Distinguishing Users with Capacitive Touch Communication

Vu, Baid, Gao, Gruteser, Howard, Lindqvist, Spasojevic, Walling

Rutgers University
Mobicom 2012

Computer Networking
CptS/EE555
Michael Carosino
Washington State University

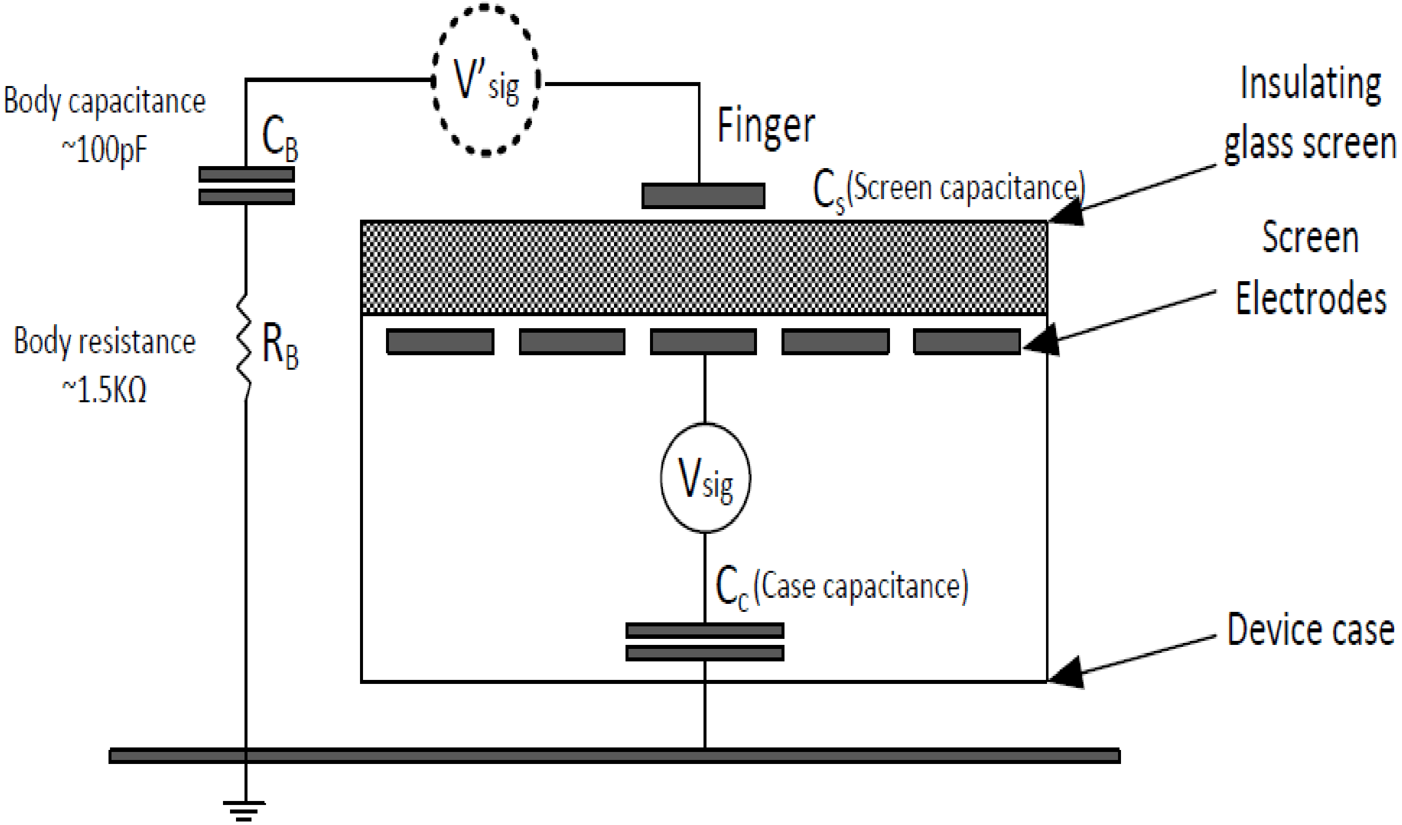
Introduction

- Mobile devices such as smart phones, tablets, laptops have become increasingly ubiquitous
- Many of these devices have adopted touch screens as the primary method of interfacing with the user
- Devices are often shared between multiple users and even used simultaneously
- User identification and authentication has become an increasing concern
- Existing methods tend to be slow, cumbersome, and exploitable

Capacitive Touchscreen Technology

- Projected Capacitive Touch (PCT) has become the standard for mobile devices
- PCT utilizes an etched grid of electrodes behind the screen
- Mutual capacitive PCT measures the capacitance at every intersection of this grid
- Provides an accurate location of touch point and supports multiple touch tracking

Capacitive Touchscreen Diagram



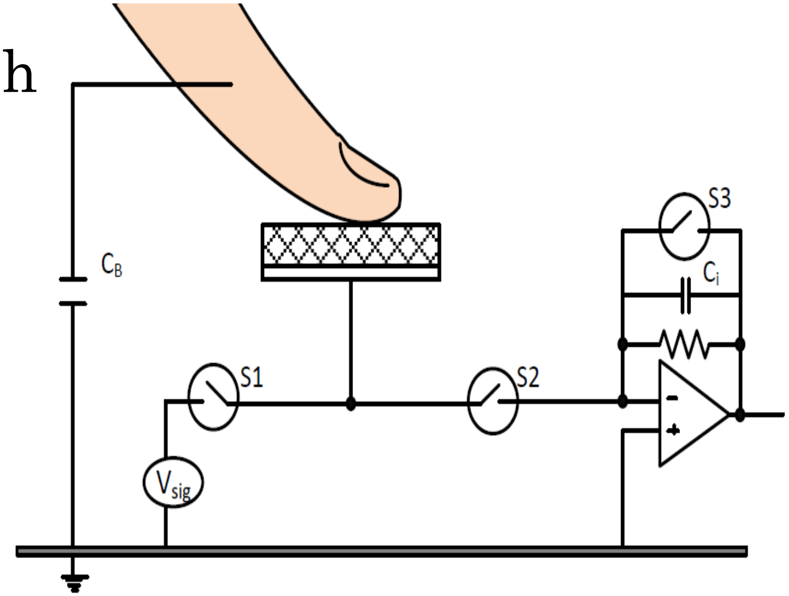
Capacitive Sensing Circuit

S3 initially closed to remove any charge on Ci

S3 and S2 are opened while S1 is closed, allowing the common node to charge fully to Vsig

S1 is opened and S2 closed, causing charge to flow onto integrating capacitor Ci

After fixed number of repetitions of the cycle, accumulated charge on Ci will reflect the proximity of the touch finger or device to the sensing node



Existing Authentication Methods

- PINs, passwords, swipe patterns are easy to implement but are observable and have low information entropy
- Authentication tokens, Magkey, RFID tokens are more costly, require specific hardware, and are prone to wireless sniffing and interference
- Iris, face, and voice recognition either require specialized hardware or are still easily exploited by attackers

Capacitive Touch Communication

- A “wireless” communication where a touchscreen acts as a receiver and small ring-like device or bio-implant acts as a transmitter
- Restricting area of study to off the shelf touchscreen devices without hardware or firmware modification for more rapid deployment
- Raw sensor voltages will not be available, must work with touch events returned by the touch screen driver

Artificial Touch Event creation

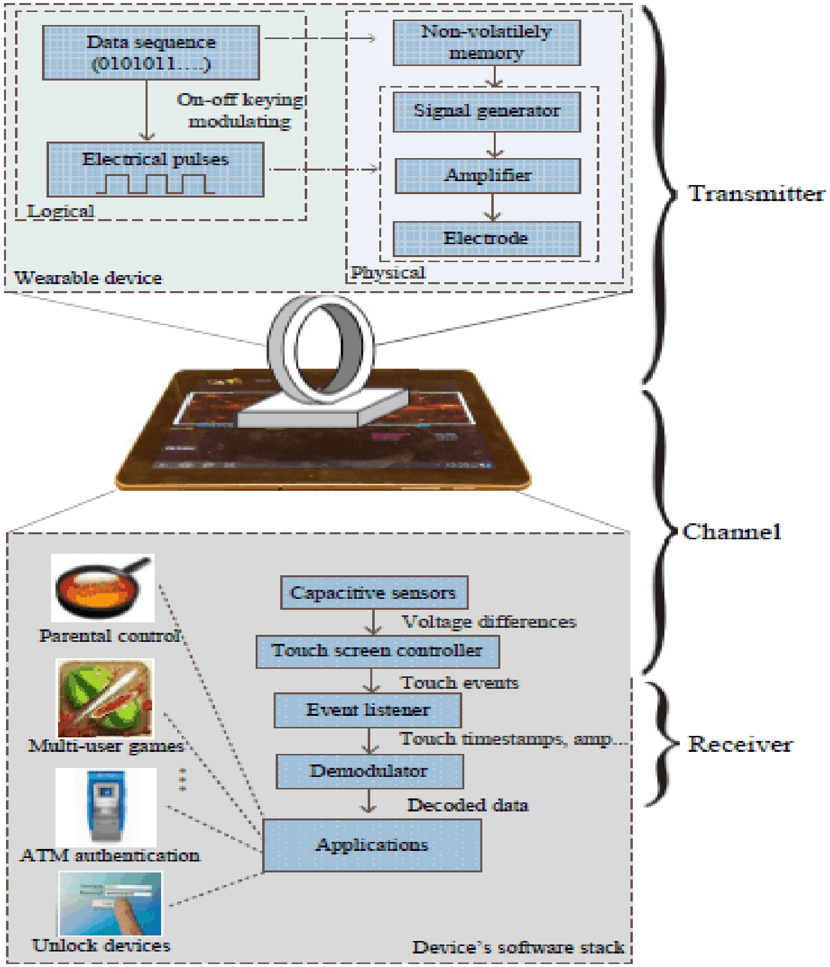
- Can manually increase or decrease charge integrated on Ci by means of injecting a synchronized signal V'sig into the circuit
- Such synchronization is not possible without access to Vsig
- Alternatively, an unsynchronized lower frequency signal is injected causing Ci to be charged/discharged asynchronously
- This method results in irregular but repetitive touch/no touch events reported by the touch screen driver

Communication System Overview

The transmitter consists of wearable ring that when pressed against the screen acts as voltage source V’sig and transmits an identifier or authentication token

The channel is made up of the touchscreen hardware components and the firmware used to detect touch events

The receiver is made up of the software to listen for touch events and utilize their timestamps in order to demodulate them using event threshold detection



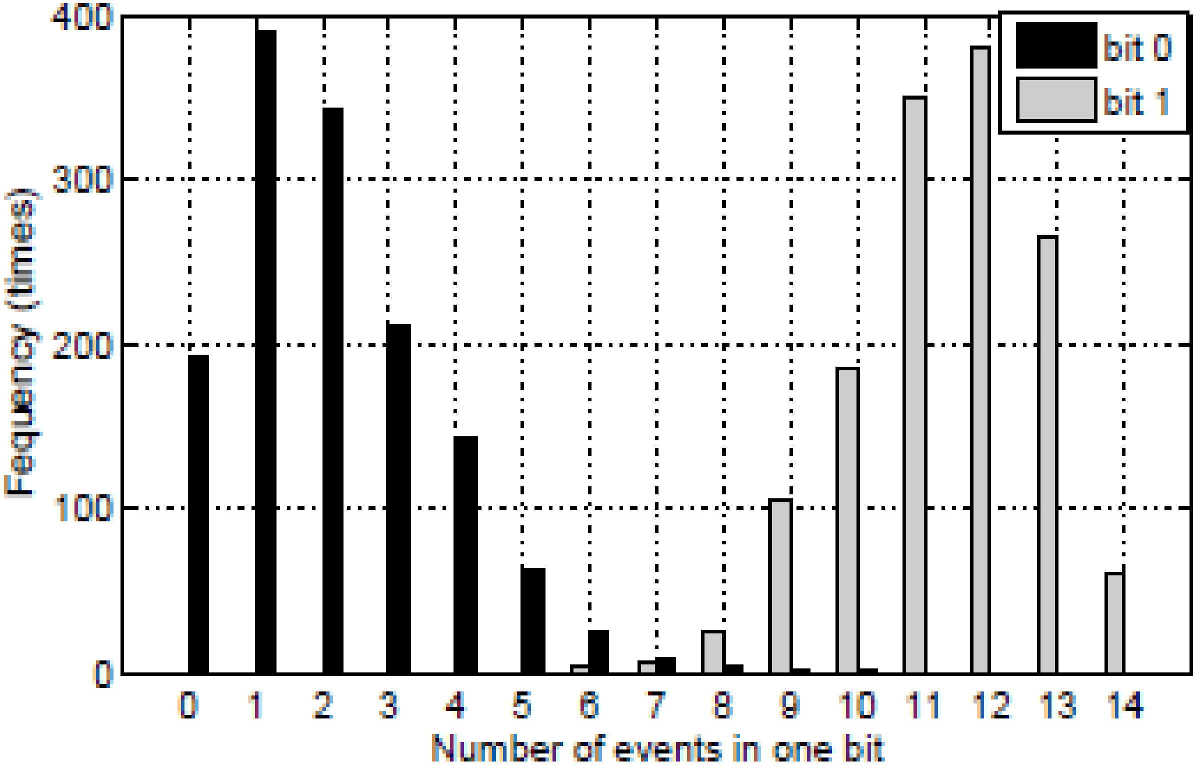
Decoder Design Issues

- In testing this method, multiple challenges have been discovered:
- Receiver responds differently to the same input when the inputs sent before it differ (channel has memory)
- Variable delay between symbol transmission and reception due to touch screen controller processing delay and jitter
- Channel adds an unknown delay between the receiver and transmitter

Characterizing the Channel

- Jitter, delay, and channel performance varies vastly between different touch devices
- To account for this, an off-line algorithm is run with a predetermined input sequence so that the output can be analyzed
- Ideally, given a set of received touch responses, the number of responses corresponding to a bit 0 should be minimized and the number corresponding to a bit 1 be maximized

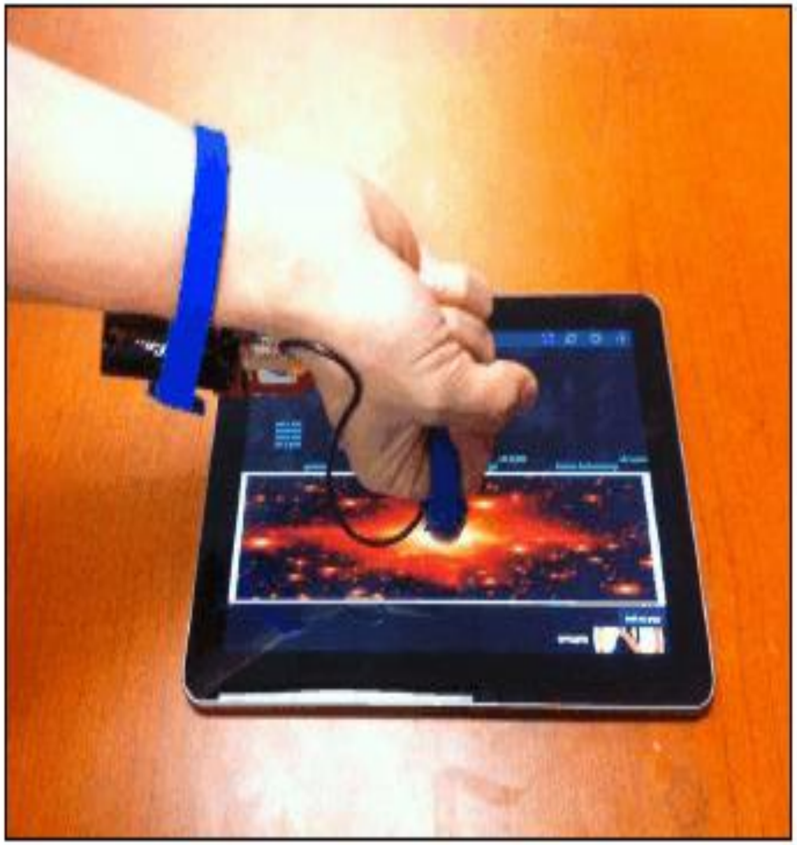
Example Channel Response Histogram

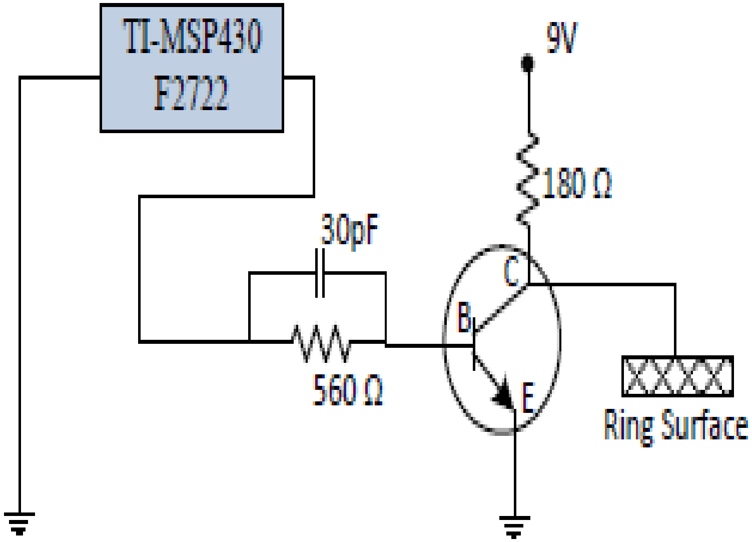


Minimum Distance Demodulation

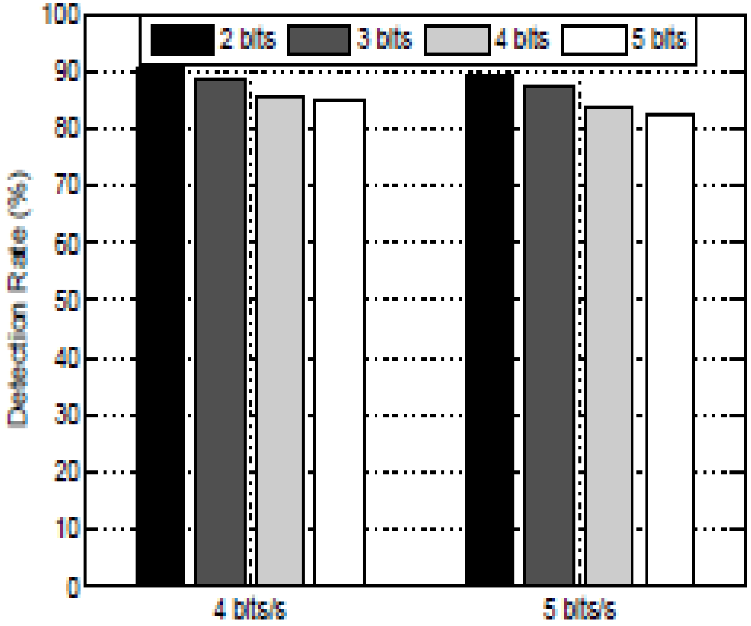
- Decoding and demodulation can proceed utilizing the previously determined event thresholds
- The minimum distance algorithm operates by first selecting the length of an event sequence via the event thresholds
- Next, the algorithm traverses all the events in the sequence to test all starting points
- At each starting point, the event sequence is compared with every possible transmitted message
- The closest or most similar message over all starting points is chosen as the decoded message

Transmitter Ring Overview

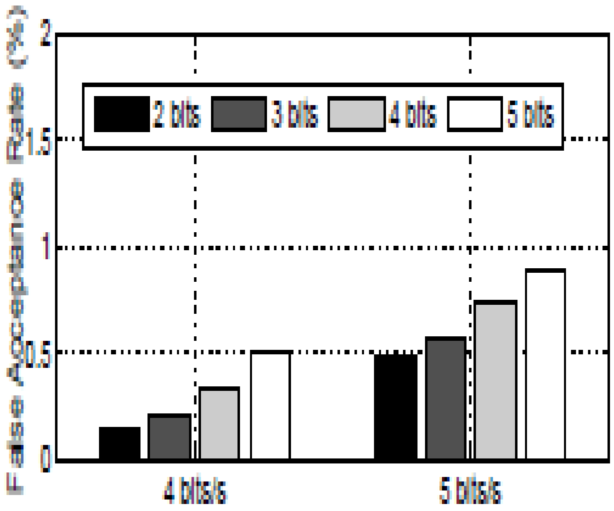




Prototype Test Results



(a) Detection rate



(b) False acceptance rate

CONCLUSIONS

- Experiments show that using the touchscreen as a communication channel is feasible
- Challenges remain in reducing channel error rate and false positives
- Data rates are on the range of 4-10 bits per second which need to be improved
- Will require significant improvements before being valuable as a secure authentication technology

Ideas for Future Work

- Investigating the touchscreen channel further and determining if higher complexity channel codes such as Turbo Codes can be used
- Research into the touch screen driver of current generation rooted phones to discover if more info is available then just touch events
- Design of a feedback photodiode into the ring which would allow for two way communication between the device and the ring
- This would allow for a challenge-response authentication and may also alleviate other issues such as timing jitter and delay.