NICScatter: Backscatter as a Covert Channel in Mobile Devices

Zhice Yang[1,2], **Qianyi Huang**[2], Qian Zhang[2]

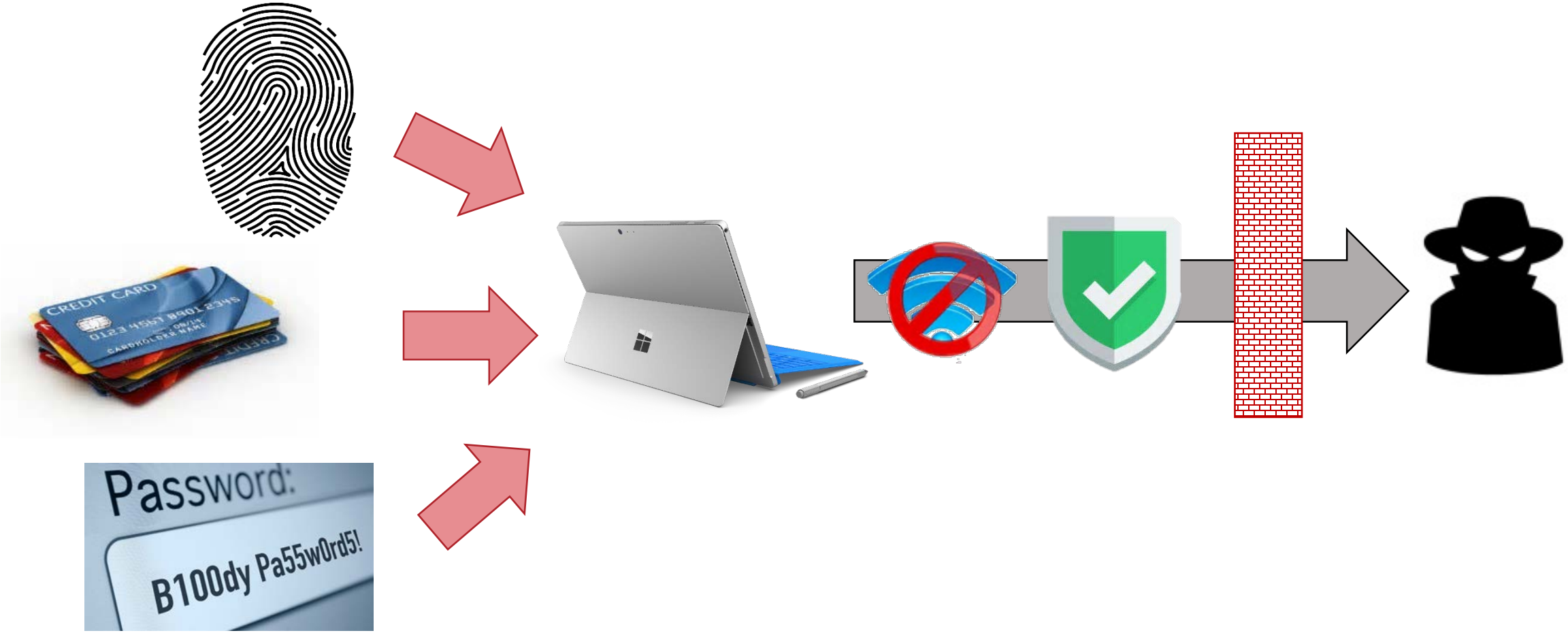
[1]SIST, ShanghaiTech University

[2]CSE, Hong Kong University of Science and Technology

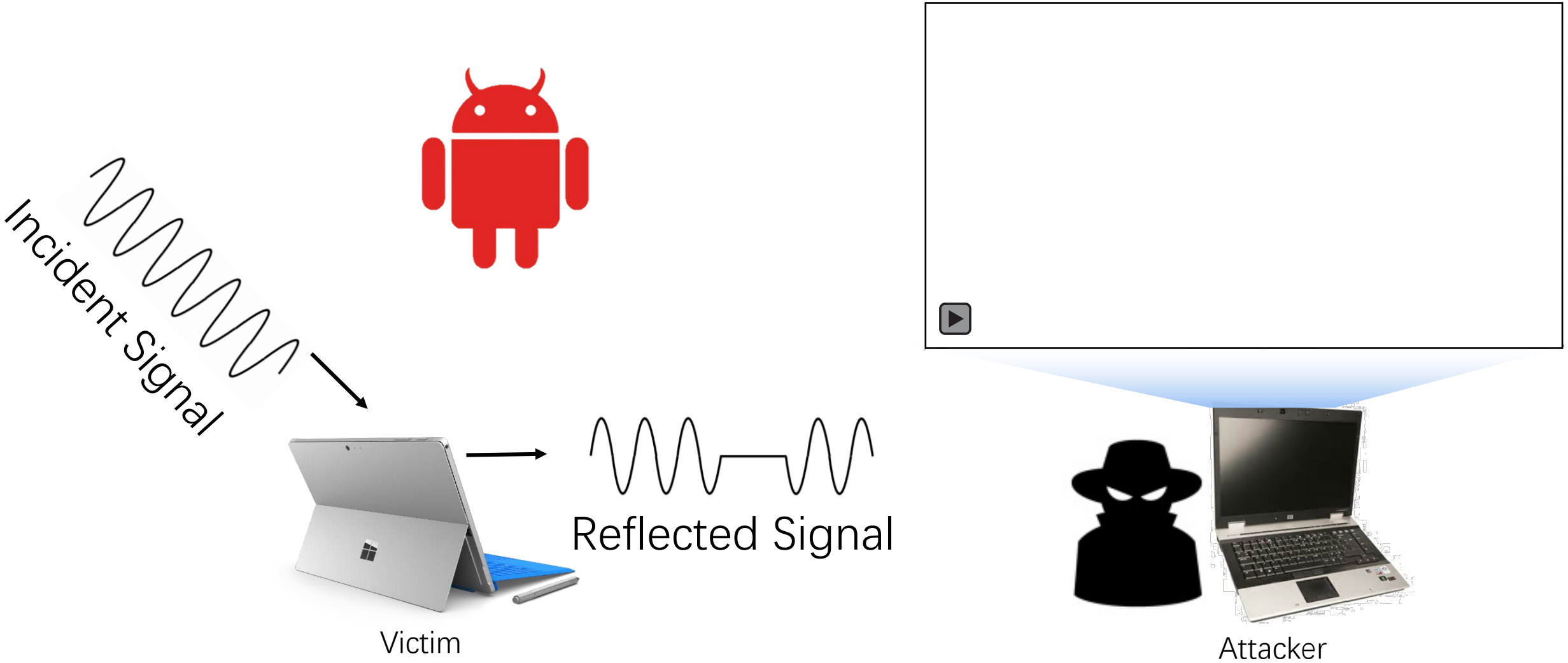
上海科技大学
ShanghaiTech University

香港科技大學
THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

Is Our Data Safe Enough ?



Information Leakage under Isolation

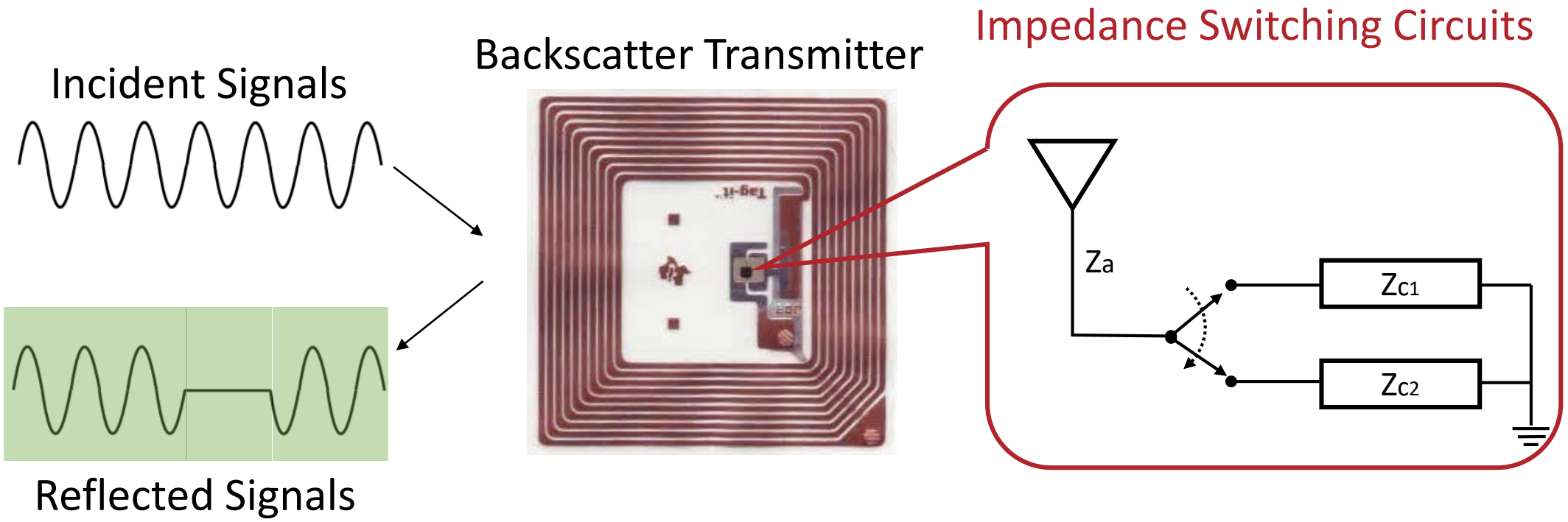


Covert Communication through Backscatter

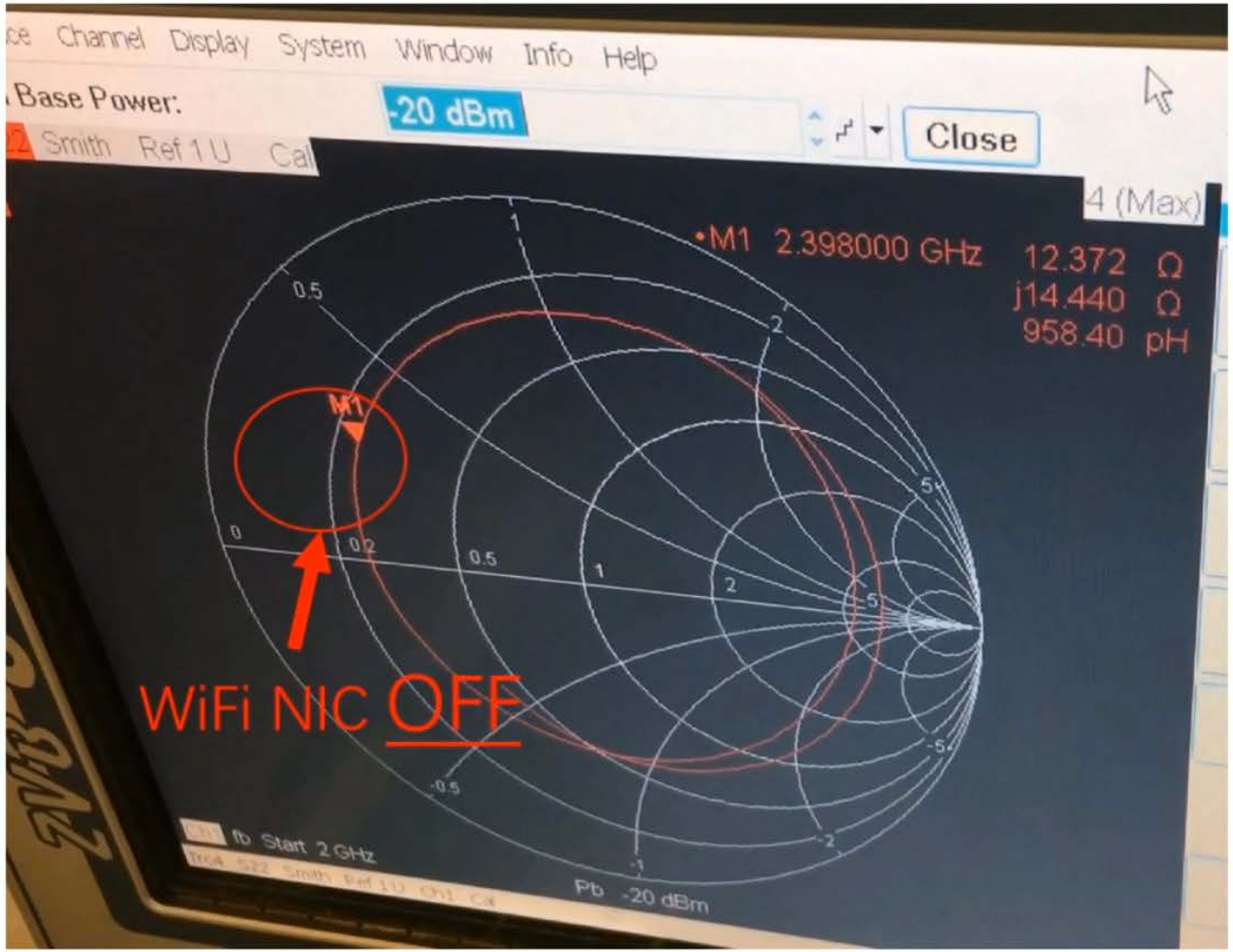
NICScatter: backscatter through commercial NICs

System vulnerabilities in smartphone and Linux notebook

Backscatter Basics



Backscatter through Commercial NICs

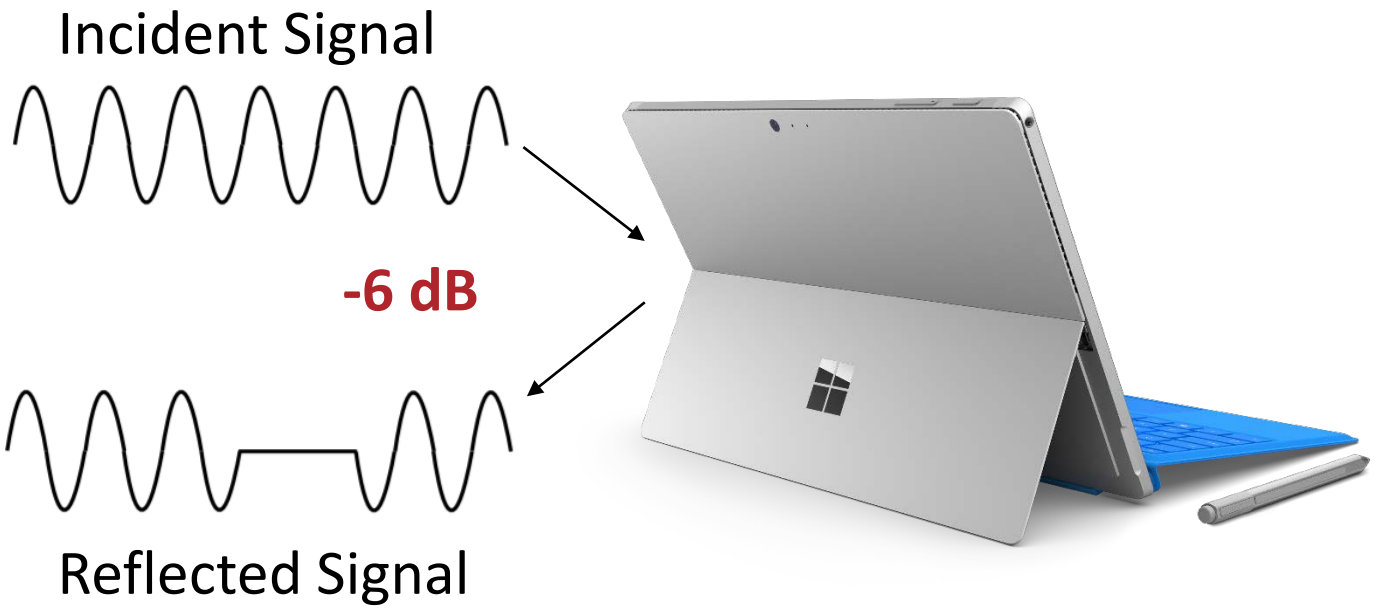


Vector Network Analyzer

BCM 1045 Wi-Fi NIC

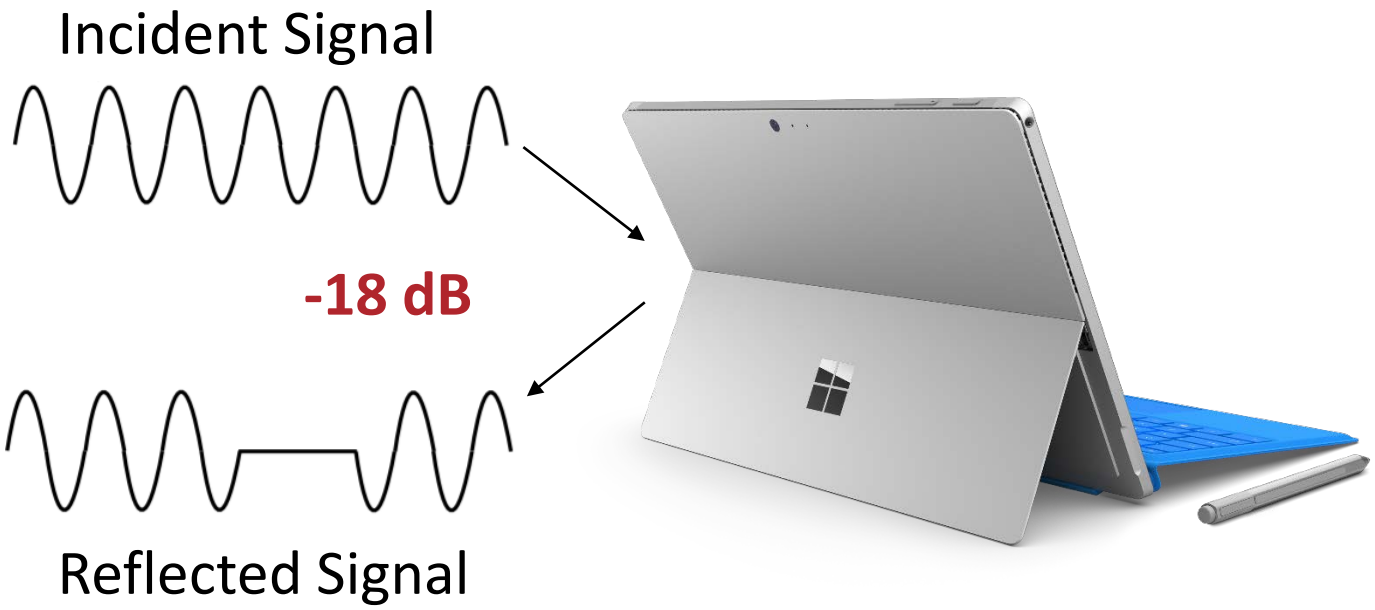
NICScatter Efficiency

Model	Off State	On State
BCM1045, ant1	12.4+j14.4	106.9-j9.8
Intel5300, ant1	119.0+j137.0	80.3+j66.8
Intel5300, ant2	54.3+j122.7	57.7+j78.4

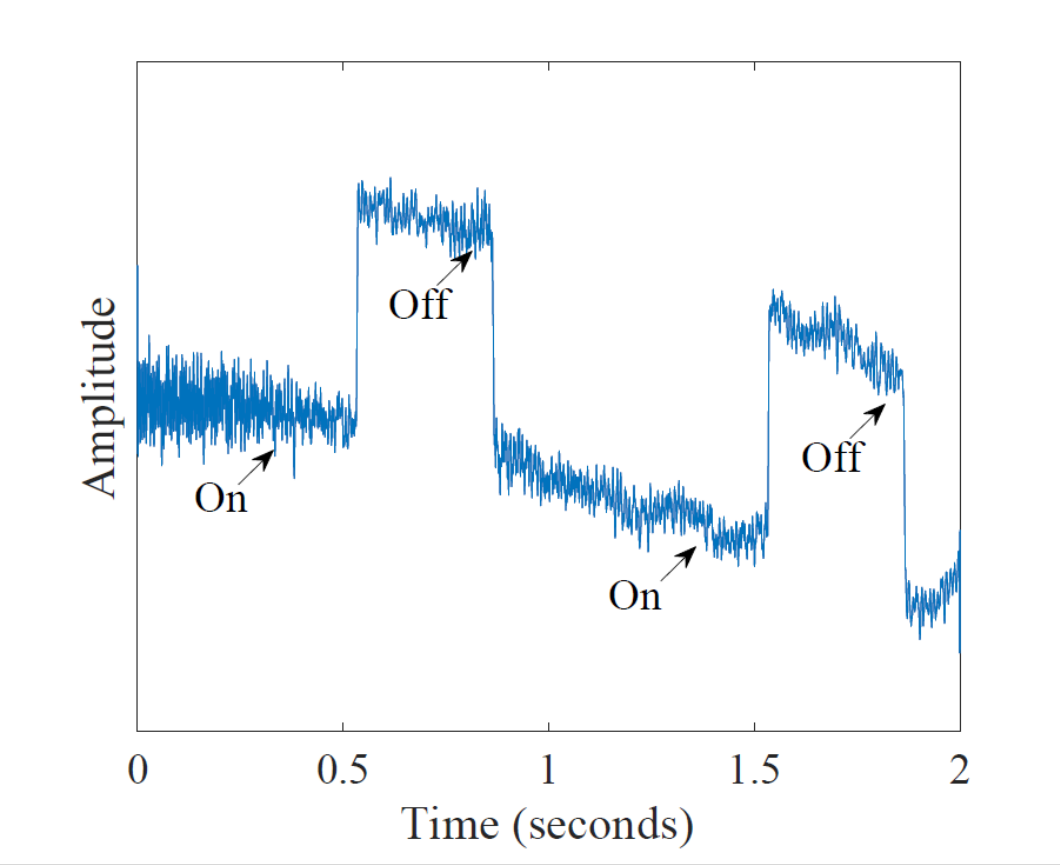


NICScatter Efficiency

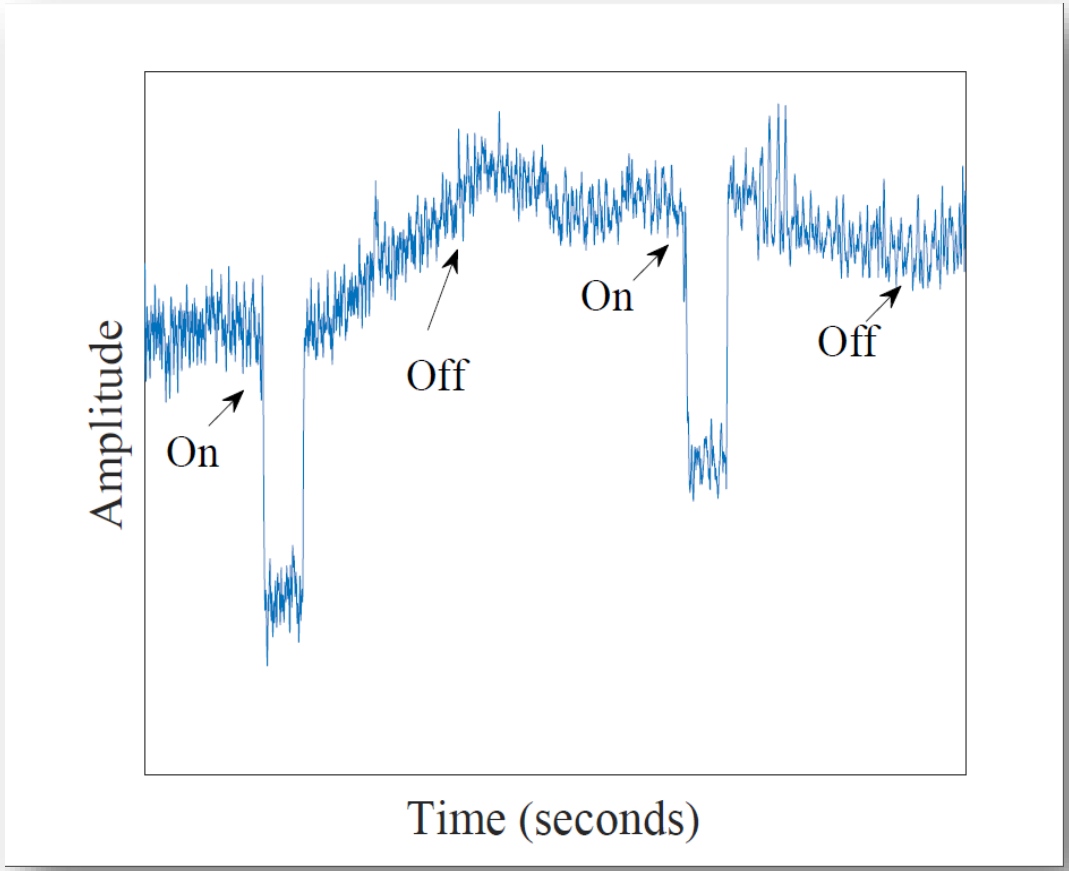
Model	Off State	On State
BCM1045, ant1	12.4+j14.4	106.9-j9.8
Intel5300, ant1	119.0+j137.0	80.3+j66.8
Intel5300, ant2	54.3+j122.7	57.7+j78.4



Reflection Diversities

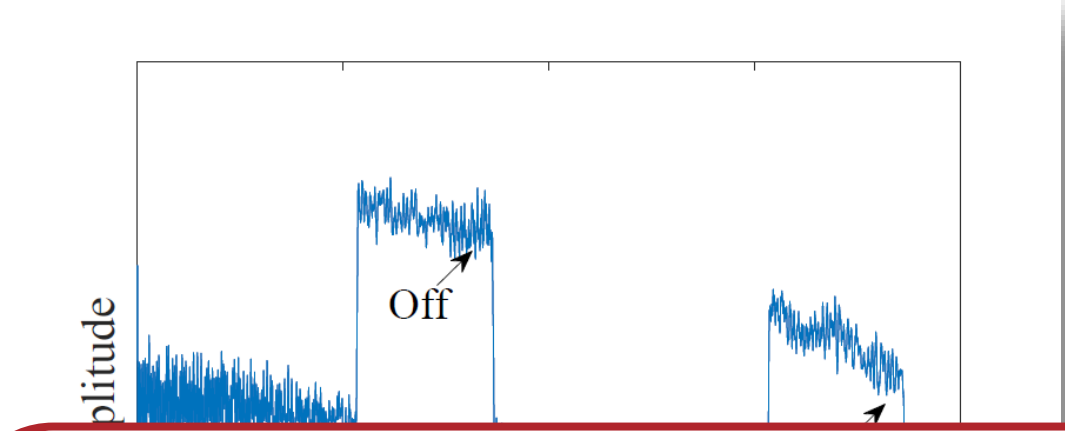


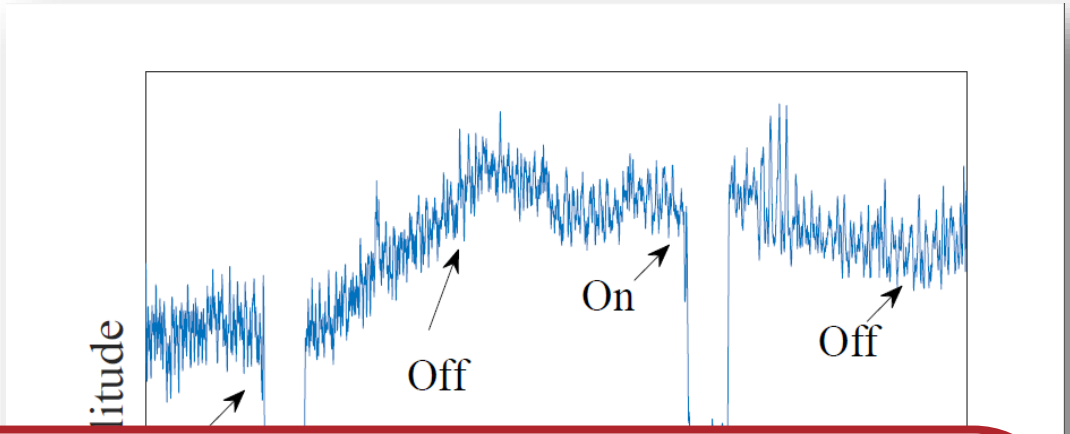
Intel 5300



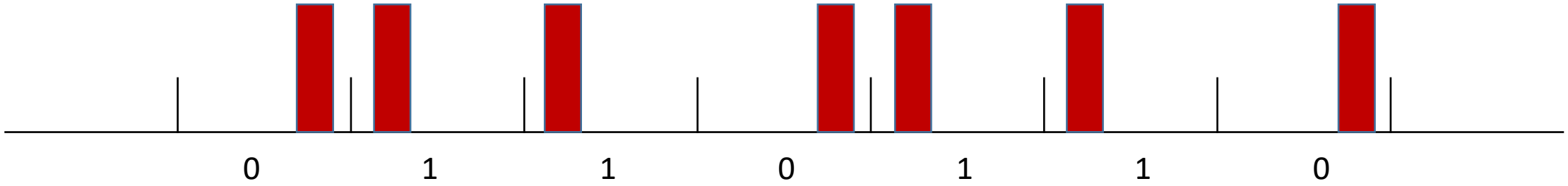
Atheros AR9285

Reflection Diversities

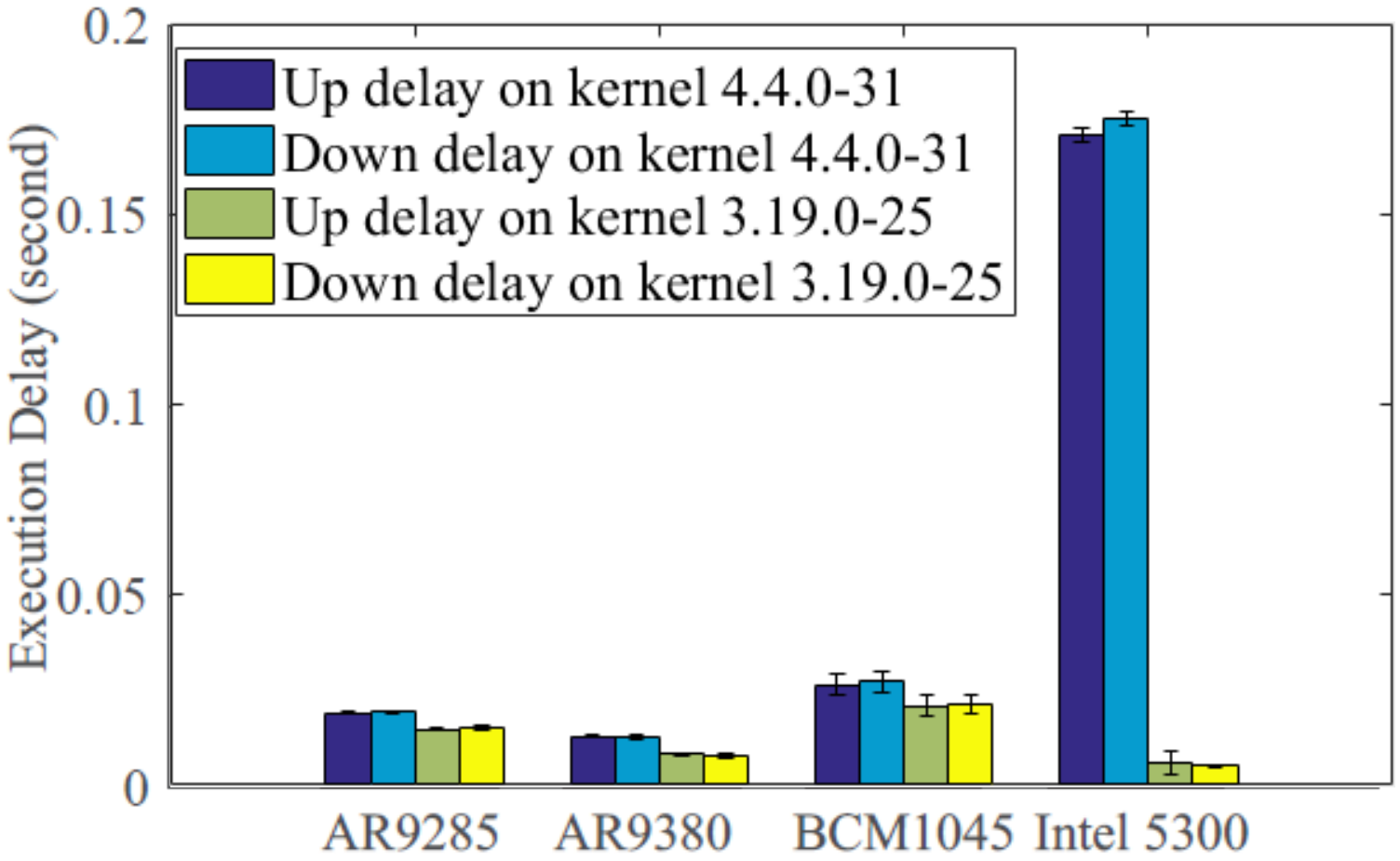




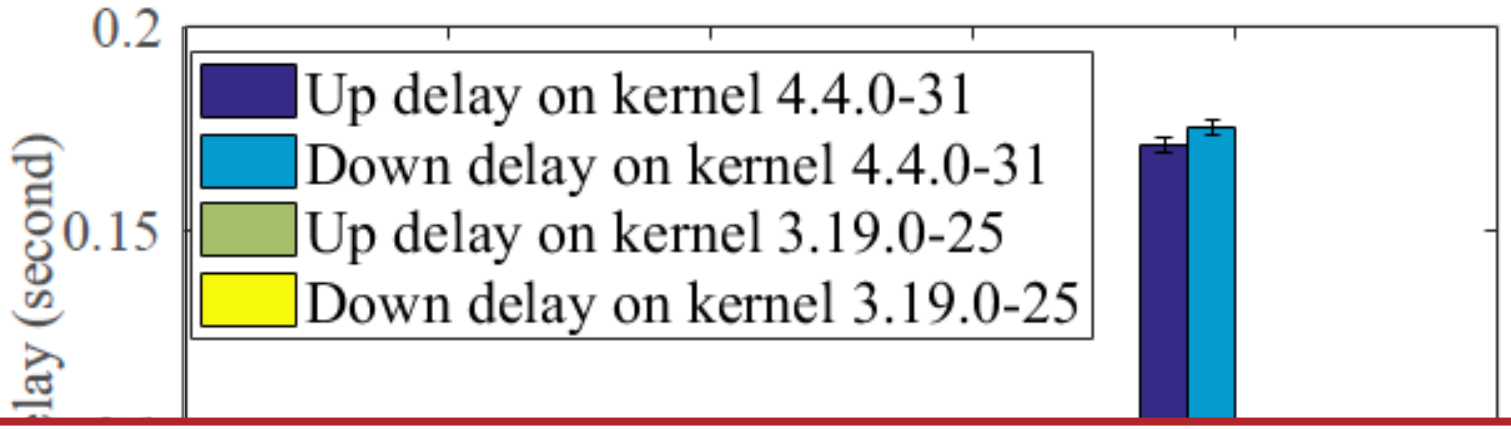
On Off Position Modulation (OOPM)



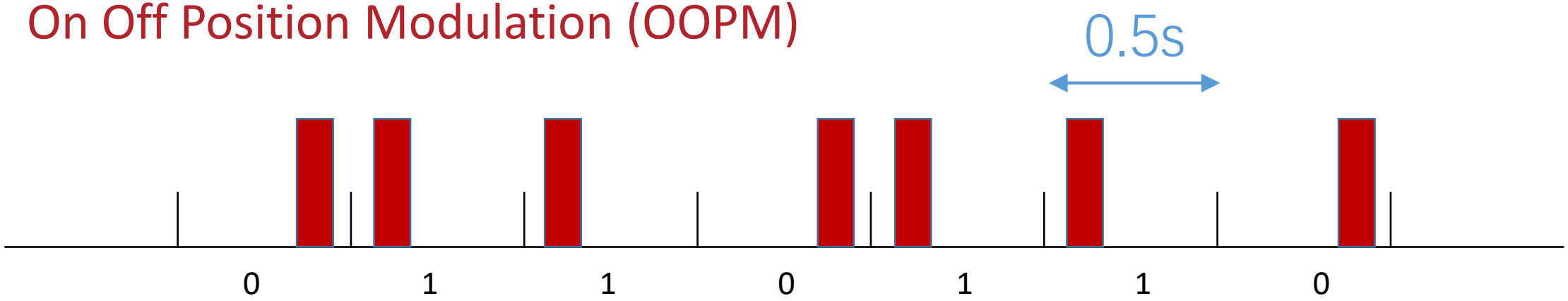
Latency Diversities



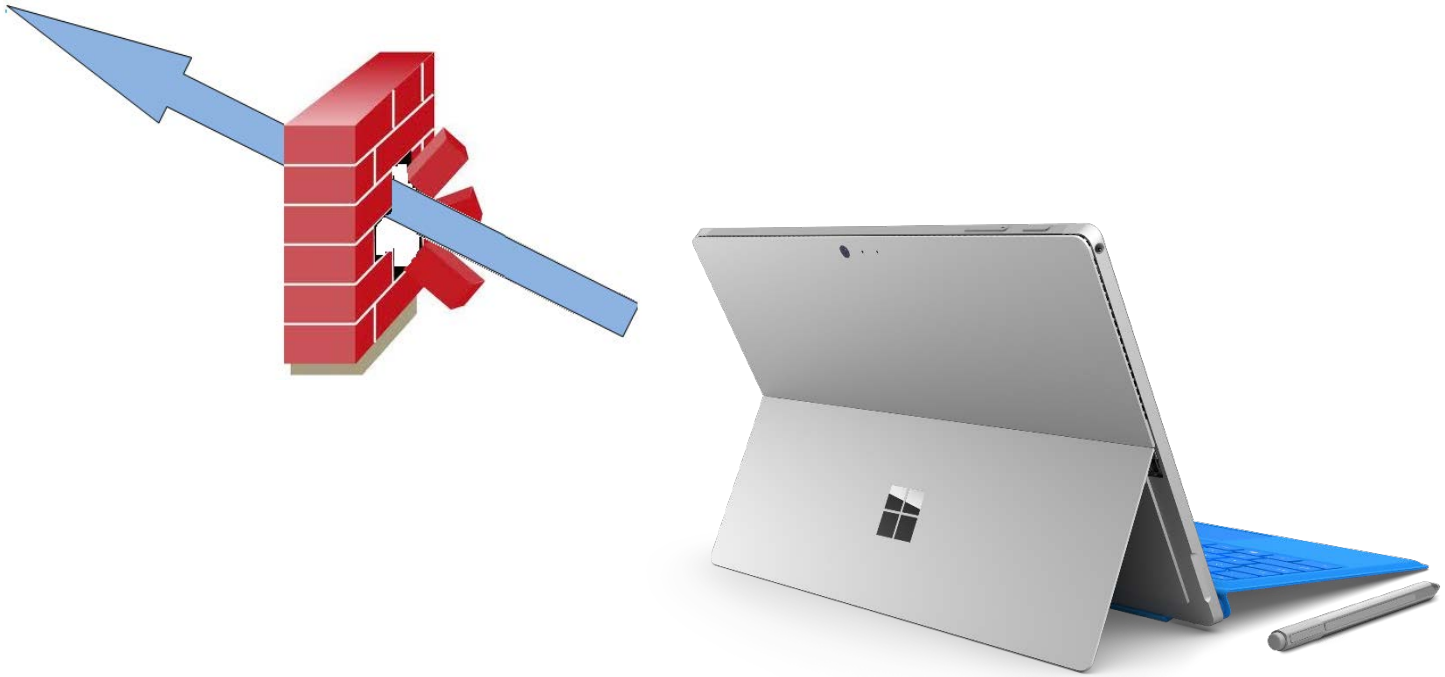
Latency Diversities



On Off Position Modulation (OOPM)

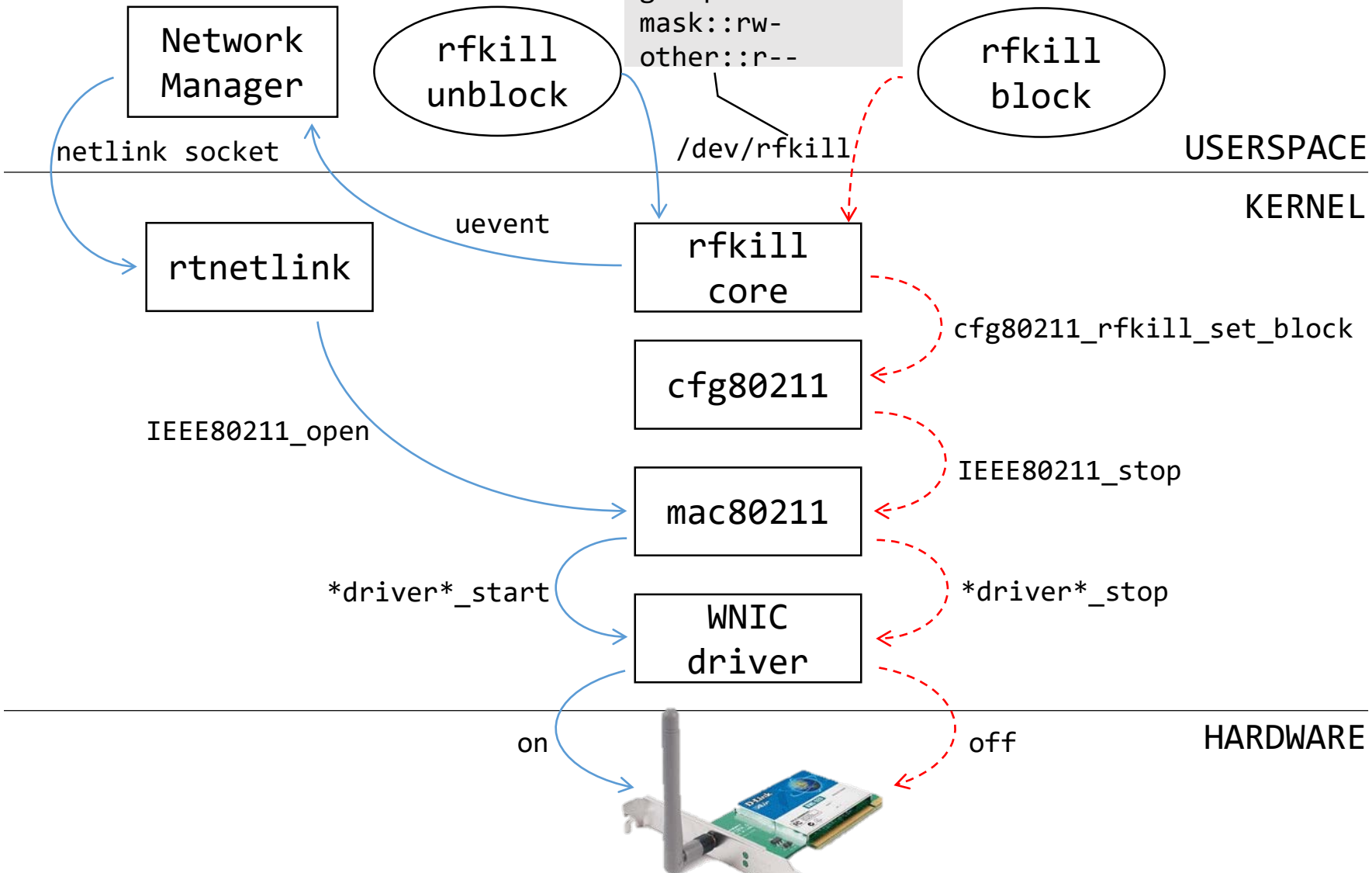


How to Hide the Communication ?



RFKILL tem

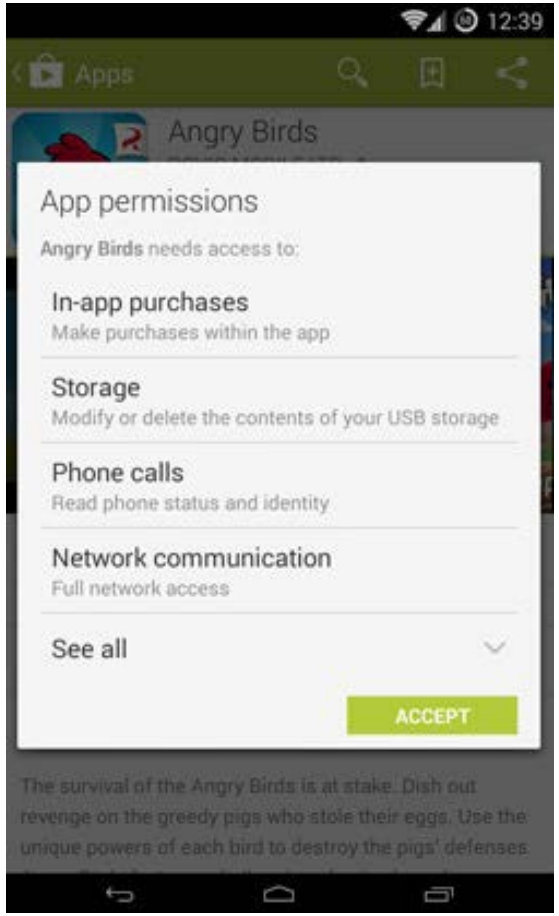
```
# file: rfkill
# owner: root
# group: netdev
user::rw-
user:testu:rw-
group::rw-
mask::rw-
other::r--
```



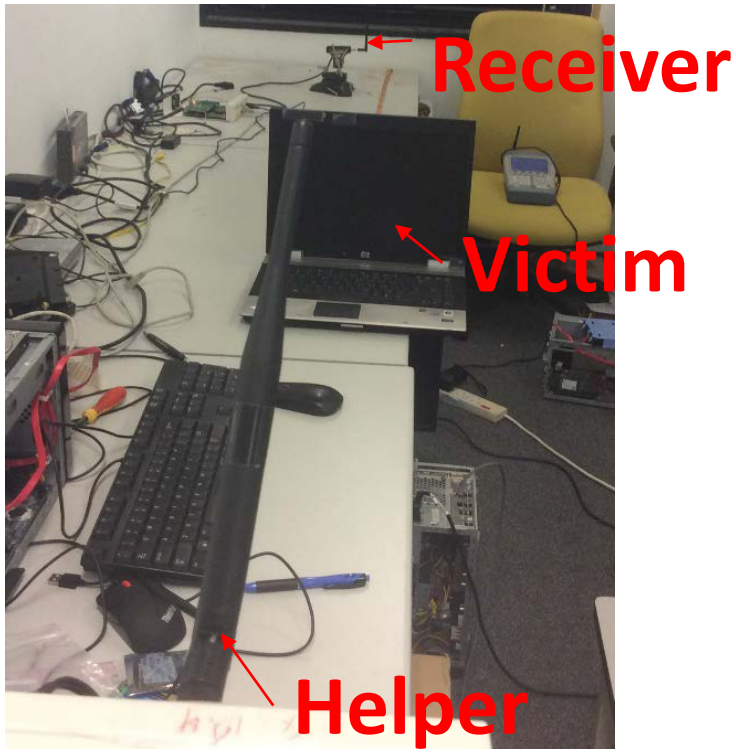
Android App Permissions

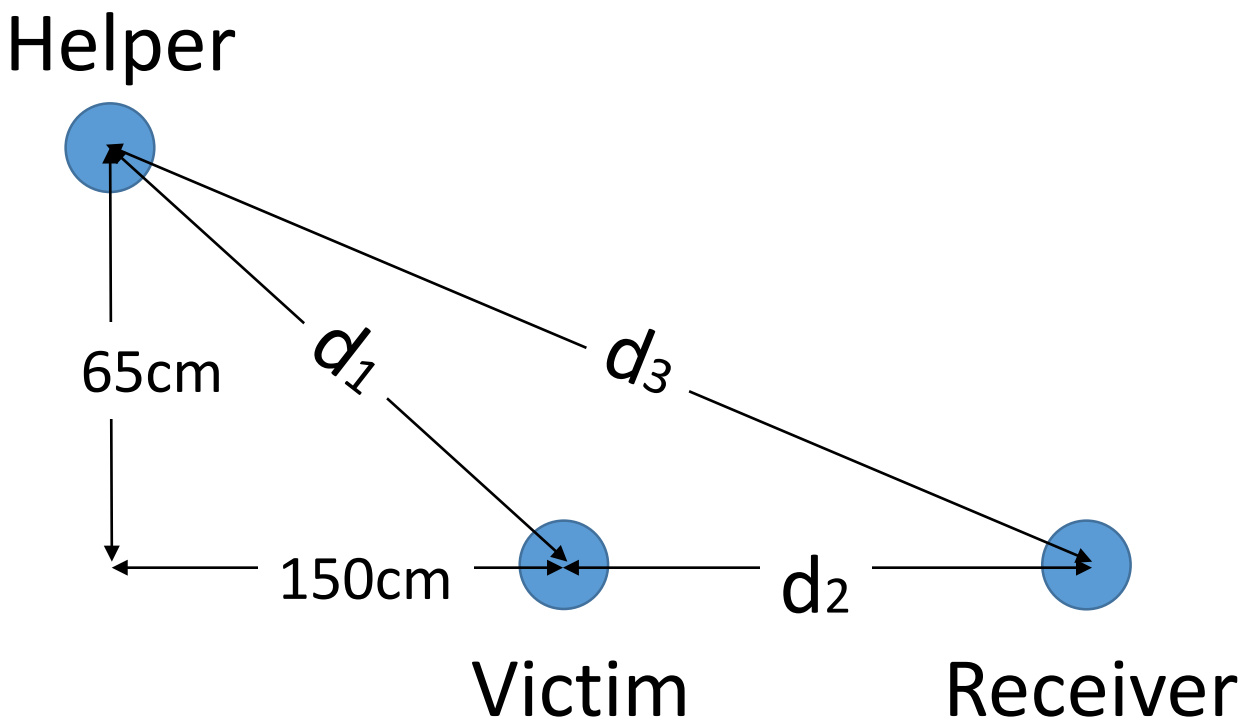
- Dangerous Permissions
  - `READ_CALENDAR, CAMERA, READ_SMS, READ_CALL_LOG …`
- Normal Permissions
  - `SET_ALARM, SET_TIME_ZONE, …`

  `CHANGE_WIFI_STATE`



Attack Scenario



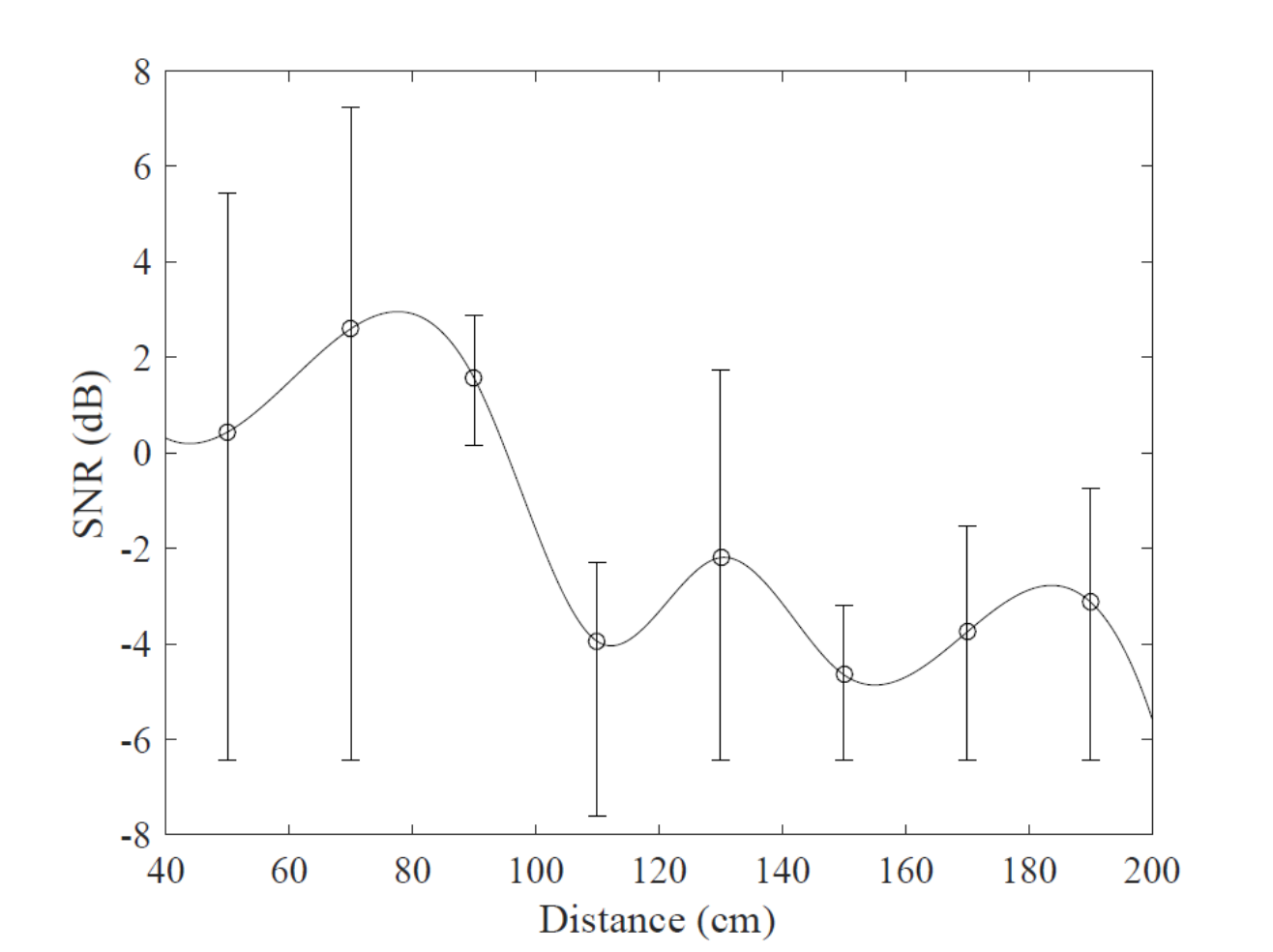


Attack Scenario

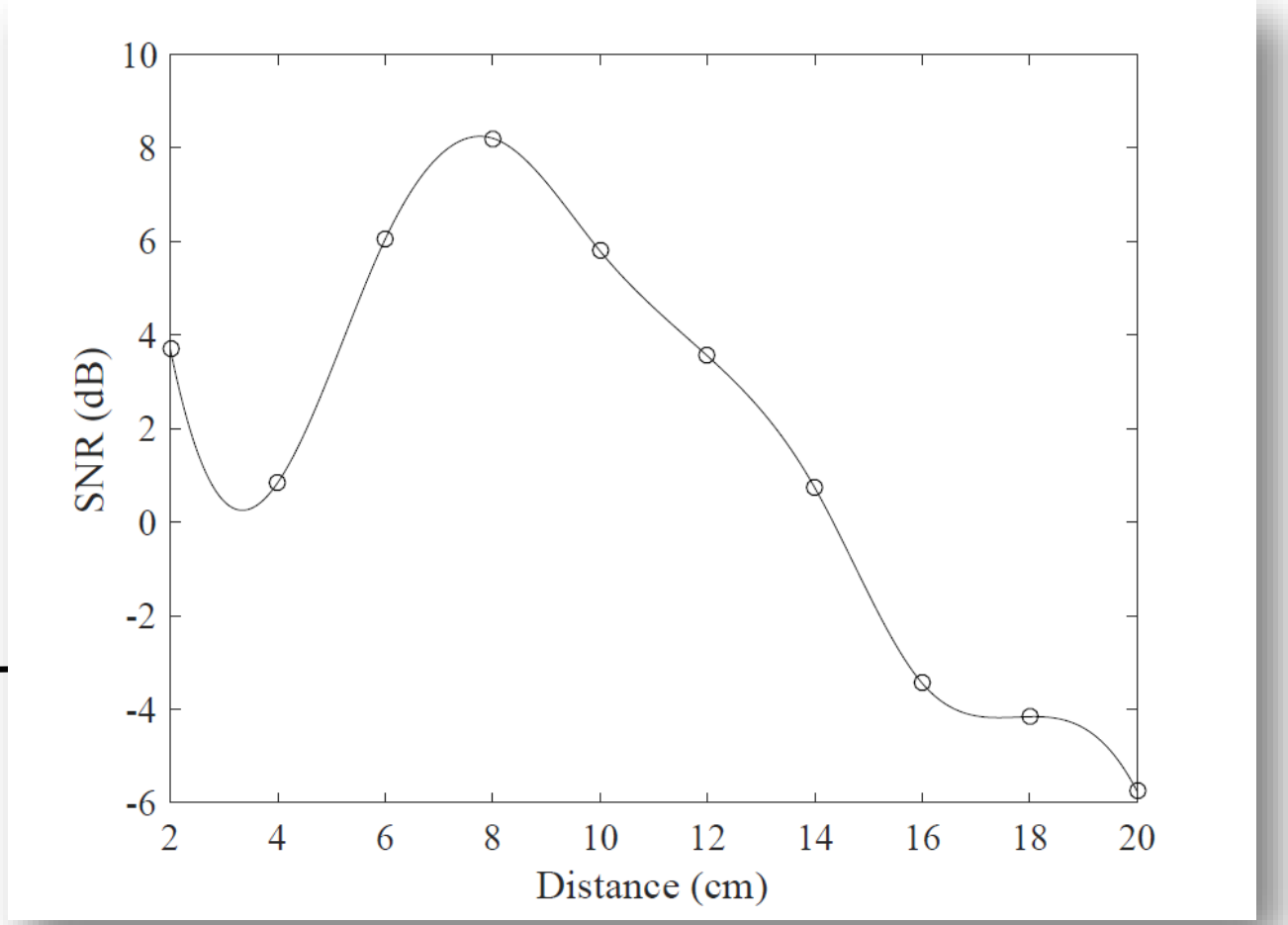
N210

Incident Signal

HP Elitebook 8530P

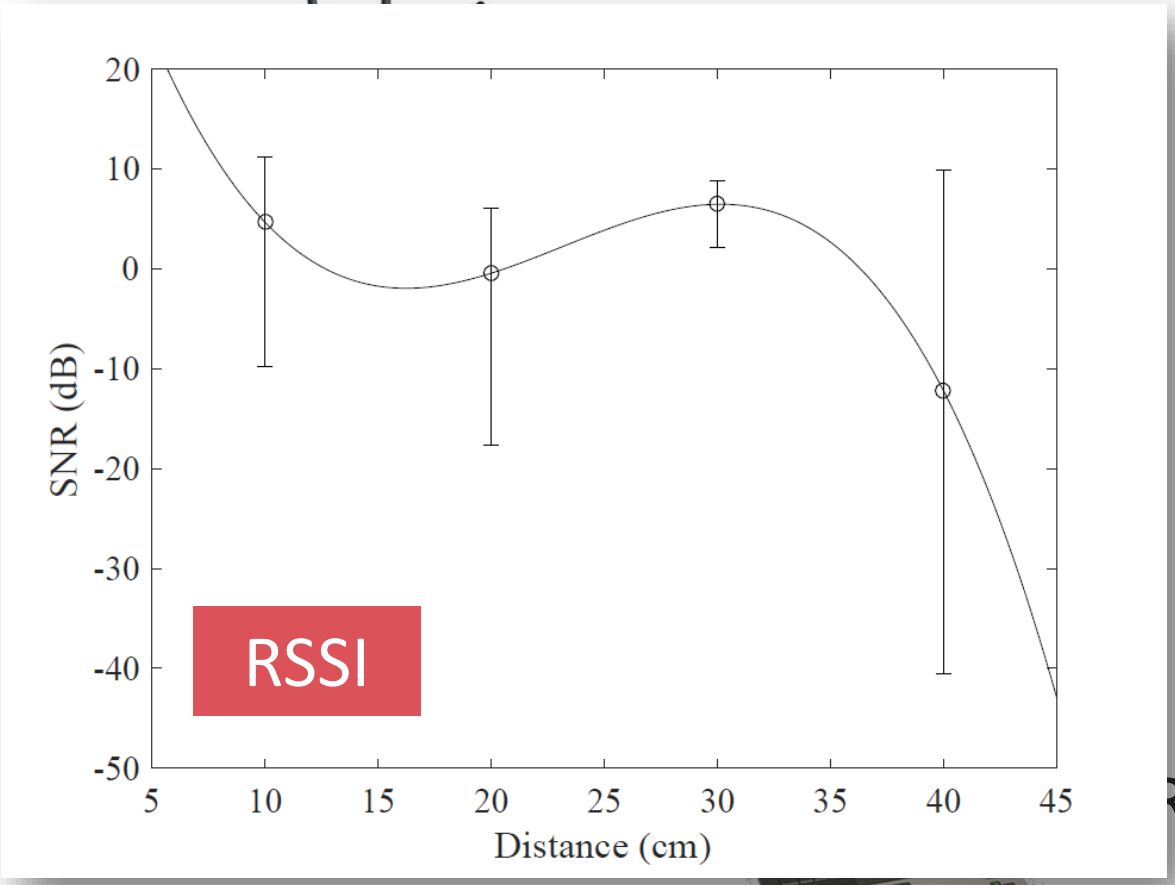


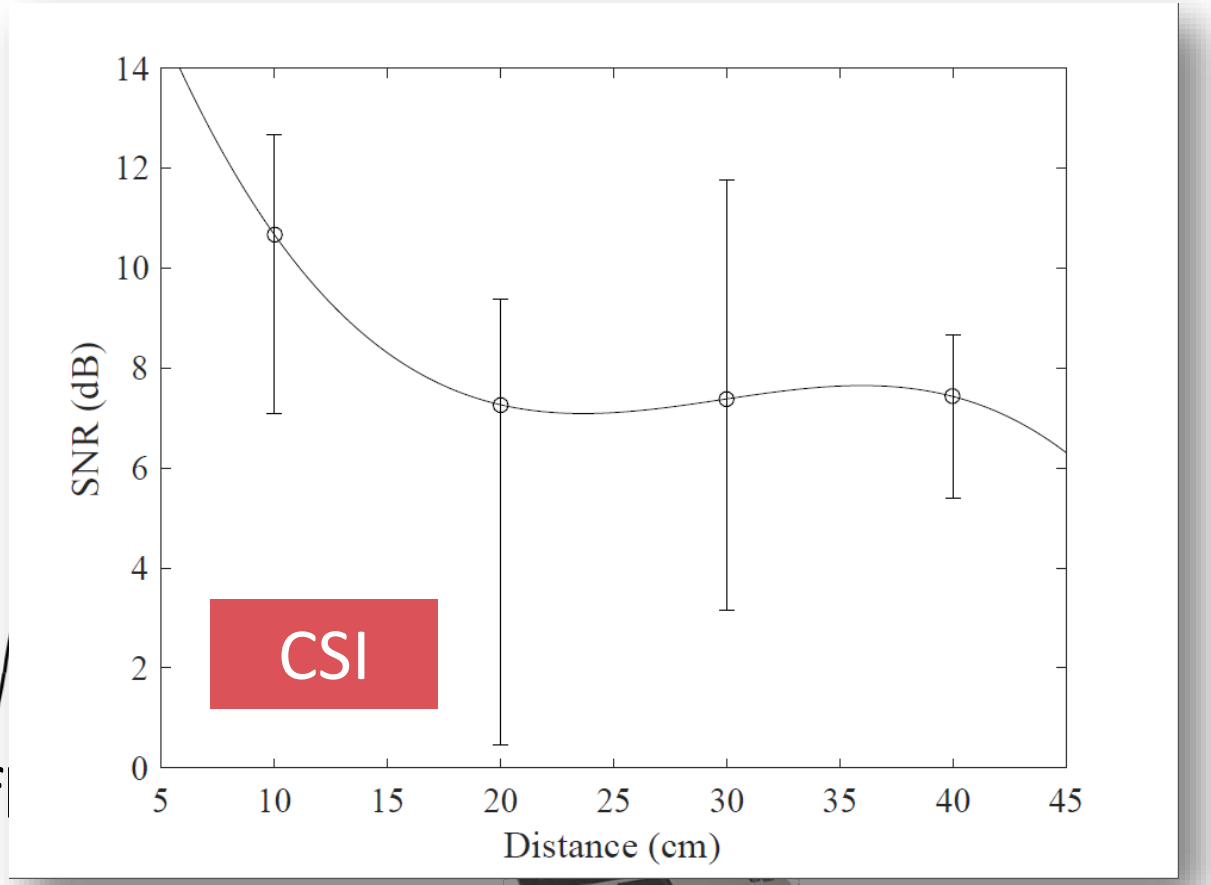
Attack Scenario



Attack Scenario

TPLink 4300



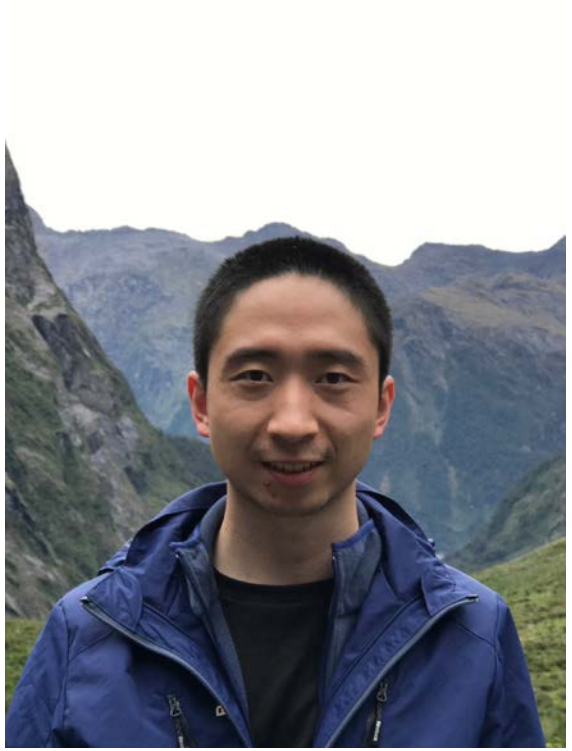


HP Elitebook 8530P

HP Elitebook 8530P

Limitations and Discussion

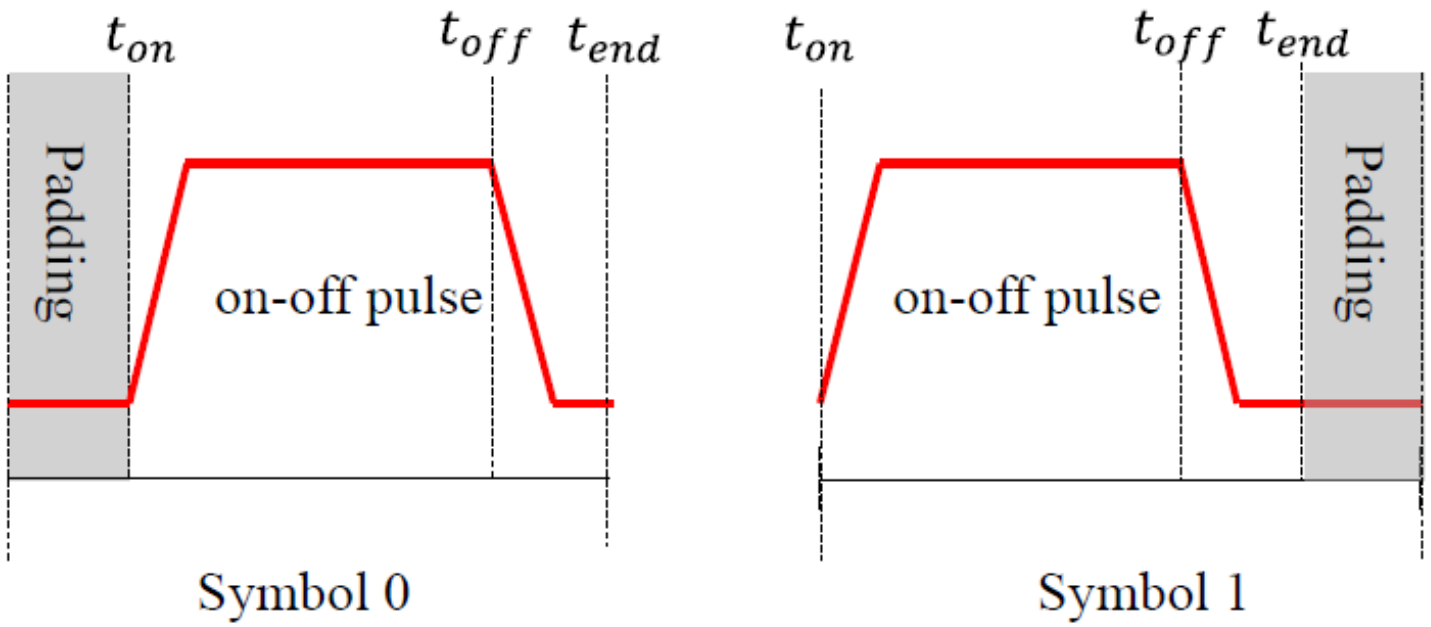
- Communication Distance
  - SINR, NIC Models, Antenna Gain, etc.
  - ➢Interference Cancellation
- Date Rate
  - Software: NIC Driver, Hardware: On-off processing logic
  - ➢Fast impedance change
- Possible Applications
  - Cross Protocol Communication, Wireless Sensing, etc.



Thank you!

Backup Slides

On-o Position Modulation (OOPM)



Transmission Time of Sensitive Information

Data	bits	Laptop@30cm	USRP@90cm
MAC Address	48	49 sec	54 sec
Plain Password	64	1.09 min	1.20 min
MD5	128	2.18 min	2.40 min
GPS Coordinate	128	2.18 min	2.40 min
SHA1 Hash	160	2.72 min	3.00 min
Disk Encryption Key	256	4.35 min	4.80 min

Receiving Range