You foot the bill! Attacking NFC with MIMO

Jingxian Wang, Yuyi Sun, Ke Li†, Swarun Kumar

Carnegie Mellon University

†ECE Summer Intern

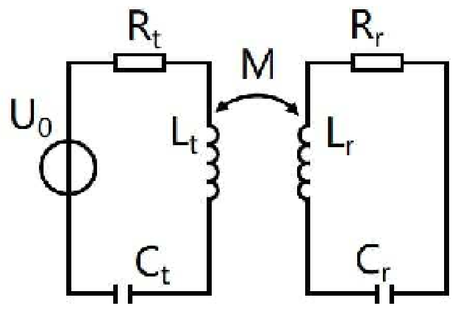
ECE Summer Undergraduate Research Symposium

MOTIVATION

Develop a blind near-field beamforming algorithm to steer maximized power for the NFC cards in the near-field (NF) with unknown locations, orientation and impedance to extend the NFC communication range from 5cm to 1m.

PRIMER ON NFC

The underlying principle of NFC is based on magnetic induction. The NFC reader as an interrogator initiates the communication in the 13.56 MHz spectrum. The current flows through the antenna coil of NFC reader will generate magnetic field which can couple with nearby NFC tags. The magnetic inductive coupling transfer the energy from the NFC reader to the tag, which generates an induced current in the tag circuit.



$$V_T = Z_T I_{T_T} - j\omega M I_R$$
$$Z_R I_R = j\omega M I_T$$

In the near field, since the strength of magnetic fields decrease rapidly with distance which results in an inverse 4-6th power diminishing, the communication range of NFC systems is around 5 cm.

BLIND NF BEAMFORMING

Recoil provides a near-field MIMO solution to beam maximized power to nearby NFC cards at unknown locations, orientations and impedance using multiple NFC readers. We call this *blind near-field beamforming*.

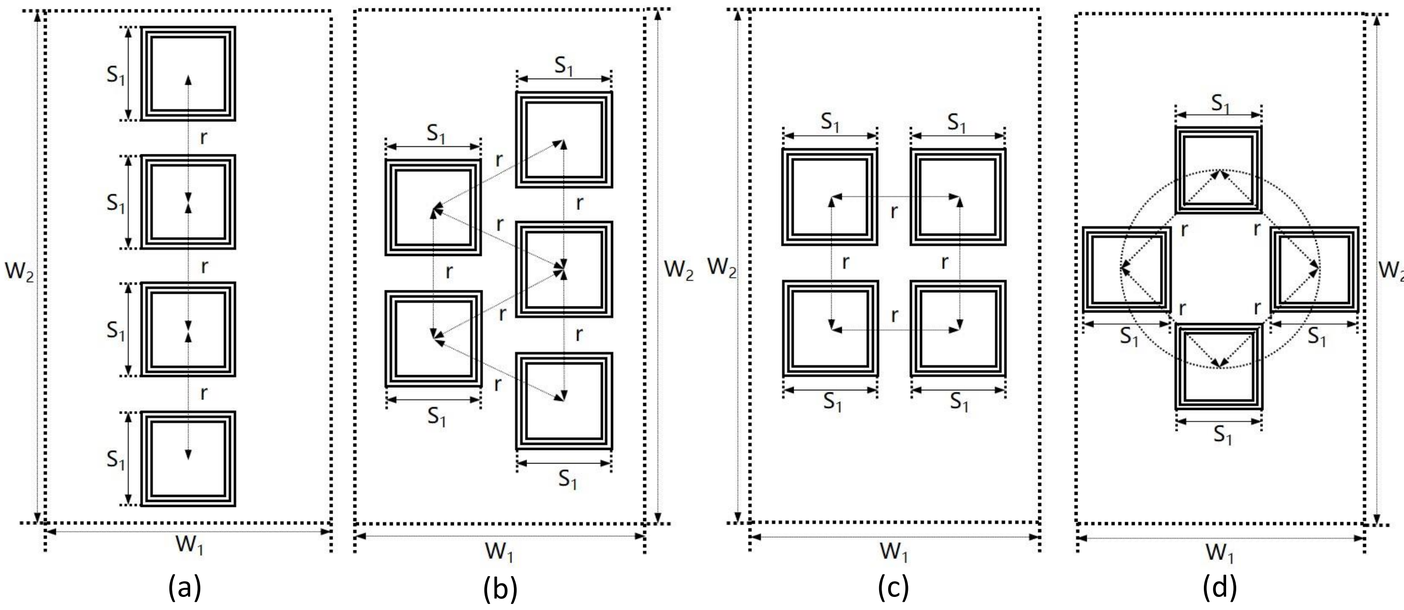
- When an NFC tag is in the proximity of an NFC reader, the tag acts as a voltage divider. The voltage variation of the reader circuit is proportional to the induced current of the tag harvested from the reader.
- Given that we assume only one tag is in the near field, we can obtain the optimal beamforming vector B_{j^*} as follows:

$$j^* = arg\min_j \sum_i^n \|V_{ij}\|^2$$

- The presence of ambient metal object performs as a DC offset and can considerably influence our optimal beamforming searching.

COIL DESIGN OPTIMIZATION

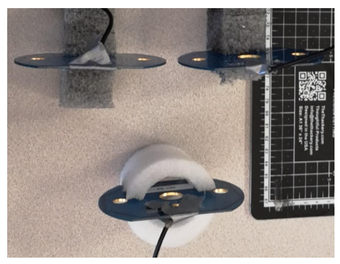
- We try to formulate our problem to find the best geometry of the beamformer. It is significant to study how to design the geometry of the transmitter coils in order to obtain the best communication distance between the beamformer and the receiver.
- Considering that the multi-transmitter attack devices should be attached on human body, the dimension parameters should be constrained by a certain area. In order to search for the optimum geometry, we divide the constraints into different situations.



(a) The coils are lined up in a row, (b) The coils are lined up in two row, and N is an odd number, (c) The coils are lined up in two row, and N is an even number, (d) N coils compose a circle.

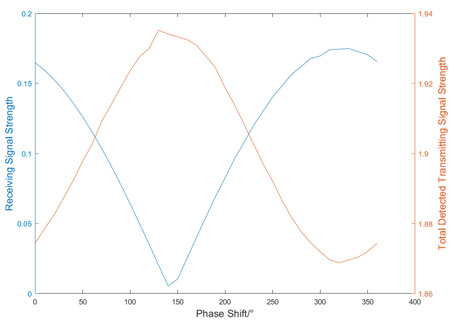
IMPLEMENTATION & EVALUATION

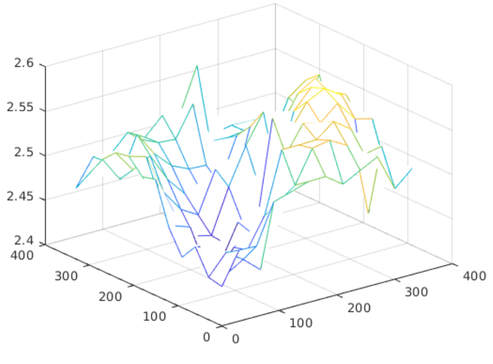
- We set up the experiment environment with two or three transmitting antennas and one receiving antenna. Commercial antennas are used first and will be replaced by self-made antennas later.



- Our evaluation covers varied system parameters:
  - Number of Transmitting Antennas
  - Geometry of the Beamformer
  - Distance between the Beamformer and the Receiver
  - Presence of the Metal Object

- The change of signal power on the transmitting end has strong negative relations with the signal strength on the receiving end.
- The curve or surface of the transmitting power is convex so Recoil can perform gradient descent to find the optimal beamforming on the receiving end without a response from the card or tag.
- Recoil reveals a maximum range of one meter between the reader to the attacked NFC card, a twentyfold improvement on the commercial distance.





Carnegie Mellon University

Electrical & Computer ENGINEERING

WiTech