Preserving Location Privacy in Radio Networks Using a Stackelberg Game Framework

Mojgan Khaledi
School of Computing
University of Utah
mojgankh@cs.utah.edu

Mehrdad Khaledi
ECSE
RPI
khalem@rpi.edu

Sneha Kumar Kasera
School of Computing
University of Utah
kasera@cs.utah.edu

Neal Patwari
ECE
University of Utah
npatwari@ece.utah.edu

ABSTRACT

Radio network information is leaked well beyond the perimeter in which the radio network is deployed. We investigate attacks where person location can be inferred using the radio characteristics of wireless links (e.g., the received signal strength). An attacker can deploy a network of receivers which measure the received signal strength of the radio signals transmitted by the legitimate wireless devices inside a perimeter, allowing the attacker to learn the locations of people moving in the vicinity of the devices inside the perimeter. In this paper, we develop the first solution to this location privacy problem where neither the attacker nodes nor the tracked moving object transmit any RF signals. We first model the radio network leakage attack using a Stackelberg game. Next, we define utility and cost functions related to the defender and attacker actions. Last, using our utility and cost functions, we find the optimal strategy for the defender by applying a greedy method. We evaluate our game theoretic framework using experiments and find that our approach significantly reduces the chance of an attacker determining the location of people inside a perimeter.

1. INTRODUCTION

Wireless devices in a wireless network create a radio wave field in and around the area in which the network is deployed. Moving objects and people can disturb the field in ways that can be measured at locations in and outside of the deployment area [1–3]. Essentially, the radio network information is leaked well beyond the perimeter in which the radio network is deployed. In our research, we investigate defense mechanisms against attacks where person location can be inferred using the radio characteristics of wireless links (e.g., the received signal strength, RSS, of wireless links). In these attacks, a person or a group has one or more wireless devices (wireless access points/sensor nodes) deployed in an area in which they expect privacy, for example, their home. An attacker can deploy a network of receivers which measure the received signal strength of the radio signals transmitted by the legitimate wireless devices, allowing the attacker to learn the locations of people moving in the vicinity of the devices, information that the attacker would not be able to know if the wireless devices did not exist. Such an attack is possible even when the network is otherwise secure against data eavesdropping.

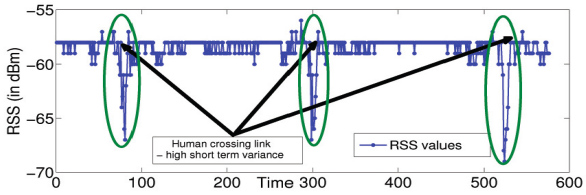

Figure 1: Detection of Line of Sight Crossing

Consider a scenario where military personnel set up a base in an area surrounded by a tall concrete wall. Among the other facilities on the base, there are various wireless networks used for voice, video, and data communications among the personnel, on and off the base. Security protocols are used so that an adversary cannot eavesdrop on the data communicated. However, an attacker sets up a network of receivers, in locations outside of the wall of the base, which measure various characteristics of any signals that these receive and can infer where the people inside the base are and choose those areas to bomb for causing maximum damage.

In a different scenario, paparazzi might use the radio network leakage to learn where in a celebrity's house people are located, and be able to know beforehand which gate and when the celebrity may exit. Having a wireless network leaking the positions and number of people in the area of the network is generally problematic in a variety of different contexts where people rightfully expect such information to be private. The potential for invasion of privacy is significant. Fundamentally, any transmitted radio signal interacts with the radio propagation environment in a way that can be measured at a receiver. By using multiple distributed receivers and observing the changes over time, an eavesdrop-

Q2SWinet'16, November 13-17, 2016, Malta, Malta

DOI: http://dx.doi.org/10.1145/2988272.2988277

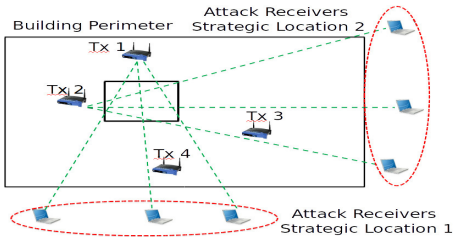

Figure 2: Radio network leakage attack.

per can estimate where the changes in the environment are occurring, and infer human or other moving object locations. Essentially, a wireless network *leaks information* about the locations of people in the vicinity of that network to anyone who wishes to and is capable of listening.

In order to motivate our research, we show a temporal plot of RSS measured by a receiver outside of a building wall, in Figure 1. One can automatically identify periods in which a person is crossing the line between transmitter and receiver by comparing the short and long term variance. In general, environmental noise causes very little variations in the RSS of a wireless link, however, human presence in the vicinity of the link causes a high temporal variation. Thus, if we monitor the variance in the RSS of each link and observe a very high short term variance in some link, we can infer that a human is obstructing the line of sight path of the link.

There is a growing amount of work ([11–13,15]) that shows how radio signal can be used for obtaining location information of moving objects that are not transmitting any radio signals themselves. Adib et al. [11] have developed WiVi to track moving humans through walls. In a follow up work [12], the authors propose an approach to track the 3d location of the moving object through walls. In another work [13], the reflection of wireless signals from a human body is used to identify human gestures. More recently, Banerjee et al. [15], have demonstrated how humans can be tracked through walls without transmitting any signals from the attack nodes. One could possibly consider using defensive jamming [16] to corrupt the transmitter signals and preserve location privacy. However, in [15] the authors demonstrate that even by adding noise to the radio network, the attacker is still able to locate persons within the building.

In this paper, we develop the first solution to the location privacy problem above, where neither the attacker nodes nor the tracked moving object transmit any RF signals, using a game theoretic framework. In our game theoretic model, the defender (the genuine wireless network) deploys multiple transmitters in different locations and changes transmitters in some random or probabilistic fashion to minimize the chance of the attack receivers locating the people inside certain parts of the building. Figure 2 shows an overview of the attack due to radio network leakage. In this figure, an attacker is interested in monitoring an area of interest inside the building. The defender deploys four transmitters. When transmitter Tx 1 transmits, it would make most sense to place the attacker receivers in strategic area 1 to monitor the area of interest. When transmitter Tx 2 transmits, it would make most sense to place the attacker receivers in the strategic area 2 to monitor the area of interest. The attacker need not deploy attack receivers in all strategic areas because of cost. More importantly, the higher number of attack receivers the attacker deploys the higher is the probability of it being detected (e.g., by security cameras or guards etc.). Furthermore, the attacker cannot "quickly" move and deploy attack receivers from one strategic area to another. Therefore, by appropriately changing the transmitter location the defender can defend against the attacker.

Note that we only show the transmitters and attack receivers in Figure 2. Movement can still be detected in the presence of other objects both inside and outside the monitored area [15]. Furthermore, while we show only one kind of transmitter, a WiFi access point, and only one kind of receivers, laptops, other wireless devices or nodes with wireless capabilities can also contribute to or be used to create radio network leakage attacks. Additionally, Figure 2 shows only one kind of building perimeter. Our research applies to other building perimeters as well.

We model this attacker-defender scenario as a Stackleberg game, which is a sequential game where the defender plays first, then attacker selects its best strategy by observing the defender's strategy. Our goal is to maximize the defender's benefit, i.e, maximize location privacy. The defender's strategy is to probabilistically schedules transmitters. The attacker deploys attack receivers in strategic areas outside the building perimeter. The attacker has limited resources and incurs a cost in deploying attack receivers, the higher number of attack receivers the attacker deploys the higher is the probability of it being detected (by security cameras or guards etc.). Therefore, the attacker tries to deploys attack receivers only in a strategic area that maximizes its chance of violating location privacy.

Game theory provides us with a methodology to allocate limited security resources to protect systems and infrastructure, taking into account the different weights of different targets and an adversary's response to any particular attack prevention strategy [8, 9]. Game theory allows for modeling situations of conflict and for predicting the behavior of participants. In situations where one of the players has the ability to enforce its strategy on the other, the game is called a Stackleberg game. In the Stackleberg game [9], the player who announces its strategy first is called the leader and the other player who reacts to the leader's strategy is called the follower. In our problem context, the leader is the defender trying to ensure that the attack receivers cannot accurately infer people location in the area of interest, and the attacker is the follower trying to suitably place the attack receivers to maximize its utility. Our goal in this paper is to use the Stackelberg game model to find a probabilistic scheduling for the defender while minimizing the possibility of determination of people location by the attacker.

Our contributions in this paper are as follows. First, we model the radio network leakage attack using a Stackelberg game. Second, we define utility and cost functions related to the defender and attacker actions. Third, using our utility and cost functions, we find the optimal strategy for the defender by applying a greedy method. We experimentally evaluate our game theoretic model in two different settings - in an open environment and a cluttered office. Our experimental results show that when using our approach, the minimum localization error for the attacker increases by $36\% - 240\%$. Higher localization error corresponds to more privacy. We expect the localization error for the attacker to be significantly higher for larger areas. We briefly discuss

the practicality of deploying our approach before concluding the paper.

The rest of this paper is organized as follows. Section 2 contains the relevant related work. Section 3 provides some preliminary game theoretic concepts. Section 4 represents our adversary model. In Section 5, we formulate the problem and develop our solution. Experimental results are reported in Section 6. Section 7 is devoted to practical considerations. The concluding remarks and some directions for future work are provided in Section 8.

2. RELATED WORK

Location of a wireless device or a human represents an important piece of information about the device or the human. This information when available to adversaries can be used for privacy violation. More seriously, it can be used by adversaries for potentially dangerous life threatening attacks. There is a growing amount of work (e.g., [1–3,14]) that shows how devices or humans can be localized in both benign and malicious settings. There are some interesting existing solutions for preserving location privacy as well (e.g., [10, 17]). However, a vast majority of these are for preserving the privacy of active transmitters locations. In these systems, the wireless device (e.g., a mobile phone, RFID tag, low-power radio transceiver) that is being located is actively communicating with the surrounding network infrastructure (e.g., WiFi APs, RFID readers, and other radio transceivers).

In their recent work [15], the authors demonstrate that the presence, location, and movements of people not carrying any wireless device can still be eavesdropped by measuring the RSS of the links between the devices composing the legitimate network and few receivers positioned outside the target area. This can be achieved without requiring a complex network infrastructure or previous access to the target area for an initial calibration. This paper [15] also proposes a defense mechanism to fool the attack receivers by changing the power at the wireless transmitters. However, it is found in [15] that the attacker can compensate for the changes in the transmit power and still determine the human locations. The compensation mechanism is based on the the intuition that an artificial transmit power change at a transmitter will impact all the links between the transmitter and the attack receivers, whereas genuine power changes due to human movement are likely to impact only some of the links. Thus, there is a need to seek newer, novel solutions that can effectively preserve human location privacy in spite of radio network leakage.

We propose a novel method based on a game theoretic framework to tackle the location privacy problem in spite of radio network leakage. Our game theoretic model is based on a Stackelberg game that has been used in attacker-defender scenarios [4–6]. However, our work is the first application of the Stackelberg game for the purpose of protecting location privacy in radio networks.

3. GAME THEORY PRELIMINARIES

Game theory is a study of strategic interactions among selfish agents that yields the desired outcome by considering the preferences of agents. Stackelberg game is a type of sequential game where one player, leader, commits to a strategy first and the other players, followers, selfishly choose their best response strategies considering the leader's strategy. This type of game is commonly used for modeling attacker defender scenarios in the security domain where the defender commits to the strategy first. Table 1, shows a simple example of the Stackelberg game between an attacker and a defender. The defender is the row player and the attacker is the column player. Here, d_1 and d_2 are the defender strategies, and a_1 and a_2 are the attacker strategies. In this game the best strategy for the defender is d_1. In this case, the attacker plays a_1. So, the utility of defender is 3. However, if the defender plays d_2, then the attacker plays a_2. As result, the utility of defender will be 1. As shown in this example, in the Stackelberg game, the goal is to maximize the utility of the first player, defender. To do this, the defender chooses a strategy with maximum utility by taking the attacker's best strategy into account.

Table 1: An Example of Stackelberg Game Payoff Table

	a_1	a_2
d_1	(3, 1)	(1, 0)
d_2	(4, 1)	(1, 3)

If the defender plays deterministically (e.g., in Table 1 it plays a pure strategy d_1), then the attacker knows the exact strategy of the defender and selects the pure strategy a_1. However, if the defender plays probabilistically (by assigning probabilities to pure strategies d_1, d_2), then the attacker is not able to find the exact action of the defender in real time.

4. ADVERSARY MODEL

We make the following assumptions about the attacker:

- The attacker is able to deploy multiple attack receivers within the transmission range of the legitimate transmitter(s) outside the area being monitored. The attacker is able to measure the physical layer information (e.g., the received signal strength) of the links between the transmitter(s) and the attack receivers and localize humans moving inside the monitored area that cross the transmitter-receiver links.

- The attacker does not have access to the content of the packets transmitted by the legitimate network nodes. It does not depend on understanding the content of the packets.

- The defender does not know where the attacker will place its receivers and the attacker does not know the exact locations of transmitters.

5. PROBLEM FORMULATION AND SOLUTION

We develop a game-theoretic framework for preserving location privacy in radio networks. Our framework is characterized by one defender and multiple target regions that the defender wishes to protect from a location privacy attack. We use the attack scenario shown in Figure 3 for our problem formulation. Figure 3 is a more generalized version of the attack scenario shown in Figure 2. Figure 3 shows multiple target regions. These target regions comprise of predefined subsections of a building where people move. In

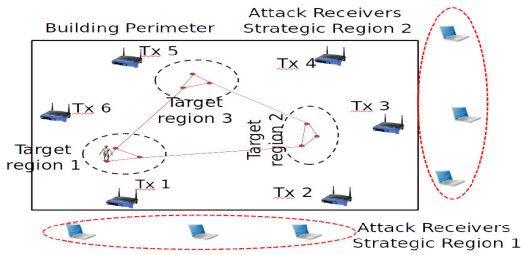

Figure 3: Radio network leakage attack scenario with multiple target regions.

this setting, the defender cannot schedules transmitters deterministically, otherwise the attacker will definitely succeed in violating the location privacy of a target region by deploying attack receivers in the best strategic area outside the building and measuring the variations in wireless signal strength. As a result, the defender should adapt an unpredictable scheduling strategy, randomizing over the transmitters with the goal of minimizing the possibility of determination of people location by the attacker. In our work, we use the Stackelberg game to formulate the defender/attacker scenario. In this game, the defender commits to a strategy first that is optimal (maximizes its expected utility). Then, the attacker plays its best strategy considering the strategy the defender plays. The goal is to maximize the utility of defender in a way that even if the attacker selects its best strategy, the utility of attacker will be minimum. This goal essentially corresponds to maximizing the localization errors for the attacker.

5.1 System Model

In our game, we have two players, a defender, d, and an attacker, a. We consider a set of transmitters, $T = \{t_1, t_2, \ldots, t_K\}$ deployed at different locations inside a building. We also consider a set of target regions, $R = \{r_1, r_2, \ldots, r_N\}$, that the defender wants to protect from a location privacy attack. In addition, we assume that set of strategic area locations $S = \{s_1, s_2, \ldots, s_M\}$ exists, where the attacker deploys its attack receivers.

The defender and the attacker strategies are dependent on the time of the day. This happens because the probability of human movements in a target region changes dependent on the time of the day. For example, in a campus environment, most students and faculty members move towards a specific place for lunch at a specific time [21] and if the attacker attacks at that time it can cause the maximum damage. To consider the variations of the attacker and the defender strategies during the time, we divide time into T slots.

In a recent work on location detection [20] using radio tomographic imaging, the authors showed that only those transmitters that have radio wave fields inside the moving area are effective in location detection. We define effective transmitters for each target region as the minimum number of transmitters that need to be turned off in order to preserve the location privacy of a specific target region. When the effective transmitters of a target region are turned off, an attacker cannot measure the change of the received signal strength caused by people movements. However, the defender cannot turn off all transmitters to protect all target regions or turn off a set of transmitters at all times to protect one target region (depending on the actual application of the transmitters). Therefore, the defender needs a strategy for turning off transmitters. The strategy should be random instead of deterministic with the goal of reducing the chance of an attacker determining the location of people inside target regions while considering the limits on the number of transmitters that can be turned off.

Table 2: Notation

Parameter	Definition
d	Defender
a	Attacker
$\vec{\sigma_d}$	Defender pure strategy
$\vec{\sigma_a}$	Attacker pure strategy
$\vec{m}$	Defender mixed strategy
r_a	Number of active attack receivers
s_a	Strategic location
N	Number of target regions
T	Number of time slots
$PD(j, \sigma_a)$	Probability of detection of the target region j by the attacker
$c_{j,t}(\vec{m})$	Probability that effective transmitters in target region j are turned off in time slot t
$Re_d(j,t), Pe_d(j,t)$	Reward and penalty for defender
$Re_a(j,t), Pe_a(j,t)$	Reward and penalty for attacker
$u_d(\vec{m}, \vec{\sigma_a})$	Utility of defender
$u_a(\vec{m}, \vec{\sigma_a})$	Utility of attacker
m	Number of target regions that defender is able to protect in each time slot
$p_{j,t}$	Probability of movement in target region j in time slot t
Δ	Increment in the probability of turning off effective transmitters of a target region in each iteration of Algorithm 1

The pure strategy for the defender, $\vec{\sigma_d} = (\sigma_d^1, \sigma_d^2, \ldots, \sigma_d^T)$, is a row vector determining the effective transmitters of which target region are turned off in each time slot and the pure strategy for the attacker, $\sigma_a = (s_a, r_a)$, is selecting one strategic area and also the number of active receivers in the strategic region.

To make it hard for attackers to find its exact actions, the defender uses a randomized, mixed strategy, instead of a pure strategy. The defender mixed strategy, $\vec{m} = (m_1, m_2, \ldots, m_{|\sigma_d|})$, essentially describes the probability of playing each pure strategy.

5.2 Utilities

The defender and attacker utilities depend on whether the attacker is able to attack or not. Let $PD(j, \sigma_a)$ denote the probability of detection of the target region j by the attacker, if the attacker plays $\sigma_a = (s_a, r_a)$. We formulate $PD(j, \sigma_a)$ as the following:

$$PD(j, \sigma_a) = I(j, s_a) D(r_a, s_a) \quad (1)$$

$I(j, s_a)$ in (1) determines if s_a, the strategic area that is selected by the attacker, is target region j's corresponding strategic area. For target region, j, s_a is a corresponding strategic area if the attacker can detect movements in target region j from that strategic area. Depending on the location of target regions inside the building, there will be multiple corresponding strategic areas for each target region.

Let $CR(j)$ denote the corresponding strategic areas for target region j. Also, let $Cov(j, s_a)$ represent the percentage of the whole area that is covered by s_a in case of movements

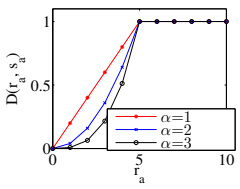

Figure 4: $D(r_a, s_a)$ with different values of α

in target region j. Then, in (1), $I(j, s_a)$ can be obtained by the following function:

$$I(j, s_a) = \begin{cases} Cov(j, s_a) & s_a \in CR(j) \\ 0 & otherwise \end{cases} \quad (2)$$

Where, $0 < Cov_i(s_a^i, t) \leq 1$.

$D(r_a, s_a)$ in (1) represents the probability of detection if the attacker deploys r_a receivers in s_a. We obtain this probability by the following function.

$$D(r_a, s_a) = \begin{cases} (\frac{r_a}{r_{max}(s_a)})^\alpha & 0 < r_a \leq r_{max}(s_a) \\ 1 & r_a \geq r_{max}(s_a) \end{cases} \quad (3)$$

Here, $r_{max}(s_a)$ in (3) is the saturation point. Based on our experimental evaluations, the probability of detection increases by increasing the number of receivers. However, the probability of movement detection does not increase by increasing the number of receivers beyond this saturation point. In other words, the probability of movement detection is 1 beyond the saturation point, r_{max}.

The value of r_{max} depends on the location of strategic region, s_a. For instance, if there are some "radio" obstacles in some strategic region outside a building (e.g., a metal door), then the attacker needs to deploy more attack receivers in those areas to detect changes in the RSS. Figure 4 shows the value of $D(r_a, s_a)$ with $r_{max}(s_a) = 5$ and α equal to 1, 2, and 3. Based on our experiment, we set $\alpha = 2$ in our evaluation.

Besides the probability of attack, $PD(j, \sigma_a)$, the utilities of the defender and the attacker also depend on whether or not the defender turns off effective transmitters of the target region. $c_{j,t}(\vec{m})$ represents the probability that effective transmitters of target region j are turned off in time slot t under mixed strategy $\vec{m}$ and is equal to $c_{j,t}(\vec{m}) = \sum_{m_i \in \vec{m}} m_i x_{j,t}(m_i)$. m_i is the probability of playing the pure strategy i. $x_{j,t}(m_i) \in \{0, 1\}$ shows whether or not the effective transmitters of target region j are turned off in time slot t for strategy i. $x_{j,t}(m_i) = 1$, if the effective transmitters of target region j are turned off in time slot t. Otherwise, $x_{j,t}(m_i) = 0$.

We obtain the utility of the defender, $u_d(\vec{m}, \vec{\sigma_a})$, and the utility of the attacker, $u_a(\vec{m}, \vec{\sigma_a})$, when the defender plays the mixed strategy $\vec{m}$ and the attacker plays $\vec{\sigma_a}$, from the following formulas.

$$u_d(\vec{m}, \vec{\sigma_a}) = \sum_{j=1}^{N} PD(j, \sigma_a) \sum_{t=1}^{T} [c_{j,t}(\vec{m}) Re_d(j, t) - (1 - c_{j,t}(\vec{m})) Pe_d(j, t)] \quad (4)$$

$$u_a(\vec{m}, \vec{\sigma_a}) = \sum_{j=1}^{N} PD(j, \sigma_a) \sum_{t=1}^{T} [(1 - c_{j,t}(\vec{m})) Re_a(j, t) - c_{j,t}(\vec{m}) Pe_a(j, t)] \quad (5)$$

We observe from equation (4) that in each time slot t and for each target region j, the utility of the defender will increase by the amount of reward, $Re_d(j, t)$, if the defender turns off the effective transmitters of target region j when being attacked in time slot t. Otherwise, this utility will decrease by the amount of penalty, $Pe_d(j, t)$. Note that the defender's goal is to maximize $u_d(\vec{m}, \vec{\sigma_a})$ in an equilibrium. This means that $\vec{\sigma_a}$ should be the best strategy for the attacker when the defender plays the mixed strategy $\vec{m}$. In addition, the defender should consider the limits on the number of transmitters that can be turned off (constraint 8), otherwise, $C = 1$ is the optimal strategy for the defender. As in the case of the defender, the utility of the attacker increases by amount of reward, $Re_a(j, t)$, in case of a successful attack (effective transmitters of target region j are turned on in time slot t) and decreases by amount of penalty, $Pe_a(j, t)$, if the attacker is unable to attack the target region j in time slot t.

The amount of reward and penalty for a successful attack on target region j in time slot t, $Re_a(j, t)$ and $Pe_d(j, t)$, depend on the probability of movement in target region j in time slot t. The attacker can causes more damages to the target region with higher probability of movement. As a result, Re_a and Pe_d are greater for a target region with a higher probability of movement.

Let P be a $N \times T$ matrix where N, and T denote number of target regions and number of time slots, respectively. In this matrix, each item, $p_{j,t}$, represents the probability of movement for target region j in time slot t. Then, $Re_a(j, t)$ and $Pe_d(j, t)$ are obtained as follows:

$$Re_a(j, t) = Pe_d(j, t) = \frac{p_{j,t}}{\sum_{j=1}^{N} p_{j,t}} \lambda_a \quad (6)$$

Here, λ_a is a constant tunable parameter for both reward and penalty in case of a successful attack.

$Re_d(j, t)$ and $Pe_a(j, t)$ depend on the number of receivers that are chosen by the attacker. As the number of receivers increases, the attacker's probability of detecting movements also increases. However, increasing the number of active receivers also increases the deployment cost of the attacker and the probability of being detected by security cameras or guards. Let $cost(\sigma_a)$ represent this cost that depends on the number of active receivers. Then, $Re_d(j, t) = Pe_a(j, t) = cost(\sigma_a)$. The dependence of this cost on σ_a is due to the fact that the attacker can deploy different number of receivers. We express this cost as $cost(\sigma_a) = r_a \times \lambda_c$, where, λ_c is the cost for adding one receiver.

5.3 Optimization problem

Having determined the utilities of the attacker and the defender, characterized in (4) and (5), we can now find the Stackelberg equilibrium. In the stackelberg game, the defender probabilistically turns off the effective transmitters in advance then the attacker make its own choice to attack a specific target region.

To find the stackelberg equilibrium, the defender has to calculate the best reply of attacker to each of its mixed strategy and selects the mixed strategy that maximizes the defender utility. Formally, the stackelberg equilibrium can be

Algorithm 1: Greedy Approach

input : : $C_{N\times T} = 0$, Δ
output: : $C_{N\times T}$

1 **while** *(1)* **do**
2 $C'_{N\times T} = C_{N\times T}$;
3 **foreach** *time slot t* **do**
  `// Initialization`
4 $u_d^* = -\infty$;
5 $selected\_target\_region = 0$;
6 **foreach** *target region j* **do**
7 $c'_{j,t} = c'_{j,t} + \Delta$;
8 Find the attacker best strategy, σ_a^*, $\sigma_a^* \in \underset{\sigma_a}{\text{argmax}}(u_a(C', \sigma_a))$;
9 **if** $u_d(C', \sigma_a^*) > u_d^*$ **then**
10 $u_d^* = u_d(C', \sigma_a^*)$;
11 $selected\_target\_region = j$;
12 **end**
13 **end**
  `// Update C`
14 $c_{selected\_target\_region,t} = c_{selected\_target\_region,t} + \Delta$;
15 **end**
16 **if** $\sum_j \sum_t c_{j,t} = mT$ **then**
17 exit;
18 **end**
19 **end**

obtained by solving the following optimization problem:

$$\underset{\vec{m},\vec{\sigma_a}}{\text{argmax}}(u_d(\vec{m}, \vec{\sigma_a}))$$

$$s.t.$$

$$u_a(\vec{m}, \vec{\sigma_a}) \geq u_a(\vec{m}, \vec{\sigma_a})\forall\vec{\sigma_a} \quad (7)$$

$$\sum_{t=1}^{T}\sum_{j=1}^{N} c_{j,t}(\vec{m}) \leq mT \quad (8)$$

The objective function in the above optimization problem maximizes the utility of the defender. Also, in order to obtain an equilibrium, the output of the optimization problem, $(\vec{m}, \vec{\sigma_a})$, should be optimal for the attacker as well. Constraint (7) represents this attacker optimality requirement. In other words, given the defender mixed strategy, $\vec{m}$, the attacker strategy, $\vec{\sigma_a}$, should be its best strategy. This ensures that if the first player, defender, plays $\vec{m}$, then the second player, attacker, plays $\vec{\sigma_a}$. Therefore, the solution of the above optimization problem, $(\vec{m}, \vec{\sigma_a})$, results in a Stackelberg equilibrium. Constraint (8) states that the sum of probabilities of turning off the effective transmitters of all target regions in T time slots must be equal to mT, where $m < N$ is number of target regions that defender is able to protect in each time slots.

In order to solve the optimization problem, we use a Greedy approach that is inspired by the scheme presented in [7]. Our Greedy approach is described in Algorithm 1. In this approach, instead of finding the optimal mixed strategy, $\vec{m}$, for the defender, we find $c_{j,t}(\vec{m})$ for all target regions and all time slots. Let C be a $N \times T$ matrix where N and T denote number of target regions and number of time slots, respectively. We know $\sum_{j=1}^{N} c(j,t) \leq m$ and $\sum_{j=1}^{N}\sum_{t=1}^{T} c(j,t) \leq mT$. We initialize $C = 0$ in the first iteration of algorithm, and update the values of C for all time slots based on the greedy strategy in each iteration. At each iteration, we add Δ to one of N target regions in the time slot that maximizes the utility of the defender in the same time slot given the attacker best strategy for current C, σ_a^* (see lines 4-14 in Algorithm 1). Δ is a small value between 0 and 1. The algorithm is repeated until $\sum_{i=1}^{n}\sum_{t=1}^{k} c(i,t) = mT$.

Time complexity: In each iteration of the greedy algorithm, we have one loop that iterates over T, the number of time slots. Also, for each time slot, we must find the target region that maximizes the utility of defender which takes $O(N)$. Recall that N is the number of target regions. Therefore, each iteration of the algorithm takes $O(TN)$. The number of iterations over the greedy algorithm is $\frac{1}{\Delta}$. Then, the time complexity of the greedy Monte Carlo algorithm is $O(\frac{1}{\Delta}TN)$. Note that the values of $\frac{1}{\Delta}$, N, and T are small.

Table 3: Average localization error in open environment when a person moves in target region 1, $\bar{\epsilon}_i$ denotes average localization error for strategic area i.

Approach	$\bar{\epsilon}_1(m)$	$\bar{\epsilon}_2(m)$	$\bar{\epsilon}_3(m)$	$\bar{\epsilon}_4(m)$
All transmitters are turned on	1.7	1.9	5.8	0.6
Effective transmitters are turned off	3	5.3	6.4	1.6
Any pair of transmitters other than effective transmitters are turned off	2	1.7	4.8	0.61

Table 4: Average localization error when all transmitters are turned on and when using optimal scheduling in cluttered office, $\bar{\epsilon}_i$ denotes average localization error for strategic area i.

Approach	$\bar{\epsilon}_1(m)$	$\bar{\epsilon}_2(m)$	$\bar{\epsilon}_3(m)$	$\bar{\epsilon}_4(m)$
All transmitters are turned on	3.4	4.1	2.8	2.5
Optimal scheduling	4.4	5.8	3.7	3.4

Table 5: Average localization error when all transmitters are turned on and when using optimal scheduling in open environment, $\bar{\epsilon}_i$ denotes average localization error for strategic area i.

Approach	$\bar{\epsilon}_1(m)$	$\bar{\epsilon}_2(m)$	$\bar{\epsilon}_3(m)$	$\bar{\epsilon}_4(m)$
All transmitters are turned on	2.8	1.9	1.2	2.1
Optimal scheduling	4.3	4.7	4.1	5.7

6. EVALUATION

In this section, we evaluate our game theoretic formulation and solution with the help of experimental results. More specifically, we wish to determine the effectiveness of the solution to our optimization problem, C, that determines the probability of turning off the effective transmitters of each target region in each time slot. We determine the effectiveness of our solution by showing that, given the optimal strategy for the defender, C, the attacker is unable to determine people location with a high accuracy.

We conduct experiments in two different areas: an open environment, and a cluttered office. In this section, we first describe an attack scenario in these two areas and then

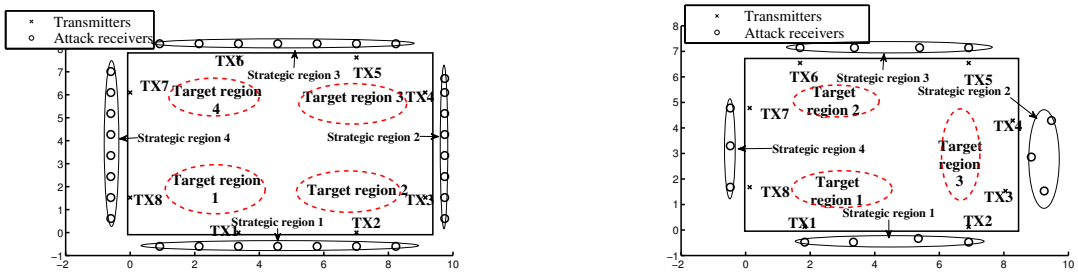

Figure 5: The experiment layout for open environment (a) and cluttered office (b).

present the evaluation of our game theoretic approach in terms of average localization error in these two areas.

6.1 Experiment layout

Open Environment: In the open environment, there are no objects or obstructions in the monitoring area. Figure 5(a) shows the layout of this experiment. In this figure, there are 8 transmitters, each an RF sensor node, that are deployed inside of a $70m^2$ area at the height of one meter from the floor. Also, there are 30 attack receivers that are placed in four heterogeneous strategic areas (see ellipse in Figure 5(a)) with r_{max} of 7, 8, 7, and 8 (these numbers of attack receivers are typical for localizing human inside perimeters [15]). The sensor nodes transmit on channels 11, 15, 18, 22 and 26 (multiple channels improve the accuracy of location determination [19]).

There are four target regions that represent bounded areas of movement during a day. To taken into account the heterogeneity of movements in time domain, we consider 3 time slots with different probability of movements in each target region. The dashed circles in Figure 5(a) determine the target regions. In our experiment, a single person moves in the target regions with the following probability matrix, P. Recall that $p_{j,t}$ represents the probability of movement for target region j in time slot t. Thus, the first column of matrix P, $(0.8, 0.2, 0, 0)$ represents a single person spending 80 percent of time in target region 1 and 20 percent of the time in target region 2 in time slot 1.

$$P = \begin{bmatrix} 0.8 & 0 & 0 \\ 0.2 & 0.4 & 0 \\ 0 & 0.6 & 0.3 \\ 0 & 0 & 0.7 \end{bmatrix}$$

Cluttered Office: This experiment is done in a cluttered area where there are several metallic obstructions such as desks, chairs, and monitors. In this experiment too, 8 transmitters are deployed inside of a $52m^2$ area at the height of one meter from the floor, as shown in Figure 5(b). The sensor nodes transmit on channels 11, 16, 21, and 26. Also, there are 14 attack receivers that are placed in four heterogeneous strategic areas with r_{max} of 4, 3, 4, and 3. In this experiment, one person moves in three target regions (see dashed circles in Figure 5(b)) and there are three time slots with the following probability matrix.

$$P = \begin{bmatrix} 0.8 & 0 & 0 \\ 0.2 & 0.2 & 0 \\ 0 & 0.8 & 1 \end{bmatrix}$$

As explained before, P represents the probability of movement.

In both experiments (open environment, and cluttered office), the sensor nodes composing the network are TI CC2531 USB dongle nodes [22]. While we only consider one person in our experiments, our framework can also work when multiple persons move in the monitored area. In this case, the amount of reward and penalty for a successful attack, $Re_a(j,t)$ and $Pe_d(j,t)$, depend on both the probability of movement and the number of moving people.

6.2 Experimental Results

To evaluate our framework, we first find the effective transmitters for each target region. As mentioned before, the effective transmitters for a target region are the minimum number of transmitters so that when these are turned off, the attacker is unable to detect movements in the target region. For example in Figure 5(a), transmitter 1 and 6 are the effective transmitters of target region 1.

Table 3 shows the localization error in open environment when a person moves in target region 1. In order to localize the moving person, we use the Multi-channel RTI approach proposed in [19] (using multiple channels increases the accuracy of localization). The first row shows the average localization error when all 8 transmitters are turned on and attack receivers are deployed in different strategic areas. The average localization error in this row shows that strategic areas corresponding to target region 1 are 1, 2, 4. Among these strategic areas, strategic area 4 has the maximum coverage. The second row of Table 3 shows the average localization error when the effective transmitters of target region 1 are turned off. This row shows that the average localization error increases between 1-3.5 meters by turning off transmitter 1 and transmitter 6 that are effective transmitters of target region 1. Note that the strategic area 3 is not suitable for target region 1, and turning off the effective transmitters of target region 1 does not change the average localization error for this strategic area. The third row of Table 3 shows the average localization error when we turn off any other pair of transmitters except transmitter 1 and transmitter 6. This row shows that the average localization error does not change much in comparison to that when we turn off the effective transmitters of target region 1.

We find the effective transmitters and corresponding strategic areas for each target region in the open environment and the cluttered office setting using the same reasoning as above. If we have more than one option for effective

transmitters of a target region, then we select the effective transmitters that have minimum overlap with the effective transmitters of other target regions. After finding the effective transmitters and corresponding strategic areas for each target region, we focus on an attack scenario where an attacker tries to determine the location of a moving person within a target region.

First, we find the optimal strategy of the defender, C, for the two scenarios (open environment and cluttered office). In both experiments, we set Δ and m to 0.001 and 1, respectively. Recall that Δ is the increment in the probability of turning off effective transmitters; and m is the number of target regions that defender is able to protect. We also set λ_a and λ_c to 1, 0.5 respectively. Recall λ_a is constant parameter for a successful attack and λ_c is the cost of adding one receiver. Our methods work for a wide-range of values of the above parameters. Here, we show results only for some specific values.

After finding the optimal strategy for the defender, C, which determines the probability of turning off the effective transmitters of each target region in each time slot, we randomly sample C to find a specific schedule for turning off the effective transmitters of each target region in each time slot. Given the optimal strategy for the defender, we evaluate the average localization error when the attack receivers are deployed in each strategic area.

Table 4 shows the average localization error for each strategic areas in the cluttered office scenario. The first row of the table shows the average localization error when all transmitters are turned on. The values in this row show that the attacker can detect the movement with minimum localization error of 2.5 meters from strategic location 4 when all transmitters are active in all time slots. The second row of this table shows the average localization error due to the optimal scheduling determined by our game theory framework for each strategic area. The values in the second row of Table 4 show that the minimum localization error for the attacker is 3.4 meters if the attacker deploys attack receivers in strategic area 4. Thus, the attacker's best strategy is to deploy attack receivers in strategic area 4. Table 4 shows that when the optimal scheduling policy determined by our game theoretic framework is used, even if the attacker plays its best strategy, the localization error increases by 36% in a $52m^2$ area. Very importantly, we expect the difference in localization errors to increase with the increase in the size of the monitored area.

Table 5 shows the average localization error in the open environment that is bigger in size than the cluttered office. This table shows that the minimum localization error when all transmitters are turned on, is 1.2 meter and it occurs in strategic location 3. Since there is no obstruction or object in the open environment and because of using more attack receivers in each strategic area, the localization error here is less than that in the cluttered office. However, when using the optimal strategy determined by our game theoretic framework, the minimum localization error increases by 240% (from 1.2 to 4.1 in strategic area 3). As we expect, the difference in localization errors is increased by increasing the size of the monitored area.

So far, we have compared the localization error due to the optimal scheduling determined by our game theory framework with that when all transmitters are active in all time slots. Essentially, by turning off the effective transmitters according to our optimal schedule, we reduce the number of transmitters and consequently, increase the localization error.

Table 6: Average localization error using random strategy in open environment and cluttered office

	Average localization error(m)	
	Open	Office
Strategic area 1	3	3.6
Strategic area 2	3.5	4.5
Strategic area 3	2.6	2.9
Strategic area 4	4	2.6

Table 7: The minimum percentage of increase in the localization error in open environment and cluttered office using random and optimal strategies.

	The minimum percentage of increase in the localization error	
	Open	Office
Random	116%	4%
Optimal	240%	36%

To demonstrate the effectiveness of our game theory framework, we measure the localization error when the defender uses a simple *random* strategy for turning off the effective transmitters of each target region in each time slot. Table 6 shows the average localization error for each strategic area using a random strategy for the defender. As shown in this table, the minimum localization error for the attacker in the cluttered office is 2.6 meters if the attacker deploys attack receivers in strategic area 4. This implies that the percentage of increase in the localization error decreases from 36% when using our optimal strategy to 4% when using the random strategy. For the open environment, the minimum localization error decreases from 4.1 when using the optimal strategy to 2.6 when using the random strategy. I.e., the percentage of increase in the localization error decreases from 240% to 116%. Table 7 shows the minimum percentage of increase in localization error using the optimal strategy and the random strategy in the open environment and the cluttered office. This table shows that the optimal strategy preforms better than the random strategy in both experiments. We believe that the random strategy will preform even worse than the optimal strategy with the increase in the number of target regions, strategic areas, and transmitters.

7. PRACTICAL CONSIDERATIONS

In this section, we briefly discuss the practicality of our game theoretic approach and solution.

First, while we have designed and evaluated our methods with specific utility and cost functions, our approach allows the defender to determine its strategy for other utility and cost functions considering the capabilities of the defender as well as the attacker. Thus, our formulation can be used for a variety of adversarial prowess and behavior. Second, the functionality to change wireless transmitters can be de-

ployed in existing enterprise networks by implementing the transmitter schedule on a *controller node* that control wireless access points [18]. Third, a controller, having complete knowledge of the schedule, can also transfer the state of active "associations" on the current access point to the next one being scheduled over a wired high speed network (e.g., Ethernet). This state also includes any keys associated with the secure transmission between the clients inside the monitored area and the current access point. Thus, the choice of the actual value of the time slot between transmitter changes would depend on the overhead of this state transfer. If we choose a high value for the time slot, we minimize this overhead, however, we also disregard the heterogeneity in human movements during the time. Based on our experiences, we recommend a value of tens of minutes for the time slot. The state transfer across access points every tens of minutes over a wired network, will not result in any significant overhead. The transmitters of the defender must use same service set identifier (SSID) so that the change of transmitters is transparent to the nodes associated with them. Even with the centrality of the controller node, there is a small chance of packet loss during the state transfer across access points. However, we expect this loss to be not significant in comparison to other wireless loss.

8. CONCLUSION

We investigated an attack on location privacy where the location of people moving inside a private area can be inferred using the radio characteristics of wireless links that are leaked by legitimate transmitters deployed inside the private area. We modeled the radio network leakage attack using a Stackelberg game and used a greedy method to obtain the optimal strategy for the defender. Our experimental results showed that our game theoretic solution significantly reduces the chance of an attacker finding the location of people inside a perimeter. In the future, we will implement our framework in a WiFi network testbed inside our department to further study and demonstrate the practicality of our approach. We will also measure any performance degradation experienced by genuine receivers inside the building as a result of scheduling transmissions through different access points.

9. REFERENCES

[1] P. Bahl and V. N. Padmanabhan, "RADAR: An In-Building RF-based User Location and Tracking System," *IEEE INFOCOM*, 2000.

[2] J. Wilson and N. Patwari, "Radio tomographic imaging with wireless networks," *IEEE Transactions on Mobile Computing*, 2010.

[3] M. Youssef and M. Mah and A. Agrawala, "Challenges: Device-free Passive Localization for Wireless Environments," *ACM MobiCom*, 2007.

[4] Z. Han and N. Marina and M. Debba and A. HjÃÿrungnes, "Physical Layer Security Game: How to Date a Girl with Her Boyfriend on the Same Table," in *IEEE GameNets*, 2009.

[5] G. Brown and M. Carlyle and J. Salmeron and K. Wood , " Defending Critical Infrastructure," *Interfaces*, 2006.

[6] P. Paruchuri and J. P. Pearce and M. Tambe and F. OrdÃşÃśez and S. Kraus, "An efficient heuristic approach for security against multiple adversaries," *Autonomous Agents and Multiagent Systems*, 2007.

[7] C. Kiekintveld and J. Marecki and M. Tambe, "Approximation methods for infinite Bayesian Stackelberg games: modeling distributional payoff uncertainty," *Autonomous Agents and Multiagent Systems*, 2011.

[8] M. Tambe., "Security and Game Theory," *Cambridge University Press*, 2011.

[9] M. Manshaei and Q. Zhu and T. Alpcan and T. Basar and J-P. Hubaux, "Game Theory Meets Network Security and Privacy," *ACM Computing Surveys*, 2013.

[10] T. Jiang and J. Wang and Y. Hu, "Preserving location privacy in wireless LANs," *MobiSys*, 2007.

[11] F. Adib and D. Katabi, "See through walls with wifi!," *SIGCOMM*, 2013.

[12] F. Adib and Z. Kabelac and D. Katabi and R. C. Miller., "3d tracking via body radio reflections," *NSDI*, 2014.

[13] Q. Pu and S. Gupta and S. Gollakota and S. Patel, "Whole-home gesture recognition using wireless signals," *MobiCom*, 2013.

[14] K. Rasmussen and C. Srdjan, "Location privacy of distance bounding protocols," *Computer and communications security*, 2008.

[15] A. Banerjee, D. Maas, M. Bocca, N. Patwari, and S. Kasera, "Violating Privacy Through Walls by Passive Monitoring of Radio Windows," *Wisec*, 2014.

[16] Y. S. Kim, P. Tague, H. Lee, and H. Kim, "Carving Secure Wi-Fi Zones with Defensive Jamming," *ASIACCS*, 2012.

[17] M. Gruteser and D. Grunwald, " Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis," *Mobile Networks and Applications*, 2005.

[18] Cisco Wireless Controllers, http://www.cisco.com/en/US/products/hw /wireless/products_category_buyers_guide.html# controllers.

[19] M. B. O. Kaltiokallio and N. Patwari, "Enhancing the accuracy of radio tomographic imaging using channel diversity," in *IEEE MASS*, 2012.

[20] M. Khaledi and S. Kasera and N. Patwari and M. Bocca, "Energy Efficient Radio Tomographic Imaging," in *IEEE SECON*, 2014.

[21] M. Khaledi and M. Khaledi and H. Rabiee, "Fuzzy mobility analyzer: A framework for evaluating mobility models in mobile ad-hoc networks," in *IEEE WCNC*, 2010.

[22] Texas Instruments. A USB-enabled system-on-chip solution for 2.4 GHz IEEE 802.15.4 and ZigBee applications.