Design of Privacy-Preserving Fog-assist Mobile Crowd Sensing Architecture with Ring Signature

Yin-Hong Hsu

05 10, 2018

Zero-knowledge Proof (ZKP)

- The Prover proves it hold the same secure message with the Verifier.
- No secure message will be revealed within the process.
- e.g. two candidates want to find out if they have the same amount of money without disclosing the exact amount.
- The difference between RS and ZKP is RS reveal all message public and preserve users' privacy by ring size; ZKP does not reveal any secure information.

Outline

Motivation

- In recent year, people are more focus on data monitoring and analysis.
- Also, more and more peripheral products for mobile phone and devices have become ubiquitous.
- It makes Mobile Crowd Sensing (MCS)[1] service more prosperity and flourish.
- How to preserve user's privacy and data correctness is the fundamental issue in MCS.

Mobile Crowd Sensing

- A Technology about user's communication, computing, sensing data collection and processing.
- Can do further analysis with sensing data.
- Collecting data from sensors like ambient light, location and movement.

Mobile Crowd Sensing

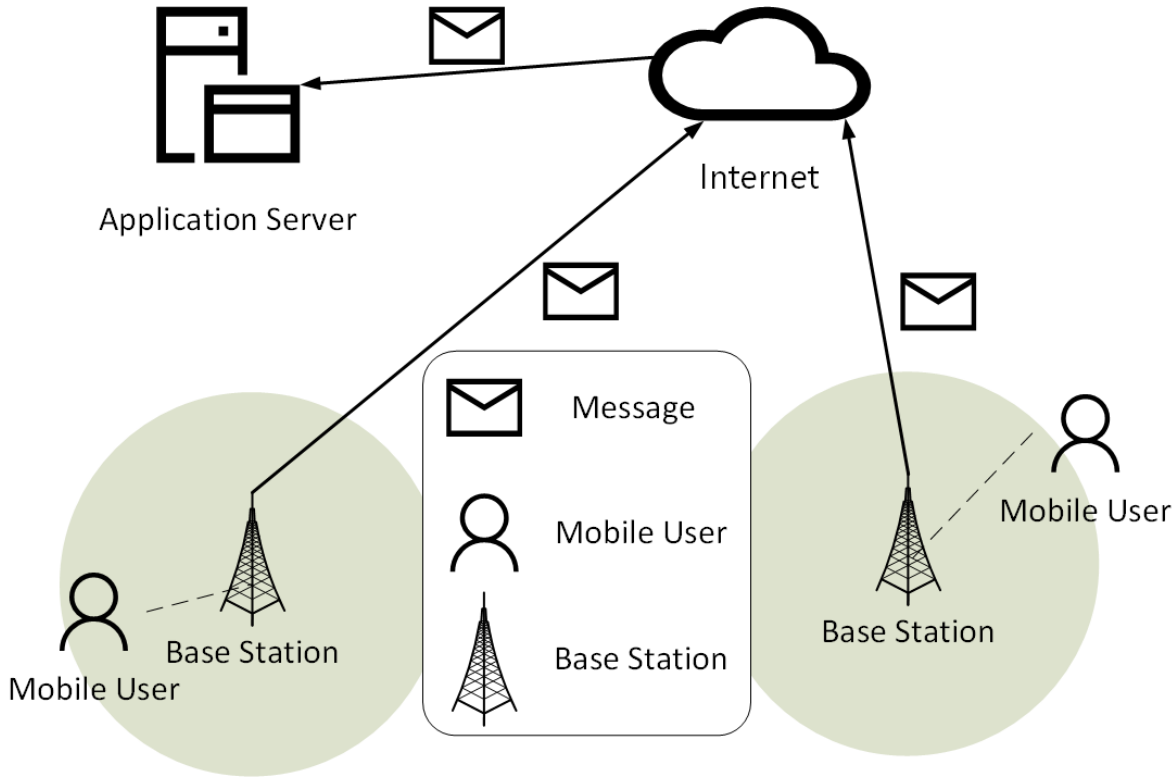


Figure: Mobile Crowd Sensing

Privacy issue

- Fulled of privacy-sensitive information.
- Privacy information leakage might cause user location exposure and further problems.
- To provide privacy-preserving MCS service is the critical issue.

Region-based Conditionally Anonymous Ring Signature 1/2

- Based on conditionally anonymous ring signature (CARS)[2].
- The ring is built up with mobile users' identity in the region.
- The region is composed of one or multiple base station.
- Inheriting features from CARS.
  - Trace
  - Revoke

Region-based Conditionally Anonymous Ring Signature 2/2

- Application Server (AS) will receive numerous upload request.
- Numerous upload request cause
  - Inadequate bandwidth
  - Network congestion
- Duplicated data.
- Fog-assist architecture.
  - Incoming connections to AS reduced
  - Fata pre-process

Fog computing

- Storage, applications, and data.
- Distributed cloud.
- Closer to end-user.

Proposed work

- A Mobile Crowd Sensing (MCS) architecture.
- A privacy-preserving mechanism in MCS.
- Alleviating network congestion caused by lots of upload request.
- Deduplicated data to save bandwidth and storage.

Illustration

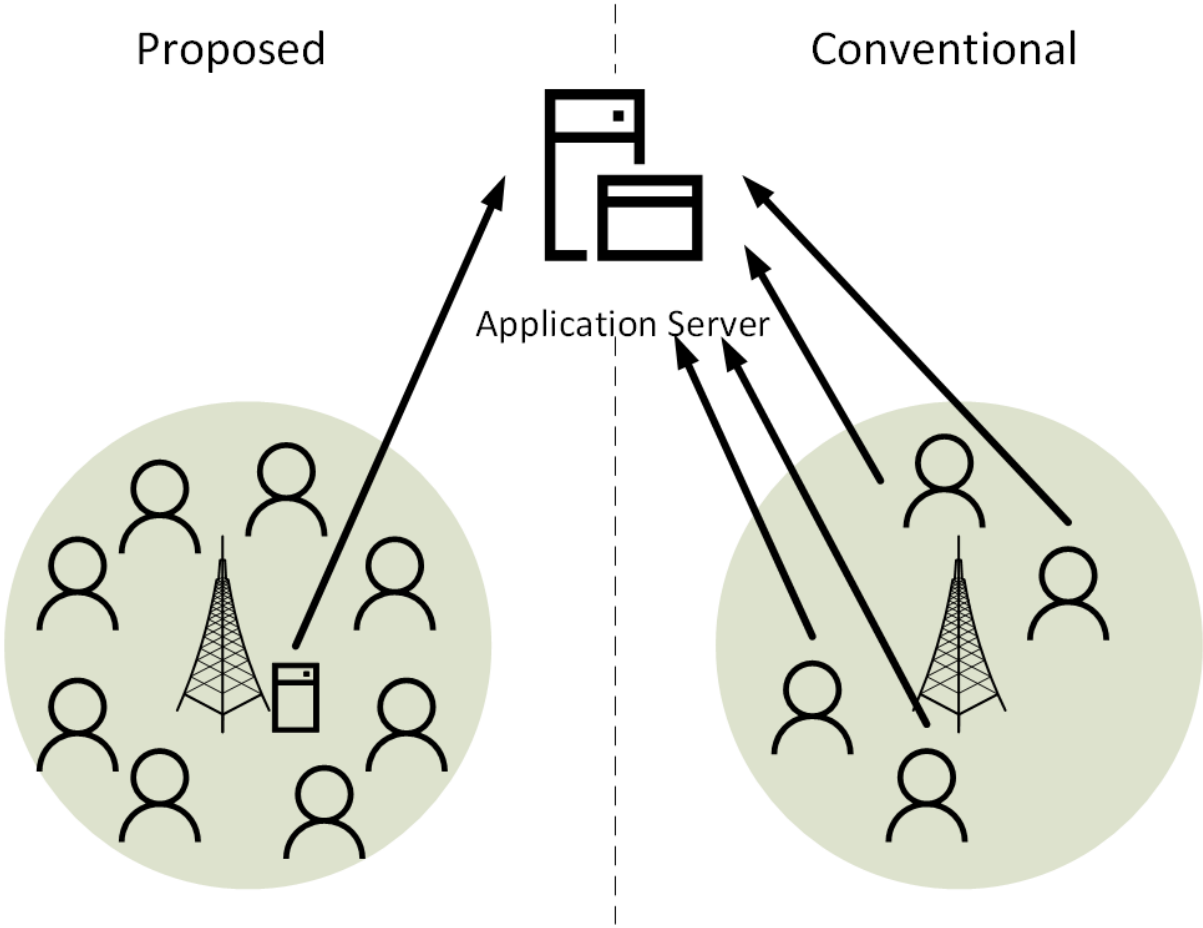


Figure: Comparing

Notation

Abbreviation	Description
Param	System parameter
KA	Key Authority
MU	Mobile User
FN	Fog Node
AS	Application Server
Msg	Message
ID_i	Identity of MU_i
eNB	eNodeB

Fog networking architecture

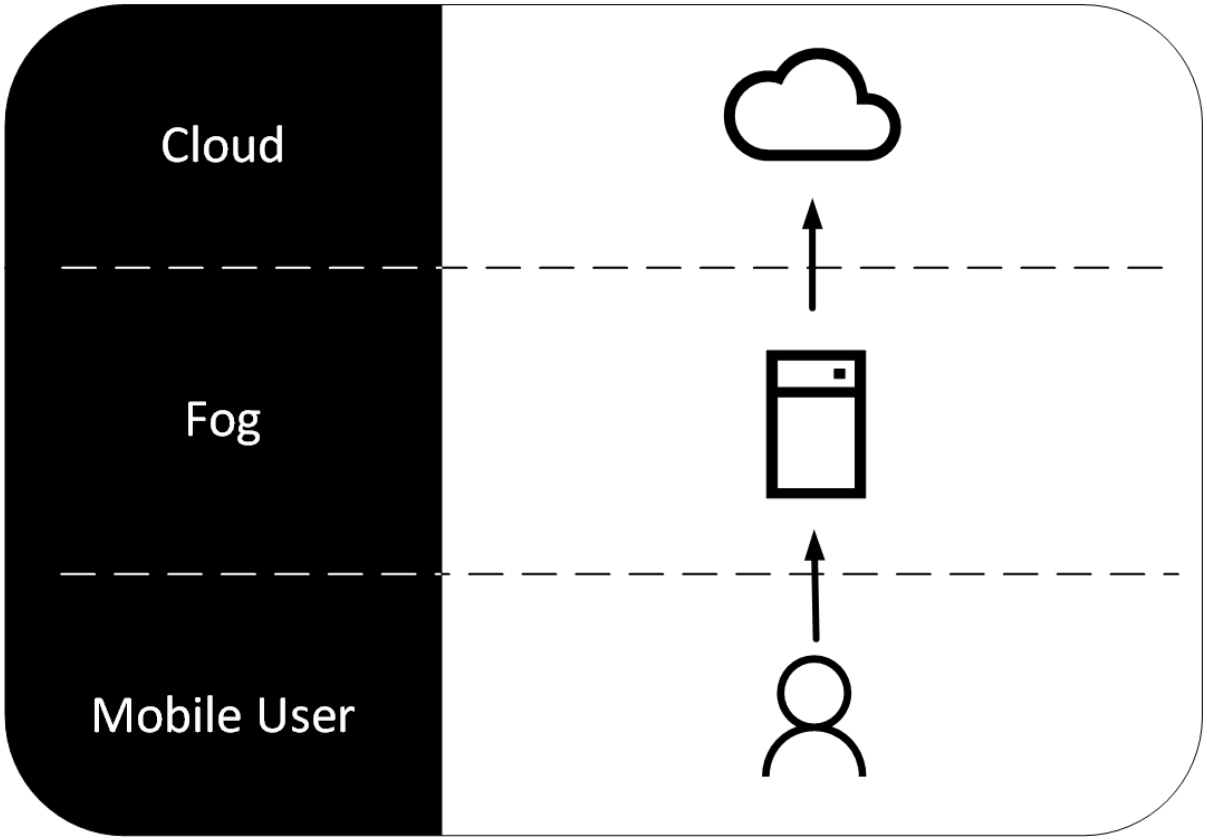


Figure: Fog networking architecture

Fog networking architecture 1/2

- Mobile device can self-organize, communicate with each other.
- Handling all communication for the near end-user.
- Fog Node act as a router, can communicate with each other.

Fog networking architecture 2/2

- Reduce traffic
- Improves service quality
- Minimizes latency
- Computation capability, can alleviate computation effort from Cloud.

Architecture

- This framework contain 3 layers
  - Cloud layer
  - Fog layer
  - Mobile user layer

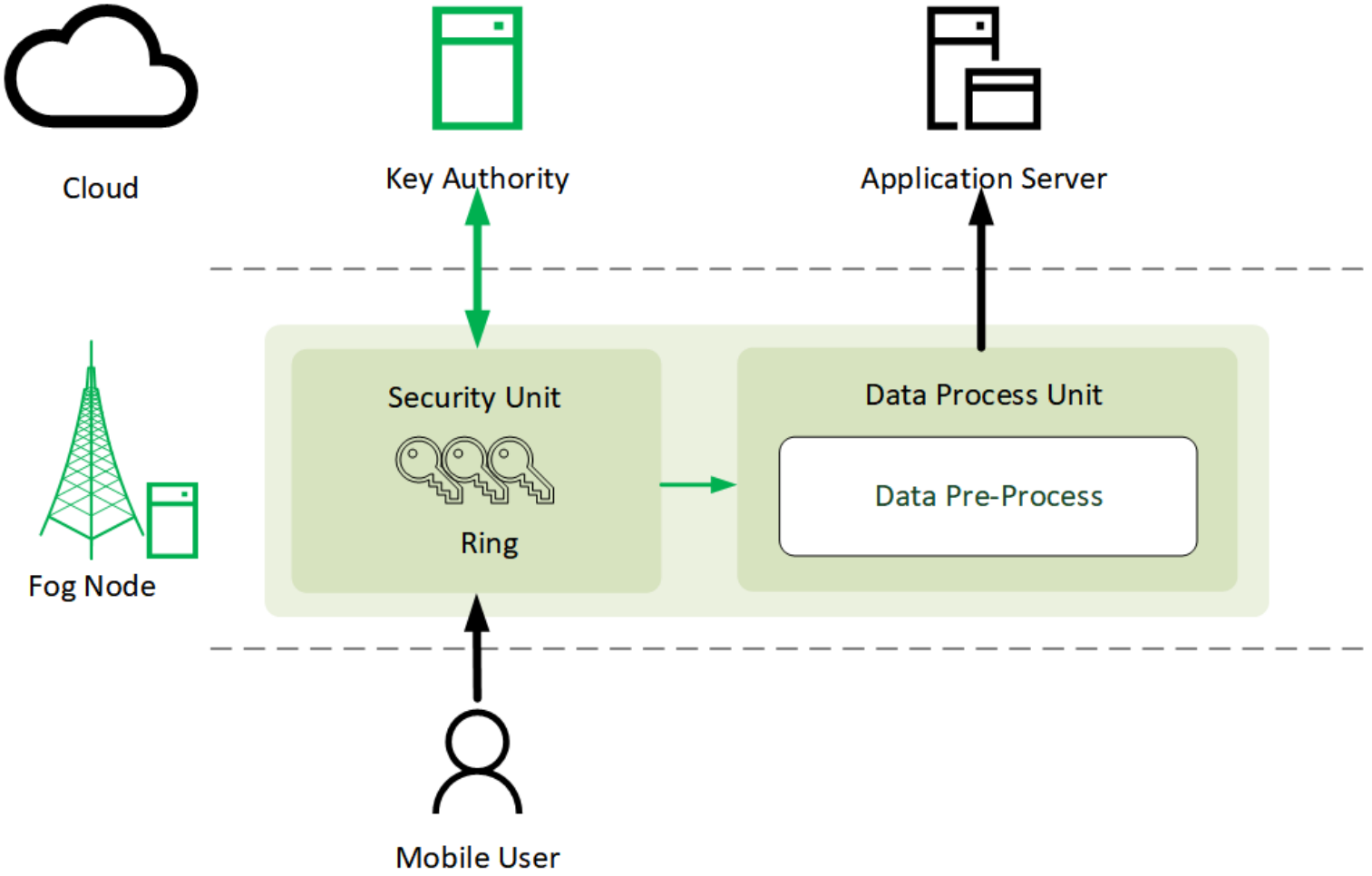


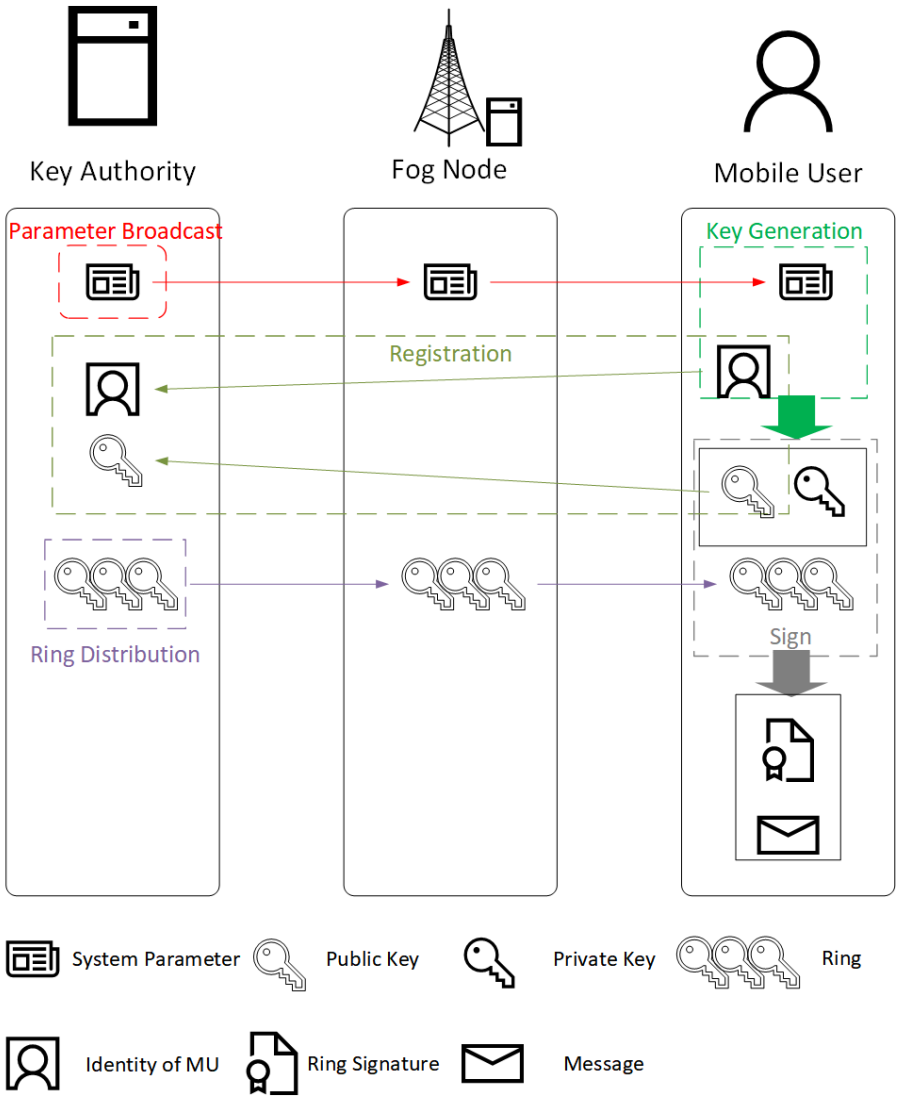
Figure: Architecture

Procedure

- Setup and Data signing
- Data upload and pre-process
- Mobile User Mobility and Ring Update

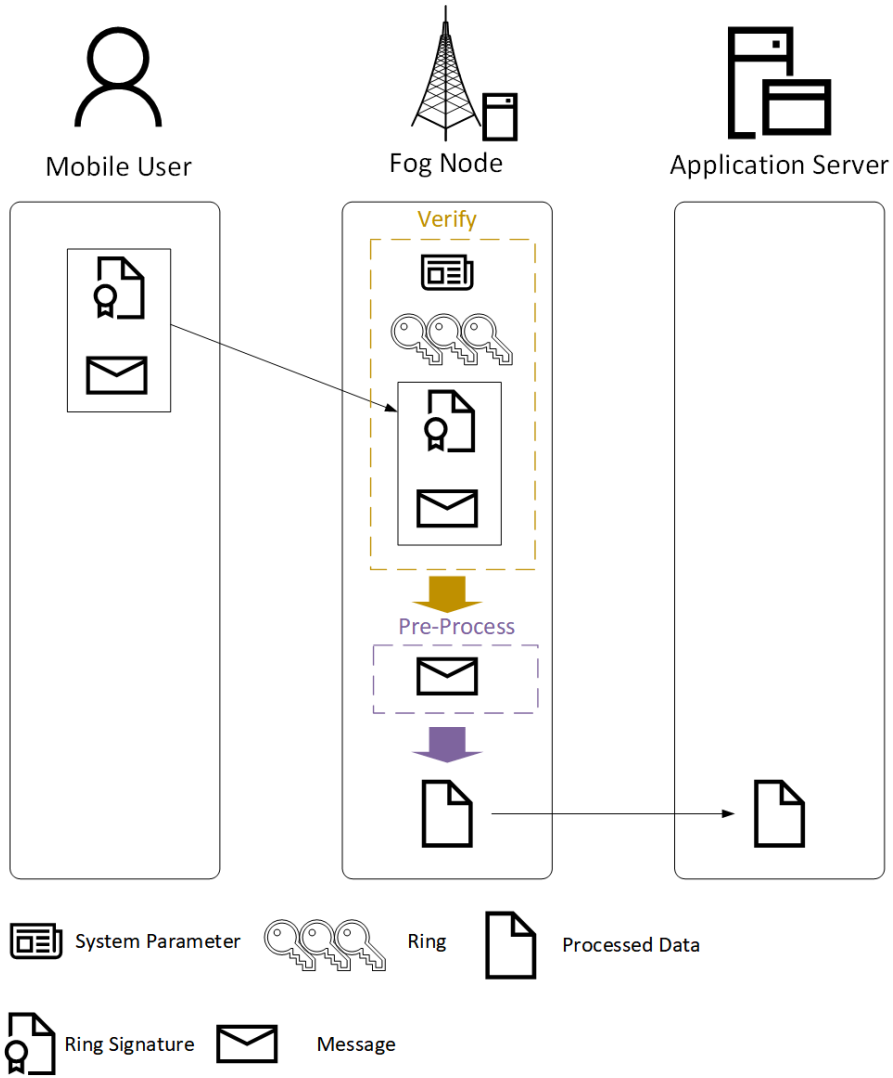
Setup

- This step contains parameter broadcasting, key generation, register...
- Can save bandwidth in Parameter Broadcasting and Ring Distribution step


Key Authority
Fog Node
Mobile User
Parameter Broadcast
Registration
Key Generation
Ring Distribution
Sign
System Parameter
Public Key
Private Key
Ring
Identity of MU
Ring Signature
Message

Data upload and pre-process

- Ring is in the Fog Node and MU, so the Application Server will not know the member in MCS service.
- Comparing to RCRS, the MU does not upload data directly to AS, but to the fog node and forward to AS.
- In data pre-processing step, the data will be deduplicated and structured


Mobile User
Fog Node
Application Server
Verify
Pre-Process
System Parameter
Ring
Processed Data
Ring Signature
Message

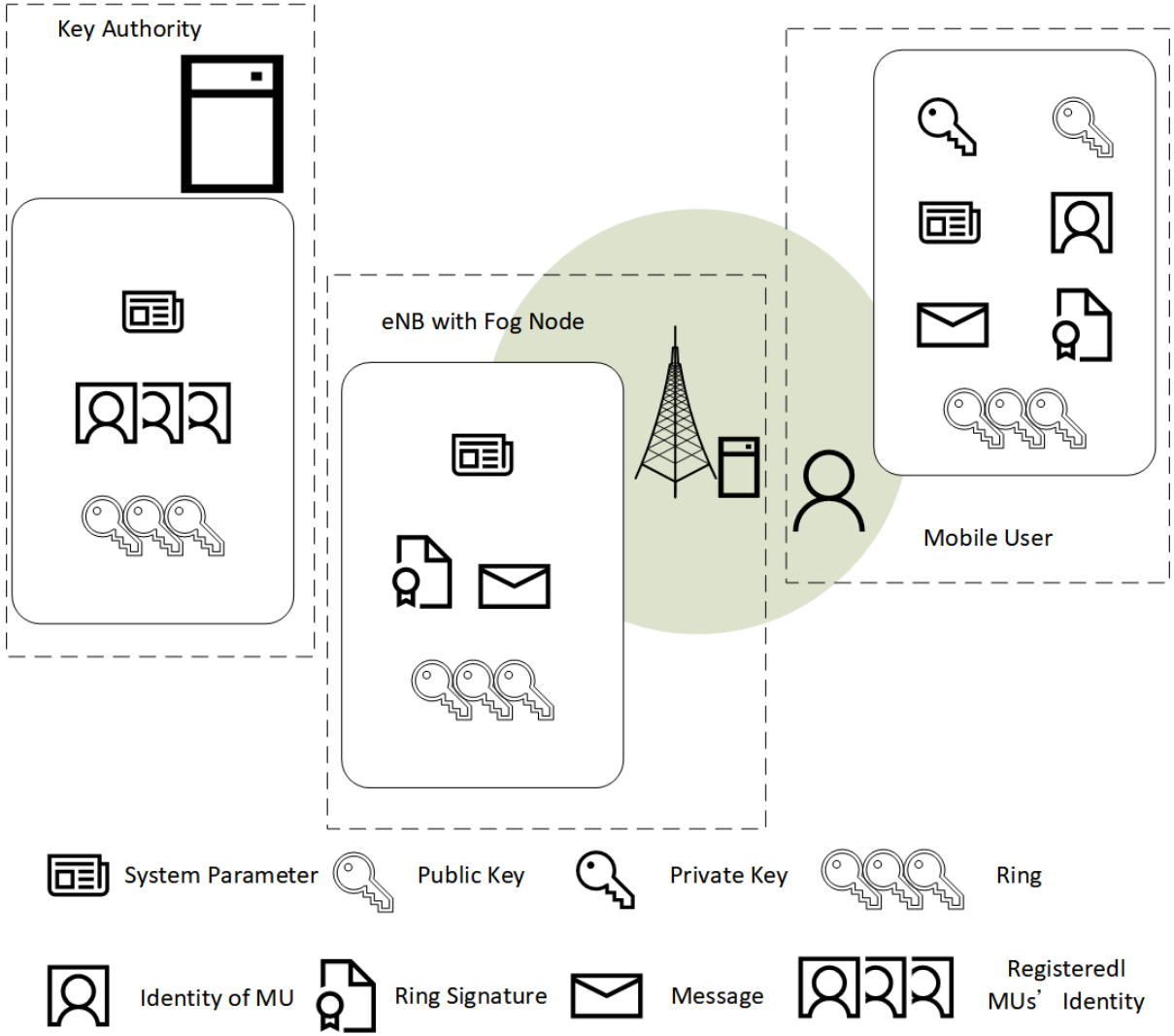


Figure: Data distribution

Mobile User Mobility and Ring Update

- When MU move to another region, the Fog Node will notify KA to move MU's public key to destination ring.
- MU only need to communicate with KA once (register).

Mobile User Mobility and Ring Update

- KA will distribute ring to each region periodic. In RCRS, KA have to broadcast to each MU, AS; In this work, KA only have to send new rings to Fog Nodes, then each Fog Node will distribute the ring to MUs in this region.

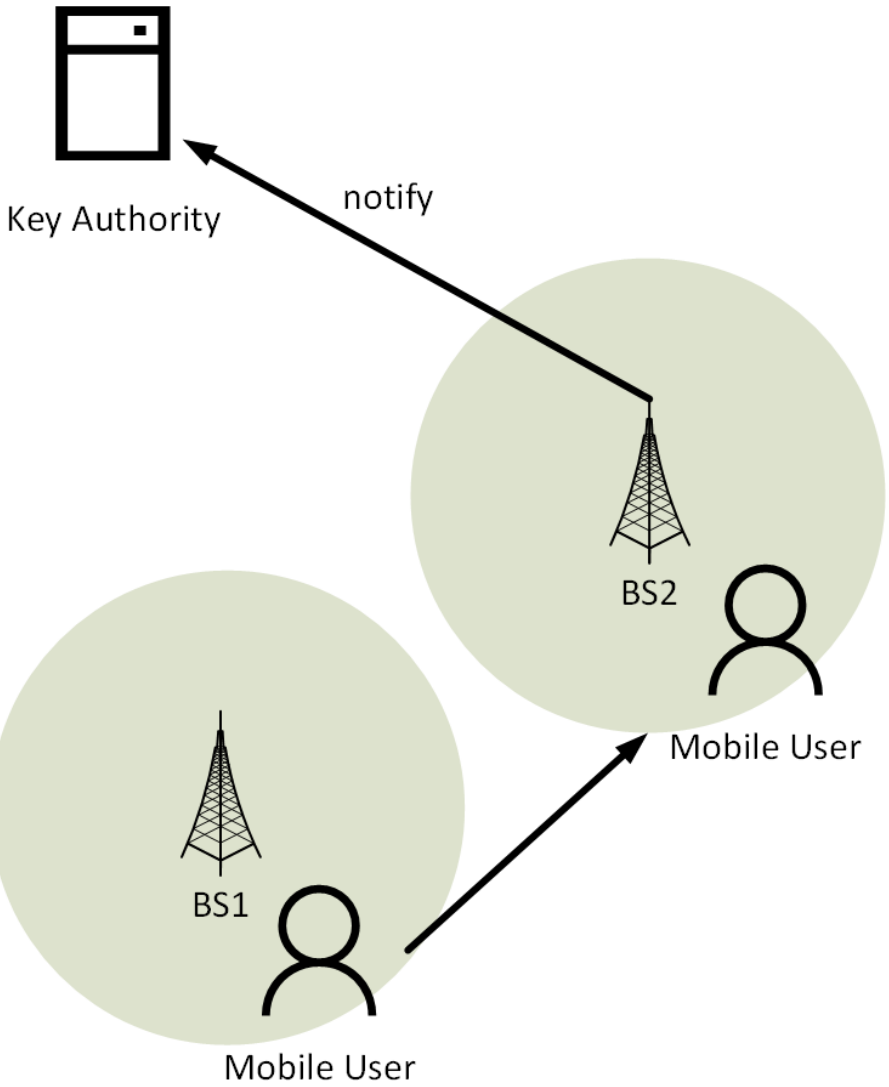


Figure: MU move to BS2 from BS1

Attack model

- trusted:
  - Key Authority
  - Fog Nodes
  - The connection between Fog Node and Fog Node
  - The connection between Fog Node and Key Authority
- untrusted:
  - Mobile User
  - Application Server
  - The connection between Mobile User and Fog Node
  - The connection between Fog Node and Application Server

Attack model

- Eavesdropping:
  - the adversary can eavesdrop get unsafe channels to get messages. In the region-based MCS, the sensed information and the corresponding ring signatures are sent through the Internet without encryption so the adversary can get all of them
- Replay attack:
  - after eavesdropping, the adversary can send a copy without modification to AS. In the RCRS, we have added a timestamp in the message structure to prevent this kind of attack so that the overdue messages would be abandoned

Attack model

- Brute force:
  - the adversary is able to try every possible keys and try to make the same signature as the one that matches the eavesdropped message. In the 256-bit RCRS scheme, the key space of MUs private key contains 2 256 possible keys. It is impossible to discover the MUs private key of the message without extremely powerful computing power
- Intersection attack:
  - If a specific signer changes the ring to use every time, the adversary can easily to find out what public key the signer is actually used

Attack model

- Location forgery:
  - In RCRS, if the MU was compromised by adversary, the adversary can tell KA that MU is leaving to another location. So that can remove MU from current ring.

References

[1] B. Guo, Z. Yu, X. Zhou, and D. Zhang, “From participatory sensing to mobile crowd sensing,” in *Proc. IEEE PERCOM 2014*, Mar. 2014, pp. 593–598.

[2] S. Zeng, S. Jiang, and Z. Qin, “An efficient conditionally anonymous ring signature in the random oracle model,” *Theoretical Computer Science*, vol. 461, pp. 106–114, Nov. 2012.

Thanks for Your Attentions