

Tracking Risks from Multi-path TDoA-based Localization in Wireless Communications

Lan-Huong Nguyen *, Van-Linh Nguyen*, Yu-Hao Liu *

*Dept. of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan
{nlh106p, nvlinh, g11410178}@cs.ccu.edu.tw

Abstract—New antenna technologies like phased array antennas are crucial to enhance high-speed data transmission in 5G and 6G high-frequency communications (mmWave/Terahertz). By exploiting spatial-temporal beamforming space (e.g., angle of arrival, angle of departure, time of arrival), directional antenna technologies can enable precise radio positioning. The feature has tremendous potential to be used in many futuristic applications, such as behavioral monitoring or assisting rescue teams moving inside a dark building. However, besides that positive side, precise radio positioning potentially poses significant tracking risks to mobile users. In this work, we demonstrate a case study of tracking a user in a restricted access building based on passively received signals. We then build an efficient mechanism to regenerate the trajectory of a target device by exploiting the characteristics of directional signals. We also exploit the capability of simultaneous localization and mapping using multipath channel information. Through theoretical analysis and simulation, we found that tracking risks of radio positioning techniques are real and challenging to resolve.

Index Terms—Wireless security, User tracking, Signal-based tracking, Signal surveillance.

I. INTRODUCTION

Radio positioning is the featured technology in indoor environments where the Global Positioning System (GPS) often performs poorly. Autonomous robots in industrial sites or augmented reality apps will not work appropriately without high-precision localization capability. Accurate location is critical information for many assisted living applications such as activity trackers [1] or gesture monitoring [2]. However, adversaries can exploit the positioning capability for potential user tracking [3]. For example, the attacker can exploit the habit of using smartphones or WiFi from a homeowner to track him accurately, even in a restricted access building. For illegal intrusion, the attacker can collect the owner's movement trajectory and identify the doors' locations. As illustrated in Figure 1, the coordinated agents are dispatched to infer cellular/WiFi signals and track the location/trajectory of a target user in a hotel complex without physical intrusion. The radio positioning can be launched from compromised WiFi access points in the building or an Unmanned Aerial Vehicle (UAV) flying over the roof of the building.

A. State-of-the-art studies

The state-of-the-art radio positioning techniques' performance has reached up to a centimeter in various environments, including for 5G mmWave and Gigabit WiFi standards (IEEE 802.11ad 60 GHz) [4]–[7]. Accordingly, the techniques

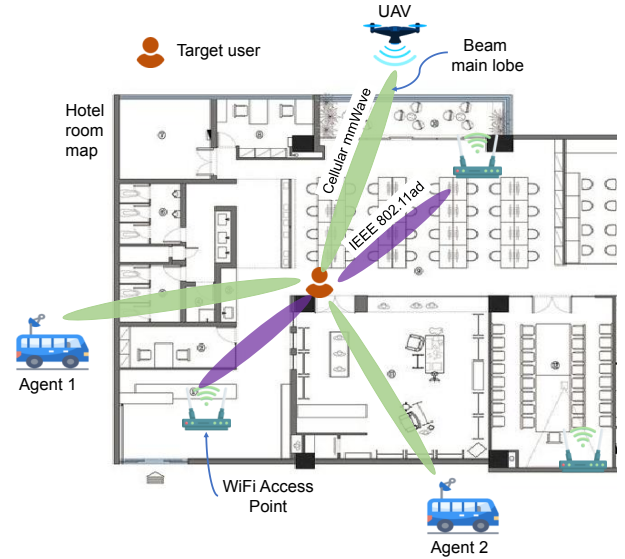


Fig. 1. The illustration of exploiting signal spatial-temporal signal processing of directional antenna technologies to track a user in an indoor building without physically going in.

can be summarized into three categories. The first one is a conventional approach where Angle of Arrival (AoA) or Time Difference of Arrival (TDOA) measurements are used for geometry-based localization, e.g., triangulation and trilateration [8]. However, its disadvantage is to require at least three base stations or anchors, which is high cost and requires excellent time synchronization mechanisms. Meanwhile, the approach's localization error can be up to dozen or hundreds of meters. This low-accuracy performance makes the technique less friendly for indoor applications.

The second approach uses a fingerprint database (e.g., amplitude, angle, Radio Signal Strength Indicator (RSSI)) and machine learning techniques (deep neural networks [7]) to predict the user location based on the ground truth values in the dataset. However, this method requires the availability of a dense fingerprint database, which can be a challenge in unknown structures. The last approach uses the multipath localization technique where the user position can be estimated from the intersection of multiple paths, e.g., various reflections or scattering [8]. Recently, this approach has gotten much attention due to the vast usage of Ultrawideband (UWB) signals and directional communications at mmWave frequencies

[8]. However, the inference or overlap issues in multipath components can significantly degrade the localization accuracy due to the complexity of accurately detecting each component with corresponding sources.

B. Contributions

This work presents a novel approach to demonstrate the indoor surveillance capability by using the cooperative passive localization of multiple anchors (aka spy agents), information from reflected Multi-Path Components (MPC), and data fusion from Kalman filters. Instead of using a fingerprint database, we exploit the propagation models and path loss statistics of well-known material penetration to estimate the relative location of a user. The estimations are then refined with empirical mapping results from ray tracing techniques or time-varying tracking. The results demonstrate that passive positioning in directional wireless communications like millimeter-wave can yield high-accuracy indoor surveillance capability, even without physical intrusion into the target environment or empirical signal sample collection.

II. SYSTEM MODEL AND PROBLEM FORMULATION

This work aims to track a specific mobile user in a building (hotel/department). We assume that the law enforcement can deploy M cooperating anchors (truck base stations) in known positions to detect/infer user signals. Let $p_i^t = [x_i^t, y_i^t, z_i^t]$, $i \in \{1, \dots, M\}$ denote the detected signal at time slot t . There are N possible users with unknown positions who are using either cellular networks or WiFi networks, or merely broadcasting initial signals to find nearby base stations. Suppose that the antennas of the anchors and the users are Uniform Linear Array (ULA) type and equipped with multiple arrays (K_T and K_R arrays). Each array is fully connected with N_T/N_R elements.

A user j ($j \in \{1, \dots, N\}$) is determined via its mobile identifier. Given the challenge of tracking 5G users via Subscription Concealed Identifier (SUCI), the identifier can be the pattern of sequence numbers of the access [9] or the access habit on a list of several services. Such information can be obtained by using fake base stations or using an SMS Broadcaster to deceive the target. For WiFi networks, the identifier is a MAC address that can be obtained through legal access requests (by law enforcement) to the access points, using rouge broadcasting stations, or hack passwords of vulnerable WiFi access points through penetration [10]. Matching the identifier to a specific suspect (i.e., labeling) is presented in Section III. In the worst case, law enforcement may require the cooperation of the network providers. In short, the fake stations (anchors) are to attract the user for establishing communications or detecting the user's signals which are then used for tracking. Finally, since the signal surveillance is performed in the physical layer, both the network types are supposed to be vulnerable to this security risk. Note that the user position can be estimated even with data transmission error in a short period. This means as long as the transmission/signals exist, tracking is entirely possible.

A. Signal and communication model

We assume that the anchors' locations are fixed to avoid the target user's suspicion. In this way, the relative location between the user to an anchor node is changed according to the user's movement. The received signal of the user j from the anchor i with sampling time T_s in the form of N_s OFDM symbols ($N_s \leq K_T \leq N_T$) is $r_{i,j}(t) = [r_{i,j}(1), r_{i,j}(T_s), \dots, r_{i,j}((N_s - 1)T_s)]^T$. $r_{i,j}(t)$ is given by

$$r_{i,j}(t) = \sqrt{\rho} H_i s_i(t - \tau_i) + I_{i,j}^t + n_{i,j}^t, \quad (1)$$

where $\sqrt{\rho}$ is the average received power. τ_i denotes the delay that can be used to measure position-related information (e.g., TDOA), $\tau_i = \frac{|p_j^t - p_i^t|}{c}$, where $|p_j^t - p_i^t|$ is the Euclidean distance between the user j and the anchor i , c is the speed of light. Measuring τ_i accurately (up to several nanoseconds) requires medium-to-high cost anchors, which we assume is possible for high-profile missions. $s_i(t - \tau_i)$ is the sample of a path representing a delayed and scaled baseband pulse s [11]. $I_{i,j}^t$ is the diffuse multi-path that is the main interference to the useful information from multi-path components. Accordingly, $I_{i,j}^t$ is a stochastic process and can be modeled as in [12], [13]. In the modern wireless networks with digital encoders/decoders, $n_{i,j}^t$ denotes the white Gaussian measurement noise with power spectral density $\frac{N_0}{2}$ and variance $\delta^2 = \frac{N_0}{T_s}$, where T_s is the predefined sampling frequency.

In this work, we assume that the channel is modeled with L scattering clusters as in [14]. Then the channel matrix H_i is given by

$$H_i = \gamma \sum_{l=1}^L \sum_{k=1}^K a_R(\phi_{l,k}^R) h_{l,k} a_T(\phi_{l,k}^T) e^{\frac{-j2\pi f_c}{T_s}}, \quad (2)$$

where K is the number of propagation paths, f_c denotes the carrier frequency, and $\gamma = \sqrt{\frac{N_R N_T}{LK}}$. The antenna array response vectors at the transmitter $a_T(\phi_{l,k}^T)$ and receiver $a_R(\phi_{l,k}^R)$ evaluated at the l th path and the k th cluster follow [14].

Suppose that the signals penetrate via multiple walls. In this work, we use the Wall Attenuation Factor model as described in [15]. Accordingly, the signal loss in decibels (dBm) caused by obstacle attenuation between the transmitter and the receiver is modeled by

$$Loss_{i,j}^t = \begin{cases} Loss(d0) - 10n \log(\frac{d_{i,j}}{d0}) - W * F & \text{if } W < C \\ Loss(d0) - 10n \log(\frac{d_{i,j}}{d0}) - C * F & \text{otherwise,} \end{cases} \quad (3)$$

where $Loss(d0)$ is the signal power at some reference distance $d0$, e.g., $d0 = 1m$. n denotes the speed of path loss that increases with distance (e.g., $n = 4$ in Non-Line-of-Sight (NLOS) areas). $d_{i,j}$ is the Euclidean distance between the anchor i and the user j . C is the maximum number of obstructions (walls), a constant. W is the estimated number of obstructions the anchor i and the user j . F is the wall attenuation factor. Both n and F depend on the building layout and construction material. The values of signal loss in

TABLE I
SUMMARY OF SIGNAL LOSS IN SEVERAL WALL MATERIALS [16], [17]

Material	Signal loss at 2.4GHz (dB)	Signal loss at 5GHz (dB)	Signal loss at 28GHz (dB)	Signal loss at 91GHz (dB)
► Brick	6	15	21	~
► Concrete (102 mm)	15	22	32	~
► Concrete (203mm)	29	48	60	~
► Reinforced concrete (203 mm)	31	55	74	~
► Glass (1cm)	1	1	2.2	3.3
► Plywood (6 mm)	1	1	2.5	6.2

several wall materials are summarized in Table I. According to the data, glass and plywood have no significant effect on signal loss for many wireless frequencies. However, for high-frequency wireless communications, it is clear that the penetration capability is low with concrete materials. This means that in high-frequency wireless communications (mmWave/THz), the base station/access points density is supposed to be high (as illustrated in Figure 1) to compensate for the signal attenuation by obstacles. The density benefits the localization capability. The detail of electromagnetic signal attenuation in other construction materials can be found in [16] (for 2-6GHz frequency) or [17] (for 27, 78, 93GHz).

For localization, Signal-to-Noise Ratio (SNR) estimation plays a critical role. We define the SNR value in the communication link between the anchor i and the user j at the time t as follows:

$$SNR_{i,j}^t(\text{dB}) = \frac{P_j - \text{Loss}_{i,j}^t}{n_{i,j}^t}, \quad (4)$$

where P_j is the signal transmission power of a cell phone. According to 3GPP specification [18], the maximum P_j of a phone, namely P_{max} , is often limited at 23dBm.

B. Problem statement

Assume that the estimated location of the user j from the passive positioning is $\hat{p}_j$. The goal of the indoor surveillance is to minimize the error between the estimation and the real location of the user as follows:

$$\begin{aligned} \min_{r_{i,j}(t), SNR_{i,j}^t} & (|\hat{p}_j - p_j|) \\ \text{s.t.} & 0 < k < K, \\ & 0 \leq P_j \leq P_{max}, \forall j \in \{1, \dots, N\} \end{aligned} \quad (5)$$

On the other hand, given the existence of wireless communications between the anchors and the user, the goal is to collect signal patterns at the anchors and run localization algorithms to minimize the localization error. Depending on the localization methods (e.g., using AoA or TDOA), the sampling frequency and channel features for collection vary. Below, we present the detail of our proposed positioning and tracking scheme for indoor surveillance.

III. OUR PROPOSED POSITIONING AND TRACKING SCHEME FOR INDOOR SURVEILLANCE

Since the building can be covered with many obstacles and signals are heavily scattered, the localization can be resolved through a Time of Arrival (TOA) method. Generally, nanosecond-level timing synchronization is required for submeter accuracy in the TOA method [8]. However, suppose the anchor is a powerful device for law enforcement. The cost is not an issue. Another simpler method is to use TDOA, as illustrated in Figure 1.

A. Multi-path localization and tracking algorithm

The different arrival of the signals in each antenna element can be used to calculate the time difference in TDOA-based localization. Note that time synchronization within a multi-array antenna is feasible in implementation. In this way, the localization can be performed at a single anchor. The phase of arrival from the user j extracted by the n th array element of a multi-array antenna is expressed as follows:

$$\phi_{j,n}(t) = \phi_0 - \frac{2\pi f_c d_{j,n}}{c}(\phi_j) + n_{i,j}^t, \quad (6)$$

where ϕ_j denotes the angle of arrival of the user j , $d_{j,n}$ is the known array distance. An observed phase vector ϕ can be built from the signal collection as follows:

$$\phi = [\phi_{j,1}(0), \phi_{j,n}(0), \phi_{j,N_R}(0), \phi_{j,1}(T_s), \phi_{j,n}(T_s), \phi_{j,N_R}(T_s)]. \quad (7)$$

The distance $\hat{d}_{i,j}$ between the anchor i and the user j can be estimated through the time difference between the same signal phase at two different antenna elements of the anchor antenna array. Without loss of generality, we assume it is the first antenna element and the N_R -th one. The angle between two elements is known in advance. Then $\hat{d}_{i,j}$ at the time t is given by

$$\hat{d}_{i,j}^t = c * (|t_{N_R} - t_1|) \cos(\phi_{j,n}(t)). \quad (8)$$

The estimated position of the user i is expressed by $\hat{p}_j = p_i + \hat{d}_{i,j}$. The direction is derived from the change of arrival of signals. The user's location can also be derived by running the DCS-SOMP/SAGE algorithm [14] on the received beamspace. At each time slot t , the arrival time of a number of MPCs is considered as the predicted delays. The arrival time is estimated from the received signal $r_{i,j}(t)$ by a high-resolution maximum likelihood channel estimation algorithm [19].

B. Data association and user identifier matching

Generally, we cannot label a specific user by signals once the target goes into the building. As illustrated in Figure 3, User 1's movements can be wrongly labeled to User 2's at the cross area. To avoid errors of wrong monitoring, we use an Unscented Kalman filter (UKF) to associate the positions of a user over a period. In this way, the user movement is highly personalized. Except for the users exchanging their smartphones at the cross areas, it is uncommon that one smartphone with a unique identifier can simultaneously appear in two places.

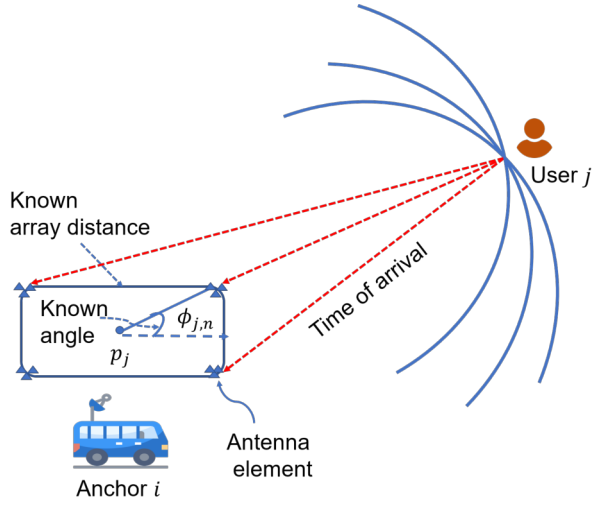


Fig. 2. The illustration of using a joint TDOA and AoA localization in multi-array transmission. The anchor is equipped with a multi-array antenna.

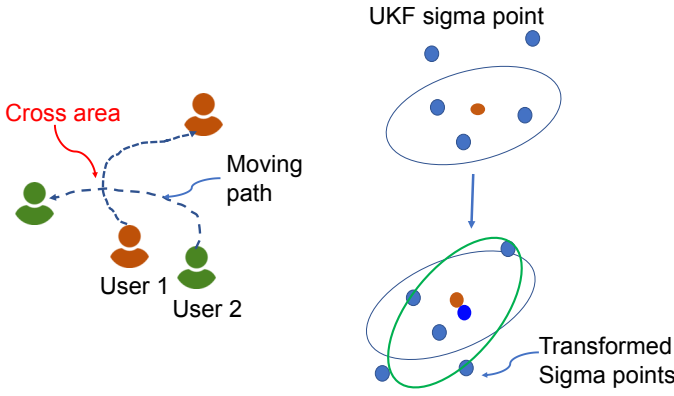


Fig. 3. The illustration of potential cross areas of the moving paths of two users. The signals of a user can be wrongly labeled to the others at the cross area.

A moving user can be modeled in the UKF state function as follows:

$$s_{t+1} = F_t s_t + u_t, \quad (9)$$

where F_t denotes the state transition. u_t is the noise with a zero-mean multivariate normal distribution, $u_t \sim \mathcal{N}(0, Q)$. For example, the next position of a user depends on her walking speed v_j and movement direction as follows:

$$\hat{p}_j^{t+1} = \hat{p}_j^t + v_j \Delta_t + u_t, \quad (10)$$

where Δ_t is the period between two tracking points. In the UKF system, the prediction can go longer as the prior estimation is still correct. Specifically, predicting $\hat{s}_{t+1|t}$ by UKF with known s_t is expressed as follows:

$$\hat{s}_{t+1|t} = F_t \hat{s}_{t|t-1} + u_t, \quad (11)$$

where $\hat{s}_{t|t-1}$ can be initialized as $\hat{s}_{0|0} = \mathbb{E}[s_0]$.

Since we have no ground truth (p_j) or empirical data to refine the error (in Equation 5), we use the data points from

Standard size of several structure (width x length in meters)

- Corridor (width): 1.5-1.8
- Hotel living room: 4.26 x 6.10 (medium)
- Lobby: 2.44 x 4.57 (medium)
- Elevator space: 10.9 x 8.5 (medium)

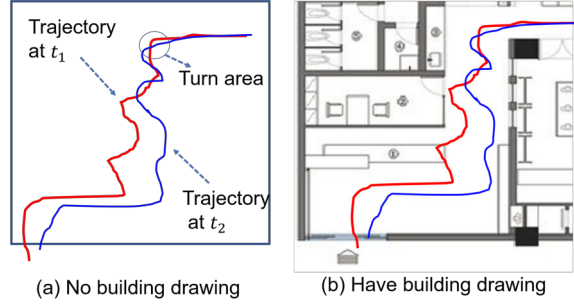


Fig. 4. The illustration of surveillance capability with and without building drawing to map the user's trajectory. In the latter scenario, knowing the exact room/place of the target is complicated and often requires a long time observation.

two different collection time points *in the same locations* to compare. For example, Figure 4(a) illustrates a user's trajectory at two collection time points t_1 and t_2 . The "same locations" can be the center points of i) the "turn areas" where the users often walk through, ii) the places that can be tracked by remote cameras/radars. Besides, the sigma points of the UKF can be built from the predictions of other anchors (in M cooperating anchors). The measurement model at the time step t , namely $z_{t|t-1}$ of the true state s_t , is defined as follows:

$$z_{t|t-1} = H_t s_t + \vartheta_t, \quad (12)$$

where H_t denotes the model to map the true state space (unknown) and the observed space (using signal-based tracking). ϑ_t indicates the noise $\vartheta_t \sim \mathcal{N}(0, R)$.

An important step in the UKF is to update the target user state estimate vector and covariance matrix from the predicted mean and covariance along with the measurement's mean and covariance as follows:

$$\hat{s}_{t+1|t} = \hat{s}_{t|t-1} + K_t(z_t - \hat{z}_{t|t-1}) \quad (13)$$

where K_t denotes the Kalman gain [11].

C. Surveillance capability with/without building drawings

A building drawing can significantly help to refine the tracking results in the previous step. By extracting distance and the building space (e.g., number of walls, locations of rooms, corridors) from the building drawing, the trajectory of the user from multiple anchors can be correlated, e.g. (1) by averaging the collected location points or (2) estimating via ray tracing on the regenerated building structure. As illustrated in Figure 4(b), the trajectory of a user at two-time points can be refined by using the left-right side coordinates of the lobby, corridor, and living room from the building drawing (e.g., for u_t estimation). In this way, the surveillance can track the user's trajectory accurately and locate which room/place they are standing.

However, it is a typical case where the tracker cannot have the drawing of the building. In this case, as illustrated in Figure 4(a), we do not know the insider structure. While revealing the in/out routes and a relative location of the target objects is still possible, knowing the exact room/place is complicated. To enhance the results of this blind tracking, the building architecture for ray tracing can be roughly estimated by the standard sizes of several structures (as our examples at the top of Figure 4). However, the furniture's influence on the signal loss can proportionally impact the accuracy of the structure regeneration. To gain the best results, the surveillance needs to run for a long time, e.g., hours or even days. By putting the habit of the targets in particular periods of the day, e.g., movement patterns during dining/sleeping time, we can reveal the functions of the locations the targets walk through to map with the known standard structures. For example, the targets may be at the elevator if the tracking signal exists in the same place for several seconds and then degrades with the changes in height. The targets may be in the living room if the signals appear around a corner area for several hours.

IV. EVALUATION RESULTS AND ANALYSIS

We evaluate this work on MATLAB with the Communications/Propagation and Channel Models toolbox. We also use the Path loss and phase change for RF propagation ray in the toolbox to trace the signals in the case where a building drawing exists. The building in this testing is a $50 \times 50m$ complex with the wall design as in Figure 1. The user walking follows the waypoint model with a maximum speed of $1.3m/s$ ($5km/h$). The sampling frequency T_s is at $2ns$. The other parameters are $K_R = K_T = 16(4 \times 4)$, and sub-carriers (WiFi frequency: 242, NR frequency: 3300). The anchor (spy agent) is at the position $(-10, 0)$ (i.e., outside of the building to avoid the suspicion of the target). Multiple agents can move around the left and the bottom side of the building with a distance of $20m$ to $30m$.

Overall, the signal-based surveillance can yield a 90% localization error under $1m$ if we can determine the strongest component of the anchor-target communication. As shown in Figure 5(a), the SNR of the target appears clearly on the signal map. If there is a building map, it highly indicates that the target is in the living room. Figure 5(b) also shows the estimated locations for building the target's trajectory with low mean estimation errors. Accordingly, accuracy degrades slightly at the positions $(25, 20)$ and $(27, 28)$, since many wall obstacles exist between the anchor and the target. In this case, the scattering and noise make SNR and signal direction estimation less accurate.

For sensitivity evaluation, we found that this signal-based surveillance can produce a significant enhancement in terms of accuracy if the high frequency is adopted in wireless communications. As shown in Figure 6, tracking on the $28GHz$ -based communications can yield an average of Root Mean Square Error (RMSE) under $0.4m$, even with less cooperation of the anchors. In this case, the high directional signals contribute to the accuracy enhancement. For the other frequencies (e.g.,

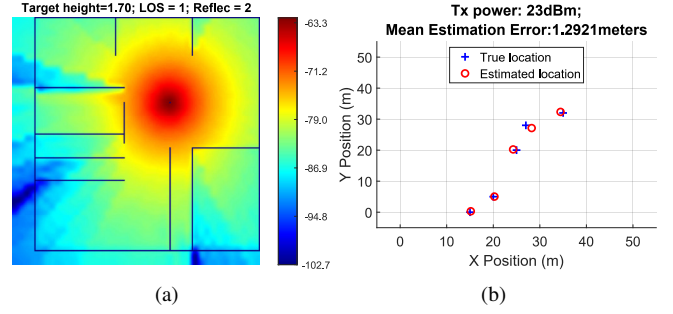


Fig. 5. The illustration of signal-based surveillance with multi-path components (LOS + reflector) and the target's trajectory with mean estimation error. The target height is 1.7m and Tx power is at 23dBm.

$2.4GHz$ and $5GHz$), the average estimation error is around $2m$. Note that the accuracy of the localization for surveillance in this work is significantly lower than the empirical methods or the studies as reported in [1], [6], [8], [11], [15]. This is because our method has no help from the ground truth comparison (i.e., the attacker cannot get into the building without a suspect of the target) to refine the results in the tracking step. The refinement is primarily based on time-varying observation. Besides, we also found that increasing the number of cooperative anchors ($M > 3$) does not enhance the accuracy. The issue raises a key finding: averaging the estimation results from many anchors at different locations can yield unexpected results. The negative influence likely worsens if the anchors' views on the target's location are so different, e.g., due to the influence of varying wall obstacle designs when communicating from different orientations.

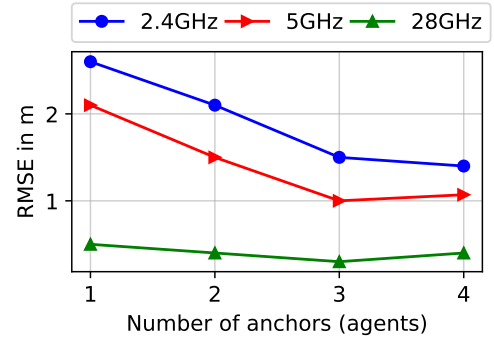


Fig. 6. The system performance with the availability of multiple anchors.

Figure 7 shows the performance comparison of our method for the time-based observation and the other methods (e.g., LEAP [4], Wicluster [6], DCNN-Particle [7]). Therefore, tracking users by time slot over hours can bring up a 62.2% improvement in accuracy compared to the other methods. This positive result reinforces the benefit of collecting estimated localization data at the same location several times for averaging in the proposed method. Deep learning-based localization methods such as LEAP and Wicluster suffer

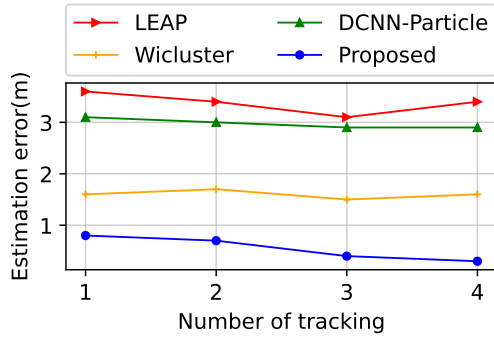


Fig. 7. The localization performance comparison between the proposed approach and the other models.

significant degradation of accuracy if there are no ground truth fingerprint patterns for reference (i.e., in the restricted access building). This method can be applied to specific surveillance missions, e.g., when targets have to enter or leave a building several times. When undertaking a one-time observation, compromising access points or cameras within the building may be useful for refining the tracking state.

For future work, given no general structure of the buildings and the challenges of obtaining the ground truth data, a possible extension for this work is to build a calculation model for finding the best locations to place the anchors where the tracking can perform best. The other approach is to exploit video object tracking techniques [20] to detect outlier data points, i.e., by using the locations of visible tracking for reference.

V. CONCLUSION

In this work, we present a simple signal-based surveillance method to track the target user in indoor buildings, even without going in. The system can reveal the moving path as well as the relative locations of the target users. The experimental results show that our method can maintain the accuracy of locating the target under two meters for typical buildings, even knowing nothing about the building structure. We believe that this tracking can cause severe concerns about personal privacy in the future, given the popularity of wireless communications and signals everywhere.

ACKNOWLEDGEMENT

This work was partly supported by the National Science and Technology Council (NSTC) of Taiwan under Grant No 111-2222-E-194-007-MY2.

REFERENCES

[1] J. A. del Peral-Rosado, R. Raulefs, J. A. López-Salcedo, and G. Seco-Granados, "Survey of cellular mobile radio localization methods: From 1G to 5G," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 2, pp. 1124–1148, 2018.

[2] L. Wang, K. Sun, H. Dai, W. Wang, K. Huang, A. X. Liu, X. Wang, and Q. Gu, "Witrace: Centimeter-level passive gesture tracking using ofdm signals," *IEEE Transactions on Mobile Computing*, vol. 20, no. 4, pp. 1730–1745, 2021.

[3] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2384–2428, 2021.

[4] J. Palacios, P. Casari, H. Assasa, and J. Widmer, "LEAP: Location estimation and predictive handover with consumer-grade mmwave devices," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, pp. 2377–2385, 2019.

[5] S. Sadowski, P. Spachos, and K. N. Plataniotis, "Memoryless techniques and wireless technologies for indoor localization with the internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 11, pp. 10996–11005, 2020.

[6] I. Karmanov, F. G. Zanjani, I. Kadampot, S. Merlin, and D. Dijkman, "Wicluster: Passive indoor 2d/3d positioning using wifi without precise labels," in *2021 IEEE Global Communications Conference (GLOBECOM)*, p. 1–7, 2021.

[7] C. Li, E. Tanghe, J. Fontaine, L. Martens, J. Romme, G. Singh, E. De Poorter, and W. Joseph, "Multistatic uwb radar-based passive human tracking using COTS devices," *IEEE Antennas and Wireless Propagation Letters*, vol. 21, no. 4, pp. 695–699, 2022.

[8] O. Kanhere and T. S. Rappaport, "Position location for futuristic cellular communications: 5G and beyond," *IEEE Communications Magazine*, vol. 59, no. 1, pp. 70–75, 2021.

[9] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A formal analysis of 5G authentication," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS '18*, (New York, NY, USA), p. 1383–1396, Association for Computing Machinery, 2018.

[10] J. A. Kurtz, "Chapter 5 - WAPs in commercial and industrial contexts," in *Hacking Wireless Access Points* (J. A. Kurtz, ed.), pp. 63–76, Boston: Syngress, 2017.

[11] T. Wilding, E. Leitinger, and K. Witrals, "Multipath-based localization and tracking considering off-body channel effects," 2021.

[12] F. M. Schubert, M. L. Jakobsen, and B. H. Fleury, "Non-stationary propagation model for scattering volumes with an application to the rural lms channel," *IEEE Transactions on Antennas and Propagation*, vol. 61, no. 5, pp. 2817–2828, 2013.

[13] E. Leitinger, P. Meissner, C. Rüdiger, G. Dumhart, and K. Witrals, "Evaluation of position-related information in multipath components for indoor positioning," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 11, pp. 2313–2328, 2015.

[14] A. Guerra, F. Guidi, and D. Dardari, "Single-anchor localization and orientation performance limits using massive arrays: MIMO vs. Beamforming," *IEEE Transactions on Wireless Communications*, vol. 17, no. 8, pp. 5241–5255, 2018.

[15] P. Bahl and V. Padmanabhan, "Radar: an in-building rf-based user location and tracking system," in *Proceedings IEEE INFOCOM 2000. Conference on Computer Communications. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (Cat. No.00CH37064)*, vol. 2, pp. 775–784 vol.2, 2000.

[16] William C. Stone, "National institute of standards and technology, construction automation program report no. 3, electromagnetic signal attenuation in construction materials," <https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir6055.pdf>, 1997.

[17] N. Hosseini, M. Khatun, C. Guo, K. Du, O. Ozdemir, D. W. Matolak, I. Guvenc, and H. Mehrpouyan, "Attenuation of several common building materials: mmwave frequency bands 28, 73, and 91 GHz," *IEEE Antennas & Propagation Magazine*, vol. 63, no. 6, pp. 40–50, 2021.

[18] 3GPP TS 36.101, "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception," tech. rep., 3rd Generation Partnership Project, 2022.

[19] K. Witrals, P. Meissner, E. Leitinger, Y. Shen, C. Gustafson, F. Tufvesson, K. Haneda, D. Dardari, A. F. Molisch, A. Conti, and M. Z. Win, "High-accuracy localization for assisted living: 5G systems will turn multipath channels from foe to friend," *IEEE Signal Processing Magazine*, vol. 33, no. 2, pp. 59–70, 2016.

[20] S. A. Ahmed, D. P. Dogra, S. Kar, and P. P. Roy, "Trajectory-based surveillance analysis: A survey," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 29, no. 7, pp. 1985–1997, 2019.