Wifi roaming and open source

Karel Kočí

12.6.2018

802.11r

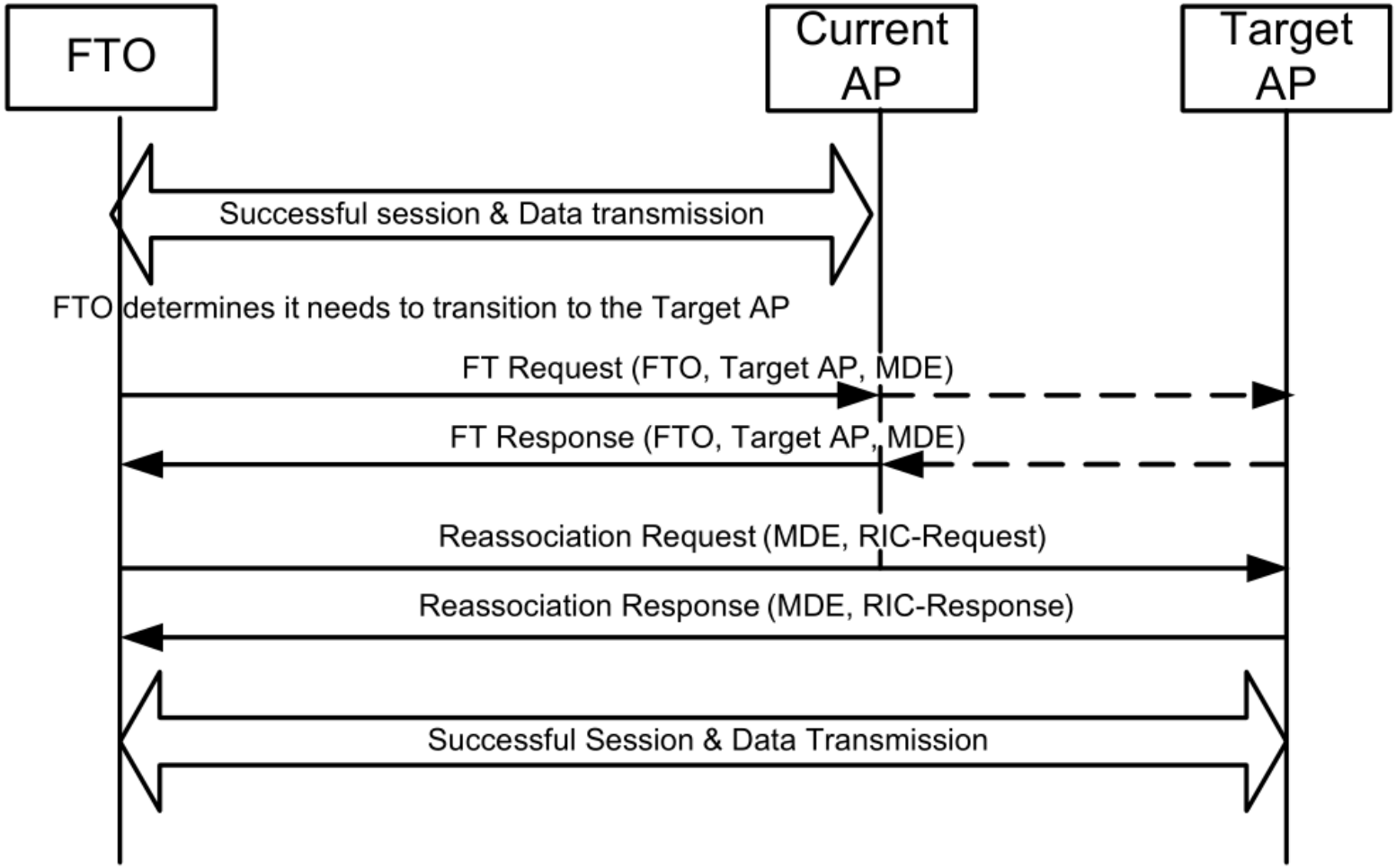
- Extension to 802.11i (WPA2)
- Allows AP switching in cooperation between both APs
- Supplicant negotiates keys before AP switch
- Usable when moving between access points
- Only in same mobility domain
- Communication between APs can be either over air or DS

802.11r terminology

- **R0KH** Derives keys for all R1KM in network
- **R1KH** Derives PTK (Pairwise transient key)
- **S0KH** in Supplicant derives R0 keys
- **S1KH** in Supplicant derives with R1KH PTK

Both R0KH and R1KH communicate with authenticator
Another point: 802.11r (FT) is advertised

Over-the-DS TF protocol (non-RSN)



Source: IEEE Standard (11:13.5.5,13-8)

Setting it up (on OpenWRT)

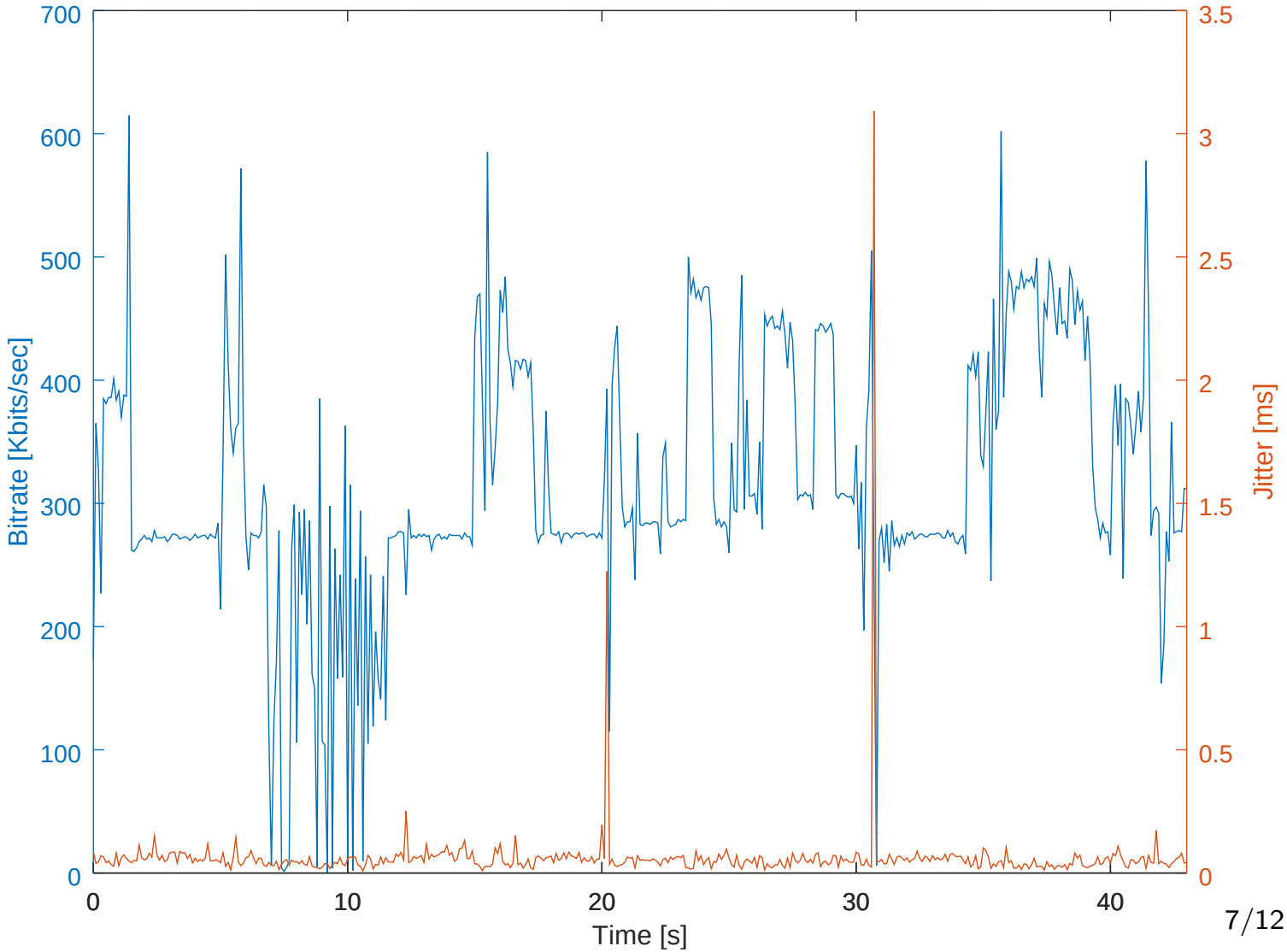
```
option ieee80211r '1'
option nasid '11'
option r1_key_holder '04F021242480'
list r0kh '04:F0:21:24:24:80,11,E1594C87BF2C30DA27E1C116C56
list r0kh '04:F0:21:24:24:5E,12,903F4FFCC7907A6562B665B6721
list r1kh '04:F0:21:24:24:80,04:F0:21:24:24:80,290856554F81
list r1kh '04:F0:21:24:24:5E,04:F0:21:24:24:5E,F38D019B98BA
```

```
list r0kh 'BSSID,NASID,KEY'
list r1kh 'BSSID,KEYHOLDER-ID,KEY'
```

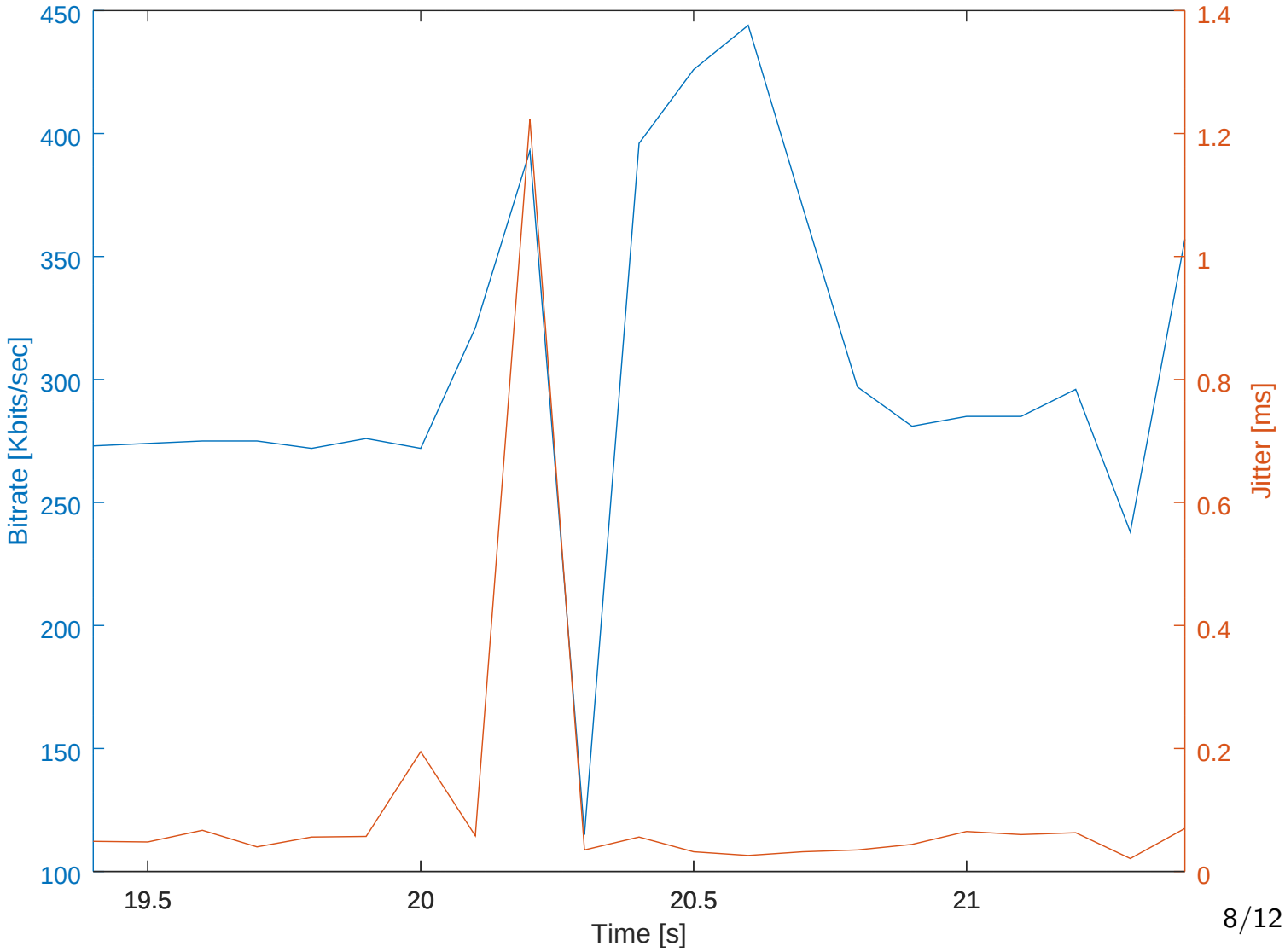
Measurements

- Two 5GHz APs with OpenWRT and configured 802.11r (hostapd, ath10k)
- PC running iperf3 server
- Laptop with wpa_supplicant running iperf3 client in UDP mode
- iperf3 configured for 600Mbits/sec

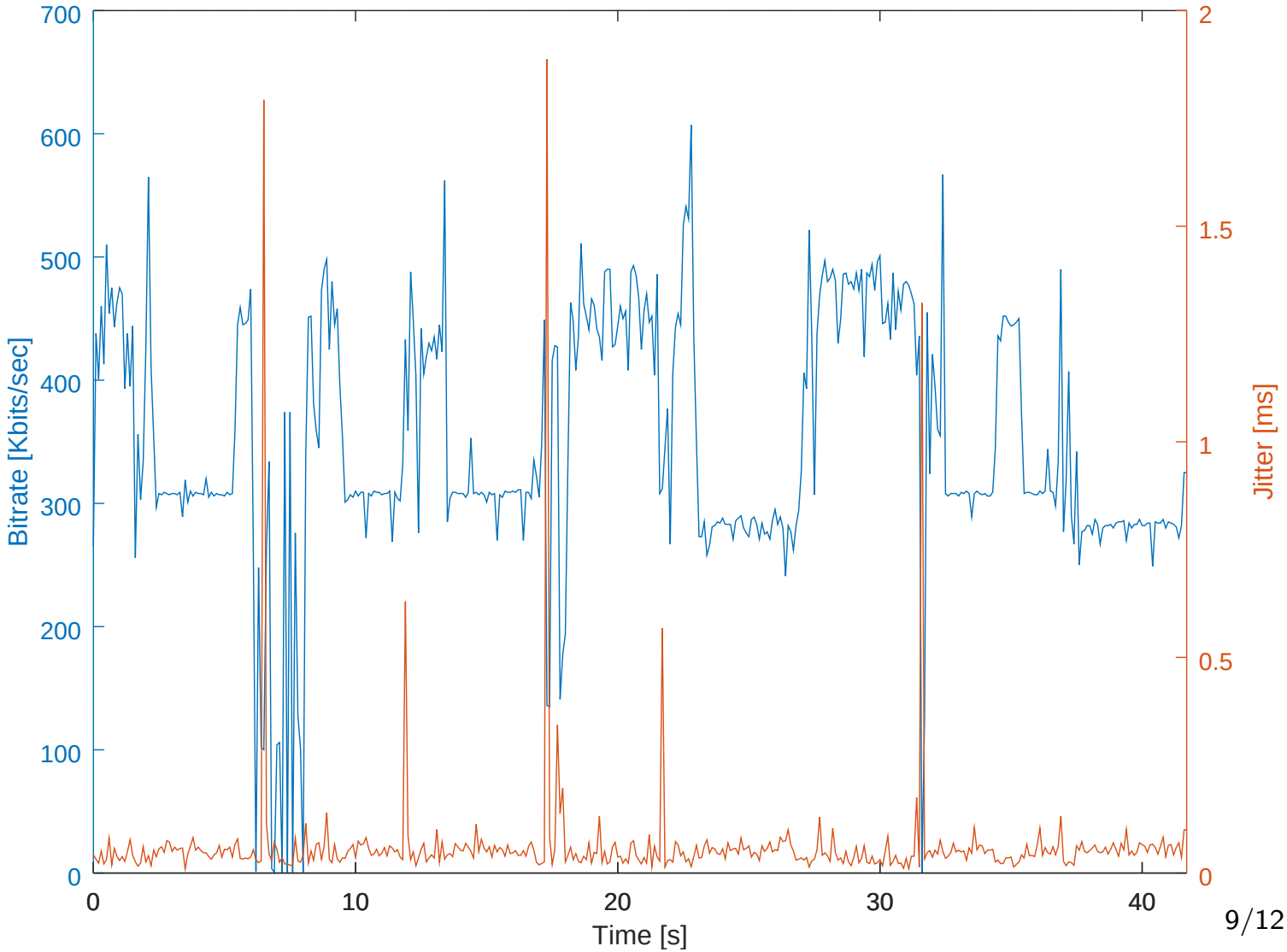
Switching with roaming



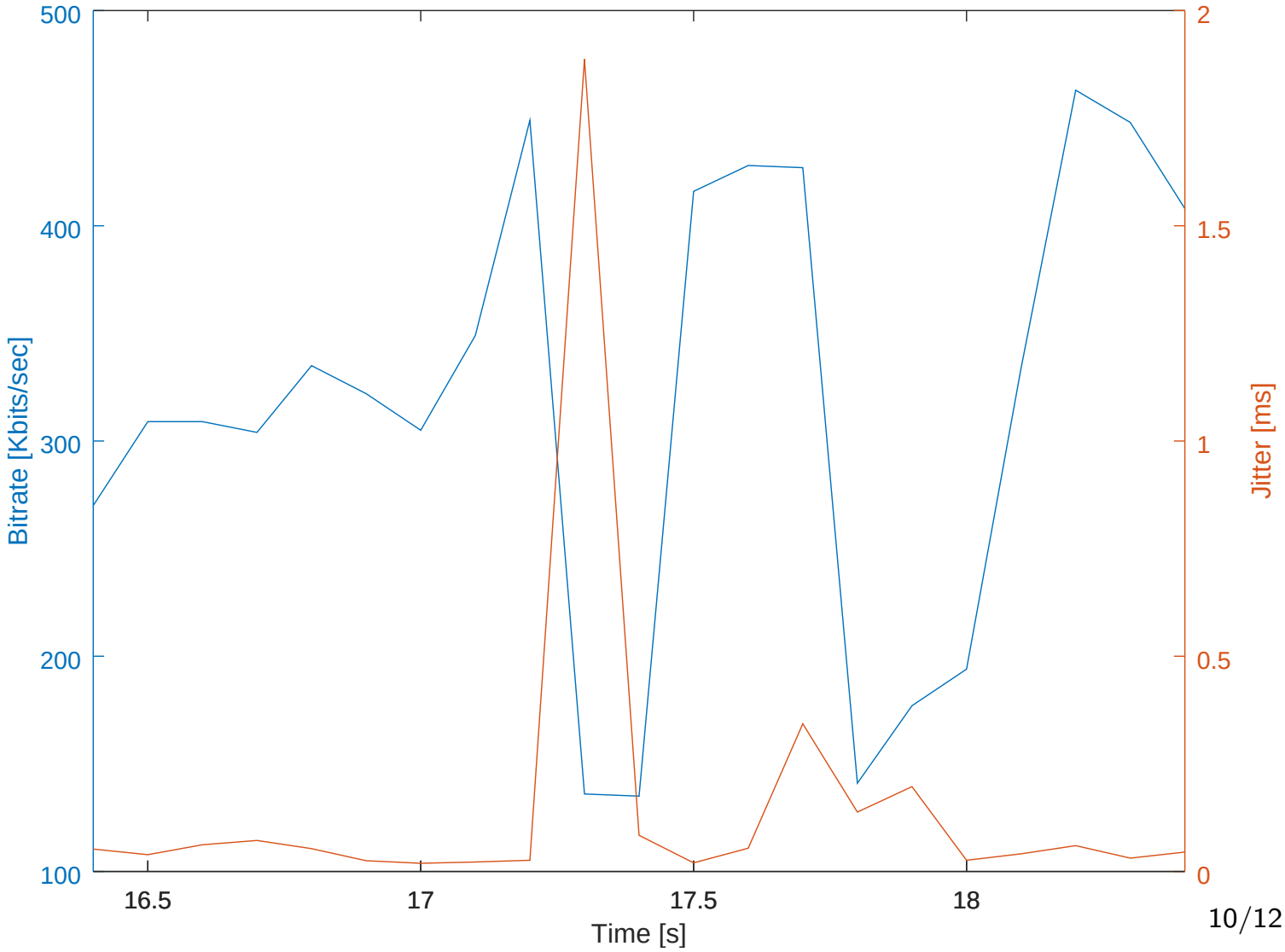
Switching with roaming



Switching without roaming



Switching without roaming



Real usability

- **Android** Lowers threshold for switch
- **Linux(wpa_supplicant)** No effect (well..)

```
# mode:short scan:threshold:long scan
bgscan="simple:5:-50:300"
```

Should we deploy it?

Probably yes?

Thank you for you attention

Karel Kočí (@karel_koci, karel.koci@nic.cz)