Blueshift: Breaking Bluetooth Adaptive Frequency Hopping

2023 National Cybersecurity Education Colloquium

Moraine 1&2, 11:30a – 11:55a

September 22, 2023

Faculty: Kun Sun, Student: Tommy Chin and Noah J Korzak
Program Manager: Stephanie Polczynski and Erik Brasile

PROJECT: INSuRE+C

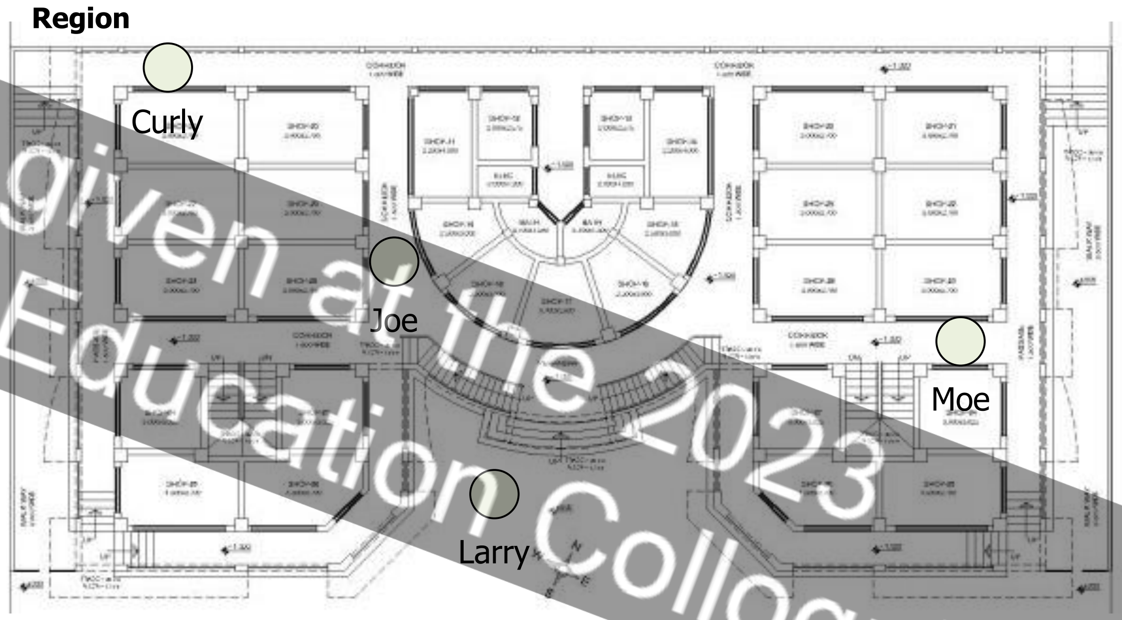
GEORGE MASON UNIVERSITY

Outline

- Overview
  - Device probing and Adaptive Frequency Hopping
  - How does AFH work and why do we care
  - Relevant studies and related works
- Blueshift
- Real-world experiments
- Preliminary results
- Conclusion

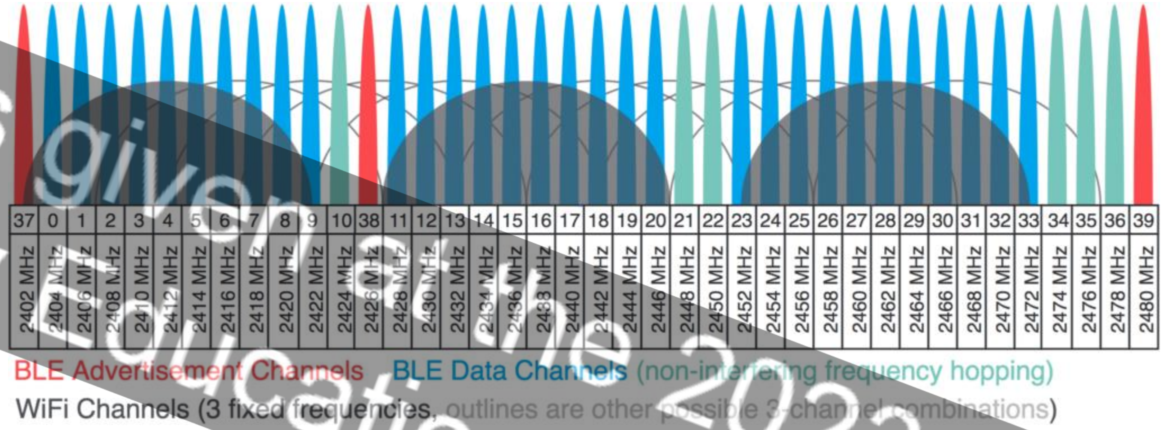
Today's world has an abundance of Bluetooth Low Energy devices

- Scenario
  - You are a Cybersecurity Specialist
  - Tasked to protect a region from threats
- A person brings a device to an area
  - What is the device?
  - What is the device doing?
  - Why should we care?
- What about multiple people?
  - How can one maintain awareness of all the activities?
  - Cost? Scale?



One achieves intent analysis through data collection efforts

- Capturing network packet data often reveals meaningful information
  - Meta data indicating content
  - Fields reflecting source and destination
- BTLE data capture challenges
  - Hard to achieve in practice
  - 3 advertisement and 37 data channels
  - Need a wideband antenna to capture all 40 channels
  - We lose information without a wideband antenna!



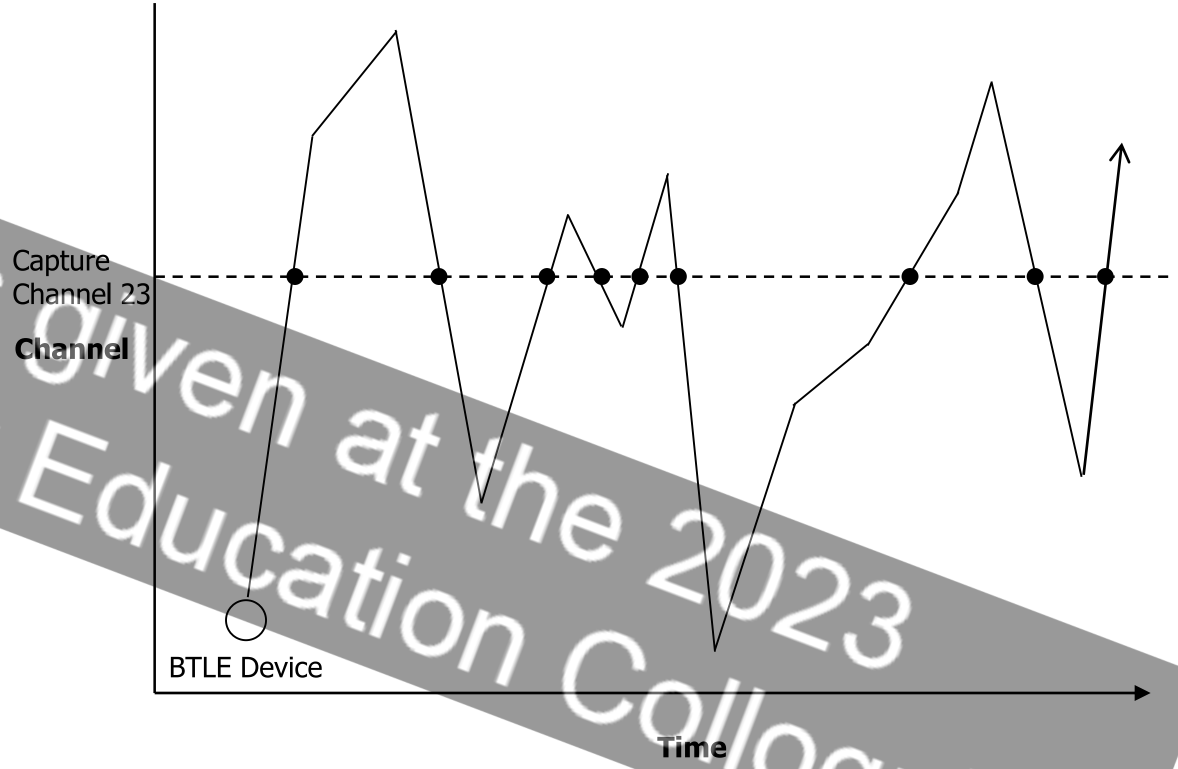
Bluetooth Low Energy wireless spectrum

Adaptive frequency hopping and the overarching problem

- The method of how BTLE devices hop
  - Defined in the Bluetooth protocol
  - Presents complication in data collection

- BTLE devices pair with one another
  - Establishes key parameters to answer
    - How to hop and when
    - Defines the initial frequency / hop interval
  - Information visible to capture

- Difficult to locate without capturing



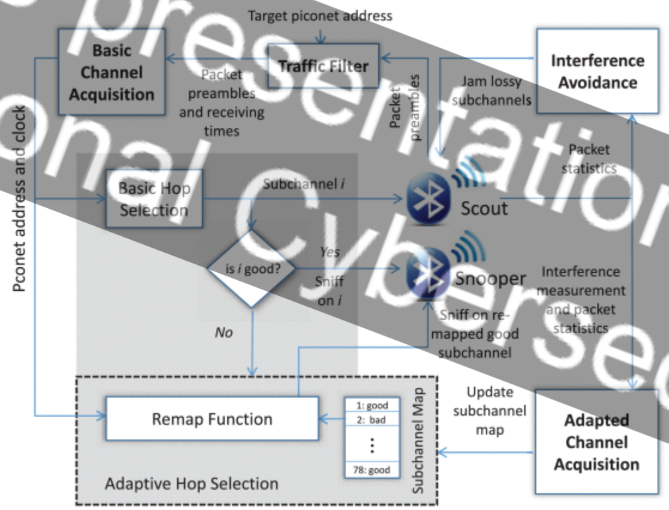
Well known studies capture BTLE traffic using an Ubertooth One

- Open-source BTLE packet sniffer
  - Open-source tooling enables following one pair of devices upon observing a connection packet
  - Limited to only one BTLE channel at a time for data collection
- Widely known in BTLE research work
- Retired on December 22, 2022

Ubertooth One

Relevant studies have attempted to tackle the AFH problem

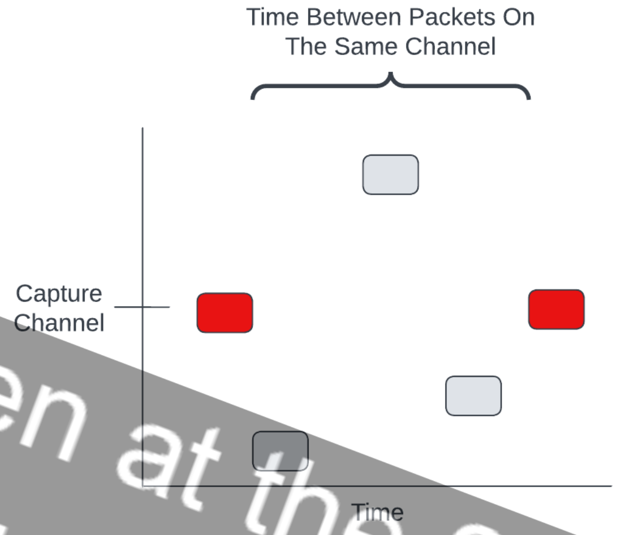
BlueEar



- Used two Ubertooth One devices
- Leverages machine learning to predict channel map
- Only works for Bluetooth Classic and uses selective frequency jamming to manipulate the BTLE pair's channel map

Albazrqaoe, W., Huang, J., & Xing, G. (2018). A practical Bluetooth traffic sniffing system: design, implementation, and countermeasure. *IEEE/ACM Transactions on Networking*, *27*(1), 71-84.

Silicon Austria Labs / Johannes Kepler University



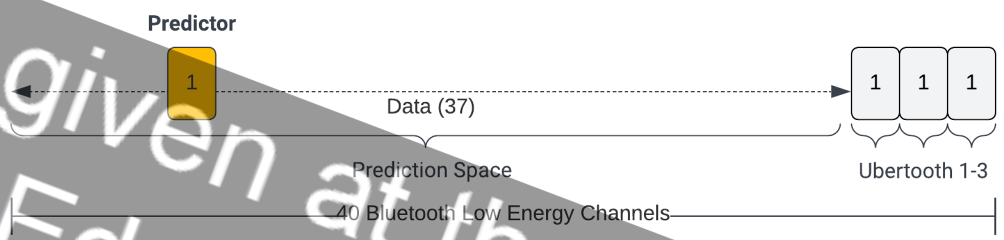
- Deployed one Ubertooth One device
- Ubertooth One stays on one channel, and predicts channel map based on time between packets
- Misses large amount of key data on other channels

Karoliny, J. W., Blazek, T., Springer, A., & Bernhard, H-P. (2023). Predicting the Channel Access of Bluetooth Low Energy. In *IEEE International Conference on Communication (ICC 2023)* (pp. 1)

Blueshift breaks collection challenges with prediction

- Blueshift
  - Enumerates all potential hopping values to create a large hop table
  - Achieved through deep study of Bluetooth protocol

- Track devices across multiple channels using a single predictor
  - Single-band antenna designed
  - Reduces the dependency for a wideband antenna



Blueshift high level overview

Mapping table enables quick lookup capabilities

- Deep study of Bluetooth protocol enabled creation of a hopping table
  - Utilizes two 2^{16}-1 hex values to reflect the Access Address and the Counter
  - Follows modern Channel Selection Algorithm #2

- The observation of a BTLE packet
  - Reveals the Access Address
  - Lacks the Counter, Channel Map, and Interval values

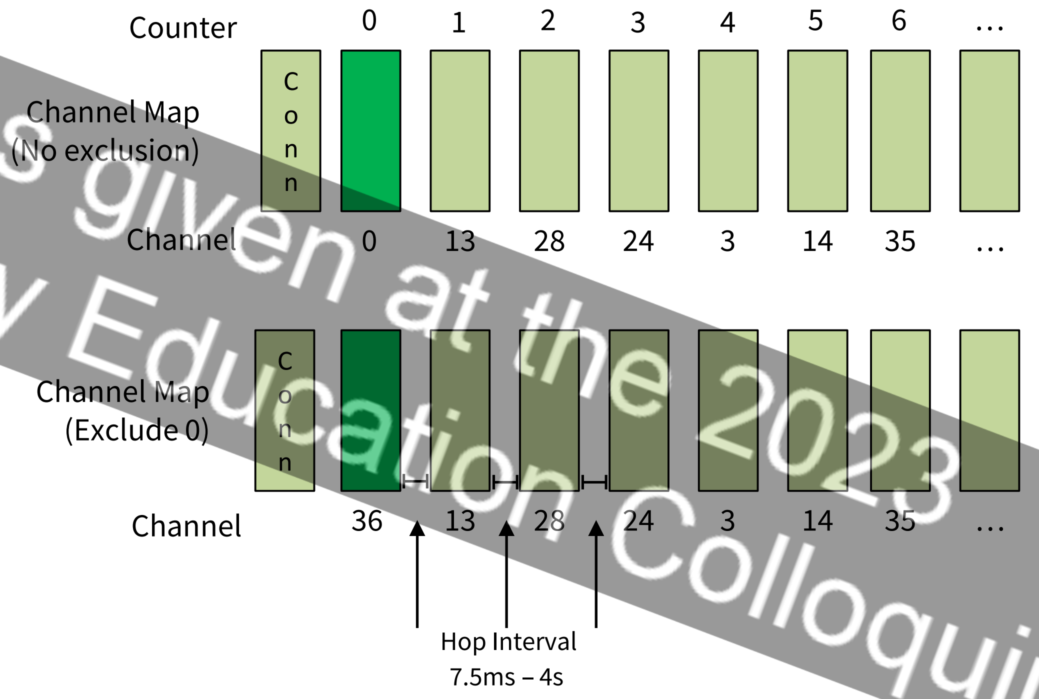
- Accuracy increases when missing values are determine

$$\mathbb{M} = \begin{bmatrix} h_{\alpha,c} & h_{\alpha,c+1} & \cdots & h_{\alpha,2^{16}-1} \\ h_{\alpha+1,c} & h_{\alpha+1,c+1} & \cdots & h_{\alpha+1,2^{16}-1} \\ \vdots & \vdots & \ddots & \vdots \\ h_{2^{16}-1,c} & h_{2^{16}-1,c+1} & \cdots & h_{2^{16}-1,2^{16}-1} \end{bmatrix}$$

$$\mathbb{M}_{0x4f126af2} = [0, 13, 28, 24, 3, \ldots, 24]$$

Observing BTLE traffic initializes an orchestration of prediction work

- Identification of the map
  - We know some parts of the AFH
    - Hopping sequence of the BTLE session
    - Potential metadata about the device
  - Missing the Connection packet causes potential unknowns to occur
    - Counter value
    - Channel Map
    - Hop Interval
- Some values are necessary to determine for prediction

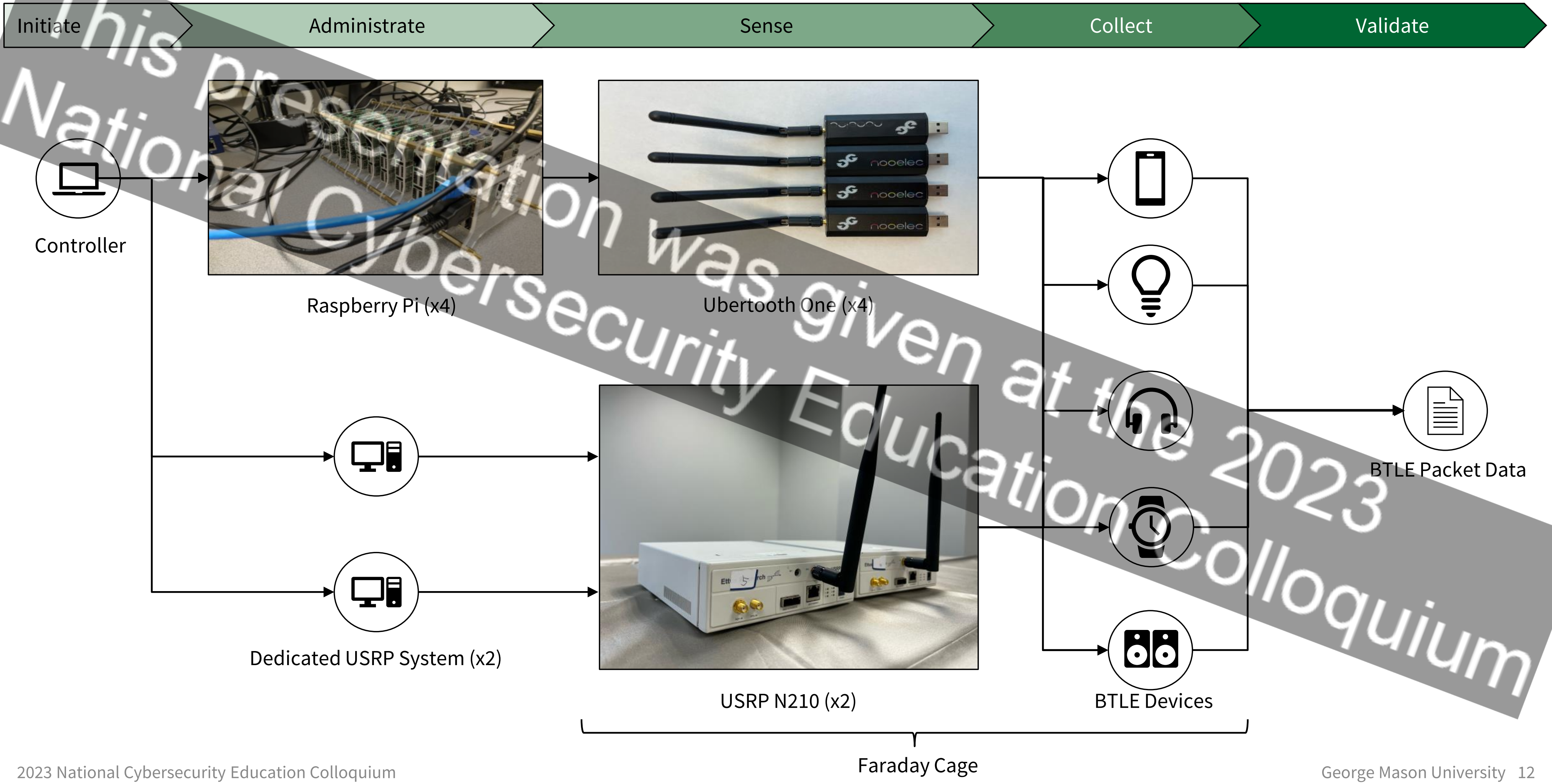


Reducing environmental noise enables effective data collection results

- Initial testing of lab environment
  - Showcased 746 unique Bluetooth devices
  - Multi-story building has many students and systems

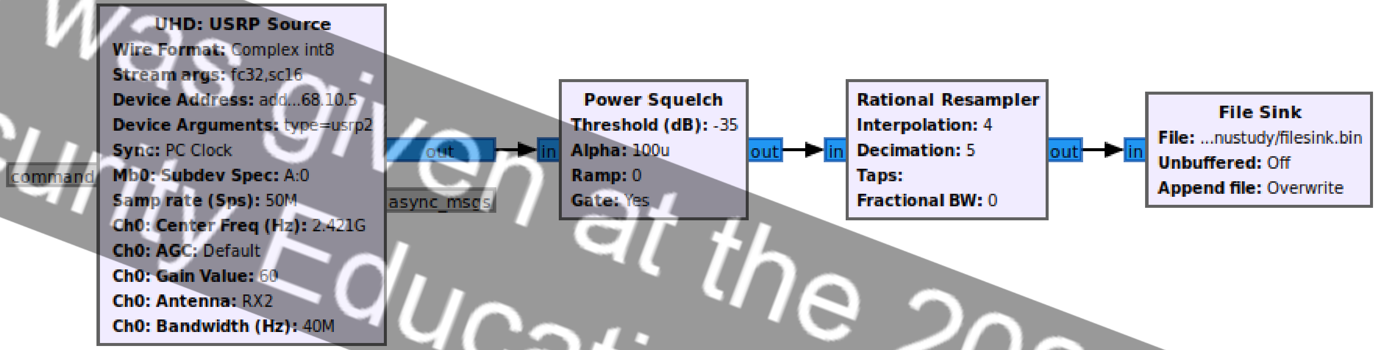
- The team created a faraday cage from a server cabinet
  - Noise reduction from -40 dBm to -89 dBm
  - Observable packets decreased from ~140 to ~10 packets per second

Architecting a testbed enables increase exposure to real-world challenges



GNU Radio Companion enables the creation of ground truth

- Configuration of USRP
  - GNU Radio Companion
  - Enables full BTLE channel coverage
  - Each USRP covers 20 channels
- Data filter from collection
  - Power Squelch removes signal data with a signal strength lower than -35 dBm
  - Rational Resampler adjusts data collection rate to match rate of BTLE data transfer
- Signal data converted to packet format using open-source library[1]



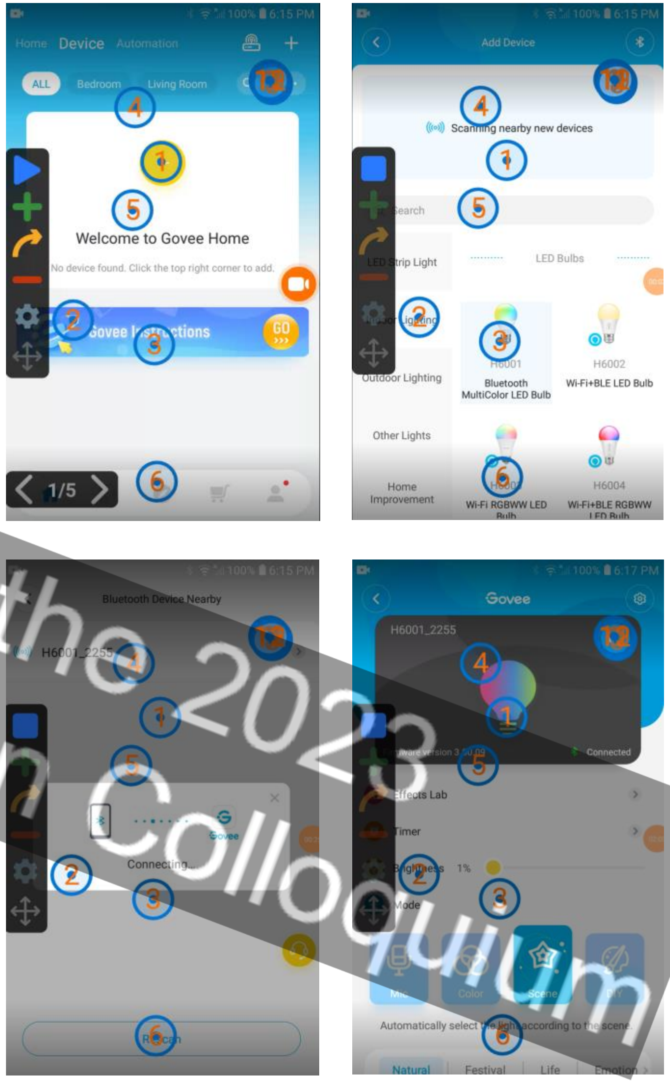
GNU Radio configuration for USRP N210 Collection

1- https://github.com/mikeryan/ice9-bluetooth-sniffer

Automation of experiment enables higher volume of data collection

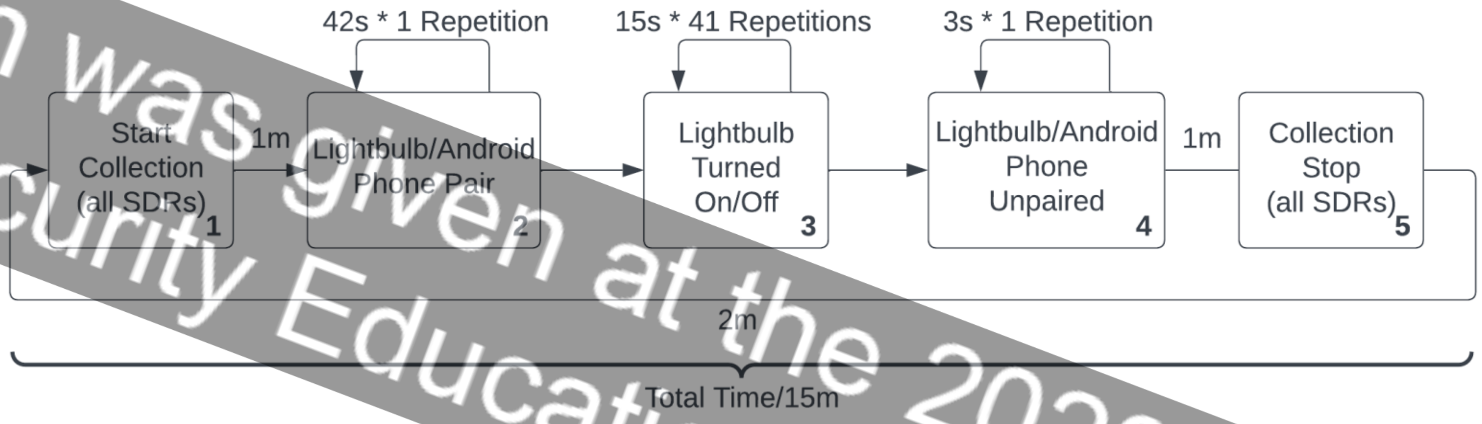
- Initial experiments explored using
  - Android Phone and Govee Lightbulb
  - Simplest device with easy visual feedback

- A clicker application enabled repetitive, automated interaction of a light bulb
  - 49 precisely timed inputs used per 15-minute experiment
  - Enable continuous experiment pending device stability and storage



Overview of Data Collection

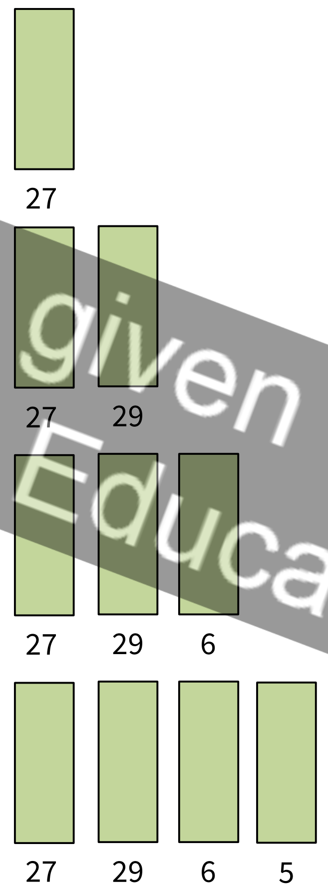
- Connecting data with BTLE devices have a high, manual labor requirement
- We pursued areas to automate to best maximize volume of data
  - SDRs collect for a minute before device pairing and after device disconnect, guaranteeing entire connection is captured
  - Lightbulb turned on/off to ensure frequent communication
  - Experiment loops until user intervention



Prediction and maintaining track of devices

- Observing the connect packet
  - Easy to identify the initial hopping pattern
  - Must continuously keep track of a device connection to identify parameter changes
- Observing only a data packet
  - Difficult to determine hopping pattern
  - Must collect more samples to make an analysis
  - Three (3) to Four (4) samples enough to quantify a recovery of the work

Observation

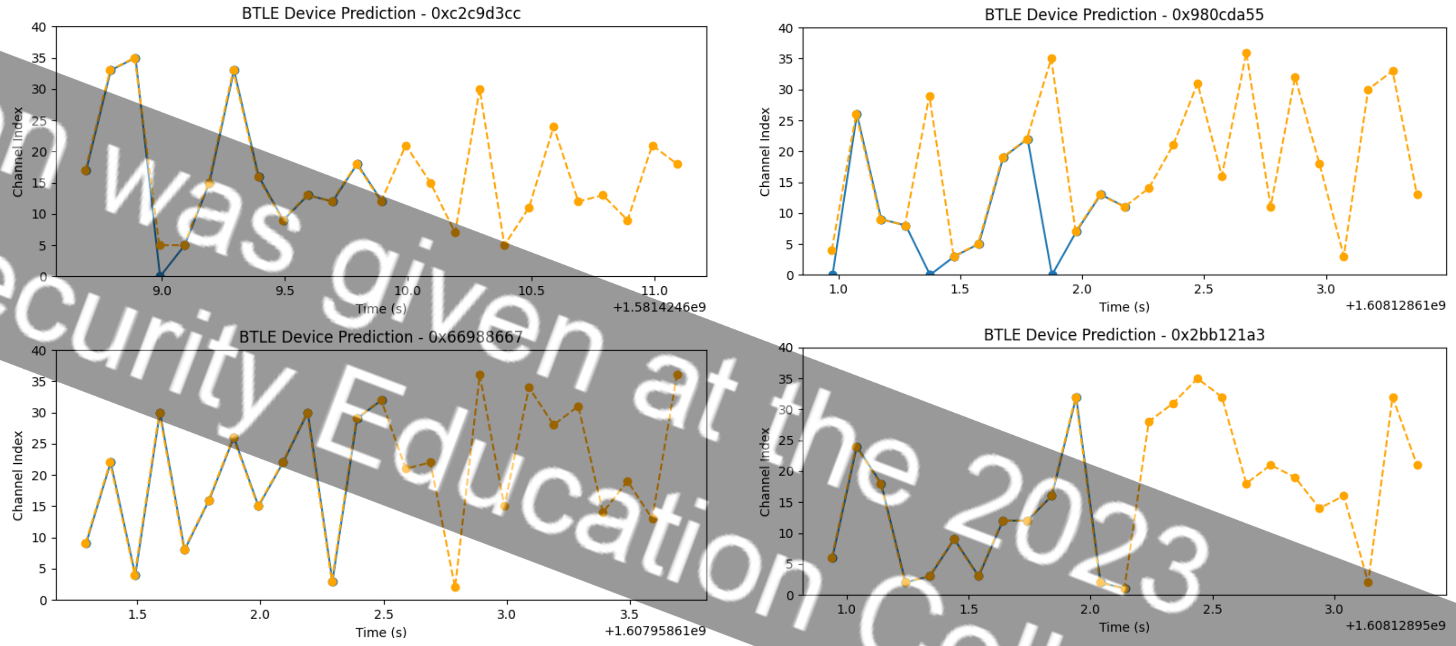


Candidate

```
1771      Too many to visualize

4         Counter=926,  [27, 29,  6,  5,  5]
          Counter=1058, [27, 29, 25, 24,  8]
          Counter=1653, [27, 29, 17, 23, 32]
          Counter=1703, [27, 29, 31, 28,  6]

1         Counter=926, [27,  29,  6,  5,  5]

1         Counter=926, [27,  29,  6,  5,  5]
```

Public dataset enables quick prototyping of code

- We followed an incremental development approach
  - Deeply studied the Bluetooth protocol
  - Created code that accurately tracks pristine BTLE data
  - Supports both Channel Selection Algorithms
- Validate the functionality of code with public data[1]
- Iterate approach with real-world experiments to finetune system



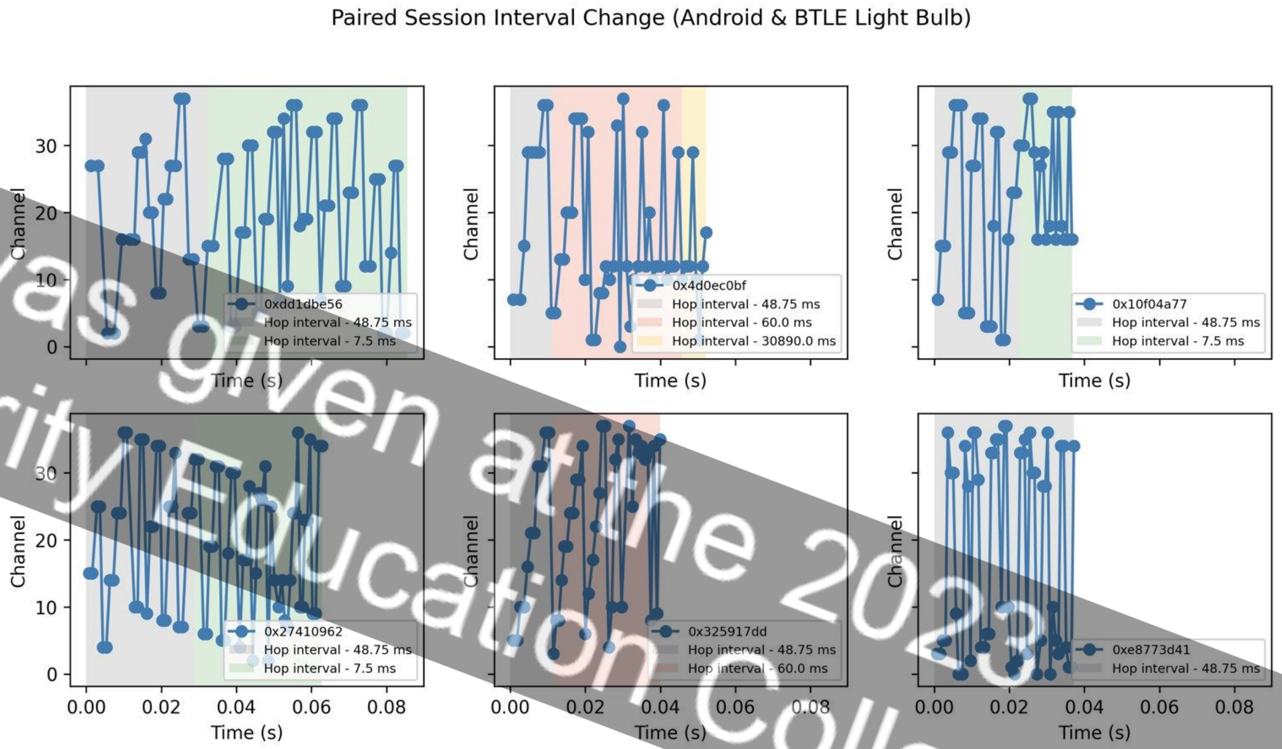
Prediction accurate using bsniffhub dataset (solid/blue=measure, dashed/orange=predict)

1- https://github.com/homewsn/bsniffhub

Hop interval changes creates complication in prediction

- Real-world experiments highlight a secondary challenge
  - Time between hop changes
  - Rate may speed up or slow down

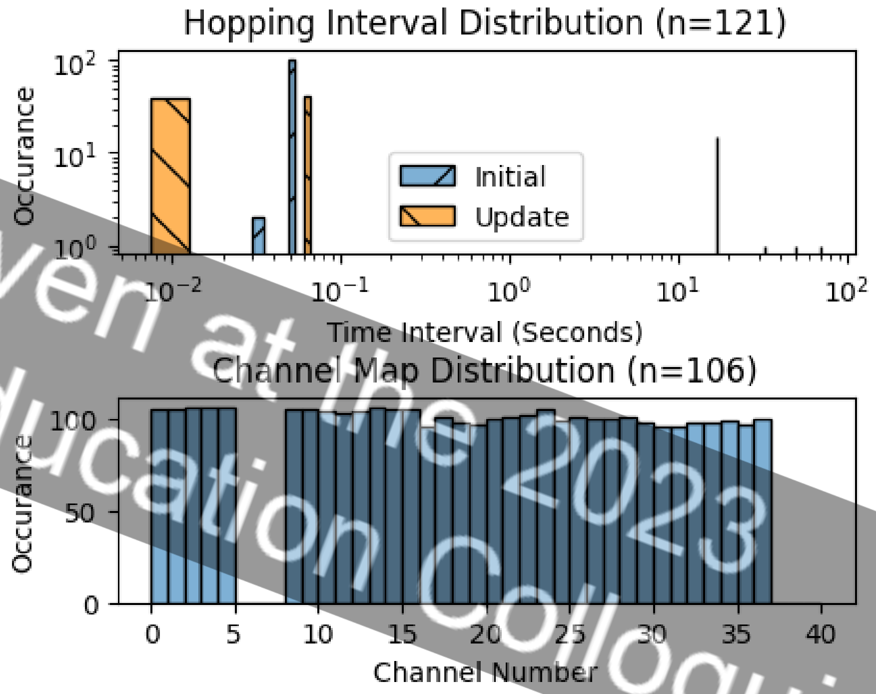
- Reproducing the interval changes difficult to achieve in the real-world
  - Environmental factor critical to mimic
  - Easy to attain through simulation



Hop interval changes with paired devices

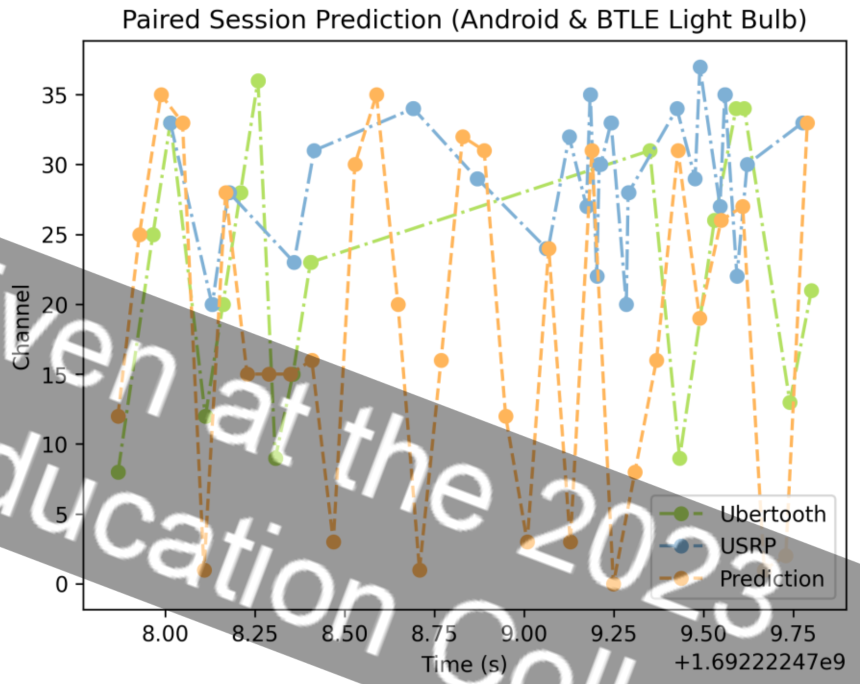
Environment changes enable frequent modifications to the channel map

- Running multiple experiments
  - Highlights many occurrences where the hop interval changes
    - Speed up
    - Slow down
  - The number of channels available
    - Relatively consistent
    - Environment favored not using some channels



Complexity of AFH presents challenging prediction effort to follow

- Several complex scenarios identified as an outcome of the analysis
  - Ubertooth One misses variable amount of data collection using native libraries when comparing to USRP output
  - Some sessions have long idle periods where a device does not heartbeat or communicate
  - Hop interval times speed up and slowdown at variable rates



- Some prediction points are on track but quickly lose accuracy as session parameter changes

Conclusion

- Implementing methods to break and defeat Adaptive Frequency Hopping
  - Trivial to address through simulation
  - Higher difficulty in real-world scenarios
    - Frequent changes in environmental spaces
    - Higher introduction of noise
  - Data collection processes has high time complexity requirements
    - Manual user intervention needed
    - Reliability of devices sometimes have discrepancies which needs a reboot

- Blueshift presents promising direction to expand and explore research area
  - Enables areas to help address producing an inexpensive mean to track devices at scale
  - Highlights areas to enhance the Bluetooth protocol to increase user privacy

Future Work

- One short paper accepted to highlight our preliminary work
  - CCS Workshop on Moving Target Defense
  - November 26, 2023, Copenhagen, Denmark
- Creating user-based use cases to increase prediction accuracy
  - User connects, disconnects, reconnects, etc.
  - Using a paired device to unpair and re-pair to a different system
- Profiling devices
  - Supports pattern of life detection
  - Classifying data to a device

Thank You! Questions?

Contact us at…

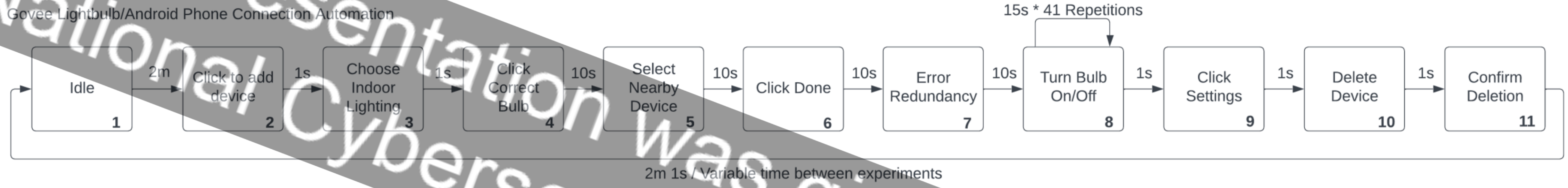
- Tommy Chin, tommy.chin@ieee.org
- Noah Korzak, nkorzak@gmu.edu
- Kun Sun, ksun3@gmu.edu

Check out our other research
https://sunlab-gmu.github.io/

Appendix

Deep dive into automating data collection

Connection Sequence for Lightbulb/Android Phone



SDR Experiment Overview