icc: iMSI catcher catcher

Jan Kuipers

j.h.kuipers@student.utwente.nl

University of Twente

David Stritzl

david.stritzl@gmail.com

University of Twente

Santiago Aragón

s.e.aragonramirez@student.utwente.nl

University of Twente

Iwan Timmer

i.r.timmer@student.utwente.nl

University of Twente

Abstract

This program tries to find nearby IMSI catchers using a RTL_SDR device. TODO: Diagram

---

1. Motivation and Outline

2. Design

2.1. Detection methods

Detections methods (DM) are defined as python scripts in detectors/some_dector.py. Every method should extend the class Detector specified in detectors/Detector.py and define its own callback function, e.g.:

```
def handle_packet(self, data):
    p = GSMTap(data)

    if p.payload.name is 'LAPDm' and
       p.payload.payload.name is 'GSMAIFDTAP' and
       p.payload.payload.payload.name is 'CipherModeCommand':
            cipher = p.payload.payload.payload.cipher_mode >> 1

            if cipher == 0:
```

```
            self.update_s_rank(Detector.SUSPICIOUS)
            self.comment = 'A5/1 detected'
    ...
```

This function will be applied packet wise and should rank the anylyzed BTS and at the end modify the `s_rank` and `comment` variables calling `self.update_s_rank(RANK)`(resp. `self.comment='A descriptive comment'`).

We define rank the suspiciones of a BTS as

```
SUSPICIOUS = 2
UNKNOWN = 1
NOT_SUSPICIOUS = 0
```

At the end of the detection the detectors return a `TowerRank` object.

3. Implementation details

4. Limitations and future work

References