SecLoc: Encryption System Based on Compressive Sensing Measurements for Location Estimation

Dimitris Milioris and Philippe Jacquet
Bell Labs, Alcatel-Lucent, Centre de Villarceaux, 91620 Nozay, France
École Polytechnique ParisTech, Route de Saclay, 91120 Palaiseau, France
Email: {dimitrios.milioris, philippe.jacquet}@alcatel-lucent.com

***Abstract*—In this paper we present an efficient encryption system based on Compressive Sensing, without the additional computational cost of a separate encryption protocol, when applied to indoor location estimation problems. The breakthrough of the method is the use of the *weakly* encrypted measurement matrices which are generated when solving the optimization problem to localize the source. It must be noted that in this method an alternative *key* is required to secure the system.**

I. Introduction

During recent years, location based services have seen a huge expansion. Location estimation and navigation systems are used in many areas, e.g. transportation, security, entertainment, medicine, etc. where accurate results are essential. Numerous solutions have been proposed based on various technologies, such as IEEE802.11, infrared, ultrasonic, bluetooth, or even a combination of optical, acoustic, and received signal-strength (RSS) along with motion attributes.

Based on the wide deployment of wireless local area networks (WLANs) using IEEE802.11 infrastructures, most indoor positioning systems employ the RSS values obtained directly from a set of access points (APs) by any mobile device which is connected to the network. The study of location based services and systems has several research challenges to address; such as shadowing and multipath fading, due to the nature and structure of indoor environments, e.g. obstacles from different materials, human motion, temperature, etc. Radio channel obstructions and RSS variations exist because of these uncertain characteristics of the indoor environments.

Compressive Sensing (CS) is an efficient way to handle the location estimation problem, since the physical space naturally motivates the use of the CS framework due to the inherent spatial sparsity. CS states that signals which are sparse or compressible in a suitable transform basis can be recovered from a highly reduced number of incoherent linear random projections, in contrast to the traditional signal processing methods, which are dominated by the well-established Nyquist-Shannon sampling theorem.

In a prior work [1], we introduced a hybrid path-tracking system, which was an extension of the fingerprint positioning approach [3] for static users. The system consist of two steps: First, we designed a region-based multivariate Gaussian model to narrow down the search space of candidate cells; then, for each region, we performed the CS reconstruction of an appropriate sparse position-indicator vector, combined with a Kalman filter, as a refinement step for the update of the estimated position.

II. Background

Assume that $\mathbf{\Psi} \in \mathbb{R}^{P\times N}$ $(P \geq N)$ is a matrix whose columns correspond to a possibly over-complete, transform basis, that describe the physical space. The measurement model generating the projections in the original space-domain is written as $\mathbf{g} = \mathbf{\Phi x}$, or via its equivalent transform-domain representation,

$$\mathbf{g} = \mathbf{\Phi \Psi w} \tag{1}$$

where $\mathbf{g} \in \mathbb{R}^M$ is the vector of compressed measurements, $\mathbf{\Phi} \in \mathbb{R}^{M\times N}$ denotes the measurement matrix, and $\mathbf{w}$ is the sparse vector of transform coefficients.

In our indoor positioning application, the training measurement model associated with the $i-$th AP is given by

$$\mathbf{g_i} = \mathbf{\Phi}_{\boldsymbol{T}}^{\boldsymbol{i}} \mathbf{\Psi}_{\boldsymbol{T}}^{\boldsymbol{i}} \mathbf{w} \tag{2}$$

and the runtime measurement model for cell c is expressed as

$$\mathbf{g_{c,i}} = \mathbf{\Phi}_{\boldsymbol{R}}^{\boldsymbol{i}} \boldsymbol{\psi}_{\boldsymbol{R,c}}^{\boldsymbol{i}} \tag{3}$$

where the subscripts T and R are used to denote the variables (matrices and vectors) generated in the training and runtime phase, respectively, and $\boldsymbol{\psi}_{\boldsymbol{R,c}}^{\boldsymbol{i}}$ is the vector of runtime RSS values collected at cell c from AP i.

For the localization problem, let $\mathbf{w} = [0\ 0\ \cdots\ 0\ 1\ 0\ \cdots\ 0]^T \in \mathbb{R}^C$ be a *position-indicator vector* whose j-th component is equal to "1" if the mobile device is located in the j-th cell. The inherent sparsity in the problem of location estimation comes from the fact that the device to be localized can be placed in exactly one of these cells. Thus, in the framework of CS, the problem of localization is reduced to a problem of recovering the 1-sparse vector $\mathbf{w}$.

The inherent property of CS acting as a weak encryption module combined with an extra *key* (the combination of number of false measurement vectors with the correct one) is exploited to guarantee with high probability that the communication between the device and the server is secured against potential intrusions of an unauthorized entity.

CS-based encryption provides both signal compression and encryption guarantees, without the additional computational cost of a separate encryption protocol and thus it could be useful in location estimation, where the implementation of an additional software layer for cryptography could be costly.

978-1-4673-1017-8/14/$31.00 ©2014 IEEE

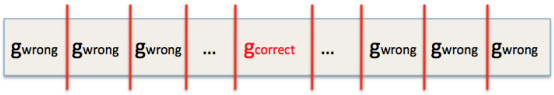

Fig. 1. N-1 false vectors plus the correct one. This *key*, i.e., the sequence of the measurement vectors reaches the server.

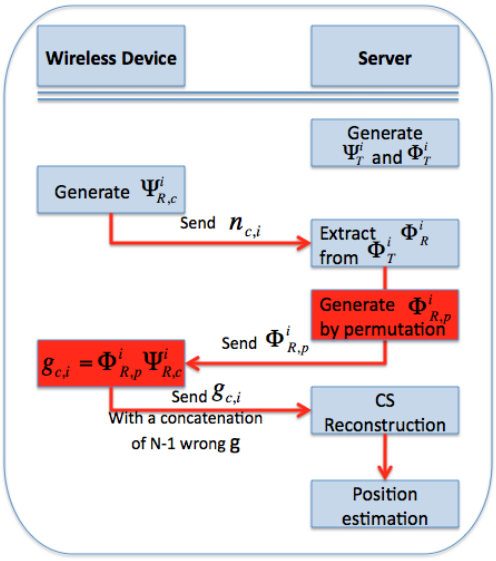

Fig. 2. SecLoc system's security architecture

III. SecLoc System Description

The method consist of two parts: (III-A) Privacy system, and (III-B) Key description.

A. Privacy system

Due to their acquisition process, CS measurements can be viewed as *weakly encrypted* for a malicious user without knowledge of the random matrices Φ^i, where i corresponds to the i-th AP, which have independent and identically distributed (i.i.d.) Gaussian or Bernoulli entries [7].

The encryption property of a CS approach relies on the fact that the matrix Φ is unknown to an unauthorized entity, since Φ can be generated using a (time-varying) cryptographic key that only the device and the server share.

More specifically, the server extracts the runtime sub-matrix Φ_R^i from the training Φ_T^i (since the runtime phase lasts significantly less time than training). The lines of Φ_R^i are permuted and the *key* of the merge of the false measurement vectors and the correct one is used, as shown in Fig. 2 and described extensively in [3].

B. Key description

The wireless device sends the measurement vector g to the server along with $N-1$ false vectors, where the reconstruction takes place. Then, the server uses the information of the physical topology, AP characteristics, previous position, etc., and estimates the location.

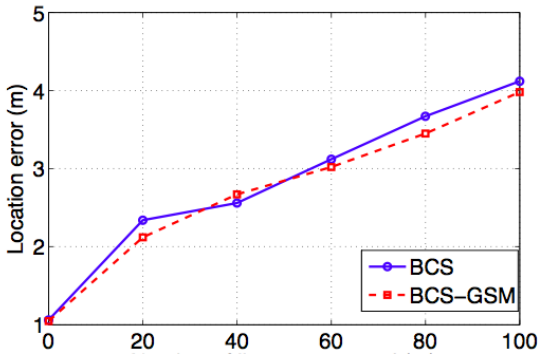

Fig. 3. Evaluation of the encryption property using BCS and BCS-GSM, for a varying number of permuted lines of Φ_R^i.

IV. Possible attacks from malicious users

An attack could follow three directions:

1. Find Φ matrix by intercepting the server (modern network cryptographic protocols could guarantee that the decryption of Φ_p – where p denotes the permutation of the lines – is almost infeasible in practice due to the combinatorial nature of the inverse problem).

2. Find g by intercepting the opposite direction (the exact knowledge of g is insufficient, resulting in a significantly increased estimation error, when the attacker does not achieve the exact estimate of Φ_R^i)

3. Find the correct measurement vector g, which increases the estimation error, without exact knowledge.

Fig. 3 shows the encryption capability of the method for the Bayesian Compressive Sensing (BCS) [5] and Bayesian Compressive Sensing Gaussian Scale Mixture (BCS-GSM) [4], [6] reconstruction algorithms.

In particular, the average localization error, over 100 Monte-Carlo runs, is shown as a function of the percentage of permuted lines from 0% to 100%, of the true matrices Φ_R^i, where the reconstruction is performed by considering exact knowledge of the measurement vectors g. The results agree with the intuition that as the complexity of the permutation increases, the estimation accuracy decreases without an exact estimate of the true measurement matrix.

References

[1] D. Milioris et al., "WLAN-based Indoor Path-Tracking using Compressive RSS Measurements", in *21st European Signal Processing Conference (EUSIPCO13)*, Marrakech, Morocco, September 2013.

[2] P. Mirowski et al., "Probabilistic RF Fingerprinting and Localization on the Run", in *Bell Laboratories Technical Journal*, Issue on Data Analytics, Vol. 18, No. 4, 2014.

[3] D. Milioris et al., "Low-dimensional Signal-Strength Fingerprint-based Positioning in Wireless LANs", in *Elsevier Ad Hoc Networks*, Vol. 12, January 2014 (doi: http://dx.doi.org/10.1016/j.adhoc.2011.12.006)

[4] G. Tzagkarakis et al., "Multiple-Measurement Bayesian Compressive Sensing using GSM Priors for DOA Estimation", in *Proc. 35th IEEE Int. Conf. on Acoustics, Speech and Sig. Proc. (ICASSP10)*, Dallas, TX, USA, March 2010.

[5] S. Ji, Y. Xue, and L. Carin, Bayesian compressive sensing, in *IEEE Trans. Sig. Proc.*, 2008.

[6] G. Tzagkarakis and P. Tsakalides, Bayesian compressed sensing imaging using a Gaussian scale mixture, in *Proc. IEEE ICASSP10*, Mar. 2010.

[7] D. Donoho, Compressive sensing, in *IEEE Trans. on Inf. Th.*, 2006.