LTE Security, Privacy, and Assurance: Key Research Challenges and Hardware Needs

Jeffrey H. Reed
Wireless@VT, Department of ECE
Virginia Tech, Blacksburg VA
reedjh@vt.edu

Vuk Marojevic
Dept. Electrical & Computer Engineering
Mississippi State University
Mississippi State, MS
Vuk.Marojevic@msstate.edu

Date: 20 September 2018
Introduction

• 4G LTE (even 5G NR) is vulnerable to attacks at all layers [1,2].
• Last year, there was evidence of “stingrays” being used in the DC area. Devices to snoop on callers.
• This presentation slides address the following:
  – Highly vulnerable 4G LTE PHY attacks and mitigation.
  – Methods to detect stingray activity
  – Challenges in performing LTE information assurance research
  – Example of Hardware Needed
  – Recommendations for a way forward in enabling research
LTE PHY Layer
Security/Assurance/Privacy Attacks

Known attacks, ignored in the past, but must be addressed for mission and life critical 5G systems and FirstNet.
Stingrays: Menacing DC

- Also known as Rogue Base stations/IMSI catchers.
- Can be easily implemented from open-source libraries such as srsLTE/OAI, while hooked to a cheap USRP.
- Detection Methods:
  - Signal Structure: Anomaly detection of spatial signature, power, and spectrum.
  - Network-level: Crowdsourcing BS behavior, deployment of “honeypot” UEs, supply fake IMSI and watch behavior.
  - Repurposing available infrastructure: Legitimate eNodeBs or crowd source UEs with collection software.

Obtaining IMSI by Software-Defined Radio (RTL-SDR) -- $32 IMSI catcher

Pictures from:
doi: 10.1109/EIConRus.2018.8316859
Challenges for Research

- Need the realism of a real situation.
  - Finding issues
  - Fixing issues
  - Getting/generating the data

- Need expensive equipment for observing protocol exchange and logging for forensics.

- Need to replace expensive equipment with inexpensive equipment so that many universities are enabled to do the needed research. – Hard

- Need to be concerned with privacy issues and impacting real networks though active probing– can inadvertently become the bad guy. FCC might get mad 😞
Hardware for Stingray Detection

Architecture and features of “spectrum enforcement” hardware
What’s Needed – A Contest on LTE Assurance, Privacy, and Security

• Common tools for researchers
  – LTE UEs and eNBs SDR-based and/or dedicated hardware.
  – LTE Protocol monitors
  – Misc. software tools
  – Reference manual for how to deal with privacy issues

• Hardware testbed – Out of the carrier’s spectrum.
  – Early phase experiments in lab or via internet
  – Later phase experiments in the field (is this a role for an NSF PAWR testbed?)

• Paid competition among researchers to determine
  – Flaws and weakness identified in the standard or interpretation of the standard
  – Defensive strategies and countermeasures
  – Forensics techniques to find new attacks and understand them

• Field-based experimentation for more realism – *Could this be a role of NSF PAWR testbeds?*

• Should we consider DSRC or cV2x instead?
  – Less investigation
  – Mission critical (life-critical)
  – Early enough research to impact deployment and standards
For Further Reading


"Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Networking and Information Technology Research and Development Program."

The Networking and Information Technology Research and Development (NITRD) Program

**Mailing Address:** NCO/NITRD, 2415 Eisenhower Avenue, Alexandria, VA 22314

**Physical Address:** 490 L'Enfant Plaza SW, Suite 8001, Washington, DC 20024, USA Tel: 202-459-9674, Fax: 202-459-9673, Email: nco@nitrd.gov, Website: [https://www.nitrd.gov](https://www.nitrd.gov)