# *Rogue Femtocell Owners: How Mallory Can Monitor My Devices*

David Malone, Darren F. Kavanagh and Niall R. Murphy

19 April 2013

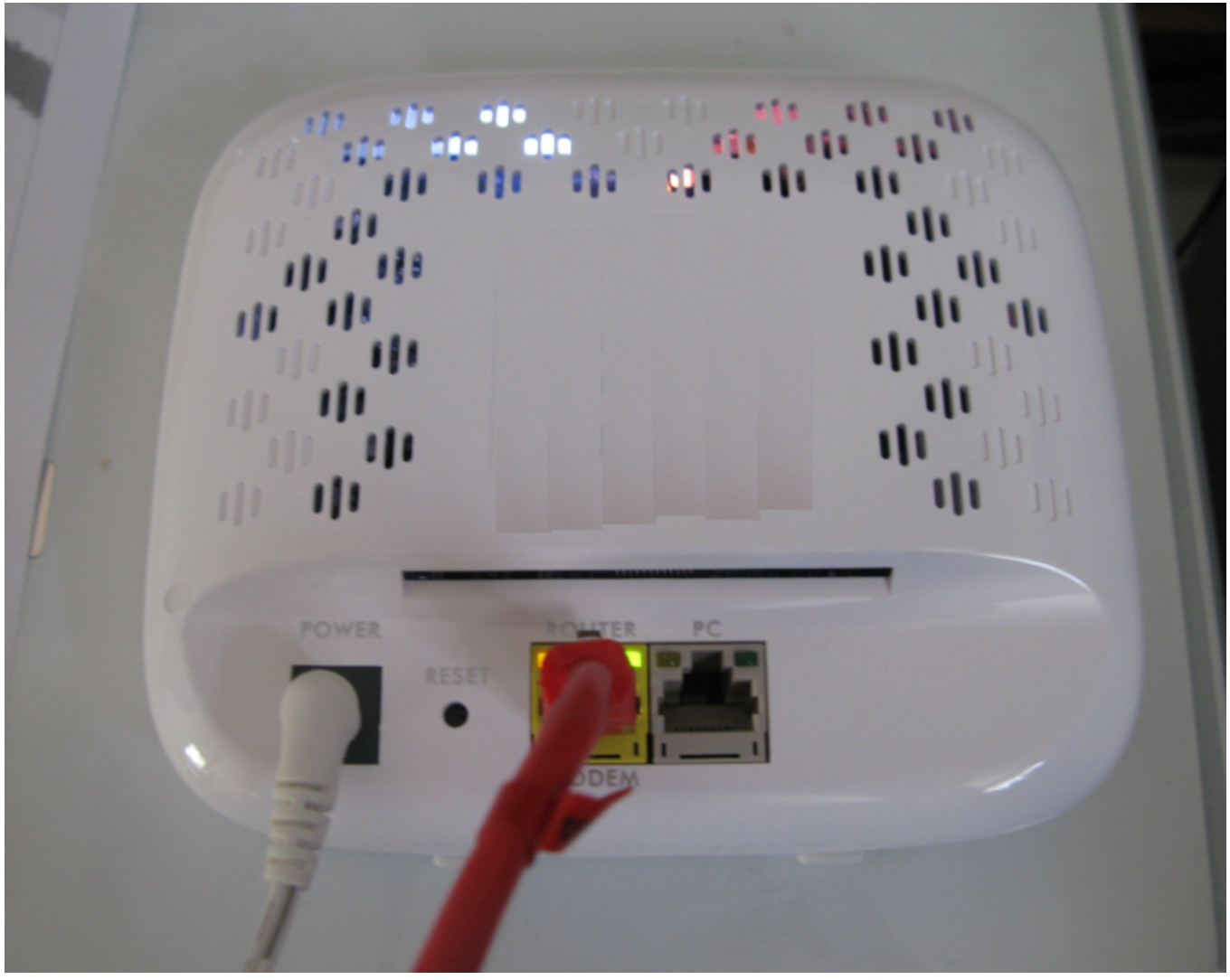
# *Femtocells*

- Small devices acting as cellular base stations.
- Deployed to extend coverage in homes, offices, . . .
- Access can be open or closed.
- No direct connection to MNO network.
- Use Internet and IPsec for backhaul.

# *Femtocell (front)*

Alcatel-Lucent 9361 Home Cell V2-V.

# *Femtocell (back)*

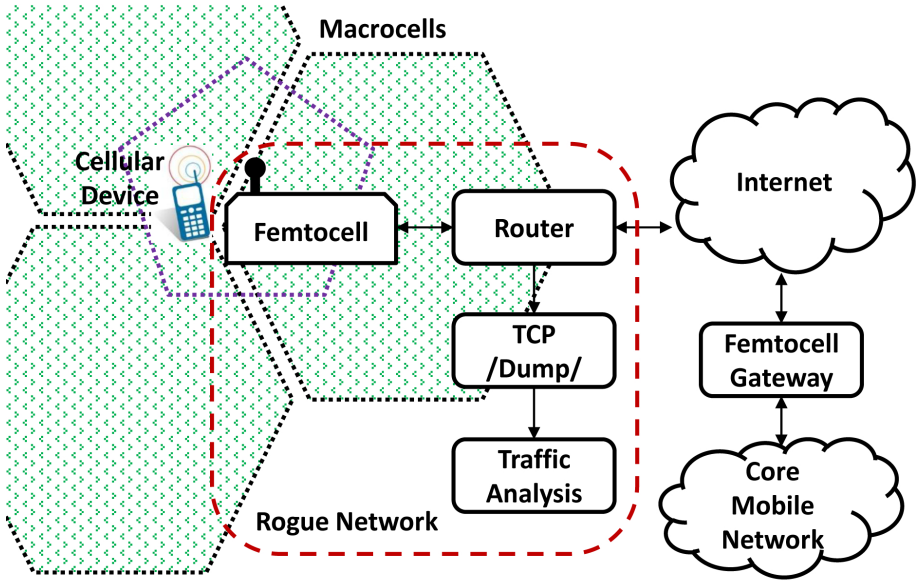



Alcatel-Lucent 9361 Home Cell V2-V.

# *Femtocell Access Control*

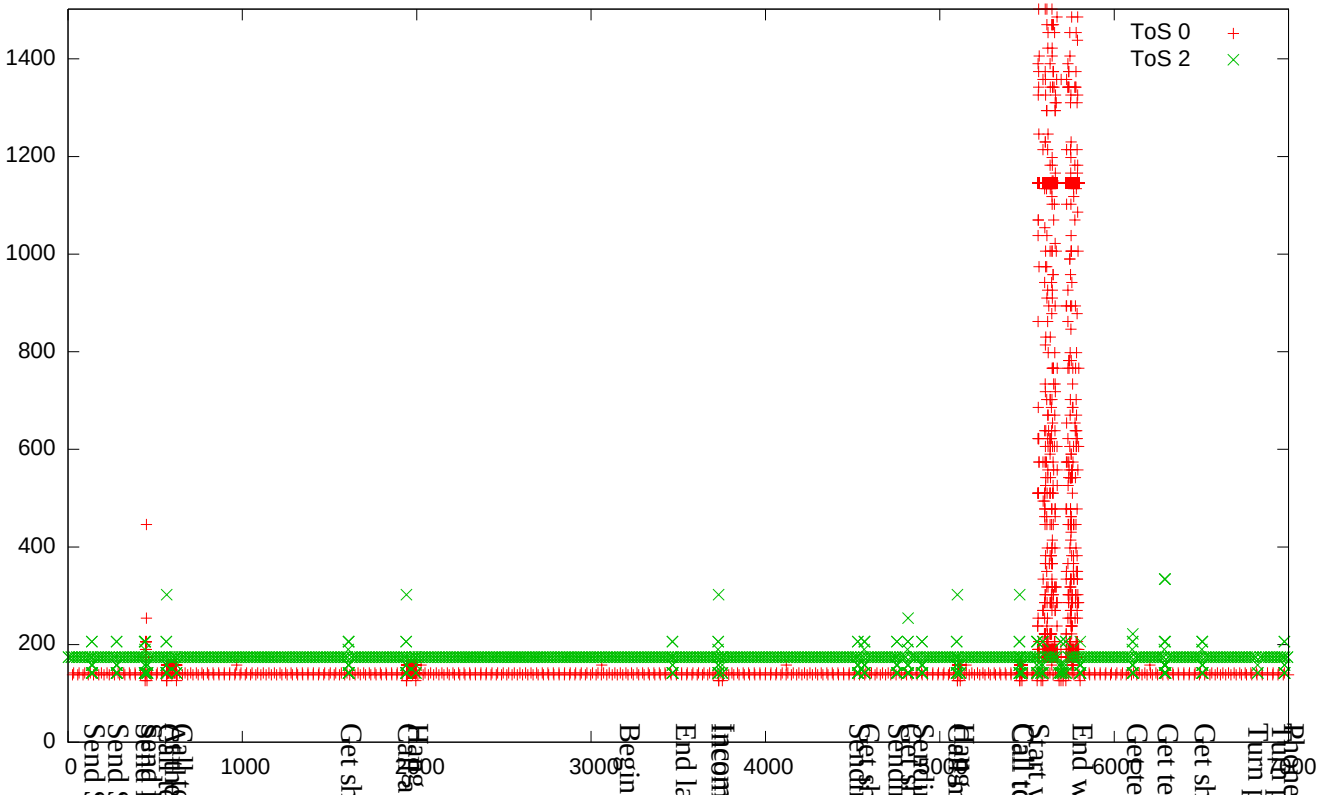
- Anyone device can connect to open femtocell.
- Closed femtocells allow ACL.
- Commonly administered by web page, list phone numbers.
- No further checking done.
- *Idea: ACL to target devices who shouldn't trust us?*
- *Idea: Use traffic analysis as passive attack.*
- Snoop on your neighbour?

# *Monitoring a device*

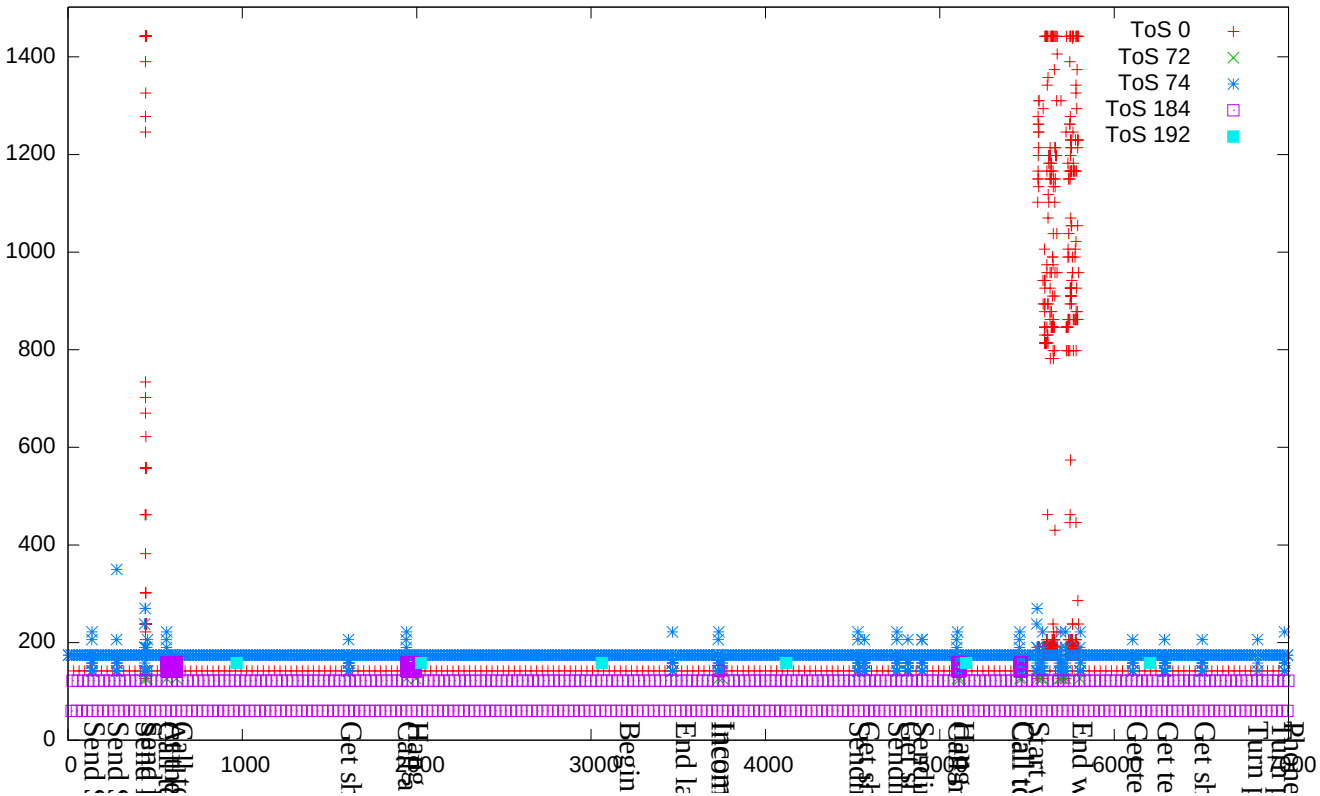



- Add phone (Nokia X6) to femtocell's ACL.
- SMS, MMS, voice calls, web browsing, management.
- Collect femtocell traffic on router.
- Traffic (mostly) encrypted, but know time, size, ToS.
- What does traffic tell us about activity?

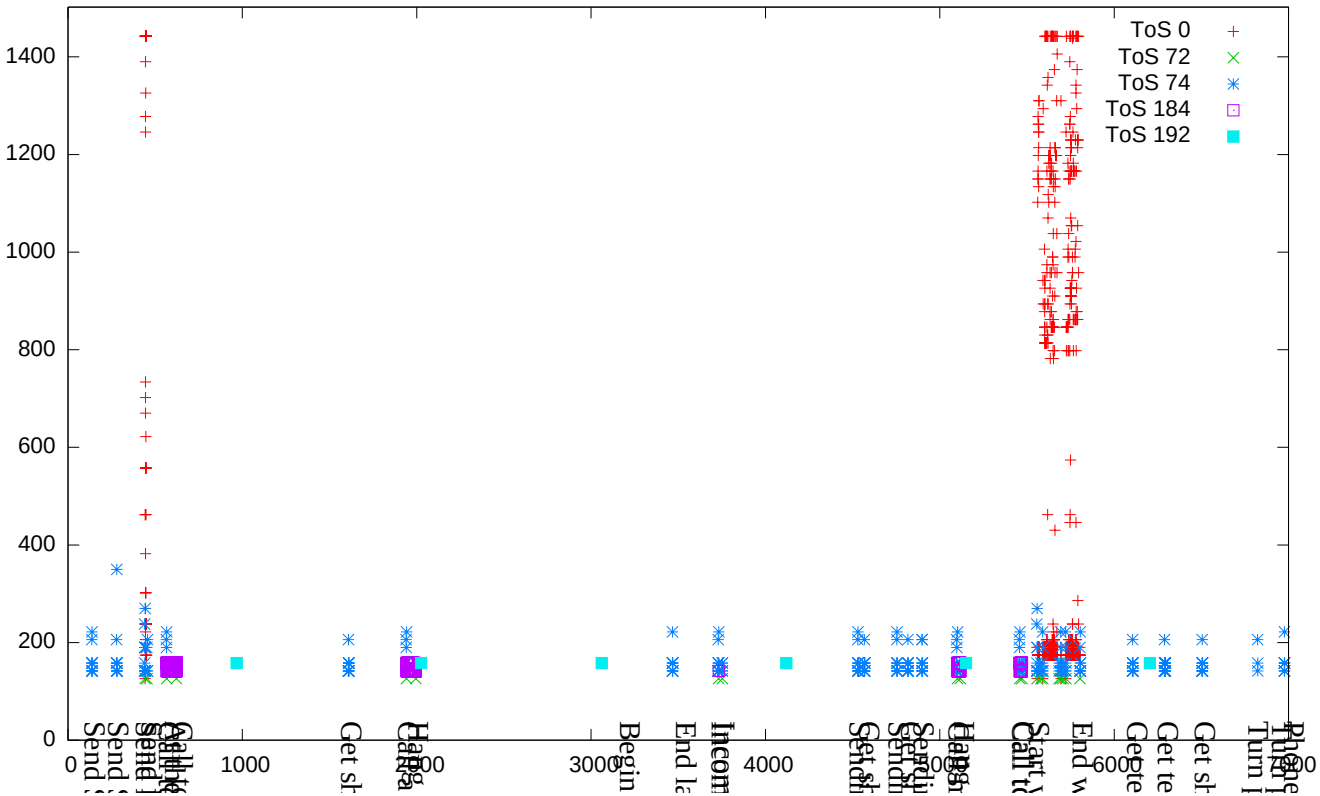
# *Traffic Analysis (to femtocell)*



# *Traffic Analysis (from femtocell)*



# *Traffic Analysis (cleaned up)*

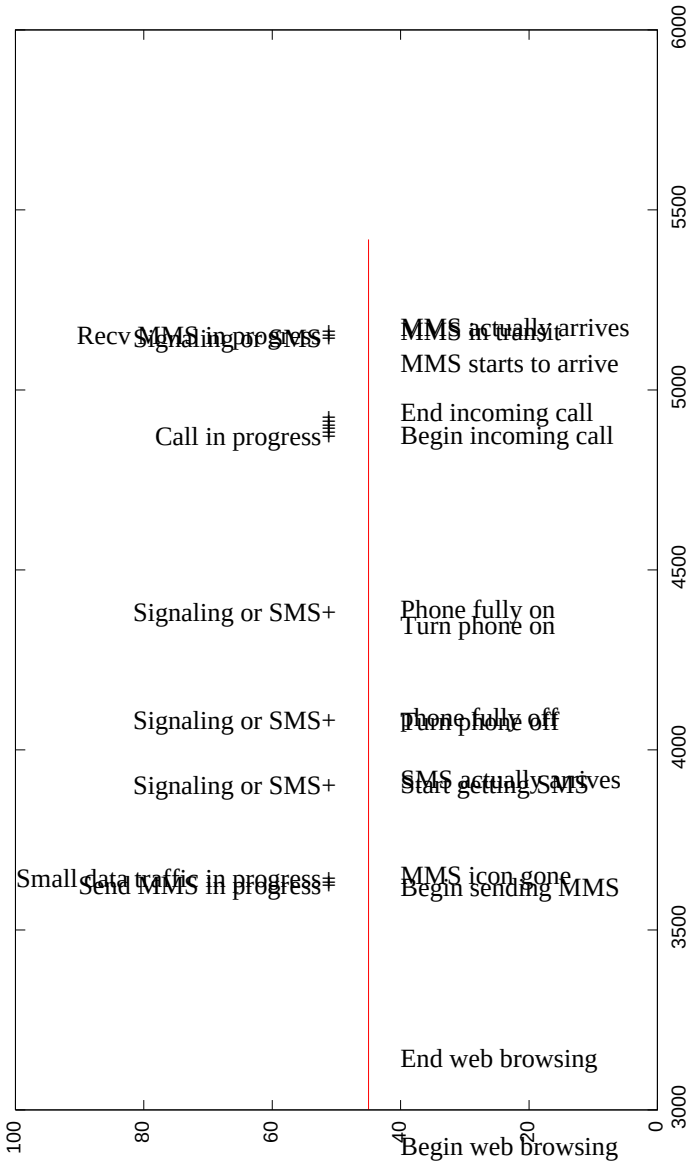


# *Classification*

- Could we classify based on this?
- Yes — hand designed algorithm based on 10s buckets.
- Some trouble telling SMS/signaling and MMS/data apart.
- Works well (15000s, 35 events, one false positive).

```
for each (10s interval) {
  Remove background traffic (size, TOS, direction)
  Count number_of packets for each (TOS, direction)
  Store largest packet size for each (TOS, direction)
  if (number_of (TOS 184,SRC) packets > 1)
    event "Call in progress";
  if (number_of (TOS 0,SRC) packets > 0) {
    if (largest (TOS 0, SRC|DST) > 800)
      event "Web session in progress";
    else if (largest (TOS 0, DST) > 800)
      event "Recv MMS in progress";
    else if (largest (TOS 0, SRC) > 800)
      event "Send MMS in progress";
    else
      event "Small Data/MMS in progress";
  }
  if (number_of (TOS 74) > 0 &&
      number_of (TOS 0|72|184, SRC) == 0)
    event "Signaling or SMS";
}
```

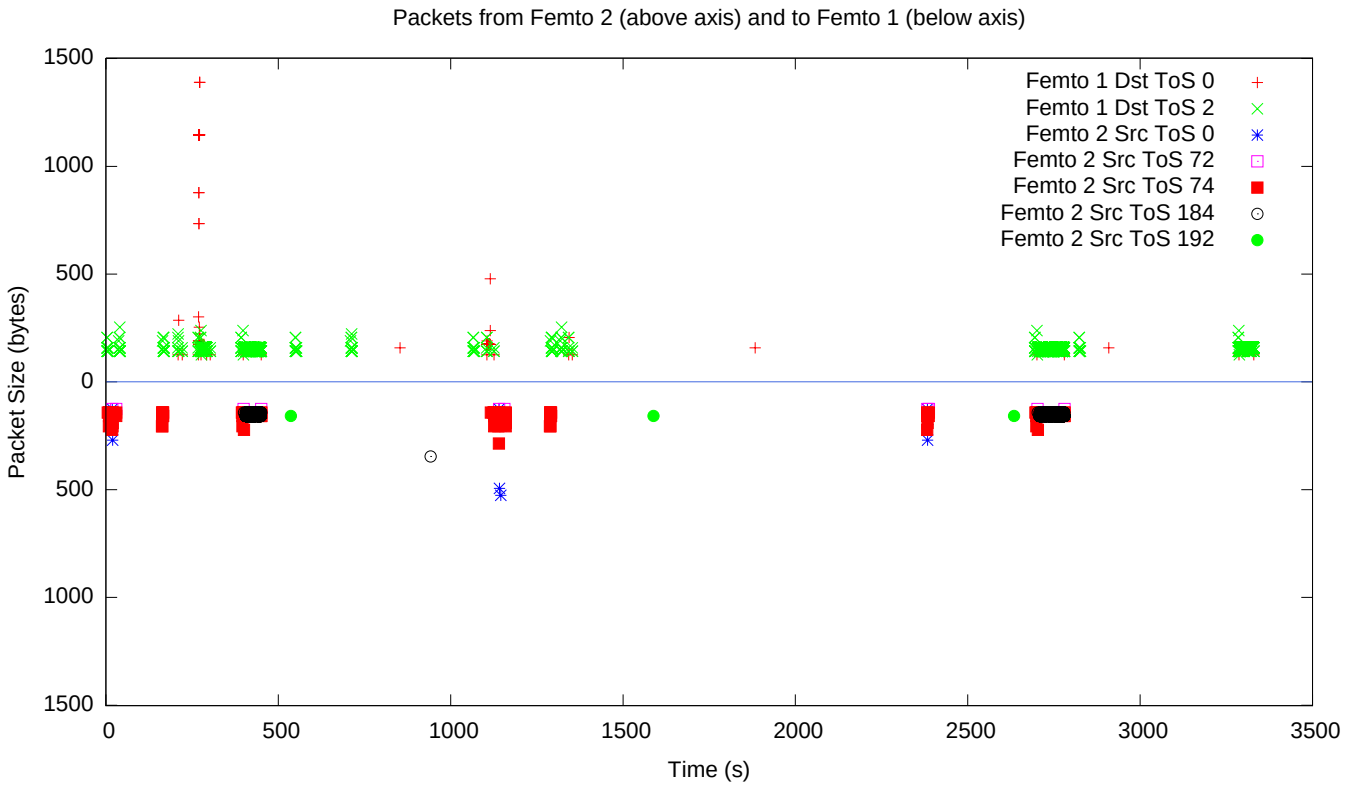
# *Classification vs. Events*



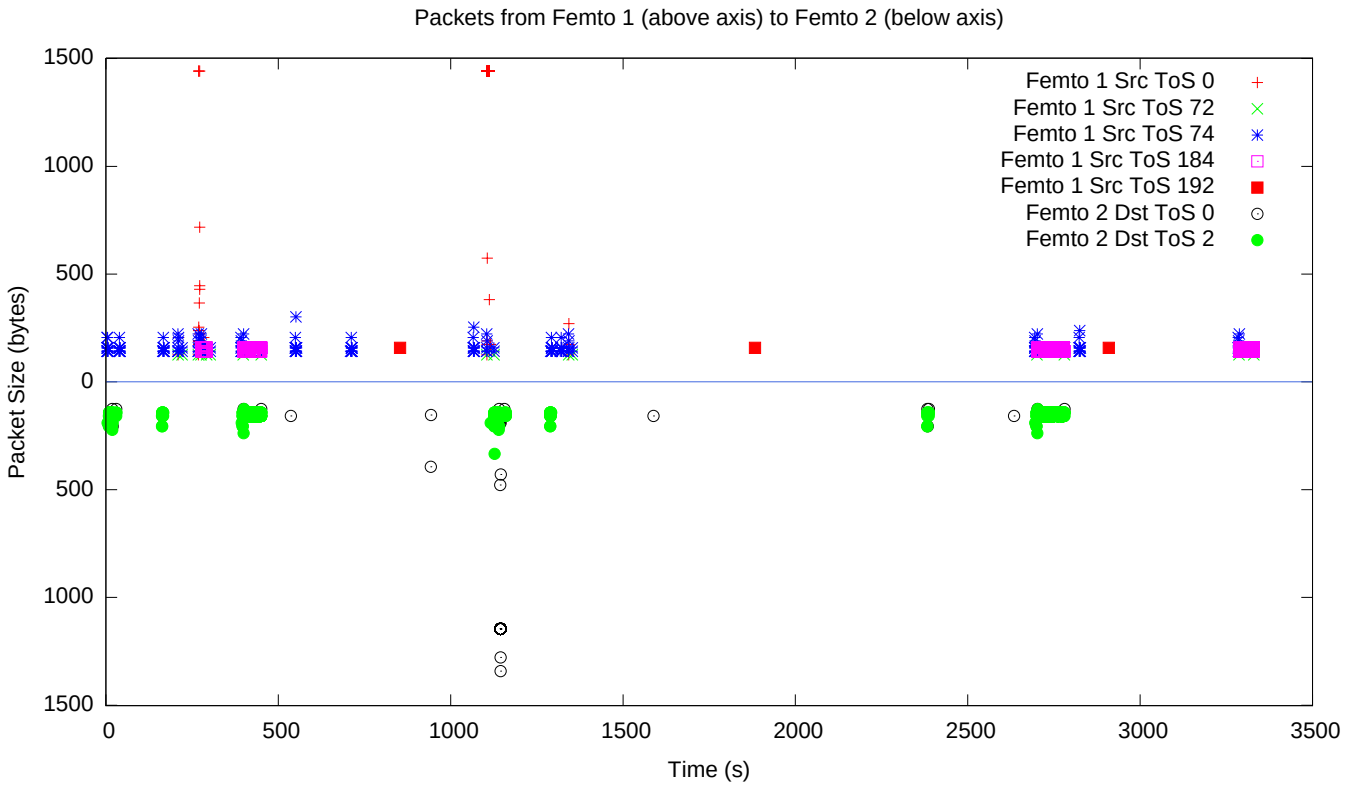
# *Two Femtocells?*

- Suppose we can snoop on two femtocells, each near a target.
- E.g. two celebrities, are they exchanging calls?
- Can we correlate the information at both ends?
- Two femtos, two gateways (NTP synced), two phones (iPhone).
- Collect traffic, compare traces.
- Run classifier, correlate results.

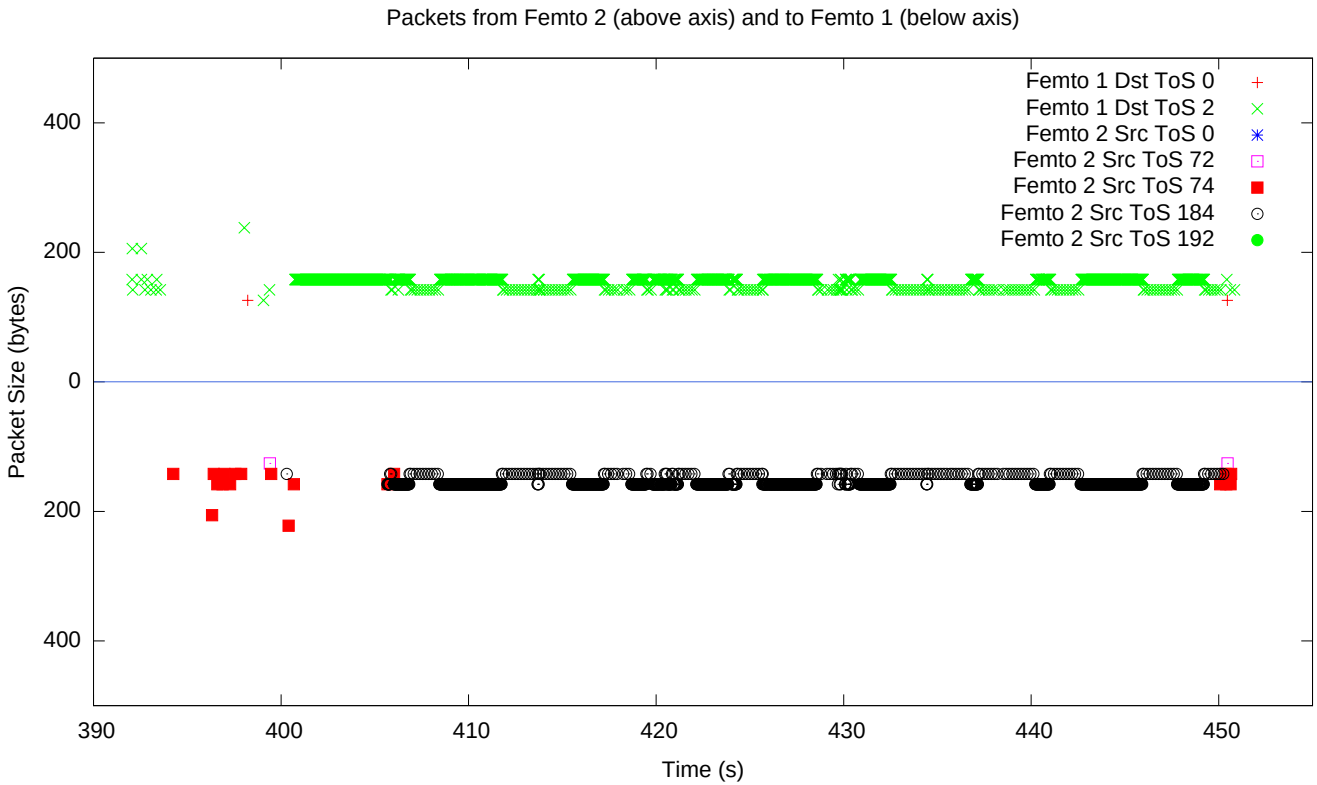
# *Traffic Analysis (two femto)*



# *Traffic Analysis (two femto)*



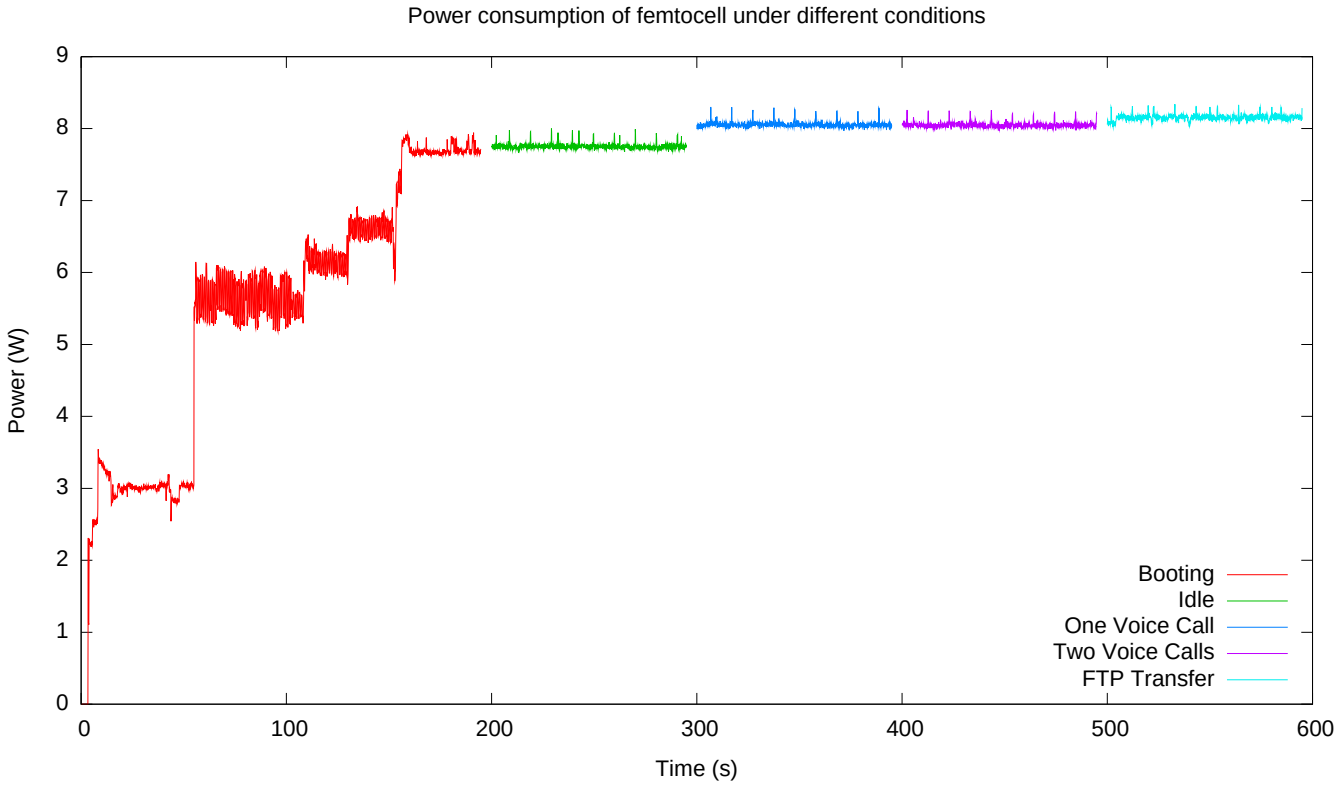
# *Traffic Analysis (two femto)*



# *Other Side Channels*

- We control femtocell's environment.
- Are there other things we can snoop on?
- RF?
- Power usage?
- LEDs?

# *Power Analysis*




Measured with help of Roberto Riggo.
Actually significant difference in means!

# *LED Analysis*

Maybe good for clearing false positives?

# *Fixes?*

*Dummy Traffic* Generate dummy traffic all the time, to hide behaviour. Unlikely to be popular.

*IMEI/IMSI Number* Ask for more information when adding phone to ACL.

*User Confirmation* Send a SMS and ask if OK to use femto?

The last addresses the issue of user consent.
Issues for dumb devices.

# *Conclusion*

- Analysis worked pretty well.
- Trusted devices with potentially rogue network administrators.
- Attacks on compressed voice (Wright et al).
- What about active attacks?
- More ambitions — botnet of femto gateways?