RF-Cloak: Securing RFID Cards Without Modifying them

Haitham Hassanieh

Jue Wang, Dina Katabi, Tadayoshi Kohno

Massachusetts Institute of Technology

wireless @mit

RFIDs Are Used in Sensitive Applications

Access Control

Credit Cards

Passports

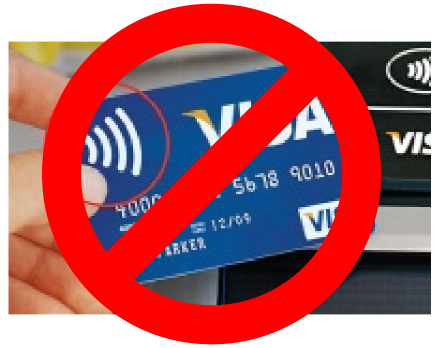
Pharmaceutical Drugs

Anti-Theft Car Immobilizers

Public Transportation

RFIDs Are Used in Sensitive Applications

Access Control
[SECRYPT'09, S&P'09 ESORICS'08, Usenix'08]



Credit Cards
[DefCon'13, ShmooCon'12, DefCon'11 , Usenix'05]

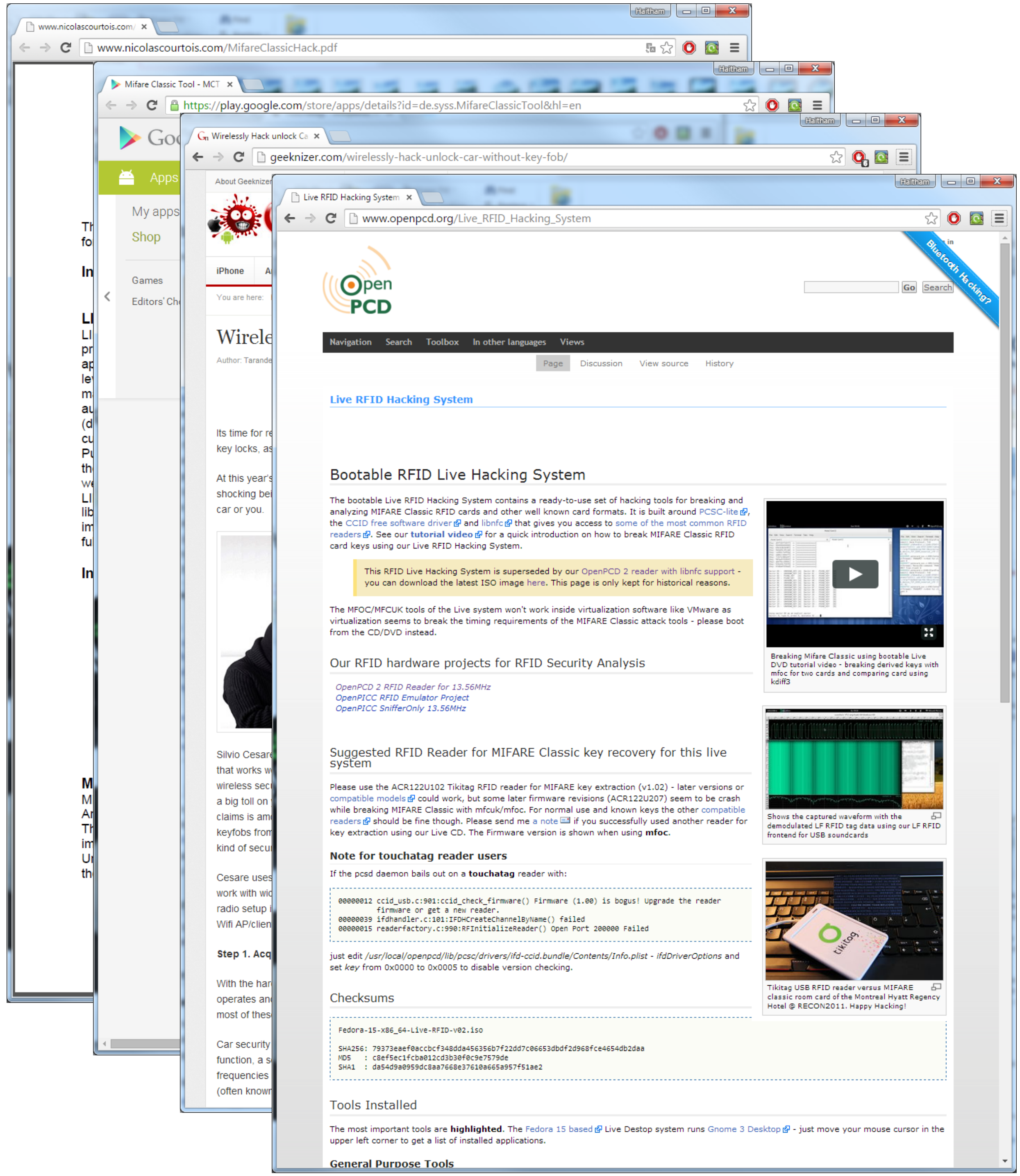
Passports
[DefCon'12, HackaDay'12, BlackHat'06]

Pharmaceutical Drugs
[CCS'09, RFID'06]

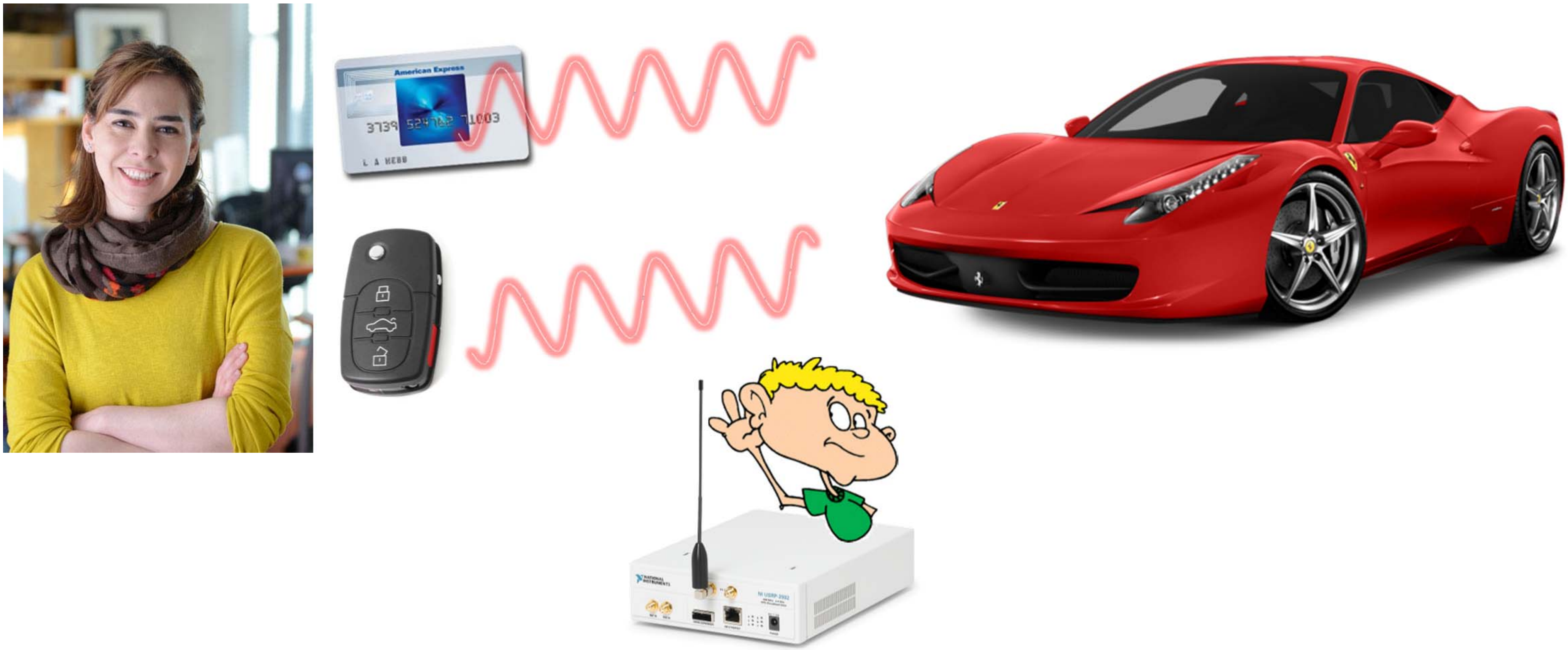
Anti-Theft Car Immobilizers
[Usenix'12, Usenix'05]

Public Transportation
[Defcon'08, MIT'08, S&P'09]

Hacking RFIDs for Dummies



Hacking RFIDs Simply By Eavesdropping



RFIDs adopt weak encryption protocols

Hacking RFIDs Simply By Eavesdropping

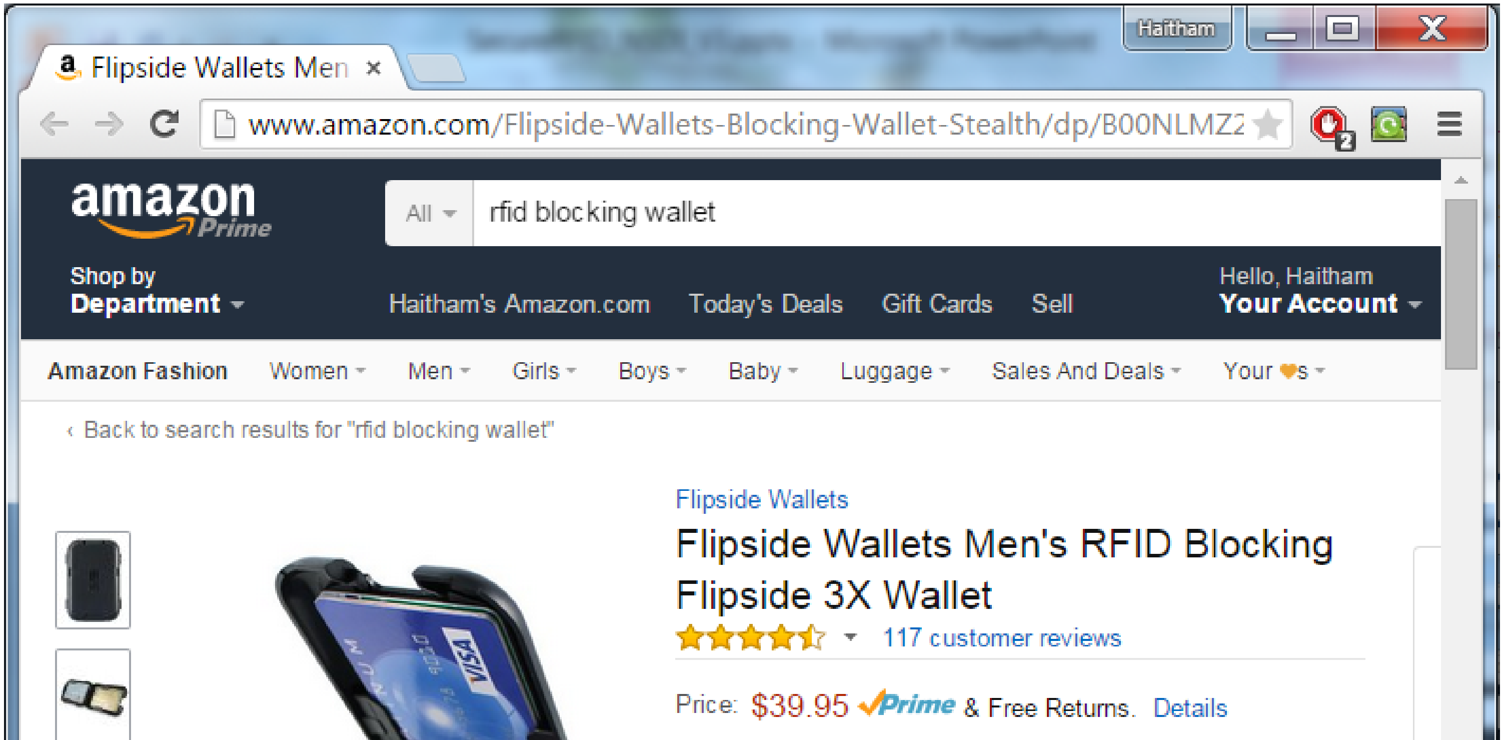
RFIDs adopt weak encryption protocols

⬇

Goal of RFID Industry: Dramatically reduce the power, size, and cost of RFIDs

Protect your RFID cards against active attacks

Protect your RFID cards against active attacks



Most attacks demonstrated by eavesdropping

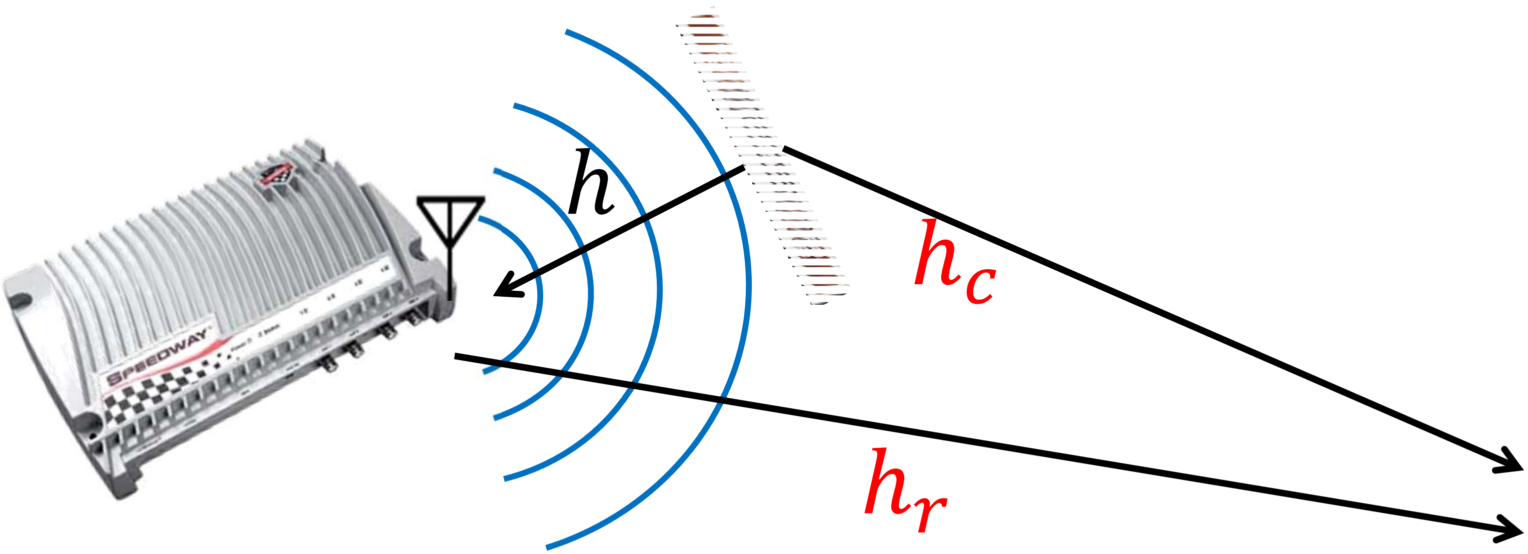
Need solution for eavesdropping that works with existing RFIDs

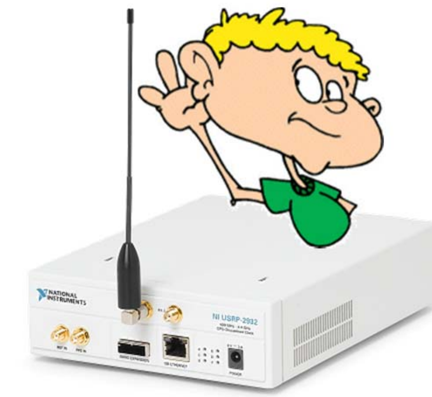
RF-Cloak

System that protects RFIDs against eavesdropping attacks

- Does not require any modification to the RFID cards
- Protects against a wide range of attackers including multi-antenna MIMO eavesdroppers
- Theoretically proven the security guarantees
- Implemented the system and empirically demonstrated its benefits

RFID Communication





Reader transmits constant waveform: C

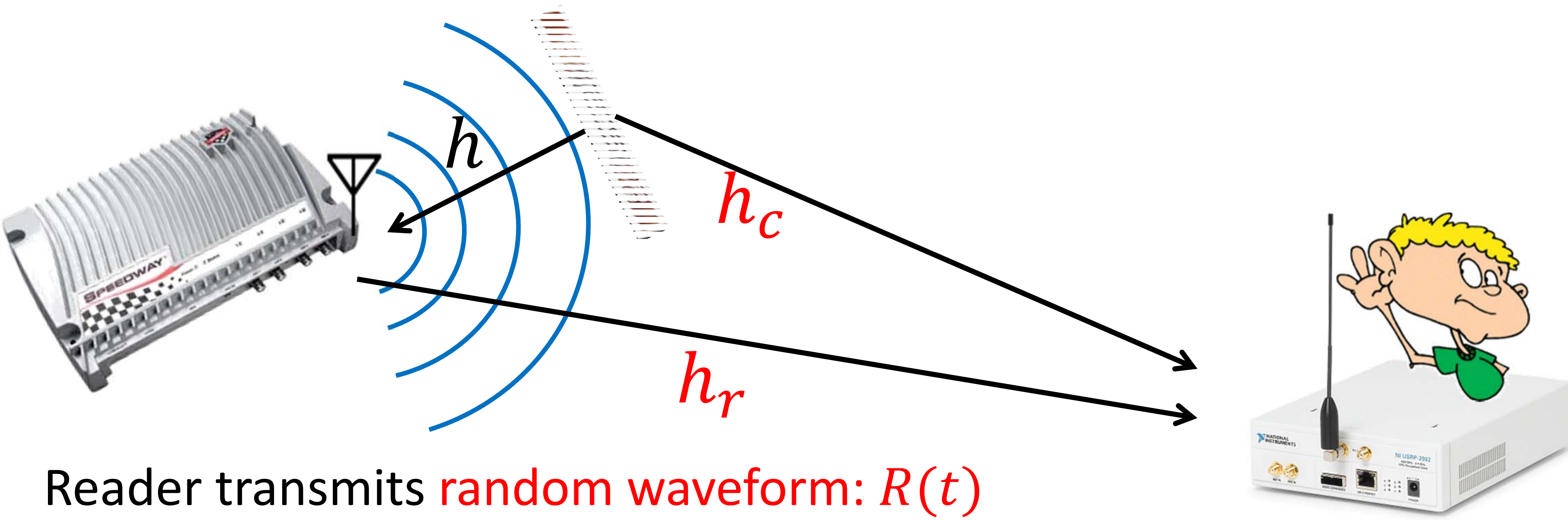
RFID reflects the reader’s signal using ON-OFF switch

Reader receives (full-duplex) : $h \times C \times bits$

Eavesdropper receives: $h_r \times C + h_c \times C \times bits$

Replace constant waveform C with a random waveform $R(t)$

RF-Cloak Solution



Reader transmits random waveform: $R(t)$

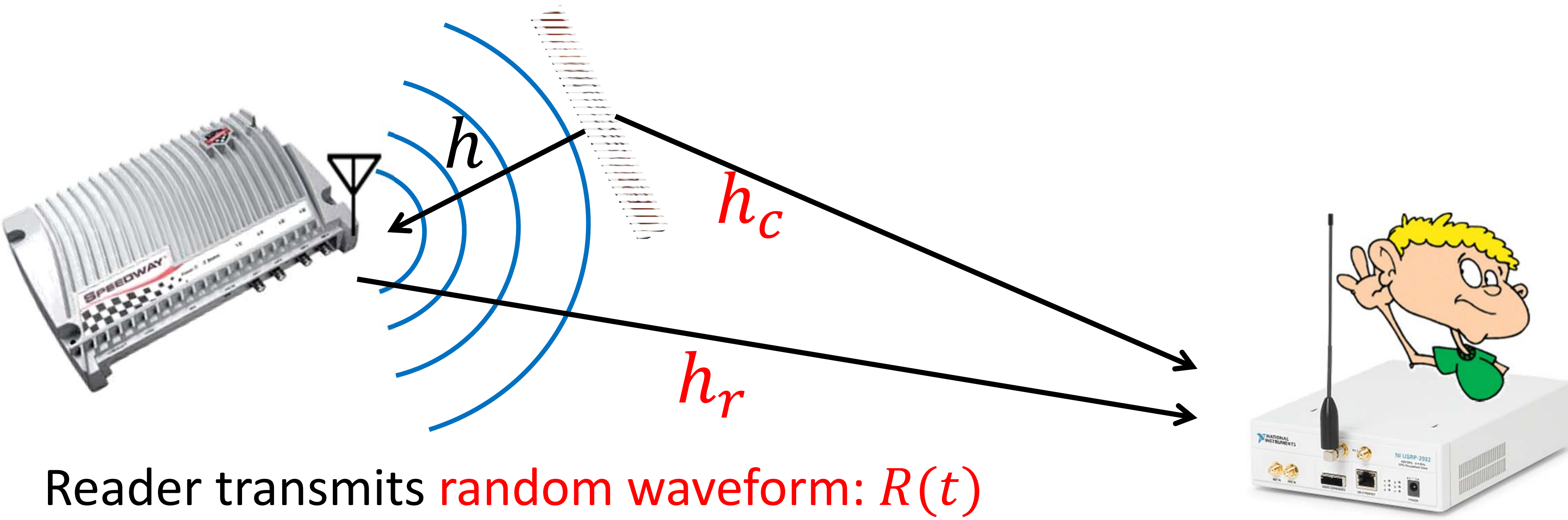
RFID reflects the reader's signal using ON-OFF switch

Reader receives (full-duplex): $h \times R(t) \times bits$

Eavesdropper receives: $h_r \times R(t) + h_c \times R(t) \times bits$

Replace constant waveform C with a random waveform $R(t)$

RF-Cloak Solution



Reader transmits random waveform: $R(t)$

RFID reflects the reader's signal using ON-OFF switch

Reader receives (full-duplex): $h \times R(t) \times bits$

Eavesdropper receives: $h_r \times R(t) + h_c \times R(t) \times bits$

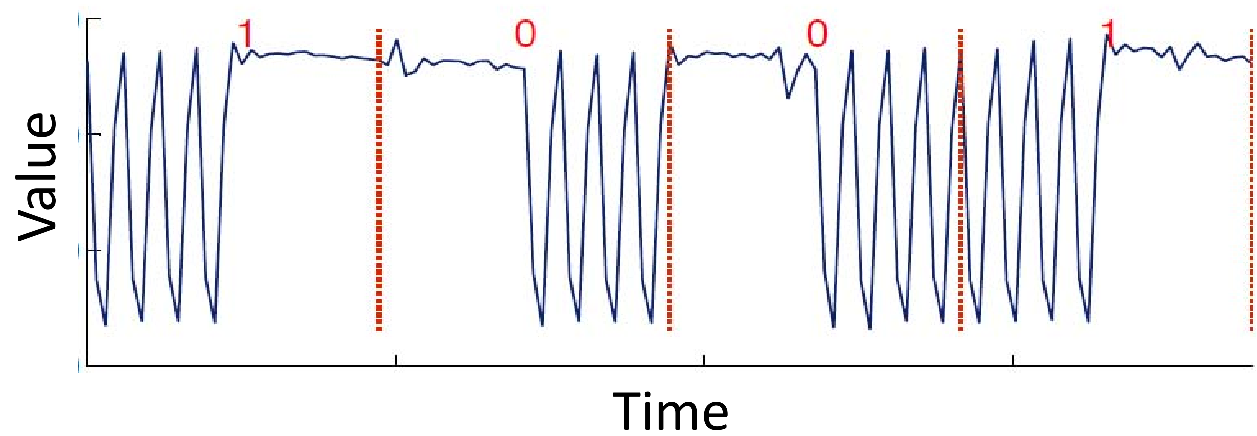
Reader knows $R(t)$ → Can decode

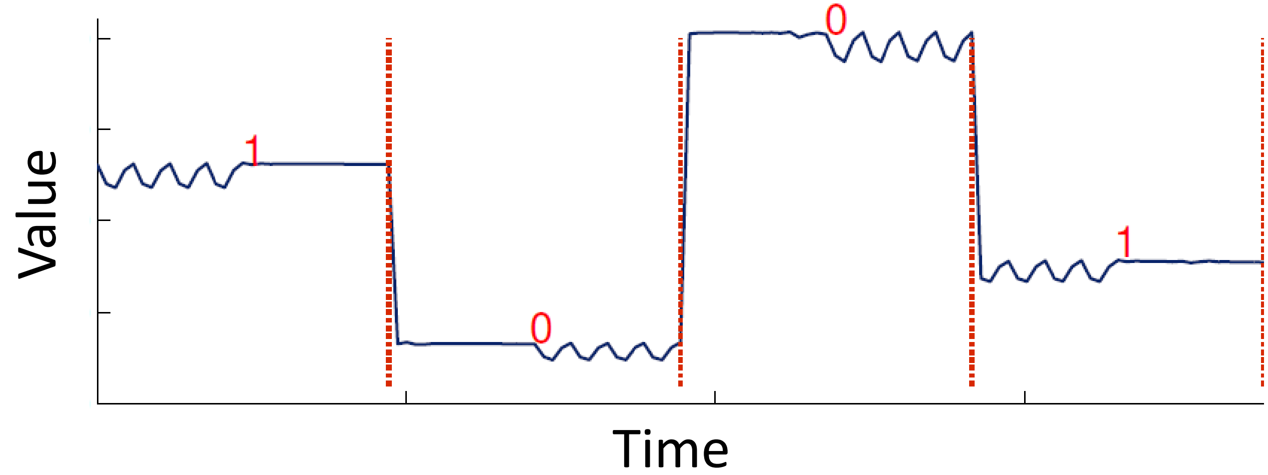
Eavesdropper doesn't know $R(t)$ → Cannot decode

RF-Cloak: Randomizing the Reader's Signal

- Random waveform acts like a one-time pad on the air
  - → Naïve solution: Multiply each bit with random number

RFID Signal:



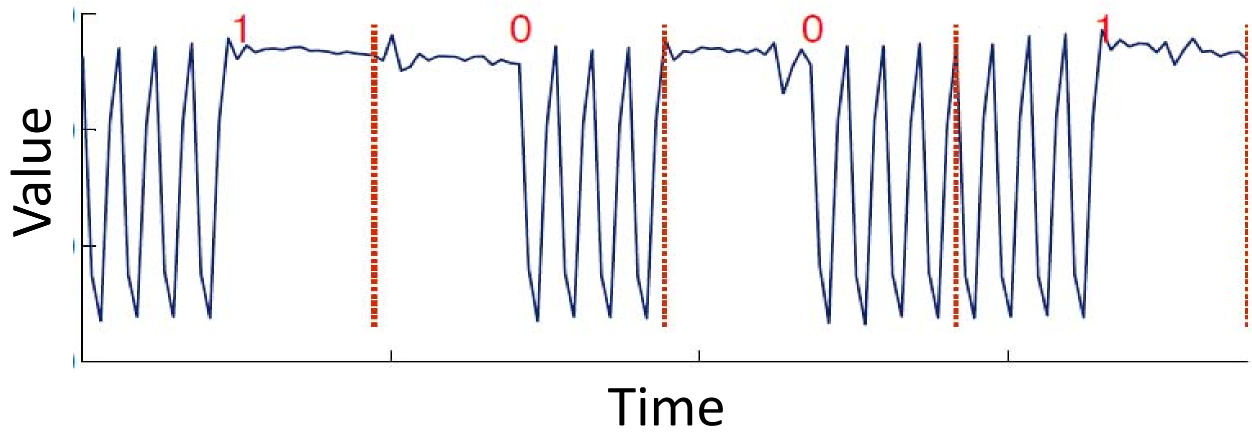


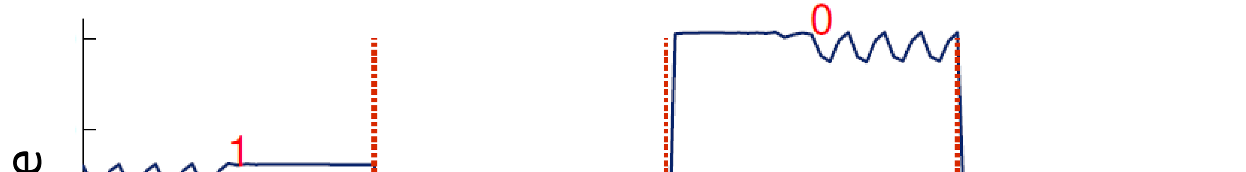
RF-Cloak: Randomizing the Reader's Signal

- Random waveform acts like a one-time pad on the air

  → Naïve solution: Multiply each bit with random number

RFID Signal:



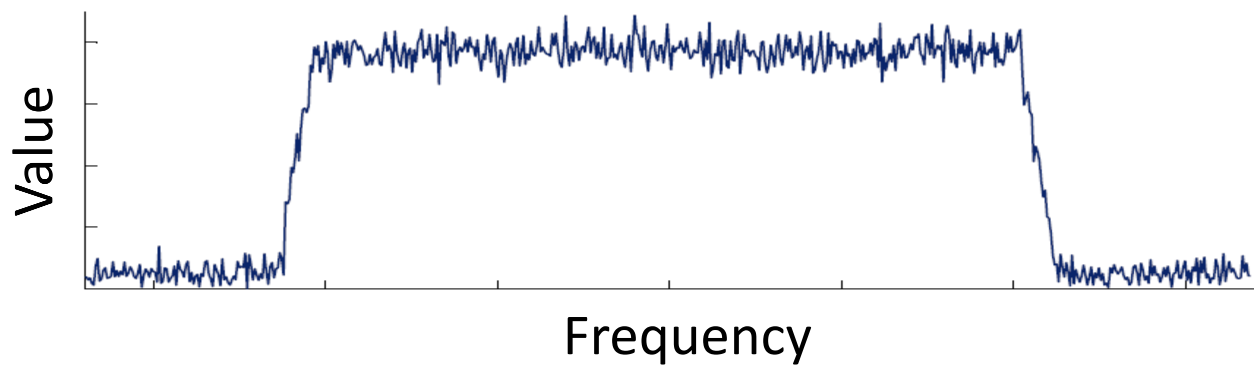


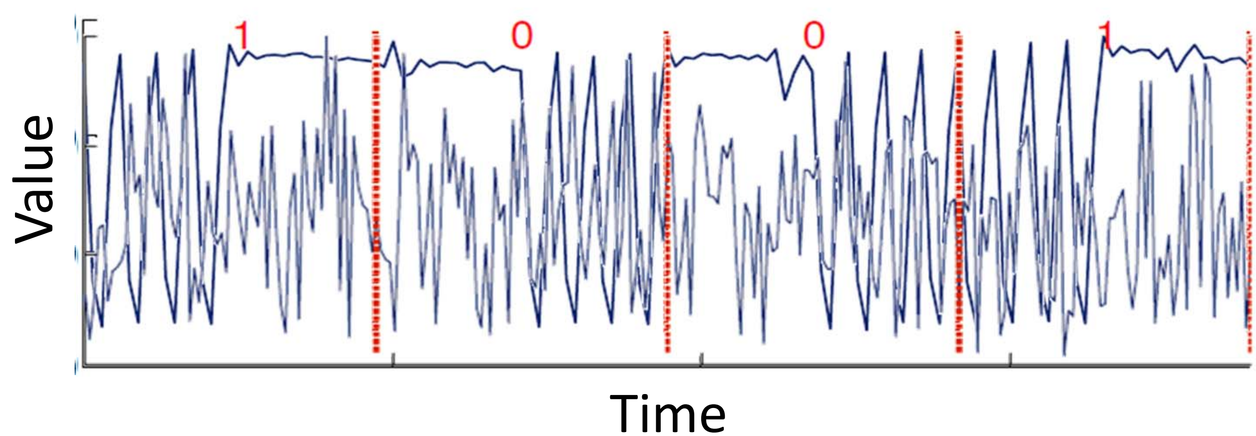
Random waveform must destroy internal signal patterns of the bits

RF-Cloak: Randomizing the Reader's Signal

Random waveform:

- Must change as fast as any transition in the RFID signal
  → has same bandwidth as RFID signal
- Must be indistinguishable from white noise i.e. flat frequency profile
  → samples taken from complex Gaussians





RF-Cloak: Randomizing the Reader's Signal

Threat model:

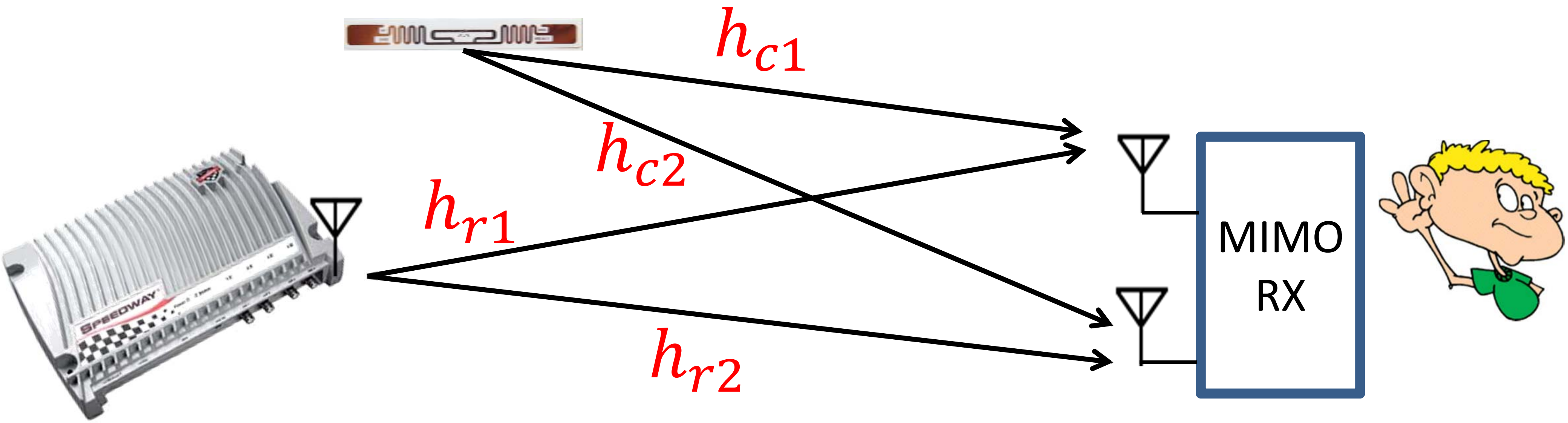
Single antenna eavesdropper using the optimal decoder

Guarantee: (informally restated)

Theorem 1: Using RF-Cloak's random signal $R(t)$*, an eavesdropper will not be able to distinguish a 0 bit from a 1 bit which is no better than a random guess*

What if the attacker has multi-antenna MIMO capability?

MIMO Eavesdropper



Reader transmits random waveform: $R(t)$

Eavesdropper receives:

1st receiver: $Y_1(t) = h_{r1} \times \cancel{R(t)} + h_{c1} \times \cancel{R(t)} \times bits$

2nd receiver: $Y_2(t) = h_{r2} \times \cancel{R(t)} + h_{c2} \times \cancel{R(t)} \times bits$

$$\frac{Y_1(t)}{Y_2(t)} = \frac{h_{r1} + h_{c1} \times bits}{h_{r2} + h_{c2} \times bits}$$

MIMO Eavesdropper

MIMO Eavesdropper can eliminate the random waveform and decode the RFID bits.

Reader transmits random waveform: $R(t)$

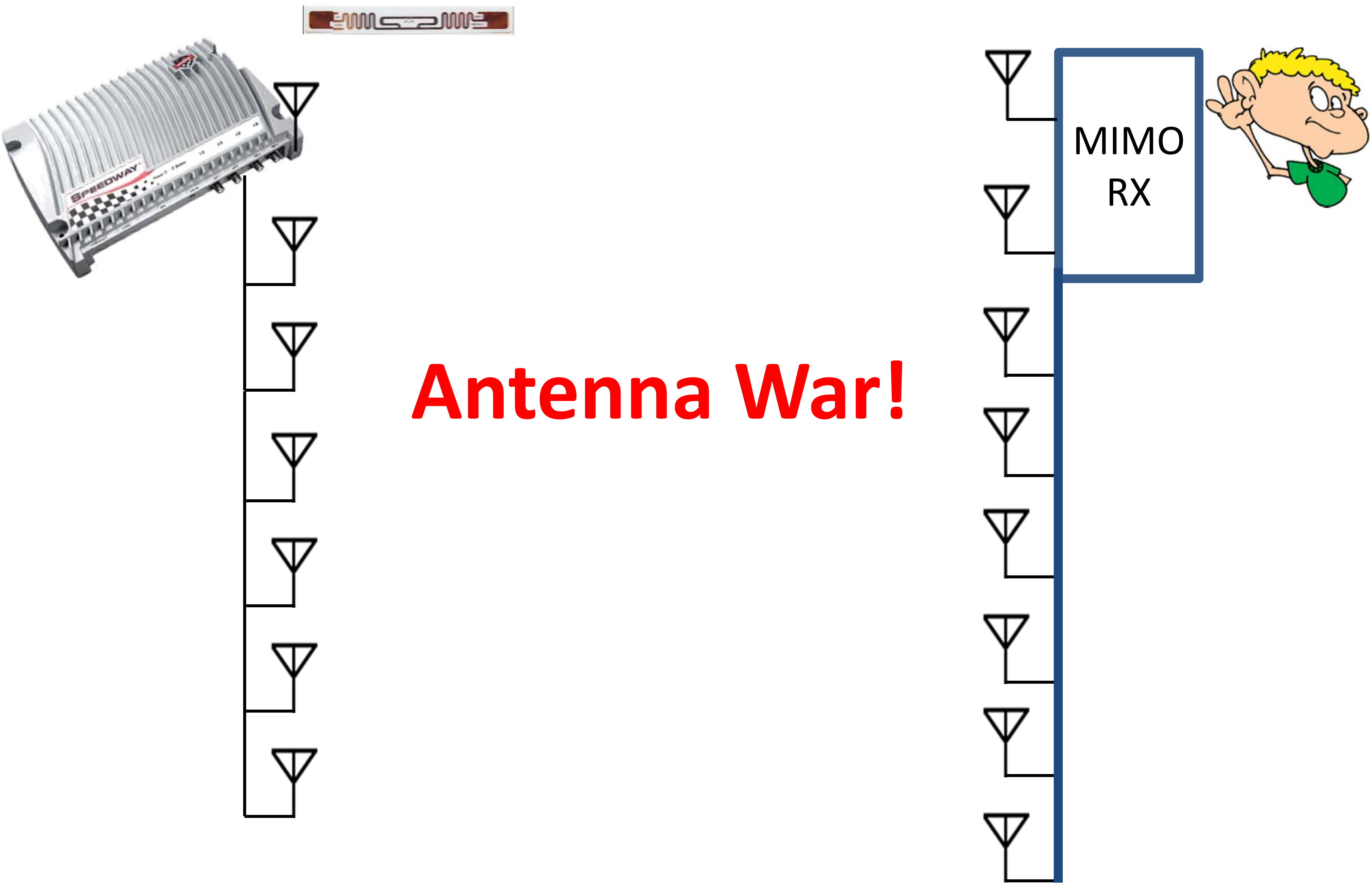
Eavesdropper receives:

1st receiver: $Y_1(t) = h_{r1} \times \cancel{R(t)} + h_{c1} \times \cancel{R(t)} \times bits$

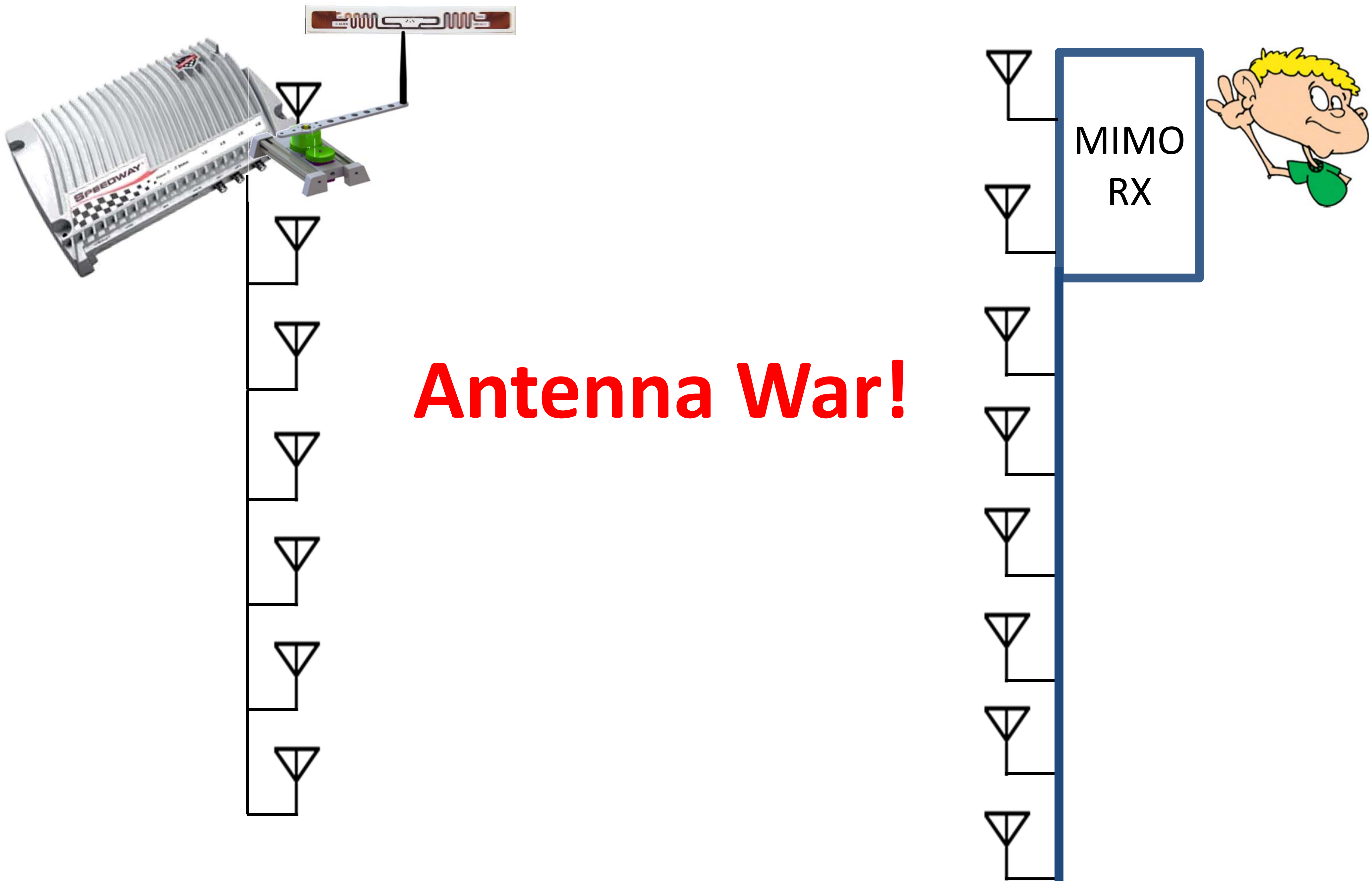
2nd receiver: $Y_2(t) = h_{r2} \times \cancel{R(t)} + h_{c2} \times \cancel{R(t)} \times bits$

$$\frac{Y_1(t)}{Y_2(t)} = \frac{h_{r1} + h_{c1} \times bits}{h_{r2} + h_{c2} \times bits}$$

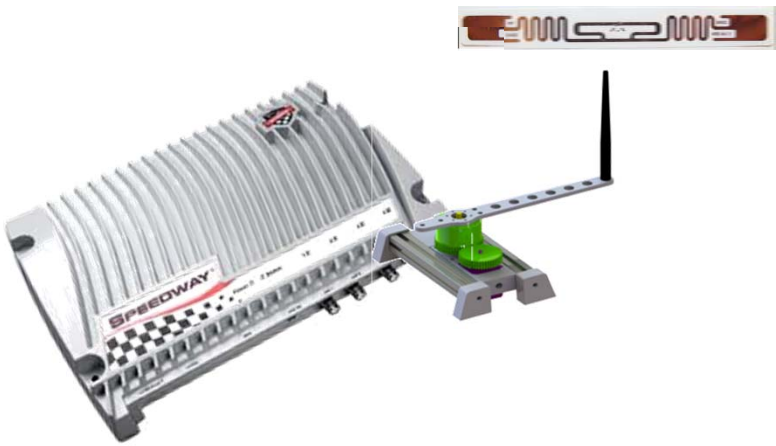
RF-Cloak vs MIMO Eavesdropper

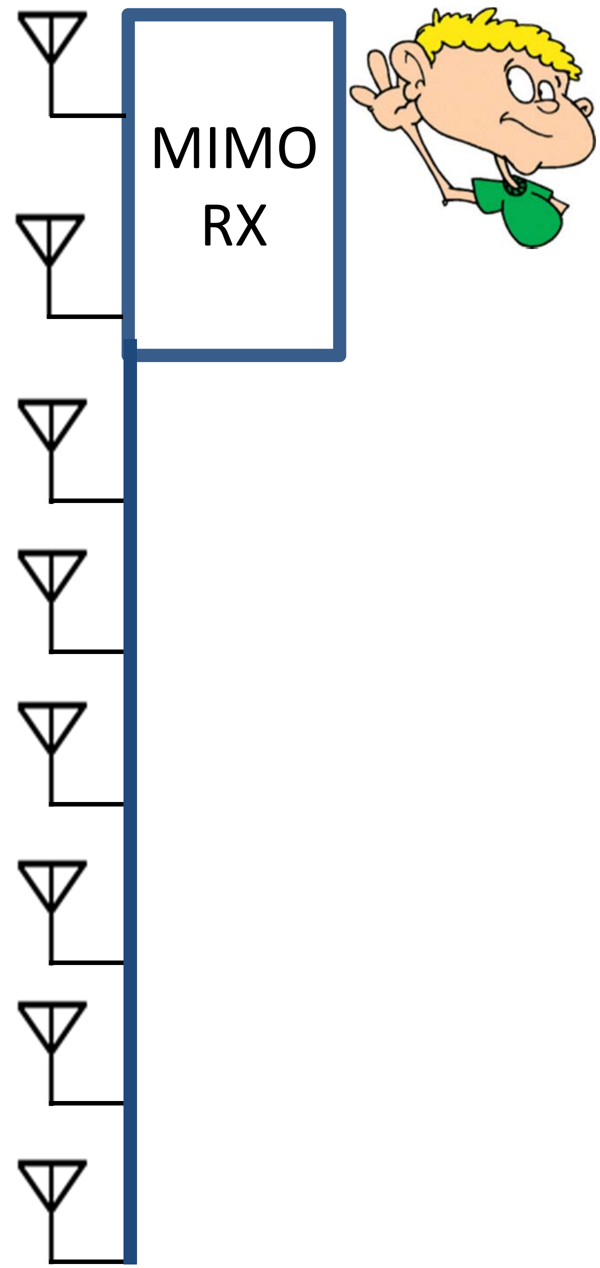


RF-Cloak vs MIMO Eavesdropper



RF-Cloak vs MIMO Eavesdropper

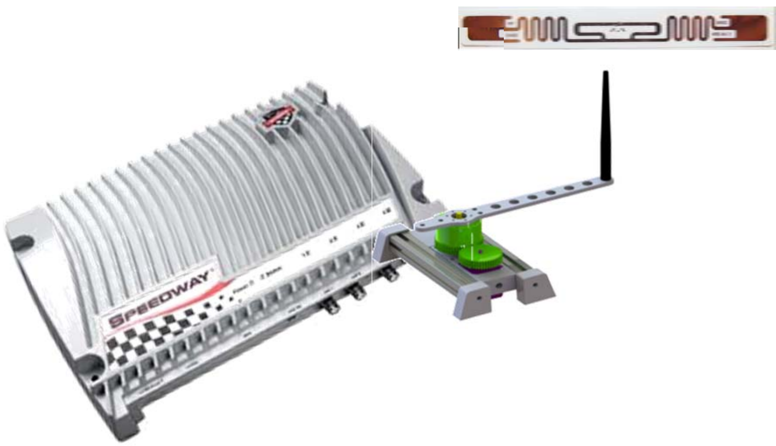




RF-Cloak combines antenna motion and rapid antenna switching

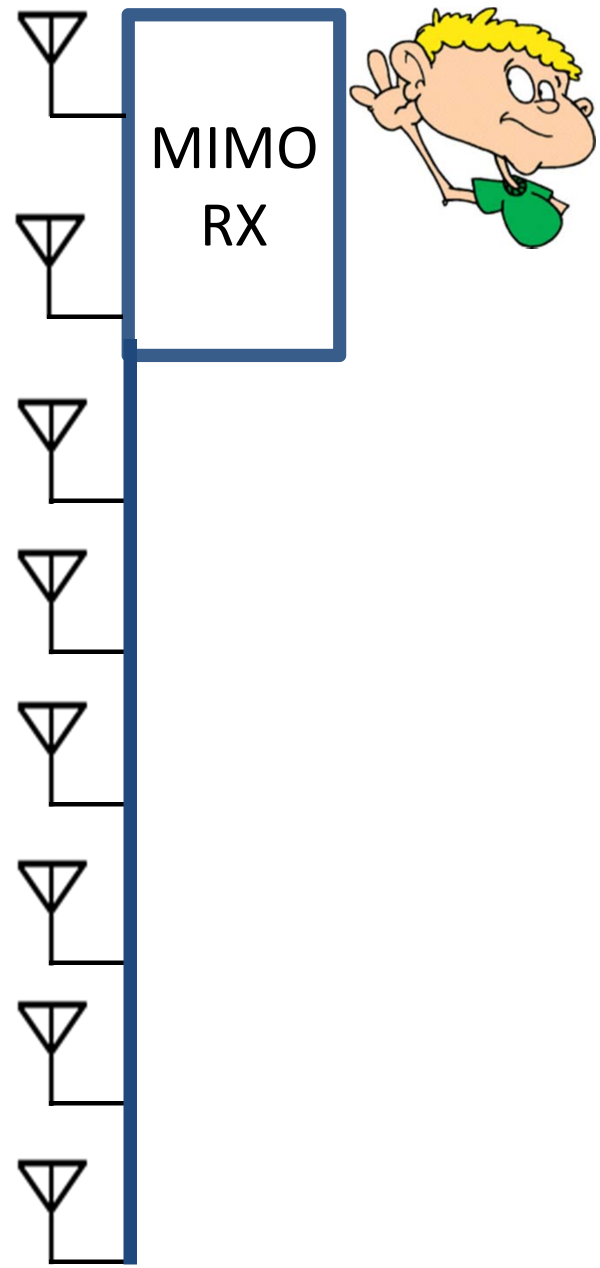
→ Emulate a very large number of fast changing antennas

RF-Cloak vs MIMO Eavesdropper



- Channels to eavesdropper change very fast → Cannot separate RFID signal from Reader signal
→ Cannot decode

- Reader (full duplex) → Only receives reflection from RFID
→ Can decode



RF-Cloak: Randomizing the Wireless Channel

Threat model:

Multi-antenna MIMO eavesdropper using the optimal decoder.

Guarantee: (informally restated)

Theorem 2: Using RF-Cloak's channel randomization, a MIMO eavesdropper will not be able to distinguish a 0 bit from a 1 bit which is no better than a random guess

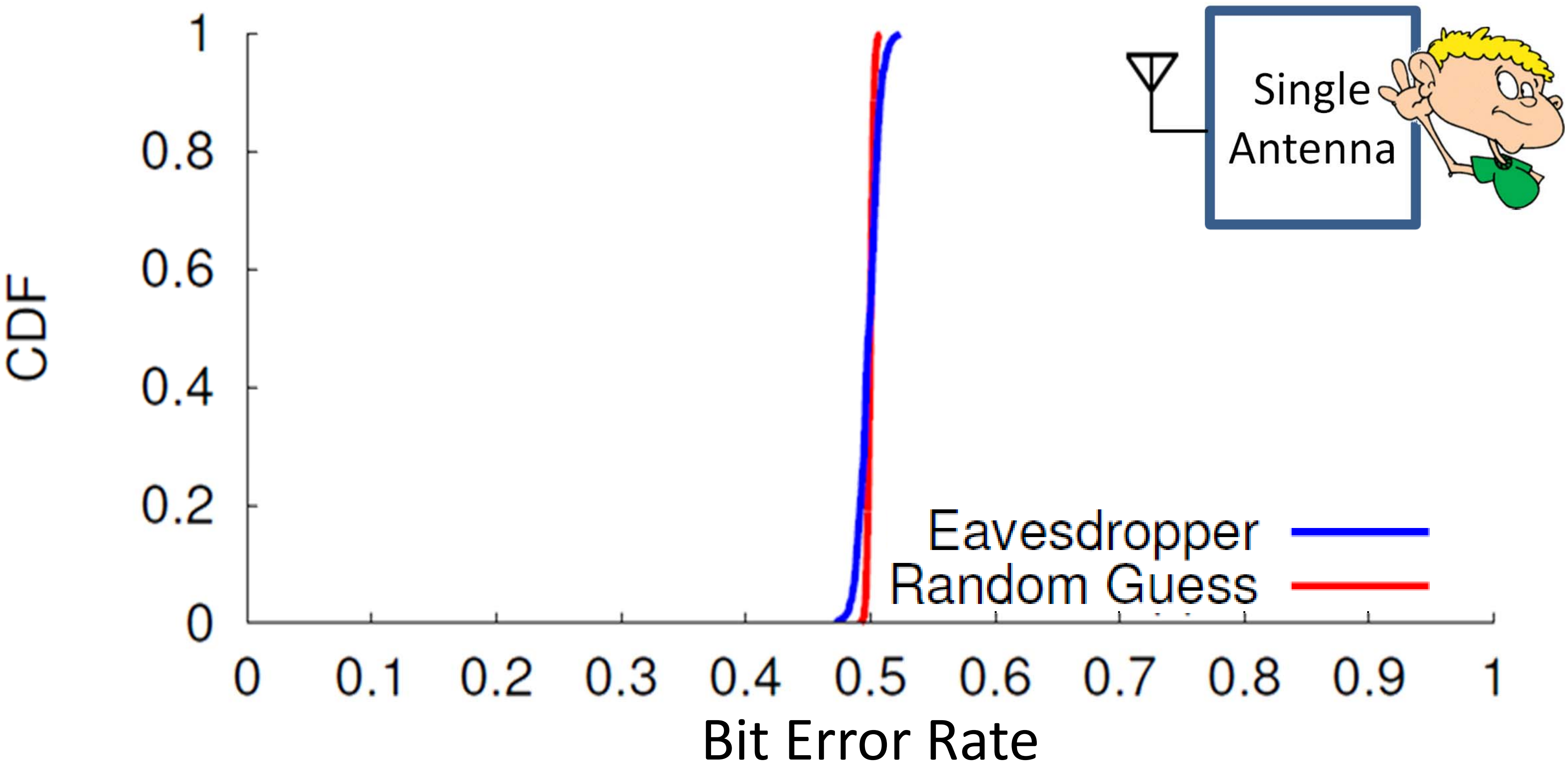
Evaluation

- Implemented RF-Cloak on USRP N210 software radios and combined it with a 1725 rpm motor and ADG904R RF switches.

- Evaluated it against different types of commercial RFID cards

- Evaluation metric : Bit error rate (BER)

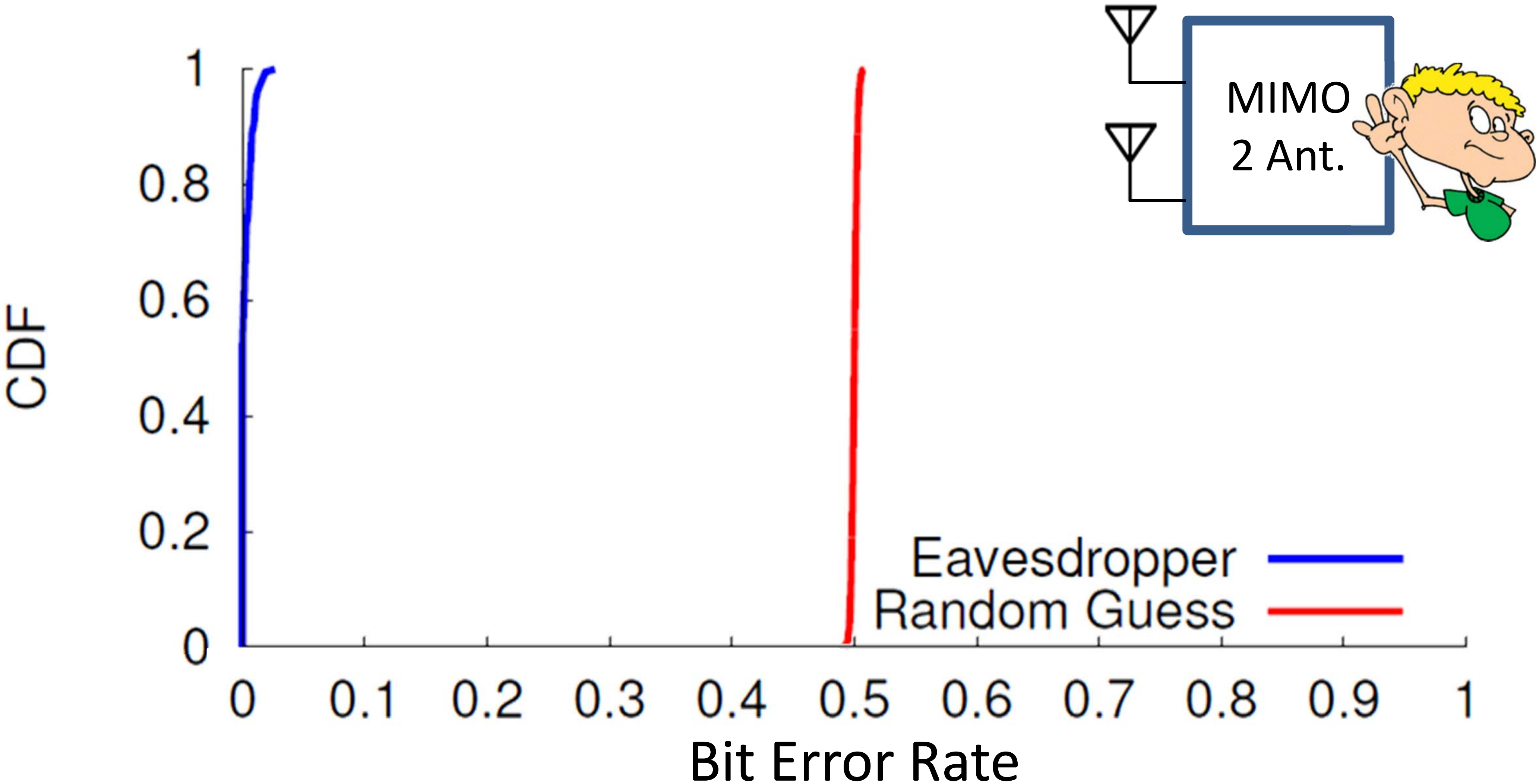
RF-Cloak Random Waveform vs Single Antenna Eavesdropper



Eavesdropper has mean BER of 0.498 with std. dev. 0.008

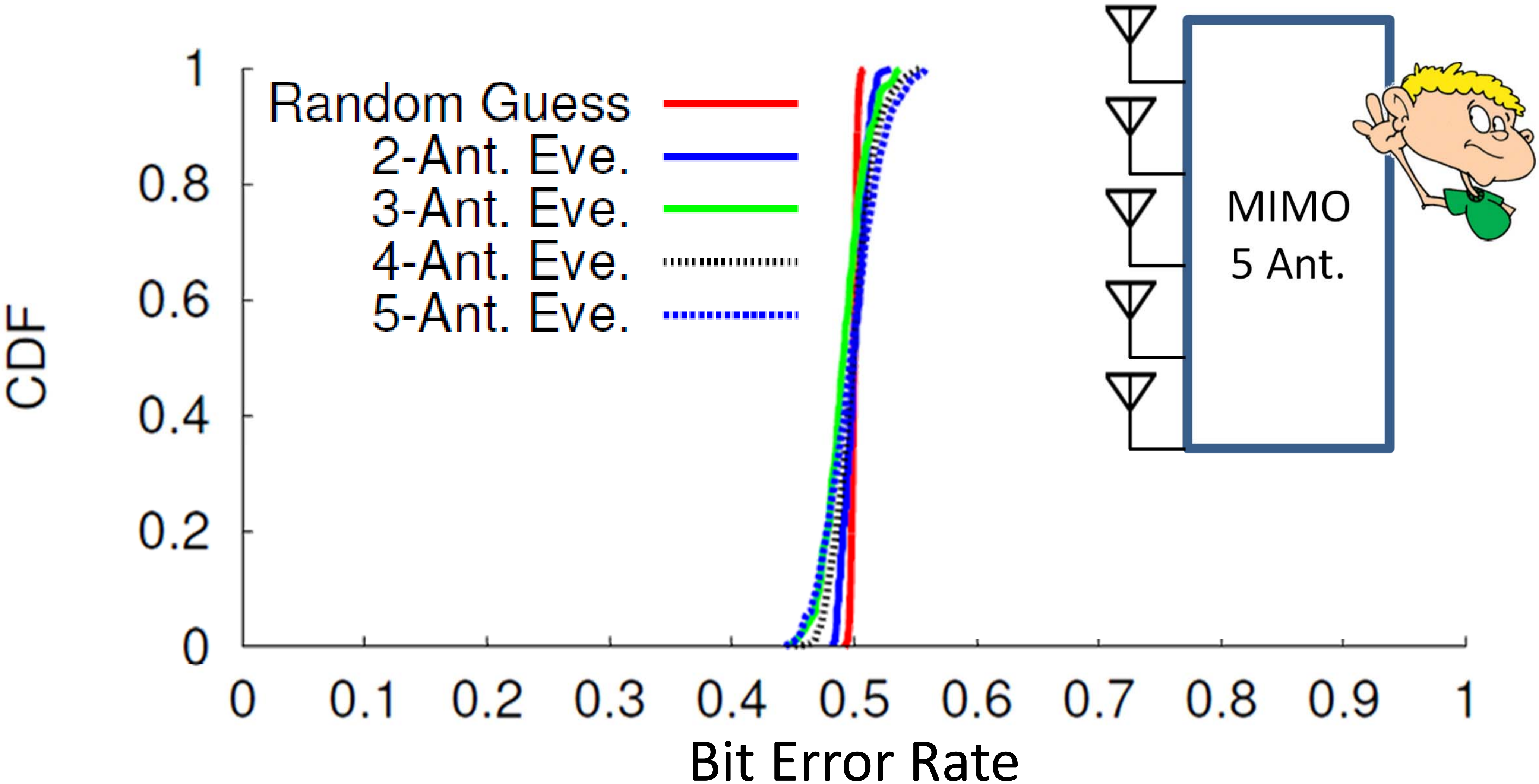
→ Very close to a random guess

RF-Cloak Random Waveform vs Two Antenna MIMO Eavesdropper



A two-antenna MIMO eavesdropper can correctly decode the RFID bits

RF-Cloak Channel Randomization vs MIMO Eavesdropper



RF-Cloak can prevent a MIMO eavesdropper from decoding the RFID's data

Related Work

- **Physical layer security:**
  [JCM’07, TCOM’13, SIGCOMM’11, Oakland’13, ICC’12, INFOCOM’11, MobiSys’13, SIGCOMM’13, MobiSys’14]

- **Securing RFIDs against eavesdropping:**
  [CHES’07, RFIDSec’11, CARDIS’06, JRSC’12, PerCom’07]

- **Moving antennas:**
  [SIGCOMM’14, MOBICOM’14, HOTNETS’14, MOBICOM’13, SIGCOM’13, HotMobile’12, ISJ’14]

Conclusion

- RF-Cloak is the first system that can protect deployed RFIDs against eavesdropping without any modification to the RFID

- RF-Cloak is the first system that can hide the signal from MIMO attacker with many antennas even when the reader has no MIMO capability.

- RF-Cloak provides a defense in depth solution.