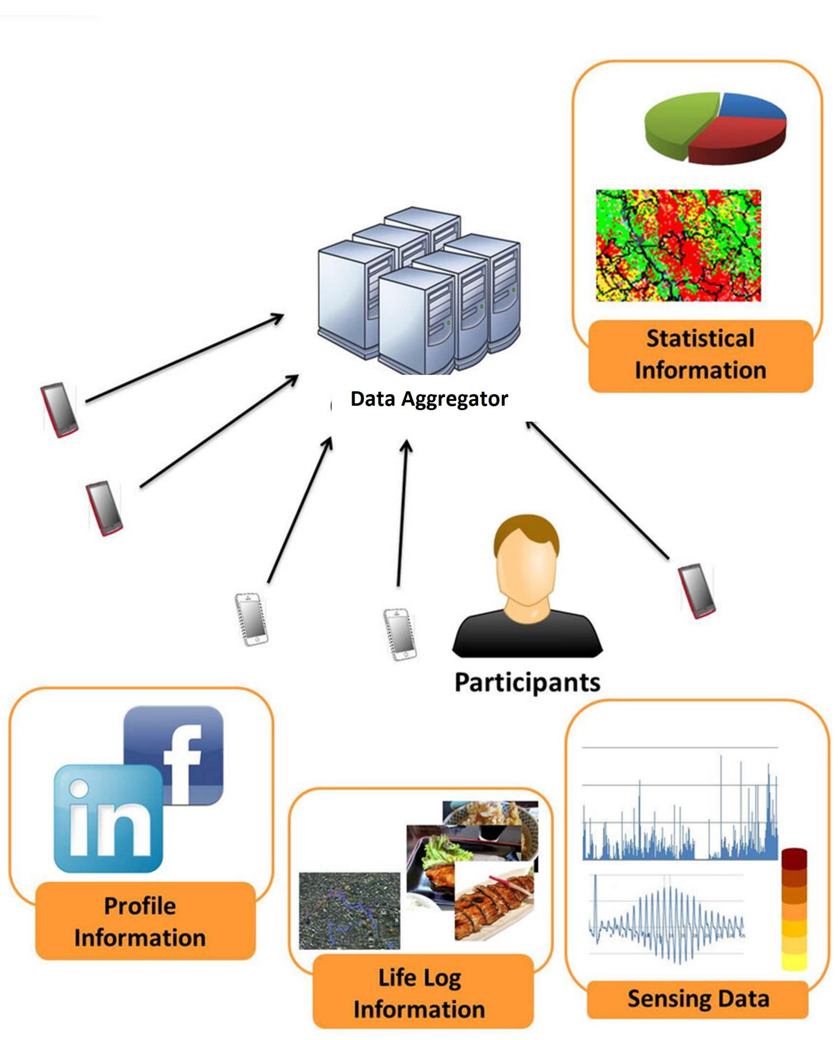
SeRaNDiP - Leveraging Inherent Sensor Random Noise for Differential Privacy Preservation In Wearable Community Sensing Applications

Ayanga Imesha Kumari Kalupahana, Ananta Narayanan Balaji, Xiaokui Xiao And Li-Shiuan Peh

National University of Singapore

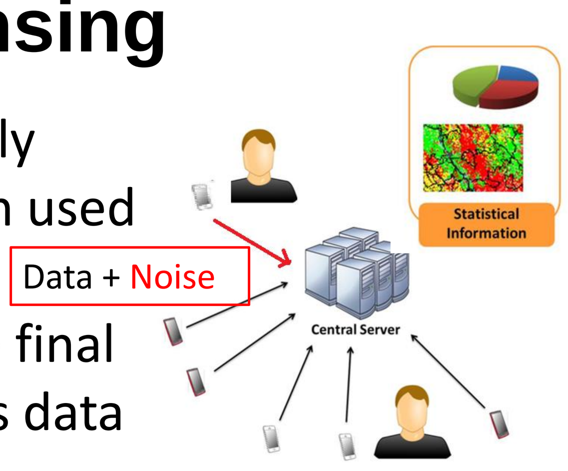
1.Introduction

- Wearable community sensing programs are conducted both locally and globally with hundreds of thousands and millions of community participation.
- Participants share their data: profile information, life log information, and sensing data using wearable devices to a central data aggregator to generate aggregated statistical information on the community.
- However, due to recent data breaches at the data aggregators, participants are/will be unwilling to take part in community sensing, if a formal guarantee of privacy preservation is not provided.

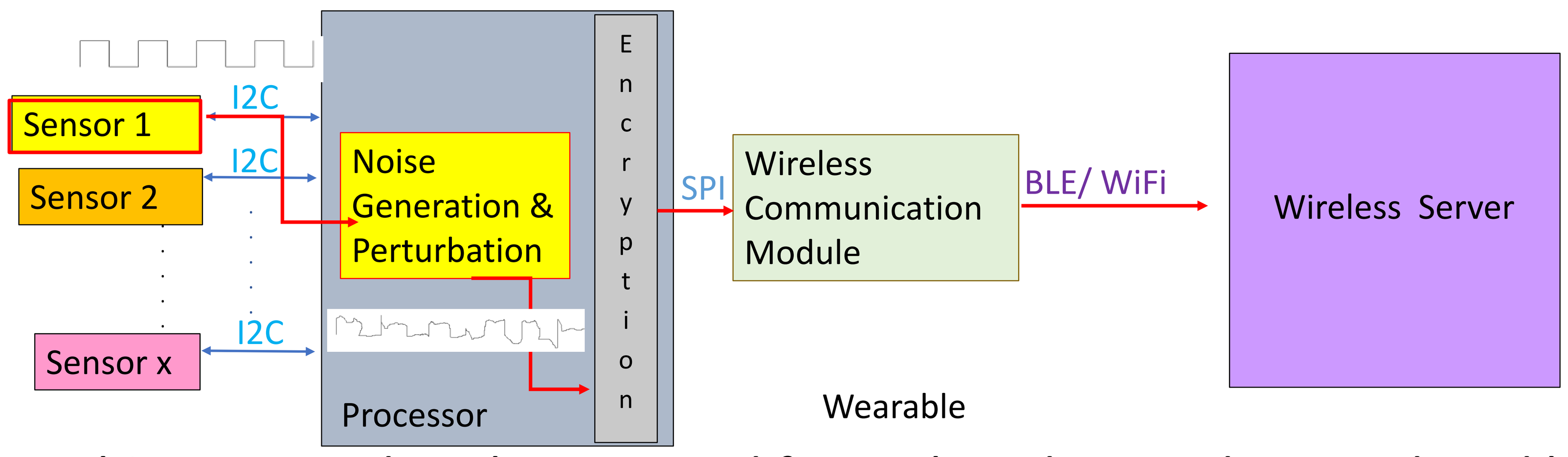


2. Differential Privacy in Wearable Community Sensing

- Differential Privacy (DP) which gives a statistically strong guarantee is a famous privacy mechanism used in community sensing
- Differential private systems make sure that the final released result is independent of the individual's data input.
- This is achieved by adding statistical noise to data before sharing it with the aggregator.



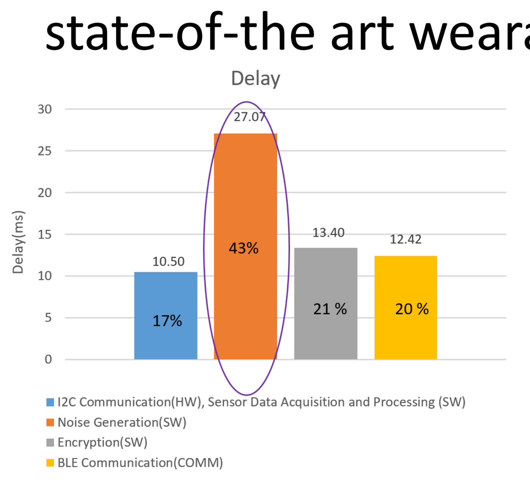
- Differential privacy has already been implemented in community sensing programs by both Apple and Google.
  - Local DP (variant of distributed DP) by Apple to learn popular emoji
  - Distribute DP by Apple and Google in Exposure Notification Privacy-preserving Analytics (ENPA) to COVID-19 management
  - The edge device is the smartphone
- Differential Privacy is enabled in state-of-the-art wearables by generating noise and perturbing sensor data at the processor.

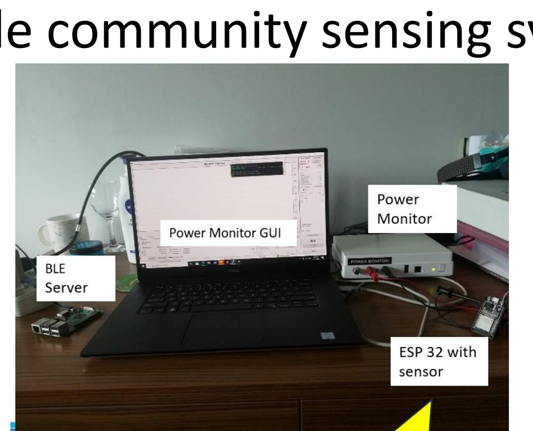


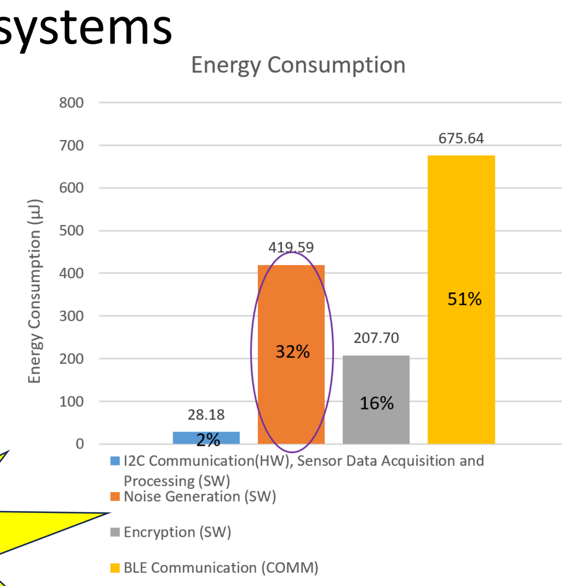
- This step needs to be repeated for each and every data produced by the sensor.

3. Explore the Overheads of Noise Generation for Wearable

- A simple wearable-based community sensing setup was implemented to measure delay and energy consumption by noise generation in state-of-the art wearable community sensing systems



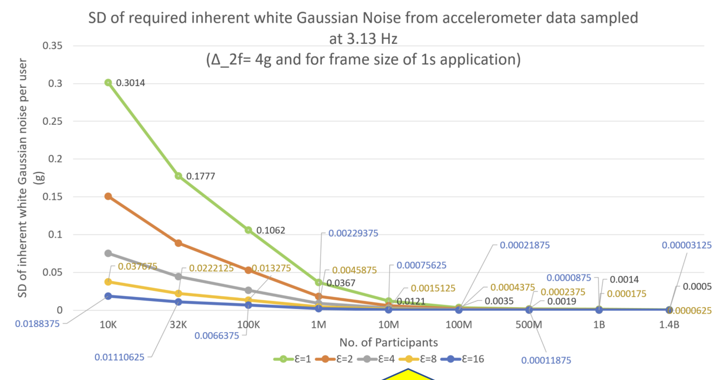




- Software noise generation
  - Adds 43% delay
  - Consumes 32% energy

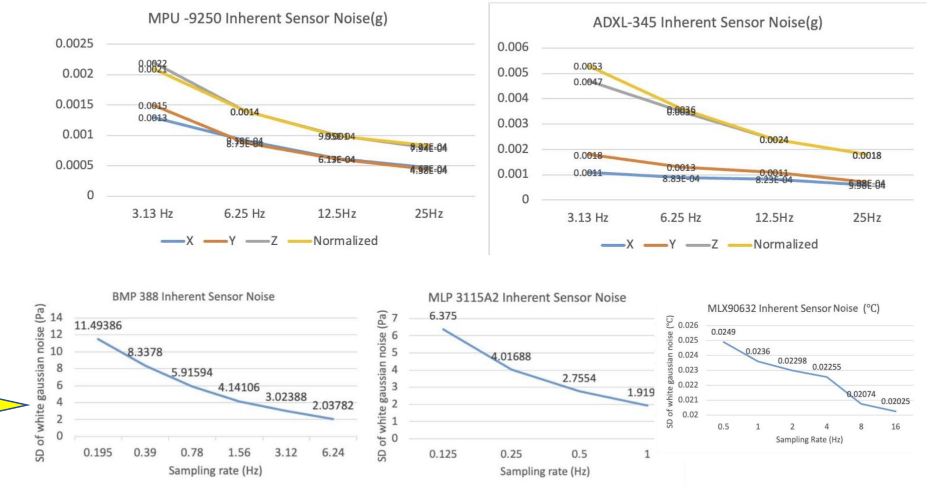
Time and energy loss is continuous

4. Differential Privacy Noise from Sensors

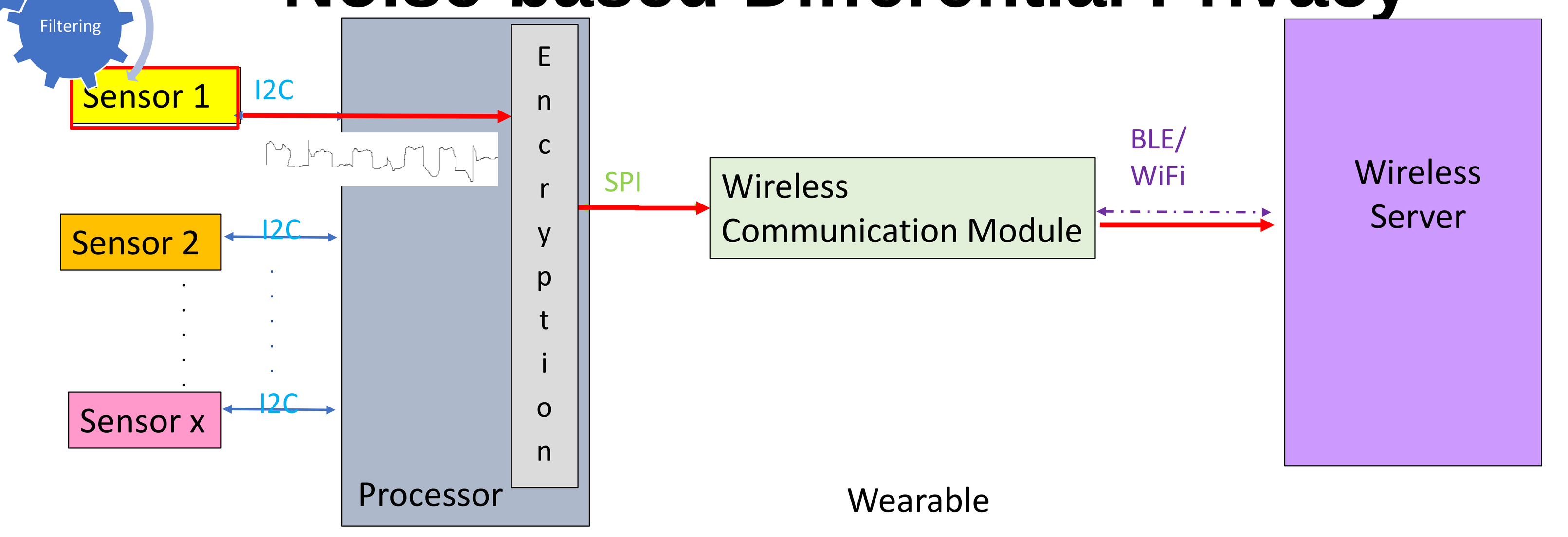


Sensors can satisfy Differential Privacy Requirements !!

SD of white Gaussian Noise available can be obtained using Allan Deviation Analysis

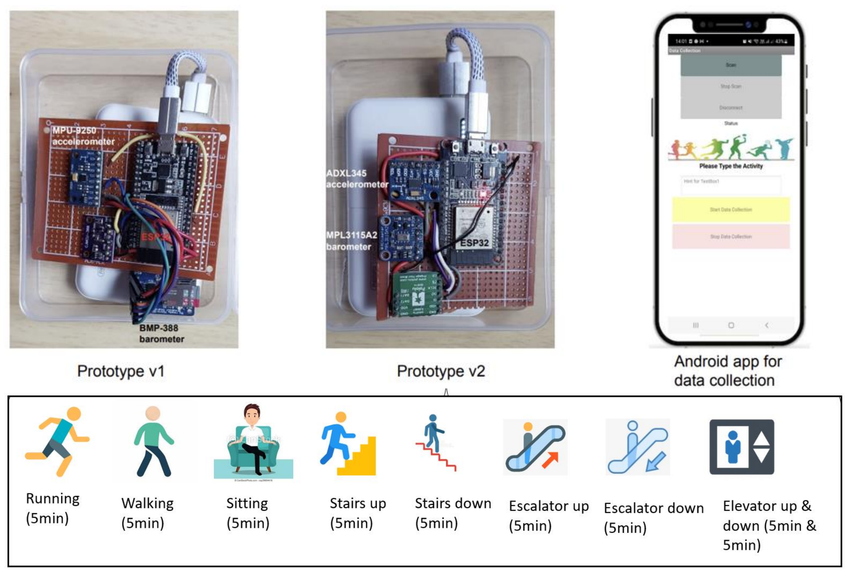


5.SeRaNDiP: Inherent Hardware Sensor Noise-based Differential Privacy



6. Evaluation

a) User Study



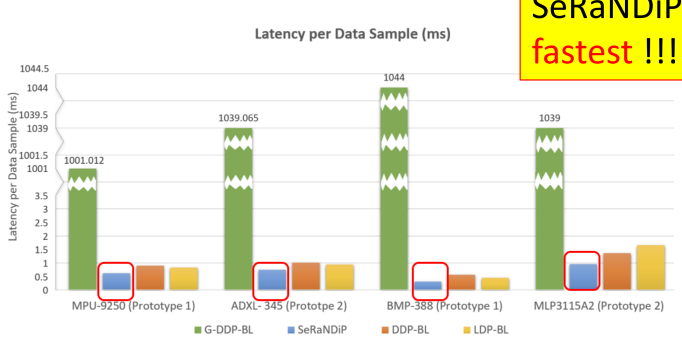
b) User-level Accuracy Evaluation

Classifier	Model	Accuracy
Physical Activity Classification	MPU 9250 Accelerometer (SeRaNDiP)	84%
	MPU 9250 Accelerometer (DDP-BL [2])	84%
	MPU 9250 Accelerometer (LDP-BL [3])	84%
	MPU 9250 Accelerometer (G-DDP-BL [4])	84%
	ADXL 345 Accelerometer (SeRaNDiP)	72%
	ADXL 345 Accelerometer (DDP-BL [2])	72%
	ADXL 345 Accelerometer (LDP-BL [3])	72%
	ADXL 345 Accelerometer (G-DDP-BL [4])	72%
Vertical Activity Classification	BMP 388 Barometer (SeRaNDiP)	64.42%
	BMP 388 Barometer (DDP-BL [2])	64.42%
	BMP 388 Barometer (LDP-BL [3])	64.42%
	BMP 388 Barometer (G-DDP-BL [4])	64.42%
	MLP3115A2 Barometer (SeRaNDiP)	52%
	MLP3115A2 Barometer (DDP-BL [2])	52%
	MLP3115A2 Barometer (LDP-BL [3])	52%
	MLP3115A2 Barometer (G-DDP-BL [4])	52%

SeRaNDiP's user-level accuracy is comparable to baselines.

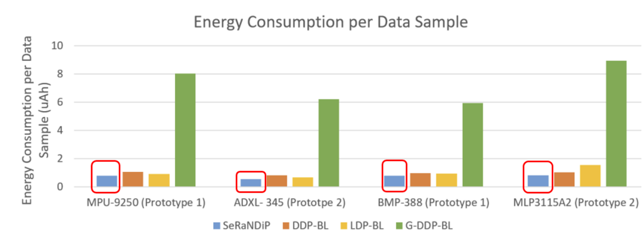
c) Latency Evaluation

SeRaNDiP is the fastest !!!



- SeRaNDiP w.r.t accelerometer is 1.4 X, -1596X times faster than baselines.
- SeRaNDiP w.r.t. barometer is 1.4X-3334X times faster than baselines.

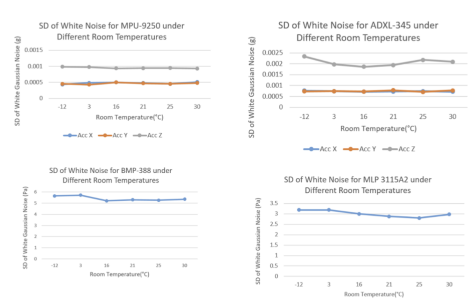
d) Energy Consumption Evaluation



- SeRaNDiP w.r.t. accelerometer is 1.4X-11.2X lower compared to baselines.
- SeRaNDiP w.r.t. barometer is 1.2X -10.7X lower compared to baselines.

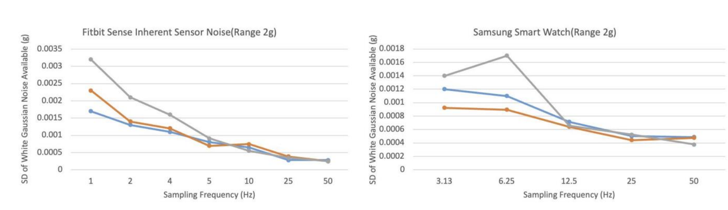
SeRaNDiP has the lowest energy consumption!!!

e) Robustness to Environmental Temperature Variation Evaluation



Validates SeRaNDiP's robustness to environmental temperature variations !!!

f) Applicability to commercial smartwatches Evaluation



SeRaNDiP can be readily applicable to commercial smartwatches !!!

7. Conclusion

SeRaNDiP

- Is a framework that considers inherent sensor random noise for differential privacy preservation in wearable community sensing applications.
- Leverages sensors' inherent noise by configuring sensor configurations at the software level without any hardware modifications.
- Can provide differential privacy to a variety of wearable sensors under different temperature conditions while delivering energy and latency savings.
- Can be readily applied to today's wearables, smartwatches, and smartphones.

For more details, please refer to our SeRaNDiP Project Page →

This research was partially funded by Singapore National Research Foundation under NRF-RSS2016-005 and NRF2018NCR-NCR002-0001.