Wireless Netw (2015) 21:2631–2647
DOI 10.1007/s11276-015-0935-y

A jamming approach to enhance enterprise Wi-Fi secrecy through spatial access control

Yu Seung Kim[1] · Patrick Tague[1] · Heejo Lee[2] · Hyogon Kim[2]

Published online: 2 April 2015

Abstract Prevalent Wi-Fi networks have adopted various protections to prevent eavesdropping caused by the intrinsic shared nature of wireless medium. However, many of them are based on pre-shared secret incurring key management costs, and are still vulnerable from practical countermeasures. In this study, we investigate the feasibility of using defensive jamming technique to protect enterprise Wi-Fi networks from potential eavesdroppers. This non-cryptographic approach requires *neither* any pre-shared key *or* high deployment costs. Defensive jammers geographically confine the wireless coverage of Wi-Fi access point, and thus block the message reception outside an arbitrary boundary at a physical layer. We provide a theoretical model fine tuning the jamming parameters for jammer placement. We then discuss practical considerations including optimized jammer arrangement algorithms, interference countermeasures to legitimate communications, and countermeasures against advanced attackers.

Keywords Defensive jamming · Eavesdropping · Wi-Fi networks

✉ Yu Seung Kim
yuseungk@cmu.edu

Patrick Tague
tague@cmu.edu

Heejo Lee
heejo@korea.ac.kr

Hyogon Kim
hyogon@korea.ac.kr

[1] Carnegie Mellon University Silicon Valley, Moffett Field, CA, USA

[2] Korea University, Seoul, Republic of Korea

1 Introduction

Ensuring confidentiality has been one of challenging problems in wireless networks. Wireless channel as a medium is shared by all nodes in the same wireless coverage, and thus plenty of efforts have been made to prevent illegitimate eavesdropping in wireless networks. One of popularized approaches is encrypting messages before they are sent over wireless channel. Another approach is to use the physical layer characteristics such as diversity of time, frequency, space, and code so as to hide wireless channel from unintended parties. All of these approaches rely on the pre-shared secret among communicating nodes, and therefore impose the intrinsic key exposure risk or at least require key management costs.

The prevalent Wi-Fi networks have been also protected by encryption based security mechanisms to ensure confidentiality. The *Wired Equivalent Privacy (WEP)* using RC4 encryption is first adopted to Wi-Fi networks. The following *Wi-Fi Protected Access (WPA)* protocol remedies lots of security vulnerabilities caused by WEP. It defines the *pre-shared key (PSK)* mode for home use, and the enterprise mode requiring authentication server and operating with the *IEEE 802.1X* port-based network access control and the *Extensible Authentication Protocol (EAP)*. This WPA protocol is again enhanced by the more secure *WPA2* implementing the IEEE 802.11i Wi-Fi security standard [3], and the WPA2 enterprise mode is widely used for securing Wi-Fi networks which require enterprise level security. An encryption key for unicast messages in the protocol is temporarily generated per session per client, and therefore the exposure of a client's encryption key does not have an impact to other clients' security in the same network.

It is perceived that the WPA2 provides a sufficiently secure protection [17], but fundamental risks still remain in

terms of confidentiality of Wi-Fi networks. The IEEE 802.11i standard aims for encrypting data frames only, and thus an attacker is still able to obtain useful meta-information about the target network by observing management frames. Even the management frame protection defined in the IEEE 802.11w standard [4] cannot resolve this issue, since it can only encrypt the management frames after the association procedure. The authentication server storing all clients' keys obviously becomes a point of failure and the delivery process of encryption key by using EAPs could be insecure. For instance, some legacy EAPs (*e.g.*, LEAP) using insecure channel to deliver the master key are still being used in practice to provide backward compatibility for legacy devices. This motivates us to devise a means which can supplement the current security mechanism used in Wi-Fi networks.

The supplementary mechanism should not be dependent on any pre-shared secret to avoid the same issues caused by existing mechanisms. There have been studies using multiple antennas for secure transmission without pre-shared secret [25, 30], but they require costly hardware and complex signal processing technique. Considering the deployment cost of Wi-Fi networks, these techniques may not be adequate. In this regard, we focus on a physical layer protection using jamming, which has no key dependency and is easily deployable with separate jamming devices. Friendly jamming is such an approach showing the theoretical feasibility of using jamming for ensuring confidentiality of wireless communications [47, 48]. However, there is a gap to apply the information-theoretic results directly to the real world Wi-Fi networks. For example, it is necessary to explain how jamming can be combined into the current Wi-Fi security mechanism, how to configure the jammers in an optimal manner, how to minimize the interference on the surrounding legitimate communication, and so on.

In a typical Wi-Fi set-up requiring confidentiality, there is a distinct geographical boundary which separates between legitimate Wi-Fi clients and the others. In this paper, we focus on protecting Wi-Fi networks from an eavesdropper locating outside a physically secured geographical area. From our previous study [20], we showed that a virtually isolated region, which is accessible to legitimate wireless devices, but is not accessible to unauthorized devices located outside the region, can be created by the defensive jamming technique and validated the mechanism through outdoor experiments. That is, the installed defensive jammers degrade the outside eavesdropper's channel by increasing the interference level around the target area. Based on the previous findings, we extend our discussion to deploy the defensive jammer in practice. We summarize our contribution as follows.

- We suggest *defensive jamming*, a non-cryptographic supplementary approach to mitigate eavesdropping in Wi-Fi networks.
- As shown by the empirical demonstration with commodity Wi-Fi devices in our previous study, the defensive jamming technique is practically deployable, since it requires *neither* modification on existing protocols *or* existing hardware.
- We provide the practical considerations in deploying defensive jamming: optimized arrangement of defensive jammers, interference minimization to legitimate communication, and countermeasures to advanced attacker.

Below, we overview the related work in Sect. 2 and specifically define our problem in Sect. 3. We then present defensive jamming mechanism to prevent eavesdropping in Wi-Fi networks by physically confining the wireless coverage in Sect. 4. We introduce algorithms to arrange defensive jammers around an arbitrary geometry and discuss consideration for real deployment in Sect. 5. We extend our discussion into minimizing interference impact on legitimate communication in Sect. 6 and defending against advanced eavesdropper in Sect. 7. Finally, we conclude the paper in Sect. 8.

2 Related work

Since the IEEE 802.11i amendment approved in 2004 [3], it has become the fundamental measure to secure Wi-Fi networks. It defines two classes of security algorithm: the *robust security network association (RSNA)* and the *pre-RSNA*. While the pre-RSNA provides weaker level of security for backward compatibility with the legacy WEP solution, the RSNA implements the *temporal key integrity protocol (TKIP)* using RC4 cipher, the more secure *counter-mode/CBC-MAC protocol (CCMP)* using AES cipher, and the 802.1X port-based authentication protocol and key management. The WPA2 enterprise mode implements the CCMP, and 802.1X-based authentication and key management. This key management protocol provides each client with the unique temporal key for encryption, and therefore exposure of a client's key to the attacker does not influence on the other clients' security. Nevertheless, vulnerabilities still remain as many of encryption based protections in wireless networks involve the innate key management problem. We analyze them in more detail in Sect. 3.

There have been many studies on physical layer protections for wireless secrecy. Strasser et al. [44] propose a mechanism to share a key between two ends under jamming, but it still requires public/private key pairs and a

trusted certification authority (CA), thus not completely being independent from the necessity of pre-shared secret. Moreover, the key establishment process is too slow to be practically used for Wi-Fi networks. On the other hand, the Shannon's information theory [41] provides a theoretical fundament on sharing secret information between communicating nodes under a potential eavesdropper. Wyner presents the wire-tap channel, which is a theoretical model showing the eavesdropper's channel can be degraded compared to the legitimate receiver's [54]. Studies on various theoretical channel models have followed this wire-tap channel [12, 24, 27, 45]. After an empirical validation by Li et al. [26], other studies have improved the secrecy rate [11, 15, 18, 23, 29]. The information shared on top of the random wireless channel can be used as an encryption key.

Another type of physical layer protections delicately manipulate wireless coverage by tuning antenna. Sheth et al. [43] use multiple access points equipped with directional antenna to confine the wireless coverage. Li et al. [25] show that secure transmission can be achieved with multiple antennas array without requiring any pre-shared key. Negi et al. [30] present a method to secure wireless communication by using multiple transmitting antennas and helper nodes. There are also 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, and specialized hardware or complex signal processing techniques.

Different from the conventional perception as an attacking means, jamming has recently drawn lots of attentions as a defense mechanism. Martinovic et al. [28] also exploit the jamming as a tool to protect from the malicious packet injection attack. Gollakota et al. [14] use a jammer to secure private data in implantable medical device (IMD) inside patients' body and to protect the IMD from unauthorized commands. Similar mechanisms have been presented for IMD security [5, 55]. Rouf et al. use jamming to prevent privacy leakage from automatic meter reading system [39]. Vilela et al. [49] present a protocol to select silent devices jamming the data frames to protect from the potential eavesdropper by utilizing the exchange of RTS/CTS frames.

Sankararaman et al. [40] define a warehouse model, which consists of the storage containing items equipped with RFID tags and the physical boundary *fence*. To prevent eavesdroppers outside the fence, multiple jammers are installed in the space between the storage and the fence, and they propose algorithms to optimize the power and the number of jammers. Prior to this jamming optimization study, there have been efforts to protect RFID privacy and fine control the access to RFID [19, 37, 38]. Vilela et al. present *friendly jamming*, showing the theoretical feasibility of using jamming for ensuring confidentiality of wireless communications [47, 48]. Similar studies are also presented for wireless secrecy with various configurations [13, 33, 58]. These are similar to ours in using jamming to achieve wireless secrecy, but in contrast we show how the defensive jamming technique can supplement the existing Wi-Fi security protocol, provide the jammer arrangement algorithms, and discuss practical consideration for real deployment. Shen et al. [42] propose *ally friendly jamming* which only jams the adversary communication, but ensures the ally communication. It requires a pre-shared key to generate a jamming signal known to ally, while our mechanism does not depend on any pre-shared secret. We compare our approach with similar jamming approaches in Table 1.

An attacker may use countermeasures to defensive jamming. Conventional spectral evasion or spatial evasion [7, 8, 56] cannot be used by an eavesdropper, because we control the operating channel of Wi-Fi AP and defensive jammers, and an eavesdropper located outside the target area is influenced by defensive jammers. We discuss an attacker using directional antenna to spatially evade the defensive jammers in Sect. 7. Xu et al. [57] propose the timing channel over which multi-senders and a receiver still can communicate under jamming. The maximum throughput supported by the timing channel is too low (<10 bps) to be used by an eavesdropper. An attacker may use interference cancellation techniques to eavesdrop the communication under jamming [9, 16]. However, these approaches require expensive implementation costs and do not properly work for the jammer changing its duty cycle. Note that the defensive jammers operate reactively with the APs, thus prohibiting an attacker from inferring the duty cycle. More detailed discussion is in Sect. 6.1. Tippenhauer et al. [46] recently present a study on the limitation of friendly jamming for confidentiality. They show how MIMO eavesdroppers can recover the legitimate signal in the 400 MHz MICS frequency band under friendly jamming. However, it is restricted to the unencrypted communication since it can partially recover the jammed bits. It is also limited in the region influenced by multiple jammers and requires very accurate antenna placement in the higher frequency band.

3 Problem definition

We first specify the assumptions on the Wi-Fi networks in this paper. We then review the possibility of eavesdropping Wi-Fi networks protected by current standard security protocol.

Table 1 We compare the proposed defensive jamming mechanism with other jamming approaches

	Proposed mechanism	Friendly jamming [48]	Ally friendly jamming [42]	RFID blocker [19]	IMD shield [14]	Jamming for good [28]
Application	Enterprise Wi-Fi	General	Hostile environment	RFID	IMD	Sensor nodes
Goals to achieve	Confidentiality	Confidentiality	Authorization	Confidentiality	Access control/ authorization	Authentication/ availability
Scalability	Multiple jammers/ transmitters/ receivers	Multiple jammers	Multiple jammers/ transmitters/ receivers	Multiple tags/ readers	None	Multiple jammers/ sensors
Mobility	Wi-Fi clients	Receivers	All nodes, but slow	All nodes	All nodes	None
Pre-shared secret	None	None	Required	Optional	Required	None

3.1 Assumptions

We assume a Wi-Fi network operating at infrastructure mode, thus consisting of APs and Wi-Fi clients. All of the Wi-Fi nodes are located inside a given geographical boundary and managed by a network administrator. The network has crucial information which should not be uncontrollably exposed outside the geographical boundary. Similar exemplary cases can be found in a government building, an enterprise R&D center handling secret information of new products, a medical institute keeping the private health records of individual patient, or even a battle field needing covert wireless communication. Accordingly, the boundary may encompass outdoor area as well as indoor area. For ensuring confidentiality, it is common to use the IEEE 802.11i standard to encrypt data frames and authenticate only the legitimate Wi-Fi clients.

3.2 Eavesdropping secure Wi-Fi networks

The WPA2 enterprise mode defined in the IEEE 802.11i standard has been widely used in Wi-Fi networks requiring enterprise level security. Nevertheless, eavesdropping Wi-Fi networks secured by the WPA2 enterprise mode is still possible. An attacker can passively eavesdrop the target network to obtain the meta information or invasively use other means to actively monitor the Wi-Fi clients' traffic.

3.2.1 Network analysis

Although an attacker does not have a legitimate account to access the Wi-Fi network secured by the WPA2 enterprise mode, they can collect lots of useful information by passively listening to the Wi-Fi channel. Since many management frames are broadcast in plain text, an attacker can easily collect basic network configurations of Wi-Fi networks by means such as wardriving software [21, 22, 31]. Most of those information are intended to be public, however, depending on the required security level in a given scenario, critical information can be exposed to the unintended outsider. Note that the IEEE 802.11w standard [4] can encrypt only the management frames after the association procedure between AP and client. Unencrypted management frames such as beacon and probe request/response include channel, SSID (Service Set Identification), BSSID (Basic SSID), source MAC address, and even vendor specific information. These parameters are used as the basic information for an attacker to launch more advanced attacks. An attacker may also use the side channel information such as traffic volume and communication timing.

3.2.2 Traffic capture

For an attacker to capture the traffic from the target Wi-Fi networks, the first step is to get authenticated to the secured Wi-Fi network. After gaining the access to the network, an attack should decrypt the other clients' traffic.

Authentication

A less technical, but a more effective way for an attacker to access Wi-Fi networks is social engineering. Reckless users may write down the passphrase in publicly accessible places or reveal the hint or passphrase itself to an attacker by answering simple questions. Moreover, many wireless connection manger software store the account name and the passphrase with the SSID of previously associated AP in clear text in the file system (*e.g.*, *wpa_supplicant* in Linux). An attacker may physically access or install a malware to capture the password file.

The legitimate Wi-Fi user's credential can be exposed to an attacker by using insecure protocols. For instance, one of obsolete EAP protocols, Cisco LEAP sends the user's logon password outside of a secure connection, thus making vulnerable to dictionary attack [10]. The publicly known tool can crack the users' password by exploiting the vulnerability [53]. But, these protocols are still being used in practice to provide the backward compatibility for legacy devices.

Decrypting Wi-Fi traffic

Without having the encryption key, it is not easy for an attacker to decrypt the messages encrypted with CCMP [17]. Neither an outsider attacker who owns the user's WPA2 authentication key nor an insider attacker can directly eavesdrop the other client's traffic. The encryption key is contained in the *pairwise transient key (PTK)*. The PTK is derived from the *pairwise master key (PMK)* and the nonces exchanged between the client and the AP. In the WPA2 enterprise mode, the PMK is derived from the *master key (MK)*, which is delivered to the client from the authentication server via the AP. In most cases, the MK is transported through the secure *transport layer security (TLS)* tunnel. In this process, an attacker may try to directly break in the TLS session by launching the *Lucky 13* attack [6], if sufficient amount of frame captures are available with offline analysis.

Another well known attacking measure is *Hole196* [32]. An attacker having access to Wi-Fi sends a spoofed ARP message that is encrypted with the *shared group key (GTK)* to the target Wi-Fi client to maliciously set the client's default gateway to the attacker's MAC address. After the target client's ARP table is successfully poisoned, every traffic destined to the Internet is sent to the AP with the attacker's MAC address as a destination. Since the AP regards it as the traffic destined to the attacker, the AP decrypts it and re-encrypts it with the attacker's PTK. Finally, the attacker can receive the traffic and easily decrypt it with its PTK.

3.3 Our approach

Figure 1 illustrates a typical enterprise Wi-Fi set up. There is a physical boundary shown as a *solid line* wherein a Wi-Fi network is used. Although all communications should be placed inside the boundary, the wireless coverage of Wi-Fi AP shown as a *dotted line* can exceed the boundary, thus providing an attacker executing the aforementioned methods with eavesdropping chances . Our approach is to physically confine the wireless coverage within the given boundary by using defensive jamming. When combined with the existing security mechanisms, this approach can contribute to minimizing the risks from potential eavesdropping.

4 Defensive jamming

In this section, we show that it is feasible to control the shape of jamming boundary with the location and the transmitting power of jammers. We define these jammers to create the protected wireless zone as *defensive jammers* and identify the parameters that dictate the shape of the *jamming boundary*, which is created by the given group of jammers. We then show how to protect Wi-Fi networks from eavesdropping by using defensive jamming technique.

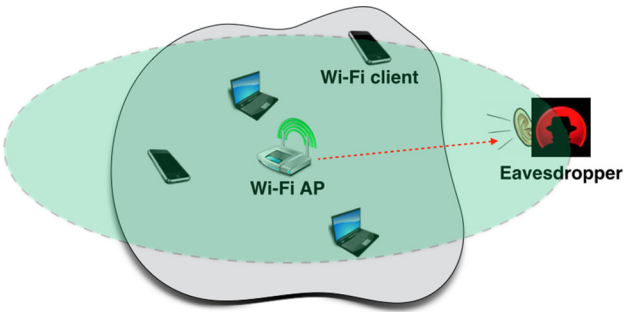


Fig. 1 A Wi-Fi AP installed inside the physical boundary represented as a *solid line* provides a wireless coverage shown as a *dotted line*. An eavesdropper located outside the physical boundary listens to the communication from the Wi-Fi AP

4.1 Jamming boundary and secure wireless zone

In order to determine the communication range of a wireless node, we 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

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

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 level.

Here, we ignore the ambient noise power N_0 for the simplicity of model derivation[1] and apply the line-of-sight (LOS) propagation model [34, 35] 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. When A and J operate on the same frequency band, (1) is thus simplified as

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

where P_A is the transmitting power of A, P_J is the transmitting power of J, G_{AS} is the antenna gain of A to S, G_{JS} is the antenna gain of J to S, 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 [35]. If A and J use the same efficiency of omni-directional antenna, (2) gives the idea that a jamming

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

boundary is dependent on the powers of A and J, and the distances from S to them.

Based on the one-transceiver-one-jammer, we now extend the model to multiple jammers. Given the set $\mathcal{J} = \{J_1, J_2, \ldots, J_k\}$ of k jammers, the SINR at S under jamming is given by

$$\gamma_{A/\mathcal{J}}(S) = \frac{P_{AS}}{\sum_{i=1}^{k} P_{J_iS} + N_0} = \beta, \tag{3}$$

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) An area $Z_A(\mathcal{J})$ is defined as an area accessible to AP, if a station in $Z_A(\mathcal{J})$ can receive data from the AP A under k jammers in a set $\mathcal{J} = \{J_1, J_2, \ldots, J_k\}$. Namely,

$$Z_A(\mathcal{J}) = \left\{ (x,y) \middle| \gamma_{A/\mathcal{J}}(x,y) > \beta \right\},$$

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 $\beta = 1$ (0 dB) in the rest of this paper. Notice that in practice there is still a chance that eavesdropping occurs outside an area accessible to AP with low probability due to the random wireless channel. The information theoretic approaches such as friendly jamming [47, 48] cannot prevent this from happening either. Since, however, the our goal is to minimize the eavesdropping risks, defensive jamming with the existing protections is expected to be sufficient to nullify the eavesdropper's attempts in Sect. 3. Therefore, we assume that the packets from AP are atomic, meaning that they are always successfully received inside an area accessible to AP and completely blocked outside the region.

In order to estimate the area accessible to AP under multiple jammers from the areas accessible to AP under individual jammer, we use Theorem 1.

Theorem 1 *The area accessible to the AP A under effects of k jammers in a set $\mathcal{J} = \{J_1, J_2, \ldots, J_k\}$ is a subset of the intersection of the areas accessible to the AP A under the effect of each single jammer.*

$$Z_A(\mathcal{J}) \subset \bigcap_{i=1}^{k} Z_A(J_i).$$

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

$$Z_A(\mathcal{J}) = \left\{ (x,y) \middle| \frac{P_{AS}(x,y)}{\sum_i^k P_{J_iS}(x,y)} > \beta \right\}. \tag{4}$$

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 $Z_A(\mathcal{J})$ satisfy the condition in $Z_A(J_p)$.

$$Z_A(\mathcal{J}) \subset Z_A(J_p),$$

where $1 \le p \le k$. □

Now we extend our discussion with multiple APs. In many scenarios such as enterprise network, multiple APs are used to expand the wireless coverage in the target area. We need not consider the case multiple APs are channel independent with each other, since the configuration of jammers operating at each AP is simply separated from the others' configuration. With the m number of channel interdependent APs, Definition 1 is generalized as follows.

Definition 2 (Area Accessible to multiple APs) Given a set of jammers $\mathcal{J} = \{J_1, J_2, \ldots, J_k\}$ and a set of APs $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$, an area $Z_{\mathcal{A}}(\mathcal{J})$ wherein a station can access to the APs is defined as

$$Z_{\mathcal{A}}(\mathcal{J}) = \left\{ (x,y) \middle| \max_{i=1,\ldots,m} \left(\gamma_{A_i/\mathcal{J}}(x,y) \right) > \beta \right\}.$$

Since it is computationally expensive to calculate all SINR values for each AP at each location, the following Theorem 2 can be used.

Theorem 2 *The area accessible to multiple APs is equal to the union set of the areas accessible to each AP.*

$$Z_{\mathcal{A}}(\mathcal{J}) = \bigcup_{i=1}^{m} Z_{A_i}(\mathcal{J}).$$

Proof

$$\begin{aligned} Z_{\mathcal{A}}(\mathcal{J}) &= \left\{ (x,y) \middle| \max_{i=1,\ldots,m} \left(\gamma_{A_i/\mathcal{J}}(x,y) \right) > \beta \right\} \\ &= \left\{ (x,y) \middle| \left(\gamma_{A_1/\mathcal{J}}(x,y) > \beta \right) \text{ or } \right. \\ &\qquad \left. \cdots \text{ or } \left(\gamma_{A_m/\mathcal{J}}(x,y) > \beta \right) \right\} \\ &= \bigcup_{i=1}^{m} Z_{A_i}(\mathcal{J}). \end{aligned}$$

□

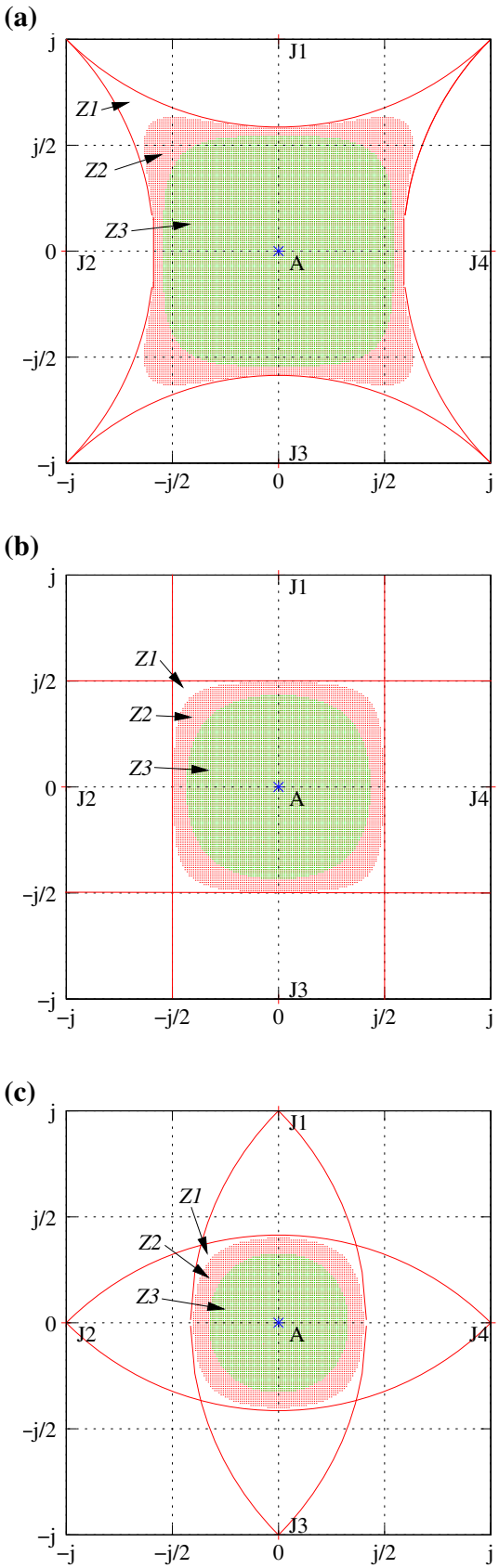


Fig. 2 The secure wireless zone formed by four jammers is illustrated ▶ for several different parameter choices. The *line* $Z1$ shows the intersection $Z(J_1) \cap Z(J_2) \cap Z(J_3) \cap Z(J_4)$ of the individual secure zones formed by each of four jammers. The line $Z2$ is the secure wireless zone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

We denote the area accessible to AP $Z_A(J_1, J_2, \ldots, J_k)$ as *secure wireless zone*, if it is walled from the outside.

Definition 3 (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 $Z_A(\mathcal{J})$ is the area accessible to a set of APs $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ under a set of jammers $\mathcal{J} = \{J_1, J_2, \ldots, J_k\}$. Then, Z is the secure wireless zone, only if

$$Z_A(\mathcal{J}) \cap L_O = \phi.$$

Figure 2 illustrates the secure wireless zone formed by a single AP A and four surrounding jammers, being placed from the A by distance j. All of them have the identical antenna gain. Three cases are considered in the figure: (1) $P_A > P_J$, (2) $P_A = P_J$, and (3) $P_A < P_J$. 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, 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. 2, the size of Z_2 is as large as 86–90 % of Z_1, while one of Z_3 is only 54–63 % 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 boundary so that a corridor of access is open between the jammers towards the AP. For instance, in Fig. 2a the four corners of the boundary can burst open so that an attacker can access the AP signal from those angles. In our previous work [20], we showed that the our theoretical jamming model is consistent with the measurements from the outdoor experiments.

4.2 Protecting downlink channel by defensive jamming

The communication channel between AP and client is divided into two folds: (1) the uplink channel from client to AP, (2) the downlink channel from AP to client. As reviewed in Sect. 3.2, one of the most crucial information (MK) during the association procedure is delivered from the authentication server to the client via the downlink channel. Besides, the downlink channel carries more information than each individual uplink channel since the AP is the converged point for all clients. Note that the message encryption key used in WPA2 enterprise mode is unique to each client, and thus the information in the uplink channel of a client is independent of the security of other clients.

By limiting the downlink channel with defensive jamming, we can make an attacker hard to obtain the server nonce and the MK, that are the essential information to derive the encryption key. Defensive jammers can be installed to limit the uplink channel either, but it is practically difficult to position jammers targeting mobile stations in the given physical boundary. If, for example, a client station locates near the physical boundary, it is not easy to install the defensive jammer creating a jamming boundary which protects clients' signal from outside eavesdropping. In this paper, we therefore consider protecting only the *downlink channel* (from AP to client) with defensive jamming to prevent the potential attacks.

5 Jammer arrangement

In this section, we discuss how to arrange the defensive jammers to carve a wireless zone around an arbitrary geometry. We also consider the field environments where defensive jammers are to be installed.

Let us first define the initial wireless zone *IWZ* as the wireless coverage of the AP A without jamming. The size of *IWZ* is confined by the transmitting power P_A of the AP A. 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 A is not on the boundary of *TZ*. We then represent a multi-objective optimization problem as

$$\begin{aligned} &\underset{\mathbb{P},\mathbb{L}}{\text{minimize}}\ \mathcal{F}_{\mathbb{P},\mathbb{L}}\left(-|SWZ|, N_J, \sum_i P_{J_i}\right), \\ &\text{subjectto } SWZ \subset TZ, \end{aligned} \tag{5}$$

where $\mathbb{P}$ is a set of transmitting powers of all jammers and $\mathbb{L}$ is a set of locations of all jammers, and $|\cdot|$ is the size of the zone. Each of three variables in $\mathcal{F}$ is an objective function with respect to $\mathbb{P}$ and $\mathbb{L}$, and therefore we want to find a parameter pair of $\mathbb{P}$ and $\mathbb{L}$ which minimizes all these objective functions. Since the importance of each objective function varies with the given situation, an optimization algorithm is devised in many different ways. The exponential series of these objective functions quickly increase with the complexity of polygon and the convexity property of functions is not guaranteed. Thus, we provide a heuristic approach adaptively adjusting jamming parameters for this optimization. In this way, the realistic jamming boundary is computed by reflecting the channel environment of installation site, instead of relying on an ideal jamming model. In real practice, defensive jammers are not only freely placed, but also restrictively positioned due to the barriers such as uncontrollable structures and neighboring legitimate wireless zones. We thus introduce algorithms to achieve optima in both cases.

5.1 Fixed defensive jammers

We first consider a scenario where the locations of jammers ($\mathbb{L}$) are already given, *i.e.*, $\underset{\mathbb{P}}{\text{minimize}}(\mathcal{F})$. Figure 3 depicts the configuration of an AP A and four jammers $J1$–$J4$. Each side of *TZ* has at least one corresponding defensive jammer. In this configuration, we introduce an algorithm providing optimal transmitting powers of defensive jammers.

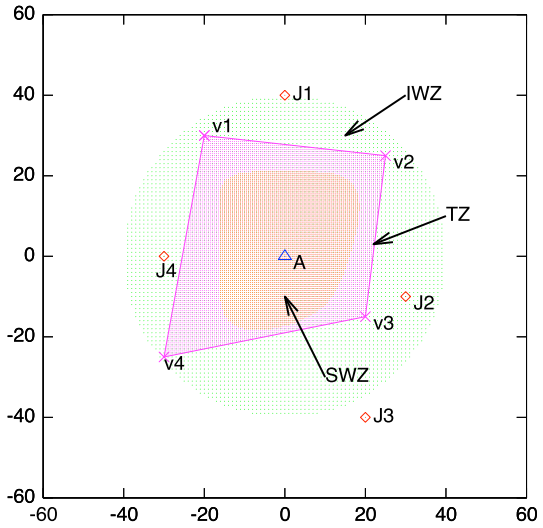


Fig. 3 The AP A is installed in the given target zone *TZ*. To limit the wireless coverage *IWZ* within *TZ*, the four defensive jammers $J1 \sim J4$ located at each point control their transmitting power. The proposed algorithm determines that $P_{J1} = 0.5P_A$, $P_{J2} = P_A$, $P_{J3} = 8P_A$, and $P_{J4} = 0.5P_A$. $\left(\frac{|SWZ|}{|TZ|} \approx 0.53, \frac{\sum P_{J_i}}{\sum P_{A_i}} = 10.0\right)$

Each jammer increases its transmitting power to be higher than A's, if the closer vertex to A in the corresponding side is closer to A than the jammer. It should increase the power until the jamming boundary does not intersect with the extended line of corresponding side. If the closer vertex to A in the corresponding side is closer to the jammer than A, the jammer inversely decreases its power until the jamming boundary intersects with the corresponding side.

In our simulation, we adjust the jamming power by exponentially increasing or decreasing with a base 2 in milliwatts scale (*i.e.*, $\sim \pm 3$ in dBm scale). For the given configuration in Fig. 3, the iterative power adaptation algorithm determines that the transmitting power of $J1, J2, J3$, and $J4$ should be 50, 100, 800, 50 % of P_A, respectively, and *SWZ* occupies about 53 % of *TZ*. This tells us that there is a limitation to maximize the *SWZ* without relocating the defensive jammers.

We detail the procedure in Algorithm 1. The procedure *GetFixedJammerPower*() takes the array $Array(L_J)$ of k jammer locations as well as L_A, P_A, and $Array(v)$. The result from *GetJammerPower*() is the array $Array(P_J)$ of calculated jammer powers. The procedure uses the following sub-functions.

- $CorrespondingJammerWith(l)$ returns the jammer corresponding with the *line l*.
- $Distance(l, p)$ calculates the minimum distance between the line l and the point p. If all of the two arguments are points, it calculates the distance between them.
- $JammingBoundary(P_J, L_J, P_A, L_A)$ returns the jamming boundary created by the given jammer transmitting the power P_J at the location L_J and the given AP transmitting the power P_A at the location L_A.
- $SearchAvailablePower(P_J, op)$ returns the next available jamming power from an ordered jamming power vector. If op is $+$, it returns an element one step bigger than P_J. If op is $-$, it returns an element one step smaller than P_J.

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

```
1: procedure GetFixedJammerPower(L_A, P_A, Array(L_J), Array(v))
2:     for v[i] in Array(v) do
3:         J ← CorrespondingJammerWith(v[i]v[i+1])
4:         v ← Arg_v(Min(Distance(v[i], L_A), Distance(v[i+1], L_A)))
5:         P_J ← P_A
6:         if Distance(v, L_J) > Distance(v, L_A) then
7:             while JammingBoundary(P_J, L_J, P_A, L_A) ⋂ ←v[i]v[i+1]→ ≠ φ do
8:                 P_J ← SearchAvailablePower(P_J, +)
9:             end while
10:        else
11:            while JammingBoundary(P_J, L_J, P_A, L_A) ⋂ v[i]v[i+1] = φ do
12:                P_J ← SearchAvailablePower(P_J, −)
13:            end while
14:        end if
15:        Array(P_J) ← P_J
16:    end for
17:    return Array(P_J)
18: end procedure
```

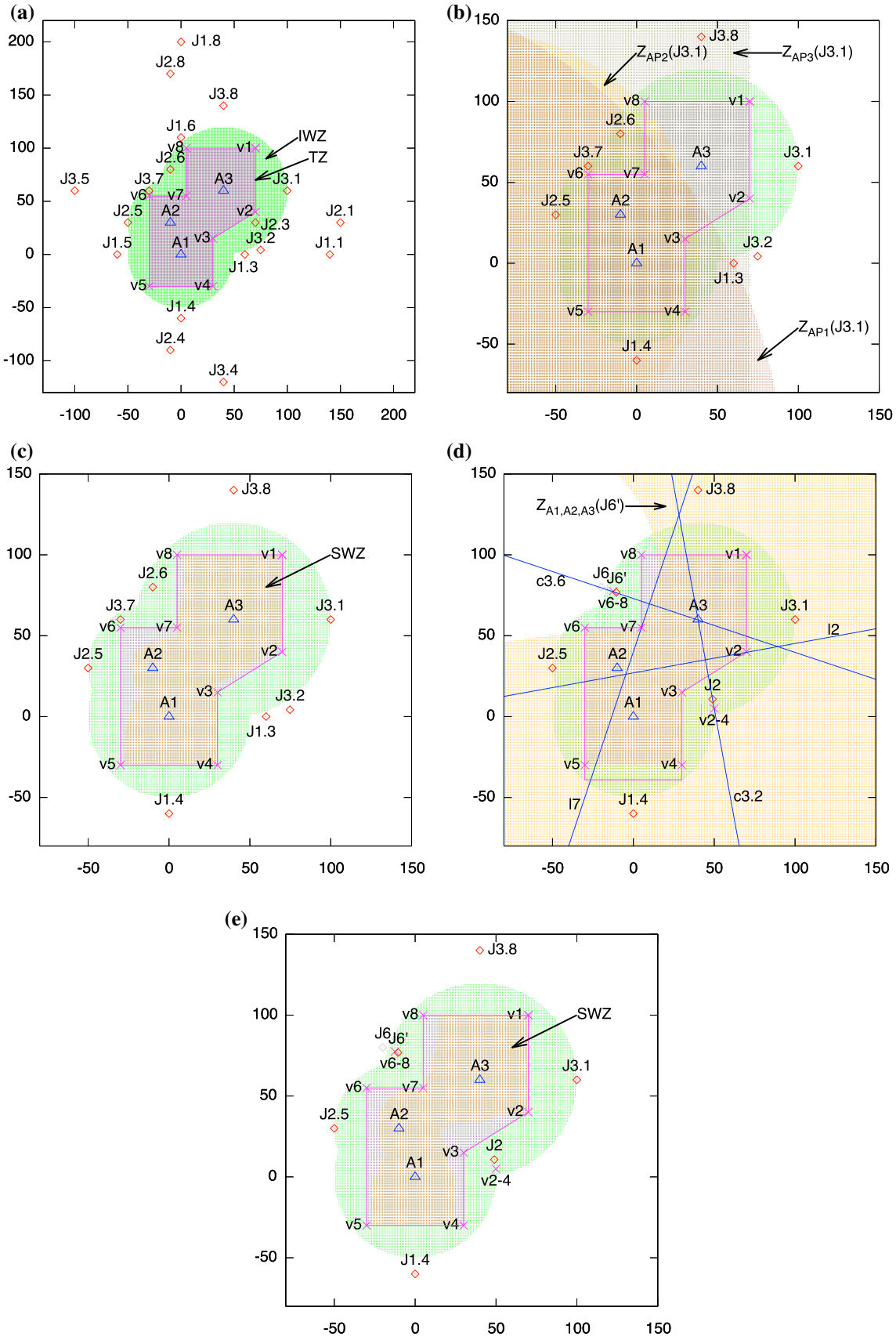
5.2 Relocatable defensive jammers

In this scenario, we assume that we can control the location of defensive jammers as well as the jamming power, *i.e.*, $\underset{\mathbb{P},\mathbb{L}}{\text{minimize}}(\mathcal{F})$. We also consider the case of multiple APs. The proposed algorithm is divided into the three different procedures: (1) jammer location determination, (2) jammer power calibration, and (3) jammer merger. We show how the proposed algorithm can determine the jamming parameters with an example scenario in Fig. 4.

5.2.1 Jammer location determination

To maximize *SWZ*, the shapes of jamming boundaries need to be straight along the side of the given polygonal *TZ*. As 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. Given the m number of channel interdependent APs in the k-polygon *TZ*, there are m number of possible locations of jammer for each side of *TZ*, which are the line symmetric points of APs. Figure 4a depicts the octagon *TZ* with having the three APs $A1 \sim A3$. The locations of jammers corresponding to the $A\{x\}$ for the side $\overline{v\{y\}v\{y+1\}}$ are represented as $J\{x\}.\{y\}$. For example, $J2.1$ is the symmetric point of $A2$ for the side $\overline{v1v2}$. The symmetric points located inside *TZ* are excluded since they lead to make *SWZ* smaller.

Among multiple jammers corresponding a side, we select only one jammer. Instead of the exhaustive search for


(a)
J1.8
J2.8
J3.8
J1.6
IWZ
TZ
v8
v1
J2.6
J3.5
J3.7
A3
J3.1
v6
v7
J2.5
A2
v2
J2.3
J2.1
J1.5
A1
v3
J3.2
J1.1
J1.3
v5
v4
J1.4
J2.4
J3.4
(b)
J3.8
Z_{AP2}(J3.1)
Z_{AP3}(J3.1)
v8
v1
J2.6
J3.7
A3
J3.1
v6
v7
J2.5
A2
v2
v3
J3.2
A1
J1.3
v5
v4
Z_{AP1}(J3.1)
J1.4
(c)
J3.8
v8
v1
SWZ
J2.6
J3.7
A3
J3.1
v6
v7
J2.5
A2
v2
v3
J3.2
A1
J1.3
v5
v4
J1.4
(d)
J3.8
$Z_{A1,A2,A3}$(J6')
v8
v1
c3.6
J6
J6'
v6-8
A3
J3.1
v6
v7
I2
J2.5
A2
v2
J2
v3
A1
v2-4
v5
v4
I7
J1.4
c3.2
(e)
J3.8
v8
v1
SWZ
J6
J6'
v6-8
A3
J3.1
v6
v7
J2.5
A2
v2
J2
v3
A1
v2-4
v5
v4
J1.4

◀**Fig. 4** Illustrated is the arrangement of defensive jammers when both their location and power are the controllable parameters. **a** For each side of *TZ*, there are equal number of mirrored points to APs as possible jammer location. $J\{x\}.\{y\}$ represents the jammer corresponding to $A\{x\}$ for the side $\overline{v\{y\}v\{y+1\}}$. **b** The eight jammers closest to each side are selected. They initially set the power equal to the corresponding AP and iteratively increase the power until the corresponding side is completely included in the created jamming region. **c** The *SWZ* created from defensive jammers is the intersection of jamming region formed by each jammer. $\left(\frac{|SWZ|}{|TZ|} \approx 0.89, \frac{\sum P_{J_i}}{\sum P_{A_i}} \approx 5.67\right)$. **d** In concave region, jammers can be merged. $J2.6$ and $J3.7$ are merged into $J6'$. $J3.2$ and $J1.3$ are merged into $J2$. **e** *SWZ* created after jammer merger $\left(\frac{|SWZ|}{|TZ|} \approx 0.81, \frac{\sum P_{J_i}}{\sum P_{A_i}} \approx 4.10\right)$

finding optimal jamming positions, we employ a heuristic approach selecting a jammer closest to each side. The rationale in this strategy is that the jammer close to all APs can finely control the jamming boundary with less energy. Consequently, the eight jammers are selected as shown in Fig. 4b.

5.2.2 Jammer power calibration

After determining the locations of jammers, each jammer calibrates the power to confine the *IWZ* within *TZ*. Each jammer initially sets the power equal to the corresponding AP. In Fig. 4b, $J3.1$ sets its power to P_{A3}. The entire jamming region created by $J3.1$ is the union of jamming regions created by $J3.1$ and each AP $\left(Z_{\{A1,A2,A3\}}(J3.1) = \bigcup_i Z_{Ai}(J3.1)\right)$. Unless the corresponding side is completely included inside the jamming region, the jammer increases its power to satisfy the condition. As in the arrangement of fixed defensive jammers, we keep doubling the jamming power in our simulation. Since the jamming region created by $J3.1$ in Fig. 4b already encloses the side $\overline{v1v2}$, $J3.1$ sets the jamming power equal to P_{A3}. After calibrating all jammers, the created *SWZ* is shown in Fig. 4c. The *SWZ* occupies about 89% of *TZ* and the total power spent by all jammers is about 5.67 times the total power spent by all APs.

5.2.3 Jammer merger

To minimize the number of jammers and the total jamming power, we merge the defensive jammers if the given target zone is a concave polygon as in Fig. 4. Let us first 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*. In our example, $v3$ and $v7$ are the concave vertices, and $\{v2, v3, v4\}$ and $\{v6, v7, v8\}$ form the respective concave side group. We thus show how the defensive jammers $J3.2$, $J1.3$, $J2.6$, $J3.7$ corresponding the concave side groups can be merged.

In Fig. 4d, $v6-8$ is the middle point between the two end vertices $v6$, $v8$ of a concave side group. At $v6-8$, the AP transmitting the strongest signal is chosen ($A3$ in this example) and the line $c3.6$ passing through the two points is used as a line where the merged jammer will be placed. Since all sides in the concave side group should be included in the jamming region, the perpendicular line $l7$ to $c3.6$ passing through $v7$ is the base jamming boundary between $A3$ and the position of merged jammer. In Fig. 4d, $J6$ is the point of symmetry of $A3$ to $l7$.

If setting the jamming power of $J6$ to be equal to $A3$ does not make all members in the concave side group included in the jamming region, $J6$ increases its power until the condition is met. Otherwise, in order to maximize *SWZ* the algorithm moves $J6$ closer to $A3$ and reduces the jamming power. In this example, our algorithm moves $J6$ five meters closer to $A3$ at each iteration and checks if the concave side group is included in the jamming region with the reduced jamming power ($\times 0.5$ at each iteration). Note that the algorithm moves the jammer closer to the AP only when the jamming power can be reduced since it should not decrease the *SWZ*.

In the simulation, the algorithm determines that the jamming position is at $J6'$ which is ten meters closer to $A3$ than $J6$, and the jamming power is reduced to $0.25P_{A3}$. With the same method, the algorithm also combines $J3.2$ and $J1.3$ into $J2$ in another concave side group by setting its power to P_{A3}. Figure 4e illustrates the result *SWZ* after applying jammer merger algorithm. The new *SWZ* occupies 81 % of *TZ* which slightly decreases, but the number of installed jammers are reduced by two and the total power spent by all jammers is reduced to about 4.10 times of the total power spent by all APs.

We detail the procedure in Algorithm 2. The procedure $GetFlexJammerSetting()$ takes the location array $Array(L_A)$ of APs, the transmitting power array $Array(P_A)$ of AP, and the array $Array(v)$ of vertices which form the k-polygonal boundary of the given target zone. It returns the array $Array(L_J)$ of the calculated jammer locations and the array $Array(P_J)$ of the calculated jammer powers. The following sub-functions are used.

- $GroupConcaveSide(Array(v))$ takes the array of vertices and returns an array of groups, each of which includes neighboring concave sides.
- $SymmetricPoint(l, p)$ returns the symmetric point of p to the line l.
- $MidPointAtCSG(C)$ returns the middle point of the two end-points of the concave side group C.
- $CorrespondingAPWith(L_J)$ returns the corresponding AP for the location of jammer L_J.

- *JammingRegion*$(P_J, L_J, Array(P_A), Array(L_A))$ calculates the jamming region created by the given jamming transmitting the power P_J at the location L_J and the given APs transmitting the powers $Array(P_A)$ at the locations $Array(L_A)$.
- *StrongestAPAt*(p) returns the AP transmitting the strongest signal at the point p.
- *PerpendLineClosestTo*(p, l, C) returns the closest line to the point p among the lines that are perpendicular to the line l and pass through the vertices in the concave side group C.
- *MoveFromAToB*(p, q, d) moves the point p the distance d closer towards the point q.

It is unusual to install the jammer indoors for the outdoor wireless network as in *S*3. It is expected that the outdoor scenario *S*4 for both the APs and the defensive jammers suffers relatively less from the multipath fading effects. When both are placed indoors, we expect the similar path loss pattern as in *S*1 only with the different path-loss exponent n.[2] If the APs stay indoors and the jammers stay outdoors (*S*2) as in Fig. 5, the signal propagations at both places cannot be identical to each other. Using (2), in the midst between the AP and the jammer, we can asymptotically derive $P_{AS}/P_{JS} = (P_A \cdot D_{JS}^{n_o})/(P_J \cdot D_{AS}^{n_i})$ for the given AP A, the receiving station S, and the jammer J, where n_i and n_o are the path-loss exponent for indoor and outdoor environments, respectively. It is well-known that the path-loss exponent increases in an indoor environment (*i.e.*, $n_i > n_o$) [34, 35]. If we place A 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 A like $b2$. This consequently provides us with the tighter secure wireless zone.

In terms of security this smaller secure wireless zone is beneficial, however it results in poor channel access to the

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

procedure GetFlexJammerSetting($Array(L_A), Array(P_A), Array(v)$)
  $Array(CSG) \leftarrow GroupConcaveSide(Array(v))$
  for $v[i]$ in $Array(v)$ **do**
    if $\overline{v[i]v[i+1]} \notin$ any CSG **then**
      for L_A in $Array(L_A)$ **do**
        $Array(J) \leftarrow SymmetricPoint(\overline{v[i]v[i+1]}, L_A)$
      end for
      $Array(L_J) \leftarrow Arg_{j \in Array(J)}(Min(Distance(\overline{v[i]v[i+1]}, j)))$
      $A \leftarrow CorrespondingAPWith(L_J)$, $P_J \leftarrow P_A$
      while $\overline{v[i]v[i+1]} \not\subset JammingRegion(P_J, L_J, Array(P_A), Array(L_A))$ **do**
        $P_J \leftarrow SearchAvailablePower(P_J, +)$
      end while
      $Array(P_J) \leftarrow P_J$
    end if
  end for
  for CSG in $Array(CSG)$ **do**
    $q \leftarrow MidPointAtCSG(CSG)$
    $A \leftarrow StrongestAPAt(q)$
    $t \leftarrow PerpendLineClosestTo(L_A, \overline{qL_A}, CSG)$
    $j \leftarrow SymmetricPoint(t, L_A)$
    $p \leftarrow SearchAvailablePower(P_A, -)$, $d \leftarrow MinAdjustableDistance$
    while side $s \in CSG$, $\forall s \subset JammingRegion(p, j, Array(P_A), Array(L_A))$ **do**
      $p \leftarrow SearchAvailablePower(p, -)$
    end while
    while side $s \in CSG$, $\forall s \subset JammingRegion(p, j, Array(P_A), Array(L_A))$ **do**
      $j \leftarrow MoveFromAToB(j, L_A, d)$
    end while
    $j \leftarrow MoveFromAToB(j, L_A, -d)$
    $Array(L_J) \leftarrow j$, $Array(P_J) \leftarrow p$
  end for
  return $Array(L_J), Array(P_J)$
end procedure

5.3 Field considerations

The jamming boundary is irregular in real practice due to the natural fading effects. It will become more severe in an indoor environment due to many obstacles hiding LOS path. Thus, it is required to do a site survey to deploy defensive jammers in the field. By adaptively adjusting the jamming parameters, one can build a realistic secure wireless zone.

Depending on the configuration on which the APs and the jammer are installed, different scenarios are shown in Table 2.

[2] We showed the different shape of the secure wireless zone with the different path-loss exponents in Fig. 2.

Table 2 Different scenarios depending on configuration

Scenario	APs	Jammers	Examples
*S*1	Indoor	Indoor	Enterprise, home
*S*2	Indoor	Outdoor	Enterprise, home
*S*3	Outdoor	Indoor	N/A
*S*4	Outdoor	Outdoor	Battle field, outdoor monitoring

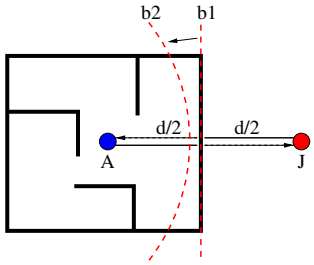


Fig. 5 In a scenario where APs are located indoor and jammers are located outdoor, the jamming boundary $b1$ pushes towards AP like $b2$ due to the higher path loss exponent in indoor environments

wireless nodes inside 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 Interference countermeasure

The defensive jamming technique significantly increases the noise level around the target area. For the practical deployment of defensive jamming, we should consider minimizing the effect on the surrounding legitimate wireless stations. In this section, we discuss how to decrease the impact of defensive jamming on the legitimate devices located both inside and outside the target zone while still protecting the wireless network from the outside attacker.

6.1 Interference to inside legitimate communication

As we investigated in Sect. 4.2, defensive jammers interfere only with the downlink channel. Therefore, it is enough to jam only the frames of the APs instead of always-on jamming noise. In so doing, the defensive jammers do not interrupt the transmission of other stations as shown in Fig. 6. It can even selectively jam the specific

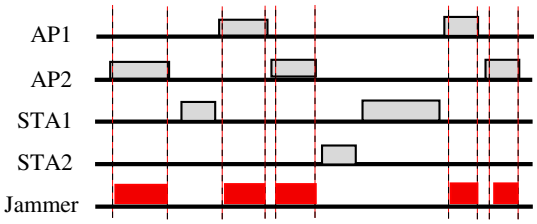


Fig. 6 By selectively jamming the frames from APs, defensive jamming can avoid interfering with the transmission of other stations

types of frame from APs. For example, in order to protect the association procedure the defensive jammers only need to jam the frames related to authentication and association from APs. Moreover, this method also significantly saves energy resources in an energy-constrained situation.

The selective jamming can be implemented by wiring the APs and defensive jammers. Whenever the APs send any frames over the channel, the APs quickly inform to the wired defensive jammers with the duration of frame transmission. The defensive jammers turn on their jamming signal during the informed duration to protect the frames of APs. For more flexible configuration, the selective jammers can also be wirelessly listens to the APs. By decoding the frame header and reading the embedded information (*e.g.*, source MAC address, rate/length), the defensive jammer can determine the AP to be jammed and the jamming duration. The detailed design and the feasibility of selective jamming have been studied in [36, 50–52]. The sensing and jamming operations can be even processed simultaneously by using a signal channel, full duplex radio [9].

Besides, another approach to be considered is adjusting the clear channel assessment (CCA) level in each Wi-Fi device. A transceiver is deprived of reserving channel if it detects any receiving signal is higher than the configured CCA level. If the transceiver increases the CCA level, it can recover its less channel reservation chance due to jamming. On the other hand, increasing the CCA level can result in the collision among the wireless stations, and therefore care should be taken to determine the value.

6.2 Interference to outside legitimate communication

In metropolitan areas, the installed defensive jammers may also interfere with the legitimate communications in neighboring buildings outside a target zone. Although defensive jamming generates noise only when the APs transmit, this behavior will result in the performance degradation of outside Wi-Fi networks. Figure 7a shows the interference pattern of defensive jammers where the interference range overlaps with the neighboring buildings. To minimize this effect, the defensive jammer can use directional antenna. The jammer $J3$ and $J7$ in Fig. 7b are

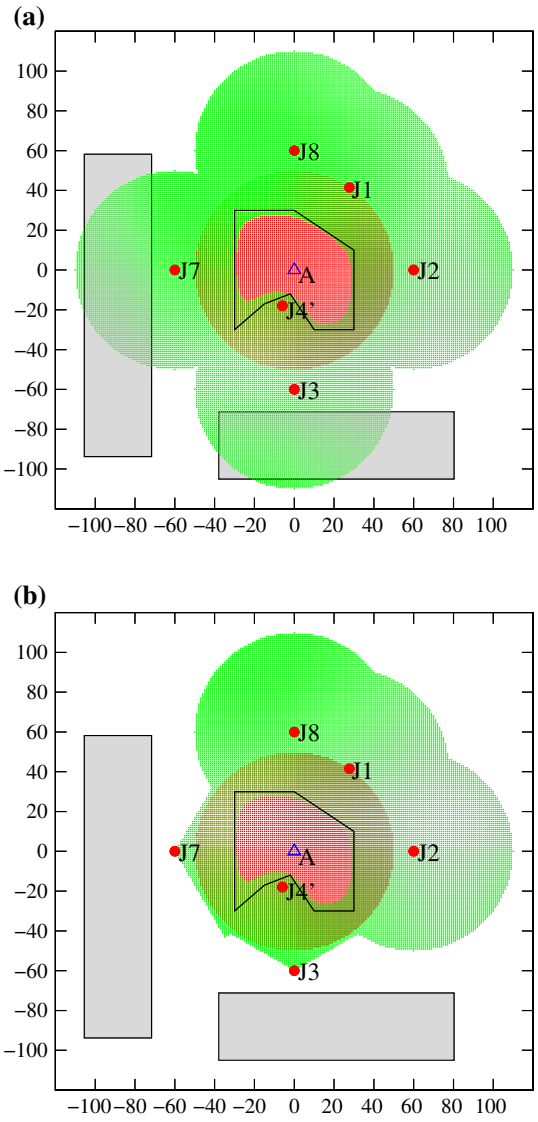


Fig. 7 Illustrated are interference patterns of defensive jammers with different antennas. **a** Omni-directional jammers. **b** Combination with directional jammers

equipped with the 120° of sector antennas. The jamming boundary created with directional antennas is calculated with the changed antenna gain in (2). Since an attacker can attempt an illegal network access from the unjammed area, the decision on deploying directional antenna should be carefully made based on the empirical performance impact by defensive jamming.

On the other hand, in a multi-story building a target zone can be vertically isolated. The signal propagation model is in theory applied in a same manner with the different antenna gain to the vertical direction, but the practical installation of defensive jammer will be difficult due to much shorter distance (height of stories). Such technical limitations need to be overcome by means such as the agreement between managements of neighboring parties.

7 Defense against advanced attacker

An attacker may afford to use more intelligent techniques requiring costly resources. One of such techniques uses the high-gain antenna. In Fig. 8, the attacker M equipped with a high-gain antenna attempts to overhear 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. This results in the significant increase in SINR at M to A, thus making J invalid.

To cope with the eavesdropper with high-gain antenna, one can increase the density of defensive jammers around the target zone or place the defensive jammers closer to A. Additionally, the location of defensive jammers should not be exposed or should be randomized by operating multiple sets of working jammers. This will reduce the chance of M to find the best direction to A for avoiding jamming signal.

Although it requires costly hardware, an attacker can use the interference cancellation technique to defeat jamming [9, 16]. However, most of these techniques assume the interference level is already known or static. If defensive jammers diversify the transmitting power and vary the jamming duty cycle, the attacker cannot properly cancel out the noise from defensive jammers. Instead, the jamming boundary created by power-diverse jammers will be depicted as a wide band, not a thin curve line. Therefore, the location of defensive jammers is chosen by considering the range of jamming power.

Lastly, an adversary may use a jamming device to disrupt the network protected by defensive jamming. The victim network will be interrupted by the adversarial jamming regardless of defensive jamming. Thus, the victim network can independently employ possible jamming mitigation in this situation. If, however, an adversary can impersonate AP to mislead defensive jammers to operate, it will harm neighboring legitimate networks. To prevent

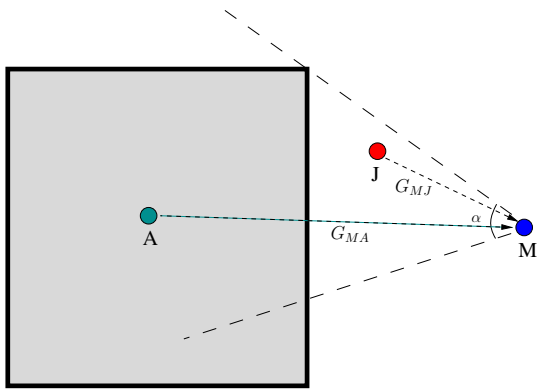


Fig. 8 Eavesdropper M uses the high-gain antenna which of beam angle is α. In the midst of beam, the antenna gain is higher than the other area ($G_{MA} > G_{MJ}$). Thus, M can listen to A better than J

such an unexpected side effect, it requires a way to authenticate legitimate APs by defensive jammers. The AP impersonation has been studied as a serious threat in Wi-Fi networks, and we do not address here in detail.

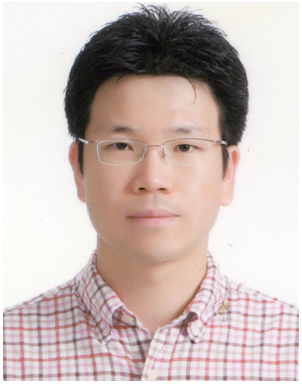
8 Conclusion

Since Wi-Fi networks based on the IEEE 802.11 WLAN protocol are widely deployed, they have suffered from many security issues. Industry and research community have developed various security mechanisms to protect the Wi-Fi network, and the WPA2 enterprise mode has been popularized after a number of trials and errors in real practice. However, the mechanism relying on shared secrets intrinsically involves the risk of key exposure. In this work, we analyzed the potential threats in Wi-Fi networks secured by the WPA2 enterprise mode. In order to mitigate the potential threats, we employed a defensive jamming approach, which does not depend on any pre-shred secret. By controlling the parameters of defensive jammers, we showed that the wireless coverage can be confined into an arbitrary geometry. We then provided the algorithms to automatically arrange defensive jammers in both the case that jammers are fixed and the case that jammers are relocatable. For practical deployment of defensive jammers, we also showed that the interference to the legitimate communication can be minimized by selectively jamming the downlink frames from AP towards stations and using directional antennas. We discussed how to mitigate the advanced attacker who can afford to use costly methods such as high gain antenna and interference cancellation techniques.

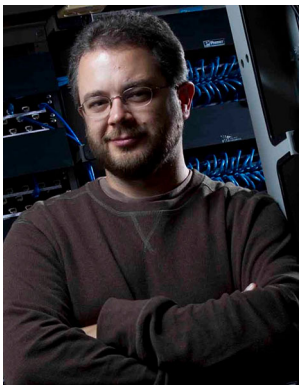
References

1. InnerWireless, Inc. http://www.innerwireless.com.
2. The AIRPATROL Cellular and Wireless Intelligence Solution. http://www.airpatrolcorp.com/products/cellular-and-wireless-intelligence-solution.php.
3. IEEE Std 802.11i-2004, Amendment 6: Medium Access Control (MAC) Security Enhancements (2004).
4. IEEE Std 802.11w-2009, Amendment 4: Protected Management Frames (2009).
5. Al-Hassanieh, H. (2011). *Encryption on the air: Non-invasive security for implantable medical devices. Ph.D. thesis*. Massachusetts Institute of Technology.
6. AlFardan, N. J. & Paterson, K. G. (2013). Lucky thirteen: Breaking the tls and dtls record protocols. In *IEEE symposium on security and privacy*.
7. Alnifie, G. & Simon, R. (2007). A multi-channel defense against jamming attacks in wireless sensor networks. In *International workshop on modeling analysis and simulation of wireless and mobile systems*.
8. Cagalj, M., Capkun, S., & Hubaux, J. (2007). Wormhole-based anti-jamming techniques in sensor networks. *IEEE Transaction on Mobile Computing*, *6*(1), 100–114.
9. Choi, J. I., Jain, M., Srinivasan, K., Levis, P., & Katti, S. (2010). Achieving single channel, full duplex wireless communication. In*Proceedings of the sixteenth annual international conference onmobile computing and networking, MobiCom '10* (pp. 1–12). NewYork, NY, USA: ACM.
10. Cisco Systems, I. Dictionary attack on cisco leap vulnerability. http://www.cisco.com/en/US/tech/tk722/tk809/technologies_security_notice09186a00801aa80f.html.
11. Croft, J., Patwari, N., & Kasera, S. K. (2010). Robust uncorrelated bit extraction methodologies for wireless sensors. In *Proceedings of the 9th ACM/IEEE international conference on information processing in sensor networks, IPSN '10* (pp. 70–81). New York, NY, USA: ACM. doi:10.1145/1791212.1791222.
12. Csiszar, I., & Korner, J. (1978). Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, *24*(3), 339–348. doi:10.1109/TIT.1978.1055892.
13. Goel, S., & Negi, R. (2008). Guaranteeing secrecy using artificial noise. *IEEE Transactions on Wireless Communications*, *7*(6), 2180–2189. doi:10.1109/TWC.2008.060848.
14. Gollakota, S., Hassanieh, H., Ransford, B., Katabi, D., & Fu, K. (2011). They can hear your heartbeats: Non-invasive security for implanted medical devices. In: *Proceedings of ACM SIGCOMM*.
15. Gollakota, S. & Katabi, D. (2011). Physical layer wireless security made fast and channel independent. In *INFOCOM, 2011 Proceedings IEEE*, pp. 1125–1133. doi:10.1109/INFCOM.2011.5934889.
16. Halperin, D., Anderson, T., & Wetherall, D. (2008). *Taking the sting out ofcarrier sense: Interference cancellation for wireless lans*. In*Proceedings of the 14th ACM international conference on Mobilecomputing and networking, MobiCom '08* (pp. 339–350). New York,NY, USA: ACM.
17. He, C. & Mitchell, J. C. (2005). Security analysis and improvements for ieee 802.11i. In *The 12th annual network and distributed system security symposium (NDSS'05)*.
18. Jana, S., Premnath, S. N., Clark, M., Kasera, S. K., Patwari, N., & Krishnamurthy, S. V. (2009). On the effectiveness of secret key extraction from wireless signal strength in real environments. In *Proceedings of the 15th annual international conference on mobile computing and networking, MobiCom '09* (pp. 321–332). New York, NY, USA: ACM. doi:10.1145/1614320.1614356.
19. Juels, A., Rivest, R. L., & Szydlo, M. (2003). The blocker tag: Selective blocking of rfid tags for consumer privacy. In *Proceedings of the 10th ACM conference on computer and communications security, CCS '03* (pp. 103–111). New York, NY, USA: ACM. doi:10.1145/948109.948126.
20. Kim, Y. S., Tague, P., Lee, H., & Kim, H. (2012). Carving secure wi-fi zones with defensive jamming. In *7th ACM symposium on information, computer, and communications security (AsiaCCS)*.
21. KISMAC: Kismac. http://kismac-ng.org/.
22. KISMET: Kismet. http://www.kismetwireless.net/.
23. Koyluoglu, O. & El Gamal, H. (2008). On the secrecy rate region for the interference channel. In: *IEEE 19th international symposium on personal, indoor and mobile radio communications, 2008. PIMRC 2008* (pp. 1–5). doi:10.1109/PIMRC.2008.4699954.
24. Leung-Yan-Cheong, S., & Hellman, M. (1978). The gaussian wire-tap channel. *IEEE Transactions on Information Theory*, *24*(4), 451–456. doi:10.1109/TIT.1978.1055917.
25. Li, X., Hwu, J., & Ratazzi, E. Array redundancy and diversity for wireless transmissions with low probability of interception. In *2006 IEEE international conference on acoustics, speech and signal processing, 2006. ICASSP 2006 proceedings* (Vol. 4, p. IV). doi:10.1109/ICASSP.2006.1661021.

26. Li, Z., Xu, W., Miller, R., & Trappe, W. (2006). *Securing wireless systems via lower layer enforcements*. In *Proceedings of the 5th ACM workshop on wireless security, WiSe '06* (pp. 33–42). New York, NY, USA: ACM. doi:10.1145/1161289.1161297.
27. Liang, Y., Poor, H., & Shamai, S. (2008). Secure communication over fading channels. *IEEE Transactions on Information Theory*, *54*(6), 2470–2492. doi:10.1109/TIT.2008.921678.
28. Martinovic, I., Pichota, P., & Schmitt, J. B. (2009). Jamming for good: Afresh approach to authentic communication in wsns. In *Proceedingsof the second ACM conference on Wireless network security, WiSec'09* (pp. 161–168). New York, NY, USA: ACM.
29. Mathur, S., Trappe, W., Mandayam, N., Ye, C., & Reznik, A. (2008). Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel. In *Proceedings of the 14th ACM international conference on mobile computing and networking, MobiCom '08* (pp. 128–139). New York, NY, USA: ACM. doi:10.1145/1409944.1409960.
30. Negi, R., & Goel, S. (2005). *Secret communication using artificial noise. In: 2005 IEEE 62nd, vehicular technology conference, 2005. VTC-2005-Fall* (Vol. 3, pp. 1906–1910). doi:10.1109/VETECF.2005.1558439.
31. Netstumbler: Netstumbler. http://stumbler.net/.
32. Networks, A. (2010). *WPA2 Hole196 vulnerability*. http://www.airtightnetworks.com/WPA2-Hole196.
33. Pinto, P., Barros, J., & Win, M. (2009). Wireless physical-layer security: The case of colluding eavesdroppers. In *IEEE international symposium on information theory, 2009. ISIT 2009* (pp. 2442–2446). doi:10.1109/ISIT.2009.5206050.
34. Poisel, R. A. (2002). *Introdunction to communication electronics warfare systems, chapter 2*. Boston: Artech House, Inc.
35. Poisel, R. A. (2004). *Modern communications jamming principles and techniques, chapter 2*. Boston: Artech House, Inc.
36. Proano, A., & Lazos, L. (2012). Packet-hiding methods for preventing selective jamming attacks. *IEEE Transactions on Dependable and Secure Computing*, *9*(1), 101–114. doi:10.1109/TDSC.2011.41.
37. Rieback, M., Crispo, B., & Tanenbaum, A. (2005). Rfid guardian: A battery-powered mobile device for rfid privacy management. In: C. Boyd & J. Gonzlez Nieto (Eds.), *Information security and privacy, lecture notes in computer science* (Vol. 3574, pp. 184–194). Berlin: Springer. doi:10.1007/11506157_16.
38. Rieback, M. R., Crispo, B., & Tanenbaum, A. S. (2007) Keep on blockin' in the free world: personal access control for low-cost rfid tags. In *Proceedings of the 13th international conference on security protocols* (pp. 51–59). Berlin: Springer. http://dl.acm.org/citation.cfm?id=1802438.1802444.
39. Rouf, I., Mustafa, H., Xu, M., Xu, W., Miller, R., & Gruteser, M. (2012). Neighborhood watch: Security and privacy analysis of automatic meter reading systems. In *Proceedings of the 2012 ACM conference on computer and communications security, CCS '12* (pp. 462–473). New York, NY, USA: ACM. doi:10.1145/2382196.2382246.
40. Sankararaman, S., Abu-Affash, K., Efrat, A., Eriksson-Bique, S. D., Polishchuk, V., Ramasubramanian, S., & Segal, M. (2012). Optimization schemes for protective jamming. In: *Proceedings of the 13th ACM international symposium on mobile ad hoc networking and computing, MobiHoc '12* (pp. 65–74). New York, NY, USA: ACM. doi:10.1145/2248371.2248383.
41. Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell System Technical Journal*, *28*(4), 656–715.
42. Shen, W., Ning, P., He, X., & Dai, H. (2013). Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time. In: *IEEE symposium on security and privacy (SP), 2013* (pp. 174–188). doi:10.1109/SP.2013.22.
43. Sheth, A., Seshan, S., & Wetherall, D. (2009). Geo-fencing: Confining wi-fi coverage to physical boundaries. In H. Tokuda, M. Beigl, A. Friday, A. Brush, & Y. Tobe (Eds.), *Pervasive computing lecture notes in computer science* (Vol. 5538, pp. 274–290). Berlin / Heidelberg: Springer.
44. Strasser, M., Capkun, S., Capkun, S., & Cagalj, M. (2008). Jamming-resistant key establishment using uncoordinated frequency hopping. In: *IEEE symposium on security and privacy, 2008. SP 2008* (pp. 64–78). doi:10.1109/SP.2008.9.
45. Tang, X., Liu, R., Spasojevic, P., & Poor, H. (2011). Interference assisted secret communication. *IEEE Transactions on Information Theory*, *57*(5), 3153–3167. doi:10.1109/TIT.2011.2121450.
46. Tippenhauer, N., Malisa, L., Ranganathan, A., & Capkun, S. (2013). On limitations of friendly jamming for confidentiality. In *2013 IEEE symposium on security and privacy (SP)*, (pp. 160–173). doi:10.1109/SP.2013.21.
47. Vilela, J., Bloch, M., Barros, J., & McLaughlin, S. (2010). Friendly jamming for wireless secrecy. In *2010 IEEE international conference on communications (ICC)* (pp. 1–6). doi:10.1109/ICC.2010.5502606.
48. Vilela, J., Bloch, M., Barros, J., & McLaughlin, S. (2011). Wireless secrecy regions with friendly jamming. *IEEE Transactions on Information Forensics and Security*, *6*(2), 256–266. doi:10.1109/TIFS.2011.2111370.
49. Vilela, J. P., & Barros, J. (2012). A cooperative protocol for jamming eavesdroppers in wireless networks. In *IEEE International conference on communications (ICC)*.
50. Wilhelm, M., Martinovic, I., Schmitt, J. B., & Lenders, V. (2011). Short paper: Reactive jamming in wireless networks: How realistic is the threat? In: *Proceedings of the 4th ACM conference on wireless network security, WiSec '11* (pp. 47–52). New York, NY, USA: ACM. doi:10.1145/1998412.1998422.
51. Wilhelm, M., Martinovic, I., Schmitt, J. B., & Lenders, V. (2011). Wifire: A firewall for wireless networks. In *Proceedings of the ACM SIGCOMM 2011 Conference, SIGCOMM '11* (pp. 456–457). New York, NY, USA: ACM. doi:10.1145/2018436.2018518.
52. Wilhelm, M., Martinovic, I., Schmitt, J. B., & Lenders, V. (2013). *Air dominance in sensor networks: Guarding sensor motes using selective interference*. arXiv preprint arXiv:1305.4038.
53. Wright, J. *Asleap–exploiting cisco leap*. http://www.willhackforsushi.com/Asleap.html.
54. Wyner, A. (1975). The wire-tap channel. *Bell System Technical Journal*.
55. Xu, F., Qin, Z., Tan, C., Wang, B., & Li, Q. (2011). Imdguard: Securing implantable medical devices with the external wearable guardian. In *INFOCOM, 2011 Proceedings IEEE* (pp. 1862–1870). doi:10.1109/INFCOM.2011.5934987.
56. Xu, W., Ma, K., Trappe, W., & Zhang, Y. (2006). Jamming sensor networks: Attack and defense strategies. *IEEE Network*, *20*(3), 41–47.
57. Xu, W., Trappe, W., & Zhang, Y. (2008). Anti-jamming timing channels for wireless networks. In: *Proceedings of the first ACM conference on wireless network security (WiSec '08)*.
58. Zhou, X., & McKay, M. (2009). Physical layer security with artificial noise: Secrecy capacity and optimal power allocation. In: *3rd International conference on signal processing and communication systems, 2009. ICSPCS 2009*. (pp. 1–5). doi:10.1109/ICSPCS.2009.5306434.

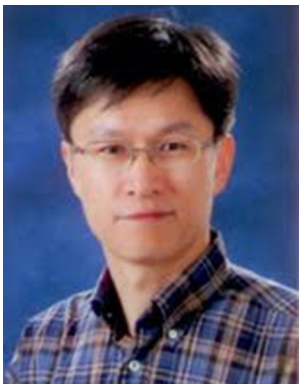


Yu Seung Kim is an automotive cybersecurity researcher at the Ford Research and Innovation Center, Palo Alto CA, USA. His research interest is in the analysis of potential threats in wireless systems and the design of practical countermeasures. He received a Ph.D. degree (2014) in Electrical and Computer Engineering at Carnegie Mellon University. His Ph.D. dissertation is titled as "Securing Wi-Fi Access by Using Location-Aware Controls". He was a member of Wireless Network and System Security group at the Silicon Valley campus of CMU led by Professor Patrick Tague. Before he joined the group, he received a B.S. degree (2002) and an ME degree (2010) in Computer Science and Engineering from Korea University as a member of the Computer and Communication Security Lab led by Professor Heejo Lee. He also has worked as a senior software engineer in Telecommunication Network Business, Samsung Electronics.



Patrick Tague is an Associate Research Professor at Carnegie Mellon University with appointments in the Electrical and Computer Engineering Department and the Information Networking Institute, and he is also the Associate Director of the INI. Patrick leads the Wireless Network and System Security group at the Silicon Valley Campus of CMU, and the group is affiliated with CMU CyLab. Patrick's research interests include wireless communications and networking; wireless/mobile security and privacy; robust and resilient networked systems; and analysis and sense-making of sensor network data. He received Ph.D. and M.S. degrees in Electrical Engineering from the University of Washington as a member of the Network Security Lab and B.S. degrees in Mathematics and Computer Engineering from the University of Minnesota. Patrick received the Yang Research Award for outstanding graduate research in the UW Electrical Engineering Department, the Outstanding Graduate Research Award from the UW Center for Information Assurance and Cybersecurity, and the NSF CAREER award.

Heejo Lee is a Professor at the Department of Computer Science and Engineering, Korea University, Seoul, Korea. Before joining Korea University, he was at AhnLab, Inc. as a CTO from 2001 to 2003. From 2000 to 2001, he was a Postdoctorate Researcher at Purdue University. In 2010, he was a visiting professor at CyLab/CMU. Dr. Lee received his B.S., M.S., Ph.D. degree in Computer Science and Engineering from POSTECH, Pohang, Korea. Dr. Lee serves as an editor of the Journal of Communications and Networks, and the International Journal of Network Management. He worked on the consultation of the cyber security in the Philippines, Uzbekistan, Vietnam, Myanmar, and Costa Rica.



Hyogon Kim is a professor at Korea University. Prior to joining Korea University, he was a research scientist at Bell Communications Research (Bellcore), Morristown, New Jersey, and an assistant professor at Ajou University, Korea. His research interests include wireless communication, Internet of Things, and security.