Privacy Preserving Data Muling System

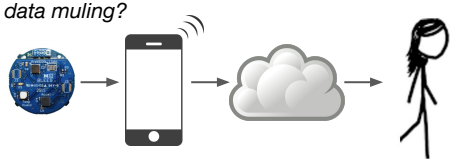
Project 2: Alvin Tan, Tess Despres, Jean-Luc Watson, Shishir Patil

Problem

Current data muling systems utilize metadata that can reconstruct mobility traces or social networks.

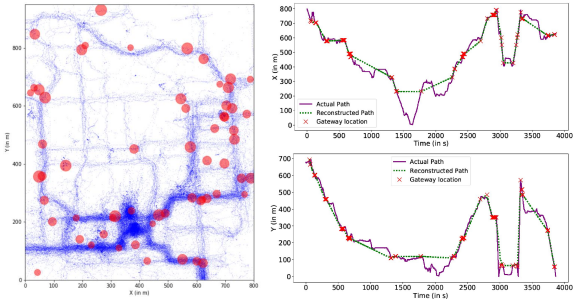
Background

What is data muling?



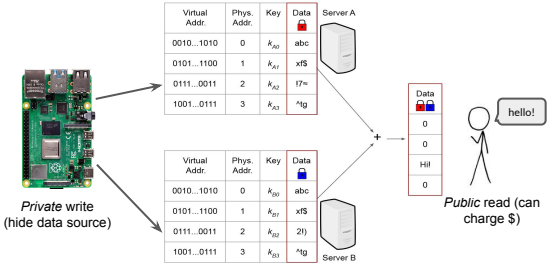
What are the privacy concerns?

We demonstrate mobility tracking through simulation using *only* sensor/mule IDs & time of transmission.

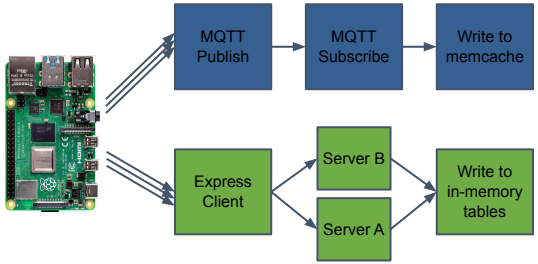


Solution

Use a state-of-the-art anonymous communication protocol, Express[1] (depicted below), to implement a privacy preserving data muling system.



We evaluate Express against a baseline plaintext implementation on hardware.

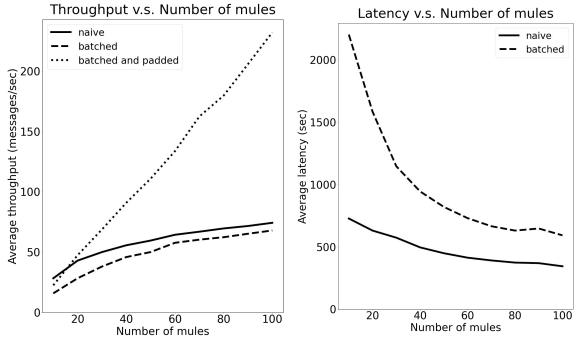


We also use a simulation to evaluate scalability with:

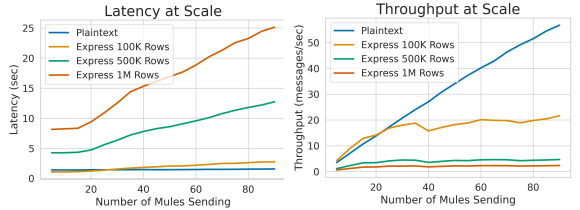
- 100 mobile mules (10-20m BLE range)
- 1000 stationary sensors (1-15m/s move speed)
- 128 byte data payloads

Results

Simulation:



System implementation:



Next Steps

- Energy evaluation of our system on embedded HW
- Bidirectional communication
- Batch writes to reduce latency
- Protection against malicious mules

[1] Eskandarian, S., Corrigan-Gibbs, H., Zaharia, M., & Boneh, D. (2021). Express: Lowering the cost of metadata-hiding communication with cryptographic privacy. In 30th USENIX Security Symposium (USENIX Security 21) (pp. 1775-1792).