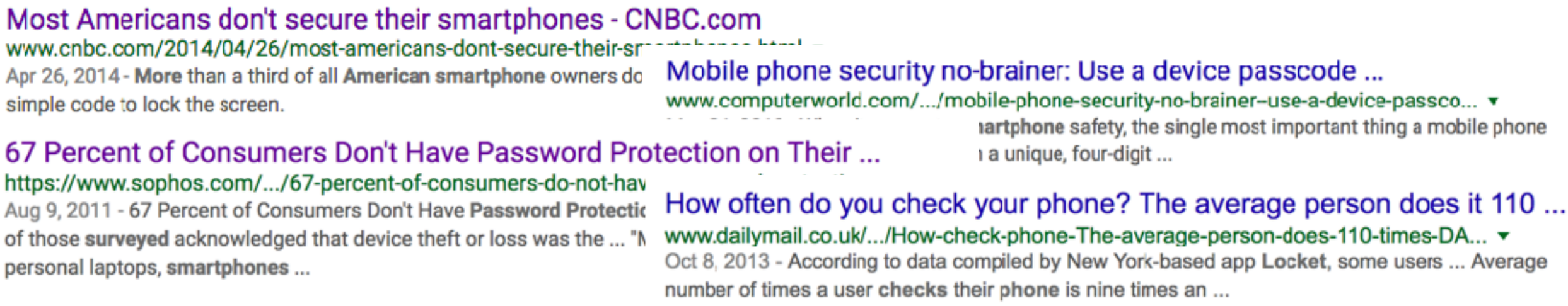
WearLock: Unlock Your Phone via Acoustics using Smartwatch

Shanhe Yi, Zhengrui Qin*, Nancy Carter, and Qun Li
College of William and Mary
*Northwest Missouri State University

Smartphone is “a pocket-size summary of your digit life”

It is common sense, that if your phone is not being using, it should be locked.

Not favored by some customers



- **53/150 (35%)** never enable any screen lock, due to inconvenient input of screen locks [Bruggen et al. SOUPS'10]

- **57.1%** of participants use none or native screen lock; **46.8%** participants consider unlocking annoying; **25.5%** want an easier way to unlock their phone [Harbach et al. SOUPS'14]

- **23** participants check their smartphone an average of **85** times a day [Andrew et al. 2015]

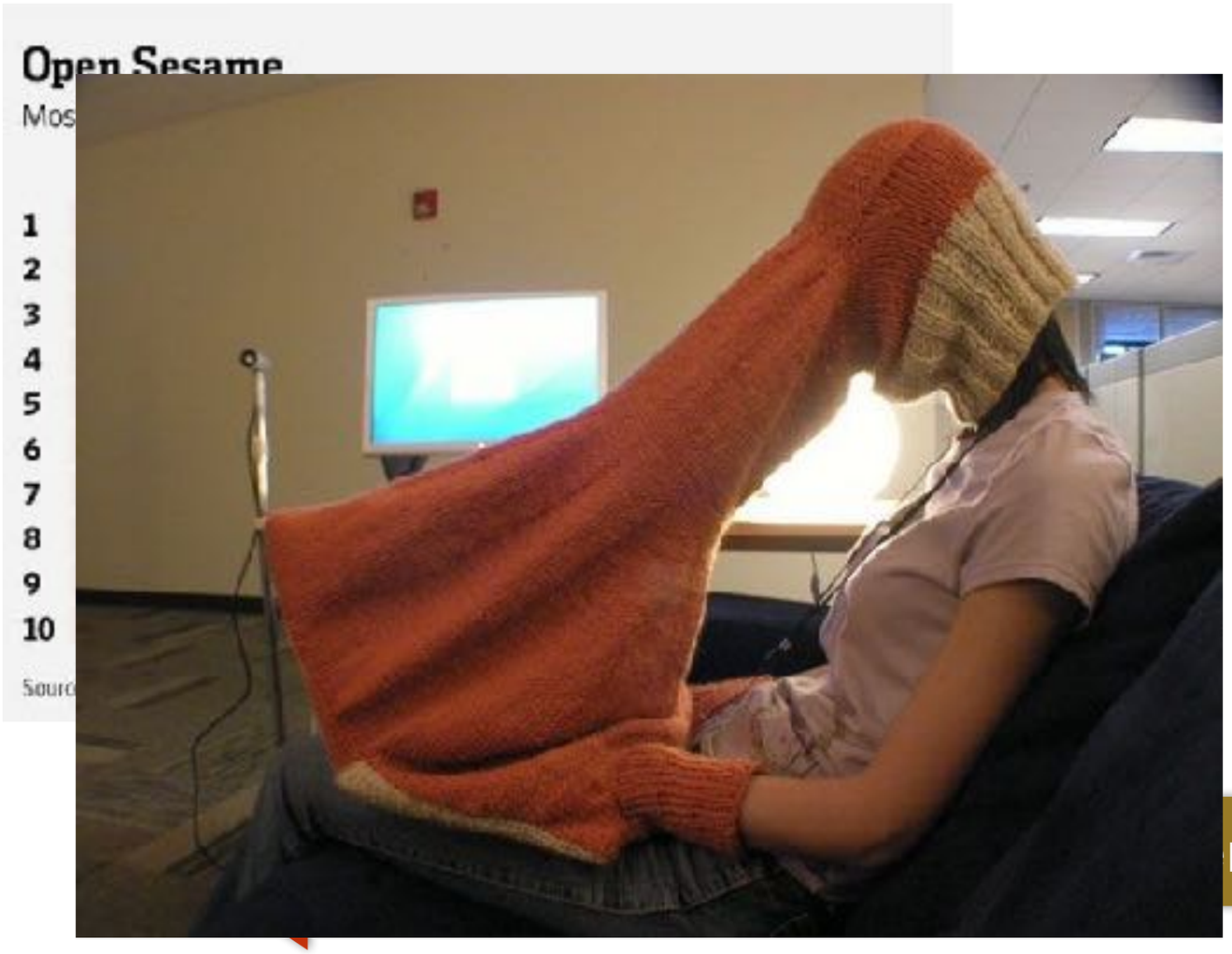
motivated to find more desirable method for smartphone unlocking:

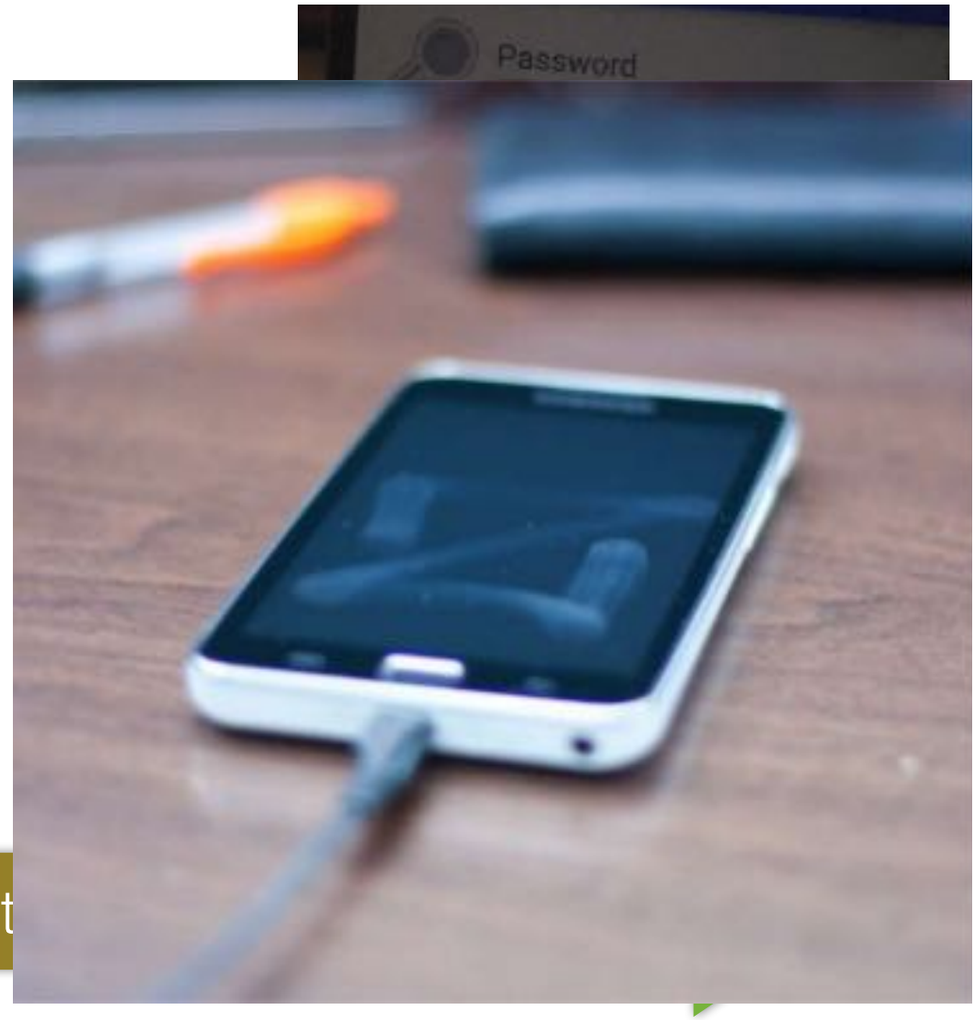
- **require minimal effort — improve user experience**
- **authenticate user on each interaction — no tradeoff on security**

WILLIAM & MARY
CHARTERED 1693

Screen Lock
- Finding Suitable Authentication Method

Passwords - what you know



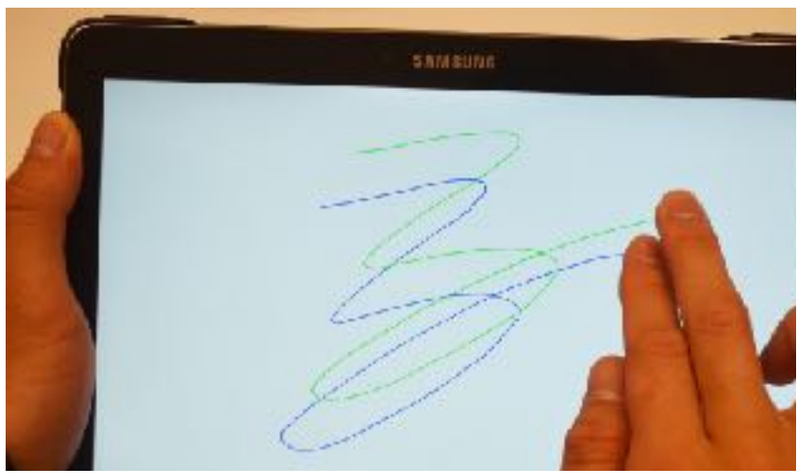


Easy to Shoulder Surfing
Easy to input

Smudge Attack
Difficult to input

Screen Lock
- Finding Suitable Authentication Method

Biometrics - who you are



Very Convenient

Uniquely tied to human body - non-replaceable

Screen Lock
- Finding Suitable Authentication Method

Tokens - what you have

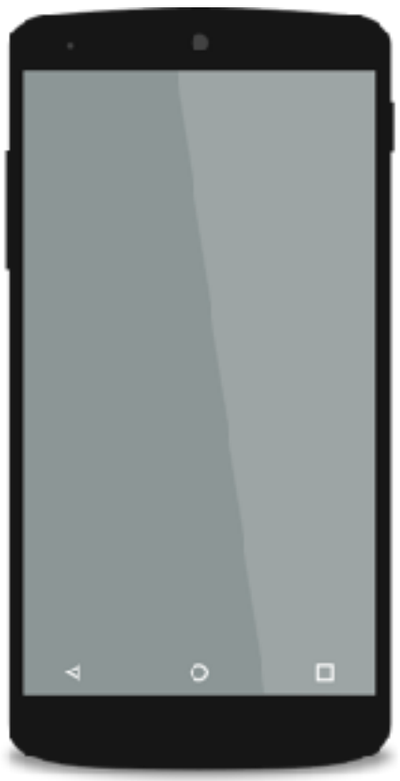
Easy-to-use **Secure** **Replaceable** **~~Additional hardware cost~~**

- **Come for free in the wearable era**.
  - 12% US consumers own at least one wearable device [Kantar Wearable Technology, 2016]
  - 55% consumers have intentions to buy at least one wearable devices [Morgan Stanley, 2014]

Research problem: How to securely and user-friendly unlock smartphone via a trusted companion wearable?

WILLIAM & MARY
CHARTERED 1693

Unlocking Your Phone via **Acoustic** Wearable Tokens

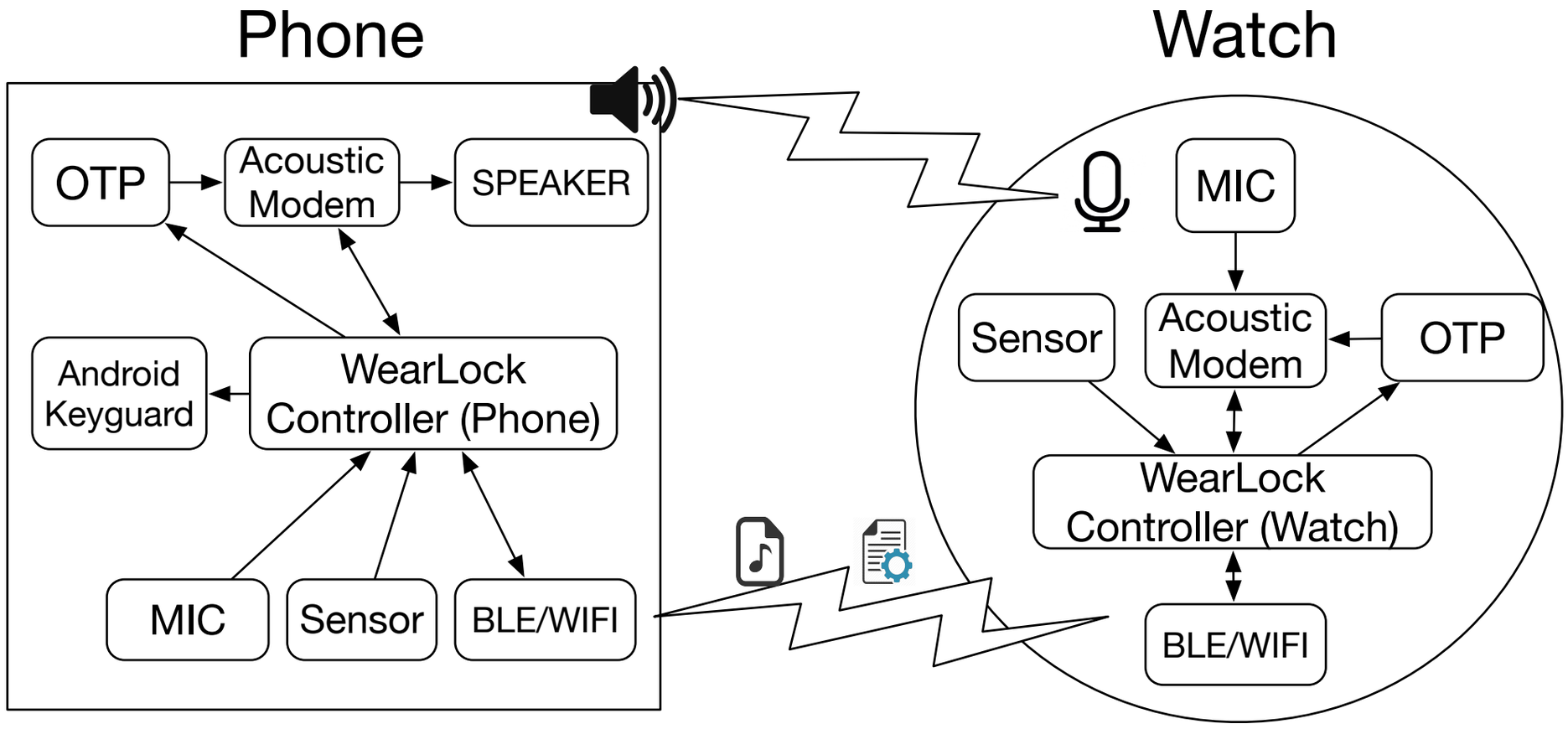


- desirable communication range (**<2m, room level**)
  - NFC communication range:10cm
  - Bluetooth communication range: 10-100m
- no extra hardware additions (**mic & speaker**)

Challenges

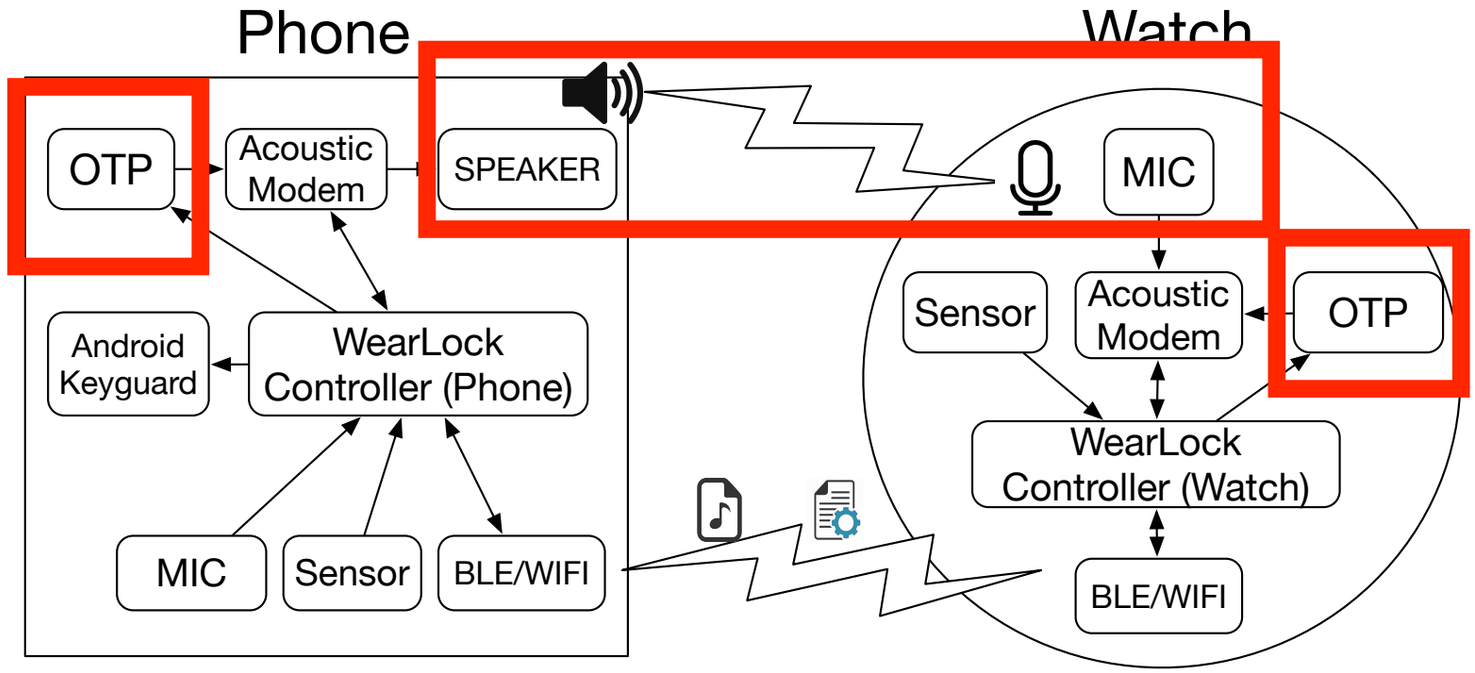
- **build an efficient, reliable and secure communication acoustic channel against ambient noise**
- **system needs to accommodate the limited battery and computation power of the wearable devices**

WearLock System Overview

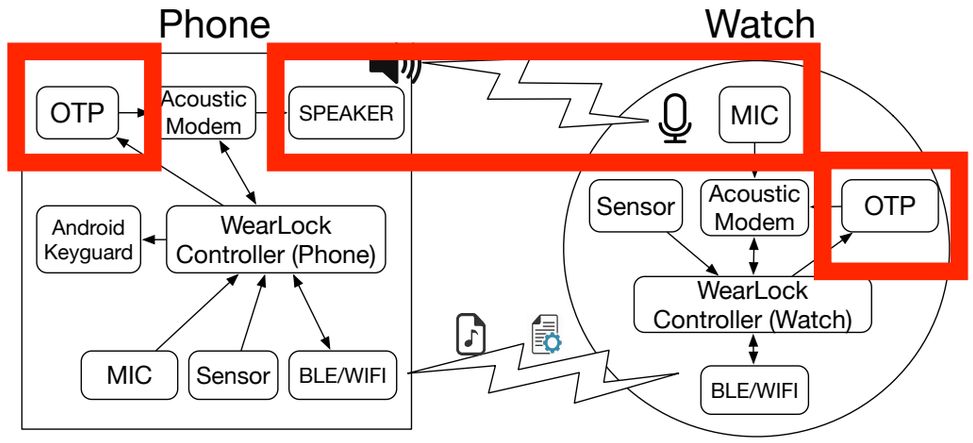


WearLock System Overview

- Acoustic - auth channel
- OTP - generate one time password



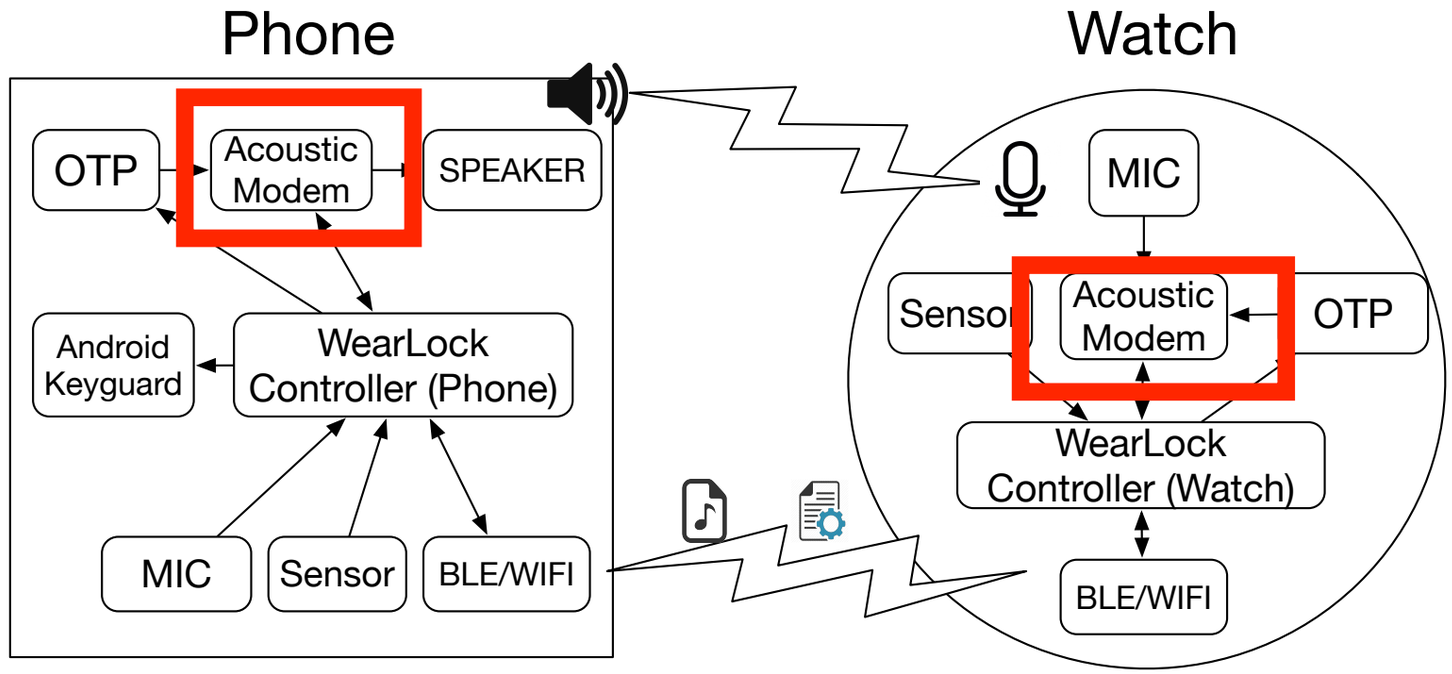
Acoustic Authentication



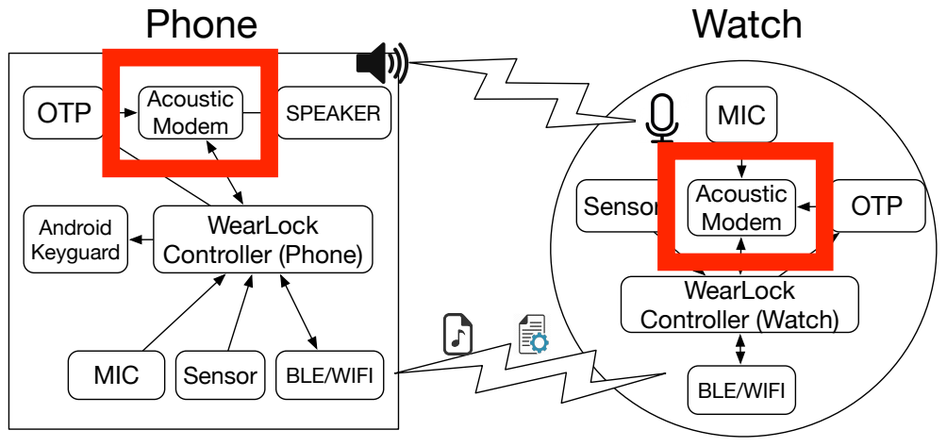
- frequency range - audible 1kHz-6kHz, near-ultrasound 15kHz-20kHz
- ambient noises (e.g., air condition) - channel probing and avoid interference channels
- sound propagation and attenuation - control volume
- secure the acoustic channel
  - phone with mic/speaker, watch with only mic
    - cannot use self-interference cancellation Dhwani(Sigcom13), PriWhisper(IoT journal 2014), Dolphin(AsiaCCS15)
  - send only one time password (counter-based HMAC-based one time password algorithm)

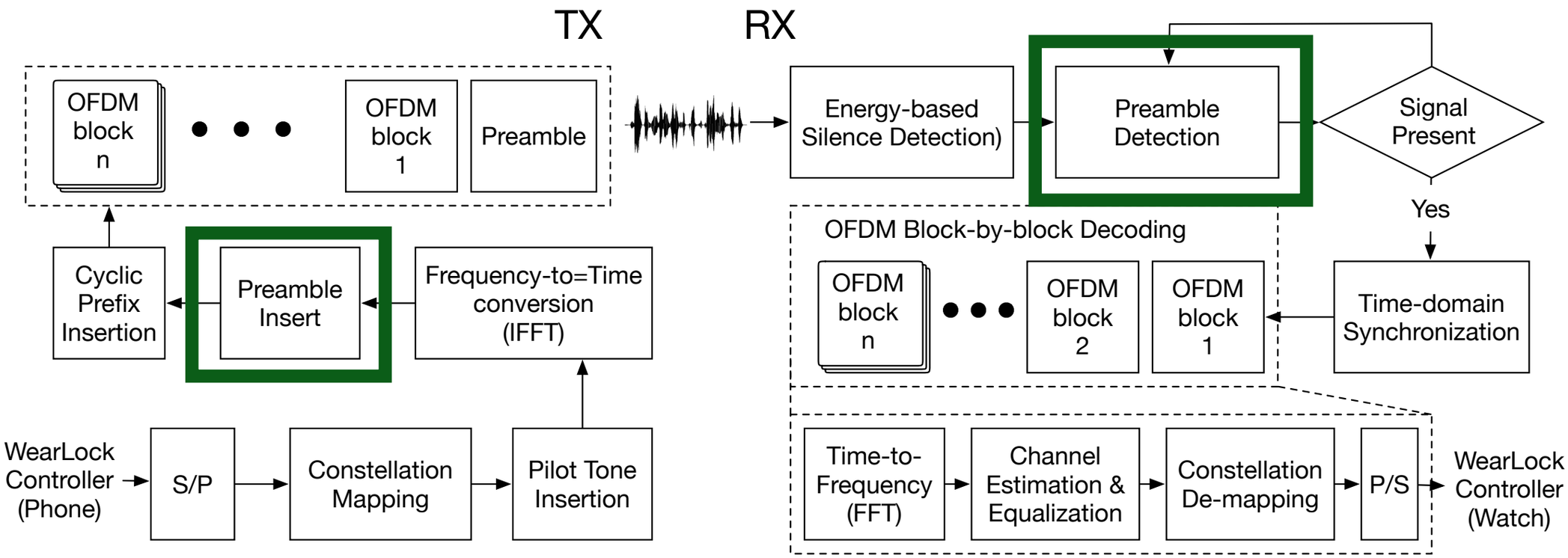
WearLock System Overview

- Acoustic Modem - modulate and demodulate OTP
  - OFDM
    - FFT-based modulation and demodulation

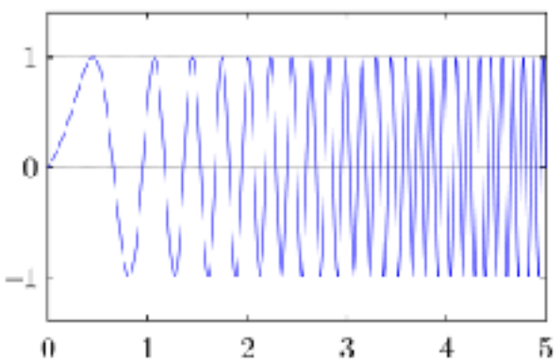


Design Acoustic Modem for Phone-Watch Pair



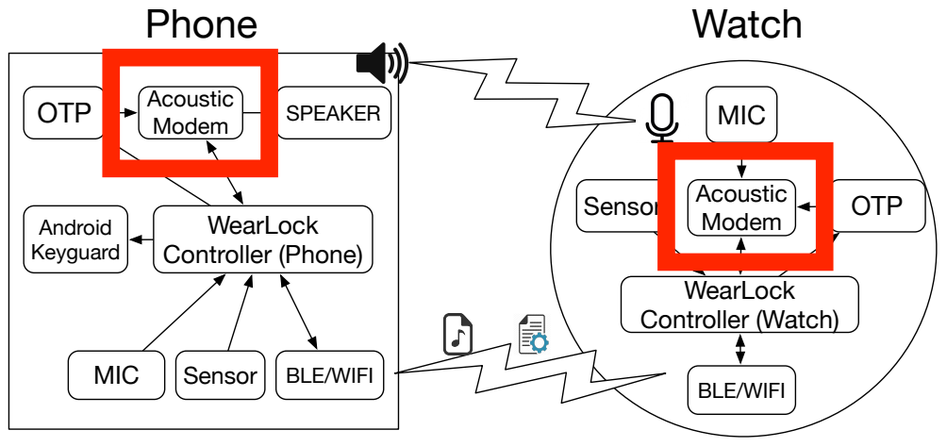


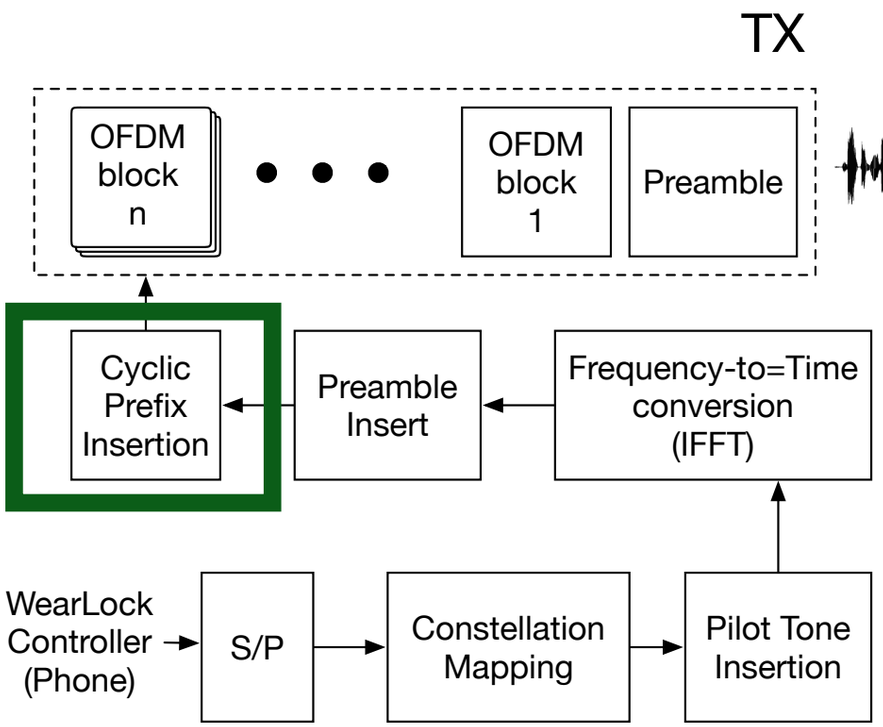
- Preamble design - linearly frequency modulation (chirp/sweep signal), detected by cross-correlation

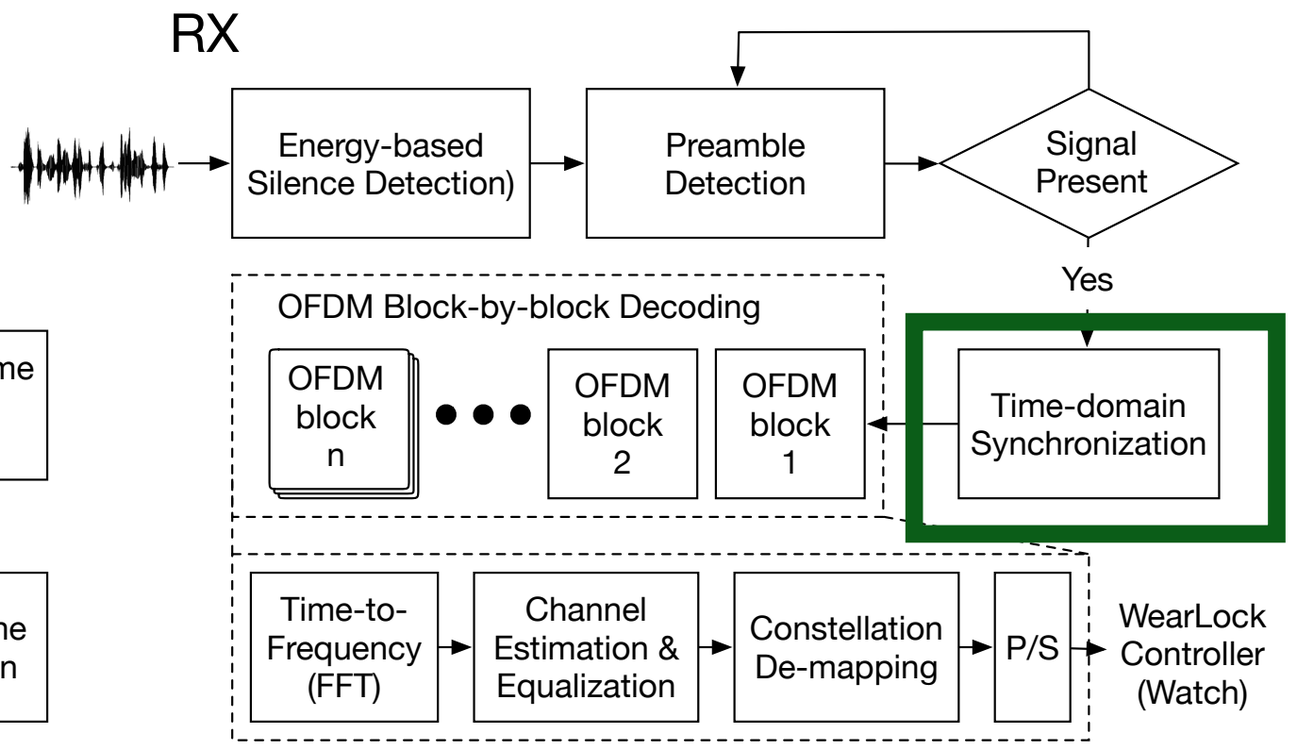


WILLIAM & MARY
CHARTERED 1693

Design Acoustic Modem for Phone-Watch Pair



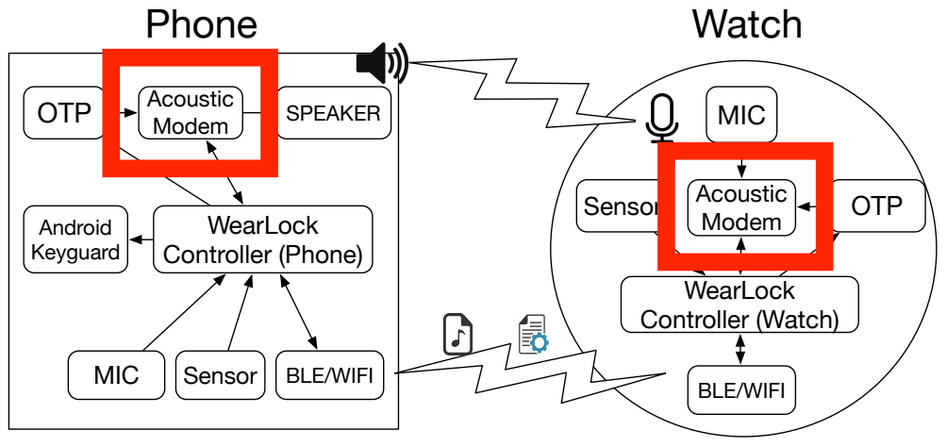


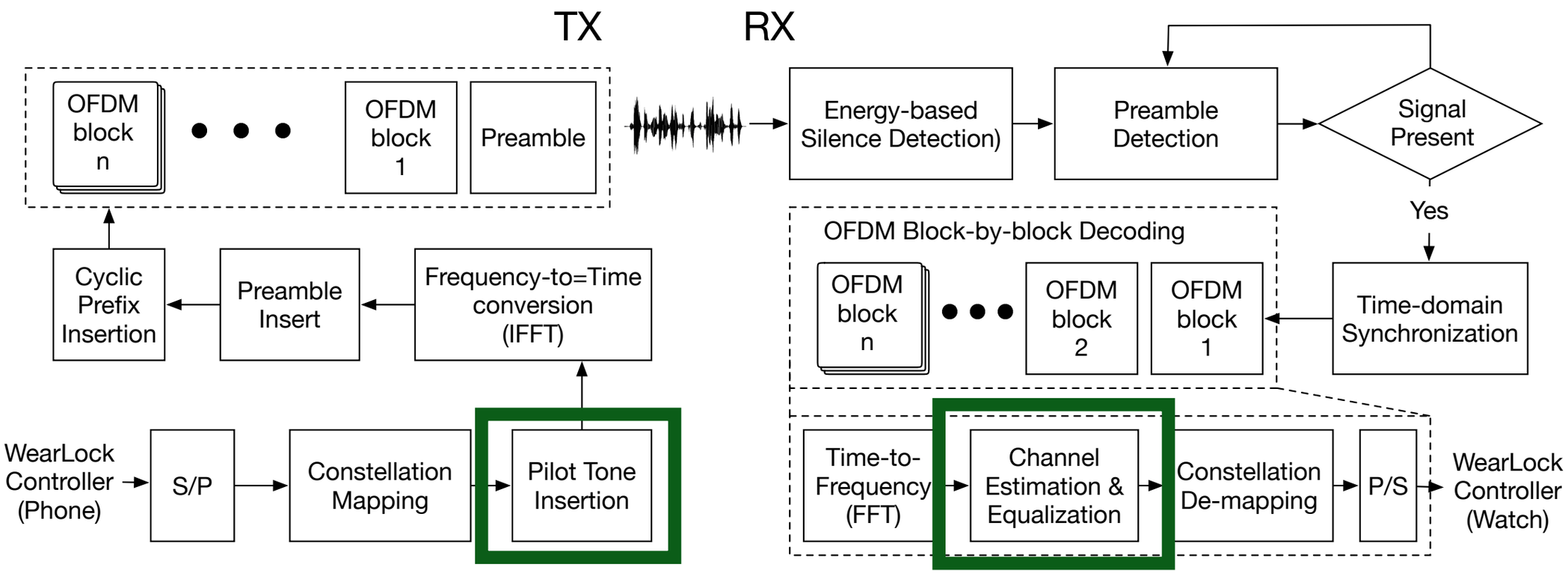


- Time-domain Synchronization
  - coarse sync via ***preamble detection***
  - fine sync via ***cyclic prefix***

$$\underset{t_f}{\operatorname{argmin}} \sum_{t=t_c+t_f}^{t_c+t_f+T_g} x(t)x(t+T_s), \quad \forall t_f \in [-\tau, \tau]$$

Design Acoustic Modem for Phone-Watch Pair





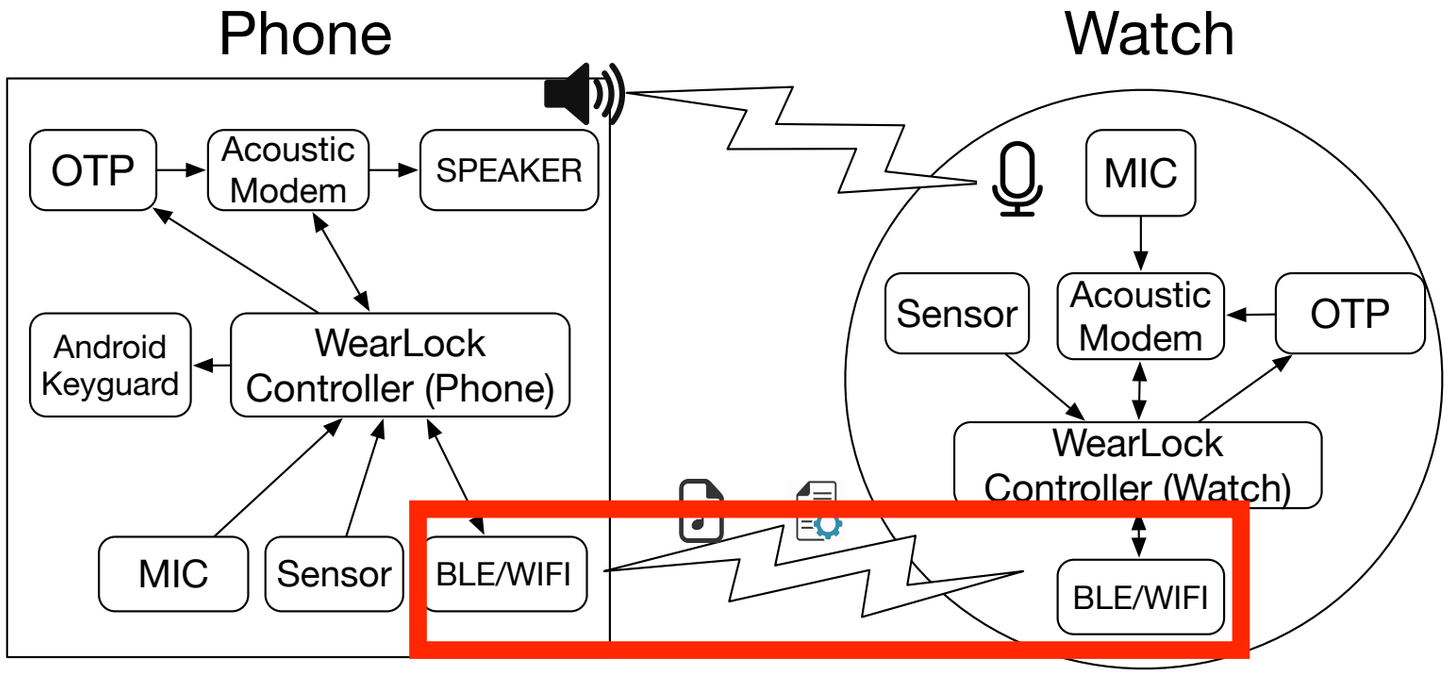
- Channel estimation and equalization - equal-spaced unit powered pilot tones
  - FFT-based interpolation -> channel frequency response
  - By equalizing the known a-priori pilot sub-channel to unit-power, we equalize the data channel at the same time

$$H(k), k \in \mathbb{P} \cup \mathbb{D}$$

$$\hat{s}(k) = \frac{z(k)}{H(k)}$$

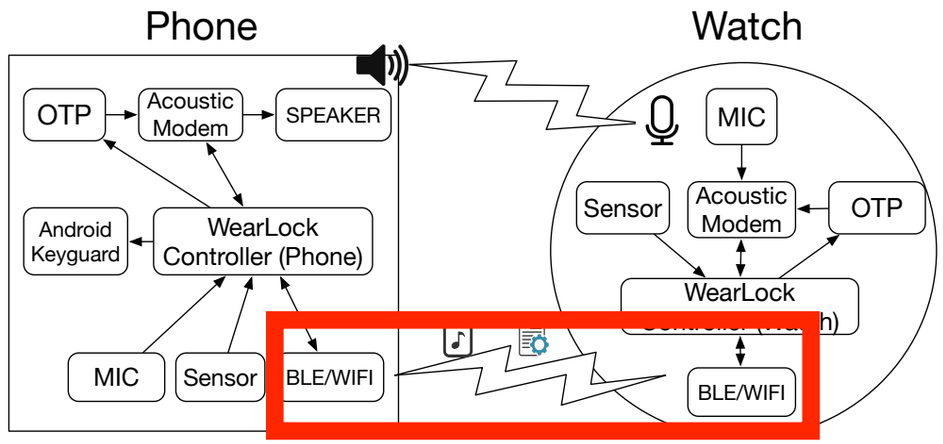
WearLock System Overview

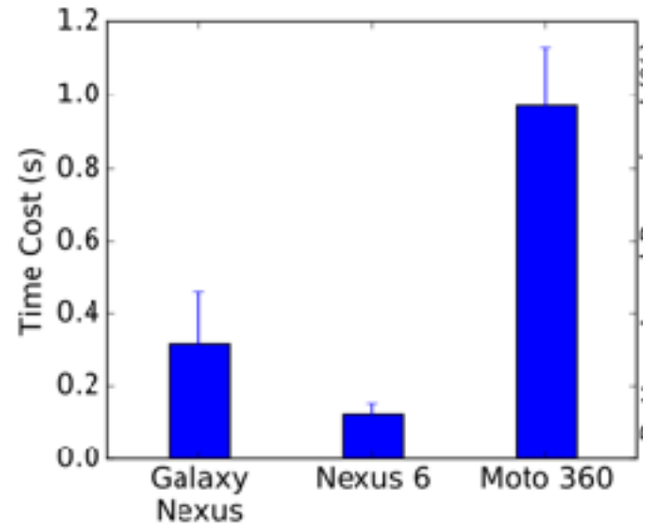
- Wireless - secure control channel



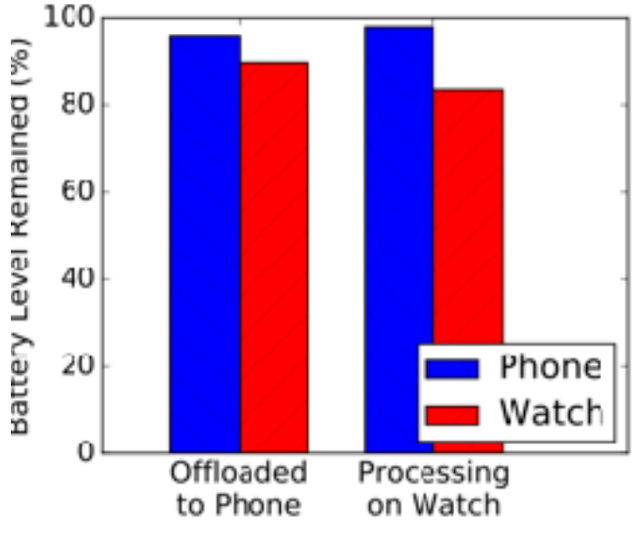
Wireless Control Channel

- sync configurations
  - secret key, counter of OTP
  - OFDM parameters
  - OFDM channel layouts
- offload audio processing
  - reduce computation delay
  - better battery consumption





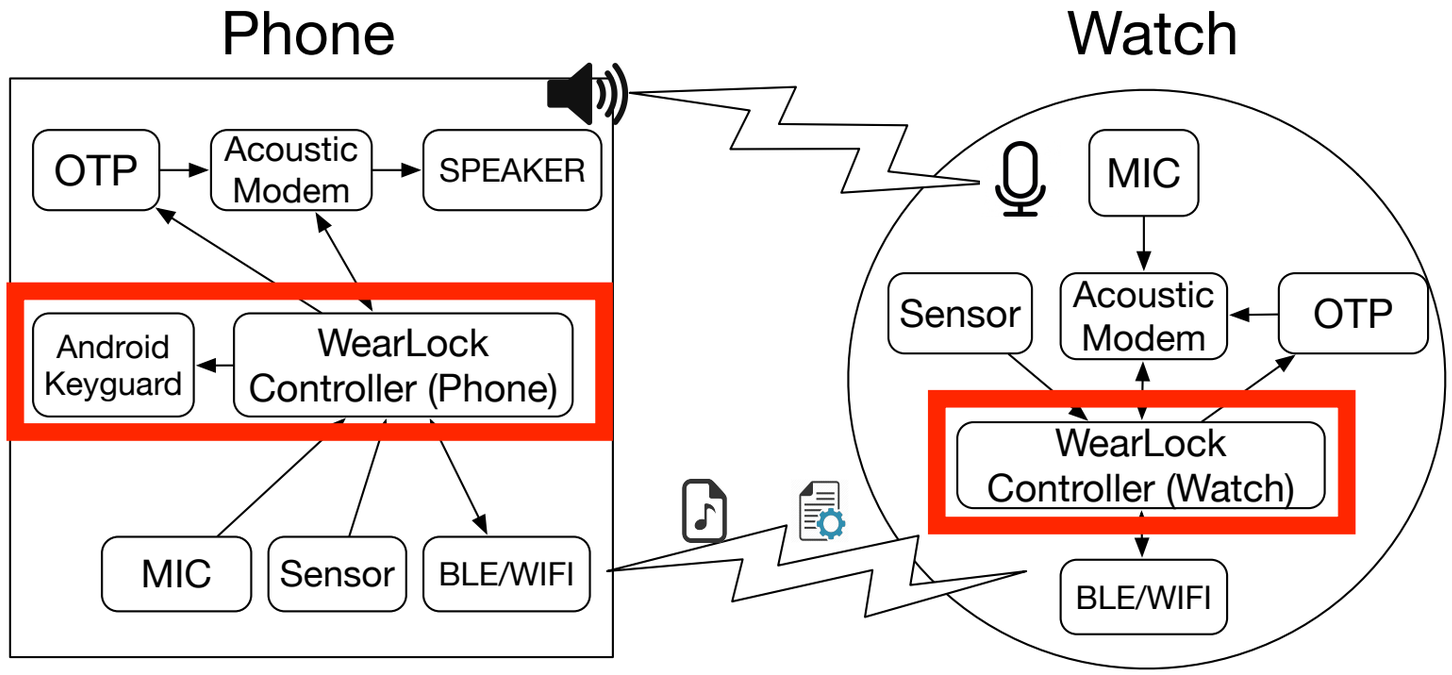
Time cost of processing location



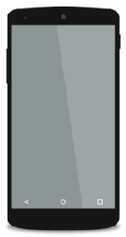
Power consumption of processing location

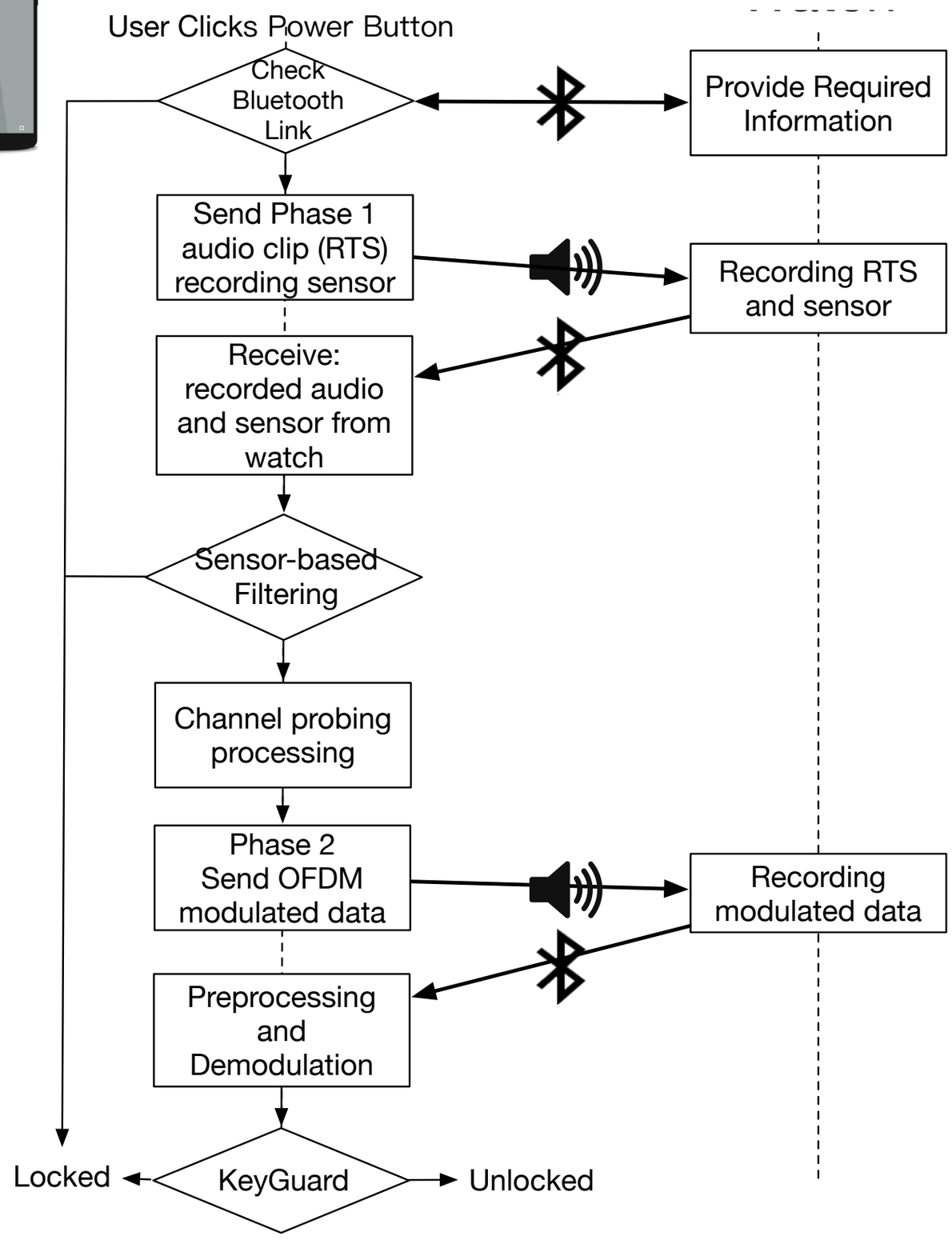
WearLock System Overview

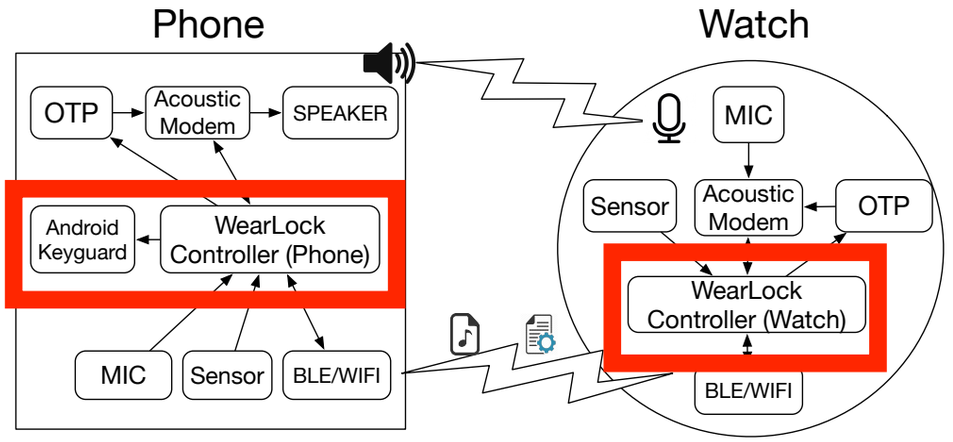
- WearLock Controller - execute the protocol
- Android Keyguard - manage the screen lock



Unlocking Protocol

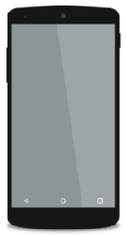


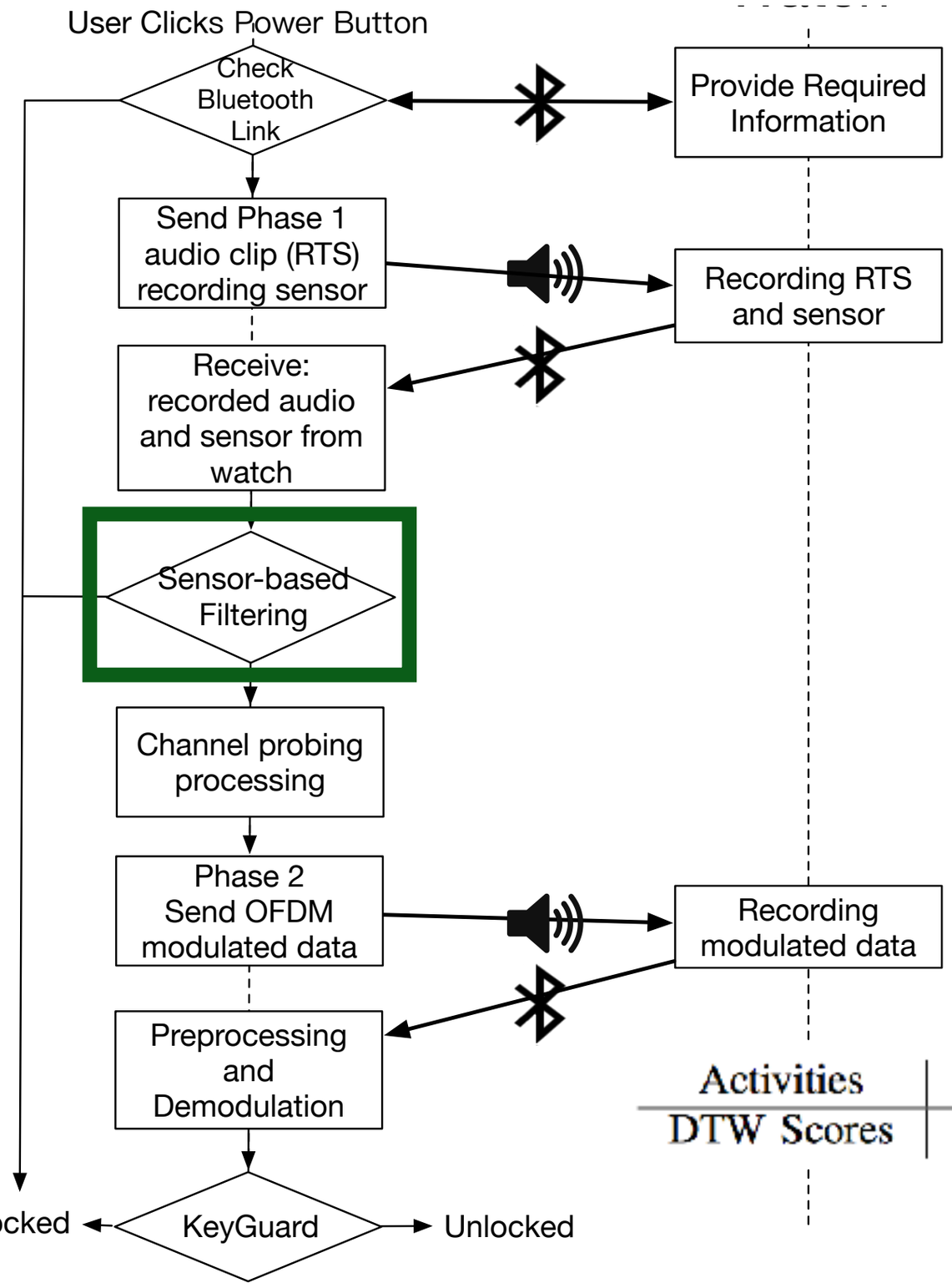




Motion-sensor based filtering

co-location detection via motion similarity





- dynamic time warping, DTW

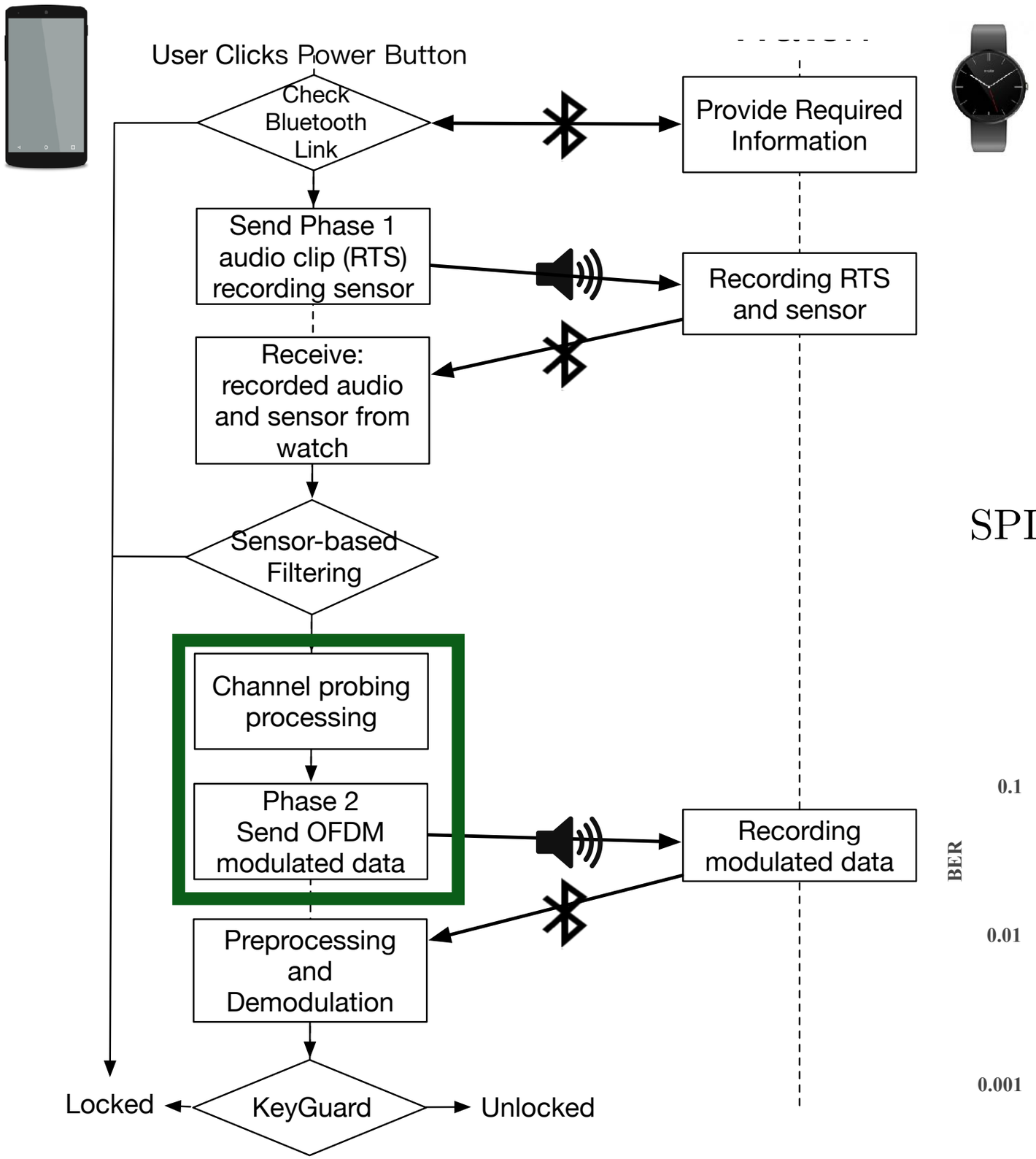
Algorithm 1 Sensor-based Filter

```
1:  procedure SENSOR-BASED FILTERING
2:      for each first phase do
3:          while recording do
4:              sp_{x,y,z} ← phone accelerometer
5:              sw_{x,y,z} ← watch accelerometer
6:          sp ← Normalized(Magnitude(sp_{x,y,z}))
7:          sw ← Normalized(Magnitude(sw_{x,y,z}))
8:          if DTW(sp, sw) > d_h then
9:              abort protocol                ▷ save the computation
10:         else if DTW(sp, sw) < d_l then
11:             skip second phase             ▷ save the computation
12:         else
13:             continue to the second phase
```

Activities	Sitting	Walking	Running	Different	Cost(ms)
DTW Scores	0.05	0.02	0.06	0.20	45.9

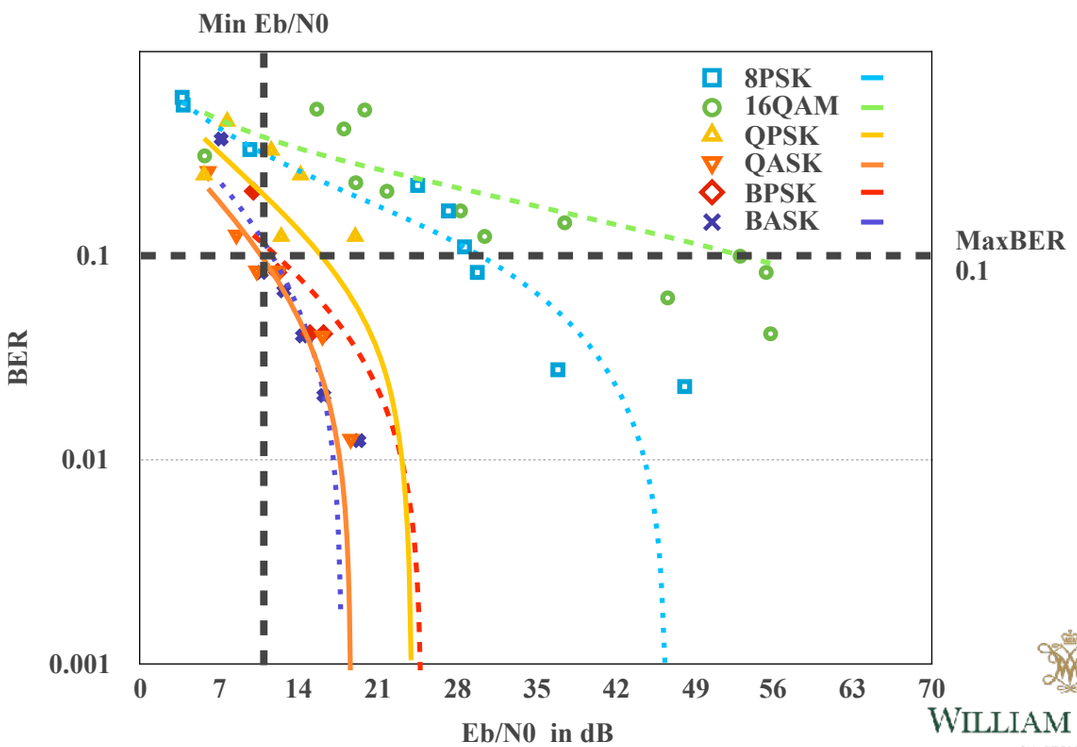
Adaptive Modulation

-select a modulation mode that maintains a BER under target BER with certain distance



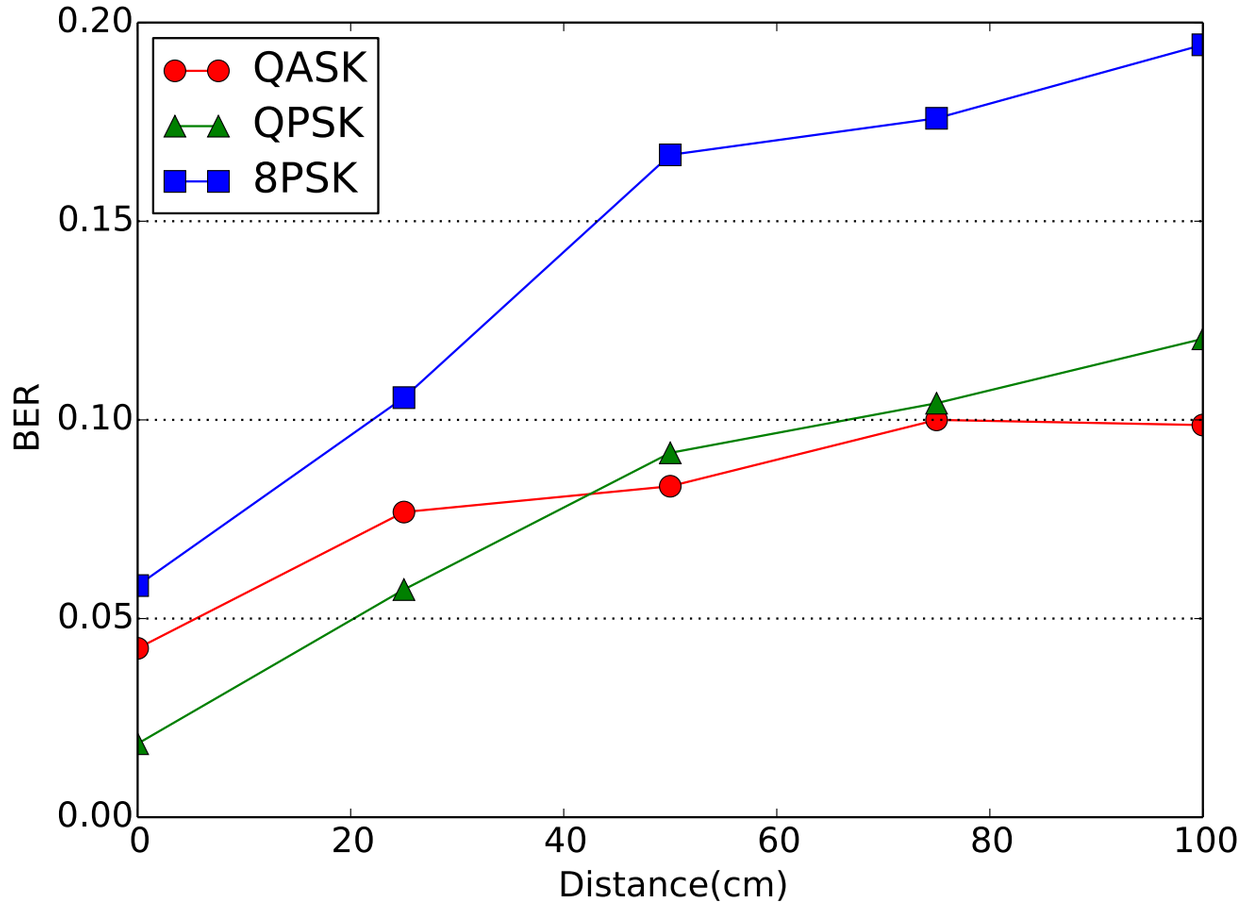
- The higher order of the modulation
  - higher data rate.
  - shorter signal for same bits.
  - more vulnerable to ambient noise and interference (**what we need**).

$$\mathrm{SPL_{tx}} - 20\log_{10}\left(\frac{1.0}{d_0}\right) - \mathrm{SPL_{noise}} > \mathrm{SNR}_{min}$$



WILLIAM & MARY
CHARTERED 1693

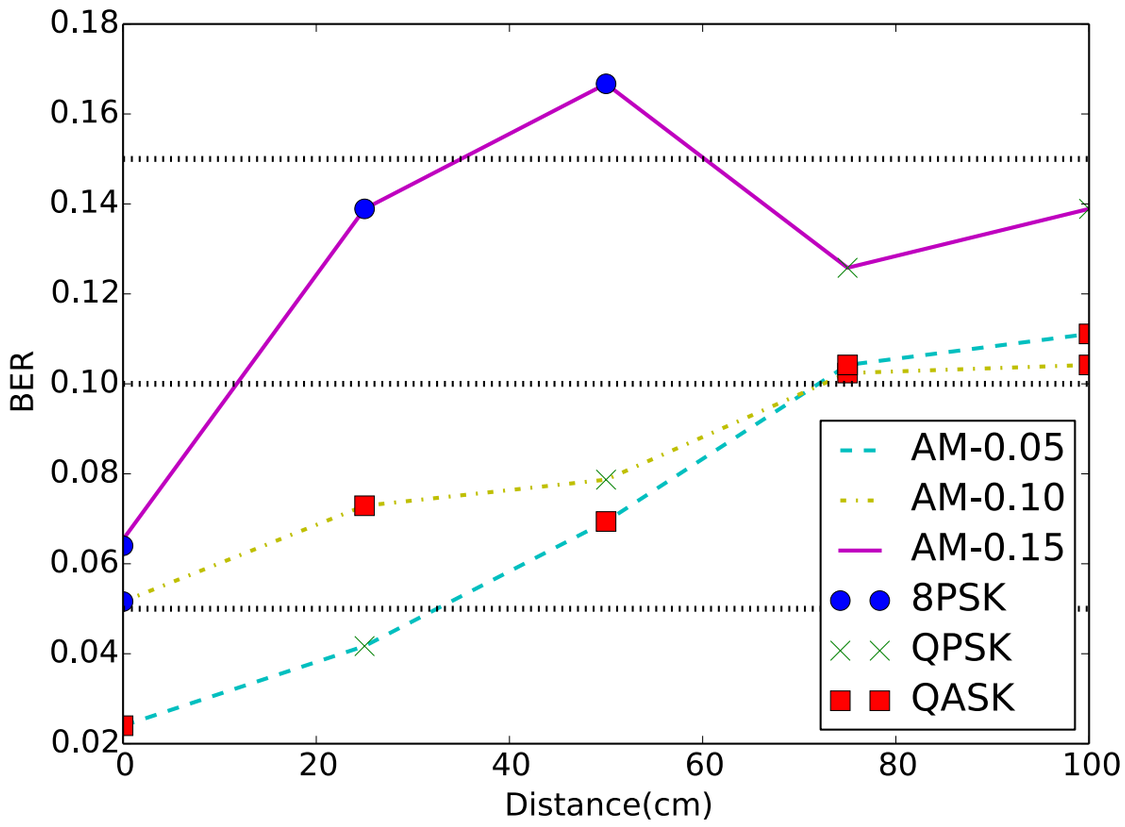
Evaluation - Communication Range



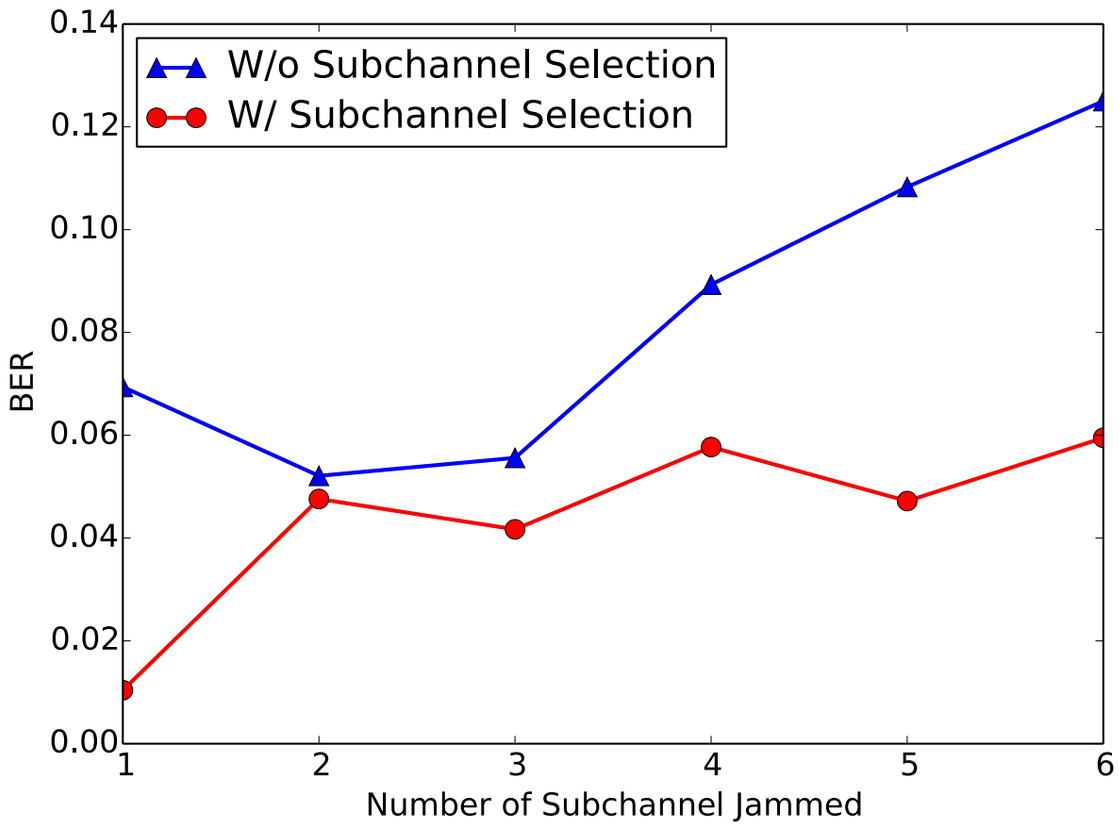
The BER in distances and transmission modes
(near-ultrasound, quiet office room, line-of-sight)

- **Higher order modulation has higher BER.**
- **Showing the feasibility that we can adaptive change the modulation scheme to constrain the max BER within one meter range.**

Evaluation - Adaptive Modulation



The BER in adaptive modulation under different BER constrains.
(near-ultrasound, quiet office room, line-of-sight)



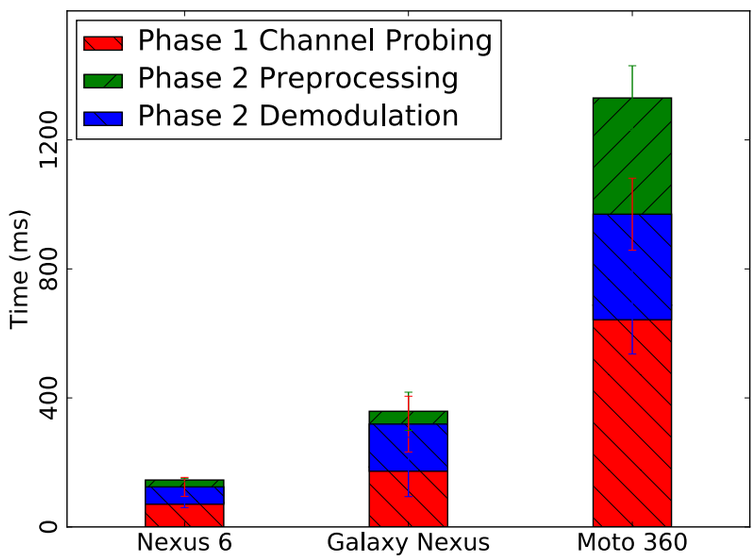
The BER under jamming and sub channel selection
(audible sound, QPSK)

- **The system can adaptively change modulation schemes to make sure the receiver within a certain distance has a BER close to its constrains.**
- **The system can adapt to ambient noise in sub-channel selections and maintain a stable BER.**

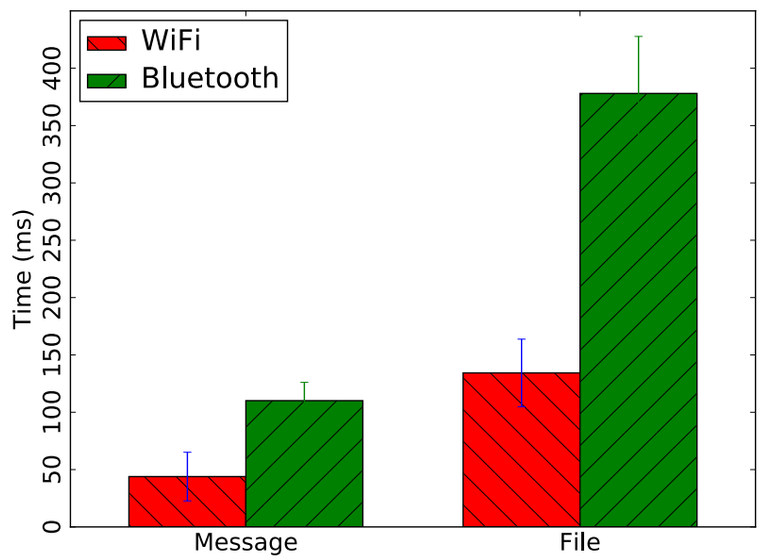
WILLIAM & MARY
CHARTERED 1693

Evaluation - System Delay

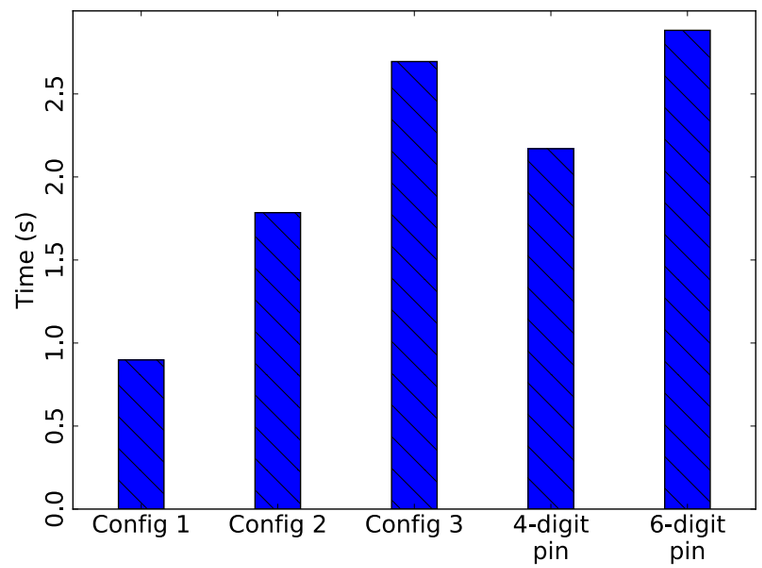
config1: moto360 - wifi - nexus 6
config2: moto360 - bluetooth - galaxy nexus
config3: locally on moto360



Computation delay breakdown



comm. delay between smartphone and smartwatch



total delay in different configurations

- **Offloading computation to smartphone reduce computation delay significantly.**
- **Control channel via WiFi outperforms Bluetooth.**
- **If offloading is enabled, WearLock has at least 17.7% (config2) speedup against manual entering PINs; in the fast case (config1), the speed up is at least 58.6%.**
- **WearLock only needs user to click the power button.**

WILLIAM & MARY
CHARTERED 1693

Evaluation - Field Test

BER vs. Location	Office	Class Room	Cafe	Grocery Store
Diff. Hand (Audible)	0.049 (8PSK)	0.033 (8PSK)	0.026 (QPSK)	0.012 (QPSK)
Same Hand (Audible)	0.089 (8PSK)	0.051 (8PSK)	0.066 (QPSK)	0.065 (QPSK)
Diff. Hand (Near-ultrasound)	0.056 (8PSK)	0.042 (QPSK)	0.023 (QPSK)	0.014 (QPSK)
Same Hand (Near-ultrasound)	0.105 (QPSK)	0.188 (QPSK)	0.197 (QPSK)	0.206 (QPSK)

Average BER is around 0.08

- **There is a direct path blocking in same hand cases.**
- **Near-ultrasound has less interference but significant signal fade in same hand cases.**
- **Audible sound is less convenient but more useable in noises cases.**
- **It would be better to use inaudible sound in quiet spaces and audible sound in noisy spaces as long as the volume is controlled.**

Conclusion

- We show that a convent and secure smartphone unlocking can be achieved by leavening a paired smartwatch.

- WearLock, the implemented system, secures the acoustic channel by adapting the transmission power and modulation configurations, and sends an OTP tokens for validation via acoustics to unlock the smartphone.

- To optimize the system performance, we offload the heavy computation to the phone, and leverage multi-source information including sensor data to reduce unnecessary audio transmissions.

- WearLock can achieve an average bit error rate of 8% in our experiments. WearLock achieves at least 18% speedup even on a low-end device, compared to entering PINs.

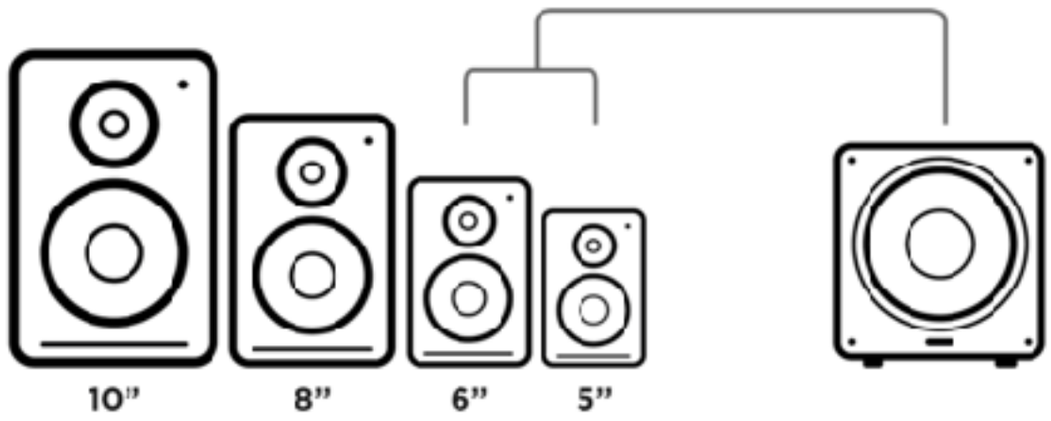
End. Thank you.

Q&A

WILLIAM & MARY
CHARTERED 1693

Security Discussion

- Security Discussion
  - Brutal Force Attack
    - 32bits (select 16 data channels in QPSK/QASK, 11 data channel in 8PSK) -> 2^{32}
  - Co-located Attack
    - <1meter and Line-of-Sight is very hard to achieve for attacker
  - Record and replay Attack
    - timing-based detection (software stack delay)
  - Relay Attack
    - Cannot defense
    - Hard to mount such attack



The most common studio monitor speaker sizes range from 5” to 10”. With a 5” or 6” speaker, consider a separate subwoofer for more bass.

NLOS detection

- analyzes the received preamble: a LFM modulated signal sent in the RTS/CTS phase

- We first check the maximal normalized cross correlation score. If the max score is below a certain threshold (0.05 in our experiment), we will abort the transmission, since it indicates a mismatch on the preamble with high possibility. Otherwise, we can coarsely synchronize the signal.

- Next, we approximate a delay profile $A(t_n)$ of the preamble using cross correlation.

- When the τ_{rms} is beyond a certain threshold we assume that there is a severe body blocking

$$\tau_{\mathrm{rms}} = \sqrt{\frac{\sum_n (t_n - \hat{\tau})^2 A(t_n)}{\sum_n A(t_n)}} \qquad t_n = \frac{n}{F_s} \qquad \hat{\tau} = \frac{\sum_n t_n A(t_n)}{\sum_n A(t_n)}$$

Android Lock Screen PIN Entering Measurement

- Same method as Harbach et al. SOUPS'14

```
public class PhoneUnlockedReceiver extends BroadcastReceiver {

    @Override
    public void onReceive(Context context, Intent intent) {
        if (intent.getAction().equals(Intent.ACTION_USER_PRESENT)){
            Log.d(TAG, "Phone unlocked");
        }else if (intent.getAction().equals(Intent.ACTION_SCREEN_OFF)){
            Log.d(TAG, "Phone locked");
        }
    }
}
```