

# Preserving Location Privacy in Wireless LANs

Tao Jiang  
University of Maryland  
College Park, MD 20742  
tjiang@umd.edu

Helen J. Wang  
Microsoft Research  
Redmond, WA 98052  
helenw@microsoft.com

Yih-Chun Hu  
UIUC  
Urbana, IL 61081  
yihchun@crhc.uiuc.edu

## ABSTRACT

The broadcast and tetherless nature of wireless networks and the widespread deployment of Wi-Fi hotspots makes it easy to remotely locate a user by observing her wireless signals. Location is private information and can be used by malicious individuals for black-mail, stalking, and other privacy violations. In this paper, we analyze the problem of location privacy in wireless networks and present a protocol for improving location privacy. Our basic approach is to obfuscate several types of privacy-compromising information revealed by a mobile node, including sender identity, time of transmission, and signal strength. Our design is driven by real-system implementation and field experiments along with analysis and simulations. Our system allows users to choose the level of privacy they desire, thereby increasing the performance of less private users (while not sacrificing private users' privacy at the same time). We evaluated our system based on real-life mobility data and wireless LAN coverage. Our results show that a user of our system can be indistinguishable from a thousand users in the same coverage area.

## Categories and Subject Descriptors

C.2 [Computer-Communication Networks]: Miscellaneous

## General Terms

Measurement, Design, Experimentation, Security

## Keywords

Privacy, Localization, 802.11

## 1. INTRODUCTION

In recent years, we have witnessed the pervasive deployment of Wi-Fi hotspots (e.g. [1, 5, 27]) which has empowered people to communicate and compute almost anywhere and anytime. The wireless medium and its broadcast nature also makes it much easier to compromise a user's privacy: an attacker that sniffs packets sent over the air can easily determine a user's communication pattern,

the contents of her communications (if unencrypted), or even to infer a user's physical location, which can be a threat to her physical security. For the latter problem of location determination, previous research [2, 23] has shown that precise positioning of a mobile node is possible: in Ladd et al.'s scheme [23], the received signal strength of the mobile node at different access points can map the node to within 1 meter range with at most 50% error. In wireless networks, traffic analysis and confidentiality can be protected through traditional approaches, such as encryption and traffic mixing [6, 25]; however, solutions for protecting a user's physical location information are scarce and lacking. In this paper, we treat the problem of location privacy.

Our basic approach to location privacy is to obfuscate privacy-compromising information that is leaked in the course of wireless communications. This leakage occurs through five sources: time, location, sender node identity (such as MAC address), receiver node identity, and content. While content can be protected by encryption and receiver identity can be protected by going through a MIX-net [6] or Crowd [25], the broadcast nature of the wireless media inevitably exposes the first three dimensions which can be used to infer the user location. We obfuscate these three dimensions as follows:

- Anonymize the user or node identity with frequently changing pseudonyms. While the analog characteristic of a wireless card may be fingerprinted and serves as a form of identity, the feasibility of RF fingerprinting of noisy wireless setting has yet to be proven. Furthermore, RF fingerprinting requires costly hardware [13], so using RF fingerprinting for user tracking would require wide deployment at a high cost to attackers.
- Unlink different pseudonyms of the same user with silent periods between different pseudonyms.
- Increase the entropy of the attackers' location estimation by reducing the precision of location algorithms; mobile nodes in our system reduce their transmission range through power control to reduce the number of nodes that can collaborate to determine the nodes' location.

While some aspects of these ideas have appeared in research literature [16, 4, 20, 21], in our work, we aim to evaluate and quantify the efficacy of these mechanisms along with their proper parameter configurations for real wireless systems by using a combination of real-system experimentation, simulation, and analysis.

In this paper, we analyze the achieved location privacy of a mobile node using the metric of *privacy entropy*. To obfuscate the transmission time, we introduce the *opportunistic* silent period, which takes place during the idle time between users' communication sessions. We further developed a methodology for deriving the

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

MobiSys'07, June 11–13, 2007, San Juan, Puerto Rico, USA.  
Copyright 2007 ACM 978-1-59593-614-1/07/0006 ...\$5.00.

duration of the silent period to satisfy certain privacy requirements, given the mobility pattern within a service area. We conducted a case study evaluating the impact of silent period on privacy using the mobility pattern of Seattle buses. We find that taking the optimal silent period, the system offers 8 bits of entropy for privacy protection; that is, after one silent period, the user is indistinguishable from  $2^8$  other users in the service area of the wireless network. To reduce the precision of location estimation, we devised a *silent* transmit power control algorithm based on our field measurements from both indoor and outdoor environments. We find that the precision of localization schemes can be reduced by a factor of 12 after applying our transmit power algorithm, which is equivalent to increasing privacy entropy by 3.7 bits. In addition, we propose *user-friendly operations* in privacy protected systems that incur minimal disruptions to user communications. This allows the systems to increase entropy for privacy-sensitive communications without reducing the performance of privacy-insensitive communications. To verify the practicality of our approach, we implemented our privacy protection mechanisms for a Netgear WG111U USB wireless card by extending its driver.

It may seem that location privacy is inherently at conflict with wireless service provisioning and popular location-based services. Indeed, some wireless service billing and authorization schemes require the identity of a user or her mobile station, and location-based services must first infer the user location before providing services based on user location. However, we argue that any such limitations are particular to the *implementation* of these services. A user need not reveal her identity to receive wireless service; telephone networks already have cash-purchased calling cards for anonymous authorization. Wireless service provision can take the same approach of separating billing from service provision and allowing billing to be anonymous, as in [20]. For location-based services, a mobile station can calculate its own current location, and only give this information to location-based services trusted by the user. Therefore, it is feasible to give users the choice of privacy in wireless networks and location-based services.

The rest of the paper is organized as follows. We first review existing RF-based localization systems and previous solutions for protecting location privacy in Section 2. We define the attacker model in Section 3. Section 4 gives the definition of privacy entropy. In Section 5, we present our detailed design for achieving location privacy including frequently changing pseudonyms, silent period and reducing location precision; our design was driven by real system experimentation, field measurement and simulation analyses. In Section 6, we describe how our location privacy-enabled mobile nodes and service providers operate. Finally, we conclude our paper and discuss remaining challenges in Section 7.

## 2. RELATED WORK

### 2.1 Location technologies

Various approaches have been proposed to estimate the location of mobile users in wireless networks. In this paper we only consider RF-based localization systems, because RF-based localization systems do not require extra infrastructure and specialized hardware and technologies that are severely limited. For instance, localization systems based on time of arrival (TOA) require multiple antennas and a very fine-grained timer. Furthermore, TOA techniques are of limited usefulness in urban environments due to multipath interference, whereas RF-based localization is effective in both indoor and outdoor scenarios.

Existing RF-based localization systems (such as [2, 23, 7]) are able to accurately locate users using already deployed access points

(APs) in WLANs, under the condition that three or more APs are in the communication range of users. Bahl and Padmanabhan [2] and Ladd et al. [23]’s experiments in normal office buildings determine location on the order of meters. For instance, Ladd et al. [23] achieve accuracy of better than 1 meter over 50% of the time. Cheng et al. [7] studied metropolitan-scale Wi-Fi location determination using available 802.11 APs in cities. Their experimental results show median accuracy of 15–30m in large outdoor areas. These systems work in two phases: a training phase and a positioning phase. The training phase uses a procedure similar to “war-driving” to obtain a large amount of signal data. The training data is then used to build a “radio map”. In the positioning phase, the signal data of the target is recorded by all APs that can hear the target’s transmissions. This data is then compared to the radio map to estimate the target’s location.

### 2.2 Application-Level Location Privacy

The location privacy problem is of great interest in location-based services because location data needs to be revealed to external services. To retain location privacy, users can use their own sensors to calculate their own location (e.g. Cricket [18]). Such systems preserve location privacy when users do not emit any detectable signals. However, in the course of transmitting their location or receiving the location-based service, mobile nodes will transmit wireless network packets, and these systems do not protect against privacy compromise inherent in such transmissions.

Gruteser and Grunwald [15] discuss schemes in which the spatial and temporal accuracy of location information is reduced such that at least  $k$  users are indistinguishable. The IETF *Geopriv* working group [12] has been chartered to design protocols and APIs that consider the privacy and security issues inherent in the transfer of high resolution location information to external services and the storage of such information at location servers. This paper differs from the work of Gruteser and Grunwald [15] and *Geopriv* [12] in that they target location information provided by applications, whereas we examine the privacy of location information that can be inferred from the wireless transmissions of network users.

### 2.3 Network-Level Location Privacy

Solutions for location privacy risks have been proposed by several research groups (e.g. [16, 4, 20, 21, 19]). All of these solutions propose the use of frequently changing user pseudonyms. He et al. [19] concentrates on the use of blind signatures to provide for the anonymous authentication of new pseudonyms. Anonymous authentication is only a small part in protecting location privacy. Other issues we address in this paper include obfuscating sender identity, time of transmission and signal strength.

Gruteser and Grunwald [16] examines the effect of pseudonym changes on locating users based on a wireless trace that contains the AP association of users. They do not, however, consider attacks correlating different pseudonyms of the same user based on mobility pattern of users. For example, if at time  $t_0$ , we know that a user moves along a direction at speed  $v$ , and later on at time  $t$  we see a packet along the same direction of distance  $v(t - t_0)$ , then we know most likely this packet is from the same user. To reduce this risk, Hu and Wang [20] and Huang et al. [21] introduce *silent periods*, where privacy-sensitive users intentionally do not transmit, in order to reduce the effectiveness of such correlations. Our work, building on top of [20] and [21], uses an *opportunistic* silent period. We further provide a methodology for calculating the optimal silent period given a mobility pattern. We give an example of such a calculation based on a case study using actual mobility from the Seattle-area bus system. Our previous work [20] brought up

the previously ignored problem of location privacy and pointed out future directions for preserving location privacy. In this work, we extend those solutions and present the protocols in detail. Furthermore, we design an operational model for location privacy preserving systems, and introduce the privacy entropy metric to measure the degree of privacy our system provides.

Mix zones [4] reduce the correlation between two pseudonyms of the same user. Users are not allowed to transmit in the mix zone; these mix zones are essentially spatial versions of the silent period. However, the mix zone scheme requires each node to know its exact location. Furthermore, the constrained communications area will reduce participation by privacy-insensitive nodes.

Reducing the precision of a location estimation scheme increases the uncertainty in determining a device’s location since many other devices are also in the same course-grained location. Görlach et al. [14] suggests that users can hinder RF-based localization techniques by distributing their data on pseudo-randomly chosen channel. An attacker would then be less able to distinguish, and thus localize, signals transmitted in this way. However, this solution assumes that the access point operator is trusted, whereas one of our objectives in this paper is to protect a user’s location privacy even when the access points cannot be trusted (e.g., communication logs on the APs are compromised). Rather than using channel-hopping to decorrelate device transmissions, we reduce transmission power to decrease the number of APs in range, so that the localization algorithms in [2] cannot succeed.

## 2.4 RF Fingerprinting

As we discussed in the previous subsection, anonymity is a prerequisite of location privacy, without which first-hop access points could easily pinpoint the location of the identified user using localization algorithms mentioned above. RF fingerprinting [17, 13] could potentially be used to identify a wireless card by analyzing imperfections in the analog components to determine whether or not two packets were sent from the same transmitter. For example, imperfections in the oscillator will cause the carrier frequency to deviate from the specified frequency by an amount unique to each transmitter.

Nevertheless, the literature has yet to establish the feasibility of RF fingerprinting. While Gerdes et al. [13] have demonstrated that it is possible to fingerprint an Ethernet device, the noise in the wireless networks would pose significant challenges and the characteristics of fingerprints are likely to change due to multipath propagation, fading, temperature variation, battery condition, Doppler shift and device aging. Because of the high variability introduced by wireless environments, and the similarity of RF fingerprints between wireless cards of the same model, the cost of building an RF fingerprinting-enabled network is very high. First, clearly distinguishing between cards having similar fingerprints requires a high speed and high resolution ADC (Analog-to-Digital Converter) in the receivers, which is expensive. In fact, Gerdes et al. [13] used an oscilloscope to sample received signals. Secondly, the training phase to build RF fingerprinting profiles requires a long time (on the order of a couple of hours), and such protocols must be updated frequently. This cannot be easily done in mobile and privacy sensitive environments.

Our privacy schemes raise the bar significantly for attackers localizing mobile users. Attackers must resort to RF fingerprinting which requires additional hardware and expensive deployment of such hardware equipment.

Furthermore, although it is not possible to duplicate a specific RF fingerprint, it is possible for privacy-sensitive devices to hide their RF fingerprints intentionally. For instance, most RF fingerprint-

ing identification schemes analyze the transient signals transmitted when devices are being turned on. By intentionally adding strong noise during the transient period, such transient signals can be made difficult to distinguish. Further research on such concealing of RF signals for privacy is an important piece of future work.

## 3. ATTACKER MODEL

In wireless networks, the problems of confidentiality, authenticity, authentication and accessibility are also very important and challenging. However, they are beyond the scope of this paper. We assume that certain mechanisms have been applied to protect these aspects of security.

The attackers of our interest are those that aim to expose the location information of mobile users in wireless networks. There are *silent* attackers and *exposed* attackers.

Silent attackers are sniffers that do not emit any signals, but only listen and localize mobile users. Silent attackers are strongest when they are densely scattered throughout wireless service areas, in which case they are capable of precisely locating a mobile user. Such an attacker would need to have substantial resources; for example, it could be a government or a competing service provider.

In contrast, exposed attackers are network providers that must provide wireless services in addition to obtaining a mobile node location. Although network providers themselves could be trustworthy, a provider may accidentally leak privacy-sensitive information; such leakage is now rampant for other types of private information, and can be due to malicious employees, hackers, theft, or lack of sufficient review and oversight.

Among exposed attackers, we further distinguish *active* attackers and *passive* attackers. Active attackers refer to network providers that dynamically adjust their base stations’ transmission power to react to the network load or to more precisely locate a user. Passive attackers are network providers that do not change base station behavior.

## 4. PRIVACY ENTROPY

The concept of *entropy* was first introduced in Information Theory [26] to quantify the uncertainty one has before an experiment. The higher the privacy entropy value is, the more uncertain attackers will be of their user location inference, and hence the better privacy protection our system offers. Given an attacker and the set of all mobile users  $\mathcal{U}$ , let  $\lambda$  be the observation of the attacker about the user at some location  $\mathcal{L}$ . Given observation  $\lambda$ , the attacker computes a probability distribution  $P$  over users  $u \in \mathcal{U}$ . We define the *privacy entropy* of this observation  $\lambda$  to be

$$H_\lambda = - \sum_{u \in \mathcal{U}} P_{u,\lambda} \log_2(P_{u,\lambda}). \quad (1)$$

We could interpret the privacy entropy as the number of bits of additional information that the attacker needs to definitively identify the user  $u$  observed with  $\lambda$  at the location  $\mathcal{L}$ . Obviously, if one user is assigned a probability of 1, then the attacker already has enough information to identify the user. To determine the privacy entropy, we need to determine the probability distribution calculated by the attacker. In Section 5, we show how this might be calculated in a realistic mobile system.

## 5. ACHIEVING LOCATION PRIVACY

In this section, we present our location privacy solutions in detail. Our approach obfuscates three sources of location privacy leakage: sender identity (Subsection 5.1), time of transmission (Subsection 5.2), and signal strength (Subsection 5.3). In order to closely

relate our design to real systems, we focus our description on a protocol built around an 802.11 WLAN, but our techniques can generalize to other types of wireless networks, such as cellular networks.

## 5.1 Pseudonym

Anonymity is a prerequisite for location privacy; without anonymity, an attacker can easily link a user to different locations. To prevent an attacker from using user identity for tracking, users must use frequently changing pseudonyms for communications. In an 802.11 WLAN, MAC and IP addresses are user identities that must be protected by using pseudonyms. However, changing pseudonyms creates several design problems.

One important factor in choosing pseudonyms is to avoid address collisions with other network nodes. Because there are only 48 bits in a MAC address, randomly chosen addresses have a high probability of collision in networks as small as  $2^{24}$  due to the birthday paradox. In our design, MAC addresses are assigned by access points. When a user comes within transmission range of an access point and wants to connect to it, the user first sends out a message to request a MAC address. This request must be sent from a MAC address, but using the interface’s unique MAC address would reveal user identity, and using a randomly chosen MAC address may conflict with an established user. In our system, the user uses a well-known address called the *join address* to avoid such conflicts, and distinguish between multiple simultaneous requests through the use of a 128-bit nonce.

When the AP receives a MAC address assignment request from the join address, it chooses an unused address from its MAC address pool and sends a reply that includes both the nonce from the request packet and the assigned MAC address. If the underlying physical layer requires acknowledgment for unicast packets (as does 802.11), this reply packet is sent as a link-layer broadcast packet to avoid an acknowledgement implosion. When a node receives such a reply packet, it checks to see if the nonce corresponds to a request that it has sent, and if so, it begins to use the MAC address assigned by the reply packet. The process of assigning MAC addresses is depicted in Figure 1.

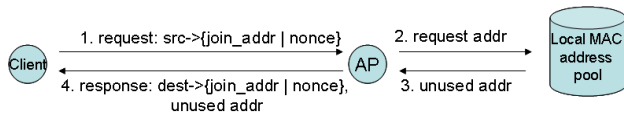


Figure 1: MAC address selection

Another network-layer identifier is the IP address. IP addresses could be assigned through Statistically Unique Cryptographically Verifiable IPv6 addresses [24]. Alternatively, since base stations already provide unique MAC addresses, they can also assign IP addresses from a pool as part of this protocol. Unlike network-layer identifiers such as MAC and IP addresses, we do not need to extract and obfuscate application layer user identities such as e-mail usernames because such identities are transmitted as transport layer payload content which can be protected through encryption.

Changing the MAC and IP addresses may cause disruptions when the user associates with a new AP. Our system only allows address changes just before the start of a new association (The detailed operating mode of mobile users is discussed in Sec. 6.). To minimize the disruption of communications, users do not change their addresses during inter-AP handoff as long as they stay associated. Another problem with IP address changes is that sources cannot easily communicate with such a node. Previous work [20]

addresses this problem through the use of trusted anonymous bulletin boards, together with cryptographic mechanisms to protect user identity.

When pseudonyms change between two associations, the attacker cannot trivially identify a user at a particular location. Without any additional information, the privacy entropy  $H$  is equal to  $\log_2(N)$ , where  $N$  is the total number of users in the network. However, when an attacker accumulates the location information for all packets sent in the network, the attacker can attempt to correlate different pseudonyms with the same user. For example, if a user was moving along a road at some speed, then a packet further along the same road is more likely sent by that user. In order to reduce such correlations, we use a *silent period* to unlink communications under different pseudonyms of the same user.

## 5.2 Opportunistic Silent Period

During a silent period, a user does not send any wireless transmissions. A silent period allows a sender to “mix” in with other possible nodes (through natural node mobility). The effectiveness of silent periods depends heavily on user density: when the user density is low, such as when a user is at home, an attacker can easily identify and locate the user even if the user frequently changes her mobile node’s pseudonym and uses a long silent period. Therefore, location privacy systems are most effective at public places with high user density, such as coffee shops and airports.

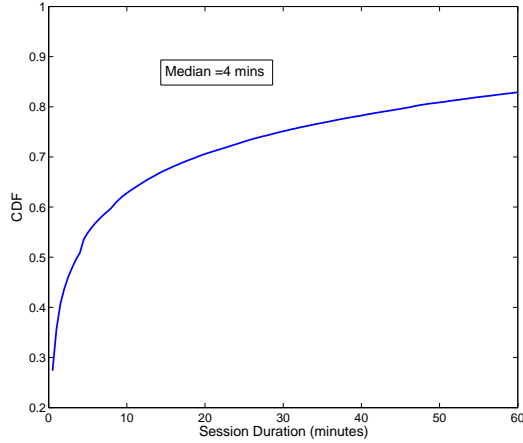
Forced silent periods can disrupt communications; for example, TCP sessions will be broken, and real-time communications cannot continue. To minimize disruptions, we introduce the concept of an *opportunistic* silent period, which takes place during the idle time between users’ communications. In an opportunistic silent period, the user’s machine detects that it has not transmitted for a period in excess of the silent period, and uses that time to change pseudonyms. This decision can result in a changed pseudonym either as soon as sufficient time has elapsed, or when the user next wishes to transmit. Opportunistic silent periods mitigate the impact of silent periods on user communications.

We analyzed the WLAN trace data at Dartmouth College from CRAWDAD [9]: 50% of the sessions have a duration of 4 minutes or less (Figure 2); more than 50% of inter-session times are longer than 10 minutes, as shown in Figure 3. This data shows that opportunistic silent periods are quite suitable for WLANs.

### 5.2.1 Methodology for Choosing a Silent Period

This section describes the methodology for determining a silent period that achieves certain privacy requirements. As mentioned earlier, the efficacy of silent period depends on user density. Therefore, we take the mobility pattern within a service area as input to our derivation. Mobility pattern data consists of triples  $\langle \text{time}, \text{pseudonym}, \text{location} \rangle$ . Such data can be easily collected and provided by third parties, and correctness can be verified by cross-checking data from multiple providers.

We compute the privacy entropy as follows. In the training phase, we derive the probability distribution given a fixed observation location  $\mathcal{L}_{ob}$ . Given the mobility pattern of the service area (the training set), we find all the users which pass  $\mathcal{L}_{ob}$ ; and denote the set of such users as  $K$ . For each time  $t_1$  that a user  $i$  is observed at  $\mathcal{L}_{ob}$ , we trace the training data backwards to time  $t_0 = t_1 - \Delta t$  (for a fixed  $\Delta t$ ), and record the location  $\mathcal{L}_i$  where user  $i$  is at  $t_0$ . By tracing backwards all users that pass the observation location, we obtain a set of  $|K|$  locations  $LOC(\Delta t) = \{\mathcal{L}_i | i \in K\}$ , where some elements in the set may be identical. Given a specific location  $\mathcal{L}_i$  from  $LOC(\Delta t)$ , we define  $\kappa_i$  to be the number of elements in  $LOC(\Delta t)$  which is the same as  $\mathcal{L}_i$ .  $\kappa_i$  represents the number



**Figure 2: CDF of session duration from Dartmouth campus-wide WLAN trace**

of users in the training set that travel from  $\mathcal{L}_i$  to  $\mathcal{L}_{ob}$  in time  $\Delta t$ . Therefore if the time interval is fixed as  $\Delta t$  and a user is observed at  $\mathcal{L}_{ob}$  at time  $t_1$ , the conditional probability that this user was at  $\mathcal{L}_i$  at  $t_0$  is

$$p_i(\Delta t) = \frac{\kappa_i}{|K|}. \quad (2)$$

This conditional probability represents how likely a user was in  $\mathcal{L}_i$   $\Delta t$  time ago, given it is observed at  $\mathcal{L}_{ob}$ .

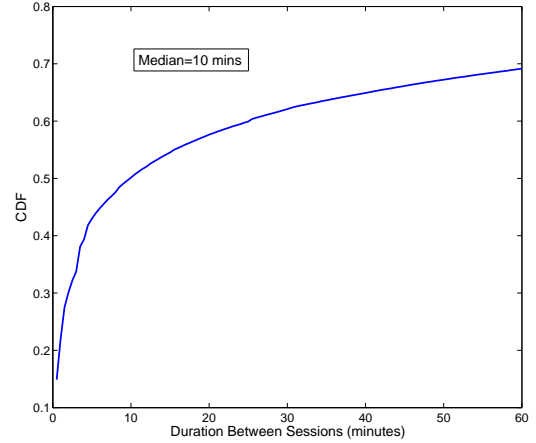
In the test phase, we use  $p_i(\Delta t)$  to compute the privacy entropy. Suppose the silent period is in the range of  $[T^{min}, T^{max}]$ . Whenever a new pseudonym is observed in  $\mathcal{L}_{ob}$  at time  $t$ , we define  $M$  as the set of the *candidate* pseudonyms from time  $t - T^{max}$  to  $t - T^{min}$  that might be linked to this new pseudonym. Suppose  $i$  is one of the candidate pseudonyms, which is in  $\mathcal{L}_i$  at time  $t - \Delta t_i$ ,  $\Delta t_i \in [T^{min}, T^{max}]$ . Then the probability that  $i$  is linked to the new pseudonym among these candidates is

$$P_{i,(\mathcal{L}_i, \mathcal{L}_{ob})} = \frac{p_i(\Delta t_i)}{\sum_{m \in M} p_m(\Delta t_m)}, \quad (3)$$

where  $P_{i,(\mathcal{L}_i, \mathcal{L}_{ob})}$  is the probability distribution used for privacy entropy. Therefore we could calculate the privacy entropy of a user in location  $\mathcal{L}_{ob}$  according to Equation (1). In addition to location information  $(\mathcal{L}_i, \mathcal{L}_{ob})$ , the observation  $\lambda$  in Equation (1) can include additional information such as speed and direction of movement, which improves the accuracy of the location inference. In the following case study on bus data, we consider location and velocity information.

The above calculation considers the worst-case scenario where the attacker has the complete mobility pattern data. When the attacker does not have complete data, such as when mobility pattern data is collected from a privacy-enabled service area, our scheme achieves even higher privacy levels.

Our goal is to choose a silent period that maximizes the privacy entropy. Previous work shows that silent periods must be randomized [20]; otherwise, if an attacker sees two pseudonyms used exactly  $t$  seconds apart (where  $t$  is the silent period) then he will know that those two pseudonyms belong to the same user with high probability. We use a random silent period of  $T_d + T_r$ , where  $T_d$  is deterministic and  $T_r$  is drawn from a uniform distribution between



**Figure 3: CDF of Duration between Sessions from Dartmouth campus-wide WLAN trace**

0 and  $T_r^{max}$ . Thus  $T^{min} = T_d$  and  $T^{max} = T_d + T_r^{max}$ . The derived silent period is an upper bound of the best possible privacy.

### 5.2.2 Case Study on Bus Mobility Data

In this section, we give a case study on how to derive silent period using the above methodology. Here, we use the mobility data of Seattle bus system from the BusView system [10]. We chose the bus data because it consists of both a realistic mobility pattern and accurate location information. To obtain such data in WLANs requires a large number of users and for each user to be equipped with a GPS system. Due to our limited resources, we used the bus data as an alternative. Though the results are definitely different from those in WLANs, we will show that they provide very valuable insights on choosing the optimal silent period.

We divided the bus data into a 5-day training set and an 8-hour test set. We quantized the time in our data to 30 second intervals and the area into square sections 300 feet on each side. Speed is quantized into bins aligned on 5mph boundaries and movement direction into 8 equally-sized slices. We chose an arbitrary area section as the observation area ( $\mathcal{L}_{ob}$ ). When a bus enters the observation area  $\mathcal{L}_{ob}$  at time  $t$ , we consider it to have started using a new pseudonym. If the length of the silent period is uniformly distributed on  $[T_d, T_d + T_r^{max}]$ , then the candidate buses which can be linked to the new pseudonym must have last been used in the time interval  $[t - T_d - T_r^{max}, t - T_d]$ . Given  $P_{i,(\mathcal{L}_i, \mathcal{L}_{ob})}$  of each of these candidates  $i$ , we calculate the privacy entropy of the new pseudonym. Because the buses are not users of a wireless data network, we do not have actual communication patterns or silent period selections, so for the purposes of this experiment, we first chose a communication schedule for each bus, based on  $T_d$  and  $T_r$ , and a communication time for each session chosen from a uniform distribution with a mean of 10 minutes. Therefore, only buses which stop one of their communication sessions during the interval  $[t - T_d - T_r^{max}, t - T_d]$  can be considered as candidate nodes.

Figure 4 shows the relationship between privacy entropy and the length of the silent period. The x-axis is the deterministic silent period  $T_d$  and each curve shows a fixed range for the random silent period  $T_r$ . Figure 4 shows that the privacy entropy reaches a maximum when  $T_d$  is around 20 minutes, independent of  $T_r$ . In particular, when  $T_r$  is 4 minutes, the system achieves its maximum

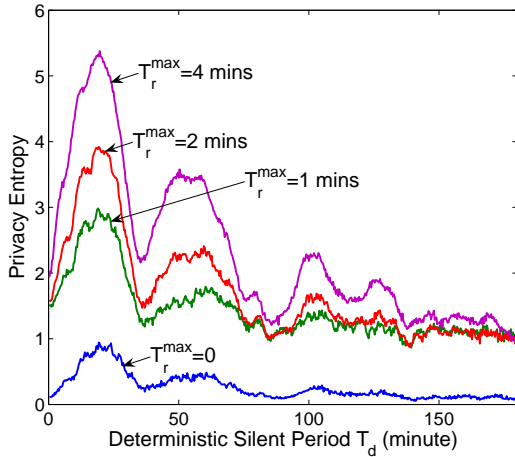


Figure 4: Privacy Entropy vs. Deterministic Silent Period

entropy  $\mathcal{H} = 5.38$  with a  $T_d$  of 19 minutes 20 seconds. When  $T_d$  is small, increasing  $T_d$  increases the entropy. However, this trend does not continue with increasing  $T_d$ . Increasing the silent period increases the fraction of buses that are in a silent period, so fewer buses transit from communicating to silence in a particular time interval. Therefore entropy decreases after it reaches a maximum point. We also observe that entropy is periodic, rather than monotonically increasing or decreasing. This is because a single bus is generally scheduled to periodically service a route for the entire day. The figure also shows that privacy entropy is monotonically increasing with increasing  $T_r$ . This is because by increasing the random silent period, the length of the silent period interval increases, so it includes more candidate buses.

To determine an optimal value for  $T_r$ , we fixed the value of the deterministic part of the silent period  $T_d$  to the optimal value of 19 minutes 20 seconds. We then plot the entropy against  $T_r^{max}$  in Figure 5. The figure shows that before  $T_r^{max}$  reaches 12 minutes,

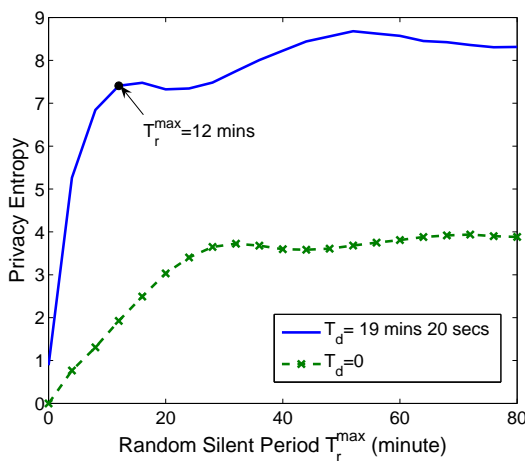


Figure 5: Privacy Entropy vs. Random Silent Period

the privacy entropy increases quickly, but after it crosses 12 minutes, the rate of increase drops sharply. To minimize the silent periods

while retaining good location privacy, we choose  $T_r^{max}$  close to but not greater than 12 minutes. We also plot the entropy against  $T_r^{max}$  when  $T_d = 0$  in Figure 5. The maximum entropy is only around 3.5 because with  $T_d = 0$ , because the target user may select silent period very close to 0. In this case, there are very few candidates, so the entropy is very low. Therefore, the system must set a lower bound  $T_d > 0$  for the silent period.

### 5.2.3 Summary

In this subsection, we provided a methodology for calculating the optimal silent period. This optimal value gives an upper bound on the necessary silent period; that is, the system cannot achieve better privacy even when using a longer silent period. In real systems, the selection of silent period depends on the tradeoff between service quality and privacy. A system requiring high privacy chooses the optimal silent period and sacrifices its service quality by introducing long communication disruptions, while a system requiring high communication quality may choose a shorter silent period.

## 5.3 Location Precision

By reducing the location precision of a localization scheme, we can offer better privacy to mobile users since the presence of the mobile user is blended in with more users in the larger area. Bahl et al. [3] have shown that the precision to which we can locate a mobile user is related to the number of APs within that user's communication range. Their experiments showed that there is significant improvement from 1 AP to 2 APs and from 2 APs to 3 APs, but the improvement is small when using more than 3 APs. To reduce location precision, we use transmit power control to minimize the number of APs in range while ensuring at least one AP for connectivity. Here, we assume APs do not dynamically adjust their transmit power; that is, they are passive attackers (Section 3). We discuss more sophisticated attackers in Section 5.3.4.

The transmit power control (TPC) problem has been studied extensively, such as the TPC service specified in 802.11h [11] and power control [22]. The goal of TPC schemes is to hold transmit power to the lowest possible productive level to minimize imposed interference and to save energy. However, because a signal emitted from a mobile station exposes its location, the TPC problem for location privacy has an additional requirement: a mobile station must perform TPC *silently*, without exchanging any messages.

Silent TPC is challenging: the only information available to the mobile station is the received signal strength (RSS) from APs within range. Due to reflection, scattering, multipath fading and absorption of radio waves, the observed signal strength varies in unpredictable ways. Moreover, wireless channels can be asymmetric. Both unpredictability and asymmetry pose difficulties to an effective, silent TPC scheme. To determine the feasibility of RSS-based TPC, we use real-system experimentation and field measurements to drive and validate our design.

### 5.3.1 Asymmetry and Variations of Wireless Channels

When we choose transmission power based on received signal strength, we rely on channel symmetry and consistency. To determine the feasibility of RSS-based TPC, we investigate the asymmetry and variation of 802.11 wireless channels. Our goal is to determine the relationship between the two directions of a channel and use the path loss in one direction to infer the loss in the other direction.

For our investigation, we set up a testbed of two mobile stations with identically configured Netgear wireless cards, node #1

and node #2. The path losses between two cards are measured by reading the Received Signal Strength Indicator (RSSI) inside the driver. Because wireless signal propagation can vary substantially between different environments, we placed the two nodes in a variety of physical environments to test channel characteristics of different scenarios. For instance, two cards were placed on two ends of a corridor, in two separate office rooms, in the corner of an office, and in an open outdoor space. We observed that the channel characteristics of all of these scenarios presented similar characteristics, so due to space constraints, we present the results of two of these scenarios, the corner of an office and the open outdoor space.

Because TPC is based on the *current* RSSI value from the target AP, we compare RSSI values of signals transmitted at the same time. We tested the difference of RSSI values when measured with very little time separation. We measure the wireless channel asymmetry as follows. Node 1 sends a probe to node 2, and then immediately after receiving the probe, node 2 sends a probe to node 1. We record the RSSI readings of the received probes on each node. We repeat this bi-directional RSSI measurement 40 times. Figure 6 shows the time-synchronized RSSI readings on each node. It is evident that despite the path asymmetry, RSSI readings for both directions are strongly correlated. This is because path loss variations are mostly caused by environmental changes, which affects both directions similarly over time. This strong correlation suggests that RSSI-based silent TPC can be quite successful.

Let  $\Delta_{asym}$  be a random variable representing the RSSI difference resulting from channel asymmetry. Figure 7 shows the probability density function (PDF) of  $\Delta_{asym}$  from our field measurements. The mean of  $\Delta_{asym}$  is denoted as  $m_{asym}$  and variance  $\sigma_{asym}^2$ . According to the PDF of  $\Delta_{asym}$ , we get  $m_{asym} = 1.84$  and  $\sigma_{asym}^2 = 1.36$  for the indoor corner scenario, and  $m_{asym} = 3.14$  and  $\sigma_{asym}^2 = 2.65$  for the open outdoor space scenario.

Next, we investigate the variation of the wireless channels over time. We recorded on a mobile node the RSSI readings of received beacons from an AP for 2 hours. Figure 8 shows the distribution of RSSI readings with its variance for both an indoor corner and an open outdoor space. Let  $\Delta_{var}$  be a random variable representing the RSSI difference resulted from channel variations with a zero mean. In our measurements, the variance of  $\Delta_{var}$ , denoted as  $\sigma_{var}^2$ , is 20.92 and 10.73 for indoor corner and open outdoor space scenarios, respectively.

Based on the values of RSSI difference resulted from channel asymmetry and RSSI variation, we calculate path loss difference between the two directions of the channel as  $\Delta = \Delta_{asym} + \Delta_{var}$ .  $\Delta_{asym}$  and  $\Delta_{var}$  are independent, then mean of the path loss difference is  $m = m_{asym} + m_{var}$ , where  $m_{var} = 0$ , and the variance  $\sigma^2 = \sigma_{asym}^2 + \sigma_{var}^2$ .

We define the *path loss margin* (PLM) to be the magnitude of the maximum difference between path losses in opposite directions that result from environmental influences and wireless channel asymmetry (that is, of  $\Delta$ ) that we are likely to experience. We arbitrarily select the 97.7th percentile ( $2\sigma$  above the mean), giving us

$$PLM = m_{asym} + 2 \times \sqrt{\sigma_{asym}^2 + \sigma_{var}^2}. \quad (4)$$

From our experimental results on path asymmetry and variation above, we choose a path loss margin of 11.3 dB for the indoor corner scenario and 10.5 dB for open outdoor space. For simplicity, we use a path loss margin of 10 dB for the rest of our discussion.

### 5.3.2 Silent TPC Design

Now we illustrate our RSS-based silent TPC design. Our design goal is to intelligently adjust the transmit power of the mobile station to reduce the number of APs in range by *only* using the path

loss (a function of RSSI) observed from the opposite direction of the path, namely, from the in-range APs to the mobile station.

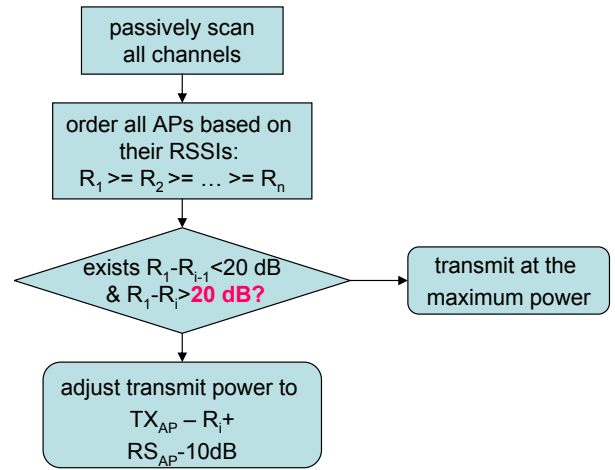


Figure 9: The Silent TPC Scheme

Figure 9 depicts our silent TPC scheme. The 20 dB threshold between  $R_1$  and  $R_i$  is derived from the 10 dB path loss margin (PLM), which ensures that it is feasible to adjust the transmission power such that  $AP_1$  is within the communication range while  $AP_i$  is not. The amount of transmit power is adjusted such that the user can reliably communicate with  $AP_1$ . After TPC, the mobile user is able to communicate with  $AP_1, AP_2, \dots, AP_{i-1}$ .

The rest of this subsection describes technical details on designing the TPC scheme and its implementation. Our silent TPC scheme begins by calculating the path loss from mobile station to AP  $PL_{STA-AP}$  based on the observed reverse path loss  $PL_{AP-STA}$  on the mobile station. The latter can be calculated as follows:

$$PL_{AP-STA} = TX_{AP} - R.$$

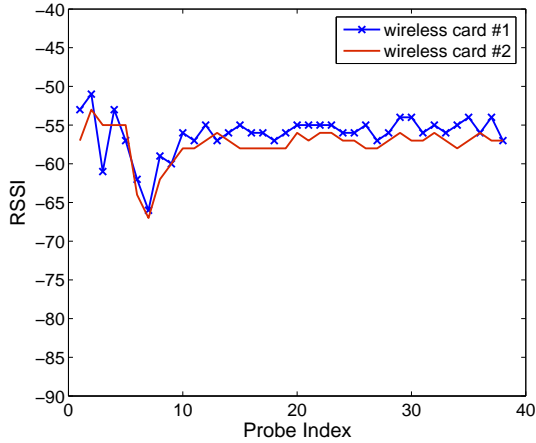
where  $TX_{AP}$  is the transmit power of the AP and  $R$  is the RSSI reading on the mobile station. We determined that the path loss margin because of path asymmetry and channel variation is considered to be 10dB. Then,  $PL_{STA-AP}$  is in the range of  $[TX_{AP} - R - 10 \text{ dB}, TX_{AP} - R + 10 \text{ dB}]$ .

The received signal strength at an access point is  $TX_{STA} - PL_{STA-AP}$  where  $TX_{STA}$  is the mobile station transmit power. Suppose  $AP_i$  cannot receive any signal from the mobile station; then the maximum receive signal strength at  $AP_i$  must be less than its *receive sensitivity*. Receive sensitivity is the minimum RF signal that can be successfully received by the receiver. This sensitivity is a function of the transmission rate and is part of the specification of the wireless card. For example, a Cisco 340 wireless network adapter has receive sensitivity of -90 dBm at 1 Mbps and -83 dBm at 11Mbps [8]. We assume that the receive sensitivity (RS) of all APs is known by the mobile station. To assure that  $AP_i$  cannot hear a mobile station's communications, the mobile station must choose a transmission power such that

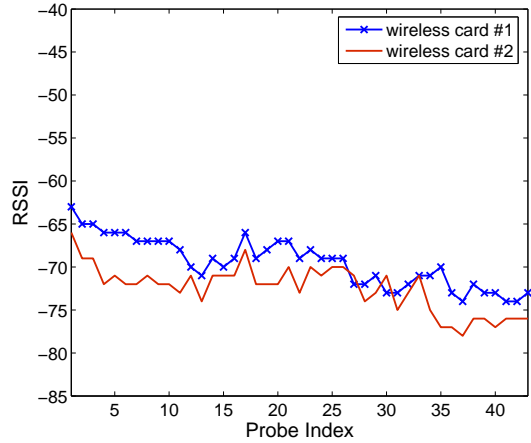
$$TX_{STA} - PL_{STA-AP} \leq TX_{STA} - (TX_{AP} - R_i - 10 \text{ dB}) < RS, \quad (5)$$

where  $R_i$  is the signal strength at which the mobile station receives packets from  $AP_i$ .

To ensure that the mobile station can communicate with the network, it must ensure that it can reliably communicate with at least



(a) indoor corner



(b) open outdoor space

**Figure 6: The Asymmetry of 802.11b Channels: Although the wireless channel is asymmetric, the RSSI are highly correlated.**

one AP, denoted as  $AP_1$ . Therefore, the minimum signal strength that reaches  $AP_1$  must be greater than  $RS$ ; that is,

$$TX_{STA} - (TX_{AP} - R_1 + 10 \text{ dB}) > RS, \quad (6)$$

where  $R_1$  is the signal strength at which the mobile station receives packets from  $AP_1$ . Subtracting Equation (5) from Equation (6), we have:

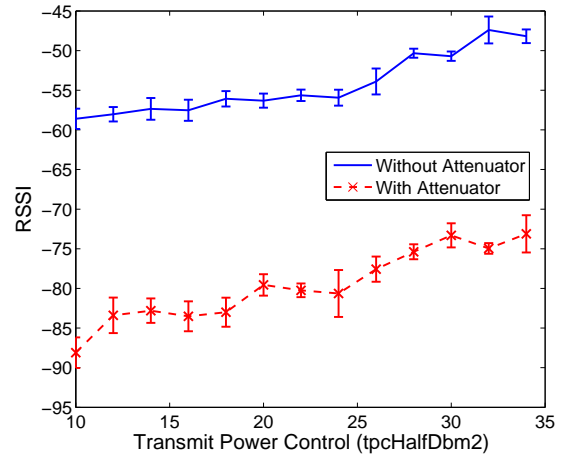
$$R_1 - R_i > 20 \text{ dB}.$$

This means that the TPC scheme can work only when receive signal strength of two APs differs by at least 20 dB, so our TPC scheme first checks whether there exists a pair of APs with RSSIs that differ by at least 20dB. If not, privacy is not improved by TPC. If there is such a pair, the mobile station adjusts its transmit power to a level such that  $TX_{STA} - (TX_{AP} - R_i - 10 \text{ dB}) < RS$ .

We implemented the TPC scheme in the driver of a Netgear WG111U USB wireless card. We modified the Windows kernel driver for this card to support the new functionality needed for transmit power control. In the Atheros driver, transmission power is controlled by a configuration parameter `tpcHalfDbm2`, which can be set to be any integer between 10 and 34, where 34 represents the maximum and default transmit power and 10 the minimum power. To analyze the relation of transmit power and `tpcHalfDbm2`, we used one card as a transmitter and varied the transmission power by changing this setting. We used another card as a receiver that recorded the RSS of each packet received from the transmitter. Figure 10 shows the RSS for each choice of `tpcHalfDbm2`, and shows that the transmit power adjustment range is limited to just 10 dB, which is usually insufficient for TPC. We therefore used an attenuator to further decrease effective transmission power by 25 dB, as shown by the lower curve in Figure 10. There is a gap of 15 dB between the minimum power of the original card and the maximum power of the card with an attenuator. The transmit power cannot be set to levels inside the gap. Nevertheless, we will show that even with limited transmit power control capabilities, our TPC scheme is still very useful and reliable.

### 5.3.3 Effectiveness of the Silent TPC

The silent TPC scheme we proposed is heuristic because of the unpredictability of signal strength. To test its validity, we tested



**Figure 10: Transmit Power Control**

our TPC scheme on an office floor inside the Microsoft wireless LAN coverage. On the third floor, there are six access points using 802.11b. We chose 356 spots to uniformly cover the entire floor, and carried a laptop with our customized wireless card (a Netgear WG111U USB wireless card with the Windows Atheros driver) to each of these spots. At each spot, the wireless card first passively listens to all the channels used by the APs and records the RSS of beacons from each AP. Based on the collected RSS values, we adjusted the card's transmit power using our TPC scheme.

We first evaluate how often a mobile station is able to adjust its transmit power to improve privacy. We used the RSS data collected at the 356 spots chosen uniformly on the floor. Figure 11 shows the reverse cumulative distribution function (reverse CDF) for the maximum RSS difference among APs at each spot  $\Delta RSS$ . More than 73 percent of the spots have RSS difference more than 20dB and can use TPC to improve privacy. Because the spots we tested are uniformly distributed over the floor, this shows that our TPC scheme is applicable in nearly three quarters of the space.

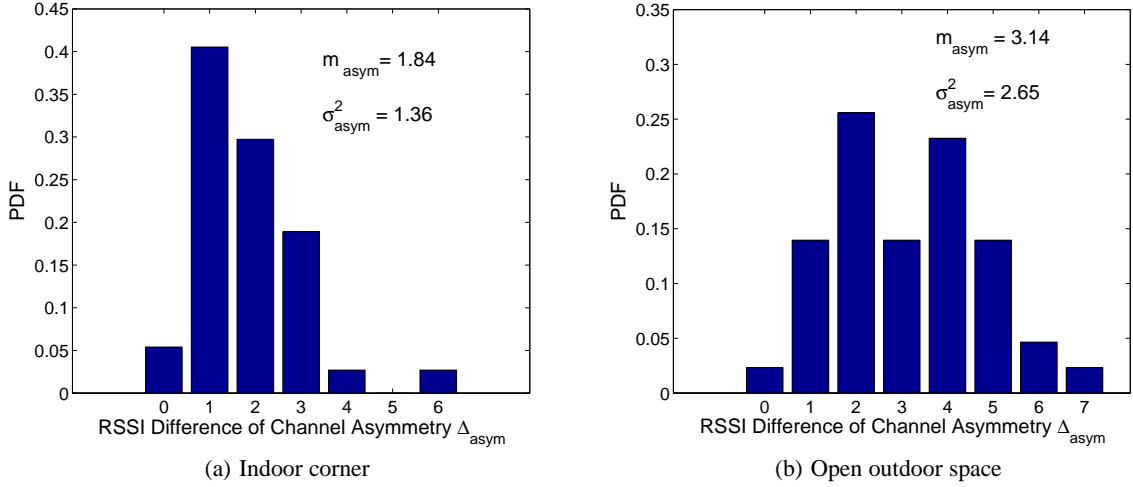


Figure 7: Distribution of RSSI Difference Due to Channel Symmetry

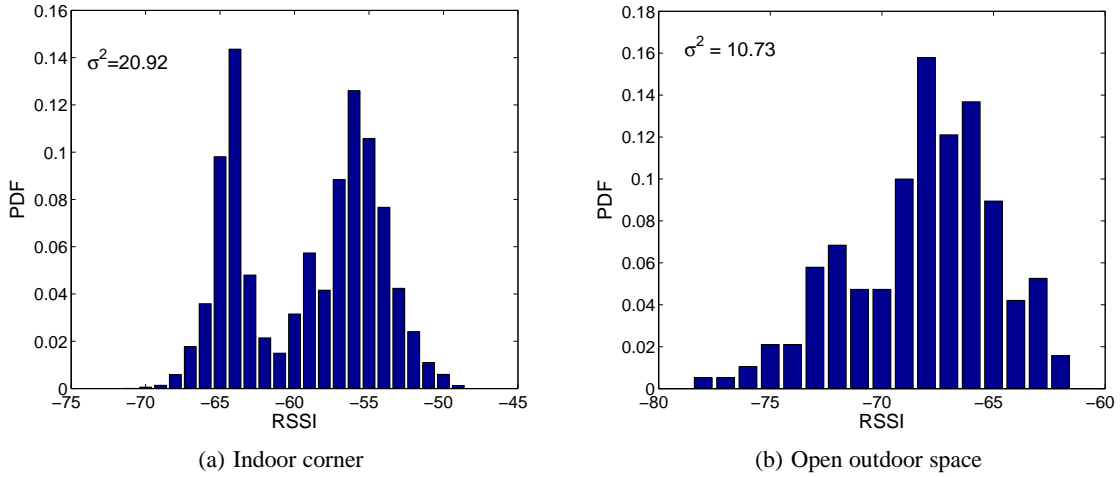


Figure 8: Distribution of RSSI values

Then, we evaluated the effectiveness of our TPC at those eligible spots. We selected ten eligible spots at random. The mobile station then adjusts its transmission power using our TPC algorithm, then sends 100 probe packets to each AP that the mobile station can hear. Instead of modifying the AP (which was serving many wireless users), we placed a promiscuous mobile station near the AP, which records probe responses the AP sends to the station. Table 1 shows the results of our experiment. AP1 is the access point with the highest RSS, while AP2 has the lowest RSS, i.e.,  $\Delta RSS = R_1 - R_2 \geq 20$  dB. The experiment result clearly shows that before TPC, both AP1 and AP2 are in the mobile station’s communication range, and after TPC, only AP1 can receive signals from the mobile station. We also looked at overall statistics on the number of APs in range for all 356 spots before and after our TPC scheme as shown in Figure 12. Before the TPC, 3% of spots have only one AP in range, after the TPC, this percentage increases to 36%. As for spots with only two APs in range, the percentage increases from 11% before TPC to 23% after TPC. Localization

schemes are inaccurate in areas where one or two APs are within range, and our scheme can increase the density of such areas from 14 percent to 59 percent.

### 5.3.4 Privacy Gain with Our Solutions

We first consider the strongest attackers: silent attackers. Such attackers are passive sniffers that transmit no identifying signals, so mobile stations are not aware of their existence. A user cannot assume that its location is private even if the user reduces her transmission power to allow only one AP to hear her. Nevertheless, even under this attacker model, the silent period can still be effective in disassociating pseudonyms from the adversary. If the adversary wants to locate mobile stations accurately at all times, he must place silent attackers densely enough such that every mobile station can be heard by at least three attackers, even when a node uses the minimum transmission power. Our experimental results show that the transmission radius  $r$  is about 10 m at the minimum transmit power. In order for a node to be heard by three attackers

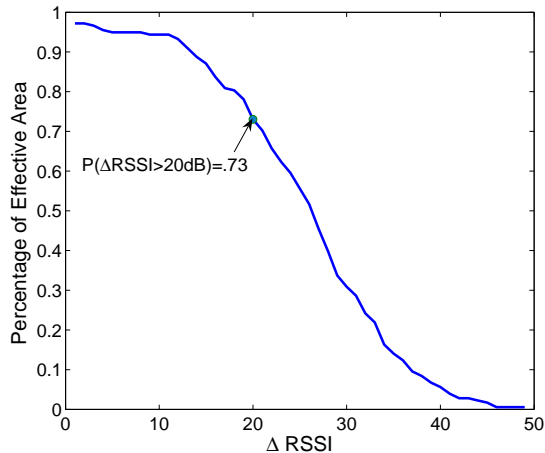


Figure 11: Percentage of Effective Area

index	$\Delta RSS(dB)$	# probe responses			
		AP1		AP2	
		before	after	before	after
1	20.1	100	100	100	0
2	20.2	91	100	100	1
3	24.4	100	100	100	0
4	28.6	100	100	100	0
5	28.7	100	100	100	0
6	30.3	100	100	100	0
7	31.1	100	100	100	0
8	32.2	100	100	100	0
9	35.0	100	100	100	1
10	37.7	100	100	100	0

Table 1: Number of probe responses before and after TPC

at all times, the attacker density  $\rho$  must be such that  $\rho \cdot \pi r^2 \geq 3$ ,  $\rho \geq 0.095$  sniffer/m<sup>2</sup>. This represents one sniffer per 100 m<sup>2</sup>. By comparison, the density of access points deployed in the building that we carried out our experiments is one AP every 500 m<sup>2</sup>, so a silent attacker deployment costs five times as much as regular AP deployment.

For active exposed attackers, network providers may dynamically adjust their access points' transmit power to interfere with our silent TPC scheme. The users could potentially detect such attackers by localizing access points using their RSS values. As users move around, they are able to collect enough information to infer AP location and detect the abnormal behavior. In-depth investigation on approaches against such attackers is future work.

With regard to passive exposed attackers, we present our empirical measurements based on the aforementioned experiments on an office building floor. We define *mix area* of an AP to be the maximum area that is covered by just this AP. The larger the mix area, the more difficult it is for attackers to determine the mobile node's location since the number of mobile nodes in the area is larger. In the office building setting, the distance between an AP and the next closest AP is around 30 meters. We selected one of the six APs as the target AP and studied the size of its mix area *after* TPC. Among 356 spots in total that were chosen uniformly on the floor, there are

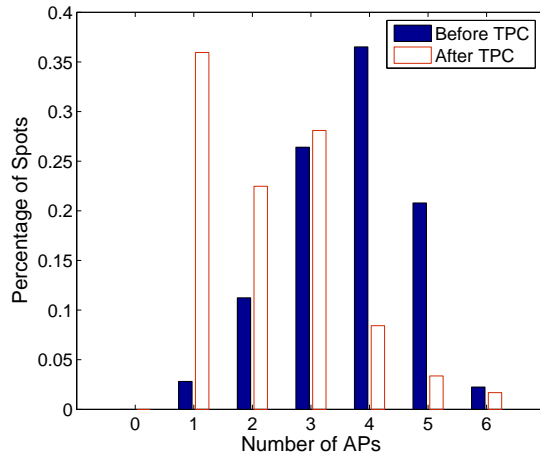


Figure 12: Number of APs in Range Before and After TPC

34 spots whose signals can be heard by only the target AP. According to the floor map, these 34 spots cover an area of approximately 352 m<sup>2</sup>. Users in the mix area of 352 m<sup>2</sup> are indistinguishable for attackers after TPC.

We compare this result to an adversary using RADAR [3] with three APs. The location precision achieved in RADAR is what the adversary could get before TPC. According to the data provided in [3], the location precision is around 3 meters in terms of the median error distance, which corresponds to a circle with area 28 m<sup>2</sup> in which users are indistinguishable before TPC. Therefore, the mix area is increased 12 times ( $=352/28$ ) by applying TPC. Assuming that mobile stations are uniformly distributed, the number of candidates for a new pseudonym is 12 times greater when using TPC. This results in an increased privacy entropy of  $\log_2(12) = 3.7$  in addition to the entropy achieved by using a silent period. If the WLAN follows the mobility pattern of the bus system, the maximum privacy entropy that our system can provide is 11.1 bits, including 7.4 bits from silent period and 3.7 bits from the transmit power control; hence, a user can be indistinguishable from more than a thousand users in the same coverage area.

For points outside of the protected area, location precision of mobile stations covered by two or more APs varies among different location schemes. We do not have detailed numerical analyses about the location precision of points outside of a protected area. However, location precision can be notably reduced if the number of APs that the user communicates is reduced from three or more to two or less [3].

## 6. OPERATIONAL MODEL

In this section, we present the privacy-enabling operations in privacy preserving systems, focusing first on mobile node operation, then on service provider operation.

### 6.1 Mobile Nodes

One goal of our work is to allow each user to configure her privacy requirements as policies and to have user-friendly operations that result in minimal disruption while satisfying the users' privacy policy. In this section, we present our design for mobile node operations that achieves this goal.

Though content privacy can be protected at the granularity of applications by encrypting the transmissions of a particular privacy-

sensitive application, location privacy requires the participation of the whole mobile system including all applications. Therefore, in our design, a user configures the location privacy of her system using a Boolean flag (e.g., a checkbox) indicating whether the user desires the location privacy or not. Figure 13 and Figure 14 show such a user interface. During a silent period (Section 5.2), any user-initiated communications are rejected and the user is alerted that she cannot transmit to protect her privacy.

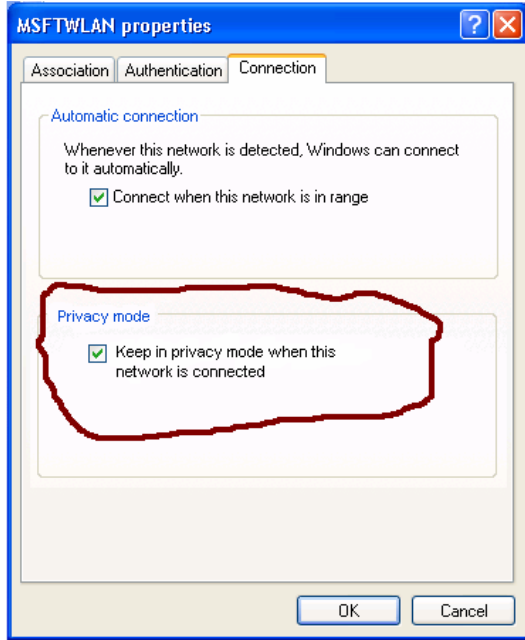


Figure 13: User Interface: Checkbox for Privacy Mode

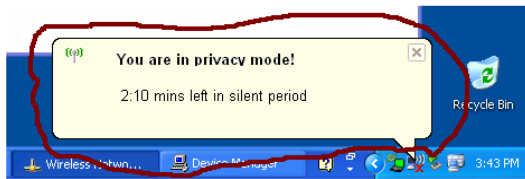


Figure 14: User Interface: Alert Message

Our system implements the opportunistic silent period (Section 5.2) and keeps track of the time period between communication sessions. When that period exceeds the silent period, a new MAC address is requested from the AP (as discussed in Section 5.1) using a transmit power decodable only by the serving AP (Section 5.3). A user may initiate communications before the end of the silent period. We illustrate the system operations under this scenario in Figure 15: our system first checks whether the user has configured the mobile station to be in privacy mode. If not, the communication session can start immediately; otherwise, the user is alerted to wait until the end of the silent period, then new MAC is requested and the user can start communicating. In this design, even non-privacy-sensitive users obtain new MAC addresses opportunistically to increase the entropy for privacy-sensitive users, while not disrupting the communications of non-privacy-sensitive users.

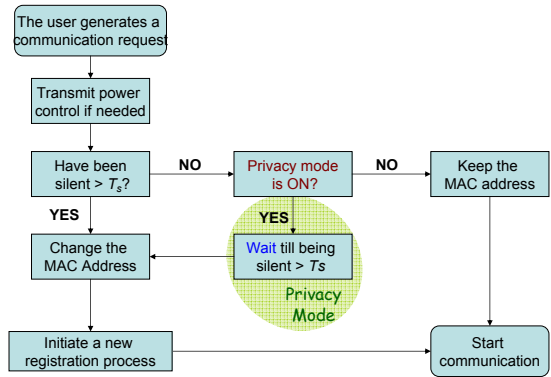


Figure 15: Mobile Node Operating Model

## 6.2 Service Providers

In Section 5.1, we described our MAC address selection scheme, by which mobile nodes frequently change their MAC addresses. In this scheme, access points need provide a DHCP-like service for MAC address selection in the association phase.

Service providers are also responsible for providing the length of silent period to their users and the corresponding degree of privacy they should anticipate. Therefore, service providers need obtain the mobility patterns of their users and choose the silent period based on the methodology described in Section 5.2.

## 7. CONCLUDING REMARKS

In this paper, we have given a thorough treatment to the problem of location privacy in wireless LANs, where users' location information can be inferred from their wireless transmissions. Our solutions can be easily applied to cellular networks as well, where the base stations are able to locate cell phone users.

Our approach in achieving location privacy is to have mobile stations frequently change their pseudonyms (e.g., MAC and IP addresses), to pause opportunistically for a silent period, and to perform silent TPC to reduce the location precision. We verified the practicality of our schemes and evaluated their efficacy by using a combination of real-system experimentation, simulation, and analysis. Given certain mobility pattern and wireless LAN coverage, our system can offer up to 11-bit entropy protection for location privacy with little performance overhead. We also designed our privacy-enabling operations on mobile nodes to be user-friendly and incur minimal disruption to both privacy-sensitive and privacy-indifferent users.

A number of open problems still remain. It is inevitable that privacy-enabled systems sacrifice service quality. Users in privacy mode will have their communications delayed if they communicate before a silent period ends. This is an inherent cost of location privacy. This is certainly disruptive to real-time applications such as Voice-Over-IP or long communication sessions such as watching video online. Nevertheless, many applications such as instant messaging, e-mail, and web surfing can still be used in privacy-enabled wireless systems. Our future work will investigate the tradeoff between privacy and service quality.

Our silent transmit power control scheme reduces the signal-to-noise ratio received at the AP, possibly reducing the data rate to ensure successful transmission. Our experiments sent all packets at the lowest bit rate. Further study is needed on the interplay of our silent transmit power control and wireless card rate control.

## 8. ACKNOWLEDGMENTS

We would like to thank Venkat Padmanabhan, Victor Bahl, Brian Zill, Ranveer Chandra and Paul Yu for many useful discussions. We thank Charlie Reis for helping us on TPC attenuation. We would also like to thank our shepherd, David Wetherall, and the anonymous reviewers for their detailed suggestions and insightful comments.

## 9. REFERENCES

- [1] D. Aguayo, J. Bicket, S. Biswas, D. S. J. De Couto, and R. Morris. MIT Roofnet implementation. Technical report, MIT, Aug. 2003. Available at <http://pdos.lcs.mit.edu/roofnet/design/>.
- [2] P. Bahl and V. N. Padmanabhan. RADAR: An in-building RF-based user location and tracking system. In *Proceedings of IEEE INFOCOM '00*, volume 2, pages 775–784, Tel-Aviv, Israel, March 2000.
- [3] P. Bahl, V. N. Padmanabhan, and A. Balachandran. Enhancements to the RADAR user location and tracking system. Technical Report 12, Microsoft Research, February 2000.
- [4] A. R. Beresford and F. Stajano. Location privacy in pervasive computing. *IEEE Pervasive Computing*, 2(1):46–55, January 2003.
- [5] P. Bhagwat, B. Raman, and D. Sanghi. Turning 802.11 inside-out. In *Proceedings of the Second Workshop on Hot Topics in Networks (HotNets-II)*, Nov. 2003.
- [6] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 4(2), Feb. 1982.
- [7] Y.-C. Cheng, Y. Chawathe, A. LaMarca, and J. Krumm. Accuracy characterization for metropolitan-scale Wi-Fi localization. In *Proceedings of Mobisys*, Seattle, WA, June 2004.
- [8] Cisco Aironet wireless LAN client adapters installation and configuration guide for Windows, 2003.
- [9] CRAWDAD: Achieving wireless data at Dartmouth College. Available at <http://crawdad.cs.dartmouth.edu>.
- [10] D. Dailey, G. Fisher, and S. Maclean. Busview and transit watch: an update on two products from the seattle smart trek model deployment initiative. In *Sixth Annual World Congress on Intelligent Transport Systems*, Nov. 1999.
- [11] M. S. Gast. *802.11 Wireless Networks, The Definitive Guide*. O'Reilly Media Inc., 2nd edition, 2005.
- [12] The IETF Geopriv working group. <http://www.ietf.org/html.charters/geopriv-charter.html>.
- [13] R. Gerdes, T. Daniels, M. Mina, and S. Russell. Device identification via analog signal fingerprinting: A matched filter approach. In *Proceedings of The 13th Annual Network and Distributed System Security Symposium, NDSS'06*, San Diego, California, February 2006.
- [14] A. Görlach, A. Heinemann, and W. W. Terpstra. Survey on location privacy in pervasive computing. In P. Robinson, H. Vogt, and W. Wagealla, editors, *Privacy, Security and Trust within the Context of Pervasive Computing*, The Kluwer International Series in Engineering and Computer Science, 2004.
- [15] M. Gruteser and D. Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. In *Proceedings of First ACM/USENIX International Conference on Mobile Systems, Applications, and Services (MobiSys)*, San Francisco, CA, May 2003.
- [16] M. Gruteser and D. Grunwald. Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis. In *WMASH '03: Proceedings of the 1st ACM international workshop on Wireless mobile applications and services on WLAN hotspots*, pages 46–55, San Diego, CA, USA, 2003.
- [17] J. Hall, M. Barbeau, and E. Kranakis. Radio frequency fingerprinting for intrusion detection in wireless networks. *IEEE Transactions on Dependable and Secure Computing*, 2005. DRAFT.
- [18] M. Hazas and A. Ward. A high performance privacy-oriented location system. In *Proceedings of PerCom 2003: First IEEE International Conference on Pervasive Computing and Communications*, page 216223, Dallas-Fort Worth, USA, March 2003.
- [19] Q. He, D. Wu, and P. Khosla. Quest for personal control over mobile location privacy. *IEEE Communications Magazine*, 42(5):130–136, May 2004.
- [20] Y.-C. Hu and H. J. Wang. Location privacy in wireless networks. In *Proceedings of the ACM SIGCOMM Asia Workshop*, Beijing, 2005.
- [21] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki. Enhancing wireless location privacy using silent period. In *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)*, New Orleans, LA, 2005.
- [22] V. Kawadia and P. R. Kumar. Power control and clustering in ad hoc networks. In *Proceedings of IEEE Infocom*, San Francisco, California, April 2003.
- [23] A. M. Ladd, K. E. Bekris, A. Rudys, G. Marceau, L. E. Kavvaki, and D. S. Wallach. Robotics-based location sensing using wireless Ethernet. In *Proceedings of MobiCom '02*, pages 227–238, Atlanta, Georgia, September 2002.
- [24] G. Montenegro and C. Castelluccia. Statistically unique and cryptographically verifiable (SUCV) identifiers and addresses. In *Symposium on Network and Distributed Systems Security (NDSS2002)*, 2002.
- [25] M. K. Reiter and A. D. Rubin. Crowds: Anonymity for web transactions. *ACM Transactions on Information and System Security*, 1(1):66–92, 1998.
- [26] C. Shannon. A mathematical theory of communication. *Bell Systems Technical Journal*, 27:379–423, 623–656, July, October 1948.
- [27] R. van Drunen, D.-W. van Gulik, J. Koolhaas, H. Schuurmans, and M. Vijn. Building a wireless community network in the Netherlands. In *Proceedings of the USENIX 2003 Annual Technical Conference*, pages 219–230, June 2003.