Proximity-Based Wireless Access Control through Considerate Jamming

Yu Seung Kim
Carnegie Mellon University
Moffett Field, CA USA
yuseungk@cmu.edu

Patrick Tague
Carnegie Mellon Univsersity
Moffett Field, CA USA
tague@cmu.edu

ABSTRACT

As diverse types of wireless devices emerge, it becomes difficult to apply the existing wireless security measures to them without efforts. Those devices lack conventional user interfaces or they are resource-constrained to process the security protocols. Meanwhile, many of them are used within a geographical boundary to access to the basestation. This motivates us to develop a complementary non-cryptographic technique to secure communication of such wireless devices. In this paper, we present *considerate jamming*, a novel wireless access control mechanism allowing access to only the wireless devices within a given boundary. The proposed mechanism does not require any modification in the wireless clients, but instead it is implemented with separate jamming devices and the modified basestation. We provide the theoretical model with system parameters and validate it through simulation.

Categories and Subject Descriptors

C.2.0 [**General**]: Security and protection; C.2.1 [**Network Architecture and Design**]: Wireless communication; D.4.6 [**Security and Protection**]: Access controls; K.6.5 [**Security and Protection**]: Authentication

Keywords

wireless access control; Internet-of-things (IoT); physical layer security; considerate jamming

1. INTRODUCTION

As we are observing the advent of the Internet-of-Things (IoT) era, it is undoubted that more and more devices have been connected via various wireless technologies. In the meantime, the convenience being brought by new connected devices should not sacrifice the security of systems and the privacy of users. Since those connected devices include even the traditional electric appliances without any visual display or resource constrained small wearable gadgets, it poses new challenges in applying the existing security mechanisms used in traditional wireless devices. For instance, if a new device connected to a Wi-Fi network needs to be secured from illegal access, Wi-Fi Protected Access 2 (WPA2) enterprise mode [2] can be considered as a solution. However, the device might not have a proper user interface to enter the passcode or computing resources processing the available Extensible Authentication Protocols (EAPs) with storing valid certificates. Even after such devices are once configured, it is possible that they are easily captured/tampered by unintended party or it is very difficult to reconfigure them without considerable human intervention.

On the other hand, despite its mobility a wireless device in nature is constrained by wireless coverage, i.e. having spatial locality. Figure 1 illustrates a wireless network geographically confined in a boundary. A variety of wireless devices within a boundary connect themselves to a Wi-Fi AP to have Internet connectivity. An attacker outside this boundary will also try to access this Wi-Fi network for many purposes such as illegal use of network resources, eavesdropping, packet injection for denial-of-service or man-in-the-middle attack, etc. If we can define the boundary that separates between the legitimate wireless devices and malicious devices, the *proximity* of wireless communication is an important attribute to cope with the security challenges mentioned above. In practice, this boundary could be a relatively small perimeter wherein a person can easily control, or a larger perimeter wherein physical security is enforced by authority.

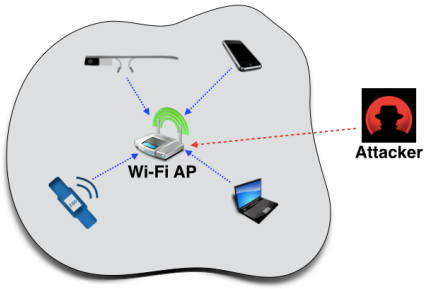

Figure 1: Legitimate wireless devices located inside a geographical boundary are connected to a Wi-Fi AP, whereas an attacker tries to access the Wi-Fi network from outside of a boundary. A solution selectively allowing access to only devices within this boundary can lower the implementation costs of security mechanism in resource constrained client devices.

In this configuration, various approaches can be used to selectively provide the network access to only the devices within the boundary. Distance bounding protocols prevent a forged claim that a claim node is located closer to a verifier node than its real location, and therefore it is useful in this domain [4, 5, 6, 15]. Because this technique however requires fast and accurate processing

SPME'14, September 07 - 11 2014, Maui, HI, USA

http://dx.doi.org/10.1145/2646584.2646588.

of exchanged information, it is difficult to implement in less powerful devices. Other approaches utilize delicate antenna techniques to geographically limit the wireless coverage [1, 10, 14]. They use directional antennas or multiple distributed antennas requiring fine turning, and therefore are not suitable to small constrained devices. Placing jammers around the geographical zone is a promising technique [8, 13, 16], since it can be separately implemented without modifying the client devices. However, the main drawback in this approach is the jamming noise also interferes with other legitimately communicating nodes.

In this paper, we propose a security mechanism which provides wireless devices with the proximity-based network access. Compared to the early approaches of jamming for good (e.g., *friendly jamming* [16]), the proposed mechanism minimizes interference on legitimate communications by "considerate jamming". It consists of jammer reactive to outside attacker and Wi-Fi AP selectively receiving packets depending on the received signal strength. The jammer installed at the boundary has two antennas: one is facing to outside to listen to the attacker's signal and the other facing to the Wi-Fi AP to emit jamming noise under a certain condition. If the sensed signal from outside is weaker than a threshold, the jammer ignores since it determines that the signal cannot be reached to the Wi-Fi AP. If the sensed signal is stronger than another threshold, it also stops jamming and the attacker's signal is ignored by Wi-Fi AP. The jammer emits noise to the Wi-Fi AP only when it detects the attacker's signal is between the two thresholds. We summarize the strengths of our mechanism as follows.

- Considerate jamming benefits from the low implementation costs, because it requires no change in resource-constrained wireless devices. It is instead implemented with separate jammers and Wi-Fi AP.
- Different from the previous approach, considerate jamming not only jams for good, but also minimizes the interference on legitimate communications by its responsive and selective action.
- When the sensed attacker's signal is above the threshold, the jammer does not race with it, but yields the control to the Wi-Fi AP, thus saving a large amount of energy. This also reduces the potential risks like denial-of-service attacks.

The rest of this paper is organized as follows. We explain the overview and detailed procedure of proposed mechanism in Section 2. We show the feasibility of proposed mechanism through the simulation results in Section 3. Then we conclude the paper with future work in Section 4.

2. PROXIMITY-BASED ACCESS CONTROL

In this section, we present the considerate jamming mechanism to geographically control the wireless access. We first explain the overview of each system component, and then detail the interaction between them.

2.1 System Model

In Figure 2, we depict the configuration of each component in our proposed mechanism. There is a base station B in the center of geographical area which an attacker A cannot be located within. Our goal is to provide a mobile station M inside the area with an exclusive access to B, whereas not A. A jamming station J is installed at the boundary.

In a typical wireless communication, a wireless packet from a transceiver t is successfully received at a receiver r when the received signal strength $P_{t\to r}$ at r satisfies

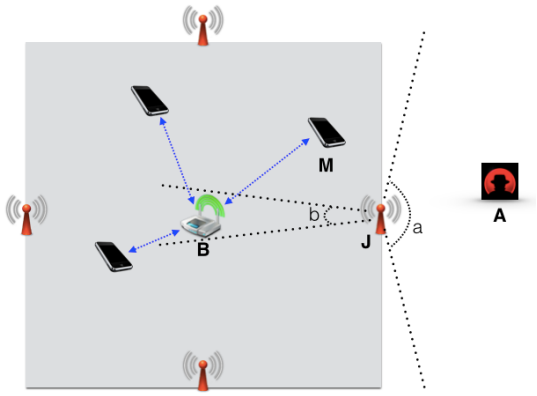

Figure 2: A basestation B provides the wireless network connection to a mobile station M within a boundary. A jamming station J is installed at the boundary. An attacker A tries to access this network from outside of boundary.

$$P_{t\to r} > \max\left(\mathcal{T}_{CCA}, (N_0 + I)\cdot \mathcal{T}_{SINR}\right), \quad (1)$$

where $\mathcal{T}_{CCA}$ is the clear channel assessment (CCA) threshold, N_0 is the ambient noise, I is the interference, and $\mathcal{T}_{SINR}$ is the signal-to-interference-noise ratio (SINR) threshold under given modulation technique. Note that the two threshold values $\mathcal{T}_{CCA}$ and $\mathcal{T}_{SINR}$ are dependent with the receiver r.

The equation (1) means that the signal can be successfully received when the received signal is above the CCA threshold *AND* the SINR of signal is above the SINR threshold. Since our goal is to make the signal from A *NOT* received at B while the signal from M received at B, we want to satisfy

$$P_{A\to B} < \max\left(\mathcal{T}_{CCA}, (N_0 + I)\cdot \mathcal{T}_{SINR}\right) < P_{M\to B}. \quad (2)$$

According to the standard radiowave propagation model, $P_{t\to r}$ is again defined as $P_{t\to r} = \beta \cdot P_t \cdot G_{tr} \cdot G_{rt} \cdot d_{tr}^{-n}$, where β is the frequency channel dependent radiowave propagation loss constant, P_t is the transmitting power at t, G_{tr} is the antenna gain of t to r, d_{tr} is the distance between t and r, and n is the loss exponent depending on the geographical configuration [11]. In this propagation model, an attacker A can easily increase its power P_A or its antenna gain G_{AB} to B, and thus it is not always guaranteed that $P_{A\to B} < P_{M\to B}$.

In our approach, we instead adjust I to satisfy (2). For instance, for the packets from M and A received above $\mathcal{T}_{CCA}$, we let I approach to 0 for the packets from M and let I increase for the packets from A by using jamming. That is, (2) is divided into the following two conditions.

$$\lim_{I\to P_{J\to B}} \quad P_{A\to B} < \max\left(\mathcal{T}_{CCA}, (N_0 + I)\cdot \mathcal{T}_{SINR}\right) \quad (3)$$

$$\lim_{I\to 0} \quad P_{M\to B} > \max\left(\mathcal{T}_{CCA}, (N_0 + I)\cdot \mathcal{T}_{SINR}\right) \quad (4)$$

In the following, we explain how we can achieve this by using jamming in detail.

2.2 System Design

We detail the design of our proposed system by explaining the jamming antenna configuration, the jamming radio operation and the basestation operation.

2.2.1 Antenna configuration

As depicted in Figure 2, a jammer station J has two directional antennas: one faces to outside with the angle a for listening signal, and the other faces to inside with the angle b for transmitting jamming noise to B. The angle a should be large enough to cover the possible locations of A, while b should be minimized in order to reduce the interference on other legitimate mobile stations. Throughout the paper, we denote the antenna facing toward the outside as receiving antenna and the antenna facing the inside as transmitting antenna. The two antennas in practice can be implemented with a hardware component by using digital beamforming technique [9]. Multiple jamming stations equipped with these two antennas are positioned at each side of boundary to cover the all possible locations for outside attacker.

2.2.2 Operation of jamming station and basestation

We show the procedural operation of jamming radio in Figure 3. In normal mode, the jamming radio listens to the channel by using the receiving antenna. Once it hears a signal above the parameter $\mathcal{P}_{min}$ and below the parameter $\mathcal{P}_{max}$, it starts decoding the header part of packet. In most wireless protocols, the total packet length is included in the header (e.g., Physical Layer Convergence Protocol (PLCP) header in IEEE 802.11 [3]). After reading the packet length, the jamming radio quickly switches itself into jamming mode, thus emitting jamming noise with the jamming power $\mathcal{P}_J$ during the packet length time until it returns to the listening mode. This can be regarded as a variant of reactive jamming, and its feasibility is well studied in other literature [12, 17].

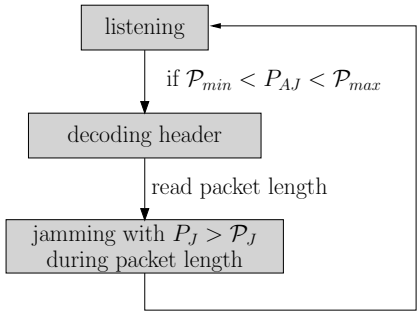

Figure 3: Operation of jamming station: the jammer J emits jamming noise if the RSS of A is between $\mathcal{P}_{min}$ and $\mathcal{P}_{max}$.

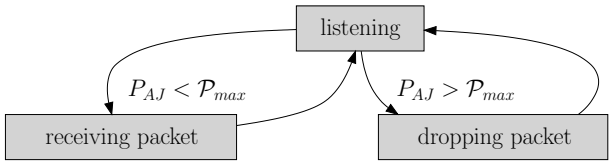

Figure 4: Operation of basestation: the basestation B drops the packet if the RSS of A at J is higher than $\mathcal{P}_{max}$.

2.2.3 Jamming system parameters

A jamming station J operates with the three system parameters $\mathcal{P}_{min}$, $\mathcal{P}_{max}$, and $\mathcal{P}_J$. The first two parameters determine the condition under which the jamming should start, and the last parameter stands for the strength of jamming noise at J.

As depicted in Figure 2, the jamming station J does not need to jam if the received signal strength (RSS) of packet from A is below the CCA threshold (i.e., $P_{A\to B} < \mathcal{T}_{CCA}$). Applying the definition of RSS of A at J to this condition based on the standard radiowave signal propagation model, $P_{A\to J}$ is represented as

$$P_{A\to J} < \mathcal{T}_{CCA} \cdot \frac{G_{AJ} \cdot G_{JA}}{G_{AB} \cdot G_{BA}} \cdot \left(\frac{d_{AB}}{d_{AJ}}\right)^n. \quad (5)$$

The term on the right hand side in (5) becomes the system parameter $\mathcal{P}_{min}$. Note that due to the near-field effect d_{AJ} cannot be 0 in this equation, and is dependent of wavelength used in operating wireless channel. As an exemplary configuration, if we assume that the attacker's antenna gains to J and B are the same, $G_{JA} = G_{BA}$, and there is one meter of buffer area outside the boundary where A cannot be located within, $\mathcal{P}_{min} = \mathcal{T}_{CCA} \cdot (d_{BJ} + 1)^n$.

Meanwhile, assuming the transmission power of legitimate mobile nodes is upper bounded by a certain level [1], a basestation B can simply ignore the signal of A above the maximum RSS of M (i.e., $P_{M\to B} < P_{A\to B}$). Note that in this case J does not transmit jamming noise. When applying the standard radio wave propagation model to this condition, P_A can be expressed with $P_{A\to J}$, which is the RSS of A observed at J. Thus, the equation is expressed as

$$P_{A\to J} > \beta \cdot P_M \cdot \frac{G_{MB} \cdot G_{JA} \cdot G_{AJ}}{G_{AB}} \cdot \left(\frac{d_{AB}}{d_{MB} \cdot d_{AJ}}\right)^n. \quad (6)$$

The term on the right hand side in (6) becomes the system parameter $\mathcal{P}_{max}$. As in case of $\mathcal{P}_{min}$, there exists a near field region between M and B. If we, for example, assume that the attacker's antenna gains to J and B are the same, $G_{MB} = G_{JA} = 1$ dBi, there is an one meter radius of buffer area around B where M cannot be located within, and there is one meter of buffer area outside the boundary where A cannot be located within, $\mathcal{P}_{max} = \beta \cdot P_M \cdot (d_{BJ} + 1)^n$.

When the jamming station senses the signal above $\mathcal{P}_{min}$ and below $\mathcal{P}_{max}$ from an outside attacker, it should generate a sufficient strength of jamming noise to satisfy (3). Assuming the signal from A is above $\mathcal{T}_{CCA}$, $P_{J\to B}$ has a lower bound as

$$P_{J\to B} > \frac{P_{A\to B}}{\mathcal{T}_{SINR}} - N_0. \quad (7)$$

In this equation, $P_{A\to B}$ can be expressed with $P_{A\to J}$, since J can observe the signal of A destined to B in the middle. Therefore, $P_{A\to B} = P_{A\to J} \cdot \frac{G_{AB} \cdot G_{BA}}{G_{AJ} \cdot G_{JA}} \cdot \left(\frac{d_{AJ}}{d_{AB}}\right)^n$. Substituting this into (7) and deploying $P_{J\to B}$, with respect to the transmitting power of J the equation is represented as

$$P_J > \frac{{d_{BJ}}^n}{\beta \cdot G_{JB} \cdot G_{BJ}} \cdot \left(\frac{P_{A\to J}}{\mathcal{T}_{SINR}} \cdot \frac{G_{AB} \cdot G_{BA}}{G_{AJ} \cdot G_{JA}} \cdot (\frac{d_{AJ}}{d_{AB}})^n - N_0\right). \quad (8)$$

This tells us that the term on the right hand side becomes $\mathcal{P}_J$ in (8) and J should transmit the stronger jamming noise than this parameter. If we also assume that the attacker's antenna is omnidirectional, all the other antenna gains are 1 dBi, one meter radius of inside and outside buffer areas, and N_0 is negligible, $\mathcal{P}_J = \frac{P_{A\to J}}{\beta \cdot \mathcal{T}_{SINR}} \cdot \left(\frac{d_{BJ}}{d_{BJ}+1}\right)^n$.

3. SIMULATION RESULTS

In this section, we validate the proposed theoretical model by using simulation. We first explain about the geographical configuration and wireless channel model used in our simulation. Then we show the system performance in the exemplary configuration.

[1] In real practice, the maximum transmitting power in most wireless protocols is regulated by legal institutions such as FCC and ETSI.

3.1 Simulation Configuration

So as to instantiate the proposed mechanism, we simulate with the infrastructure-mode Wi-Fi network. In our simulation, a Wi-Fi AP serves as a basestation, and Wi-Fi clients play a role of mobile stations. The system parameters follow the standard IEEE 802.11g protocol. Adopting the result of previous empirical study [7], for the base rate of traffic we set the high SINR threshold $\mathcal{T}_{SINR,h}$ nearly achieving 1.0 of frame delivery ratio (FDR) to 5 dB and the low SINR threshold $\mathcal{T}_{SINR,l}$ dropping FDR=0 to 3 dB. In this configuration, the RSS over distance from the two transmitters (20 dBm and 30 dBm) is plotted as Figure 5. Assuming the operating channel is at 2.4GHz and the antenna gains of both transmitter and receiver are 1, the receiver can successfully receive the 20 dBm of transmitter within about 114 meters and the 30 dBm of transmitter within about 269 meters.

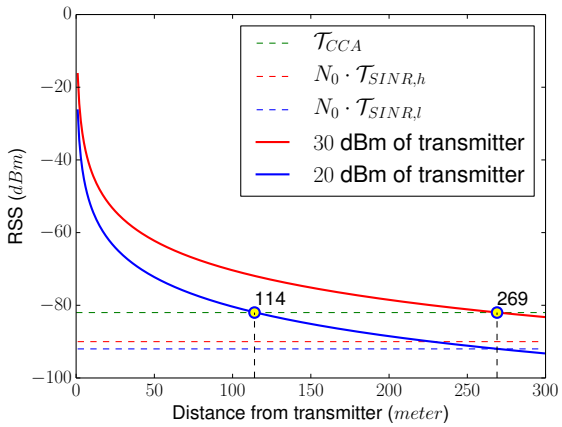

Figure 5: In our simulation configuration, the RSS over distance is shown for the two transmitters, of which transmitting powers are 20 dBm and 30 dBm, respectively. The operating frequency channel is 2.4GHz, $\mathcal{T}_{CCA} = -82$ dBm, $\mathcal{T}_{SINR,h} = 5$ dB, $\mathcal{T}_{SINR,l} = 3$ dB, $N_0 = -95$ dBm, $n = 2.7$, and we assume that the antenna gains of both transmitter and receiver are 1 dBi.

Based on these wireless channel related parameters, we depict the geographical configuration of system components in Figure 6. The Wi-Fi AP B is located in the center of boundary represented as a gray area. The Wi-Fi client M is also located inside this boundary, but cannot be inside the inner buffer zone represented as a blue area. The jammer J is at the boundary and the attacker A is outside the boundary. There is also an outer buffer zone (represented as a green area) where A cannot be located within. In our simulation, we set the width of these two buffer zones to one meter, and the distance between B and J is 80 meters, and the distance between B and A is unknown.

In practice, the attacker A's signal can be observed by multiple jammers depending on the configuration. However, jamming by multiple jammers increase the interference on B, thus not impairing the security performance of proposed system. Therefore, without loss of generality we simulate with one jammer installed at one side of boundary.

We limit the transmitting power of all Wi-Fi clients to 20 dBm, and therefore M can successfully send packets to B anywhere within this boundary according to the RSS curve in Figure 5. We set the antenna gains of B, M, and J to all 1 dBi. When M is closest to B (i.e., $d_{MB} = 1$), the RSS observed at B is $P_{M\to B} = -26.37$ dBm. On the other hand, for example, if the antenna gain of A to

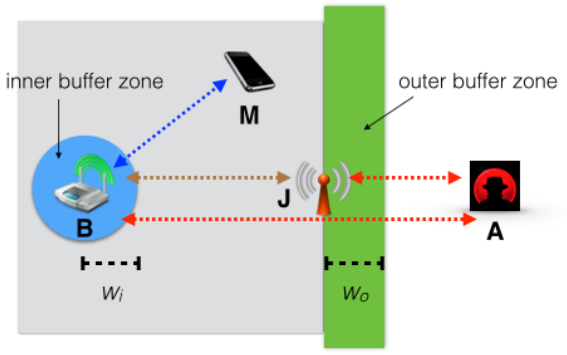

Figure 6: Depicted is the geographical placement of system component in our simulation. ($W_i = W_o = 1$ meter, $d_{BJ} = 80$ meters, and $d_{BA} \geq d_{BJ} + W_o$)

B is $G_{AB} = 1$ dBi, $P_A = P_M$, and $d_{BA} = 100$ meters, then $P_{A\to B} = -80.37$ dBm, and therefore A can easily gain the network access to B.

3.2 Simulation Results

Since in our configuration $d_{BA} \geq 81$, the jamming system parameters $\mathcal{P}_{min}$ and $\mathcal{P}_{max}$ are respectively computed as $\mathcal{P}_{min} = -30.47$ dBm and $\mathcal{P}_{max} = 25.15$ dBm according to (5) and (6). We also set $\mathcal{P}_J$ to $\mathcal{P}_J = \frac{P_{A\to J}}{\beta \cdot \mathcal{T}_{SINR}}$ which satisfies (8). Since we do not allow any packets from A to be delivered to B ($FDR \to 0$), we use the conservative SINR threshold, i.e., $\mathcal{T}_{SINR} = 3$ dB. Figure 7 shows the jamming power of J depending on its RSS observation for A.

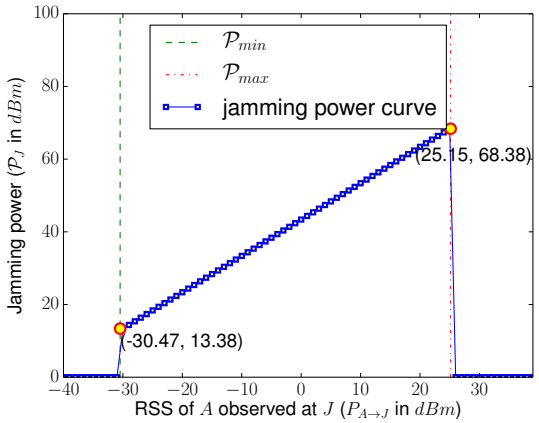

Figure 7: Depending on the observed RSS of the attacker A, the jamming station J changes its transmitting power. For an easy presentation, we plot 0 mW (no jamming) to 0 dBm in y-axis.

The jammer J starts jamming when the observed RSS of A is at $\mathcal{P}_{min}$, and stops when it reaches $\mathcal{P}_{max}$. When J observes the RSS of A as $\mathcal{P}_{max}$, $P_{A\to B}$ is equal to -26.37 dBm. Thus, the Wi-Fi AP B only accepts packets if the RSS is between $\mathcal{T}_{CCA}$ and -26.37 dBm as shown as a green zone in Figure 8. Without J, B receives the packets from A when the RSS curve of $P_{A\to B}$ passes through the green zone. When J operates, the condition of packet reception at B should also satisfies (1). The purple zone above the

red dotted curve corresponds the condition. Consequently, B does not receive any packets from A unless their RSS values are within the intersection area Z_1 and Z_2.

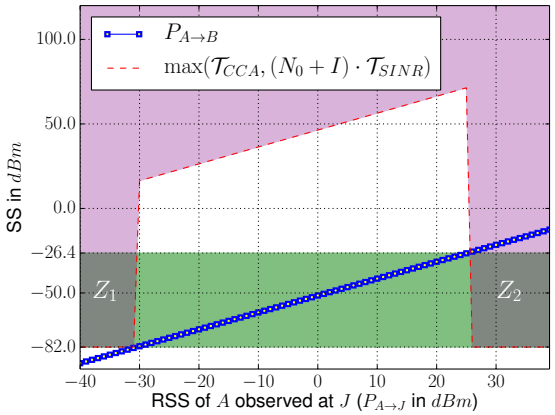

Figure 8: The blue linear curve represents the RSS of A at B per RSS observation at J. According to the system parameters, B only receives packets if the RSS is within the green zone. The red dotted curve shows the minimum signal strength allowing the packet reception when J operates as it observes the A's signal. By these two conditions, the A's packets are received only when they are across the zone Z_1 and Z_2. Therefore, any packets from A cannot reach to B in our simulation.

4. CONCLUSION AND FUTURE WORK

In this paper, we presented a proximity-based wireless access control mechanism using considerate jamming. Since the mechanism does not require any modification in wireless clients, it is useful for securing resource constrained wireless devices in a geographical configuration. It is reactive to outside attacker and selectively interferes with the basestation, thus reducing impact on legitimate communications. We provided the theoretical model with system parameters, and validated it through simulation.

The preliminary result presented in this paper opens more research opportunities. For example, more advanced attacker trying to divert the proposed mechanism should be considered. An attacker can use a high gain antenna (or even beamforming antenna) to surpass the Z_1 and Z_2 in Figure 8. In fact, in our theoretical model we assume the antenna gain of an attacker to the jammer and the basestation are identical. To cope with this type of attacker, the locations of jammers and basestation need to be in secret. In the case that an attacker finds the location of inside basestation by eavesdropping beacon signals, one may also consider generating fake signals at different locations.

In the further study, we will validate the feasibility of proposed mechanism with the real world system. Due to the randomness of wireless channel, it will be challenging to apply our approach in real practice. The system parameters should be carefully determined with empirical measurements to be marginally resistant to observation errors.

5. REFERENCES

[1] InnerWireless, Inc.

[2] IEEE Std 802.11i-2004, Amendment 6: Medium Access Control (MAC) Security Enhancements, 2004.

[3] IEEE Std 802.11-2012, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2012.

[4] S. Brands and D. Chaum. Distance-bounding protocols. In T. Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 344–359. Springer Berlin Heidelberg, 1994.

[5] M. Cagalj, S. Capkun, and J.-P. Hubaux. Key agreement in peer-to-peer wireless networks. *Proceedings of the IEEE*, 94(2):467–478, Feb 2006.

[6] S. Capkun and J.-P. Hubaux. Secure positioning of wireless devices with application to sensor networks. In *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, volume 3, pages 1917–1928 vol. 3, March 2005.

[7] D. Halperin, W. Hu, A. Sheth, and D. Wetherall. Predictable 802.11 packet delivery from wireless channel measurements. *SIGCOMM Comput. Commun. Rev.*, 40(4):159–170, Aug. 2010.

[8] Y. S. Kim, P. Tague, H. Lee, and H. Kim. Carving secure wi-fi zones with defensive jamming. In *7th ACM Symposium on Information, Computer, and Communications Security (AsiaCCS)*, May 2012.

[9] J. Litva and T. K. Lo. *Digital Beamforming in Wireless Communications*. Artech House, Inc., Norwood, MA, USA, 1st edition, 1996.

[10] R. Negi and S. Goel. Secret communication using artificial noise. In *Vehicular Technology Conference, 2005. VTC-2005-Fall. 2005 IEEE 62nd*, volume 3, pages 1906–1910, 2005.

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

[12] A. Proano and L. Lazos. Packet-hiding methods for preventing selective jamming attacks. *Dependable and Secure Computing, IEEE Transactions on*, 9(1):101–114, Jan.-Feb. 2012.

[13] S. Sankararaman, K. Abu-Affash, A. Efrat, S. D. Eriksson-Bique, V. Polishchuk, S. Ramasubramanian, and M. Segal. Optimization schemes for protective jamming. In *Proceedings of the thirteenth ACM international symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc '12, pages 65–74, New York, NY, USA, 2012. ACM.

[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] D. Singelee and B. Preneel. Key establishment using secure distance bounding protocols. In *Mobile and Ubiquitous Systems: Networking Services, 2007. MobiQuitous 2007. Fourth Annual International Conference on*, Aug 2007.

[16] J. Vilela, M. Bloch, J. Barros, and S. McLaughlin. Wireless secrecy regions with friendly jamming. *Information Forensics and Security, IEEE Transactions on*, 6(2):256–266, June 2011.

[17] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders. Short paper: reactive jamming in wireless networks: how realistic is the threat? In *Proceedings of the fourth ACM conference on Wireless network security*, WiSec '11, pages 47–52, New York, NY, USA, 2011. ACM.