A privacy-preserving protocol for indoor Wi-Fi localization

University College Cork, Cork Ireland

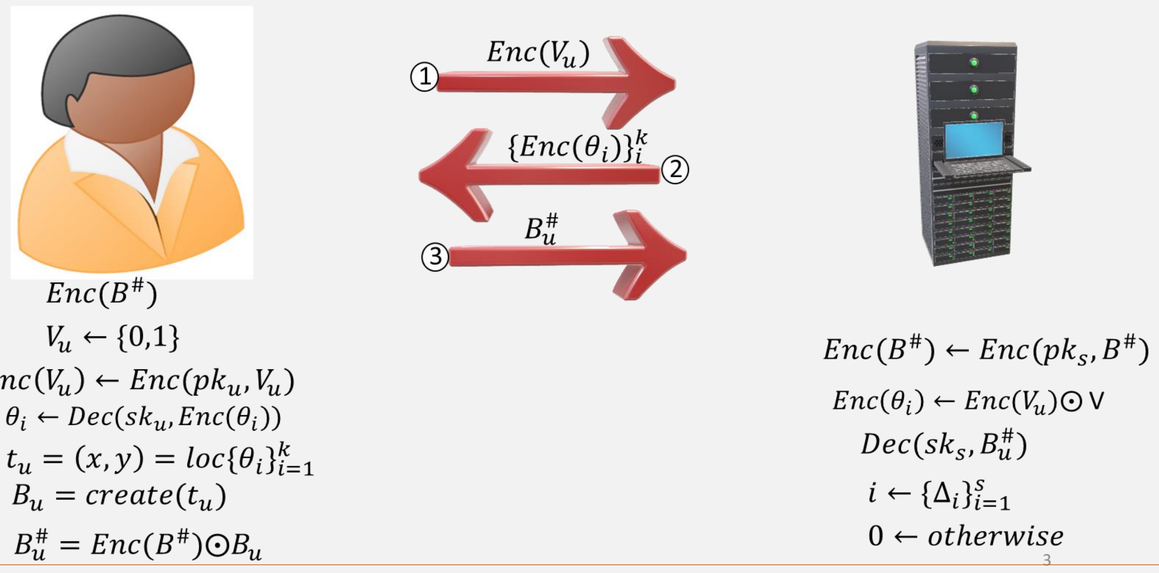
SAMUEL N. ESHUN
s.eshun@cs.ucc.ie

Supervisor: PAOLO PALMIERI
p.palmieri@cs.ucc.ie

Background

Indoor localization is gaining popularity due to the weak signals of GPS in an indoor environment. As a result, Wi-Fi fingerprinting is becoming increasingly popular as an alternative as it allows localizing users in an indoor environment. However, there are privacy concerns that come with indoor localization, especially in sensitive settings such as an airport or hospital. To solve this problem, most of the literature focuses on the privacy of the user neglecting the Service Provider (SP), thereby exposing the SP's database. Another area that has not been adequately addressed so far is how the SP can have real-time access to the user's location without, at the same time violating the user's privacy. For example, an employer may wish to monitor his employees in areas deemed sensitive, without violating their privacy elsewhere in the building; and can this be achieved indoor with a secured database that cannot be used for malicious activities by users?

Privacy preserving protocol for indoor Wi-Fi



Security definitions

- The protocol uses an *honest-but-curious* security model, i.e. both parties will follow the protocol but try to learn additional information about the other
- The protocol is secure if a user's exact location:
  - Is privacy preserved and
  - the server learns only the predefined area of interest of the user's location but not the exact location
- The protocol is data privacy preserved if the user is unable to
  - Obtain the list of reference Wi-Fi fingerprint (the Radio map)
  - Privacy of the predefined areas encoded in the filter are preserved

The Euclidean distance (θ)

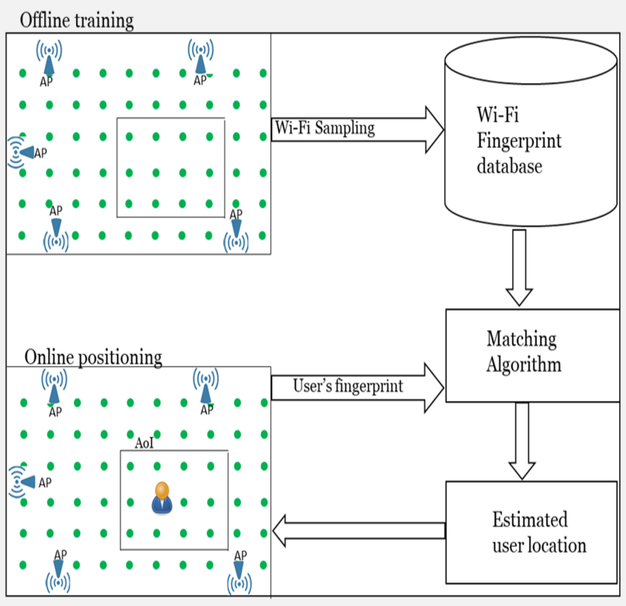
- $\theta = \|V_i - V_{u_i}\| = \sqrt{\sum_{j=1}^{N}(V_i - V_{u_j})^2}$
- $\theta = \|V_i - V_{u_i}\|^2 = \sum_{j=1}^{N}(r_{ij} - r_{u_j})^2$
- $\sum_{j=1}^{N} r_{ij}^2 + \sum_{j=1}^{N} r_{u_j}^2 + \sum_{j=1}^{N} -2r_{ij} \cdot r_{u_j}$

Applying the properties of homomorphic encryption yields:

- $\prod_{j=1}^{N} enc(r_{ij}^2) \cdot enc(r_{u_j}^2) \cdot enc(-2r_{ij} \cdot r_{u_j})$
  - $where\ enc\left(-2r_{ij} \cdot r_{u_j}\right) = enc(-2r_{u_j})^{r_{ij}}$

Wi-Fi Fingerprinting

- The process is divided into two-phases:
  - Offline phase
  - Online phase



Wi-Fi fingerprint reference database

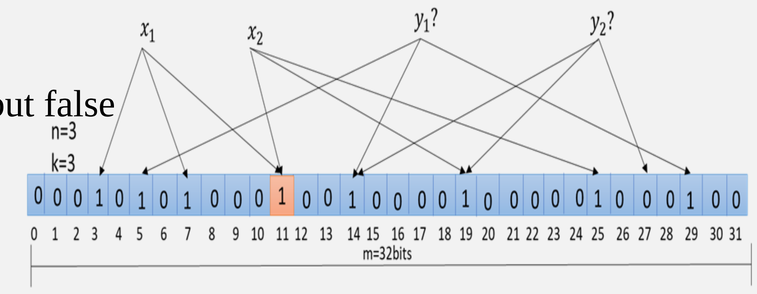
l_i	ap_1	ap_2	ap_3	⋯	ap_n
1	$r_{1,1}$	$r_{1,2}$	−100	⋯	$r_{1,n}$
2	−100	$r_{2,2}$	$r_{2,3}$	⋯	−100
3	$r_{3,1}$	−100	$r_{3,3}$	⋯	$r_{3,n}$
⋮	⋮	⋮	⋮	⋮	⋮
l	$r_{l,1}$	$r_{l,2}$	−100	⋯	$r_{l,n}$

Security Discussion

- Privacy of the user:
  - User's fingerprint sent to the server is encrypted
  - The server cannot determine the closest neighbors of the user's location without the user's private key
  - The exact location is encoded using spatial Bloom filter before being sent to the server
  - The filter is permuted to conceal the exact location of the user from the server
  - The server learns only the area of interest after decrypting the filter
  - The server learns nothing about the user's location if the user is not in the area of interest
- Privacy of the Server:
  - The closest neighbours are always blinded with a random number to prevent the user from knowing the Euclidean distances
  - The server encrypts the filter with the predefined encoded areas before sending to the user
  - The user cannot determine the predefined areas without the server's secret key

Bloom Filters

- Data structure to approximate set membership queries
- No knowledge of the set
- False positives are allowed, but false negatives are not possible
- M binary set with $0s$
- Given set $S = \{x_1, x_2, x_3\}$
- $H = \{h_1, \dots, h_k\}$ $H: \{0,1\}^* \rightarrow \{1, \dots, m\}$
- Insert set members by:
  - if $h_i(x_i) = a$ set $B\{a\} = 1$
- To check if $y \in S$
  - $[h_i(y)] = 1$ for all k hash functions, minus the probability of false positive



Conclusion and future works

- The two-party protocol for indoor localization guarantees the location privacy of the user using homomorphic encryption
- Most of the computational overhead at the user-side is delegated to the server while hiding the exact location
- The user cannot determine the predefined areas
- The protocol preserves the privacy of the SP's database
- The server can only learn the user's location in predefined areas but not the exact location
- Designing a two-party protocol against malicious (active) adversaries
- A three-party model defending against malicious adversaries to outsource most of the computation to the user-side

Samuel N. Eshun and Paolo Palmieri. 2019. A privacy-preserving protocol for indoor wi-fi localization. In Proceedings of the 16th ACM International Conference on Computing Frontiers (CF '19). ACM, New York, NY, USA, 380-385. DOI: https://doi.org/10.1145/3310273.3323400