Dhwani: Peer–Peer Secure Acoustic NFC

Rajalakshmi Nandakumar
Krishna Chintalapudi
Venkata Padmanabhan
Ramarathnam Venkatesan

Microsoft Research India
Near Field Communication (NFC)

- Communication between physically proximate devices.
- **Key Advantage:** No network configuration effort.
- **Association by proximity:** devices are connected to each other by virtue of proximity
- Used in contactless payments, short data transfer, ticketing, healthcare etc.
NFC - Limitations

• Low levels of penetration of NFC hardware today
  – Works on the principle of magnetic induction-special hardware
  – 12% in U.S., as of 2012
  – penetration is expected to be under 50% globally by 2017

• NFC standard does not define security at the physical layer
  – Assumes security is inherent due to low range
  – Snooping NFC transactions has been demonstrated (NISK 2009)

Can we enable secure NFC-like communication in today’s devices?
Yes. We can!

**Dhwani - acoustic NFC system**
- Uses phone’s speaker and microphone.
- Software only – can be a downloadable app.
- Currently supports upto 2.4 Kbps data rate over 1 KHz bandwidth.

**JamSecure – secure communication**
- Information-theoretic approach to security.
- Security at physical layer by jamming and self-interference cancellation at the receiver.
Today’s Talk

• **Dhwani : Acoustic NFC system**
  - Challenges in acoustic communication
  - Dhwani – system design

• **JamSecure : Secure NFC technique**
  - JamSecure - Idea
  - Scope and Limitations

• **Dhwani : Performance**
  - Performance of JamSecure and communication system.
Acoustic Communication

RF Communication

Message → 0001101.. → Modulation → Sender antenna → Decode

Acoustic Communication

Message → 0001101.. → Modulation → Speaker → mic → Decode
Acoustic Communication - Challenges

**RF Communication**

1) Antenna frequency response is flat

2) Multipath (in µs)

3) Channel is defined – interference is limited

**Acoustic Communication**

1) Speaker-mic frequency selectivity

2) Echo (in ms)

3) Channel not defined – ambient noise interference
Challenge 1 : Frequency selectivity

- Imperfect electromechanical conversion
- Frequency response is not uniform
- Significant degradation above 12 KHz – significant data loss in that band
Challenge 2: Ringing and rise time

- 5ms long sine wave was transmitted and received by a nearby device.

Received signal

15 ms ringing time
Causes ISI

2 ms rise time
Challenge 3: Ambient noise

- Ambient noise measured in various locations
- Significant till 6KHz in noisy malls
- Can cause interference

Frequency spectrum of Ambient noise
**Dhwani – Design**

Software designed Acoustic OFDM radio

- Ideal for frequency selective channels
- Carrier-less design
- 128 sub-carriers each 171 Hz width
- Operating Bandwidth : 1 KHz (6-7 KHz)
- Band pass filter at the receiver

- 4 ms cyclic prefix. Handles ISI caused by ringing of devices and multipath

- 8 PSK in each sub-carrier gives 2.4 Kbps data rate

No interference from ambient noise (< 6KHz)
Better frequency response
Dhwani - Design

- Software defined acoustic OFDM radio
  - Ideal for frequency selective channels {challenge 1}

  - Carrier-less design
  - 128 sub-carriers each 171Hz
  - 4ms cyclic prefix {challenge 2}
  - operating bandwidth 1 KHz (6-7KHz)
  - high pass filter at the receiver {challenge 3}
  - 8 PSK in each subcarrier gives 2.4 Kbps data rate.
Today’s Talk

• **Dhwani : Acoustic NFC system**
  
  • Challenges in acoustic communication
  
  • Dhwani – system design

• **JamSecure : Secure NFC technique**

  • JamSecure - Idea
  
  • Scope and Limitations

• **Dhwani : Performance**

  • Performance of JamSecure and communication system.
JamSecure - Idea

Transmitter

\[ A \]

\[ P_A \]

Receiver

\[ B \]

\[ P_B \]

Eavesdropper

\[ E \]

\[ \text{SIC gain} = IC \text{ db} \]

\[ \text{SNR}_B = P_A - P_B + IC \text{ db} \]

\[ \text{SNR}_E = P_{AE} - P_{BE} \text{ db} \]

\[ \text{SNR}_E \approx P_A - P_B \text{ db} \]

How much jamming is needed?

\[ \text{5dB cancellation} \]

\[ \text{no cancellation} \]

\[ \text{Packet Success Probability} \]

\[ \text{SNR [dB]} \]

- \text{SNR at the eavesdropper is to the left of the curve and SNR at the receiver is to the right of the curve.}
Key Challenge – Self Interference cancellation

\[ s(t) \neq r(t) \]

\[ s(t) \]

\[ r(t) \]

Hence estimate the received signal \( r(t) \)

Channel estimation based SIC

- Estimate the frequency dependant channel gain by sending a known sequence
- The frequency resolution depends on the reverberation in the channel

Since reverberation is high (>15ms), these techniques does not give high SIC
Key Observation

received signal $r(t) \approx$ signal sent $s(t)$

- Speaker Microphone characteristics (static)
- Synchronization error (dynamic)
- Multipath (dynamic)

Frequency response mostly remains constant

Frequency selectivity is mostly due to static speaker – microphone characteristics

It can be pre-computed and saved
JamSecure

Training Phase:

• generates a library of n PN sequences

\[ PN_i^{xmit} \quad i = 1..N \]

• Transmits each of PN sequence and records the received signal.

\[ PN_i^{recv} \quad i = 1..N \]
JamSecure

Actual Jamming:

• If one jamming sequence is chosen randomly, eavesdropper can learn the library over time.

\[
JamPN_{j}^{xmit}(m) = \frac{1}{K} \sum_{i=1}^{i=K} PN_{n_i}^{xmit}(m)
\]

Due to linearity

\[
JamPN_{j}^{recv}(m) = \frac{1}{K} \sum_{i=1}^{i=K} PN_{n_i}^{recv}(m)
\]

Key Advantage:

• Eliminates effects due to speaker – mic.
• Computationally intractable to learn PN sequences for eavesdropper.
Compensating for dynamic errors

• **Synchronization errors:**
  – Receiver maintains time-shifted versions of all signals.
  – compares the received PN signal with all the time shifted versions at different sample offsets
  – Identifies the preamble start and sampling offset

• **Multipath errors:**
  – Estimates the channel using first few samples by fourier transform.
  – Applies the corrections for each frequency component.
Limitations of JamSecure

The transmitter and the intended receiver are trusted devices.

**DoS attacks:**
Happens when the eavesdropper also starts jamming.
But does not leak the private data.

**Directional antenna attacks:**
Eavesdropper focuses only on the transmitter
Hard in practice as it has to focus into < 10cm.
Outline

• **Dhwani : Acoustic NFC system**
  • Challenges in acoustic communication
  • Dhwani – system design

• **JamSecure : Secure NFC technique**
  • JamSecure - Idea
  • Scope and Limitations

• **Dhwani : Performance**
  • Performance of JamSecure and communication system.
Dhwani – Communication range

Packet success rates at different transmission ranges

- Dhwani enables NFC like communication with range < 10cm
- PSR is 100% for BPSK and 90% for QPSK
Performance of SIC

Self interference cancellation

Locations:
- L1: small conference room
- L2: large conference room
- L3: open pantry
- Li-Lj: training at Li and testing at Lj

For training and testing at the same location (L1-L1), SIC > 10db when k = 5
For training and testing at different locations, SIC > 6db
Dhwani

• Enables NFC in today’s devices
• Software only solution
• Provides security at physical layer
Related Work

Acoustic communication

“Audio Networking – The forgotten wireless technology” (IEEE pervasive computing 2005)
- Provides extensive review of short and long distance acoustic communication
- Uses on-off keying
- 270 bps data rate

JamSecure

IMDShield – “They can hear your heartbeats : Non-invasive security for implanted medical devices” (Sigcomm 2011)
- Security for IMD without modifying them.
- Base station that continuously listens to IMD transmissions and transmits a jamming signal to secure it from eavesdroppers.
- Channel estimation based SIC
- Dhwani a) software only b) pre-computed library based SIC