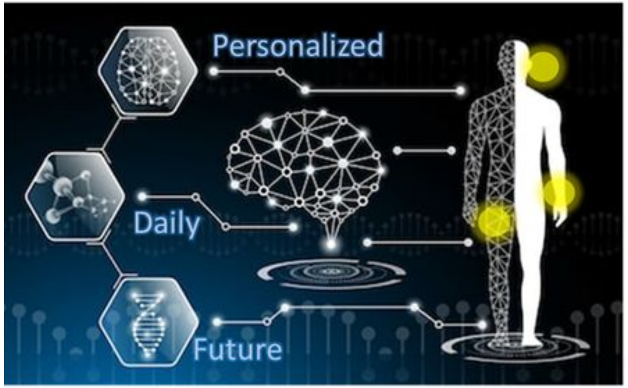
Final Presentation: Same-body Sensor Network Security

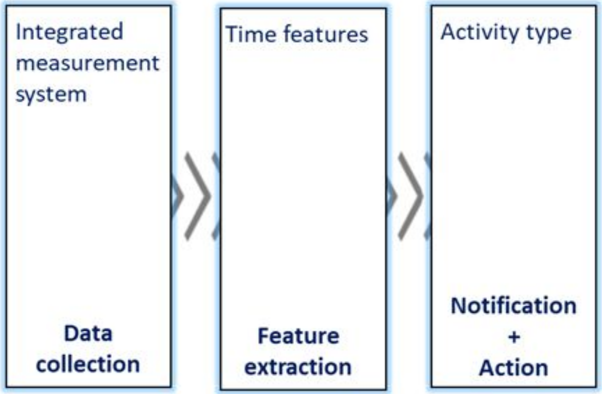
Presented by:
Mark Chen (405430125)
Hannaneh Hojaiji (704614134)
Riyya Hari Iyer (305427411)

UCLA Samueli School of Engineering

Overall Project Goals and Specific Aims

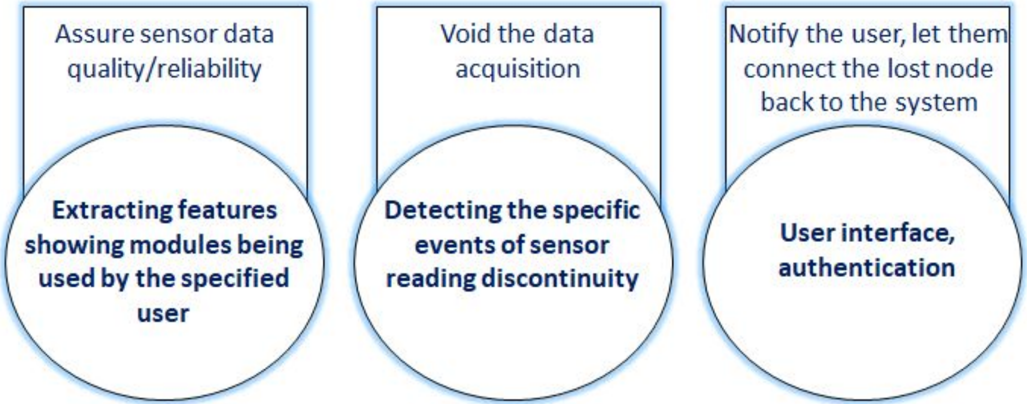
- The seamlessing pairings of off-the-shelf wearable sensors may lead to inaccurate sensor data collection and loss of devices due to the lack of user attentions.
- Our authentication system aims to secure and associate sensor readings of a user's body sensor network to that particular user.





Overall Project Goals and Specific Aims

- In addition, the system provides actionable feedback and on-board abnormality detection when verifying the integrity of a body sensor network.
- It notifies the user about the lost/stolen node in the body sensor network before that node loses its bluetooth connection.



Deliverables

- An Android app that authenticate and periodically verifies whether a three-device sensor network (phone, moto 360 watch, and eSense earable) is on the same body
- Data analysis plots of collected sensor data from some of these devices' accelerometers and gyroscopes
- Codes and scripts that authenticate phone and wearables, periodically check body sensor network integrity, record the sensor data, and analyze the correlations among the sensor data
- Video demo that illustrates the uses of our Android app in recognizing lost/stolen devices and notifying user to recover them.

UCLA Samueli School of Engineering

Threat Model

- A user pairs up and wears the two wearables (eSense and watch) to perform personal sensor data collection

- Collected data can be messed up and/or the wearables can be stolen by the following two scenarios:
  - User forget one of the wearables on an stationary object such as table
    - An adversary can then take away the wearable
  - The adversary directly grabs one of the wearables from the user
    - Can apply man-in-the-middle attack (MITM) to steal the device in stealth

UCLA Samueli School of Engineering

Technical Approach

- In this three-device body sensor network, we implement two same-body checking mechanisms.
  - Accelerometer and gyroscope correlation sensing for same-body checking between phone and eSense
  - Heart rate sensing for same-body checking between phone and watch

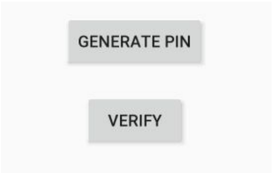
- We ensure proper device placements and pairings on a selected user before authenticate this person’s sensor data collection

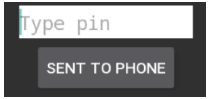
- The phone app continuously checks for sensor signatures from this same user and terminates data acquisition upon any of the two mentioned scenarios is met (see next slide).

UCLA Samueli School of Engineering

Implementation

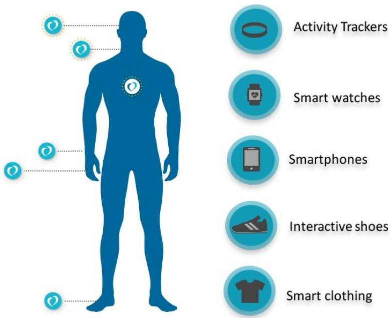
- First Phase: Build initial authentication module that applies across the paired phone, eSense, and watch
  - User generates a pin on the phone (NO visual display)
  - The eSense speaks out the pin to user via text-to-speech
  - The user receives the pin from eSense
  - The user then types the pin on watch then send it to the phone
  - The phone enables sensor data collection upon confirming the received typed pin is the same as the one that generated earlier.
- This cyclic authentication through all devices ensures that the same person is using the sensor array

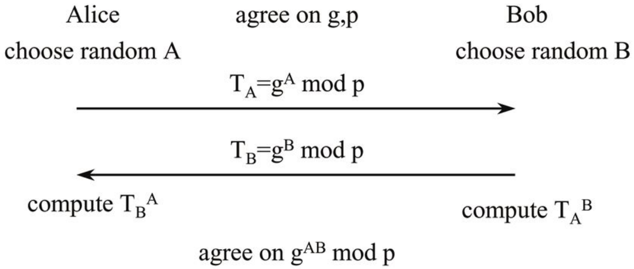




UCLA Samueli School of Engineering

Implementation

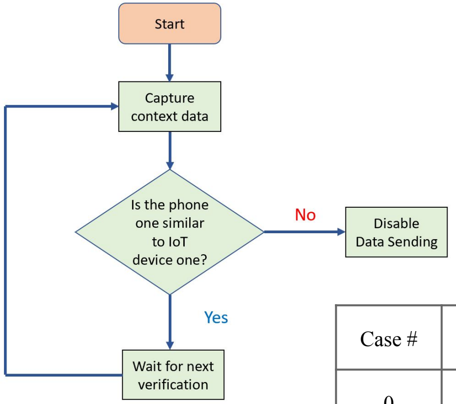




- Second Phase: Digest literature Reviews of continuous validation/authentication based on shared context for designing our detection algorithm
  - Use time series to implicitly authenticate/communicate a secure channel[1,2]
  - Use anonymous key agreement like Diffie-Hellman[3] (not robust with attack models)
  - Reviewed methods introduced in body area network device-to-device authentication paper and continues pairing methods papers[4, 5]
  - We extract unique accelerometer, displacement, velocity, gyroscopic and heart rate data for more devices and ensure data is collected from the intended user by observing the contextual behaviours.
  - We introduce more details in the following slide

UCLA Samueli School of Engineering

Implementation



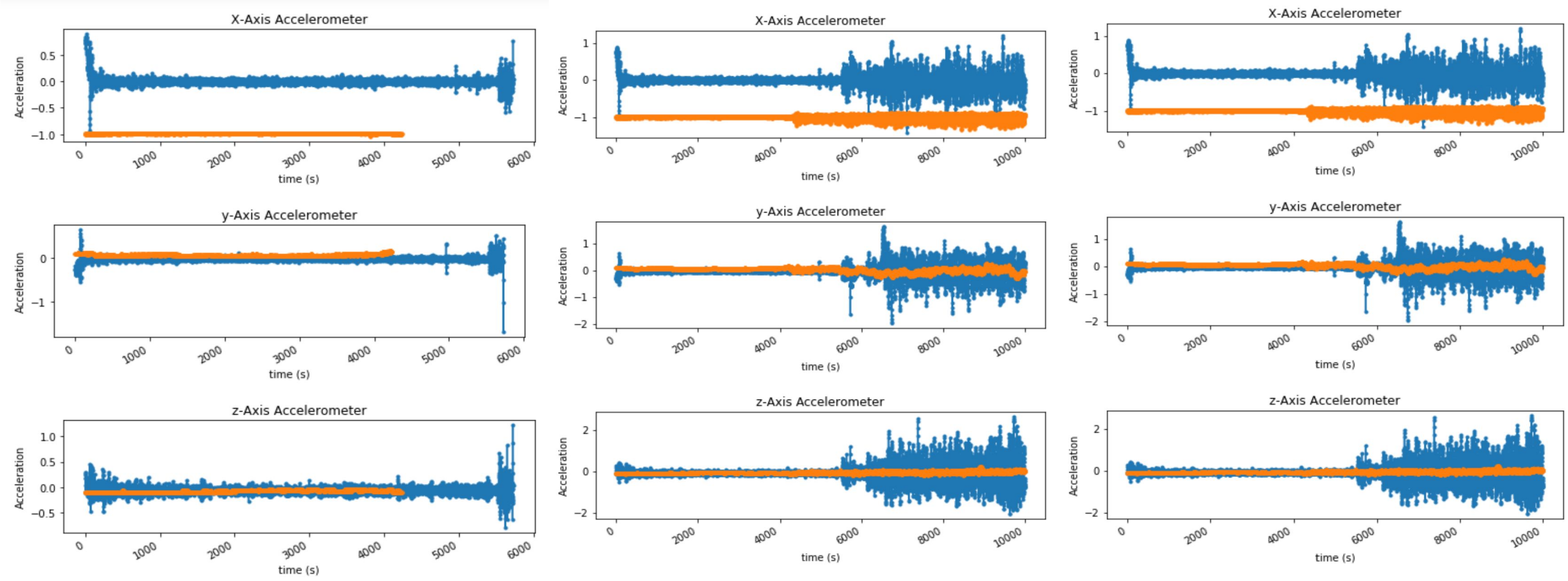
- Third Phase: Add continuous verification module for eSense's and watch's same-body monitoring
    - Collect contextual modalities (accelerations, angular velocities, and heart rate) in time series from the two wearables
    - Extract signatures/features (*e.g.* peak values) from these modalities for same-body verification
    - Perform feature analysis by windowing the sensor data
    - Apply decision trees to check if a wearable is still on the same user's body via correlation across the features of these modalities
    - Based on the resulting decisions, disable data communication of a wearable if it is said to be detached from user's body

Case #	Action monitored
0	Sitting
1	Walking
2	Running
3	Put earable in from table
4	Take earphone out from ear
5	put earphone on table and get up
6	Earphone stolen and walk slowly
7	Earphone stolen thief running

UCLA Samueli School of Engineering

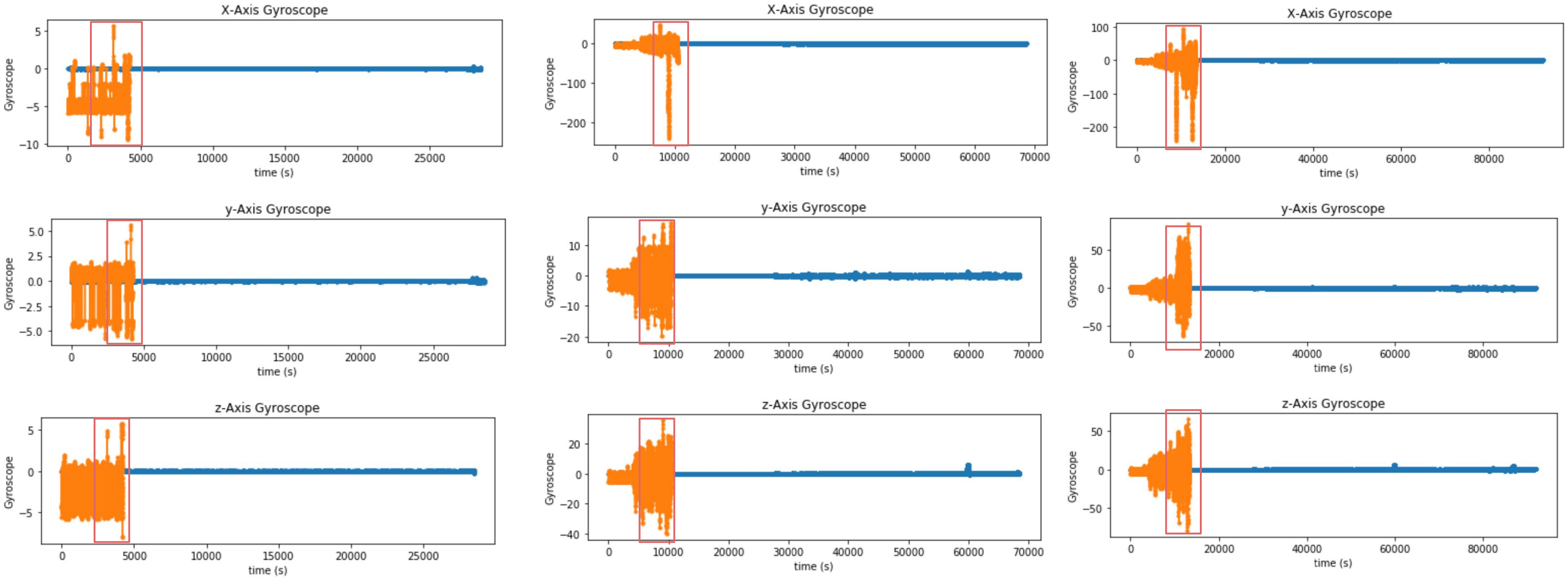
Experimental Results and Evaluations

- Acceleration: (more in depth analysis results on github)
- 3 cases (sitting, running, walking)



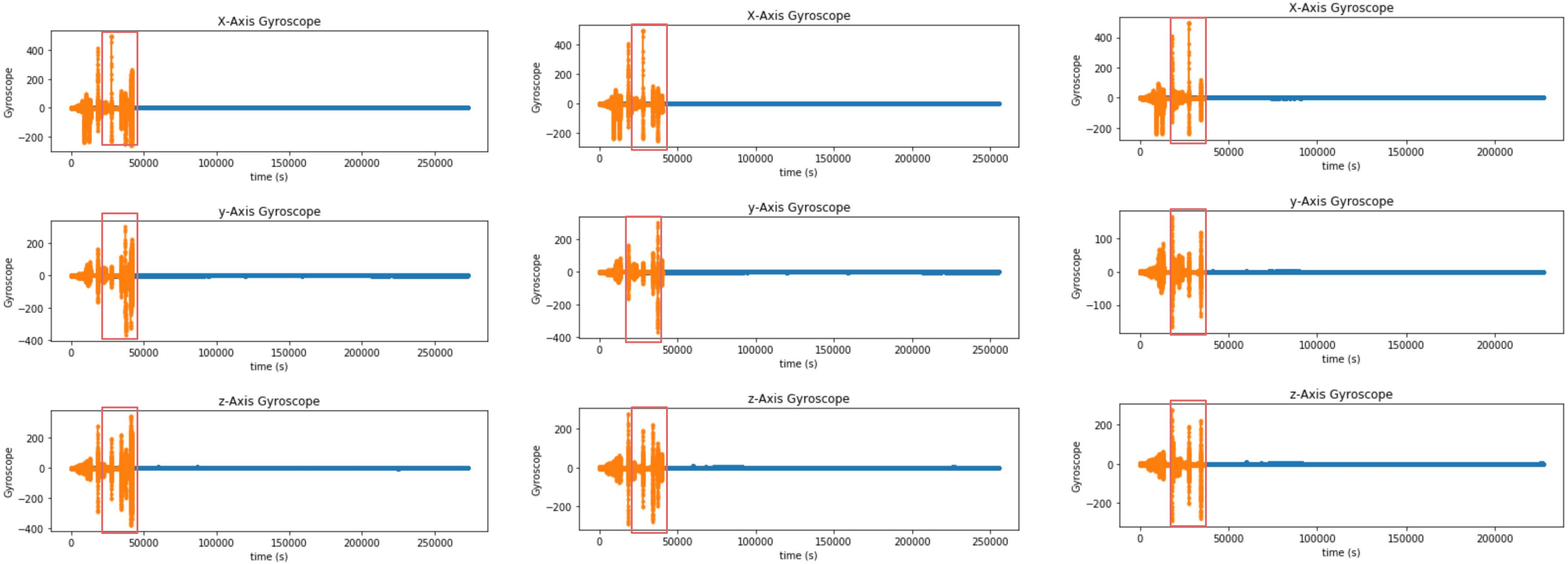
Experimental Results and Evaluations

- Gyroscope: (more in depth analysis results on github)
- 3 cases (sitting, running, walking)



Experimental Results and Evaluations

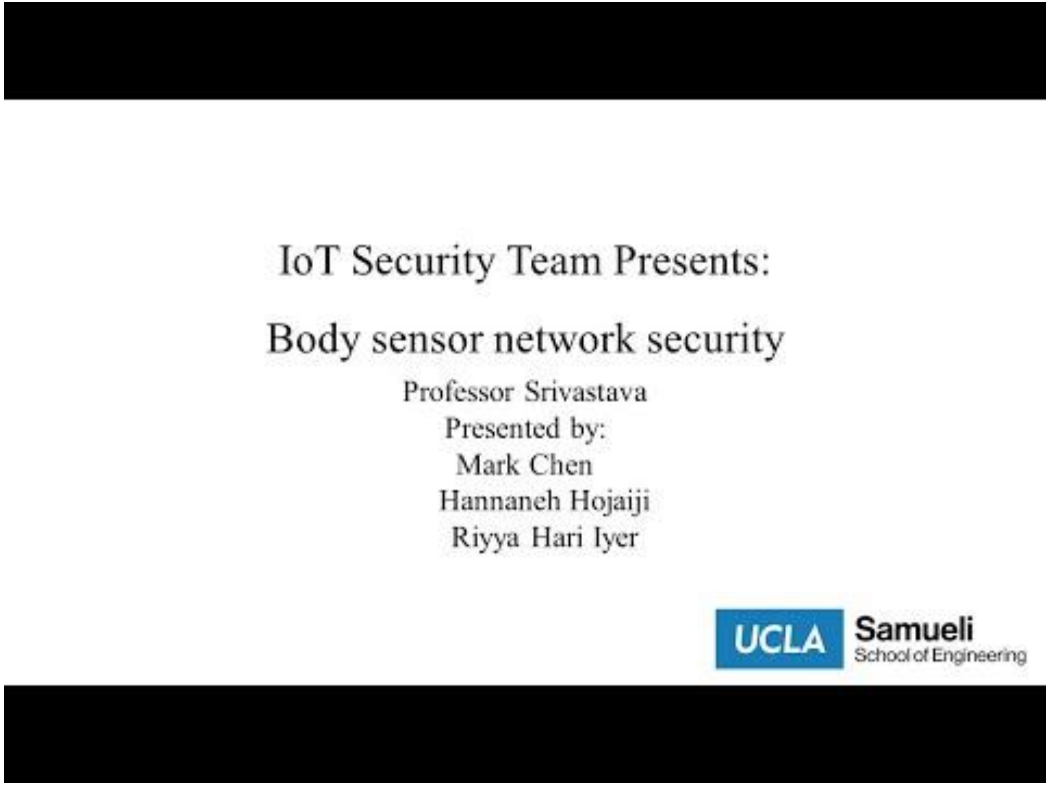
- Gyroscope :
- 3 cases (Adversary takes the device (running and with the same pace, the device is forgotten)



System Demo

- Please watch this brief demo on YouTube to see how critical parts of our platform work in action:

- https://youtu.be/Vbj39Gpa_f0



System Evaluation

- Key Findings:
  - Peak detection on collected sensor data gives good insights on user' actions/motions
  - Correlating multiple modalities (*i.e.* acceleration and angular velocities) provides better decisions on whether a wearable is detached from the user's body
  - Good control on sensors can be done through registering/unregistering sensor listeners inside the app

- Metrics of Success:
  - Properly collect wearables' sensor data through wireless transmission ✓
  - Implementation of decision trees based on sensor signatures to detect adversarial events ✓
  - Quick notification/toast to user about the detachment of a wearable ✓

UCLA Samueli School of Engineering

Prior work and our success

- There has been research in the domain of context sensing and ensuring that the devices are on the same person. WiFi-enabled authentication [5] is an example of the research work in this domain

- Shi, Liu and Chen's work talks about extracting Channel State Information (CSI) from the WiFi signals of IoT devices and use a deep learning based algorithm to identify individual users[6].

UCLA Samueli School of Engineering

Prior work and our success

- There have been some developments for continuous authentication and verification. F.Wang's[5] publication is one such paper discussing that.
- It talks about BodyPIN, a light-weight and robust technique that performs user authentication through computer execution and denies access when authentication fails
- Accelerometer data is a reliable sensor for extracting signatures for this purpose. Cornelius and Kotz's[7] research talks about the reliability and economical cost of accelerometer
- We built upon these methods choosing the best approaches utilizing the array of sensor signatures introduced. We also devised the initial authentication mechanism through random number generation

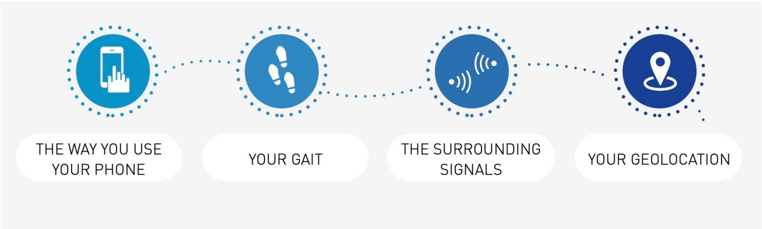
UCLA Samueli School of Engineering

Limitations

- Need to collect more data samples from more individuals to refine the decision trees.
- Wearable sensors' sensing accuracies affect the outcome of adversarial detection.
  - Accelerometer and gyroscope are okay, but heart rate sensor is not
  - Pedometer (step counting) ends up not working due to drifting in eSense.
- Must concatenate the sensor values collected from the watch in a package to synchronize better and more smoothly.
- Updates in Android packages and APIs cause unnecessary overheads when incorporating more sensors for adversarial detection
  - Frequent maintenance on the app's source code is required to ensure usability

UCLA Samueli School of Engineering

Future directions



- Train and use a machine learning algorithm/model that is resilient User-specific behavioural signatures.
- Add more sensor types and proper authentication/verification configurations to the system for enabling personalization on same-body sensor network.
- Search or develop more accurate sensing devices to improve the reliability of the system
- Apply this methods to healthcare platforms as was mentioned in Lin et al. paper[8].

UCLA Samueli School of Engineering

Contributions

- Mark:
  - Performed literature review
  - Performed data collection
  - Programmed Android application for sensor data collection from phone and earable
  - Programmed earphone data storage
  - Implemented sensor collection with the watch
  - Planned experiments
  - Debugged watch authentication interface and application connectivity
  - Integrated applications for the modules
  - Implemented Bluetooth connection and algorithm
  - Implemented the decision tree algorithm
  - Prepared final demo
  - Maintained and wrote github report
  - Developed and completed midterm and final reports

Contributions

- Hannaneh:
  - Performed literature review
  - Programmed Android application for sensor array data collection and plotting from phone
  - Programmed Android application for sensor array data collection and plotting from watch
  - Programmed data storage on the phone
  - Performed data collection
  - Developed data analysis algorithm in python
  - Devised and implemented the decision tree algorithm in the app
  - Implemented watch authentication interface
  - Planned out the experiments
  - Developed watch interface
  - Debugged the application package and API compatibility
  - Created and wrote github report and website
  - Took and made final demo
  - Developed and completed midterm and final reports

UCLA Samueli School of Engineering

Contributions

- Riyya:
  - Implemented text to speech conversion in the app
  - Implemented random number generator in the app
  - Created the initial authentication mechanism
  - Implemented earphone IMU data communication and storage
  - Helped with data storage of phone values in phone
  - Helped with accessing gyroscope values in phone
  - Reviewed data analysis in Python
  - Performed literature review
  - Helped with app integration
  - Helped with github repo
  - Prepared midterm and final report

UCLA Samueli School of Engineering

References and Resources

[1] Al Ameen, Moshaddique, Jingwei Liu, and Kyungsup Kwak. "Security and privacy issues in wireless sensor networks for healthcare applications." *Journal of medical systems* 36.1 (2012): 93-101.

[2] Stajano, Frank, et al., eds. *Security and Privacy in Ad-hoc and Sensor Networks: 4th European Workshop, ESAS 2007, Cambridge, UK, July 2-3, 2007, Proceedings*. Vol. 4572. Springer Science & Business Media, 2007.

[3] Huang, X., Wang, Q., Bangdao, C., Markham, A., Jäntti, R., & Roscoe, A. W. (2011, October). Body sensor network key distribution using human interactive channels. In Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies (pp. 1-5).

[4] Schürmann, D., Brüsch, A., Sigg, S., & Wolf, L. (2017, March). BANDANA—Body area network device-to-device authentication using natural gAit. In *2017 IEEE International Conference on Pervasive Computing and Communications (PerCom)* (pp. 190-196). IEEE.

[5]Wang, F., Li, Z., & Han, J. (2019). Continuous user authentication by contactless wireless sensing. *IEEE Internet of Things Journal*, *6*(5), 8323-8331.

[6] Shi, C., Liu, J., Liu, H., & Chen, Y. (2017, July). Smart user authentication through actuation of daily activities leveraging WiFi-enabled IoT. In *Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing* (pp. 1-10).

[7] Cornelius, C. T., & Kotz, D. F. (2012). Recognizing whether sensors are on the same body. *Pervasive and Mobile Computing*, *8*(6), 822-836.

[8] Lin, S., *et al.* (2019). Natural Perspiration Sampling and in Situ Electrochemical Analysis with Hydrogel Micropatches for User-Identifiable and Wireless Chemo/Biosensing. *ACS sensors*.

Thank you for your time!

Report repository and website: https://hannahojaiji.github.io/HannaHojaiji209.github.io/