Enhancing Privacy in LTE Paging System Using Physical Layer Identification

Tuan Ta and John S. Baras

Institute for Systems Research
University of Maryland, College Park, MD 20742, USA
{tta,baras}@umd.edu

Abstract. User location privacy is a growing concern in cellular networks. It has been recently shown that the paging architecture in GSM networks leaks user location information. In this paper, we first prove theoretically that LTE networks also have the same vulnerability. We then propose a solution making use of a novel signal processing technique, physical layer identification. The idea is to embed users' unique tags onto the downlink paging signal waveforms so that the tags are stealthy and robust. We show that our scheme not only improves users' privacy, but also saves system bandwidth.

Keywords: LTE, location privacy, physical layer identification, paging.

1 Introduction

In all cellular networks, mobile stations (MS) mostly run on battery. To prolong the operational time of the MSs, the network architecture allows them to go into idle mode after being inactive for a certain period of time. In idle mode, the MSs do not sustain a connection with the serving base stations (BS). When there is a need to create a connection with an idle MS, e.g. voice calls, data, or system information updates, the BS sends out a notification to the MS in the form of a paging message. The location of an idle MS may have changed since the last time it was in communication. Therefore, the network maintains a tracking area for each idle MS. A tracking area consists of several cells. The MS has to report if it moves out of the assigned tracking area. In general, paging messages are sent without any confidentiality protection. As a result, everybody can listen to those messages. The privacy of those who are being paged is provided through the use of temporary IDs. Those are IDs which only have meaning in the context of the idle MS and the serving network within the tracking area. Recently, Kune *et al.* have shown that despite the use of temporary IDs, the location of a user's cellphone in a GSM network can still be leaked [1]. In particular, they show that an attacker can check if a user's cellphone is within a small area, or absent from a large area, without the user's awareness. As the authors highlighted, such vulnerability can lead to serious consequences. For example, in an oppressive regime, locations of dissidents are revealed to suppressive agents without cooperation from reluctant service providers. Another example is that a thief,

R. Di Pietro et al. (Eds.): DPM 2012 and SETOP 2012, LNCS 7731, pp. 15–28, 2013.

who attempts a break-in, can use the knowledge of the absence of the target to reduce the threat of encounter.

To perform this location attack, the attacker in [1] requires 2 capabilities:

- Cause paging request messages to appear on the GSM *Paging Control Channel* (PCCH)
- Listen on the GSM PCCH broadcast channel

In GSM networks, paging messages are sent on dedicated time-division channels. The *Temporary Mobile Subscriber Identity* (TMSI) is used for paging messages. The idea behind the location attack is that the adversary initiates a connection request to the user cellphone (this of course assumes that he knows the target's number), which results in a paging message being sent in the user's tracking area. By observing the paging channel, the adversary obtains a set of possible temporary IDs for the target user. Repeating this procedure several times, the adversary collects several sets of possible temporary IDs, from which he can do set intersection to get the temporary ID associated with the user's cellphone. Practical experiments on T-Mobile and AT&T GSM networks show that after 2 or 3 repetitions, the adversary can pinpoint the temporary ID of a user's cellphone [1]. To keep the user unaware of the attack, the connection request to his cellphone has to be terminated before a connection is established, but after the paging message is sent out. In [1], the authors, through experiments, show that by calling the target's number and hanging up within 5 seconds, a paging message would be sent out, but the user's phone would not ring. Another way of achieving this goal is to send "silent SMS", a controversial method used by German and French police to track people [4], [5].

After reviewing the paging architecture in LTE and proving that the same attack is possible in LTE networks, we propose a solution using physical layer identification tags. Most security measures operate on the bit level and above. We go further down, to the physical level of electromagnetic transmissions. Our method does not rely on cryptographic primitives. Addressing the attack, the mitigations in [1] either require additional control signaling (sending paging messages out to several tracking areas, changing TMSI more frequently), or introduce delay in response to users' requests. Our solution requires neither. In fact, it requires less signaling than the current standard. However, it does require additional signal processing steps and therefore needs to be incrementally deployed. We want to emphasize that even though the additional signal processing is not in the standard, it is not computationally expensive. Therefore the effect on power consumption of the UEs is minimal. Our technique is inspired by the physical layer authentication scheme in [2], [3]. In those works, Yu *et al.* describe a stealthy authentication technique in which the authenticating entity's credential is embedded as a watermark in the transmitted physical waveform. The authenticator detects the presence of the tag in the received waveform, and decides whether the waveform was transmitted by the legitimate transmitter or not. We extend this technique to the LTE paging system by assigning to each user equipment (UE) a unique tag. These tags are superimposed onto the paging transmitted waveform if the corresponding UEs are paged. The tags are

transmitted with very low power such that they can only be *detected*, and not *decoded*. By detecting the presence of its tag, a UE learns that it is paged. Because of the stealth property of the tags, an eavesdropper observing the paging waveform learns nothing about who are being paged.

The paper is structured as follows. In Section 2, we review the LTE paging system and show that it has the same vulnerability as the GSM system. Next, in Section 3, we describe our scheme. In Section 4, we evaluate the performance of our scheme through simulations. We finish with some conclusions and remarks.

2 LTE Paging System

In this section, we highlight some technical specifications of LTE which allow us to conclude that the location attack in [1] can be performed in an LTE network. We will use these details in the analysis of our scheme in subsequent sections.

Control Signaling: In contrast to the GSM architecture, in LTE there is no dedicated resource for paging. Instead, the paging messages are delivered in the same frequency band as normal data; and the existence of such paging messages in each subframe (1ms) is indicated in the control channel. In normal operation mode, at the beginning of each LTE downlink subframe, there are up to 4 (out of 14) OFDM symbols used to transmit control data. These *Downlink Control Information* (DCI) messages carry resource allocation information, Hybrid-ARQ, system information and paging indicator among others. Each control message is encapsulated in a *Physical Downlink Control Channel* (PDCCH) message. The DCI can be targeted to a specific user equipment (UE), or a group of UEs as in the case of a paging indicator. If the DCI is for a specific UE, the 16-bit CRC generated for that DCI will be XORed with the last 16 bits of the temporary ID of the targeted UE (e.g. *Cell Radio Network Temporary Identifier* C-RNTI). If the DCI is for a group of UEs, its CRC will be masked with one of the predefined IDs for group control information. The paging indicator ID, P-RNTI, is *FFFE* (in hexadecimal) [8].

UE Decoding: The UEs do not know a priori which PDCCH in the control region of a subframe is intended for them. Therefore they perform *blind decoding*, in which they try all possible sizes of PDCCH. The list of such allowable sizes can be found in [7]. If after unmasking the CRC of a possible PDCCH message with either a common ID or the UE's temporary ID, the CRC check returns true, then the UE knows that it has successfully decoded a valid PDCCH message. To reduce the number of PDCCH the UEs have to try to decode, each UE is given a *search space*. The search space is all possible starting positions of a PDCCH. There are UE-specific search spaces and common search spaces. The latter are locations which all UEs have to try decoding from. Group control information, including paging indicator, is sent on the common search space. Due to the requirement that broadcast control information has to reach users with poor channel conditions, group PDCCH have bigger sizes than other PDCCH, which allows for lower code rates to be used. Two allowable sizes for these PDCCH are

72 and 144 *resource elements* [7]. Resource element is the smallest resource unit in LTE, comprising of 1 subcarrier in 1 OFDM symbol. All control information are modulated with QPSK, therefore the paging PDCCH can have either 144 or 288 bits.

The DCI format for paging indicator is either 1A or 1C [7]. Depending on the system bandwidth (1.4 - 20 MHz), DCI format 1A, and 1C can have 36 - 44, and 24 - 31 bits respectively [10]. This DCI has the location of the paging record in the data portion of the subframe. The UE decodes that location in the *Physical Downlink Shared Channel* (PDSCH) to get the record. The paging record contains a list of IDs of UEs being paged, which can be either *System Architecture Evolution TMSI* (S-TMSI) or *International Mobile Subscriber Identity* (IMSI) [9]. In normal cases, the temporary ID S-TMSI is used instead of the permanent ID IMSI. If the UE sees its ID in the list, it knows that it is paged. Figure 1 illustrates an example of paging PDCCH and PDSCH positions in an LTE downlink subframe.

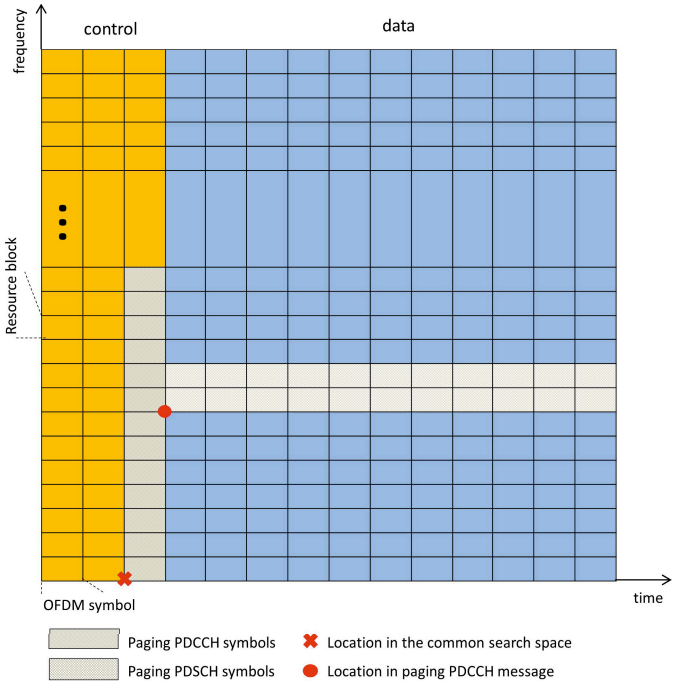

Fig. 1. An example of positions of paging PDCCH and PDSCH in an LTE downlink subframe. Pilots and other types of physical channels are omitted for clarity.

Attacker Model: We will use an analogous attacker model as [1]. The only difference is that our attacker is capable of causing paging request messages in LTE networks and listen on LTE paging channels. While the first capability of the attacker remains the same as in the original paper, the above procedure

serves to justify the practicality of the second capability. The attacker can listen on the control channel, and unmask PDCCH with P-RNTI. Once he decodes a paging indicator, he can go the specified location in PDSCH to obtain the list of paged IDs. In [1], Kune *et al.* use an open source GSM baseband software implementation [12] to read the TMSI of paged MSs. While an equivalent open source software for LTE baseband is not available at this moment, it is reasonable to expect that one will be developed in the future. We therefore conclude that the same location attack is feasible in LTE, and security measures should be taken proactively.

3 Privacy-Enhanced Paging Messages

To combat the vulnerability in the LTE paging system described in Section 2, we propose to use a UE's temporary ID as an input to create a tag unique to that UE. If a UE is paged during a subframe, its tag is embedded onto the paging PDCCH. The only requirement for the tags is that tags from 2 different UEs are uncorrelated. Here "embed" means that the tag is superimposed onto the PDCCH QPSK symbols. To be backward compatible with older user equipment, the content of the paging indicator is left unchanged. A simple scenario where one old UE (Alice) and one new UE (Bob) are paged in the same subframe is illustrated in Figure 2. If the tag embedding does not cause too much degradation to the PDCCH signal quality, Alice is still able to decode the control information and follow the standard procedure to see if she is paged. Bob, however, can determine if he is paged just by detecting the presence of his unique tag in the PDCCH. Therefore he does not need to decode the PDSCH, which saves battery considering that most UEs which expect paging messages are in idle mode. Listening on the paging channel, Eve can obtain Alice's temporary ID, but she cannot get Bob's tag. As will be shown later, Bob's tag is transmitted

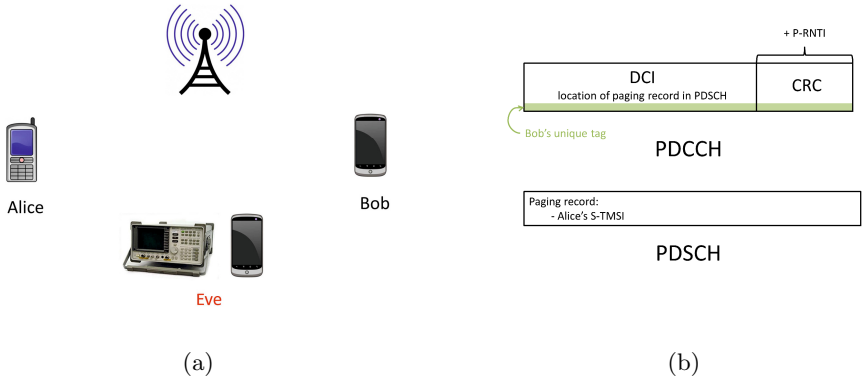

Fig. 2. (a) Simple scenario with one old UE (Alice) and one new UE (Bob) being paged at the same subframe. The eavesdropper, Eve, can listen on the paging broadcast channel and analyze the PDCCH waveform; (b) PDCCH and PDSCH paging messages.

with very low power so that nobody (including Bob) can decode it. Bob, however, can detect the presence of his tag in the paging PDCCH. Another benefit of this scheme comes in the form of downlink data bandwidth increase. Since Bob's ID is no longer needed to be transmitted in PDSCH, that bandwidth can be used for data transmission. The new UE capability as well as paging mechanism can be negotiated with the base station (eNodeB in LTE terms) at connection establishment. The operations at the eNodeB and UE are shown in Figure 3.

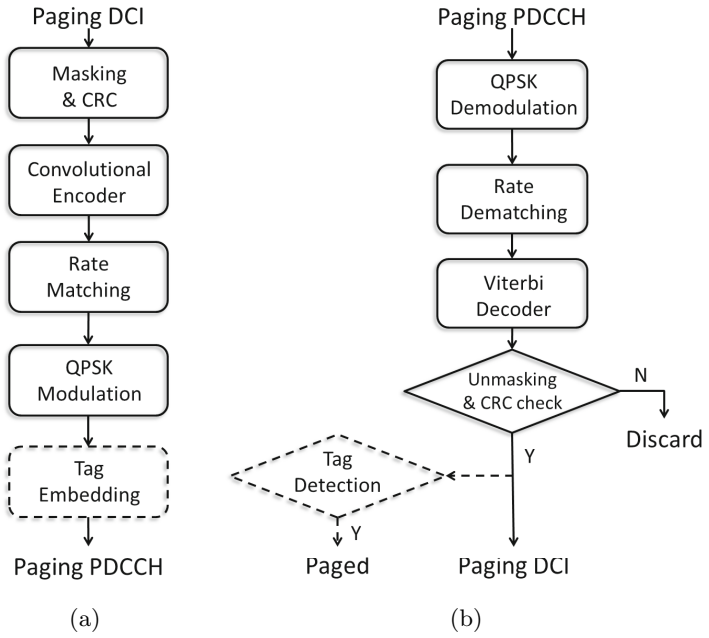

Fig. 3. Flow charts for (a) eNodeB and (b) User Equipment. Dashed boxes are additional operations required by the scheme.

To maximize the robustness of the tags, we choose to put a tag symbol on every paging indicator PDCCH symbol. We use QPSK to modulate the tags. With this configuration, the tags have the same length as the paging indicator PDCCH, which is either 144 or 288 bits. During a subframe, multiple tags can be superimposed on the same PDCCH, corresponding to multiple UEs being paged at the same time. In LTE standard, the maximum size of the paging record is 16 [9]. In other words, the 3GPP standard leaves room for up to 16 UEs to be paged during 1 subframe. In subsequent sections, we analyze the performance of our scheme with respect to the number of simultaneous tags, N_t.

3.1 eNodeB Operations

Let $\mathbf{b}$ be the paging DCI. The PDCCH symbols that encapsulate this DCI are $\mathbf{s} = f_e(\mathbf{b})$. Here $f_e(\cdot)$ is the encoding function, which includes CRC, convolutional encoding, rate matching, and QPSK modulation. Let $\mathbf{k}_i, i = 1, \ldots, N_t$, be the i^{th} paged UE's ID. Generate the tag $\mathbf{t}_i = g(\mathbf{k}_i)$. As mentioned above, the functionality of the generator function $g(\cdot)$ is to create uncorrelated tags. The elements of $\mathbf{b}$ and $\mathbf{k}_i$ are in bits; while the elements of $\mathbf{s}$ and $\mathbf{t}_i$ are in QPSK symbols $\{\pm 1, \pm i\}$. The tags are superimposed onto the PDCCH to create the transmitted message

$$\mathbf{x} = \rho_s \mathbf{s} + \frac{\rho_t}{\sqrt{N_t}} \sum_{i=1}^{N_t} \mathbf{t}_i \tag{1}$$

Let $\mathbf{s} = (s^{(1)}, \ldots, s^{(L)})$, i.e. there are L QPSK symbols in the PDCCH signal. For paging indicators, $L = 72$ or 144. Assuming that each symbol of the PDCCH signal and of the tag has zero-mean and unit variance, we have

$$\begin{aligned} &\mathrm{E}[s^{(k)}] = 0, \mathrm{E}\left[|s^{(k)}|^2\right] = 1 \qquad \text{for} \qquad k = 1, \ldots, L \\ &\mathrm{E}[t_i^{(k)}] = 0, \mathrm{E}\left[|t_i^{(k)}|^2\right] = 1 \qquad\qquad\quad i = 1, \ldots, N_t \end{aligned} \tag{2}$$

Since the tags are uncorrelated among themselves and independent of the PDCCH symbols,

$$\mathrm{E}[\mathbf{s}^H \mathbf{t}_i] = 0, \quad i = 1, \ldots, N_t \tag{3}$$

$$\mathrm{E}[\mathbf{t}_i^H \mathbf{t}_j] = 0, \quad i, j = 1, \ldots, N_t, \quad i \neq j \tag{4}$$

In (1), ρ_s and ρ_t are system parameters controlling the amount of power allocated to the signal and the tags, respectively. The power constraint is

$$\rho_s^2 + \rho_t^2 = 1 \tag{5}$$

From (1) - (5), we have

$$\begin{aligned} &\mathrm{E}[\mathbf{s}] = \mathrm{E}[\mathbf{t}_i] = \mathrm{E}[\mathbf{x}] = 0 \\ &\mathrm{E}[|\mathbf{s}|^2] = \mathrm{E}[|\mathbf{t}_i|^2] = \mathrm{E}[|\mathbf{x}|^2] = L, \qquad i = 1, \ldots, N_t \end{aligned} \tag{6}$$

3.2 User Equipment Operations

Decode DCI. Assuming a frequency selective fading channel, the received signal at the UEs is

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{w} \tag{7}$$

where $\mathbf{H}$ is a diagonal matrix, with the elements being the attenuations at each subcarrier frequency. $\mathbf{w}$ is thermal noise at the transmitter and receiver circuitry. In LTE, pilot symbols are transmitted on fixed resource elements to help in channel estimation at the receivers [6]. There are many techniques that the

receiver can use to perform channel estimation, e.g. LMMSE [11]. In general, the channel estimate can be written as

$$\hat{\mathbf{H}} = \mathbf{H} + \nu \tag{8}$$

where ν is the estimation error.

Let $\hat{H}^{(k)}, k = 1, \ldots, L$ be the diagonal elements of $\hat{\mathbf{H}}$, the receiver estimates the message symbols as

$$\begin{aligned} \hat{x}^{(k)} &= \frac{\hat{H}^{(k)^*}}{|\hat{H}^{(k)}|^2} y^{(k)} \\ &= x^{(k)} - \frac{\nu^{(k)} x^{(k)}}{\hat{H}^{(k)}} + \frac{w^{(k)}}{\hat{H}^{(k)}} \end{aligned} \tag{9}$$

It then decodes the DCI

$$\hat{\mathbf{b}} = f_d(\hat{\mathbf{x}}) \tag{10}$$

Here $f_d(\cdot)$ is the decoding function, which maps QPSK symbols to bits, undoes rate matching, performs Viterbi decoding, and removes CRC. After unmasking with the paging ID (*FFFE*), the CRC check returns true if the DCI is successfully decoded.

Tag Detection. The UE regenerates the message symbols from the decoded DCI, $\hat{\mathbf{s}} = f_e(\hat{\mathbf{b}})$, and subtracts it from the received signal to get the residue

$$\mathbf{r} = \frac{1}{\rho_t} (\hat{\mathbf{x}} - \rho_s \hat{\mathbf{s}}) \tag{11}$$

Assuming that the UE performs perfect channel estimation, we have

$$\mathbf{r} = \frac{1}{\sqrt{N_t}} \sum_{i=1}^{N_t} \mathbf{t}_i + \frac{1}{\rho_t} \hat{\mathbf{H}}^{-1} \mathbf{w} \tag{12}$$

It then checks for the presence of its tag, $\mathbf{t}$, by performing hypothesis testing on the statistic

$$\tau = \mathbf{t}^H \mathbf{r} \tag{13}$$

The hypotheses are

$$\begin{aligned} H_0 :&\quad \mathbf{t} \text{ is not present in } \mathbf{r} && \text{(null hypothesis)} \\ H_1 :&\quad \mathbf{t} \text{ is present in } \mathbf{r} && \text{(alternative hypothesis)} \end{aligned}$$

The statistic under null hypothesis:

$$\tau | H_0 = \frac{1}{\sqrt{N_t}} \sum_{i=1}^{N_t} \mathbf{t}^H \mathbf{t}_i + \frac{1}{\rho_t} \mathbf{t}^H \hat{\mathbf{H}}^{-1} \mathbf{w} \tag{14}$$

Condition on $\mathbf{t}$, the second term in (14) is the sum of L Gaussian random variables

$$\eta_2 = \frac{1}{\rho_t}\mathbf{t}^H\hat{\mathbf{H}}^{-1}\mathbf{w} = \frac{1}{\rho_t}\sum_{k=1}^{L}\frac{t^{(k)^*}w^{(k)}}{\hat{H}^{(k)}} \tag{15}$$

The resulting Gaussian random variable has mean zero and variance

$$\sigma^2_{\eta_2} = \frac{1}{\rho_t^2}\sum_{k=1}^{L}\frac{\sigma_w^2}{|\hat{H}^{(k)}|^2} = \frac{1}{\rho_t^2}\sum_{k=1}^{L}\frac{1}{\gamma^{(k)}} \tag{16}$$

where $\gamma^{(k)}$ is the SNR of the k^{th} subcarrier.

The first term in (14) can be written as

$$\eta_1 = \frac{1}{\sqrt{N_t}}\sum_{i=1}^{N_t}\mathbf{t}^H\mathbf{t}_i = \frac{1}{\sqrt{N_t}}\sum_{i=1}^{N_t}\sum_{k=1}^{L}t^{(k)^*}t_i^{(k)} \tag{17}$$

η_1 is the sum of N_tL i.i.d. symbols from the set $\{\pm 1, \pm i\}$. According to the Central Limit Theorem, it can be approximated by a Gaussian random variable with zero-mean and variance $\sigma^2_{\eta_1} = L$.

From (14) - (17), we have

$$\tau|H_0 \sim \mathcal{N}\left(0, L + \frac{1}{\rho_t^2}\sum_{k=1}^{L}\frac{1}{\gamma^{(k)}}\right) \tag{18}$$

The statistic under alternative hypothesis: Without loss of generality, let $\mathbf{t} = \mathbf{t}_1$. The statistic is

$$\tau|H_1 = \frac{1}{\sqrt{N_t}}\left(|\mathbf{t}_1|^2 + \sum_{i=2}^{N_t}\mathbf{t}_1^H\mathbf{t}_i\right) + \frac{1}{\rho_t}\mathbf{t}_1^H\hat{\mathbf{H}}^{-1}\mathbf{w} \tag{19}$$

Condition on $\mathbf{t}_1$, the term inside the parentheses in (19) can be approximated as a Gaussian random variable with mean $|\mathbf{t}_1|^2 = L$ and variance $(N_t - 1)L$. Therefore

$$\tau|H_1 \sim \mathcal{N}\left(\frac{L}{\sqrt{N_t}}, \frac{N_t - 1}{N_t}L + \frac{1}{\rho_t^2}\sum_{k=1}^{L}\frac{1}{\gamma^{(k)}}\right) \tag{20}$$

The UE performs a threshold test on τ to determine the presence of its tag in the residue.

$$H = \begin{cases} H_0 & \text{if } \tau \leq \tau^0 \\ H_1 & \text{if } \tau > \tau^0 \end{cases} \tag{21}$$

In making the comparison in (21), we use only the real part of τ. The imaginary parts of $\tau|H_0$ and $\tau|H_1$ have very similar statistic, and therefore do not provide much information. By abuse of notation, we still call the real part τ.

The threshold τ^0 is a value between $\left[0, L/\sqrt{N_t}\right]$. The greater τ^0 is, the higher the probability of miss detection; whereas the smaller τ^0 is, the higher the probability of false alarm. We choose $\tau^0 = L/2\sqrt{N_t}$ for good performance in both criteria. With this choice of the threshold, the probability of missing a tag is

$$P_m = \Phi\left(\frac{-\frac{L}{2\sqrt{N_t}}}{\left(\frac{N_t-1}{N_t}L + \frac{1}{\rho_t^2}\sum_{k=1}^{L}\frac{1}{\gamma^{(k)}}\right)^{1/2}}\right) \tag{22}$$

where $\Phi(\cdot)$ is the standard Gaussian cumulative distribution function. To get an idea of the theoretical performance of the scheme, let us look at a special case where the channel is flat fading with SNR = 10dB. Assume 10% of the transmitted power is allocated to tags, i.e. $\rho_t^2 = 0.1$; and 288 bits are used for PDCCH message, i.e. $L = 144$. When 4 users are paged simultaneously, i.e. $N_t = 4$, we have $P_m = 0.01$. So we can see under that condition, the tags are detected 99% of the time.

4 Simulations

As mentioned in Section 2, the PDCCH messages are designed to be very robust. In particular, convolutional code with low rate (1/3) is used. In addition, the paging DCI message can have 24 - 44 bits. Together with a 16-bit CRC, the size of the message before convolutionally encoded ranges from 40 to 60 bits. Thus the size of the message after convolutionally encoded ranges from 120 to 180 bits. When the PDCCH size is 144 bits, puncture may occur during rate matching. When the PDCCH size is 288 bits, redundant encoded bits are transmitted, which effectively increases the SNR at the receiving UEs. In order to evaluate the effect of our embedded tags on the probability of successfully decoding the DCI, we first simulate the DCI decoding performance with respect to different SNR levels. The result is shown in Figure 4. Here we use the energy per bit to noise power spectral density (EbNo) as the metric for SNR. Also shown is BER of the PDCCH message at the same EbNo levels. Figure 4 gives us a clear intuition of the PDCCH BER requirements for various DCI decoding performances. For instance, with PDCCH size of 288 bits, we can see that the probability of unsuccessfully decoding a paging DCI decreases rapidly from 0.4 at EbNo = -1 to 10^{-5} at EbNo = 5. Thanks to the convolutional encoder, the BER requires for PDCCH to achieve 10^{-5} DCI error rate is only 0.03. When the size of PDCCH is 144 bits, the UEs need an additional 1dB in SNR to get equivalent performance.

Next we want to see the effect of allocating part of the transmission power to the tags on the PDCCH BER. As long as the resulting BER conforms to the requirement obtained above, our scheme will not have negative effect on the DCI decoding performance. Figure 5 shows the BER of PDCCH message for various tag powers. We can see that the effect of tag embedment is minimal for $\rho_t^2 \leq 0.02$. When the channel condition is good, e.g. EbNo = 10dB, 20% of the

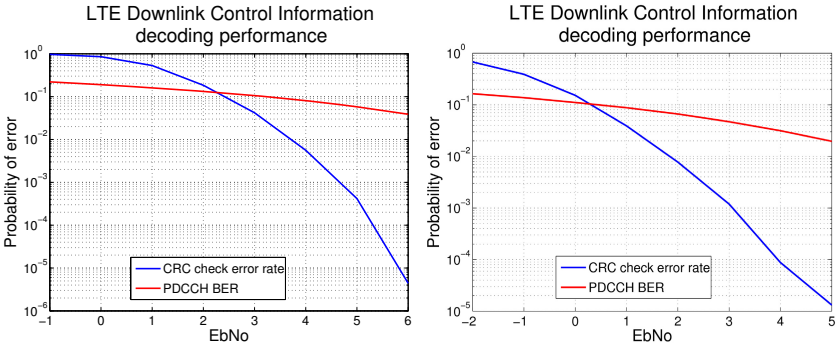

Fig. 4. DCI decoding performance as a function of SNR. Here the DCI size is 44 bits. The PDCCH size is (a) 144 bits, (b) 288 bits

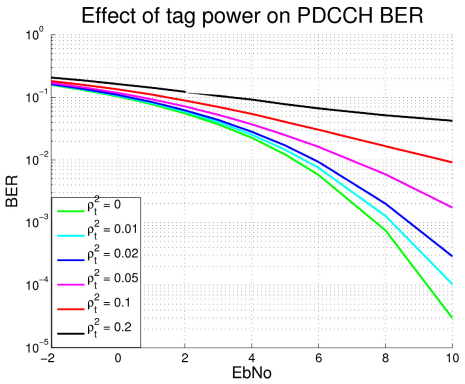

Fig. 5. PDCCH BER for various values of tag power allocation. Here the PDCCH size is 288 bits, 16 tags are embedded.

power can be allocated to tags, which results in BER of 0.04. Referring back to Figure 4, this BER corresponds to a DCI decoding error rate of 10^{-4}.

After confirming that we can indeed allocate part of the transmission power to the identification tags, we evaluate the tag detection performance under various system settings. In particular, we alter 3 parameters: tag length, tag power and number of simultaneous tags. We expect the detection performance to increase with tag length and decrease with number of simultaneous tags. Referring back to (18) and (20), we see that the variance of the test statistic decreases monotonically with increased tag power, and therefore the detection performance will increase monotonically with increased tag power. However, we also know that increasing tag power degrades DCI decoding performance. If that degradation causes the UEs to fail to decode the paging PDCCH then the tags will be useless. Referring to Figure 5, we choose tag power allocation $\rho_t^2 = 0.05$ to be conservative.

Figure 6 shows the probability of detecting that the unique tag for a UE is present in 2 cases: the UE is being paged, and the UE is not being paged (misdetection). We can see a clear superior performance when 288-bit PDCCH is used. Let us consider a rather bad channel condition, EbNo = 2dB, 4 UEs are paged simultaneously. Figure 6 shows that our scheme still provides tag detection rate of 90% and false alarm rate of 2% if we use 288-bit PDCCH and allocate 5% of the transmission power for the tags. A natural question would be how this performance compares to the current paging system's. Both schemes rely on the successful decoding of the paging PDCCH. After this stage, our scheme's performance ties directly to the detection probability of the tags; whereas the current scheme's performance depends on the success of decoding the paging PDSCH. Since these are apples and oranges, a meaningful comparison can only be done through experiments. We are certainly interested in pursuing them in our future work. For now, it is worth noticing that the constellation size and code rate used for data channels are a lot more aggressive than those used for control channels. Therefore it is expected that decoding performance of data channels are worse than that of control channels in the same SNR condition.

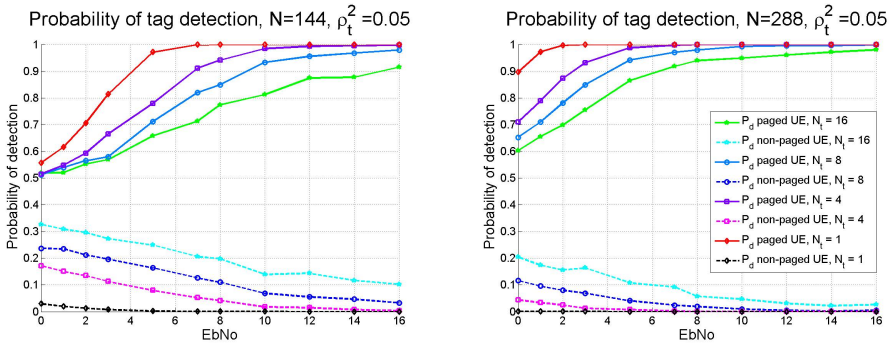

Fig. 6. Probability of tag detection for PDCCH size (a) 144 bits, (b) 288 bits

The idea behind the physical layer identification technique is to make use of channel noise to obfuscate the tags at the eavesdropper. Assuming that the eavesdropper, Eve in Figure 2(a), successfully decodes the paging PDCCH, regenerates the signal **s** in (1), and subtracts it from her received waveform. What she has left is the sum of the superimposed tags and the channel noise. Since the individual tags are modulated as QPSK symbols $\{\pm 1, \pm i\}$, the normalized sum of multiple tags will have the constellation as in Figure 7. The identity of a UE's tag, say Bob's, is hidden under 2 layers. First, the channel noise limits Eve to only partial information about the normalized sum of the tags. Second, since the tags are uncorrelated, the sum of them does not reveal any information about

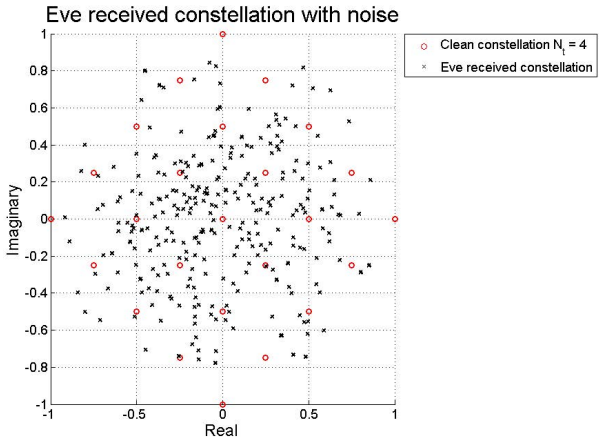

Fig. 7. Eavesdropper's received constellation at SNR = 20dB, $N_t = 4$

Bob's tag to Eve. We conclude that Eve has no reliable way of obtaining Bob's tag, and thus she cannot perform the location attack described in Section 1.

5 Conclusions

In this paper we have proposed a novel method to page user equipments in LTE network while protecting their privacy. The proposed method makes use of physical layer identification tags, which are designed to be robust and stealthy. Our scheme protects the privacy of paged users by hiding their ID in the transmitted waveforms. Using channel noise to our advantage, the scheme prevents an attacker from decoding the paged user's tag. As a result, attacks on the open nature of paging channel, e.g. [1], are no longer a threat. The scheme also provides bandwidth saving by not requiring the actual user IDs to be transmitted. Here we analyze our technique specifically for an LTE network; however, our technique is also applicable to other cellular networks such as GSM, WCDMA, WiMAX.

Acknowledgment. This material is based upon work partially supported by the Defense Advanced Research Projects Agency (DARPA) and the Semiconductor Research Corporation Focused Center Research Program through contract award number SA00007007, by the Army Research Office through MURI grant award W911-NF-0710287, by the AFOSR through MURI grant award FA9550-10-1-0573, and by the NSF through grant award CNS1018346.

Any opinions, findings and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of any of the funding agencies mentioned.

References

1. Kune, D.F., Koelndorfer, J., Hopper, N., Kim, Y.: Location leaks over the GSM air interface. In: Proc. 19th Annual Network and Distributed System Security Symposium (2012)
2. Yu, P., Baras, J.S., Sadler, B.: Physical-Layer Authentication. IEEE Trans. on Information Forensics and Security 3, 38–51 (2008)
3. Yu, P., Baras, J.S., Sadler, B.: Multicarrier authentication at the physical layer. In: WoWMoM (2008)
4. Nohl, K., Munaut, S.: GSM Sniffing, http://events.ccc.de/congress/2010/Fahrplan/attachments/1783_101228.27C3.GSM-Sniffing.Nohl_Munaut.pdf
5. F-Secure: 440,783 "Silent SMS" Used to Track German Suspects in 2010 (2010), http://www.f-secure.com/weblog/archives/00002294.html
6. 3GPP TS 36.211: Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation (version 10.4.0) (2011)
7. 3GPP TS 36.213: Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures (version 10.4.0) (2011)
8. 3GPP TS 36.321: Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC); Protocol specification (version 10.4.0) (2011)
9. 3GPP TS 36.331: Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification (version 10.4.0) (2011)
10. Baker, M., Moulsley, T.: Downlink Physical Data and Control Channels. In: LTE The UMTS Long Term Evolution, ch. 9, pp. 189–214 (2011)
11. Edfors, O., Sandell, M., van de Beek, J.J., Wilson, S.K., Borjesson, P.O.: OFDM channel estimation by singular value decomposition. IEEE Trans. on Communications 46, 931–939 (1998)
12. The OsmocomBB project - Open source GSM baseband software implementation, http://bb.osmocom.org/