Carving Secure Wi-Fi Zones with Defensive Jamming

Yu Seung Kim[1], Patrick Tague[1], Heejo Lee[2], and Hyogon Kim[2]
[1]Carnegie Mellon University, USA
[2]Korea University, South Korea
[1]{yuseungk, tague}@cmu.edu, [2]{heejo, hyogon}@korea.ac.kr

ABSTRACT

With rampant deployment of wireless technologies such as WLAN, information leakage is increasingly becoming a threat for its serious adopters such as enterprises. Research on antidotes has been mainly focused on logical measures such as authentication protocols and secure channels, but an inside collaborator can readily circumvent such defenses and wirelessly divert the classified information to a conniver outside. In this paper, we propose a novel approach to the problem that forges a walled wireless coverage, a secure Wi-Fi zone in particular. Inspired by the fact that jamming as an attack is inherently difficult to defeat, we turn the table and use it as a *defensive* weapon to fend off the covert illegal access from outside. To validate the proposed approach, we conduct extensive outdoor experiments with the IEEE 802.11g Wi-Fi adapters. The measurements show that the forged secure zones match well with the model prediction and that the defensive jamming approach can indeed be used to protect wireless networks against information leakage. Lastly, we propose the algorithms to configure defensive jammers in arbitrary geometry.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*security and protection (e.g., firewalls)*; C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*wireless communication*; C.2.2 [**Computer-Communication Networks**]: Network Protocols

General Terms

Algorithms, Performance, Security

1. INTRODUCTION

Over the past decade, wireless networks have made huge progress in both diversity and volume. More novel solutions are being added even today to satisfy the growing needs for easy and flexible connectivity. Although the ease and flexibility are the fortes of wireless technology, there is a flip side to it, which are the vulnerabilities arising from the shared-medium communication. Among many, *information theft* is quickly becoming a pressing issue, as more and more enterprises adopt wireless technology for their business.

A variety of mechanisms has been proposed to prevent illegal access to confidential data over wireless networks. The diversity in term of time, frequency, space, code, etc. is used in the physical layer to secure the communication channel (*e.g.* spread spectrum). On the link layer, security protocols are frequently adopted to authenticate the users and/or encrypt sensitive data. For example, the most widely deployed IEEE 802.11 WLAN includes an security protocol extension such as IEEE 802.11i. Upper layer protocols like IEEE 802.1x are also used.

Still, however, there have been many problems in coping with the information theft with the aforementioned mechanisms. Most of physical layer methods requires costly hardware or complex techniques. In many widely deployed wireless protocols the secret key used for spreading techniques is publicly revealed or possibly guessed by analyzing beacons and frequency usage pattern. Moreover, what if the keys used in the security protocols are exposed to unauthorized parties, or more importantly an insider makes an illegal wireless connection to an outside AP?

Admittedly, it is not possible to have a complete solution working in a single layer by the nature of the layered architecture of current wireless protocols. In this paper, we present a novel approach which can enhance the existing security mechanisms to defend against information leakage and can make the attacking cost expensive. Different from the traditional approach, we turn our attention to *how to isolate the specific geographical area from the illegal wireless access*. The idea is inspired by the non-isotropic jamming model [10], which is used to fight off radio interference. The difference, however, is that we use the jamming model to physically cordon off the given area from the covert external access. It is known that there is no wide-spread countermeasure against jamming [5]. At the same time, the cost to launch jamming attacks is relatively low. But by the same argument, this very property allows us to develop a lightweight and rugged method that strongly resists the illegitimate access from outside and cuts off information leakage from a protected wireless network almost completely.

Below, we begin the discussion by presenting theoretical jamming models for the secure wireless zone in Section 2. In Section 3, we reveal how well the theoretical model is matched with the real world measurements. We introduce an algorithm for defensive jammer arrangement to carve the wireless zone into a specified geometry in Section 4. Section 5 overviews the related work. Finally, we conclude the paper in Section 6.

2. THEORETICAL JAMMING MODEL

ASIACCS '12, May 2–4, 2012, Seoul, Korea.

In this section, we first specify the assumptions in our approach. Then we discuss the wireless communication range under the effect of jamming with the one-transceiver-one-jammer model, and extend the model by adding more jammers. Lastly, we address the issue related to the jamming frequency selection in order to cope with the attackers' spectral evasion.

2.1 Assumptions

We want to protect the Wi-Fi networks which are vulnerable to the information leakage explained in Section 1. All of the wireless nodes of the network are located inside a physical perimeter. Assuming the wireless network is basically protected by standard security protocols such as IEEE 802.11i and IEEE 802.1x, we develop a non-cryptographic physical-layer mechanism to complement the existing crypto-based security. The mechanism must not depend on any pre-shared secrecy and must not require any specialized hardware or significant modifications of existing standards.

Our approach exploits jamming to build a physical cordon between the Wi-Fi coverage to be protected and the outside area. We can control the parameters of jammers such as positions and transmitting powers without restrictions. The jammers are plugged into the power sources, and therefore the energy is not a serious concern.

A malicious insider might use the alternative wireless communication channel such as cellular networks to covertly carry the information in the target network to the outside colluder. These, however, are under control of network administrator, and thus we assume that the cellular infrastructure can easily monitor and prevent this type of misbehavior.

There are some mechanisms to defeat jamming (e.g., interference cancellation [4, 3], high-gain antenna, etc.), but because these are very expensive to implement we can significantly increase the attacking cost and efficiently mitigate the attack. The timing channel under jamming proposed in [11] cannot deliver large data due to its low throughput (e.g. slower than 10bps).

Lastly, the intentional jamming might be not permitted due to the related regulations (*e.g.* FCC regulations in US). But, this approach is still useful in places without these restrictions or where the permission is granted for special purposes. Different countries have different regulations and the detailed legal interpretation is out of topic in our paper.

2.2 Jamming Boundary and Shape Control

In order to decide the communication range of a wireless node, we can use the signal-to-interference-noise ratio (SINR). For the transceiver A, the receiver S, and the jammer J, S can hear A if the SINR $\gamma_{A/J}(S)$ at S for the A's signal to the J's noise is higher than the threshold β which is decided by the used modulation technique. Hence, the jamming boundary which decides the hearing range of S under jamming is expressed as follows.

$$\gamma_{A/J}(S) = \frac{P_{AS}}{P_{JS} + N_0} = \beta, \tag{1}$$

where P_{AS} is the amount of power received by S from A, P_{JS} is the amount of power received by S from J, and N_0 is the ambient noise power.

Here, we ignore the ambient noise power N_0 for the simplicity of model derivation and apply the line-of-sight (LOS) propagation model [7] to the received power at S. Note that the LOS propagation model is only used as an example. Depending on the field configuration, any propagation model can be used instead. We assume that A and J use the same efficiency of omni-directional antenna and they operate on the same frequency band. Note that the network administrator controls the jammer as well, so this configuration is reasonable to assume (though not necessary). Eq. (1) is thus simplified as

$$\frac{P_{AS}}{P_{JS}} = \frac{P_A}{P_J} \cdot \left(\frac{D_{JS}}{D_{AS}}\right)^n = \beta, \tag{2}$$

where P_A is the transmitting power of A, P_J is the transmitting power of J, D_{JS} is the distance between J and S, D_{AS} is the distance between A and S, and n is the path-loss exponent, which varies with surrounding environments. It is known that $n = 2$ for free space, $n = 4$ for flat surface, and $n > 4$ for indoor environments except tunnels [7].

Eq. (2) gives the idea that a jamming boundary is dependent on the powers of A and J, and the distances from S to them. The loss exponent n is determined by the surrounding area. We use both the free-space propagation model (n=2) and the flat-surface propagation model (n=4) to show the relationship as n changes. Fig. 1 depicts the jamming boundaries on the x-y plane when the transceiver A is located at $(0, 0)$, the jammer J is located at $(j, 0)$, and the SINR threshold $\beta = 1$. Table 1 shows the power relationship between A and J for the boundaries shown in Fig. 1. Although not shown for brevity, this relationship is maintained for other values of n as well.

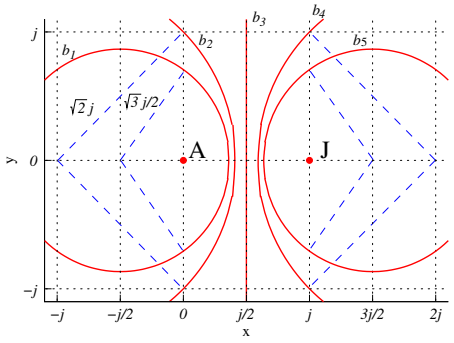


Figure 1: Jamming boundaries with various parameters

Jamming boundary	Loss exponent	
	$n = 2$	$n = 4$
b_1	$3P_A = P_J$	$9P_A = P_J$
b_2	$2P_A = P_J$	$4P_A = P_J$
b_3	$P_A = P_J$	$P_A = P_J$
b_4	$P_A = 2P_J$	$P_A = 4P_J$
b_5	$P_A = 3P_J$	$P_A = 9P_J$

Table 1: Relationship between P_A and P_J for each jamming boundary in Fig. 1

The precise circular curves depicted in Fig. 1 are only approximations according to the LOS propagation model used in Eq. (1) and Eq. (2). Therefore, the approximations (and hence the model) can be intentionally conservative or generous to provide an appropriate buffer to either side of the line where reception may or may not occur.

Based on the one-transceiver-one-jammer, we now extend the model to multiple jammers. Given the k number of jammers, the SINR at S under jamming is given by

$$\gamma_{A/(J_1,\cdots,J_k)}(S) = \frac{P_{AS}}{\sum_{i=1}^{k} P_{J_i S} + N_0} = \beta, \qquad (3)$$

For the realistic model, we now consider an infrastructure Wi-Fi network which consists of an AP and multiple stations under the effects of multiple jammers. Let us define the *area accessible to AP* using the SINR function above as follows.

DEFINITION 1. *(Area Accessible To AP) If a station in the area $Z_A(J_1, J_2, \cdots, J_k)$ can receive data from the AP A under k jammers, Z_A is defined as an area accessible to AP. Namely,*

$$Z_A(J_1, J_2, \cdots, J_k) = \Big\{(x,y)\Big|\gamma_{A/(J_1,J_2,\cdots,J_k)}(x,y) > \beta\Big\},$$

where γ is the SINR function of (x, y) which is the location of a station on the x-y plane, and β is a positive constant which varies with modulation and coding.

Without loss of generality, we assume that $\beta = 1$ (0dB) in the rest of this paper.

The area accessible to the AP A under effects of k jammers is a subset of the intersection of the areas accessible to the AP A under the effect of each single jammer. The proof of this is detailed in [6]. We call the area $Z_A(J_1, J_2, \cdots, J_k)$ the *secure wireless zone*, when the area accessible to AP is walled from the outside.

DEFINITION 2. *(Secure Wireless Zone) Let O be an outside station which is not supposed to be a member of the given wireless network, L_O be the area in which O can be located, and Z_A is the area accessible to AP A. Then, Z_A is the secure wireless zone, only if*

$$Z_A(J_1, J_2, \cdots, J_k) \cap L_O = \phi.$$

2.3 Jamming Frequency Selection

In the jamming model above, jammers only jam the single channel on which the legitimate AP and the legitimate stations communicate. In practice, however, multiple channels can be in use, and can cause problems to the model. For instance, different 802.11 BSS's in the given enterprise may opt to use different channels just to minimize interference between them, or the insider rogue stations may find an unjammed channel to open a covert association to a colluder outside. For such cases, we could (1) introduce broadband jamming that jams multiple frequency bands simultaneously [5], or (2) jam with narrow-band jammers which operate on different frequency bands. Comparing the pros and cons of these two approaches is beyond the scope of this paper, and we simply explore the impact of narrow-band jamming on neighboring channels in Section 3.

3. EXPERIMENTS

We validate our proposed model by measurements with widely used IEEE 802.11g WLAN in the 2.4GHz band. We use the flat-surface propagation model with loss exponent $n = 4$ to compare with the measurements. The experiments are conducted in an outdoor site that is free of existing signals in the 2.4GHz band. The test site is a 10×10 meter square with concrete floor.

The experiment is divided into two parts. First, we demonstrate that the shape of the jamming boundary between a jammer and a transmitter follows the theoretical model. Second, we measure the jamming effect on neighboring channels and estimate how many channels should be jammed to block the attacker who tries to evade spectrally.

3.1 Jamming Boundary Formation

We use three laptops equipped with Atheros 5212 based Wi-Fi adapters for a jammer, a transmitting AP, and a receiving station. They operate on Linux kernel with MadWifi driver. We use the modified MadWifi driver for the jammer. The modification disables the carrier sense and skips the back-off procedure, and thereby emitting the meaningless frames constantly, regardless of the activities of nearby Wi-Fi devices. All of nodes operate on the same frequency channel. The AP is placed 10 meters apart from the jammer and sends 1Mbps UDP traffic to the wireless station by using iperf. We change the location of the station in the test site square and measure the delivery status of the traffic from the AP.

We record the signal-to-noise ratio (SNR) and the packet delivery ratio (PDR) which is defined as the number of successfully received frames by the station to the number of frames sent from the AP at intervals of one meter on the 10×10 meter grid. We use wavemon v.0.4.0b and iperf to measure the SNR and the PDR.

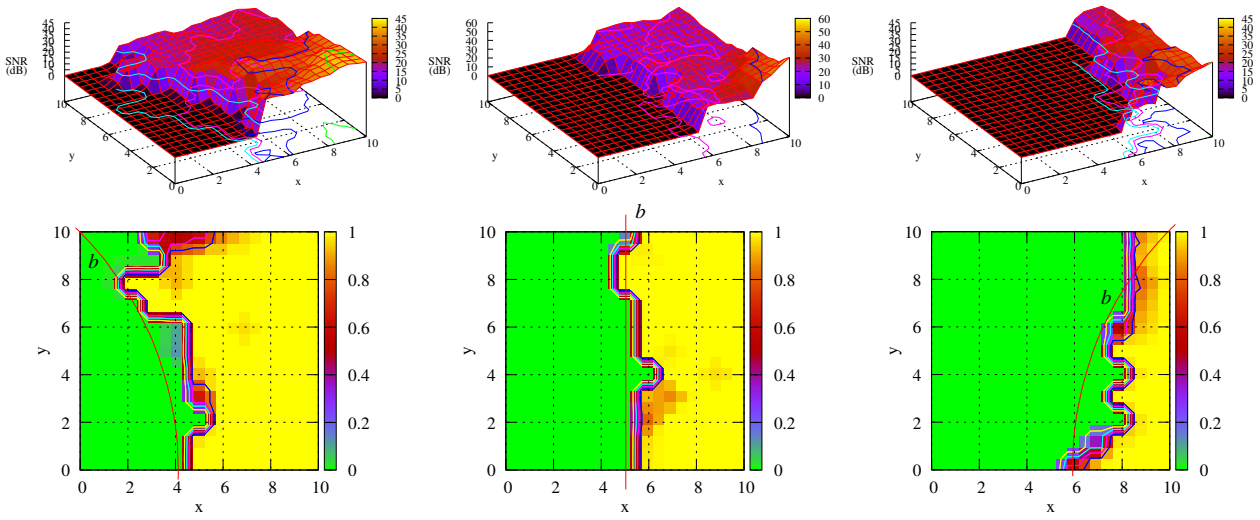
We conduct the experiments for the three different configurations of the transmitting powers of the AP and the jammer. For each pair of the AP and the jammer, we set the transmitting powers to (6dBm, 0dBm), (0dBm, 0dBm), and (0dBm, 6dBm). Each pair of configuration corresponds to $P_A = 4P_J$, $P_A = P_J$, and $4P_A = P_J$, respectively.

The result of the first experiment is plotted in the graphs of Fig. 2. The pattern of the SNR in each configuration is similar to that of the PDR. The SNR in theory should decrease smoothly as the station recedes from the AP, but the results show that it drops rapidly near the jamming boundary. This is because wavemon measures the SNR only with the signal strength of the successfully received packets. Hence, the SNR appears to drop precipitously to zero when the association between the station and the AP is disconnected around the jamming boundary. Likewise, the PDR drops to zero when the station is disconnected from the AP. Along the theoretical model, the jamming boundary bends toward the one emitting less power. The jamming boundary in Fig. 2(a) is approximate to b_4 in Fig. 1, and the same trend holds in Fig. 2(c) with b_2. When their transmitting powers are equal, the jamming boundary is formed along the centerline between them like b_3.

3.2 Jamming Effect on Neighboring Channels

To investigate the jamming effect on neighboring channels, we use the laptops equipped with the Wi-Fi adapter based on the Atheros chip-set. The jammer, the AP, and the receiving station are all located within one-meter radius. The AP sends the 1 Mbps UDP traffic to the receiver station by using iperf. While the AP transmits on one channel, we sequentially change the jamming channel and observe the PDR of the traffic between the AP and the receiving station. We repeat this process for all 13 channels. The transmitting powers of both the AP and the station are fixed at the maximum (18dBm), and we conduct the experiment for the two different cases of jamming power (0dBm and 18dBm) to analyze the influence of the jamming power.

The minimum-power jammer perfectly disconnects the communication in the jamming channel and its neighboring two channels on average. The maximum-power jammer influences on the wider channels. We find that the whole 2.4GHz ISM frequency bands used by IEEE 802.11g are completely jammed by either the minimum-power jammers which jam five channels (Ch. 2, 5, 8, 11, 12) or the maximum-power jammers which jam four channels (Ch. 3, 7, 10, 12).



(a) SNR and PDR for $P_A = 6dBm, P_J = 0dBm$ ($P_A \approx 4P_J$)

(b) SNR and PDR for $P_A = 0dBm, P_J = 0dBm$ ($P_A = P_J$)

(c) SNR and PDR for $P_A = 0dBm, P_J = 6dBm$ ($4P_A \approx P_J$)

Figure 2: Jamming boundaries are formed by one jammer at $(0, 0)$ and one AP at $(10, 0)$.

4. JAMMER ARRANGEMENT

In this section, we discuss how to arrange the defensive jammers to carve a wireless zone around an arbitrary geometry. Note that our interest is not in developing an optimal algorithm, but in presenting the feasibility of automatic placement of defensive jammers.

Let us define the initial wireless zone IWZ as the wireless coverage of an AP without jamming. The size of IWZ is confined by the transmitting power P_A of AP. Because IWZ exceeds the specified target zone TZ on which any intruder cannot physically trespass, we want to confine IWZ into the secure wireless zone SWZ which fits into TZ, by installing N_J number of defensive jammers around TZ. The algorithms determine the transmitting power P_{J_i} and the location L_{J_i} of each jammer J_i to satisfy this condition.

For simplicity we assume that TZ is a polygon and the AP is not on the boundary of TZ. Our objectives are: 1) maximizing SWZ, 2) minimizing N_J, 3) minimizing $\sum_i P_{J_i}$. In a real scenario, defensive jammers not only can be freely placed, but also cannot be placed in random positions due to the barriers such as uncontrollable structures and neighboring legitimate wireless zones. We address both of the cases and provide the detailed algorithms for each case in [6].

4.1 Relocatable Defensive Jammers

In this scenario, we assume that we can control the location of defensive jammers as well as the jamming power. To maximize SWZ, the shapes of jamming boundaries need to be straight along the side of the given polygonal TZ. As we investigated earlier, a straight boundary is formed when the jammer and the AP are line symmetrical to the jamming boundary and their transmitting powers are equivalent.

If, however, the given target zone is a concave polygon, then the placement of jammers should be considered more cautiously. Simply finding the points of symmetry results in unsuitable positioning of jammers especially in the concave region of the given polygon. In Fig. 3(a), a concave octagon consists of vertices, $v1 \sim v8$. Different from other vertices, the internal angles of $v5$ and $v6$ are larger than their external angle. Let us define the *concave vertex* as a vertex at which the internal angle is larger than its external angle, and the *concave side group* as the group of sides which include adjacent *concave vertices*. A concave polygon can have multiple of *concave side group*, but the polygon in this example has only one for simplification. Instead of placing three jammers corresponding to three sides in the *concave side group* of the example, only one jammer can cover the concave area.

The vertex $v4.7$ is the middle point between the two end vertices of the *concave side group*, $v4$ and $v7$. The line c passes through AP and $v4.7$, four perpendicular lines $l4$, $l5$, $l6$, and $l7$ to c pass through each vertex included in the *concave side group*. Among these perpendicular lines, we choose $l5$ which is closest to AP. In Fig. 3(a), the location of jammer $J4$ is obtained by finding the point of symmetry of AP to the selected line $l5$.

While the number of required defensive jammers is reduced by two, the formed SWZ only occupies about 65% of TZ. To maximize SWZ, we can reduce the transmitting power P_{J4} of $J4$. Here, $J4$ should move closer towards AP for SWZ not to exceeds TZ. In our simulation, a defensive jammer can adjust its transmission power at intervals of ten percent of the AP. We found SWZ is at peak size when $P_{J4} = P_A/10$ and $J4$ moves to the point $J4'$. In so doing, the size of SWZ increases to about 80% of the given TZ.

4.2 Fixed Defensive Jammers

Fig. 3(c) shows the scenario in which we can only control the transmitting powers of defensive jammers. We assume that each side of TZ has at least one corresponding defensive jammer. Each jammer increases its transmitting power to be higher than AP's, if the closer vertex to AP in the corresponding side is closer to AP than the jammer. It should increase the power until the jamming boundary intersects with the extended line of corresponding side. If the closer vertex to AP in the corresponding side is closer to the jammer than AP, the jammer inversely decreases its power until the jamming boundary intersects with the corresponding side. By using this method, the simulation in Fig. 3(c) determines that the transmitting power of $J1$, $J2$, $J3$, and $J4$ should be 40%, 100%, 420%, 60% of P_A, respectively, and SWZ occupies about 56% of TZ. This tells us that there is a limitation to maximize the SWZ without relocating the

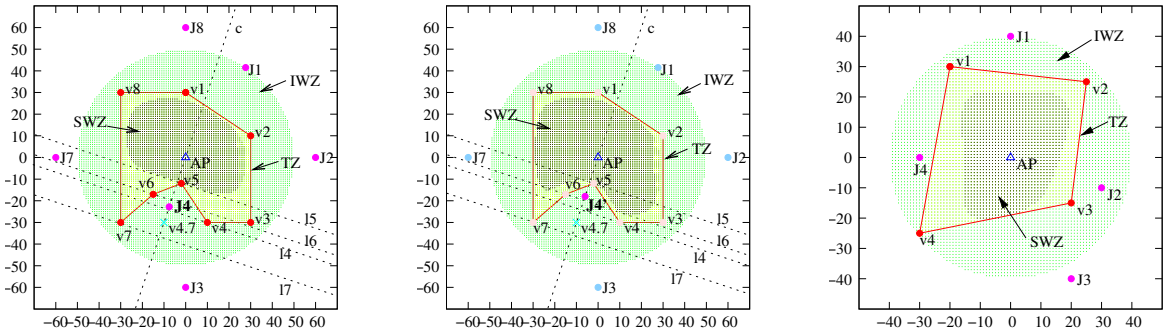


Figure 3: Jammer arrangement: jammers are relocatable in (a) and (b), and jammers are fixed in (c).

defensive jammers.

5. RELATED WORK

There is a thick literature on protecting the confidentiality in wireless networks. As mentioned in the introduction, most of them focus on message encryption or authentication protocols, which involve the innate key management problem. Our approach is different from them in that it does not require any pre-shared secrecy between nodes.

In [8], Sneth *et al.* uses multiple access points equipped with directional antenna to confine the wireless coverage. Their mechanism, however, cannot defend against the information leakage. There are commercial products and services based on wireless physical access control using location-based access policy management [1] or fine tuned distributed antennas [2]. All of these approaches are very costly since they require accurate site survey, testing, parameterization of the building or zone of interest, and specialized hardware/software systems. Tiwari *et al.* propose a radio device to prevent access from the exterior of secure wireless area in [9]. This device waits until receiving the internal wireless signal and sends the jamming signal to the direction of the outside for cloaking messages. It requires the complex hardware including two separate antenna for receiving and transmitting, and should interpret the receiving signal in a very short period.

6. CONCLUSION

Traditionally, jamming has been regarded only as an attack method. In this paper, we completely reverse the view and explore its potential as a defensive weapon against information leakage through covert wireless channel establishment. As much as the jamming attack is hard to defend against, the proposed "defensive jamming" can provide a formidable physical barrier that both logical and physical information leaking attempts can hardly break.

The protected geography created by defensive jamming, which we term "jamming boundary", is defined by the power and location arrangements of the protected APs and the jammers. We derive a computational model of the jamming boundary as a function of the powers and locations of the APs and the jammers. To validate the proposed model, we take extensive outdoor measurements and demonstrate the SNR and the PDR indeed drops to zero at the jamming boundary. Lastly, we discuss how to find the optimal jammer placement given the desired protected topology.

7. REFERENCES

[1] The AIRPATROL Cellular and Wireless Intelligence Solution. Available from: `http://www.airpatrolcorp.com`.

[2] InnerWireless, Inc. Available from: `http://www.innerwireless.com`.

[3] J. I. Choi, M. Jain, K. Srinivasan, P. Levis, and S. Katti. Achieving single channel, full duplex wireless communication. In *Proceedings of the sixteenth annual international conference on Mobile computing and networking*, MobiCom '10, pages 1–12, New York, NY, USA, 2010. ACM.

[4] D. Halperin, T. Anderson, and D. Wetherall. Taking the sting out of carrier sense: interference cancellation for wireless lans. In *Proceedings of the 14th ACM international conference on Mobile computing and networking*, MobiCom '08, pages 339–350, New York, NY, USA, 2008. ACM.

[5] Y. S. Kim and H. Lee. On classifying and evaluating the effect of jamming attacks. In *The 24th edition of the International Conference on information Networking (ICOIN)*, 2010.

[6] Y. S. Kim, P. Tague, H. Lee, and H. Kim. Carving secure wi-fi zones with defensive jamming. Technical report, Wireless Network and System Security Lab, CMU, Apr. 2012. Available from: `http://wnss.sv.cmu.edu/papers/TR-DefJam.pdf`.

[7] R. A. Poisel. *Modern Communications Jamming Principles and Techniques*. Artech House, Inc., 2004.

[8] A. Sheth, S. Seshan, and D. Wetherall. Geo-fencing: Confining wi-fi coverage to physical boundaries. In H. Tokuda, M. Beigl, A. Friday, A. Brush, and Y. Tobe, editors, *Pervasive Computing*, volume 5538 of *Lecture Notes in Computer Science*, pages 274–290. Springer Berlin / Heidelberg, 2009.

[9] S. Tiwari. Wireless perimeter security device and network using same, March 2008. Available from: `http://www.freepatentsonline.com/7349544.html`.

[10] W. Xu. On adjusting power to defend wireless networks from jamming. In *4th Annual International Conference on Mobile and Ubiquitous Systems : Networking & Services*, 2007.

[11] W. Xu, W. Trappe, and Y. Zhang. Anti-jamming timing channels for wireless networks. In *Proceedings of the first ACM conference on Wireless network security (WiSec '08)*, 2008.