An Opportunistic Power Control Scheme for Mitigating User Location Tracking Attacks in Cellular Networks

Inkyu Bang, *Member, IEEE*, Taehoon Kim, *Member, IEEE*, Han Seung Jang, *Member, IEEE*, and Dan Keun Sung, *Life Fellow, IEEE*

***Abstract*— Cellular networks have been successfully evolved over the decades. Especially, Long-Term Evolution (LTE) has been exceedingly successful and the security threats against LTE systems have increased rapidly. Particularly, *tracking* LTE user devices has been shown to be effective as the *temporary* user identifiers (IDs) are easily extracted and used to locate targeted devices by passive eavesdroppers. We notice that naive approaches, such as frequent updates of temporary user IDs, are *insufficient* to mitigate user-tracking attacks since the new and old temporary IDs for the same user device are easily *linkable* by adversaries who can measure the wireless channel characteristics between the user device and herself. In this paper, we propose an opportunistic uplink power control scheme to minimize the probability of successful user tracking by an adversary whose location is unknown. We devise the notion of average inference error probability in order to measure the level of users' location privacy. Moreover, we derive the closed-form expression of the approximated average inference error probability and formulate an optimization problem to maximize the average inference error probability under a constraint of an allowable power budget for each user. Against a passive adversary, our proposed power control scheme effectively degrades an adversary's inference ability by 50% when 10 users are scheduled in each transmission time slot, which will lead to almost 100% inference error at the adversary over multiple time slots.**

***Index Terms*— Physical-layer security, wireless network security, cellular networks, location privacy, power control, inference error probability.**

Manuscript received June 28, 2021; revised December 9, 2021; accepted January 15, 2022. Date of publication February 16, 2022; date of current version March 22, 2022. This work was supported by the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT (MSIT), Korea Government, under Grant 2020R1F1A1069934 and Grant 2021R1F1A1058795. An earlier version of this paper was presented in part at the 2021 IEEE International Conference on Communications (ICC), Montreal, Canada, June 2021 [DOI: 10.1109/ICC42927.2021.9500553]. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Stefano Tomasin. *(Corresponding authors: Taehoon Kim; Han Seung Jang.)*

Inkyu Bang is with the Department of Intelligent Media Engineering and the Department of Information and Communication Engineering, Hanbat National University, Daejeon 34158, South Korea (e-mail: ikbang@hanbat.ac.kr).

Taehoon Kim is with the Department of Computer Engineering, Hanbat National University, Daejeon 34158, South Korea (e-mail: thkim@hanbat.ac.kr).

Han Seung Jang is with the School of Electrical, Electronic Communication, and Computer Engineering, Chonnam National University, Yeosu-si, Jeollanam-do 59626, South Korea (e-mail: hsjang@jnu.ac.kr).

Dan Keun Sung is with the School of Electrical Engineering, College of Engineering, Korea Advanced Institute of Science and Technology (KAIST), Daejeon 34134, South Korea (e-mail: dksung@kaist.ac.kr).

Digital Object Identifier 10.1109/TIFS.2022.3152403

I. Introduction

MOBILE communication is one of the most important network access technologies for our modern society. Particularly, Long-Term Evolution (LTE) networks have become the worldwide de facto standard for mobile broadband; e.g., the penetration of LTE networks in developed countries is as high as 97.49% in South Korea and 90.32% in the USA as of February 2018. The huge success of LTE networks have attracted great attention from adversaries who aim to hijack telephone calls of targeted victims [1]–[3], block specific victim's calls and Internet access [4], [5], or create free calls and Internet connectivities [6]. Attacks on LTE networks are real; e.g., in March 2017, the Department of Homeland Security of the US has identified an unusually high amount of suspicious cell phone activity in the nation's capital, indicating potential hacking or tracking by foreign nations [7].

Particularly, *tracking* LTE user devices (e.g., smartphones) is a serious threat to users' location privacy, as the movements of these devices often accurately offer the trajectories of their users, revealing their life patterns or private information about them (e.g., religions, sexual or political orientations). In 2016, Shaik *et al.* demonstrate an attack that easily finds the cell (i.e., a geographic area covered by an LTE base station) in which a real-world user (e.g., Facebook account or mobile phone number) is currently located by exploiting the locality of LTE paging signals [4]. In addition, more fine-grained location analysis is investigated by Kumar *et al.* [8] by exploiting physical wireless channel characteristics of cellular signals.

We have observed that one of the main reasons why LTE devices are easily tracked by adversaries is that the LTE systems use several *temporary physical-layer identifiers (IDs)* to indicate LTE user devices (user equipments or *UEs*) and the IDs are easily extracted by any eavesdropper who is capable of sniffing the signals from targeted UEs and/or their LTE base station (or eNodeB) [4]. In other words, in the current LTE systems, for every uplink/downlink transmission, a unique physical-layer ID is sent in plaintext to identify a UE, which can be used to track any targeted UE in a cell. Worse yet, according to multiple studies [4], [8], [9], the physical-layer IDs of the UEs are often not changed for several hours, even days, which makes tracking attacks straightforward. Lots of previous studies [4], [8], [9] have explicitly (or implicitly)

mentioned that LTE operators should update the temporary IDs more frequently (e.g., every minute or second) so that UEs in a cell become indistinguishable by their physical-layer IDs. Yet, the effectiveness of the frequent physical-layer ID changes have not been evaluated or analyzed.

In this paper, we argue that frequent updates of physical-layer IDs are *insufficient* to mitigate tracking attacks since the new and old IDs for the same UE are easily *linkable* by passive adversaries who can simply measure the wireless channel characteristics (e.g., received signal strength) between the UE and herself. To that end, we propose a purely physical-layer based solution that dynamically controls the uplink transmit power of the UEs in order to confuse the passive adversaries and significantly limit their ability to distinguish UEs in a cell. The main insight and contributions of this paper can be summarized as follows[1]:

1) Proper *metrics* for measuring the level of user location privacy have not been extensively investigated in the literature. Accordingly, we devise a notion of an inference error probability.
2) In practice, it is difficult to know the location information of passive adversaries in advance. Thus, we consider a randomly distributed adversary and derive a closed-form of an upper bound of the inference error probability.
3) Dynamic power control can potentially degrade the uplink transmission rates, which creates undesired *trade-offs* between the level of privacy and the rate performance. Consequently, we formulate an optimization problem under a constraint of a minimum data rate requirement. We finally propose an opportunistic power control scheme to maximize the average inference error probability.

In the rest of the paper, we first introduce previous studies related to wireless network security, especially, focusing on location privacy in LTE networks (see Section II). Then, we briefly introduce our problem including an overview of our proposed solution and some challenges which we tackle (See Section III). We define the notion of average inference error probability to measure the level of location privacy of LTE users, in which we derive the tight approximation of average inference error probability as a closed-form expression (see Section IV). Based on our analytic result, we formulate an optimization problem to maximize the average inference error probability under a constraint of allowable power budget for each user. By solving the optimization problem, we propose a defense mechanism based on an opportunistic uplink power control scheme (see Section V). Through numerical simulations, we verify the effectiveness of our proposed scheme against the passive attack model (see Section VI). Further, we discuss practical aspects such as a powerful adversary model, user mobility pattern, and battery power drain issues (see Section VII). Finally, we provide conclusive remarks and discuss future work (See Section VIII). The notations used in this paper are summarized in Table I.

[1]Note that we are particularly focusing on security threats of tracking mobile devices in LTE systems but our contribution can provide an intuition to design a way of enhancing wireless security in the next-generation communication systems such as 5G and 6G.

TABLE I
LIST OF NOTATION

Notation	Description
N	The number of scheduled UEs in a single cell
$\mathcal{N}$	Set of scheduled user indexes, i.e., $\{1, \cdots, N\}$
$h_n(t)$	Channel fading coefficient from user n to adversary at time t
$w_n(t)$	Extra fading term independent of $h_n(t)$ for user n at time t
σ_n^2	Variance of channel coefficients for user n
ρ	Time-correlation factor of channel coefficients
$\hat{h}_n(t)$	Measured value of $h_n(t)$ at the adversary
$\hat{\sigma}_{n,t}^2$	Variance of $\hat{h}_n(t)$
η_0	Reference constant related to channel and device parameters
$P_{n,t}$	Uplink transmit power of user n at time t
r_n	Distance between the attacker and user n
α	Path-loss exponent
u	Index of the targeted user
$\mathcal{P}_e$	Inference error probability
$F_Y(\cdot)$	Cumulative distribution function of a random variable Y
$f_X(\cdot)$	Probability density function of a random variable X
$r_{\max}$	Maximum distance between a user and the adversary
$\mathbf{r}_n$	Random variable where its instance is r_n
$\bar{\mathcal{P}}_e$	Average inference error probability
$\hat{\mathcal{P}}_e$	Tight upper-bound of $\bar{\mathcal{P}}_e$
$g_u(t)$	Channel coefficient from user u to the base station at time t
N_0	Noise Variance
R_0	Data rate constraint of a user device
$P_{\text{tx}}^{\min}$	Minimum transmit power constraints of a user device
$P_{\text{tx}}^{\max}$	Maximum transmit power constraints of a user device

II. RELATED WORK

We study and discuss a set of wireless security research papers related to our work, especially, focusing on location privacy in LTE networks.

Even for the advent of the 5G era, still, LTE networks are the mainstream of cellular services in most of the world. LTE standards provide strong security features but commercial LTE networks reveal, in most cases, several security vulnerabilities due to misunderstandings in their configuration and implementation [10]. Accordingly, in recent years, specific security threats have been continuously uncovered in many studies: a passive identity mapping, website fingerprinting, domain name system (DNS) spoofing, and battery drain attacks [3], [4], [9], [11].

On the other hand, traditionally, location privacy in wireless networks has been one of main issues in security aspects, and thus, it has been extensively investigated through several papers [12]–[16]. Jiang *et al.* analyzed the problem of location privacy in wireless networks (Wi-Fi) and proposed a new protocol to improve location privacy by obfuscating location-related information (e.g., sender identity, signal

strength) [12]. Shokri *et al.* introduced a framework to measure the effectiveness of various location privacy protection mechanisms (LPPM) by formally quantifying the location privacy of mobile users [13]. Further, Shokri *et al.* formulated the mutual optimization of user-adversary objectives (i.e., location privacy vs. correctness of localization) based on Stackelberg Bayesian games, and proposed a user-centric LPPM [14]. In recent, Zhang *et al.* investigated a privacy-utility tradeoff focusing on a trace-level (i.e., a set of multiple locations) location-privacy, instead of a single location, based on an information-theoretic approach [15]. In addition, Oya *et al.* investigated the effect of outdated location-related information on LPPM designs [16].

Specifically, there are also several papers on the location-privacy in LTE networks. Kumar *et al.* proposed an open platform to monitor fine-grained spatial measurement on LTE signals using a notion of synthetic aperture radar (SAR) system [8]. Shaik *et al.* investigated several kinds of location information leakage attacks in LTE networks, including a rogue eNodeB-based active location attack with GPS-level accurate and a paging-based passive location attack which has a cell-level granularity (usually, less than 2 kilometers) [4]. Similarly, Jover analyzed the vulnerability of location leakage in LTE radio signals during the paging procedure [17]. Roth *et al.* investigated the vulnerability of the timing advance (TA) parameter used in LTE paging signal and estimated a possibility of location leakage with an accuracy of 40 meters when a TA-based attack and triangulation are exploited together [18]. Qi *et al.* also focused on location leakage in LTE signaling data and proposed a trajectory tracking system only using publically obtained LTE signals such as signaling data (e.g., TA value), which can be badly exploitable by an adversary [19].

Particularly, in [4] and [17]–[19], location leakage attacks in LTE networks were initiated by eavesdropping broadcast LTE signals and exploiting unintended relationships between LTE system parameters (e.g., paging and TA values). Jover suggested frequent updates of LTE users' physical-layer IDs to prevent location leakage from passive eavesdropping [17]. However, unfortunately, the frequent update of physical-layer IDs is a naive solution since the adversary can utilize signal strength to link frequently updated physical-layer IDs of the target user. Another approach to mitigate location leakage attacks in wireless systems such as LTE networks is to obfuscate the wireless signal itself (e.g., transmit power control or TPC) since the received signal strength is powerful evidence for the adversary to predict the location of the target. Accordingly, TPC-based solutions have been investigated from various aspects [20]–[22]. However, in this paper, we analyzed location privacy from the perspective of physical-layer of LTE systems and proposed the TPC-based solution, which has not been thoroughly investigated in previous studies.

III. Problem Definition

In this section, to specifically define our security problem, we first introduce an overview of LTE networks, describe the considered user location tracking attack in LTE networks, and briefly mention a basic idea of our proposed solution.

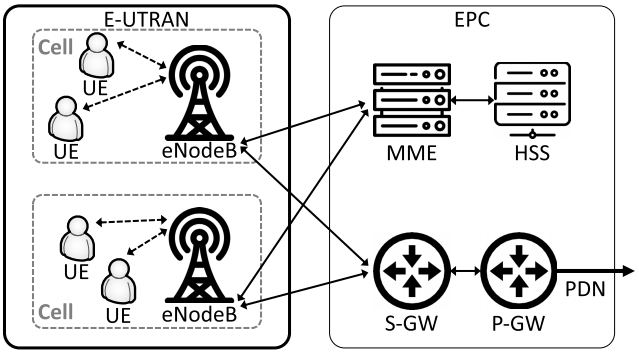


Fig. 1. Overall architecture of LTE network.

A. LTE Primer

Fig. 1 shows the architecture of LTE networks, which consist of the Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and the Evolved Packet Core (EPC). The E-UTRAN consists of mobile users (user equipments or UEs) and base stations (evolved NodeBs or eNodeBs) and provides the air interface between UE and eNodeB including the connection to the EPC. One eNodeB serves multiple UEs located in a certain geographical region classified as a term 'cell' and manages radio resource assignment among UEs. The Orthogonal Frequency Division Multiplexing (OFDM) is used at the physical layer of E-UTRAN, and a subcarrier and an OFDM symbol are the basic elements of the time-frequency radio resource. The EPC consists of several network elements such as the Serving Gateway (S-GW), the Packet Data Network Gateway (P-GW), the Mobility Management Entity (MME), and the Home Subscriber Server (HSS). The EPC is connected to Packet Data Network (PDN) through P-GW. The MME is the key control entity responsible for authentication, security, data connectivity, handover, and macro level of user location [23].

In LTE networks, downlink/uplink transmissions are carried over a number of different physical control and data channels as follows: physical downlink control channel (PDCCH), physical downlink shared channel (PDSCH), physical uplink control channel (PUCCH), and physical uplink shared channel (PUSCH). Particularly, the PDCCH channel carries the downlink control information such as resource allocation on downlink/uplink scheduling and paging notification. Interested readers may refer to [24] for detailed descriptions of all the LTE channels. It is worth noting that downlink control information is *public* to all UEs in the cell. Thus, any LTE receiver (even non-registered one) can decode all control data transmitted through PDCCH. Each registered UE can decode its own control message only by referring its own temporary unique physical layer identifier used between an eNodeB and the UE [25].

UEs in LTE networks interact with various entities in the network (e.g., eNodeBs or MMEs) and are assigned and use multiple different identifiers for each interaction [26], [27].

- **International Mobile Subscriber Identity (IMSI)**: IMSI is a permanent and unique number identifying a mobile subscriber associated with all cellular networks.

- **Temporary Mobile Subscriber Identity (TMSI)**: TMSI is a temporary ID for the MME to identify the UE in a certain tracking area.
- **Cell Radio Network Temporary Identifier (C-RNTI)**: C-RNTI is a physical layer ID issued by an eNodeB for uniquely identifying a UE in the cell.

The main purpose of using temporary IDs (e.g., TMSI and C-RNTI) is to avoid revealing the UE's permanent identifier (i.e., IMSI) to eavesdroppers. As such, temporary IDs are only valid in a certain area and time period. For example, a C-RNTI assigned to a UE changes when the UE moves to a new cell (handover) or re-accesses to the network from the idle-state (random access) [28].

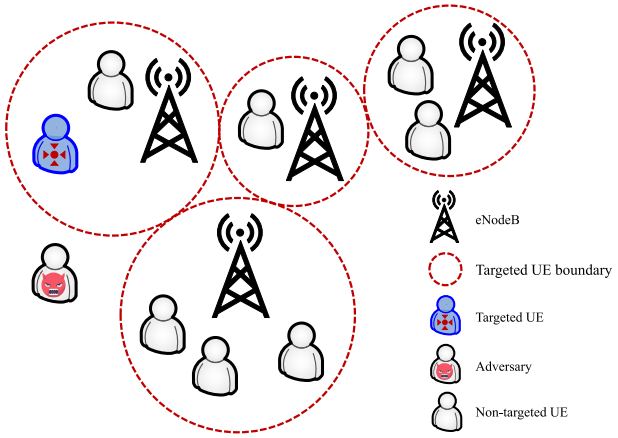
B. User Location Tracking Attack

Although temporary IDs (e.g., TMSI and C-RNTI) for UEs are designed to conceal the UEs' identification in LTE networks, unfortunately, those can be interpreted as hints for the locations of UEs. Most temporary IDs are used to uniquely distinguish a UE in a certain area. In addition, temporary IDs transmitted over the air are sent in clear or can be easily decoded. Thus, the locations of UEs can be easily tracked by sniffing LTE signals and mapping real-world identities and temporary IDs [4], [17].

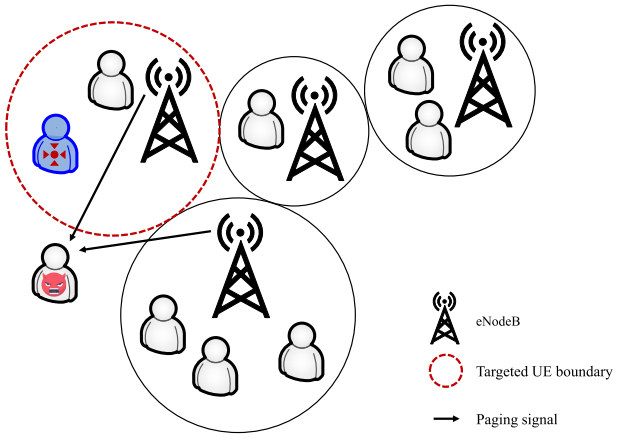
Intuitively, these kind of tracking attacks are mitigated by frequently changing UE's temporary ID to disturb mapping between UE's real-world identity and temporary ID [17]. However, frequent updates of temporary IDs are *insufficient* to mitigate tracking attacks since the newly created IDs for the same UE are easily *linkable* by passive adversary if she can use side information such as wireless channel characteristics (e.g., received signal strength).

In this paper, we consider a user location tracking attack in LTE networks, shortly, an ULT attack. The main objective of an adversary is to track the location of a targeted UE. We assume the following conditions for the adversary.

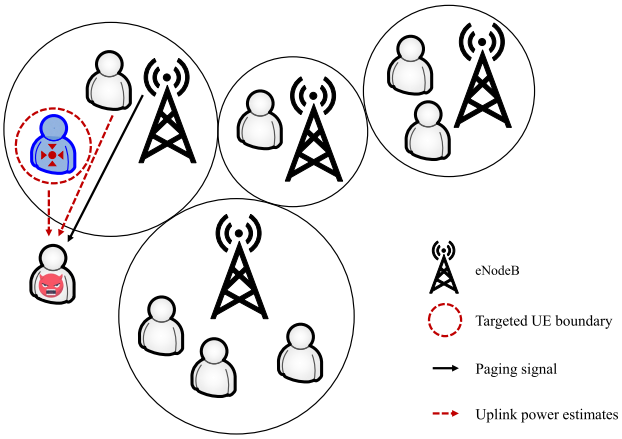
- The adversary is able to learn the location of the targeted UE at least in cell-level (more accurate than cell-level) since a random temporary physical layer ID contains the associated cell information and received signal power provides an estimated distance from the one.
- The adversary exploits a wireless passive sniffer that can overhear LTE signals transmitted over the air to obtain the targeted UE's random temporary ID and to estimate a distance from the targeted UE based on received power.
- We assume that mapping between the targeted UE's real-world identities (e.g., mobile phone number or Facebook account) and an initially assigned random temporary ID (C-RNTI) is available at the adversary based on conventional paging attack [4].



(a) Step 1: ready to eavesdrop LTE signals (targeted UE boundary: multiple cells)



(b) Step 2: sniffing LTE paging signals (targeted UE boundary: one specific cell)



(c) Step 3: measuring LTE uplink signals from multiple UEs (targeted UE boundary: one specific UE)

Fig. 2. A procedure of the ULT attack.

Fig. 2 briefly describes the overall procedures of the ULT attack. In the first step (Fig. 2a), an adversary is ready to eavesdrop LTE signals. The adversary does not have any information for the targeted UE yet. Thus, the targeted UE boundary would be very wide (e.g., an area covering multiple cells). In the second step (Fig. 2b), the adversary is able to narrow down the targeted UE boundary (e.g., one specific cell) by sniffing the paging signals from eNodeBs. In the third step (Fig. 2c), the adversary can utilize the measured uplink transmit power from multiple UEs in a single target cell to specify the location of the targeted UE.

Note that the adversary can exploit temporary ID mapping (i.e., C-RNTI) and uplink power measurement to track locations of the targeted UE. In Fig. 2, we do not explain details on

the ULT attack since the implementation of the ULT attack is not our main focus in this paper. Details of its implementation are described in several papers [4], [17]–[19] and thus we assume that the ULT attack is practical and feasible in LTE networks.

C. Solution Overview

A simple solution such as frequently updating temporary IDs cannot be applicable to the ULT attack that uses channel characteristics (i.e., measured uplink power) as side information. Thus, we need to investigate a fundamental solution using wireless physical channel characteristics rather than a naive approach such as frequent updates of temporary IDs.

We propose an opportunistic uplink power control scheme to disturb the passive adversary's correct inference for identifying the targeted UE based on channel characteristics, which significantly limit her ability to distinguish UEs in a cell. However, unfortunately, designing the power-control based mitigation against the ULT attack has a number of practical challenges, as shown in the list below.

- *Unknown adversary location:* UEs and eNodeBs do not know the location of passive adversaries in advance as their passive operations are hard to detect. This means that our defense design must be agnostic to adversary location and strategies.
- *Lack of metrics:* We do not have proper *metrics* for measuring the level of user location privacy in terms of associating dynamically changing physical-layer IDs.
- *Non-trivial performance-privacy trade-off:* Dynamic power control can potentially degrade the uplink transmission rates while limiting the effectiveness of UE tracking attacks. The clear performance-privacy *trade-offs* will arise and finding the right sweet spots for various cell environments (e.g., cell size, the number of active UEs) seems non-trivial.

In the subsequent sections, we address these challenges and demonstrate the effectiveness of our defense schemes.

IV. Inference Error Modeling

In this section, we introduce an inference error modeling to quantify the adversary's inference ability for mapping different temporary IDs (i.e., C-RNTI) of the same UE in order to keep tracking the location of the targeted UE in case of frequent update of C-RNTI.

A. System Model

As shown in Fig. 3, we consider a single cell LTE network which consists of one base station (eNodeB), one attacker, and N scheduled users (UE). We assume that each node is equipped with a single antenna. We consider a scenario where all users are uniformly distributed in a cell area and move at low mobility (≤ 3 km/h) in a straight street [29], [30].

Further, we assume a time-correlated Rayleigh block-fading channel [31]. Let $h_n(t) \in \mathbb{C}$ denotes the channel fading coefficient from user n to the attacker at time t for $n \in \mathcal{N} \triangleq \{1, \cdots, N\}$ and is assumed to be a complex Gaussian

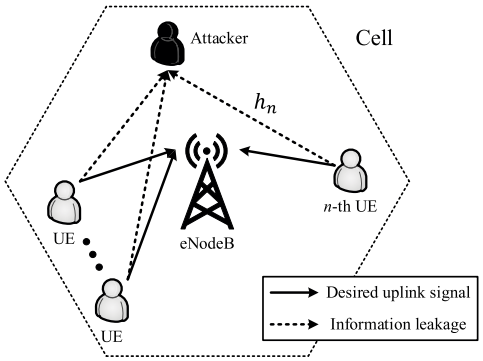


Fig. 3. A single cell LTE network with one attacker and N users.

random variable with zero mean and variance σ_n^2, i.e., $h_n(t) \sim \mathcal{CN}(0, \sigma_n^2)$. Then, the channel coefficient $h_n(t)$ is given by

$$h_n(t) = \rho^t h_n(0) + \sqrt{1-\rho^{2t}}\, w_n(t) \quad \text{for } t \geq 1, \tag{1}$$

where ρ and $w_n(t)$ denote the time-correlation factor and an extra fading term independent of $h_n(t)$. $w_n(t)$ is also assumed to follow a complex Gaussian distribution with zero mean and variance σ_n^2, i.e., $w_n(t) \sim \mathcal{CN}\left(0, \sigma_n^2\right)$. Note that $w_n(k)$ and $w_n(l)$ are independent of each other for all $k \neq l$.

Let $\hat{h}_n(t)$ denote the measured (or effective) channel coefficient at the adversary's device (e.g., universal software radio peripheral or USRP), which includes the effect of UE's transmit power. Note that, instead of a real channel coefficient (i.e., $h_n(t)$), only $\hat{h}_n(t)$ is available at the adversary, since she does not have any knowledge of the uplink transmit power for user n. The variance of the measured channel at the adversary for user n at time t (i.e., $\hat{\sigma}_{n,t}^2$) is affected by the uplink transmit power of user n. Then, the variance of the measured channel is expressed as follows:

$$\hat{\sigma}_{n,t}^2 = \frac{\eta_0 P_{n,t}}{r_n^\alpha}, \tag{2}$$

where η_0 is a reference constant related to channel and device parameters such as antenna gain and carrier frequency, $P_{n,t}$ is the uplink transmit power of user n at time t, r_n denotes the distance between the attacker and user n, and α is a path-loss exponent. Thus, we have $\hat{h}_n(t) \sim \mathcal{CN}\left(0, \hat{\sigma}_{n,t}^2\right)$. Throughout the paper, we assume $\eta_0 = 1$ for analytical tractability since inference error probability is expressed as the ratio of variances of the measured channel rather than variance itself.

In the ULT attack, the adversary exploits a power level of the uplink signals transmitted from UEs to specify and link different temporary IDs (i.e., C-RNTI) of the targeted UE. Thus, it is important for the adversary to keep monitoring the power level of the uplink signals transmitted from UEs, which experiences wireless fading channels.

In this paper, we mainly focus on a threat model where the adversary only observes the measured power levels at two different time slots and exploits this information to identify the targeted UE from multiple other UEs at the physical-layer. However, it is worth noting that our analysis from the current threat model assuming to exploit two different time slots is necessary in order to further analyze the powerful adversary case such that multiple measurements (i.e., power level) can be

exploitable together to identify the targeted UE. Further, a user mobility pattern becomes more important when we consider for the adversary to measure multiple power levels in time rather than to observe power levels at two different time slots. Accordingly, we additionally discuss the powerful adversary model as a separate topic in Section VII.

B. Inference Error Probability

For analytic tractability, we focus on two consecutive time intervals (e.g., subframes): t and $t+1$. Let u denote the index of the targeted user (UE).

The attacker can obtain all C-RNTIs at t and $t+1$ by decoding the PDCCH. However, the C-RNTIs at $t+1$ has to be correctly mapped with those at t to link C-RNTIs of user u. As discussed in Section III, linking the C-RNTIs of a certain user at t and $t+1$ is based on a similarity of the measured channel coefficients, including the effect of UE's transmit power. We define the similarity between two channel coefficients as a inverse of $\left\| \hat{h}_n(t+1) - \hat{h}_m(t) \right\|^2$ for $n, m \in \mathcal{N}$. The attacker is not able to correctly link different C-RNTIs of user u at time t and $t+1$ if the other user's channel characteristics (e.g., user n) at time $t+1$ is more correlated to that of user u. In other word, an inference error event occurs at the attacker if

$$\left\| \hat{h}_u(t+1) - \hat{h}_u(t) \right\|^2 \geq \left\| \hat{h}_n(t+1) - \hat{h}_u(t) \right\|^2. \quad (3)$$

Thus, the inference error probability, $\mathcal{P}_e$, is defined as follows:

$$\mathcal{P}_e \triangleq \Pr\left\{ \left\| \hat{h}_u(t+1) - \hat{h}_u(t) \right\|^2 \geq \min_{\forall n \in \mathcal{N}, n \neq u} \left\| \hat{h}_n(t+1) - \hat{h}_u(t) \right\|^2 \right\}. \quad (4)$$

Let us denote $X = \left\| \hat{h}_u(t+1) - \hat{h}_u(t) \right\|^2$, $Y_n = \left\| \hat{h}_n(t+1) - \hat{h}_u(t) \right\|^2$, and $Y_{\min} = \min_{\forall n \in \mathcal{N}, n \neq u} Y_n$ for notational simplicity. In order to obtain the closed-form expression of (4), we firstly need to derive the distributions of X, Y_n, and $Y_{\min}$. Since $\hat{h}_u(t)$ follows a complex Gaussian distribution, $\hat{h}_u(t+1) - \hat{h}_u(t)$ and $\hat{h}_n(t+1) - \hat{h}_u(t)$ also follow complex Gaussian distributions given by

$$\begin{aligned} \hat{h}_u(t+1) - \hat{h}_u(t) &\sim \mathcal{CN}\left(0, \sigma_x^2\right), \\ \hat{h}_n(t+1) - \hat{h}_u(t) &\sim \mathcal{CN}\left(0, \sigma_{y_n}^2\right) \quad \text{for } \forall n \neq u, \end{aligned} \quad (5)$$

where $\sigma_x^2 = \hat{\sigma}_{u,t+1}^2 + \hat{\sigma}_{u,t}^2 - 2\rho\hat{\sigma}_{u,t+1}\hat{\sigma}_{u,t}$ and $\sigma_{y_n}^2 = \hat{\sigma}_{n,t+1}^2 + \hat{\sigma}_{u,t}^2$. Thus, X and Y_n follow exponential distributions with mean of σ_x^2 and $\sigma_{y_n}^2$, respectively. Additionally, since $Y_{\min}$ is a minimum of $N-1$ independent exponential random variables with mean of $\sigma_{y_n}^2$, the cumulative distribution function (CDF) of $Y_{\min}$ is given by

$$F_{Y_{\min}}(y) = \begin{cases} 1 - \sum_{\forall n \in \mathcal{N}, n \neq u} e^{-\frac{y}{\sigma_{y_n}^2}} = 1 - e^{-\mu y}, & \text{if } y \geq 0, \\ 0, & \text{otherwise,} \end{cases} \quad (6)$$

where $\mu = \sum_{n \in \mathcal{N}, n \neq u} \frac{1}{\sigma_{y_n}^2}$.

Therefore, the inference error probability in (4) is obtained as follows [32]:

$$\begin{aligned} \mathcal{P}_e &\triangleq \Pr\left\{ X \geq \min_{\forall n \in \mathcal{N}, n \neq u} Y_n \right\} = \int_0^\infty F_{Y_{\min}}(y)\ f_X(y)\ dy \\ &= \int_0^\infty \left(1 - e^{-\mu y}\right) \frac{1}{\sigma_x^2} e^{-\frac{y}{\sigma_x^2}} dy = 1 - \frac{1}{1 + \sigma_x^2 \mu}, \end{aligned} \quad (7)$$

where $f_X(\cdot)$ denotes the probability density functions (PDF) of X, $F_{Y_{\min}}(\cdot)$ and μ are defined in (6).

Further, σ_x^2 in (5) can be rewritten as follows:

$$\begin{aligned} \sigma_x^2 &= \hat{\sigma}_{u,t+1}^2 + \hat{\sigma}_{u,t}^2 - 2\rho\hat{\sigma}_{u,t+1}\hat{\sigma}_{u,t} \\ &= r_u^{-\alpha}\left(P_{u,t+1} + P_{u,t} - 2\rho\sqrt{P_{u,t+1}P_{u,t}}\right) \\ &= r_u^{-\alpha} P_x, \end{aligned} \quad (8)$$

where $P_x = P_{u,t+1} + P_{u,t} - 2\rho\sqrt{P_{u,t+1}P_{u,t}}$.

Similarly, $\sigma_{y_n}^2$ in (5) is rewritten as follows:

$$\sigma_{y_n}^2 = \hat{\sigma}_{n,t+1}^2 + \hat{\sigma}_{u,t}^2 = r_n^{-\alpha} P_{n,t+1} + r_u^{-\alpha} P_{u,t}. \quad (9)$$

Using (8) and (9), (7) can be further derived and it is given by (10), as shown at the bottom of the next page.

Remark 1: The inference error probability in (10) *is a function of measured uplink transmit power and the distances between the attacker and users. Thus, we know that there exists an optimal power control strategy for maximizing the inference error probability. It will be analyzed in the next section. In addition, calculating* (10) *does not require the instantaneous channel state information of the attacker. However, the distances between the attacker and users (equivalent to the variance of the measured channel) are still required in the calculation, which is impossible to estimate since the attacker usually does not reveal its location. Therefore, we assume that the exact location of the attacker is not available but randomly (and uniformly) located in the cell.*

The uniform distribution of the attacker is equivalent to uniformly locate each user when the adversary is located at origin [33]. Let $r_{\max}$ denote the maximum distance between a user and the adversary, i.e., $r_n \in [0, r_{\max}]$ for $\forall n \in \mathcal{N}$. Here, we use $\mathbf{r}_n$ to indicate a random variable where its instance is r_n. Since each user is uniformly distributed in two-dimensional space, the PDF of $\mathbf{r}_n$ is obtained by using polar coordinates and it is given by $f_{\mathbf{r}_n}(r_n) = \frac{2r_n}{r_{\max}^2}$. The average inference error probability for user u is defined as (11), as shown at the bottom of the next page, where $F_{\mathbf{r}_n}(\cdot)$ denotes a CDF of $\mathbf{r}_n$. Unfortunately, it is difficult to obtain the exact closed-form expression of (11). Alternatively, we focus on the approximation of (11).

Theorem 1: For $\alpha = 2$, the tight upper-bound of $\bar{\mathcal{P}}_e$ in (11)*, i.e., $\hat{\mathcal{P}}_e$, is given by* (12)*, as shown at the bottom of the next page, where $P_x = P_{u,t+1} + P_{u,t} - 2\rho\sqrt{P_{u,t+1}P_{u,t}}$.*

Proof: Let $\hat{\mathcal{P}}_e$ denote the upper-bound of $\bar{\mathcal{P}}_e$. Then, the tight upper-bound of (11) is obtained by using Jensen's inequality and it is given by

$$\hat{\mathcal{P}}_e \triangleq 1 - \frac{1}{1 + \mathbb{E}\left[\sigma_x^2 \mu\right]} \geq \mathbb{E}\left[1 - \frac{1}{1 + \sigma_x^2 \mu}\right]. \quad (13)$$

In (13), $\mathbb{E}\left[\sigma_x^2 \mu\right]$ is calculated as follows:

$$\mathbb{E}\left[\sigma_x^2 \mu\right] = \sum_{n\in\mathcal{N}, n\neq u} \int_0^{r_{\max}} \cdots \int_0^{r_{\max}} \frac{\sigma_x^2}{\sigma_{y_n}^2} dF_{\mathbf{r}_1} \cdots dF_{\mathbf{r}_N}.$$

For analytical tractability, let us define $\psi(r_n)$ for user u as follows:

$$\psi(r_n) = \int_0^{r_{\max}} \frac{\sigma_x^2}{\sigma_{y_n}^2} dF_{\mathbf{r}_u}. \tag{14}$$

For $\alpha = 2$, $\psi(r_n)$ in (14) is obtained as follows:

$$\begin{aligned}\psi(r_n) &= \int_0^{r_{\max}} \frac{r_u^{-2} P_x}{r_n^{-2} P_{n,t+1} + r_u^{-2} P_{u,t}} \times \frac{2r_u}{r_{\max}^2} dr_u \\ &= \frac{r_n^2 P_x}{r_{\max} P_{n,t+1}} \log\left(\frac{r_{\max} P_{n,t+1} + r_n^2 P_{u,t}}{r_n^2 P_{u,t}}\right). \end{aligned} \tag{15}$$

Thus, $\mathbb{E}\left[\sigma_x^2 \mu\right]$ is rewritten by using $\psi(r_n)$ and it is given by

$$\mathbb{E}\left[\sigma_x^2 \mu\right] = \sum_{n\in\mathcal{N}, n\neq u} \int_0^{r_{\max}} \psi(r_n)\, dF_{\mathbf{r}_n}. \tag{16}$$

In (16), $\int_0^{r_{\max}} \psi(r_n)\, dF_{\mathbf{r}_n}$ is further reduced to

$$\begin{aligned}&\int_0^{r_{\max}} \psi(r_n)\, dF_{\mathbf{r}_n} \\ &= \frac{P_x}{2P_{n,t+1}} \left(\log\left(\frac{P_{n,t+1} + P_{u,t}}{P_{u,t}}\right) \right. \\ &\quad \left. + \frac{P_{n,t+1}}{P_{u,t}} - \frac{P_{n,t+1}^2}{P_{u,t}^2} \log\left(\frac{P_{n,t+1} + P_{u,t}}{P_{n,t+1}}\right)\right). \end{aligned} \tag{17}$$

Finally, $\hat{\mathcal{P}}_e$ is obtained by plugging (16) and (17) into (13). ■

Remark 2: Note that the gap between $\bar{\mathcal{P}}_e$ and $\hat{\mathcal{P}}_e$ results from Jensen's inequality in (13)*. Fortunately, the tightness of Jensen's gap has been extensively investigated in [34] and [35] and it is also applicable to our modeling in* (13)*. Accordingly, in this paper, we interchangeably use both terms "tight upper-bound" of $\bar{\mathcal{P}}_e$ and an "approximation" of $\bar{\mathcal{P}}_e$. Further, when we consider the optimization problem in the next section, we use $\hat{\mathcal{P}}_e$ instead of $\bar{\mathcal{P}}_e$ for analytical tractability.*

V. Defense Against the ULT Attack

In this section, we propose an opportunistic uplink power control scheme to prevent the attacker from linking the different C-RNTIs of the targeted UE against the ULT attack.

A. Optimization Problem

When we consider a defense scheme against the ULT attack, the main objective of the defense mechanism is to maximize the average inference error probability at the attacker. Here, we formulate an optimization problem to consider data rate and transmit power constraints. In addition, the defense scheme should be achievable in a distributed manner by each user. Thus, we consider an optimization problem from the perspective of the targeted user u and it is formulated as follows:

$$\underset{\mathbf{p}_u}{\text{maximize}}\ \hat{\mathcal{P}}_e \tag{18a}$$

$$\text{subject to}\ \log_2\left(1 + \frac{\|g_u(t)\|^2 P_{u,t}}{N_0}\right) \geq R_0, \tag{18b}$$

$$\log_2\left(1 + \frac{\|g_u(t+1)\|^2 P_{u,t+1}}{N_0}\right) \geq R_0, \tag{18c}$$

$$P_{\text{tx}}^{\min} \leq P_{u,t} \leq P_{\text{tx}}^{\max}, \tag{18d}$$

$$P_{\text{tx}}^{\min} \leq P_{u,t+1} \leq P_{\text{tx}}^{\max}, \tag{18e}$$

where $\hat{\mathcal{P}}_e$ is defined in (12), and $\mathbf{p}_u$ denotes a pair of transmit power at time t ant $t+1$ (i.e., $P_{u,t}$ and $P_{u,t+1}$), and $g_u(t)$

$$\begin{aligned}\mathcal{P}_e &= 1 - \frac{1}{1+\sigma_x^2\mu} \\ &= 1 - \frac{\prod_{\forall n\in\mathcal{N}, n\neq u} \left(r_n^{-\alpha} P_{n,t+1} + r_u^{-\alpha} P_{u,t}\right)}{\prod_{\forall n\in\mathcal{N}, n\neq u} \left(r_n^{-\alpha} P_{n,t+1} + r_u^{-\alpha} P_{u,t}\right) + \sum_{\forall n\in\mathcal{N}, n\neq u} r_u^{-\alpha} P_x \prod_{\forall m\in\mathcal{N}, m\neq u, m\neq n} \left(r_m^{-\alpha} P_{m,t+1} + r_u^{-\alpha} P_{u,t}\right)}. \end{aligned} \tag{10}$$

$$\begin{aligned}\bar{\mathcal{P}}_e &\triangleq \mathbb{E}\left[\mathcal{P}_e \mid \mathbf{r}_n, \forall n \in \mathcal{N}\right] = \mathbb{E}\left[1 - \frac{1}{1+\sigma_x^2\mu}\right] = \int_0^{r_{\max}} \cdots \int_0^{r_{\max}} 1 - \frac{1}{1+\sigma_x^2\mu} dF_{\mathbf{r}_1} \cdots dF_{\mathbf{r}_N} \\ &= \int_0^{r_{\max}} \cdots \int_0^{r_{\max}} \left(1 - \frac{1}{1+\sigma_x^2\mu}\right) f_{\mathbf{r}_1}(r_1) \cdots f_{\mathbf{r}_N}(r_N) dr_1 \cdots dr_N \\ &= \int_0^{r_{\max}} \cdots \int_0^{r_{\max}} \left(1 - \frac{1}{1 + \sum_{n\in\mathcal{N}, n\neq u} \frac{r_u^{-\alpha} P_x}{r_n^{-\alpha} P_{n,t+1} + r_u^{-\alpha} P_{u,t}}}\right) f_{\mathbf{r}_1}(r_1) \cdots f_{\mathbf{r}_N}(r_N) dr_1 \cdots dr_N, \end{aligned} \tag{11}$$

$$\hat{\mathcal{P}}_e = 1 - \frac{1}{1+\mathbb{E}\left[\sigma_x^2\mu\right]} = 1 - \frac{1}{1 + \sum_{n\in\mathcal{N}, n\neq u} \frac{P_x}{2P_{n,t+1}} \left(\log\left(\frac{P_{n,t+1}+P_{u,t}}{P_{u,t}}\right) + \frac{P_{n,t+1}}{P_{u,t}} - \frac{P_{n,t+1}^2}{P_{u,t}^2} \log\left(\frac{P_{n,t+1}+P_{u,t}}{P_{n,t+1}}\right)\right)}, \tag{12}$$

and N_0 represent the channel coefficient between user u and the base station at time t, and noise variance, respectively. In (18b) and (18c), we consider R_0 data rate constraint (i.e., minimum achievable rate at each time). In (18d) and (18e), $P_{\text{tx}}^{\min}$ and $P_{\text{tx}}^{\max}$ indicate the minimum and maximum transmit power constraints, respectively.

Note that we formulate the optimization problem in (18a) from the perspective of one specific user (i.e., the targeted user) during two time-intervals (i.e., t and $t+1$). Thus, solving the optimization problem in (18a) is to obtain an optimal $\mathbf{p}_u^\star$, which means that other users' parameters (i.e., $P_{n,t+1}$) are not optimization variables since we consider a distributed solution applicable to each user without any cooperation among users. In other words, we only need to determine $P_{u,t+1}^\star$ and $P_{u,t}^\star$. Fortunately, for given $P_{u,t}$, we can obtain $P_{u,t+1}^\star$, which will be discussed in the next subsection (Section V-B). Thus, if we properly set an initial value of $P_{u,0}$, then we can obtain a series of optimal values $(P_{u,1}^\star, P_{u,2}^\star, P_{u,3}^\star, \cdots)$ in the rest of the operation time.

B. Opportunistic Uplink Power Control Scheme

Now, we derive a near-optimal solution of (18a) and propose an opportunistic uplink power control scheme able to mitigate the ULT attack.

To solve the optimization problem in (18a), we first need to consider its feasibility. In (18b) and (18c), after some manipulations, we have the following inequalities:

$$\begin{aligned} P_{u,t} &\geq \frac{N_0}{\|g_u(t)\|^2}\left(2^{R_0}-1\right) \triangleq P_{r,t}, \\ P_{u,t+1} &\geq \frac{N_0}{\|g_u(t+1)\|^2}\left(2^{R_0}-1\right) \triangleq P_{r,t+1}, \end{aligned} \tag{19}$$

where we define $P_{r,t} = \frac{N_0}{\|g_u(t)\|^2}\left(2^{R_0}-1\right)$ and $P_{r,t+1} = \frac{N_0}{\|g_u(t+1)\|^2}\left(2^{R_0}-1\right)$ for notational simplicity.

Thus, the optimization problem in (18a) is feasible only if $P_{\text{tx}}^{\max} \geq \max\left\{P_{r,t}, P_{r,t+1}\right\}$. In this paper, we do not consider the infeasible case of (18a) since it means that the required data rate (i.e., R_0) cannot be achieved under a given power constraint.

Excluding the infeasible case of (18a), the optimization problem in (18a) is reduced to

$$\underset{\mathbf{p}_u}{\text{maximize}}\ \hat{\mathcal{P}}_e \tag{20a}$$

$$\text{subject to}\ P_{\Delta,t} \leq P_{u,t} \leq P_{\text{tx}}^{\max}, \tag{20b}$$

$$P_{\Delta,t+1} \leq P_{u,t+1} \leq P_{\text{tx}}^{\max}, \tag{20c}$$

where $\hat{\mathcal{P}}_e$ is defined in (12), and $P_{\Delta,t} = \max\left\{P_{\text{tx}}^{\min}, P_{r,t}\right\}$ and $P_{\Delta,t+1} = \max\left\{P_{\text{tx}}^{\min}, P_{r,t+1}\right\}$.

Theorem 2: For given $\rho > 0$, $g_u(t)$, $g_u(t+1)$, R_0, and $P_{u,t}$, $P_{u,t+1}^\star$ in (20) is determined as follows:

$$P_{u,t+1}^\star = \begin{cases} P_{tx}^{max} & \text{if } \left(\dfrac{\sqrt{P_{tx}^{max}}+\sqrt{P_{\Delta,t+1}}}{2\rho}\right)^2 > P_{u,t}, \\ P_{\Delta,t+1} & \text{otherwise}, \end{cases} \tag{21}$$

where $P_{\Delta,t+1} = \max\left\{P_{tx}^{min}, \frac{N_0}{\|g_u(t+1)\|^2}\left(2^{R_0}-1\right)\right\}$.

Proof: In order to maximize the approximation of average inference error probability in (12), the term $\mathbb{E}\left[\sigma_x^2\mu\right]$ has to be maximized. $\mathbb{E}\left[\sigma_x^2\mu\right]$ is a function of $P_{u,t}$ and $P_{u,t+1}$.

Let β denote the difference between $P_{u,t}$ and $P_{u,t+1}$, i.e., $P_{u,t+1} = P_{u,t} + \beta, \beta \in \left[\beta^{\min}, \beta^{\max}\right]$ where $P_{u,t} + \beta^{\max} = P_{\text{tx}}^{\max}$ and $P_{u,t} + \beta^{\min} = P_{\Delta,t+1}$. Then, $\mathbb{E}\left[\sigma_x^2\mu\right]$ is a function of β since a value of $P_{u,t}$ is given. Using (16), (17), and β, $\mathbb{E}\left[\sigma_x^2\mu\right]$ can be a rewritten as follows:

$$\begin{aligned} f(\beta) &= \mathbb{E}\left[\sigma_x^2\mu\right] \\ &= \sum_{n\in\mathcal{N}, n\neq u}\left(2P_{u,t}+\beta-2\rho\sqrt{P_{u,t}^2+\beta P_{u,t}}\right)\Psi_n \\ &= \left(2P_{u,t}+\beta-2\rho\sqrt{P_{u,t}^2+\beta P_{u,t}}\right)\sum_{n\in\mathcal{N}, n\neq u}\Psi_n \\ &= \left(2P_{u,t}+\beta-2\rho\sqrt{P_{u,t}^2+\beta P_{u,t}}\right)\Phi_u, \end{aligned} \tag{22}$$

where Ψ_n denotes a constant given by the whole terms in (17) except for $P_x = 2P_{u,t}+\beta-2\rho\sqrt{P_{u,t}^2+\beta P_{u,t}}$ and it is expressed as $\Psi_n = \frac{1}{2P_{n,t+1}}\times\log\left(1+\frac{P_{n,t+1}}{P_{u,t}}\right)+\frac{1}{2P_{n,t+1}}\times\frac{P_{n,t+1}}{P_{u,t}}-\frac{1}{2P_{n,t+1}}\times\frac{P_{n,t+1}^2}{P_{u,t}^2}\log\left(1+\frac{P_{u,t}}{P_{n,t+1}}\right)$, and $\Phi_u = \sum_{n\in\mathcal{N}, n\neq u}\Psi_n$ for notational simplicity.

Now, we will show $f(\beta)$ is a convex function when $\rho > 0$. The second order derivative of $f(\beta)$ is given by

$$f''(\beta) = \frac{d^2 f(\beta)}{d\beta^2} = \frac{\rho P_{u,t}^2}{\left(P_{u,t}^2+\beta P_{u,t}\right)^{\frac{3}{2}}}\Phi_u. \tag{23}$$

In (23), $\Phi_u = \sum_{n\in\mathcal{N}, n\neq u}\Psi_n \geq 0$ due to $\Psi_n \geq 0, \forall n$, and it is proved as follows:

$$\begin{aligned} \Psi_n &= \frac{1}{2P_{n,t+1}}\times\log\left(1+\frac{P_{n,t+1}}{P_{u,t}}\right) \\ &\quad+\frac{1}{2P_{n,t+1}}\left(\frac{P_{n,t+1}}{P_{u,t}}-\frac{P_{n,t+1}^2}{P_{u,t}^2}\log\left(1+\frac{P_{u,t}}{P_{n,t+1}}\right)\right) \\ &\geq \left(\frac{1}{2P_{n,t+1}}\right)\left(\frac{P_{n,t+1}}{P_{u,t}}-\left(\frac{P_{n,t+1}}{P_{u,t}}\right)^2\log\left(1+\frac{P_{u,t}}{P_{n,t+1}}\right)\right) \\ &\geq 0, \end{aligned}$$

where the first inequality holds since $P_{n,t+1} > 0$, $P_{u,t} > 0$, and the first term $\frac{1}{2P_{n,t+1}}\times\log\left(1+\frac{P_{n,t+1}}{P_{u,t}}\right) \geq 0$. The second inequality holds since $\frac{1}{2P_{n,t+1}} > 0$ and the term $\frac{P_{n,t+1}}{P_{u,t}} - \left(\frac{P_{n,t+1}}{P_{u,t}}\right)^2\log\left(1+\frac{P_{u,t}}{P_{n,t+1}}\right)$ is a form of $\frac{1}{x}-\frac{1}{x^2}\log(1+x)$ where $x = \frac{P_{u,t}}{P_{n,t+1}} > 0$ and it is always greater than or equal to 0 for $x > 0$.

Thus, $f''(\beta) \geq 0$ and $f(\beta)$ is a convex function. According to the convex optimization theory [36], a maximum value of a convex function defined in an interval is determined at one of the boundary points. Therefore, $f(\beta)$ is maximized when $\beta = \beta^{\max}$ or $\beta = \beta^{\min}$.

Note that we need to determine an optimal $P_{u,t+1}^\star$ that maximizes $\mathbb{E}\left[\sigma_x^2\mu\right] = f(\beta)$. Thus, $P_{u,t+1}^\star = P_{u,t} + \beta^{\max} = P_{\text{tx}}^{\max}$ if $f(\beta^{\max}) > f(\beta^{\min})$. Otherwise,

$P^{\star}_{u,t+1} = P_{u,t} + \beta^{\min} = P_{\Delta,t+1}$. The condition $f(\beta^{\max}) > f(\beta^{\min})$ determines whether $P^{\star}_{u,t+1}$ is set to $P^{\max}_{\text{tx}}$ or $P_{\Delta,t+1}$ and it is reduced as follows:

$$\begin{aligned} f(\beta^{\max}) &= \left(2P_{u,t} + \beta^{\max} - 2\rho\sqrt{P^2_{u,t} + \beta^{\max}P_{u,t}}\right)\Phi_u \\ &= \left(P_{u,t} + P^{\max}_{\text{tx}} - 2\rho\sqrt{P_{u,t}P^{\max}_{\text{tx}}}\right)\Phi_u \\ &> \left(P_{u,t} + P_{\Delta,t+1} - 2\rho\sqrt{P_{u,t}P_{\Delta,t+1}}\right)\Phi_u \\ &= f(\beta^{\min}) \\ &\iff \left(\frac{\sqrt{P^{\max}_{\text{tx}}} + \sqrt{P_{\Delta,t+1}}}{2\rho}\right)^2 > P_{u,t}. \end{aligned}$$

Finally, we derive $P^{\star}_{u,t+1} = P^{\max}_{\text{tx}}$ if $\left(\frac{\sqrt{P^{\max}_{\text{tx}}}+\sqrt{P_{\Delta,t+1}}}{2\rho}\right)^2 > P_{u,t}$ and $P^{\star}_{u,t+1} = P_{\Delta,t+1}$ in other case, which completes the proof. ∎

Remark 3: Theorem 2 indicates that each user has to alternatively change his/her transmit power between given power budget boundaries (i.e., $P_{\Delta,t+1}$ and P^{max}_{tx}) when we consider low mobility ($\leq$ 3 km/h, i.e., $\rho \approx 1$)[2] and time-sequential optimal values of $P_{u,t+1}$. For example, if $P_{u,0}$ is properly set, $P^{\star}_{u,1} = P^{max}_{tx}$, $P^{\star}_{u,2} = P_{\Delta,2}$, $P^{\star}_{u,3} = P^{max}_{tx}$, $P^{\star}_{u,4} = P_{\Delta,4}, \cdots$.

Interestingly, Remark 3 supports our intuition that, if any cooperation among users and information for the attacker's location are not available, the best effort of each user for disturbing the attacker is to make a big power fluctuation. Further, we verify the result of Theorem 2 and our intuition through simulations in the next section (Section VI).

Algorithm 1 describes our proposed opportunistic uplink power control (OUPC) scheme to mitigate ULT attack. Note that the OUPC scheme does not require other users' parameters such as channel information (e.g., $g_n(t), \forall n \neq u$). Thus, the OUPC scheme can be employed in distributed manner by each user.

VI. Performance Evaluation

In this section, we first verify the feasibility of Theorem 2 by searching all combinations of transmit power in two consecutive time slots. Then, we show the performance of the proposed defense scheme against ULT attack. For comparison, we consider two power control schemes for references: fixed power control (FPC) and random power control (RPC) schemes, which will be explained in Section VI-B. We use MATLAB version 9.10.0 (R2021a) [37] to obtain both analytical results in (12) and simulation results for given parameters. Simulation parameters are listed in Table II. We perform simulations with 100,000 iterations to calculate the average inference error probability.

[2]Note that the time correlation factor ρ is determined by a function of $J_0\left(2\pi f_c \tau \upsilon c^{-1}\right)$ where $J_0(\cdot)$ denotes the zero-th order Bessel function of the first kind, f_c is the carrier frequency, τ is the duration of time slot, υ is the speed of UE, and c is the speed of light [23]. Further, the ρ value is approximated to $0.999 \approx 1$ if we consider LTE system parameters such as $\tau = 1$ ms and $f_c = 2.6$ GHz.

Algorithm 1 Opportunistic Uplink Power Control Scheme

Input: ρ, $\{g_u(0), g_u(1), \cdots, g_u(t)\}$, R_0, $P^{\min}_{\text{tx}}$, and $P^{\max}_{\text{tx}}$
Output: $\left\{P^{\star}_{u,0}, P^{\star}_{u,1}, \cdots, P^{\star}_{u,t}\right\}$

```
for k ← 1 to t do
    P_{Δ,k} ← max{ P^min_tx, (N_0 / ||g_u(k)||^2)(2^{R_0} − 1) }
    if k = 0 then
        P*_{u,k} ← randomly select P_{Δ,0} or P^max_tx
    else
        if ( (√P^max_tx + √P_{Δ,k}) / (2ρ) )^2 > P*_{u,k−1} then
            P*_{u,k} ← P^max_tx
        else
            P*_{u,k} ← P_{Δ,k}
        end if
    end if
end for
```

TABLE II
Simulation Parameters and Values

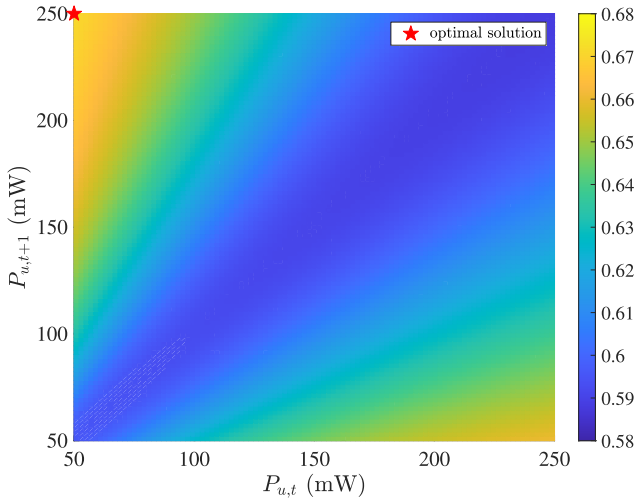
Parameter	Value
$P^{\min}_{\text{tx}}$ (mW)	$\{50, 150\}$
$P^{\max}_{\text{tx}}$ (mW)	$\{150, 250\}$
N	$\{5, 10, 20, 30, 40, 50, 60, 70, 80, 90, 100\}$
$r_{\max}$ (m)	500
α	4
R_0 (bps/Hz)	1.0
ρ	$\{0.80, 0.85, 0.90, 0.95, 0.96, 0.97.0.98, 0.99, 0.999\}$

A. Feasibility of Theorem 2

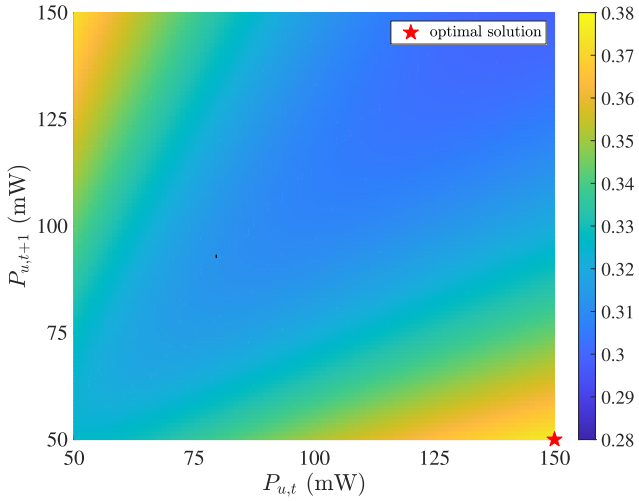
Fig. 4 shows average inference error probability, defined in (10), of the proposed defense scheme for all combinations of $P_{u,t}$ and $P_{u,t+1}$. For system parameters, we consider two cases as shown in Fig. 4a and Fig. 4b. For both cases, a time-correlation factor ρ is set to 0.999 corresponding to low mobility (i.e., 3 km/h), and $P_{\Delta,t+1} = P_{\Delta,t} = P^{\min}_{\text{tx}}$ is assumed for simplicity. Fig. 4a shows the result of a user (indexed by u) when $P^{\min}_{\text{tx}} = 50$ mW, $P^{\max}_{\text{tx}} = 250$ mW and $N = 10$. The average inference error probability increases when a gap between $P_{u,t}$ and $P_{u,t+1}$ (i.e., $|P_{u,t+1} - P_{u,t}|$) increases. As we discussed in Theorem 2, an optimal solution (the largest value of the average inference error probability, indicated by star-shaped red marker) is achieved when $P_{u,t} = P^{\min}_{\text{tx}}$ and $P_{u,t+1} = P^{\max}_{\text{tx}}$. Similarly, Fig. 4b shows the result of user u when $P^{\min}_{\text{tx}} = 50$ mW, $P^{\max}_{\text{tx}} = 150$ mW and $N = 5$. An optimal solution is achieved when $P_{u,t} = P^{\max}_{\text{tx}}$ and $P_{u,t+1} = P^{\min}_{\text{tx}}$. Thus, as discussed in Remark 3, alternatively changing transmit power $P^{\max}_{\text{tx}}$ and $P^{\min}_{\text{tx}}$ (equivalently $P_{\Delta,t+1}$) after choosing an initial value as in Algorithm 1 can be one of the most effective mitigation against ULT attack.

B. Numerical Results

We evaluate the performance of our proposed defense scheme in terms of the average inference error probability

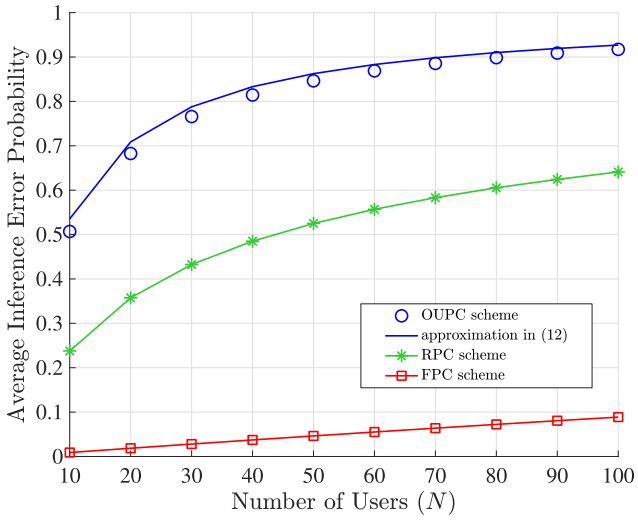


(a) $P_{\text{tx}}^{\min} = 50$ mW, $P_{\text{tx}}^{\max} = 250$ mW and $N = 10$

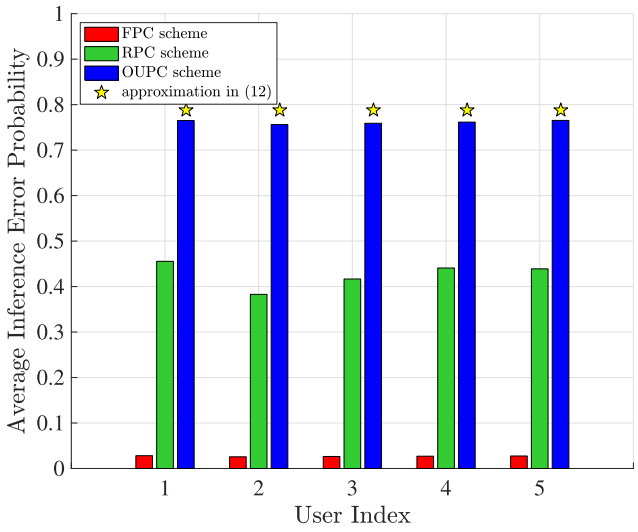


(b) $P_{\text{tx}}^{\min} = 50$ mW, $P_{\text{tx}}^{\max} = 150$ mW and $N = 5$

Fig. 4. Average inference error probability of the proposed defense scheme for all combinations of $P_{u,t}$ and $P_{u,t+1}$.



(a) Average result for all users

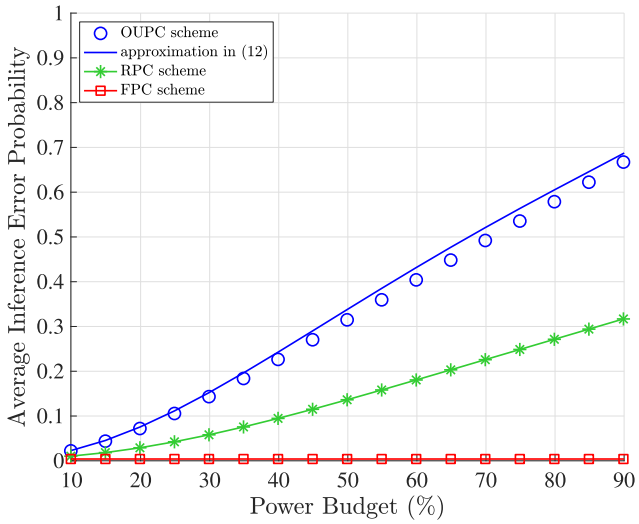


(b) Individual result for selected five users ($N = 30$)

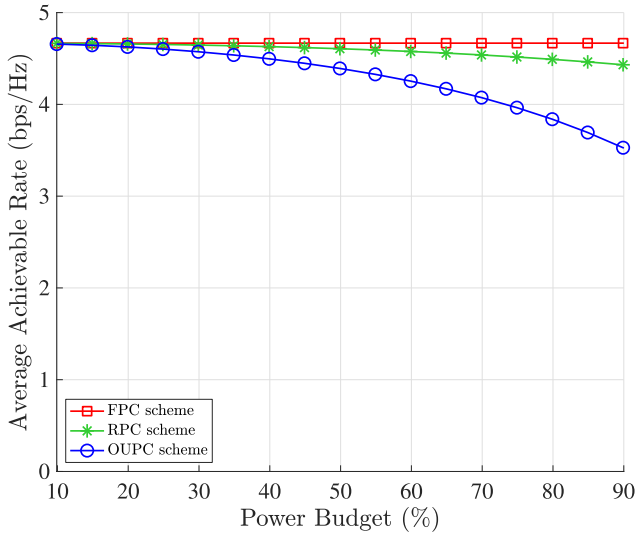
Fig. 5. Average inference error probability for varying the number of users where $P_{\text{tx}}^{\min} = 50$ mW and $P_{\text{tx}}^{\max} = 150$ mW.

measured between two consecutive time slots. OUPC scheme indicates our proposed scheme that controls uplink transmit power as in Algorithm 1. FPC scheme is to transmit the constant uplink power (e.g., maximum power) at each time slot. RPC scheme is that each device randomly selects its transmit power within an allowable power budget. For a fair comparison, we consider the same power consumption in average over multiple time slots. For example, if the OUPC scheme consumes 100 mW at $t = 1$ and 200 mW at $t = 2$, the FPC scheme consumes 150 mW at both time slots. For default system parameters, we set $R_0 = 1.0$ bps/Hz and a channel time-correlation factor ρ as 0.999 which corresponds to low mobility environments (3 km/h) for all users. We consider that user devices and an attacker are randomly located in a cell with a radius of 0.5 km. Note that we consider a data requirement constraint (i.e., R_0) only when we observe an outage probability defined as a probability that a given data rate is not supported.

Fig. 5 shows the average inference error probability for varying the number of users in the system when we consider $P_{\text{tx}}^{\min} = 50$ mW and $P_{\text{tx}}^{\max} = 150$ mW. Through simulations, we verify our analytical result for the approximation in (12), indicated by blue line in Fig. 5a and star-shaped marker in Fig. 5b, respectively. In Fig. 5a, the average inference error probabilities of all schemes increase as the number of users increases since the attacker is more confused to track the location of one specific user when a large number of active users exist in the system. The FPC scheme shows very low inference error probability even for $N = 100$ while the OUPC scheme shows the best performance for all ranges. The RPC scheme shows moderate performance since it does not fully utilize its power budget at each time slot. In detail, the OUPC scheme effectively degrades an adversary's inference ability by 50% when we consider 10 active users whereas FPC causes only 1% interference error. Fig. 5b shows the average inference error probability of five users randomly selected when we consider $N = 30$. From the perspective of each user, a certain level of the average inference error probability has to be guaranteed since we do not know which user is targeted by



(a) Average inference error probability for varying the power budget



(b) Average achievable rate for varying the power budget

Fig. 6. Comparison between average inference error probability and average achievable rate for varying the power budget when $N = 5$.

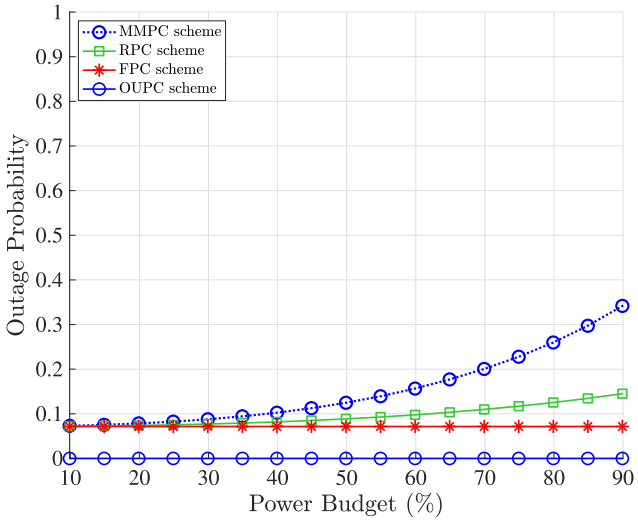


Fig. 7. Outage probability for varying the power budget when $R_0 = 1.0$ bps/Hz and $N = 5$.

the attacker. The OUPC scheme shows the best performance even for considering each user separately and its performance gap achieved by each user is negligible. In other words, the OUPC scheme ensures almost the same average inference error probability of the attacker for any user.

Fig. 6 compares the average inference error probability (Fig. 6a) and the average achievable rate (Fig. 6b) for varying the power budget when $N = 5$. We define the power budget as an adjustable power range based on the average transmit power set to 100 mW. For example, 30% power budget indicates that $P_{\text{tx}}^{\min} = (1 - 0.3) \times 100 = 70$ mW and $P_{\text{tx}}^{\max} = (1 + 0.3) \times 100 = 130$ mW for all schemes. Fig. 6a shows the average inference error probability for varying the power budget when $N = 5$. As discussed in Section VI-A, the average inference error probabilities increase for all schemes when the power budget increases. The OUPC scheme always shows the best performance, since it fully utilizes the range of $P_{\text{tx}}^{\min}$ mW and $P_{\text{tx}}^{\max}$ for a given power budget whereas other schemes do not. Fig. 6b shows the average achievable rate for varying the power budget when $N = 5$. Instead of the target data rate $R_0 = 1.0$ bps/Hz, we evaluate the average achievable rate when each power control scheme is employed. Clearly, there is a trade-off between achieving security (inference probability) and enhancing performance (achievable rate). Thus, performance loss in terms of data rate is inevitable when the OUPC scheme is employed. However, it is worth noting that the OUPC scheme achieves much larger gain in security (average inference error probability, 0.40% $\rightarrow$ 66.73% at power budget 90%) but relatively less loss in performance (average achievable rate, 4.667 bps/Hz $\rightarrow$ 3.528 bps/Hz at power budget 90%), compared with the FPC scheme.

Fig. 7 depicts the outage probabilities, also an important system requirement in addition to the average achievable rate, for varying the power budget. An outage event occurs when a user's data rate is less than a data rate requirement (i.e., $R_0 = 1.0$ bps/Hz). To clearly observe the effect of the data rate requirement constraint, we newly consider a max-min power control (MMPC) scheme that changes transmit power alternatively between $P_{\text{tx}}^{\max}$ and $P_{\text{tx}}^{\min}$, similarly following a principle of Algorithm 1. Here, we consider the proposed OUPC scheme with the data rate constraint. All the reference schemes (MMPC, FPC, RPC) do not guarantee the data rate requirement and thus cause communication outages. Further, outage probabilities increase when the power budget increases due to the decrease of $P_{\text{tx}}^{\min}$ for MMPC and RPC schemes. On the other hand, the OUPC scheme is designed to adjust user's minimum power to carefully take the data requirement into account and thus can achieve zero outage probability.

Fig. 8 shows the average inference error probability for varying the channel time-correlation factor when $N = 5$. The time-correlation factor is determined by several parameters in the system such as the speed of the device, carrier frequency, and time slot duration, and it is given by $\rho = J_0\left(2\pi f_c \tau \upsilon c^{-1}\right)$ where $J_0(\cdot)$ denotes the zero-th order Bessel function of the first kind, f_c is the carrier frequency, τ is the time duration between two sampling instances, υ is the speed of the device,

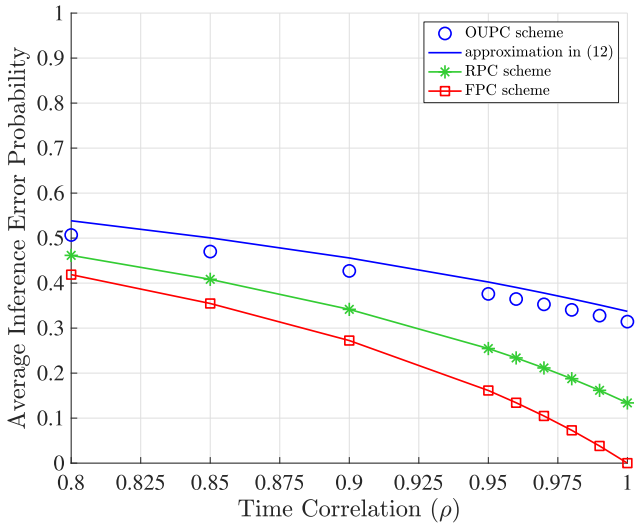


Fig. 8. Average inference error probability for varying the channel time-correlation when $N = 5$.

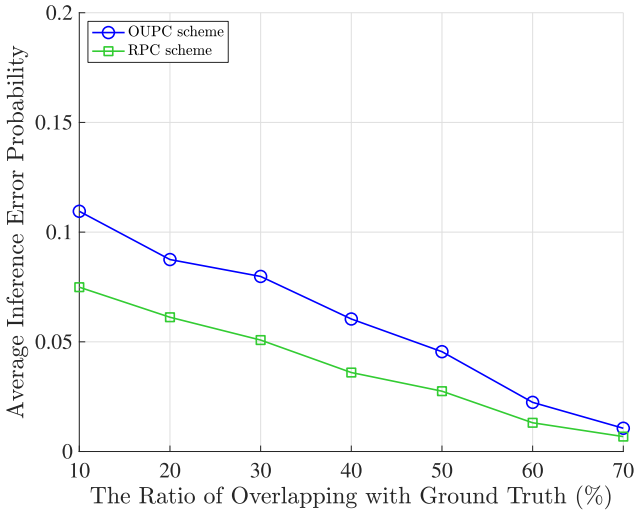


Fig. 9. Average inference error probability for powerful adversary model and $N = 2$.

and c is the speed of light [23]. We consider $f_c = 2.6$ GHz and $\tau = 1$ ms. Accordingly, the ρ values of 0.999, 0.95, and 0.8 correspond to 3 km/h, 30 km/h, and 60 km/h, respectively. For all schemes, the average inference error probabilities decrease as the channel time-correlation increases since it is more difficult for the attacker to track the location of users who move faster. When the channel time-correlation varies from 0.8 to 0.999 (≈ 1), the average inference error probability of the OUPC scheme decreases from 0.5069 to 0.3144 but that of the FPC schemes decreases from 0.4188 to 0, respectively. Thus, the OUPC scheme is robust to the variation of the channel time-correlation factor, compared with other schemes, which indicates that our proposed scheme can be easily employed independent of system parameters and environment.

VII. Discussion

In this section, we additionally discuss practical aspects such as a powerful adversary model and battery power drain issues.

A. Powerful Adversary Model

Throughout the paper, we have mainly focused on the adversary only exploiting the measured power levels at two different time slots. However, the measured power levels at multiple time slots help the adversary to track the targeted UE. Accordingly, a more powerful adversary model assuming to collect the measured power levels at multiple time slots and to exploit them together for the attack needs to be investigated. It is worth noting that a principle of alternatively changing between high and low transmit power is still effective when we consider a more powerful adversary model.

Fig. 9 shows the average inference error probability when we consider only two UEs and the powerful adversary model. Here, we generate a measured power profile for each UE, which includes the effect of power control schemes and distance between adversary and UE. We assume that UEs and the adversary are located at (-100,0), (100,0), and (0,75) in the two-dimension area (unit: meter), respectively. The targeted UE is moving toward the adversary on the x-axis and another UE is moving away from the adversary on the x-axis. They are moving at 3 km/h and the adversary observes measured power for 1 minute. Then, the adversary tries to determine whether which power profile is for the targeted one when the ground truth power profile is given. We further assume that a certain ratio of ground truth power profile is overlapped with the newly measured power profile (only for the targeted one). Although we only consider two UEs and assume a certain ratio of overlapping between new measures and ground truth, the proposed scheme can still make the adversary confused in a certain probability. Further, we should carefully consider a specific user mobility pattern and a notion of mix-zone [38], [39] to design more securely effective power control mechanisms against more complicated user tracking attacks, which remains for further work.

B. Battery Power Drain

One can concern about the power draining issue of using our proposed scheme since the proposed scheme changes transmit power alternatively between extremely high and low within the power budget. Fortunately, this issue can be mitigated if we carefully design the operation of battery charging.

To the best of our knowledge, an extreme power cycling pattern in a mobile device has not been investigated yet. However, a similar power cycling pattern can be observed in electric vehicle (EV) battery usage (i.e., excessively high and low discharging rates alternate when the vehicle starts and stops abruptly). In this application, the power drain has been also regarded as one of the critical challenges for safe and stable operation of EV batteries, and, thus, there have been a number of studies for tackling the corresponding challenge. In [40], it is known that the major factors that affect the battery lifetime are both temperature and discharge current-rate (C-rate), which implies that how to set the value of C-rate is much more important to avoid power drain rather than the variation of actual transmit power. For reference, if we apply 1 C-rate, the considered battery fully discharges for

one hour. However, in practice, we can use the battery much less than one hour with 1 C-rate due to various factors. For this reason, by carefully setting the value of $P_{\text{tx}}^{\max}$ (e.g., $P_{\text{tx}}^{\max} = 0.6\times$C-rate), the excessive power consumption affecting power drain can be effectively avoided.

VIII. Conclusion

In this paper, we investigated a new framework for employing a secure power control scheme against the user location tracking (ULT) attack in cellular networks (e.g. LTE systems). We devised the notion of average inference error probability as a new performance metric to measure the level of users' location privacy. With the formulation of the optimization problem, we proposed an opportunistic uplink power control scheme to protect physical layer identifiers able to be exploited by ULT attack. Through numerical simulations, we verified that our proposed defense scheme is effective and achieves the best secrecy performance, compared with conventional schemes (FPC and RPC schemes). Extension of our framework to be applicable to 5G standards and its implementation in a practical network setting (e.g., 5G testbed based on software-defined radios) are one of the future research directions.

References

[1] A. Lilly, "IMSI catchers: Hacking mobile communications," *Netw. Secur.*, vol. 2017, no. 2, pp. 5–7, Feb. 2017.

[2] S. F. Mjølsnes and R. F. Olimid, "Easy 4G/LTE IMSI catchers for non-programmers," in *Proc. Int. Conf. Math. Methods, Models, Archit. Comput. Netw. Secur.*, 2017, pp. 235–246.

[3] D. Rupprecht, K. Kohls, T. Holz, and C. Popper, "Breaking LTE on layer two," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2019, pp. 1121–1136.

[4] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, "Practical attacks against privacy and availability in 4G/LTE mobile communication systems," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2016, pp. 1–15.

[5] S. R. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, "LTEInspector: A systematic approach for adversarial testing of 4G LTE," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2018, pp. 1–15.

[6] H. Kim *et al.*, "Breaking and fixing VoLTE: Exploiting hidden data channels and mis-implementations," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2015, pp. 328–339.

[7] CBS. *Suspicious Cellular Activity in D.C. Suggests Monitoring of Individuals' Smartphones*. Accessed: Dec. 9, 2021. [Online]. Available: http://www.cbsnews.com/news/suspicious-cellular-activity-in-dc-suggests-monitoring-of-individuals-smartphones/

[8] S. Kumar, E. Hamed, D. Katabi, and L. E. Li, "LTE radio analytics made easy and accessible," in *Proc. ACM SIGCOMM Comput. Commun. Rev.*, Aug. 2014, pp. 211–222.

[9] S. R. Hussain, M. Echeverria, O. Chowdhury, N. Li, and E. Bertino, "Privacy attacks to the 4G and 5G cellular paging protocols using side channel information," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2019, pp. 1–15.

[10] M. Chlosta, D. Rupprecht, T. Holz, and C. Pöpper, "LTE security disabled: Misconfiguration in commercial networks," in *Proc. 12th Conf. Secur. Privacy Wireless Mobile Netw.*, May 2019, pp. 261–266.

[11] A. Shaik, R. Borgaonkar, S. Park, and J.-P. Seifert, "New vulnerabilities in 4G and 5G cellular access network protocols: Exposing device capabilities," in *Proc. 12th Conf. Secur. Privacy Wireless Mobile Netw.*, May 2019, pp. 221–231.

[12] T. Jiang, H. J. Wang, and Y.-C. Hu, "Preserving location privacy in wireless LANs," in *Proc. 5th Int. Conf. Mobile Syst., Appl. Services (MobiSys)*, 2007, pp. 246–257.

[13] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying location privacy," in *Proc. IEEE Symp. Secur. Privacy*, May 2011, pp. 247–262.

[14] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, and J.-Y. Le Boudec, "Protecting location privacy: Optimal strategy against localization attacks," in *Proc. ACM Conf. Comput. Commun. Secur. (CCS)*, 2012, pp. 617–627.

[15] W. Zhang, M. Li, R. Tandon, and H. Li, "Online location trace privacy: An information theoretic approach," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 1, pp. 235–250, Jan. 2019.

[16] S. Oya, C. Troncoso, and F. Perez-Gonzalez, "Rethinking location privacy for unknown mobility behaviors," in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS&P)*, Jun. 2019, pp. 416–431.

[17] R. P. Jover, "LTE security and protocol exploits," Shmoocon, Washington, DC, USA, 2016.

[18] J. D. Roth, M. Tummala, J. C. McEachen, and J. W. Scrofani, "On location privacy in LTE networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1358–1368, Jun. 2017.

[19] H. Qi, Y. Shen, and B. Yin, "Intelligent trajectory inference through cellular signaling data," *IEEE Trans. Cognit. Commun. Netw.*, vol. 6, no. 2, pp. 586–596, Jun. 2020.

[20] T. Wang and Y. Yang, "Location privacy protection from RSS localization system using antenna pattern synthesis," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 2408–2416.

[21] O. Arana, F. Garcia, and J. Gomez, "Analysis of the effectiveness of transmission power control as a location privacy technique," *Comput. Netw.*, vol. 163, Nov. 2019, Art. no. 106880.

[22] J. Jiang, G. Han, H. Wang, and M. Guizani, "A survey on location privacy protection in wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 125, pp. 93–114, Jan. 2019.

[23] S. Sesia, I. Toufik, and M. Baker, *LTE-the UMTS Long Term Evolution: From Theory to Practice*. Hoboken, NJ, USA: Wiley, 2009.

[24] *Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and Modulation (Release 14)*, document TS 36.211, v14.1.0, 3GPP, Dec. 2016.

[25] *Evolved Universal Terrestrial Radio Access (E-UTRA); Multiplexing and Channel Coding (Release 14)*, document TS 36.212, v14.1.1, 3GPP, Jan. 2017.

[26] *Numbering, Addressing and Identification (Release 14)*, document TS 23.003, v14.3.0, 3GPP, Mar. 2017.

[27] *Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) Protocol Specification (Release 14)*, document TS 36.321, v14.1.0, 3GPP, Dec. 2016.

[28] *Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol Specification (Release 14)*, document TS 36.331, v14.1.0, 3GPP, Dec. 2016.

[29] *Model Parameters for the Physical Statistical Wideband Model in Recommendation ITU-R P.681*, document Report ITU-R P.2145-2, ITU-R, Sep. 2017.

[30] R. Vogt, I. Nikolaidis, and P. Gburzynski, "A realistic outdoor urban pedestrian mobility model," *Simul. Model. Pract. Theory*, vol. 26, pp. 113–134, Aug. 2012.

[31] S. M. Kim, W. Choi, T. W. Ban, and D. K. Sung, "Optimal rate adaptation for hybrid ARQ in time-correlated Rayleigh fading channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 968–979, Mar. 2011.

[32] A. Papoulis and S. U. Pillai, *Probability, Random Variables and Stochastic Processes*. New York, NY, USA: McGraw-Hill, 2002.

[33] S. N. Chiu, D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic Geometry and its Applications*. Hoboken, NJ, USA: Wiley, 2013.

[34] S. Abramovich and L.-E. Persson, "Some new estimates of the 'Jensen gap,'" *J. Inequal. Appl.*, vol. 2016, no. 1, pp. 1–9, Dec. 2016.

[35] Y. Kim and H. J. Yang, "Sum-rate maximization of multicell MISO networks with limited information exchange," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7247–7263, Jul. 2020.

[36] S. Boyd, S. P. Boyd, and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[37] *MATLAB, Version 9.10.0 (R2021a)*, MathWorks, Portola Valley, CA, USA, 2021.

[38] M. Jadliwala, I. Bilogrevic, and J.-P. Hubaux, "Optimizing mix-zone coverage in pervasive wireless networks*," *J. Comput. Secur.*, vol. 21, no. 3, pp. 317–346, Jul. 2013.

[39] J. Freudiger, R. Shokri, and J.-P. Hubaux, "On the optimal placement of mix zones," in *Proc. Int. Symp. Privacy Enhancing Technol. Symp.*, 2009, pp. 216–234.

[40] S. Saxena, D. Roman, V. Robu, D. Flynn, and M. Pecht, "Battery stress factor ranking for accelerated degradation test planning using machine learning," *Energies*, vol. 14, no. 3, p. 723, Jan. 2021.

Inkyu Bang (Member, IEEE) received the B.S. degree in electrical and electronic engineering from Yonsei University, Seoul, South Korea, in 2010, and the M.S. and Ph.D. degrees in electrical engineering from the Korea Advanced Institute for Science and Technology (KAIST), Daejeon, South Korea, in 2012 and 2017, respectively. He was a Research Fellow with the Department of Computer Science, National University of Singapore (NUS), from 2017 to 2019. From March 2019 to July 2019, he was a Senior Researcher with the Agency for Defense Development (ADD). He is currently an Assistant Professor with the Department of Intelligent Media Engineering (adjunct with the Department of Information and Communication Engineering), Hanbat National University. His research interests include information-theoretic security (physical-layer security), wireless network security, 5G/IoT, simultaneous wireless information and power transfer (SWIPT), and machine learning application in wireless communications.

Taehoon Kim (Member, IEEE) received the B.S. degree in media communications engineering from Hanyang University, Seoul, South Korea, in 2011, and the M.S. and Ph.D. degrees in electrical engineering from the Korea Advanced Institute for Science and Technology (KAIST), Daejeon, South Korea, in 2013 and 2017, respectively. He was a Senior Researcher with the Agency for Defense Development (ADD), South Korea, from September 2017 to February 2020. He has been an Assistant Professor with the Department of Computer Engineering, Hanbat National University, Daejeon, since March 2020. His research interests include wireless communications, resource management for 5G/IoT, machine learning applications in wireless communications, and physical-layer security.

Han Seung Jang (Member, IEEE) received the B.S. degree in electronics and computer engineering from Chonnam National University, Gwangju, South Korea, in 2012, and the M.S. and Ph.D. degrees in electrical engineering from the Korea Advanced Institute for Science and Technology (KAIST), Daejeon, South Korea, in 2014 and 2017, respectively. From May 2018 to February 2019, he was a Post-Doctoral Fellow with the Information Systems Technology and Design (ISTD) Pillar, Singapore University of Technology and Design (SUTD), Singapore. He was also a Post-Doctoral Fellow with Chungnam National University, Daejeon, from September 2017 to April 2018. He is currently an Assistant Professor with the School of Electrical, Electronic Communication, and Computer Engineering, Chonnam National University, Yeosu-si, South Korea. His research interests include cellular Internet of Things (IoT)/machine-to-machine (M2M) communications, machine learning, smart grid, and energy ICT.

Dan Keun Sung (Life Fellow, IEEE) received the B.S. degree in electronics engineering from Seoul National University in 1975 and the M.S. and Ph.D. degrees in electrical and computer engineering from The University of Texas at Austin in 1982 and 1986, respectively. Since 1986, he has been with the faculty of the Korea Advanced Institute of Science and Technology (KAIST), Daejon, South Korea, where he is currently a Professor Emeritus with the School of Electrical Engineering. From 1996 to 1999, he was the Director of the Satellite Technology Research Center (SaTReC), KAIST. His research interests include mobile communication systems and networks with special interest in resource management, cellular M2M, smart grid, energy networks, energy ICT, WLANs, WPANs, traffic control in wireless and wired networks, performance and reliability of communication systems, and microsatellites. He is a fellow of the Korean Academy of Science Technology and a Life Fellow of the National Academy of Engineering of Korea. He was a recipient of the 1992 National Order of Merits, the Dongbaek, the 1997 Research Achievement Award, the 2000 Academic Excellence Award, the 2004 Scientist of the Month from the Ministry of Science and Technology and the Korea Science and Engineering Foundation, the 2013 Haedong Academic Grand Award from the Korean Institute of Communications and Information Sciences, and the 2017 National Order of Merits, the Okjo Medal. He had served as a Division Editor for the *Journal of Communications and Networks* from 1998 to 2007. He also had served as an Editor for *IEEE Communications Magazine* from 2002 to 2011.