the channel is idle when the receiver is being jammed, and will send its frames. From the receiver's perspective, the jammer interference is added to the desired transmission thus degrading the signal to interference and noise ratio (SINR). A decrease in the SINR entails an increase in the number of packet errors. IEEE 802.11 standards define several sets of modulations and coding rates for the different physical layers. For example, IEEE 802.11b specifies four modes: 11Mbps (8-bit CCK), 5.5Mbps (4-bit CCK), 2Mbps (DQPSK) and 1Mbps (DBPSK) to be used in the 2.4GHz frequency band. Each different scheme provides a different transmission rate, but the higher the chosen rate, the worse it performs in the presence of noise and interference.

In order to observe the differences we predicted about the impact of the jammer depending on the direction of the traffic (tx or rx), we measured the saturation throughput (UDP) between two stations placed 5m apart. The jammer is in line of sight with only one of the stations. Fig. 1 shows the different behaviors that appear when the station affected by the jammer is transmitting or receiving, using a robust and a faster modulation. For a robust modulation, it is more effective to target the transmitter's CCA. On the contrary, a faster modulation is more sensitive to packet errors produced at the receiver. Note that the probability that a frame is received in error increases by increasing the frame size. On the other hand, bigger frames make the protocol more efficient. As a result, we observed that the frame size has no impact on the performance of the network under jamming.

## 2. DETECTING A JAMMER

As stated before, the presence of a jammer is evident after a noticeable decrease in the carried throughput. However, such a decrease could be easily explained by other causes (e.g. the Occam's razor would lead us to think that users have reduced their offered traffic). In [1] authors propose the use of the packet delivery ratio (PDR), defined as the ratio of packets that are successfully delivered compared to the number of packets sent. Note that both an increase in the number of active stations (i.e. increased collision probability), and a channel degradation produced by the nodes' mobility, etc. will produce a low PDR. For these reasons, authors suggest the combination of PDR with signal strength measurements: a low PDR together with high signal levels mean that there is an ongoing attack. However, as stated in [6], even a small interference may cause a low PDR.

A more sophisticated mechanism is proposed in [7] which determines whether the distribution of the *explainability* of the collisions (i.e. the probability that a collision can be explained by the events observed in the network) deviates significantly from that under normal conditions. Although their model can be extended, in its current form it assumes that all reception errors are caused by collisions (ignoring poor channel conditions). In [8], the AP measures the transmission delay of its clients. Then, if there is a sudden increment of the delay, the client is considered under attack, since it may have reduced its transmission rate due to the interference caused by the jammer. However, as with PDR, this fact can also be explained by mobility, obstacles, etc.

### 2.1 Our approach: deferred transmissions

All the aforementioned detection mechanisms are not effective when the jammer is close to the transmitter, since it will defer any transmission upon detection of a busy channel. In this case, Xu et. al. [1] propose measuring the carrier sensing time (CST), that is, the time a station waits for the channel to become idle. Unfortunately, the value of CST increases not only in the presence of a jammer, but also when number of active stations is high. However, the CST during normal operation may be determined theoretically or empirically and thus compared to the values obtained under jamming. Building a complete mathematical model that captures the IEEE 802.11 MAC is extremely difficult and would require a considerable amount of computational resources. Recall that our aim is to develop a detection mechanism that runs in low featured devices (i.e. the APs). Therefore we focus on the second approach.

The accurate measurement of the CST requires access to firmware functions or hardware registers that are not always available to the developer. In contrast, other manufacturers, such as Intersil eased this task by opening access to their Prism chipset documentation and software. Among the measurements offered by Prism devices to higher layers, the *TxDeferredTransmissions* counter, which represents the total number of MSDUs for which one or more transmission attempt was deferred to avoid a collision [9], could be as useful as the CST. Whenever a transmission is deferred due to a CCA channel busy indication, *TxDeferredTransmission* is incremented. Therefore, the following ratio:

$$T_f = \frac{TxFrames + TxDeferredTransmissions}{TxFrames} \qquad (1)$$

where *TxFrames* is the total number of frames that have been sent to the channel, defines the average number of transmission attempts per frame. A jammer will produce an increment in $T_f$, but this value also increases with load. In order to distinguish between normal and abnormal failed attempts, we implemented a threshold mechanism based on $T_f$ measurements carried out in different scenarios. The AP measures load and $T_f$ periodically; if $Tf$ is above the value expected for that load, a jammer is present. The load is measured in terms of occupation time. In our implementation, a linux-based AP running the HostAP driver [10] and a Prism 2 WLAN card, measures the portion of time spent in transmitting and receiving frames. As detailed in [11], this can be easily done thanks to the statistics provided by the driver. The maximum expected values for $T_f$, obtained after a large number of measurements in different scenarios, are shown in Fig. 2.

The resulting application occupies only 14kB of memory and requires low CPU resources, making it suitable for running on commercial APs. The detector module has been tested under different traffic conditions (varying offered throughput, frame sizes, number of active stations, etc.). In our tests, the activation of the jammer was always correctly detected at a distance of 50m or less, even before its presence could be noticeable on the carried throughput (cf Fig. 1). Sudden increments in $T_f$, after driving the network into saturation, did not produce false positives. Moreover, due to the fact that an AP periodically sends *beacon* frames and therefore has to sense the channel frequently, the our modeule was able to detect the jammer even when no clients were attached to it.

HostAP driver only supports Intersil Prism chipsets, versions 2, 2.5, and 3. This limits our experiments to IEEE 802.11b devices. However, the conclusions derived in our study can be extrapolated to IEEE 802.11a/g given that all 802.11 versions share the same MAC layer definition, which is the origin of the vulnerabilities exploited by the jammer.

# 3. COUNTERMEASURES

In [6], it is shown that adjusting certain parameters such as frame size or modulation is not effective to face a strong interference. However, as stated in [12], this kind of adaptations may be useful in front of some types of attack. A quick literature review shows that, in general, the most accepted solution is based on channel switching. Among these approaches there are two different types of defense: proactive and reactive.

Using a proactive channel switching strategy, the network performs a periodic frequency hopping regardless of the channel state. An example of proactive defense is proposed in [13], where the stations change their frequency every 100 ms following a pseudo-random sequence that is known by all participants. In [6] a similar solution is described, but in that case, the hopping sequence is announced by the AP when it detects a degradation of the channel due to the possible presence of a jammer. In a purely reactive solution, the network moves to another frequency only after detecting the presence of a jammer in the channel in use. This implies not only the presence of a reliable jammer detector module (not needed in the proactive approach), but also a mechanism that enables the channel switch synchronization even for those stations that did not detect the jamming attack. In [14], for example, a channel switch is detected after prolonged periods without communication.

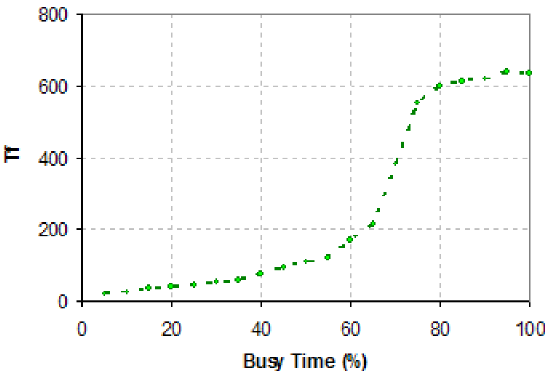

**Figure2. Measurement based $T_f$ threshold**

Nevertheless, none of these strategies are valid in the presence of a wideband jammer [15]. Under such circumstances, the only definitive solution is to locate and neutralize the attacker. In the meantime, all we can do is to implement mechanisms intended to minimize the damage caused by the jammer. In this sense, there are studies focused on multihop networks that suggest to avoid the geographical area under attack by diverting the traffic through safer paths [16][17]. The case of infrastructure-based WLANs (use of access points, or APs) has been scarcely studied. In [8], for example, authors study the *implicit jamming attack*: the case where only a portion of the AP's clients are being jammed. To avoid the loss of efficiency in the cell caused by the use of slower modulations in the communications with the affected nodes, the authors propose the implementation of traffic shaping techniques. However, there is nothing to do when the AP itself is under attack.

In the context of the proposals that seek to minimize the impact of a jammer in an AP-based IEEE 802.11 network, we propose the use of load-balancing techniques, such as cell breathing.

## 3.1 Our approach: cell breathing

Cell breathing consists in dynamically modifying cell dimensions by increasing or reducing transmission power. Cell breathing is a side effect in CDMA networks that reduces the cell coverage when more users are supported, but this could be advantageous in load balancing techniques if optimal strategies are applied. The concept of cell breathing for load balancing in WLANs is as follows: a highly congested AP reduces its coverage radius so that the furthest stations lose connectivity and try to roam to less loaded APs. An under-utilized AP may increase transmit power in order to expand its coverage. Consequently, new users will roam to this AP and the load on neighboring APs will decrease.

The presence of a jammer should be interpreted as if the attacked AP is carrying a huge load, although in practice, the effect of the jammer surely reduces the traffic on the AP. It is therefore essential that either the metrics used to assess the actual load of an AP take into account the effect of interference, or that a reliable jammer detection module is present. In [18], we showed that the capacity available in an AP (AAC) provides an efficient load metric. Logically, low AAC values → load is high. This metric incorporates the effects of the offered traffic, the number of competing stations, its physical rate and the quality of the channel.

The details of the selected algorithm for the load balancing based on cell breathing are given in [20]. In short, each AP calculates its own load (AAC). According to its load, and compared to its neighbors', an AP can be in one of the following three states: *Gull* (AP load is larger than the average load in the neighborhood), *Fair* (AP load is similar to the average load) and *Willing* (AP load is below the average load). A *Fair* AP will not take any action regardless of its neighbor's behavior. A *Gull* AP is willing to reduce its cell and will ask its neighbors for help. Finally, a *Willing* AP is willing to increase its cell in response to a neighbor's appeal. *Willing* and *Gull* APs will gradually adjust their cell sizes until equilibrium is achieved or the maximum/minimum transmitted powers are reached.

Cell dimensions are established by adjusting the transmission power from the AP, but reducing power entails signal degradation

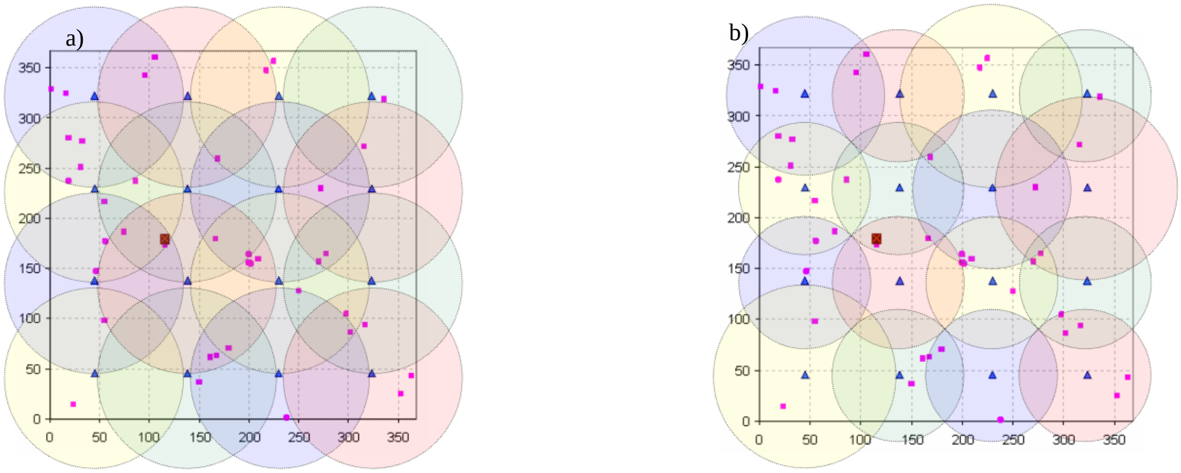

**Figure 3. Random scenario: a) 16 APs transmitting at 20dBm b) Running with cell breathing**

at the receiver. However, from the client station's point of view, the cell dimensions are determined by the energy of received Beacon frames and Probe Responses. Therefore, an AP can set its optimal cell dimension so that the farthest client that the AP must serve receives Beacons above a given threshold. On the other hand, the power used to transmit data frames can be higher so that the user's experience is not degraded.

Fig. 3 shows an example of its operation, in a scenario, where 16 APs are evenly placed. Cell dimensions are computed following a semi-open office propagation model. A jammer is placed in a randomly chosen position (red dot at coordinates 115, 180). In the figure, the triangles represent the 802.11 APs, while the small squares are client devices, which are distributed randomly over the scenario. The figure on the left shows a conventional WLAN network, where all cells have the same size, while the right figure shows the behavior of a WLAN with cell breathing, where the APs that are closer to the jammer have reduced their coverage. In contrast, those APs further away have increased their cells with the intention of offsetting the impact of the jammer.

# 4. EVALUATION

Although the behavior of the cell breathing algorithm (CB, hereafter) is simulated, the throughput values used in this evaluation process are obtained from analytical models that take into account all the phenomena that affect the capacity of an 802.11 network. This model has been described and evaluated in [18][19], adding the effects of the jammer shown in Fig. 1.

To evaluate the impact of the CB technique on a network under the attack of a wideband jammer, a large number of simulations were performed in the scenario depicted in Fig. 3. That is, a 370 x 370m square area where the position of 16 IEEE 802.11b APs is fixed. We assume there are no coverage gaps even if all APs are transmitting at the minimum allowed power (10 dBm). An efficient frequency management strategy is also assumed so that we can neglect inter-cell interference even when all the APs are transmitting at maximum power (20 dBm). Users are static and the coordinates of their position are chosen randomly. The modulation used for each client depends on the quality of the signal received from the AP and can be 1, 2, 5.5 or 11 Mbps.

## 4.1 Jamming a Hotspot (in saturation)

As explained in [18], users are static and tend to be spatially concentrated. In the first simulations we introduce these characteristics by placing users at random, but forcing them to be concentrated in a square area of 170x170m centered at the coordinates of one of the APs (138, 138). In order to maximize its impact, the jammer is positioned at the same point. In the first test, all users are in saturation, i.e. there is always a 1500 Byte datagram waiting to be transmitted on each client's queue.

Fig. 4 compares the performance of the network described when the jammer is inactive (*Off*) or active (*On*). We study the impact of the jammer in a network where the APs implement the CB algorithm and two other cases in which the transmission power of the APs are fixed: APs transmitting at maximum power (MAX) and APs with random transmission power (RND). At a first glance, it is easily observable how the CB technique improves the performance of the network no matter whether the jammer is active or not. All three transmit power strategies yield a similar performance when the network is highly loaded and hence the implementation of load balancing has little effect. The impact of the jammer over the carried throughput is between 20 and 40%, although it is slightly lower when CB is run (22% on average, with 29% for RND and 27% for MAX).

But CB not only succeeds in improving the overall performance of the network in terms of throughput, but also it is able to minimize the differences in the level of service received by different users, even though these are affected to a different extent by the jammer. This level of service is measured by means of the known Jain's fairness index [21]. Jain's index can be interpreted as follows: an index of 1 means that all users receive the same service (measured in carried throughput). An index of 0.5 could be interpreted as if, on average, 50% of the users receive an equitable service, while the rest of the stations did not get any service. In this regard, and as shown in Fig. 4 b), the presence of CB makes a big difference.

## 4.2 The jammer moves away (non-saturated)

When all users are in saturation, the observation of the total throughput can be misleading, given that unaffected stations are able to obtain a larger throughput at the expense of the stations affected by the jammer. For that reason, in the following tests two different CBR traffic profiles are assigned randomly to the users: *low* (500kbps with 500Byte frames) and *medium* (1Mbps with 1000Byte frames). In Fig. 5 a) we see how the impact of the jammer decreases as it moves away from the centre of the hotspot. With the absence of nodes in saturation, the improvements provided by the CB become more visible. In the worst case scenario (jammer in the center of the hotspot), CB improves 25% (compared to RND) and 20% (compared to MAX).

Another metric for fairness is given by finding the minimum throughput a station is able to achieve. This is shown in Fig. 5 b), where those stations completely blinded by the jammer are not taken into account. With regards to fairness, the worst case scenario is obtained when the jammer is halfway between two APs, thus affecting two cells simultaneously. Hence, jammed stations are not able to successfully send or receive frames to/from neither of the closest APs. Again, CB clearly reduces the impact of the jammer: in the worst case, the minimum throughput with CB is three times the value obtained by MAX or RND.

## 4.3 Random scenario

Finally, we show carried traffic estimations after generating and evaluating thousands of scenarios where both jammer and users are randomly distributed throughout the whole scenario, according to a uniform distribution. Traffic demands are also randomly chosen among three different profiles (*saturation*, *medium* and *low*). As expected, in this scenario the impact of the jammer is lower due to a higher dispersion of the users. In Fig. 6 a), the presence of the jammer lowers the carried throughput in nearly 12% on average (values between 10 and 15%). In such a scenario, the improvements provided by the CB algorithm are less remarkable since the load is already balanced due to the uniform distribution of users. As shown in Fig. 6 b), CB improves the performance of a network under normal circumstances, but in the presence of a jammer, these improvements are even greater.

# 5. CONCLUSIONS

In this paper, we have proposed a jamming detector module for IEEE 802.11 WLANs, based on the inspection of the number of transmission attempts per frame. The detector was implemented and tested in a Linux-based AP, in order to prove the effectiveness of our approach. The application is able to detect the jammer even before its impact on the carried throughput is noticeable.

Furthermore, since there is no possible escape from a wideband jammer, we proposed the implementation of a load balancing mechanism, based on cell breathing, with the aim of minimizing its impact. The evaluation of this solution showed that the presence of load balancing effectively reduces the impact of the jammer, both in terms of throughput and fairness.

Although our study is based on 802.11b, the conclusions derived from both the study of the detection process and the evaluation of our approach can also be extrapolated to 802.11a/g given that all 802.11 versions share the same MAC layer definition, which is the origin of the vulnerabilities exploited by the jammer.

# 6. ACKNOWLEDGMENTS

This work has been supported in part by the Spanish Government through project TEC2009-11453 and CDTI, Ministerio de Industria, through Segur@ project.

# 7. References

[1] W. Xu, W. Trappe, Y. Zhang, and T. Wood, “The feasibility of launching and detecting jamming attacks in wireless networks,” Proceedings of MobiHoc’05, pp 46-57, May 2005

[2] E. Bayraktaroglu, C. King, X. Liu, G. Noubit, R. Rajaraman and B. Thapa “On the performance of IEEE 802.11 under Jamming”. in Proceedings of Infocom'08, April 2008

[3] D. Thuente and M. Acharya, “Intelligent jamming in wireless networks with applcations to 802.11b and other networks,” Proc. of IEEE MILCOM’06, Octover 2006.

[4] T. S. Rappaport, Wireless Communications Principles and Practices. Prentice Hall PTR, Upper Saddle River, NJ, USA, 2nd edition, December 2001.

[5] IEEE, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. ANSI/IEEE Std IEEE Std. 802.11-2007, June 2007.

[6] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan, “Understanding and mitigating the impact of RF interference on 802.11 networks,” Applications, technologies, architectures, and protocols for computer comm., SIGCOMM'07, pp. 385-396. 2007.

[7] A. Lopez and X. Wang, “Robust detection of MAC layer Denial-of-Service attacks in CSMA/CA wireless networks,” IEEE Trans. on Information Forensics and Security, vol. 3, n. 3, pp 347-358, 2008

[8] I. Broustis, K. Pelechrinis and D. Syrivelis, “FIJI: fighting implicit jamming in 802.11 WLANs,” in Security and Privacy in Communication Networks, vol 19, pp. 21-40, Springer, Oct. 2009

[9] Intersil, PRISM Driver Programmer's Manual. (For distribution under NDA only) version 2.30, June 2002.

[10] Jouni Malinen. Host AP driver for Intersil Prism2/2.5/3, hostapd, and WPA Supplicant. http://hostap.epitest.fi

[11] E. Garcia, D. Viamonte, R. Vidal, and J. Paradells, “Achievable Bandwidth Estimation for Stations in Multi-Rate IEEE 802.11 WLAN Cells,” Proc. of WoWMoM'07, June 2007.

[12] X. Liu, G. Noubir, R. Sundaram and S. Tan, “SPREAD: Foiling Smart Jammers using Multi-layer Agility”, Proceedings of Infocom'07.

[13] V. navda, A. Bohra, S. Ganguly and D. Rubenstein, “Using Channel Hopping to Increase Resilence to Jamming Attacks”, Proceedings of Infocom'07

[14] W. Xu, T. Wood, W. Trappe and Y. Zhang, “Channel Surfing and Spatial Retreats:Defenses Against Wireless Denial of Service”, ACM Workshop on Wireless Security, p. 80 – 89, 2004

[15] K. Pelechrinis, C. Koufogiannakis and SV. Krishnamurthy, “Gaming the Jammer: Is Frequency Hopping Effective?”, In WiOpt, June 2009

[16] AD. Wood, JA. Stankovic and SH. Son, “JAM: A Jammed-Area Mapping Service for Sensor Networks”, Proceedings of RTSS’03.

[17] M. Cagalj, S. Capkun, and J. Hubaux, “Wormhole-based anti-jamming techniques in sensor networks”, in IEEE Transactions on Mobile Computing vol. 6, n. 1, p. 100–114. 2007

[18] E. Garcia, J.L. Ferrer, E. López, R. Vidal, and J. Paradells, “Client-driven load balancing through association control in IEEE 802.11 WLANs,” European Transactions on Telecommunications, vol. 20, n. 5, pp. 494-507, August 2009.

[19] E. Garcia, “Available Admission Capacity Estimations in IEEE 802.11 Access Points” Tech Report, 2008: http://hdl.handle.net/2117/2045

[20] E. Garcia, R. Vidal and J. Paradells, “Cooperative load balancing in IEEE 802.11 networks with cell breathing”, in ISCC'08, pp. 1133-1140, July 2008

[21] R. Jain, D. Chiu, and W. Hawe. A Quantitative Measure of Fairness and Discrimination for Resource Allocation in Shared Computer Systems. DEC Research Report TR-301, September 1984.

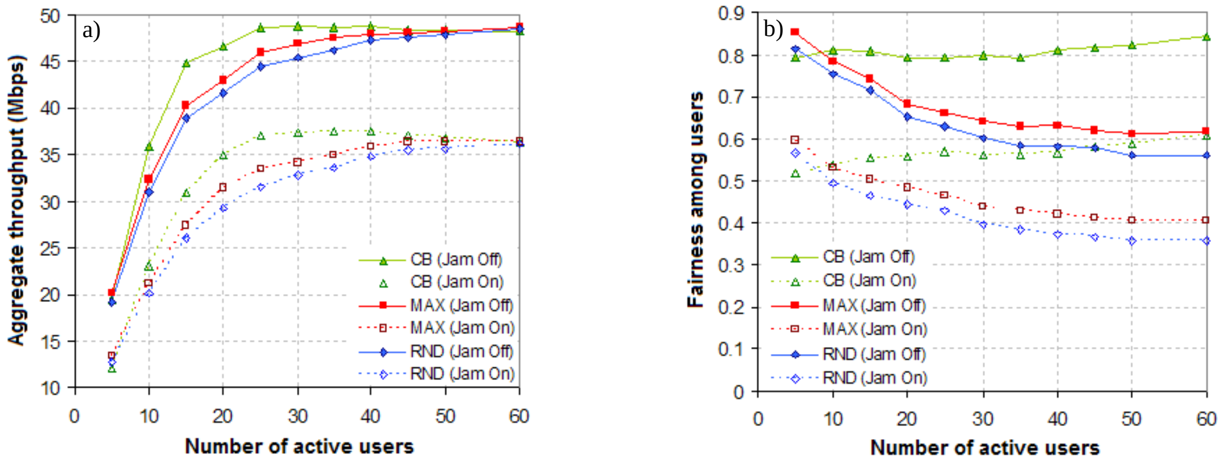

Figure 4. Jamming a hotspot in saturation: a) carried throughput b) Fairness among users

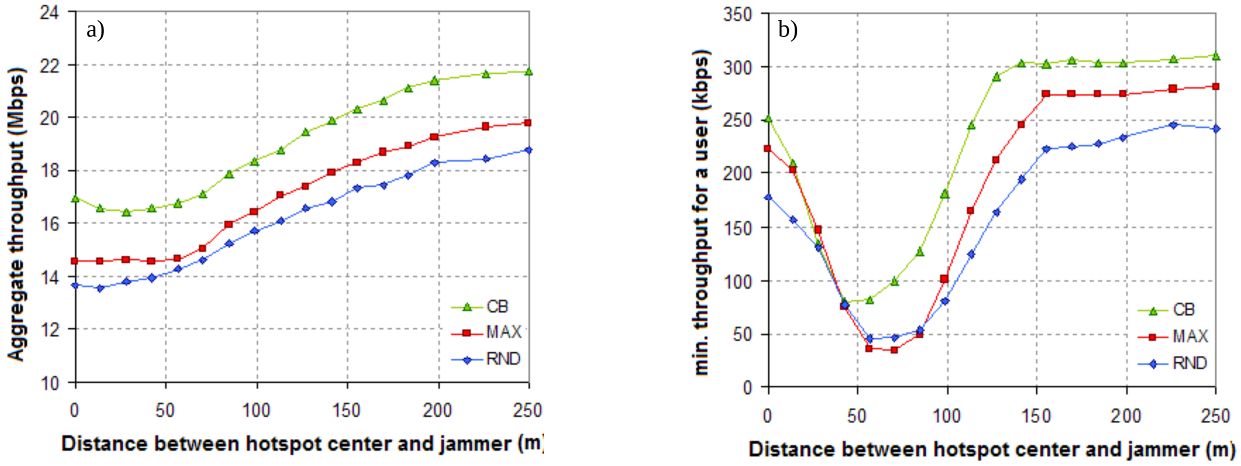

Figure 5. The jammer moves away: a) Carried throughput b) Fairness (min. throughput for a user)

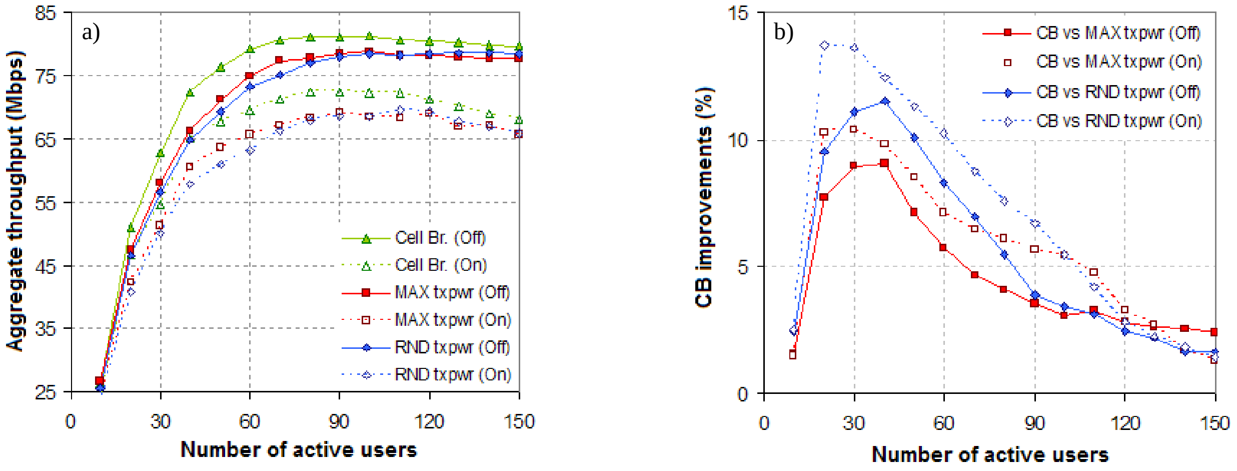

Figure 6. Random scenario: a) Carried throughput b) Improvements achieved by running CB