POSTER: Enclave-Based Privacy-Preserving Localization

Joseph I. Choi
University of Florida, Gainesville, FL
choijoseph007@ufl.edu

Dave (Jing) Tian
University of Florida, Gainesville, FL
daveti@ufl.edu

Tyler Ward
University of Florida, Gainesville, FL
tsward@ufl.edu

Kevin R. B. Butler
University of Florida, Gainesville, FL
butler@ufl.edu

Patrick Traynor
University of Florida, Gainesville, FL
traynor@ufl.edu

John M. Shea
University of Florida, Gainesville, FL
jshea@ece.ufl.edu

Tan F. Wong
University of Florida, Gainesville, FL
twong@ece.ufl.edu

ABSTRACT

In cooperative spectrum sensing, multiple sensors work together to perform tasks such as localizing a target transmitter. However, the exchange of spectrum measurements leads to exposure of the physical location of participating sensors. Furthermore, in some cases, the sensitive characteristics of all participants can be revealed through the compromise of any one sensor. Accordingly, without guarantees about how data will be handled, there is little reason for such devices to work together. In this work, we protect the location of sensors cooperating in spectrum sensing by processing measurements within attestable containers, or enclaves. We use the enclave as a building block for new privacy-preserving particle filter protocols. We instantiate this enclave using Intel Software Guard Extensions (SGX) and investigate how the inclusion of enclaves impacts sensor privacy, carefully enumerating the different threats present in centralized and decentralized architectures. We show that enclave-based particle filter protocols incur minimal overhead (adding 16 milliseconds of processing to the measurement processing function versus unprotected computation), whereas cryptographically-based approaches suffer from multiple orders of magnitude greater costs. Our work demonstrates that enclaves can be effectively deployed in a decentralized architecture while dramatically improving current data handling techniques.

CCS CONCEPTS

• **Security and privacy → Privacy-preserving protocols**; *Mobile and wireless security.*

KEYWORDS

localization; location privacy; enclave

ACM Reference Format:
Joseph I. Choi, Dave (Jing) Tian, Tyler Ward, Kevin R. B. Butler, Patrick Traynor, John M. Shea, and Tan F. Wong. 2019. POSTER: Enclave-Based Privacy-Preserving Localization. In *WiSec '19: ACM Conference on Security and Privacy in Wireless and Mobile Networks, May 15–17, 2019, Miami, FL, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3317549.3326307

1 INTRODUCTION

Cooperative spectrum sensing allows for wireless devices to cooperatively measure channel usage across space, frequency, and time. An important application of this sensing is cooperative localization[1] of RF emitters. Sensors deployed in multiple locations collect and exchange measurements of a transmitted signal to arrive at a more precise measurement than any one sensor could produce alone.

The location of participating sensors should be kept private, but an adversary may use the exchanged information to localize the sensors. In many scenarios, sensors are owned by multiple parties. Even in cases where all sensors are under the control of a single party (e.g., military applications), the compromise of a single device may yield the potentially sensitive locations of all other sensors.

To minimize data leakage, we consider a new application of *enclave-based computing* to preserve the location privacy of sensors. An enclave is an example of a trusted execution environment (TEE), whereby secure regions of memory are maintained that allow unobservable execution of code. We make the following contributions:

- **Apply Enclave-Based Computing to Spectrum Sensing:** We demonstrate that the application of cryptographic techniques creates too much overhead for practical use. We instead apply an enclave-based approach to protect data.
- **Design and Implement SGX-Hardened Sensing:** We design and implement a particle filter-based protocol for localization, and protect the execution of this system using Intel Software Guard Extensions (SGX), demonstrating its application in centralized and decentralized architectures.
- **Measure and Evaluate Performance using Enclaves:** We demonstrate that our approach substantially improves security over traditional mechanisms, with minimal overhead.

2 DESIGN CONSIDERATIONS

We begin by discussing two threat models, based on how data is aggregated by cooperating sensors. We then justify the selection

[1] Applications of localization include finding adversarial jammers, locating pirate radio stations and cellular towers, tracking submarines, and pinpointing distress beacons.

WiSec '19, May 15–17, 2019, Miami, FL, USA

ACM ISBN 978-1-4503-6726-4/19/05.
https://doi.org/10.1145/3317549.3326307

of enclave-based techniques by exploring the tradeoffs inherent to using solely cryptographic-based techniques.

2.1 Threat Model

We are primarily concerned with preserving location privacy: no participant (including a centralized fusion center (FC)) should be able to determine the physical location of any other participant.

2.1.1 Centralized Architecture. The FC is untrusted and potentially malicious. The FC may use collected particles to break the location privacy of all participants. The FC may not faithfully perform the computation, outputting an incorrect/skewed result.

Unless a sensor colludes with the FC, it gains no access to the particles of other sensors. We assume sensors are honest-but-curious.[2]

2.1.2 Decentralized Architecture. No trusted third party such as a permanent FC is present. A new node is elected (through a consensus protocol[3]) as the "leader" for each localization round. The remaining nodes form a tree structure to efficiently pass and process observations that are ultimately communicated to the leader. This architecture also relies on the establishment of symmetric keys between pairs of sensors, generally coordinated by the leader.

The majority of sensors are assumed to be honest-but-curious. An adversarial sensor can break the location privacy of its children. Without colluding, the leader cannot break location privacy.

2.2 Cryptographic Approaches

Dramatic advances in the performance of cryptographically-based, secure multiparty computation (MPC) algorithms makes such techniques[4] potentially attractive for deployment in this setting. Unfortunately, they remain extremely resource-intensive. For instance, recent work demonstrated that garbled circuit-based techniques required an average of 300x increase in runtime for relatively small circuits [1]. For large inputs and circuit sizes, performance is slowed by *four to five orders of magnitude* [2]. The setting of our particular application, where cost of wireless communications and availability of spectrum are generally precious, makes cryptographically-based approaches even less practical.

3 DESIGN AND IMPLEMENTATION

We consider the addition of enclaves to both centralized and decentralized architectures. We use Intel SGX to instantiate the enclave.

3.1 Centralized Architecture

We require the FC to host an enclave for receiving and correctly processing sensor inputs. Enclaves are not needed at the sensors.

3.2 Decentralized Architecture

To support role agility,[5] we require all sensors to be SGX-enabled. The leader may perform preliminary signal-to-noise ratio (SNR) processing outside an enclave, as SNR values provide only limited information about a sensor's relative location to the target.

3.3 Localization Algorithm

Centralized and *decentralized* indicate the nature of localization participants and the flow of messages between participants. The underlying algorithm is ultimately the same for either architecture.

We base our localization algorithm on the particle filter[6] [3–5]. Particles are quartets: $\langle latitude, longitude, PLE, weight\rangle$.

Simulation. We adapt the protocol proposed by Ward et al. [5], extract the core algorithm, and implement a simulator in C++.

Enclave. We place the simulation logic for the processing of input particles by each sensor into the enclave, ensuring the current sensor's latitude/longitude and RSS values are only used in-enclave.

4 EVALUATION

In our experiments,[7] we feed real spectral measurements (and corresponding GPS coordinates) to our simulation. We find:

- The cost of remote attestation is 3 seconds (on average).
- SGX-enabled simulation of particle processing within the enclave is slower than normal simulation, with 46.3% overhead in the case of 20,000 particles, or 15.9 ms (on average), which is negligible compared to the cost of remote attestation.

5 CONCLUDING REMARKS

We demonstrate that our proposed enclave-based approach using SGX adds minimal computational overhead to cooperative localization. More work is needed to (1) determine the applicability of our approach to ARM architectures, in which case we may instead build on TrustZone; (2) explore alternative, offline attestation schemes; and (3) extend our simulation to capture networking overhead.

ACKNOWLEDGMENTS

This work is supported in part by the US National Science Foundation under grant numbers CNS-1642973 and CNS-1540217.

REFERENCES

[1] Raad Bahmani, Manuel Barbosa, Ferdinand Brasser, Bernardo Portela, Ahmad Reza-Sadeghi, Guillaume Scerri, and Bogdan Warinschi. 2017. Secure Multiparty Computation from SGX. In *Proceedings of FC.*

[2] Joseph I. Choi, Dave (Jing) Tian, Grant Hernandez, Christopher Patton, Benjamin Mood, Thomas Shrimpton, Kevin Butler, and Patrick Traynor. 2018. *A Hybrid Approach to Secure Function Evaluation using SGX.* Technical Report FICS-TR-2018-0002. Florida Institute for Cybersecurity Research.

[3] Stiven S. Dias and Marcelo G. S. Bruno. 2013. Cooperative Target Tracking Using Decentralized Particle Filtering and RSS Sensors. *IEEE Transactions on Signal Processing* 61, 14 (July 2013).

[4] C. Morelli, M. Nicoli, V. Rampa, U. Spagnolini, and C. Alippi. 2006. Particle Filters for RSS-Based Localization in Wireless Sensor Networks: An Experimental Study. In *Proceedings of IEEE ICASSP.*

[5] Tyler Ward, Joseph I. Choi, Kevin Butler, John M. Shea, Patrick Traynor, and Tan Wong. 2017. Privacy Preserving Localization Using a Distributed Particle Filtering Protocol. In *Proceedings of IEEE MILCOM.*

[2] We assume sensors will provide particles generated from the correct measurements, as they have a common interest in localizing the target transmitter.

[3] We assume the consensus protocol cannot be gamed by an adversary to substantially increase its likelihood of becoming the leader.

[4] Because data is never decrypted by intermediaries, the guarantees offered by these techniques are extremely strong.

[5] Leaf sensors do not necessarily require enclaves; however, in a future ordering, what were previously leaf sensors may be placed higher in the hierarchy.

[6] Particle filters allow discretization of the posterior belief of a transmitter's location in a way that guarantees the amount of data being transferred. Particle filters are also well-suited for noisy measurement data (affected by real-world environmental irregularities) and an ambiguous channel path-loss exponent (PLE).

[7] We conduct our evaluation on an HP machine with an Intel Skylake quad-core CPU supporting SGXv1 and 8 GB of memory. The machine is equipped with Ubuntu version 18.04 and Intel SGX SDK version 2.4. Results are based on 100 runs.