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. From an existing non-isotropic jamming theory, we construct a computational model for the protected geography forged by the defensive jamming. The model is spelled out in terms of the arrangement of the jammers, the transmitter, and the receiver, and the transmitting powers. Parameters are included in order to fine-tune the model to fit with the given physical environment. 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 and discuss the considerations for the practical deployment of our approach.

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?

Such problem cases are illustrated in Fig. 1, with an enterprise network example. The environment consists of a wired network protected by firewalls, and WLANs providing additional access to the wired backbone. The physical coverages of the APs are mostly contained in the physical perimeter PA_E of the enterprise, for example the access-point AP_1 has coverage WA_1. However, it is possible for wireless intrusions to occur, of which there are three types as exemplified as follows.[1]

- Case 1 : The rogue station ST_2 outside connects to the ill-protected access-point AP_2 inside.
- Case 2 : The rogue station ST_3 inside connects to the rogue access-point AP_3 outside.
- Case 3 : The ill-protected station ST_4 inside connects to the rogue access-point AP_4 outside.

Most of security protocols developed for wireless networks so far intend to protect the network from the attacker outside (*i.e.*, Case 1). Since, however, an insider who attempts

[1] We assume that enterprises can and do detect the rogue APs inside, and the case is excluded from our discussion.

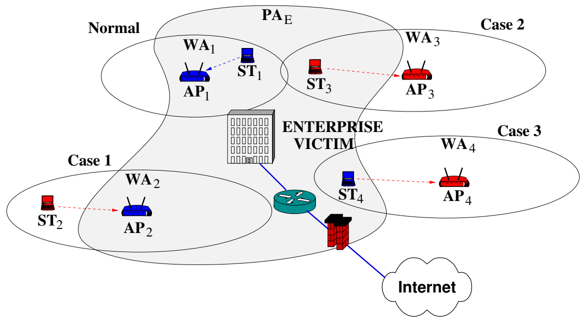


Figure 1: Different ways of information leakage

to pilfer the critical information may divulge the secret key, these protocols do no good. The wrongdoer can create a covert channel to the collaborator located outside as in Case 2. It is even possible that an innocent and less tech-savvy user inside unknowingly builds the wireless association with the rogue AP outside as in Case 3. Indeed, many of today's wireless connection management softwares are happy to associate automatically with any open APs around.

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 [17], 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 [13]. 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. Starting from the non-isotropic model used in [17], we show how we can *shape the protected areas* using jammers, and identify the parameters that control the shape. In Section 3, we reveal how well the theoretical model is matched with the real world measurements, which we conducted using the IEEE 802.11g WLAN devices, noting that our method is not limited to the IEEE 802.11 technology; the physical jamming model applies to any other wireless networks. We introduce an algorithm for defensive jammer arrangement to carve the wireless zone into a specified geometry in Section 4. We discuss the considerations for the real application of the proposed mechanism in Section 5. Section 6 overviews the related work. Finally, we conclude the paper in Section 7.

2. THEORETICAL JAMMING MODEL

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. In this model, we define what we call the *jamming boundary*, which encloses the protected wireless zone created by the given group of jammers. We identify the parameters that dictate the shape of the protected zone. 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 cryptography-based security. The mechanism must not depend on any preshared 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 [7, 6], high-gain antenna, etc.), but because these are very expensive to implement we can significantly increase the attacking cost and efficiently mitigate the attack. We will also discuss the possible countermeasures to defend against these techniques in the later section.

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.

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

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[2] and apply the line-of-sight (LOS) propagation model [11, 12] to the received power at S. Here, 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

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

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 [12].

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. In the theoretical analysis, we will 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. 2 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 $\beta = 1$. When two sources A and J have a symmetric transmitting power, the jamming boundary is a line between them (b_3). As P_J increases, however, the boundary pushes towards A. For instance, if we increase P_J fourfold, the boundary will be the circle whose center is at $(-j, 0)$ and the radius is $\sqrt{2}j$ (b_2). With nine fold increase of P_J, the boundary constrains the signal reception from A further (b_1). In essence, higher P_J moves the center of the boundary circle closer to A, and makes the radius smaller. In contrast, the jamming boundaries are formed around the jammer if P_A becomes larger than P_J (b_4 and b_5). Although not shown for brevity, this relationship is maintained for other values of n as well. For one instance, Table 1 shows the power relationship between A and J for the boundaries shown in Fig. 2.

The precise circular curves depicted in Fig. 2 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.

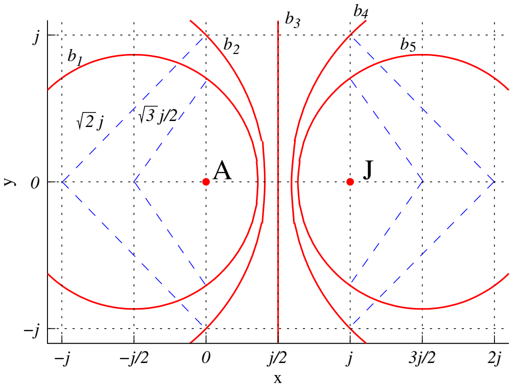


Figure 2: Jamming boundaries with various parameters

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. 2

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

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

In practice, note that there is a small probability the attackers can get access for very short time durations due to natural fluctuations in the channel quality or noise parameters. The neglect of the noise N_0 gives a conservative estimate of the SINR.

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.

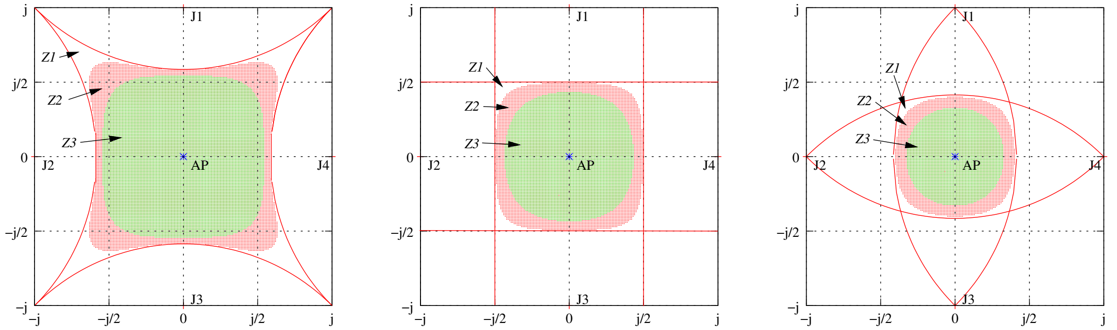
Definition 1. *(Area Accessible To AP) If a station in the area $Z_A(J_1, J_2, \cdots, J_k)$ can receive data from the AP A under k jammers, Z_A is defined as an area accessible to AP. Namely,*

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

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.

[2] This simplifying assumption will lead to a slight overestimation of the protected area.



(a) $P_A = 4P_J$ for $n = 4$, $P_A = 2P_J$ for $n = 2$

(b) $P_A = P_J$ for both $n = 4$ and $n = 2$

(c) $4P_A = P_J$ for $n = 4$, $2P_A = P_J$ for $n = 2$

Figure 3: The secure wireless zone formed by four jammers is illustrated for several different parameter choices. The line $Z1$ shows the intersection $Z(J_1) \cap Z(J_2) \cap Z(J_3) \cap Z(J_4)$ of the individual secure zones formed by each of four jammers. The line $Z2$ is the secure wireless zone formed by the four jammers for the path-loss exponent $n = 4$. The line $Z3$ is for $n = 2$.

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 Theorem 1 of Appendix A. 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*

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

Fig. 3 illustrates the secure wireless zone formed by a single AP A and four surrounding jammers, each of which is placed from the AP by distance j. Three cases are considered in the figure: (1) $P_A > P_J$, (2) $P_A = P_J$, and (3) $P_A < P_J$. In particular, we apply the parameters used in Fig. 2: $P_A = 4P_J$, $P_A = P_J$, and $4P_A = P_J$ for $n = 4$ and $P_A = 2P_J$, $P_A = P_J$, and $2P_A = P_J$ for $n = 2$. In the figure, Z_1 is the intersection of the areas, which are delimited by red lines, accessible to the AP under each single jammer, Z_2 is the area accessible to the AP under four jammers for $n = 4$, and Z_3 is for $n = 2$. As in Theorem 1 of Appendix A, it also satisfies that $Z_2 \subset Z_1$, and $Z_3 \subset Z_1$. Notably, for the larger n, the size of area accessible to AP increases and approximates to Z_1. In Fig. 3, the size of Z_2 is as large as 86 $\sim$ 90% of Z_1, while one of Z_3 is only 54 $\sim$ 63% of Z_1. Intuitively, this is because the larger path-loss exponent makes the jamming power decrease more rapidly, thus diminishing the effect of far jammers compared to that of the nearby jammer.

The shaded areas in the figure are the secure wireless zones. As expected, the size of the secure wireless zone decreases as P_J increases. Note that the area accessible to AP for $P_A > 4P_J$ at $n = 4$ may not be a secure wireless zone because there can be an area which L_O intersects with $Z_A(J_1, J_2, J_3, J_4)$. Intuitively, the increased AP power "pushes away" the jamming so that a corridor of access is open between the jammers towards the AP. For instance, in Fig. 3(a) the four corners of the boundary can burst open so that an attacker can access the AP signal from those angles.

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 [13], 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 map of the test site is given in Fig. 4. At the center there is a 10×10 meter square with concrete floor.

The experiment is divided into three parts. First, we demonstrate that the shape of the jamming boundary between a jammer and a transmitter follows the theoretical model. Second, we show the secure wireless zone can be shaped as desired by using multiple jammers. Third, 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

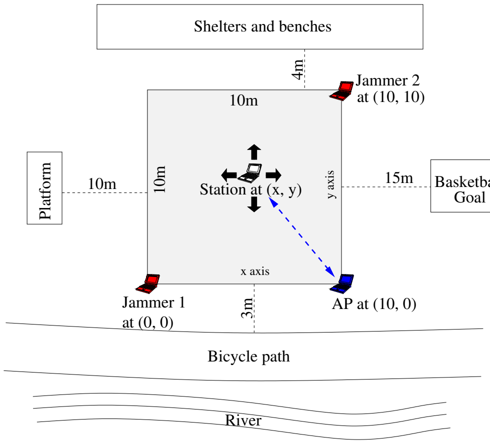


Figure 4: Geographic environment for experiments

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 [15]. We use the modified MadWifi driver [4] 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 [10]. We change the location of the station in the test site square and measure the delivery status of the traffic from the AP. The AP and the jammers are denoted as AP and Jammer 1 in Fig. 4.

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 [9] and iperf [10] 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. 5. 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. 5(a) is approximate to b_4 in Fig. 2, and the same trend holds in Fig. 5(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 Secure Wireless Zone Shaping

In this experiment, we use two jammers to show that the secure wireless zone can be carved out from two angles. For convenience's sake, we do not use four jammers, which would be necessary to fully encircle the AP. Symmetry will ensure that the complete isolation (from all four angles) will be achieved there.

The disposition of Wi-Fi nodes is shown by the AP and the two jammers in Fig. 4. We use the identical jammer in the first experiment and set the power level to 0dBm. In order to show that the result is not dependent on a specific hardware platform, we use the different type of Wi-Fi adapters which is based on Ralink chip-set and equipped with the external antenna for the AP and the station. The adapters operate with the commercial device driver on Windows XP. We set their transmitting power to 3dBm. Without jammers the PDR is measured as 100% in any position of the test site.

As shown in Fig. 6, a secure wireless zone is formed by two jammers although the different types of Wi-Fi adapters are used for the AP and the station. At this time, the SNR changes smoothly and the PDR is not completely zero at some points outside the secure wireless zone. We believe that this is due to the higher antenna gain from the external antenna and the different measuring method of the bundled software for the Wi-Fi adapter.

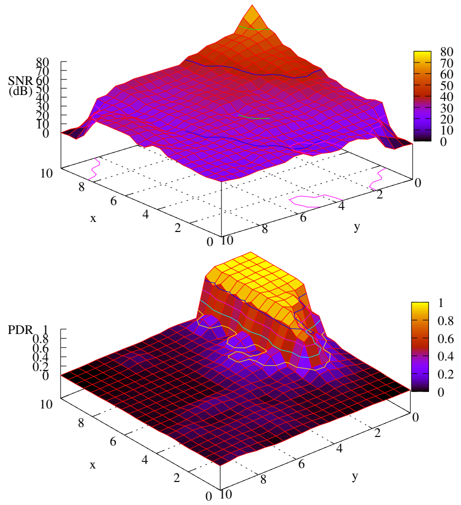
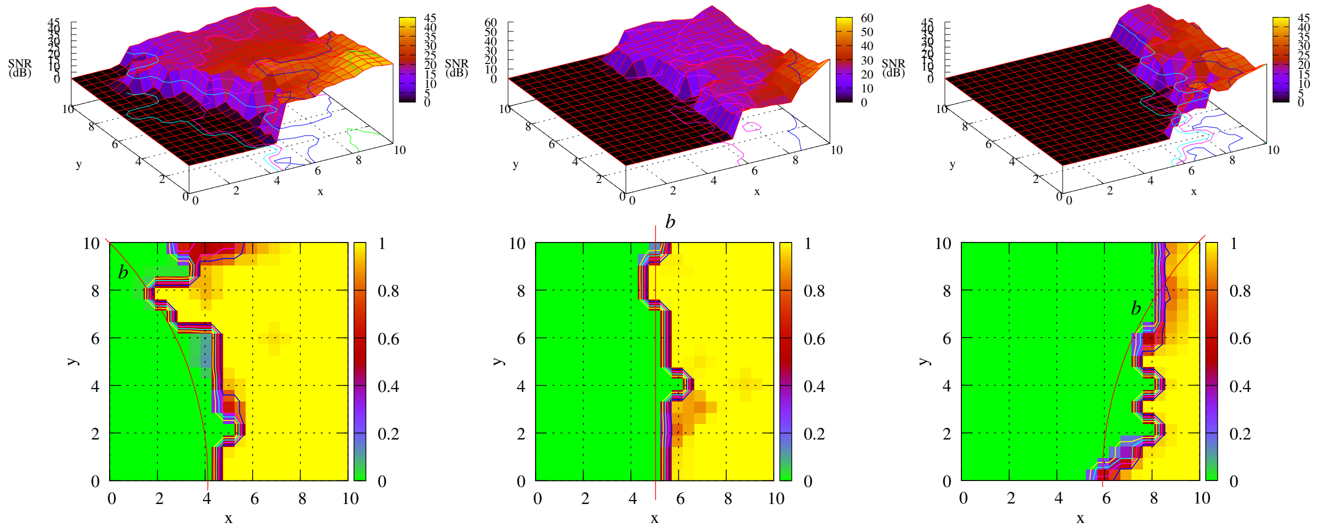


Figure 6: Experiment 2 - isolated area formed by two jammers at $(0, 0)$, $(10, 10)$ and one AP at $(10, 0)$

3.3 Effect of Jamming 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



(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 5: Experiment 1 - jamming boundary formed by one jammer at $(0, 0)$ and one AP at $(10, 0)$

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). We expect that this consistency will be still remained even when the Wi-Fi nodes locate farther away from the jammer because the distance affects rather the signal strength than the frequency.

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. Table 2 summarizes the zone notations.

Symbols	Definition
IWZ	Initial wireless zone of AP without jamming
SWZ	Secure wireless zone carved by jammers
TZ	Target zone enclosed by physical perimeter

Table 2: Zone Notations

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, neighboring legitimate wireless zones, and so on. Thus, we address both of the cases. We provide the detailed algorithms for the two cases in Appendix B.

4.1 Relocatable Defensive Jammers

In this scenario, we assume that the location of defensive jammers is controllable. Of course, the transmitting power of jammers are also adjustable. In order to maximize SWZ, the shape of jamming boundaries needs 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. As shown in Fig. 7, the locations of defensive jammers are easily calculated by finding the point of symmetry of the AP to each side of the given TZ. In Fig. 7, SWZ created by jammers $J1 \sim J3$ occupies about 89% of TZ.

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

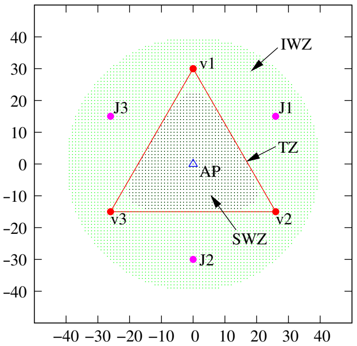
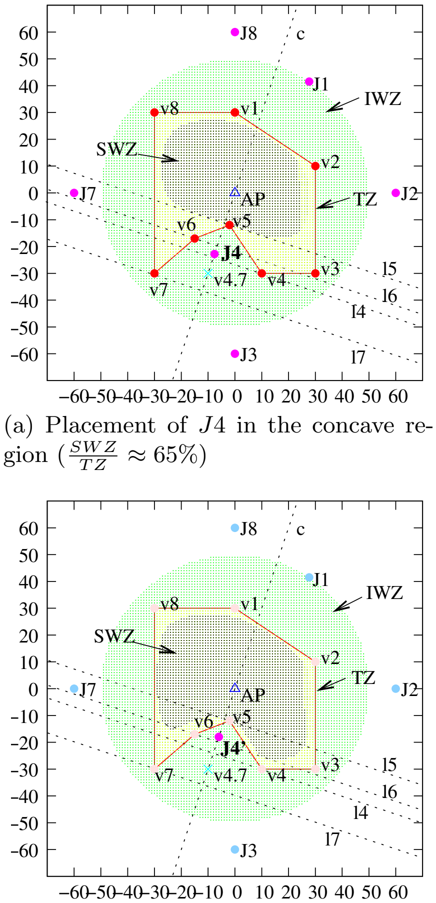


Figure 7: Jammer arrangement for triangular zone ($\frac{SWZ}{TZ} \approx$ 89%)



(a) Placement of $J4$ in the concave region ($\frac{SWZ}{TZ} \approx 65\%$)

(b) Transmitting power reduction of $J4$ ($\frac{SWZ}{TZ} \approx 80\%$)

Figure 8: Jammer arrangement for concave octagon

unsuitable positioning of jammers especially in the concave region of the given polygon. In Fig. 8, 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 a *concave vertex* be a vertex at which the internal angle is larger than its external angle. And a *concave side group* is expressed 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 $v4.7$. And four lines $l4$, $l5$, $l6$, and $l7$ pass through each vertex included in the *concave side group* and are perpendicular to c. Among these lines, $l5$ which is closest from AP is chosen to decide the location of jammer. In Fig. 8(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 adjust the transmitting power P_{J4} of $J4$. If we reduce P_{J4} in Fig. 8, $J4$ should move closer towards AP for SWZ not to exceeds TZ. In the simulation, the 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. 9 shows the scenario in which we can only control the transmitting powers of fixed 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. 9 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 defensive jammers.

5. PRACTICAL CONSIDERATIONS

In this section, we discuss more considerations for the practical deployment of the proposed approach.

5.1 Interference to Legitimate Communication

The defensive jammers can interfere with the legitimate communication inside the target wireless network. In the Wi-Fi network based on CSMA/CA, the wireless stations close to the jammers will suffer from the difficulty in channel reservation for frame transmission. A transceiver senses the channel reservation if it detects any receiving signal is higher than the clear channel assessment (CCA) level. Thus, we can reduce the interference from the defensive jammer by increasing the CCA level in the legitimate wireless stations. On the other hand, the CCA level increment can result in

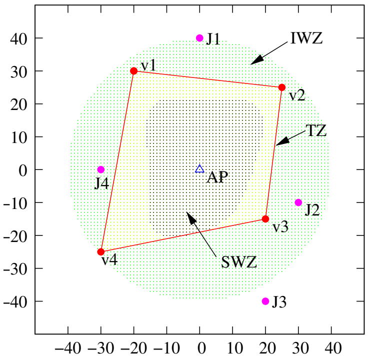


Figure 9: Arrangement of fixed defensive jammers ($\frac{SWZ}{TZ} \approx$ 56%)

the collision among the wireless stations, and therefore the value should be cautiously chosen.

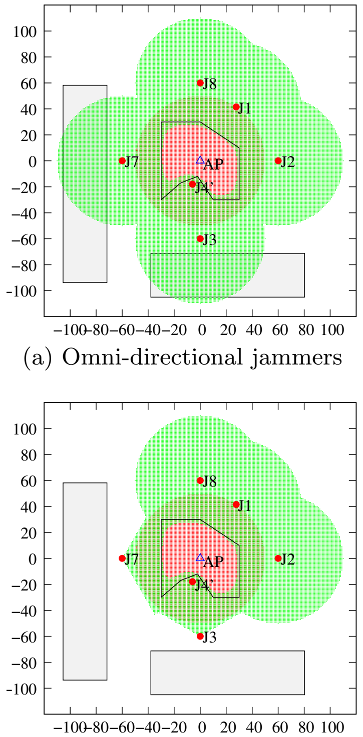
In the metropolitan area the installed defensive jammers may also interfere with the legitimate communications in neighboring buildings. Fig. 10(a) shows the interference pattern of defensive jammers and the interference range overlaps with the neighboring buildings. In this case, we can use the directional antenna for defensive jammer. The jammer $J3$ and $J7$ in Fig. 10(b) are equipped with the 120 degree of sector antennas. The deployment of directional antenna, however, should be carefully considered because an attacker's device can be placed in the unjammed area to attempt the illegal access to the target network.

5.2 Buffer Zone for Defensive Jammer Placement

If the jammer is too close to the wireless stations inside the target zone, the jamming signal will severely affect the legitimate communication of the wireless stations. The jammer J should thus be placed at minimum the distance $d_{min,S}$ away from the possible location of the wireless station S. If J is too close to the outside attacker M, it will give more chances that M can win J by increasing its transmitting power or avoiding the jamming signal with the directional antenna. This also makes J to be distant enough from the outside attacker M and we denote this distance as $d_{min,M}$. As we increase $d_{min,M}$, the SINR at the inside station to the attacker's signal will become lower. Therefore, if possible in the real configuration, it is better to have a separate buffer zone in which any attacker cannot be placed around the target area. In Fig. 11, the buffer zone is represented as BZ which of the width is $d_{min,S} + d_{min,M}$.

5.3 Defense against More Intelligent Attacker

Depending on the attacking scenario, an attacker might afford to use the more intelligent techniques which require costly resources. One of those techniques uses the high-gain antenna. In Fig. 12(a), the attacker M who has a high-gain antenna attempts to get the illegal access to the AP A. The attacker M will tilt the antenna to make the antenna gain G_{MA} of M to A larger than the antenna gain G_{MJ} of M to J. A malicious inside station S can also do the same as M does. This results in the significant increase in SINR at both M and A to the other end of each, and thus making J invalid. This will occur even when the attacker is willing to and able to spend high transmitting power to defeat jamming.



(a) Omni-directional jammers

(b) Combination with directional jammers

Figure 10: Interference pattern of defensive jammers

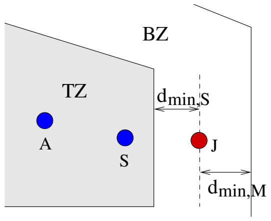
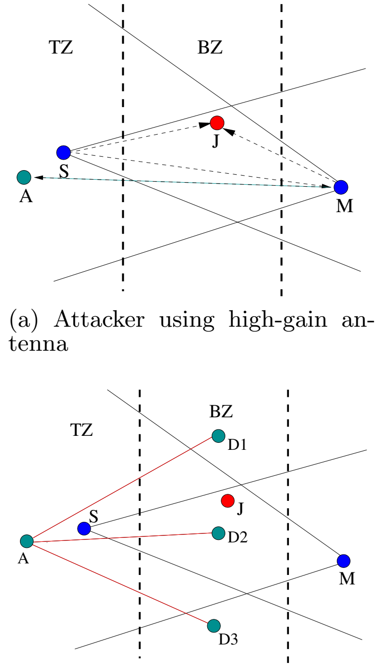


Figure 11: Buffer zone setting

To cope with this type of intelligent attack, we can install the special detectors denoted as $D1$, $D2$, and $D3$ in the buffer zone as in Fig. 12. The detectors are connected to a central point such as the AP with the separate wirelines. All of inside wireless stations are regulated to use the transmitting power under a given threshold ψ_{max}. If any inside station tries to transmit any frame to the outside with the transmitting power higher than ψ_{max}, some of detectors will sense the stronger signal than the threshold ρ_{in} and report this malicious behavior to the central point via the wired channel. Likewise, if the outside attacker transmits any frame with high-gain antenna and high transmitting power, some of detectors will also detect it by the receiving power higher than the threshold ρ_{out} and report to the central point. The reported central point can take relevant actions such as frame dropping depending on the situation. The values of ψ_{max}, ρ_{in}, and ρ_{out} are determined by the relative position of each detector to the target area and their density. The detailed discussion on the value selection is out of scope here and we will investigate in our future work.



(a) Attacker using high-gain antenna

(b) Defense mechanism for intelligent attacker

Figure 12: Intelligent attacker and defense mechanism

5.4 Field Considerations

As shown in experiments, the real jamming boundary is not regular in real practice due to the natural fading effects. It will become more severe in an indoor environment due to many obstacles hiding LOS communication path. Thus, it is required to do a site survey to deploy the defensive jammers in the field. By adaptively adjusting the parameters of each jammer, one can build a reasonable secure wireless zone.

Depending on the configuration on which the wireless stations and the jammer are installed, there are different scenarios as shown in Table 3.

Scenario	Stations	Jammers	Examples
$S1$	indoor	indoor	enterprise, home
$S2$	indoor	outdoor	enterprise, home
$S3$	outdoor	indoor	N/A
$S4$	outdoor	outdoor	battle field, outdoor monitoring

Table 3: Different scenarios depending on configuration

It is generally unusual to install the jammer indoors for the outdoor wireless network as in $S3$. The outdoor scenario $S4$ for both the wireless nodes and the defensive jammers will suffer relatively less from the multipath fading effects. When both type of nodes are placed indoors, they will experience the similar pattern of path loss. Thus, we expect the similar results in $S1$ with $S4$ except for the different path-loss exponent n.[3]

If the wireless nodes stay indoors and the jammers stay outdoors ($S2$) as in Fig. 13, then the path-loss to each type of nodes will be different. It is well-known that the path-loss gets worse in an indoor environment, thus increasing the path-loss exponent n [11, 12]. Similar to Eq. (2), we can derive $P_{AS}/P_{JS} = (P_A \cdot D_{JS}^{n_o})/(P_J \cdot D_{AS}^{n_i})$ for an AP A, a receiving station S, and a jammer J, where n_i and n_o are the path-loss exponent for indoor and outdoor environments, respectively. If we place AP and J equally distant from the wall of the building and set their transmitting power to the same, then the original jamming boundary $b1$ pushes toward AP like $b2$. This will eventually provide us with the tighter secure wireless zone.

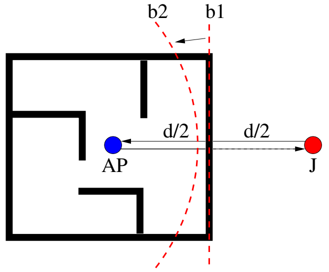


Figure 13: AP indoor and jammer outdoor

In terms of security this smaller secure wireless zone is beneficial, however it provides poor channel access to the wireless nodes within the building in return. If there is an available buffer zone along the wall of the building, we can both increase the secure wireless zone and provide the reasonable protection from the outside attacker by slightly decreasing the power of defensive jammer. The buffer zone should be large enough to cover the curvature of the jamming boundary around the wall. At the same time, the curvature around the wall should be small enough by the intricate power control of jammer not to expose the access breach to the outside attacker.

6. 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 [14], 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 scenarios in the introduction. Martinovic *et al.* also exploit the jamming as a tool to defend against attack [8]. They focus on protecting from the malicious packet injection.

[3] We show the different shape of the secure wireless zone with the different path-loss exponents in Fig. 3.

There have been studies about mitigating the effect of jamming. In [18], Xu *et al.* suggest the channel surfing and the spatial retreat as defensive measures against jamming attacks. Obviously, the spatial retreat cannot circumvent the proposed mechanism as long as the eavesdropper is influenced by defensive jammers outside the target zone. The channel surfing is also invalid if all available channels are occupied by broadband jamming or multi-channel jamming. In [5, 3], the authors suggest similar approaches using multi-channels. In [19], Xu *et al.* propose the timing channel over which multi-senders and a receiver still can communicate with each other under jamming. However, it is useful only for low-speed signals, not for high-speed data due to its low throughput (slower than 10 bps). In addition, the timing channel is vulnerable to the random jamming.

Tiwari *et al.* hold a patent, which defines a radio device to prevent access from the exterior of secure wireless area [16]. 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, which includes two separate antenna for receiving and transmitting and should interpret the receiving signal in a very short period. Moreover, this approach cannot help interfering with the neighboring legitimate communications since the jamming device always emits the signal outside.

There are some commercial products and services for wireless physical access control using location-based access policy management [2] or finely-tuned distributed antennas [1]. But, 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.

7. 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 essentially defined by the power and location arrangements of the protected APs and the jammers. Based on the theoretical propagation model, we derive a computational model of the jamming boundary as a function of the powers and locations of the APs and the jammers. In order 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 and the practical considerations for our approach.

Acknowledgement

The authors would like to thank Ju-suk Lee for his help in conducting experiments and giving valuable advices to this work.

8. REFERENCES

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

[2] The AIRPATROL Cellular and Wireless Intelligence Solution. Available from: `http://www.airpatrolcorp.com/products/cellular-and-wireless-intelligence-solution.php`.

[3] G. Alnifie and R. Simon. A multi-channel defense against jamming attacks in wireless sensor networks. In *International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems*, 2007.

[4] E. Anderson, G. Yee, C. Phillips, D. Sicker, and D. Grunwald. Commodity ar52xx-based wireless adapters as a research platform. Technical Report CU-CS-XXXX-08, University of Colorado at Boulder, Department of Computer Science, Campus Box 430, Apr. 2008.

[5] M. Cagalj, S. Capkun, and J. Hubaux. Wormhole-based anti-jamming techniques in sensor networks. *IEEE Trans. Mobile Computing*, 6(1):100–114, Jan. 2007.

[6] 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.

[7] 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.

[8] I. Martinovic, P. Pichota, and J. B. Schmitt. Jamming for good: a fresh approach to authentic communication in wsns. In *Proceedings of the second ACM conference on Wireless network security*, WiSec '09, pages 161–168, New York, NY, USA, 2009. ACM.

[9] J. Morgenstern. Wavemon 802.11 monitor (v.0.4.0b), Dec. 2002. Available from: `http://eden-feed.erg.abdn.ac.uk/wavemon/`.

[10] NLANR/DAST. Iperf v2.0.3, Mar. 2008. Available from: `http://sourceforge.net/projects/iperf`.

[11] R. A. Poisel. *Introdunction to Communication Electronics Warfare Systems*, chapter 2, pages 27–33. Artech House, Inc., 2002.

[12] R. A. Poisel. *Modern Communications Jamming Principles and Techniques*, chapter 2. Artech House, Inc., 2004.

[13] Y. seung 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.

[14] 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.

[15] The MadWifi project team. Madwifi v0.9.4, Feb. 2008. Available from: `http://madwifi-project.org/`.

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

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

[18] W. Xu, K. Ma, W. Trappe, and Y. Zhang. Jamming sensor networks: attack and defense strategies. *Network, IEEE*, 20(3):41 – 47, May 2006.

[19] 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.

APPENDIX

Appendix A. Area Accessible to AP under Multiple Jammers

THEOREM 1. *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.*

$$Z_A(J_1, J_2, \cdots, J_k) \subset Z_A(J_1) \cap Z_A(J_2) \cap \cdots \cap Z_A(J_k)$$

PROOF. Ignoring N_0 in Eq. (3), Z_A is expressed as follows.

$$Z_A(J_1, J_2, \cdots, J_k) = \Big\{(x,y)\Big|\frac{P_{AS}(x,y)}{\sum_i^k P_{J_iS}(x,y)} > \beta\Big\}. \quad (4)$$

Let $\alpha_p(x,y) = \sum_i^k P_{J_iS}(x,y) - P_{J_pS}(x,y)$ for given x and y, where $1 \le p \le k$. Then,

$$\frac{P_{AS}(x,y)}{\sum_i^k P_{J_iS}(x,y)} = \frac{P_{AS}(x,y)}{P_{J_pS}(x,y) + \alpha_p(x,y)} > \beta.$$

Since $\alpha_p(x,y) > 0$ for any x, y, and p,

$$\frac{P_{AS}(x,y)}{P_{J_pS}(x,y)} > \frac{P_{AS}(x,y)}{P_{J_pS}(x,y) + \alpha_p(x,y)} > \beta.$$

This means that all elements in $Z_A(J_1, J_2, \cdots, J_k)$ satisfy the condition in $Z_A(J_p)$.

$$Z_A(J_1, J_2, \cdots, J_k) \subset Z_A(J_p),$$

where $1 \le p \le k$. □

Appendix B. Defensive Jammer Arrangement Algorithms

We introduce the detailed procedures which are mentioned in Section 4 to arrange the defensive jammers. In Algorithm 1, it is assumed that the jammers can be placed at any points around the given target zone. The procedure $GetJammerSetting()$ takes the location L_{AP} of AP, the transmitting power P_{AP} of AP, and the array $Array(v)$ of vertices which form the k-polygonal boundary of the given target zone. The array $Array(L_J)$ of the calculated jammer locations and the array $Array(P_J)$ of the calculated jammer powers are returned by $GetJammerSetting()$. In Algorithm 2, it is assumed that the location of each jammer is fixed. The procedure $GetJammerPower()$ takes the array $Array(L_J)$ of k jammer locations as well as L_{AP}, P_{AP}, and $Array(v)$. The result from $GetJammerPower()$ is the array $Array(P_J)$ of calculated jammer powers. Each procedure uses the following sub-functions.

- $GroupConcaveSide(Array(v))$ - This takes the array of vertices and returns an array of groups, each of which includes neighboring concave sides. The concave side is defined as a side which includes any concave vertex at which internal angle is larger than the external angle.
- $SymmetricPoint(l,p)$ - This takes the line l and the point p. The returned value is the symmetric point of p to l.
- $MidPointBwnEndVertices(l)$ - Literally, this returns the middle point of the two end-points of the given line l.
- $PerpendLine(l,p)$ - This returns the perpendicular line to the given line l while passing the given point p.
- $Distance(l,p)$ - The calculates the distance between the line l and the point p.
- $MinDistTwdAP(P_J, P_{AP}, L_J, L_{AP}, Array(v))$ - For the given power P_J of jammer, the given power P_{AP} of AP, the given location L_J of jammer, and the given location L_{AP} of AP, this function calculates the jamming boundary between the jammer and the AP. If the jamming boundary locates outside the target zone specified by the array $Array(v)$ of vertices, this function returns at least how much the jammer J should move towards to the AP to make the jamming boundary locate inside the target zone.
- $MoveFromAToB(p,q,d)$ - This moves the point p towards the point q with the d units of distance.
- $CorrespondingJammerWith(l)$ - This returns the index of jammer which directly faces with the given line l.

Algorithm 1 Arrangement of defensive jammers for k-polygon ($\forall i, L_{J_i}$ is a variable)

```
procedure GetJammerSetting($L_{AP}, P_{AP}, Array(v)$)
    $Array(CSG) \leftarrow GroupConcaveSide(Array(v))$
    for $\overline{v[i]v[i+1]}$ in $Array(v)$ do
        if $\overline{v[i]v[i+1]} \notin$ any CSG then
            $Array(L_J) \leftarrow SymmetricPoint(\overline{v[i]v[i+1]}, L_{AP})$
        end if
    end for
    for each $CSG$ in $Array(CSG)$ do
        $q \leftarrow MidPointBwnEndVertices(CSG)$
        $l \leftarrow \overline{q \cdot L_{AP}}$
        for each vertex $v$ in $CSG$ do
            $m \leftarrow PerpendLine(l, v)$
            $Array(< d, m >) \leftarrow Distance(m, L_{AP})$
        end for
        $t \leftarrow Arg_m(Min_d(Array(< d, m >)))$
        $j \leftarrow SymmetricPoint(t, L_{AP})$
        $p \leftarrow P_{AP}$, $d \leftarrow 0$
        while $(p- = MinAdjustablePower) > 0$ do
            $temp \leftarrow MinDistTwdAP(p, P_{AP}, j, L_{AP}, Array(v))$
            if $temp <= 0$ then
                break
            end if
            $d \leftarrow temp$
        end while
        $Array(P_J) \leftarrow p$
    end for
    $Array(L_J) \leftarrow MoveFromAToB(j, L_{AP}, d)$
    return $Array(L_J), Array(P_J)$
end procedure
```

Algorithm 2 Arrangement of defensive jammers for k-polygon ($\forall i, L_{J_i}$ is a constant)

```
procedure GetJammerPower($L_{AP}, P_{AP}, Array(L_J), Array(v)$)
    for $v[i], v[i+1]$ in $Array(v)$ do
        $i \leftarrow CorrespondingJammerWith(\overline{v[i]v[i+1]})$
        $d_{AP} \leftarrow Min(\overline{v[i]L_{AP}}, \overline{v[i+1]L_{AP}})$
        $d_{J_i} \leftarrow Distance(\overline{v[i+1]L_{AP}}, Arg_v(Min(\overline{v[i]L_{AP}})), L_i)$
        $P_{J_i} \leftarrow P_{AP}$
        if $d_{J_i} > d_{AP}$ then
            while $JammingBoundary \bigcap \overleftrightarrow{v[i]v[i+1]} \neq \phi$ do
                $P_{J_i} = P_{J_i} + MinAdjustablePower$
            end while
        else
            while $JammingBoundary \bigcap \overline{v[i]v[i+1]} \neq \phi$ do
                $P_{J_i} = P_{J_i} - MinAdjustablePower$
            end while
        end if
        $Array(P_J) \leftarrow P_{J_i}$
    end for
    return $Array(P_J)$
end procedure
```