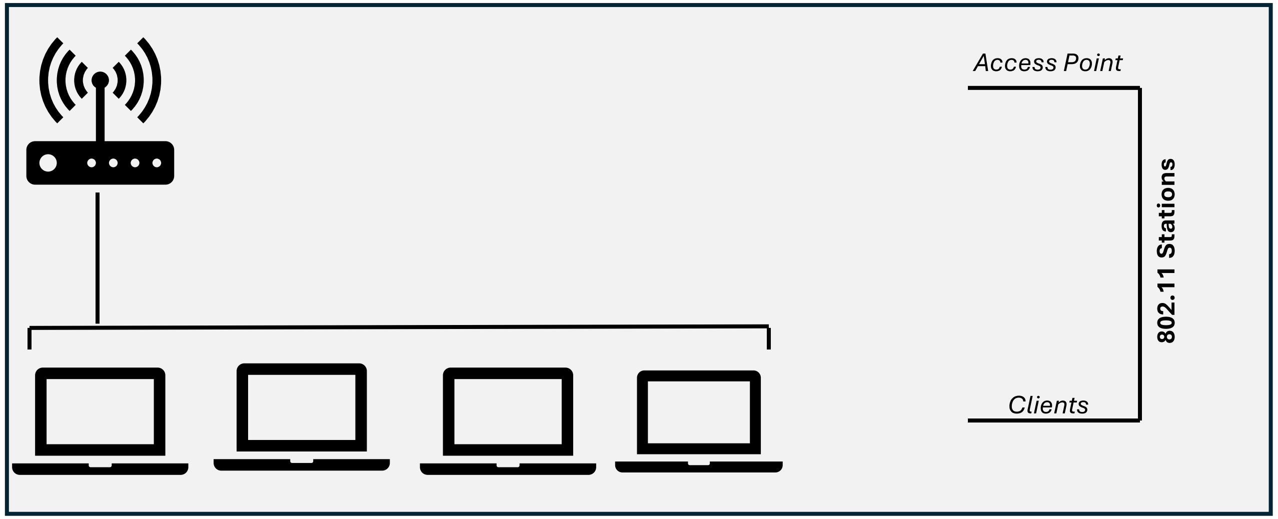
CHAOS:
Exploiting Station Time Synchronization in 802.11 Networks

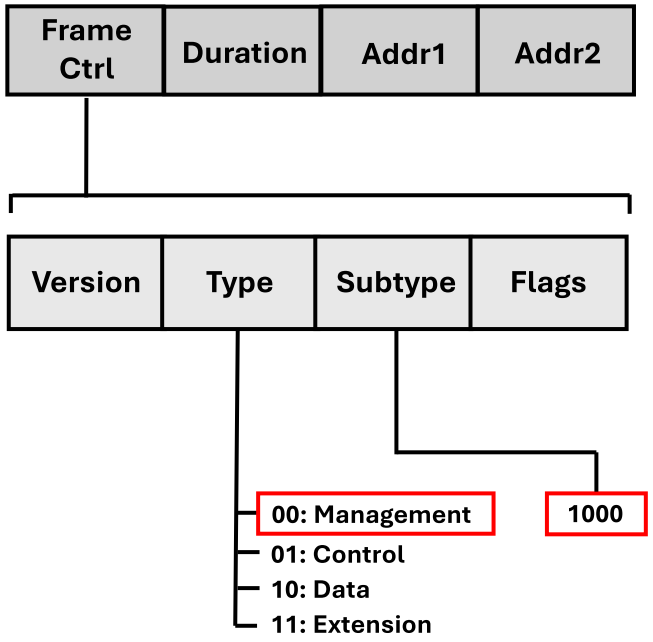
Sirus Shahini

Robert Ricci

THE UNIVERSITY OF UTAH

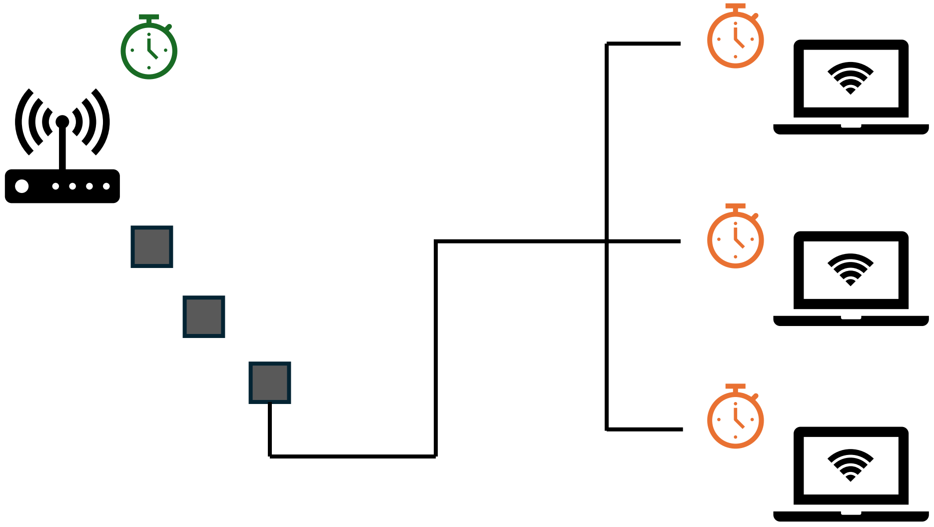
Introduction: Radio Frames



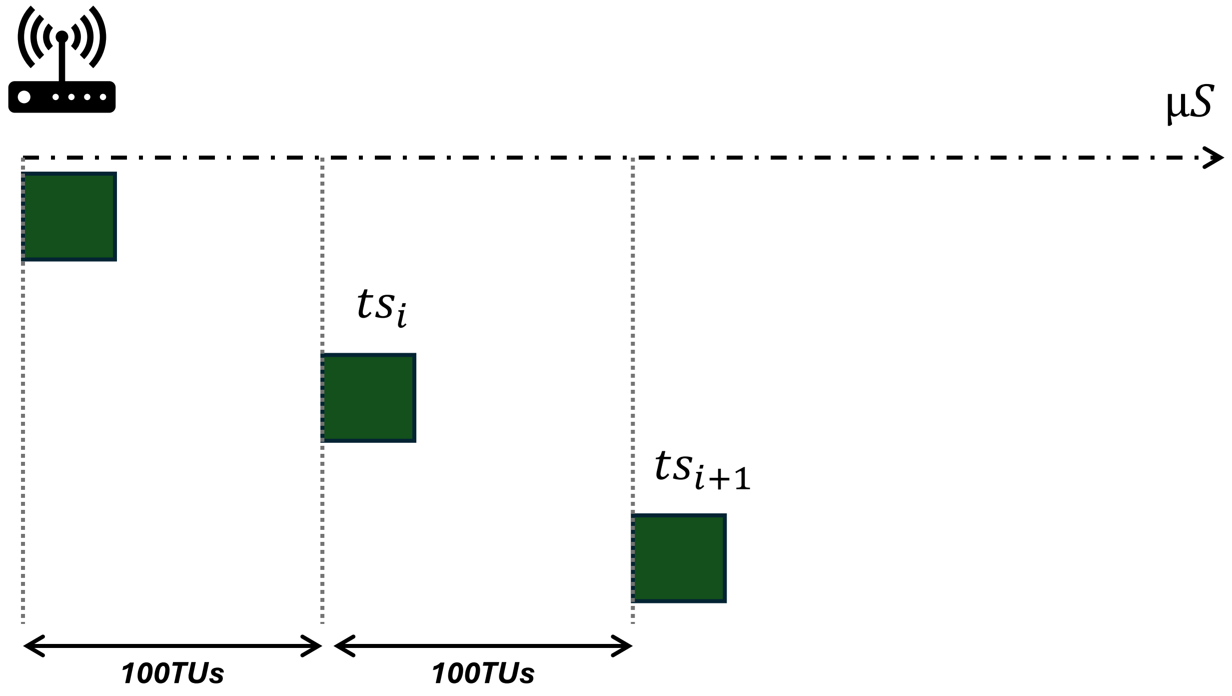


Introduction: Beacons

- 802.11 Frames
  - Control
    - **Beacon**
      - Network presence
      - Association params
      - **Synchronization**



Introduction: Beacons

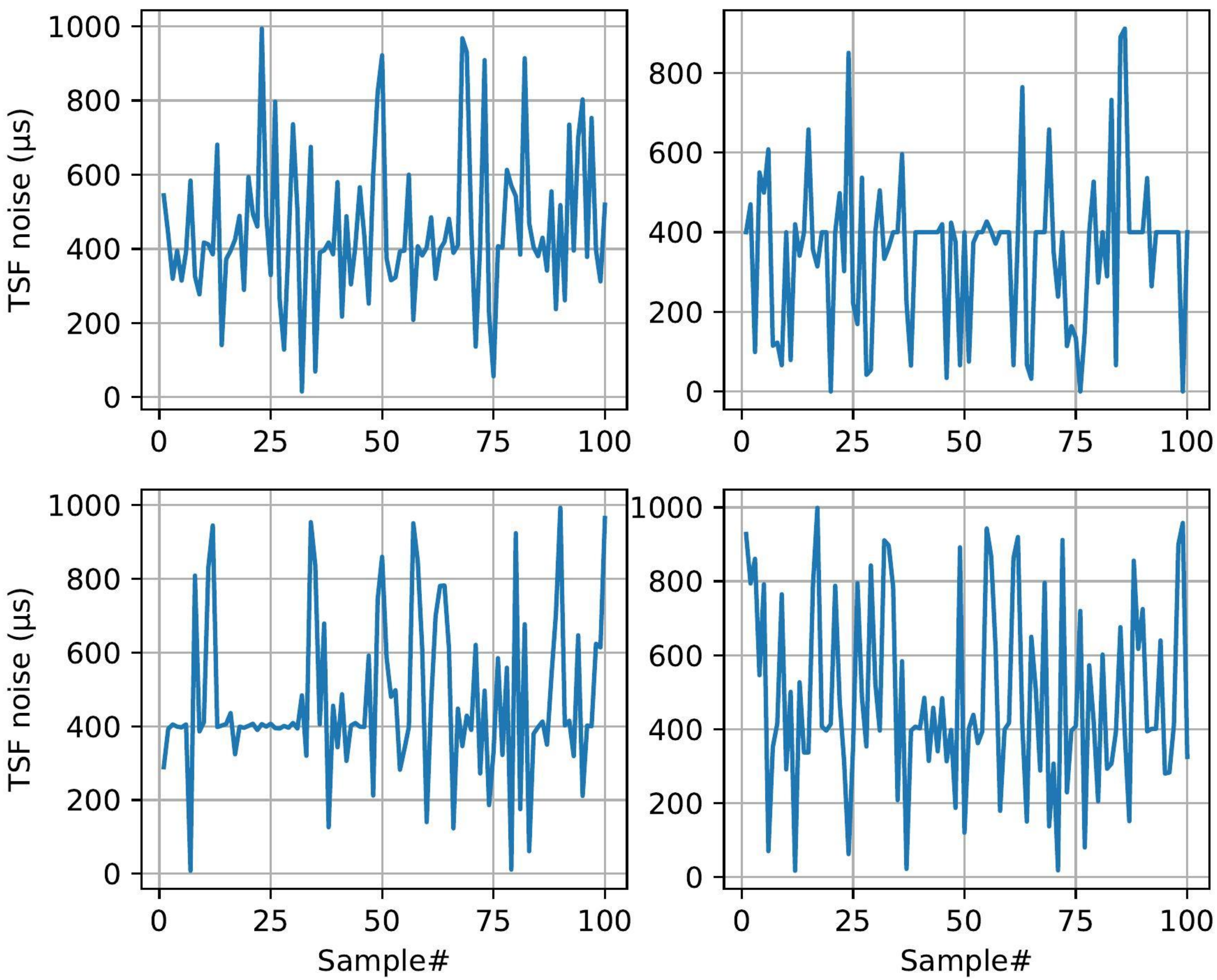


$$\boxed{ts_{i+1} = ts_i + TBTT}$$

TSF noise (μS)

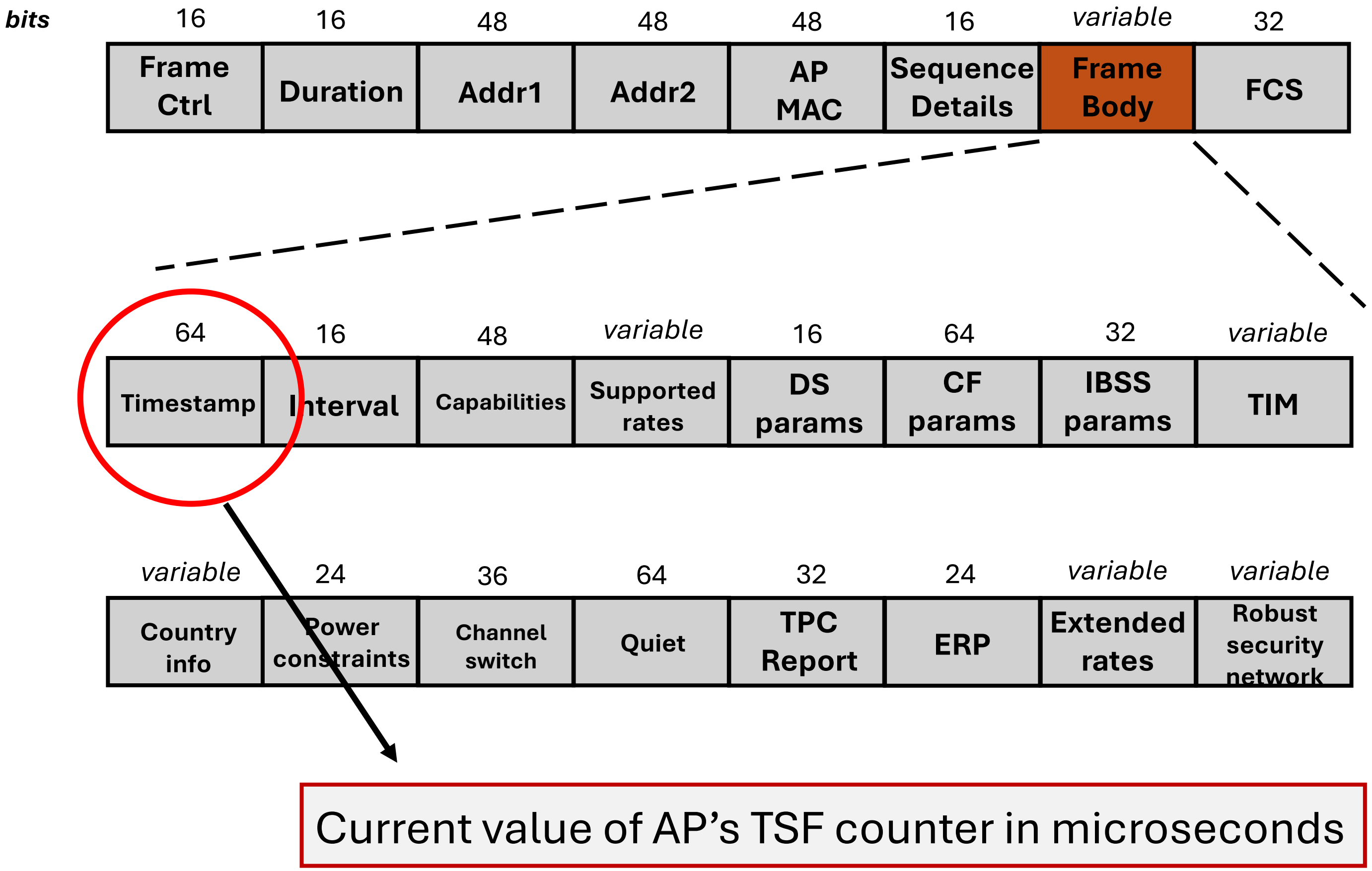
$$\boxed{ts_{i+1} = ts_i + TBTT + \varepsilon}$$

Beacons: Implicit Periodic Noise

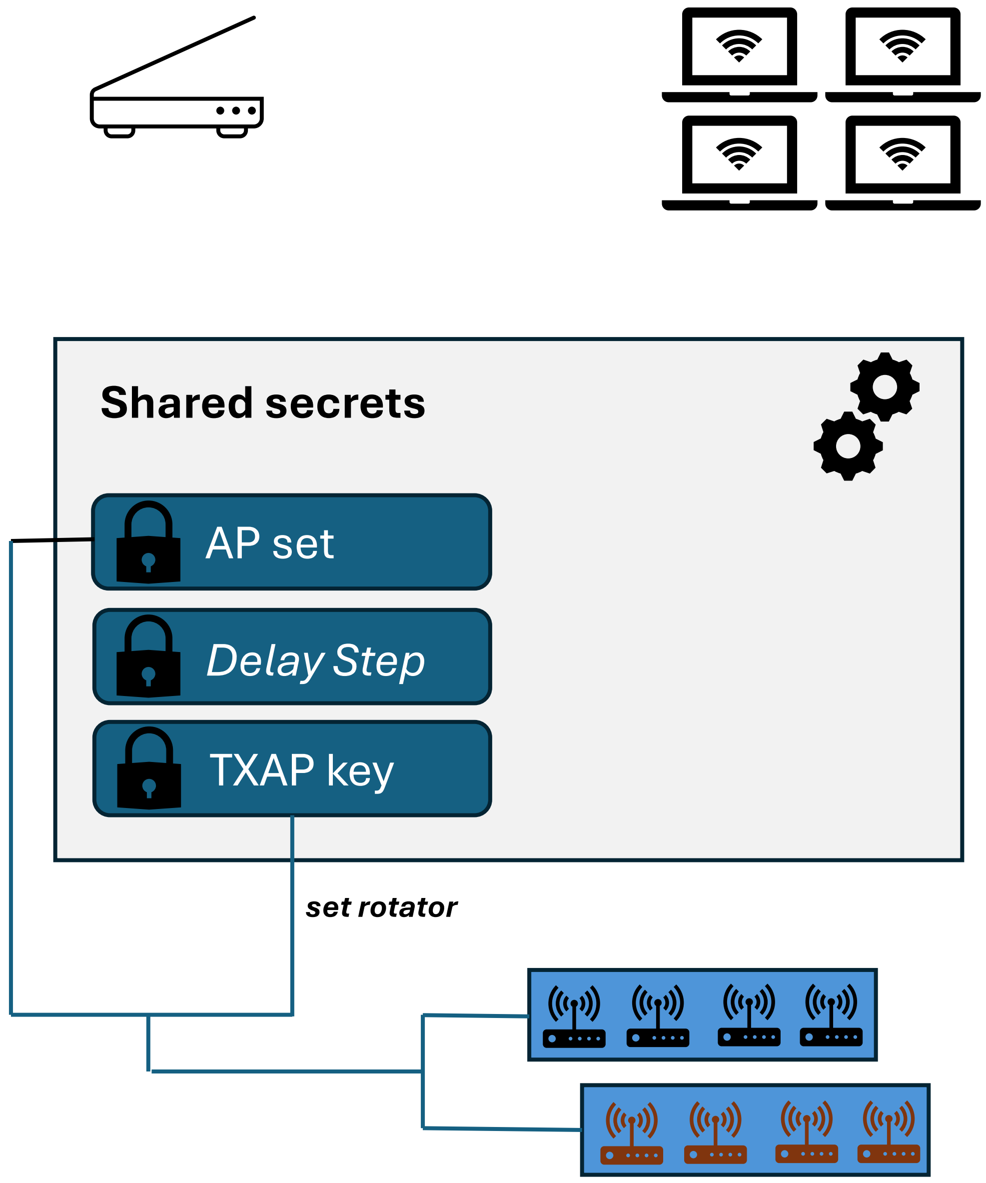


Time Synchronization Function

- TSF: Unique characteristics
    1. Periodic transmission
    2. Mirrored resolution

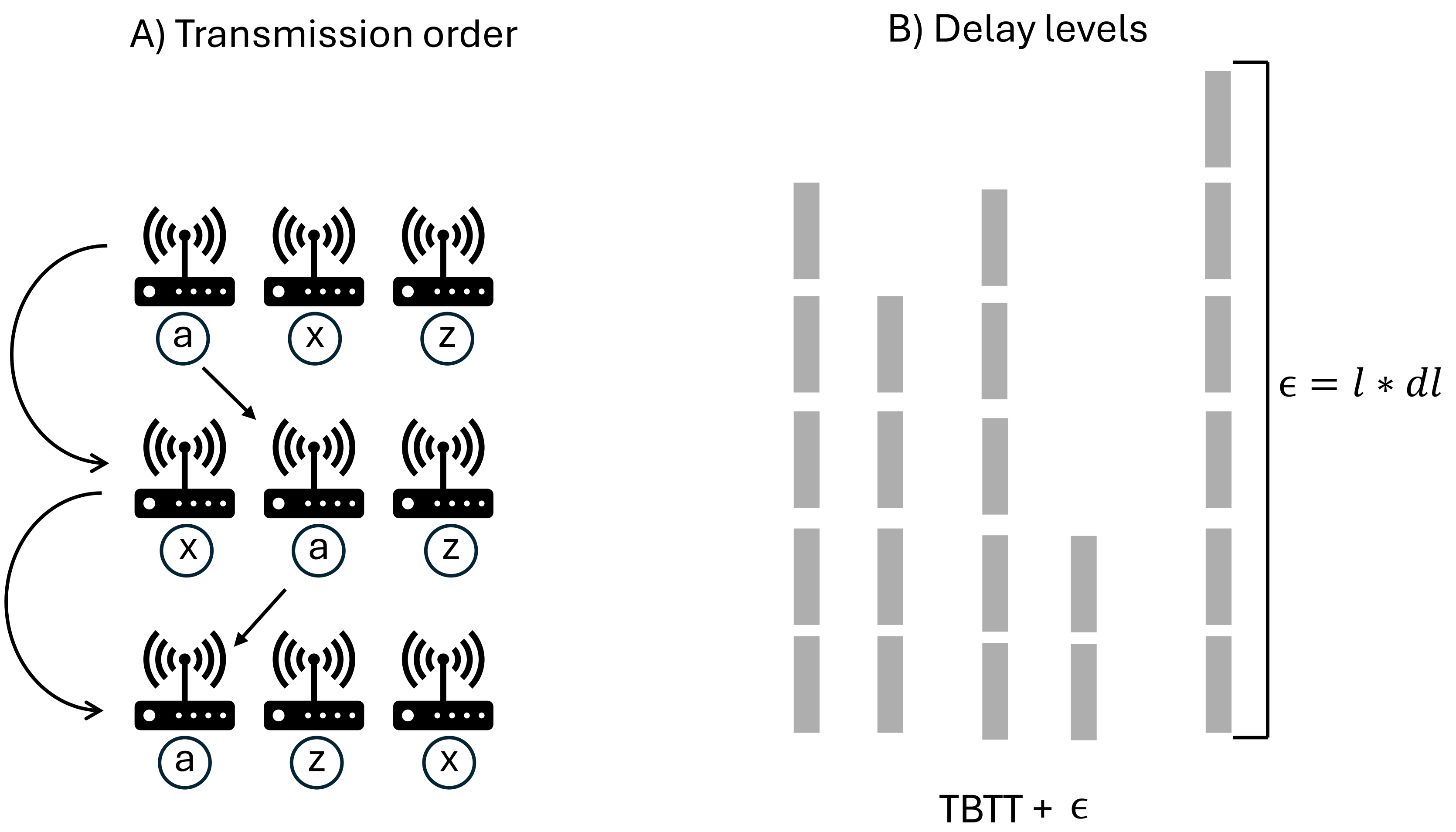


CHAOS: Communication Model



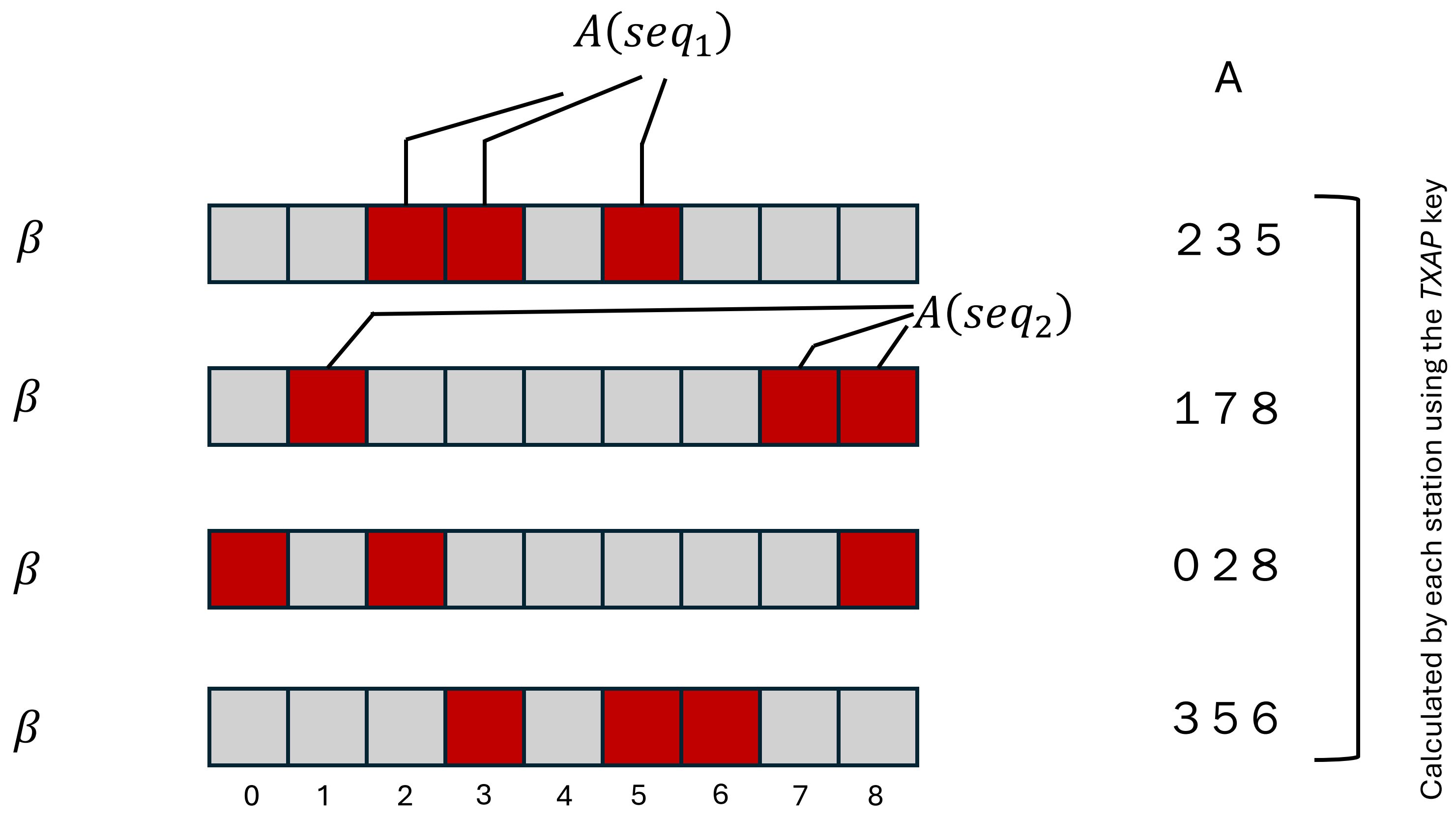
CHAOS: Communication Model

- We Broadcast covert payload through mapping a bit stream in a secret permutation space
- We make use of two permutation components:



CHOAS: Statistical Adaptation

- CHAOS APs blend in the crowd
- We created *TXAP rotation* in CHAOS to make the generated TSF noise, statistically look like ambient TSF
- Modify ***A*** assignments at each burst
- Missed frames are handled through burst synchronization



Experimental Results: Bandwidth

- Theoretical bandwidth is a function of TXAP set size and delay levels
- In practice, burst recovery affects bandwidth due to missed frames
- Frame miss rate is directly affected by the burst size (n).
- Using regular consumer grade NICs, a burst size of 6 yielded promising results.

Sample permutation config

$$n = 6$$

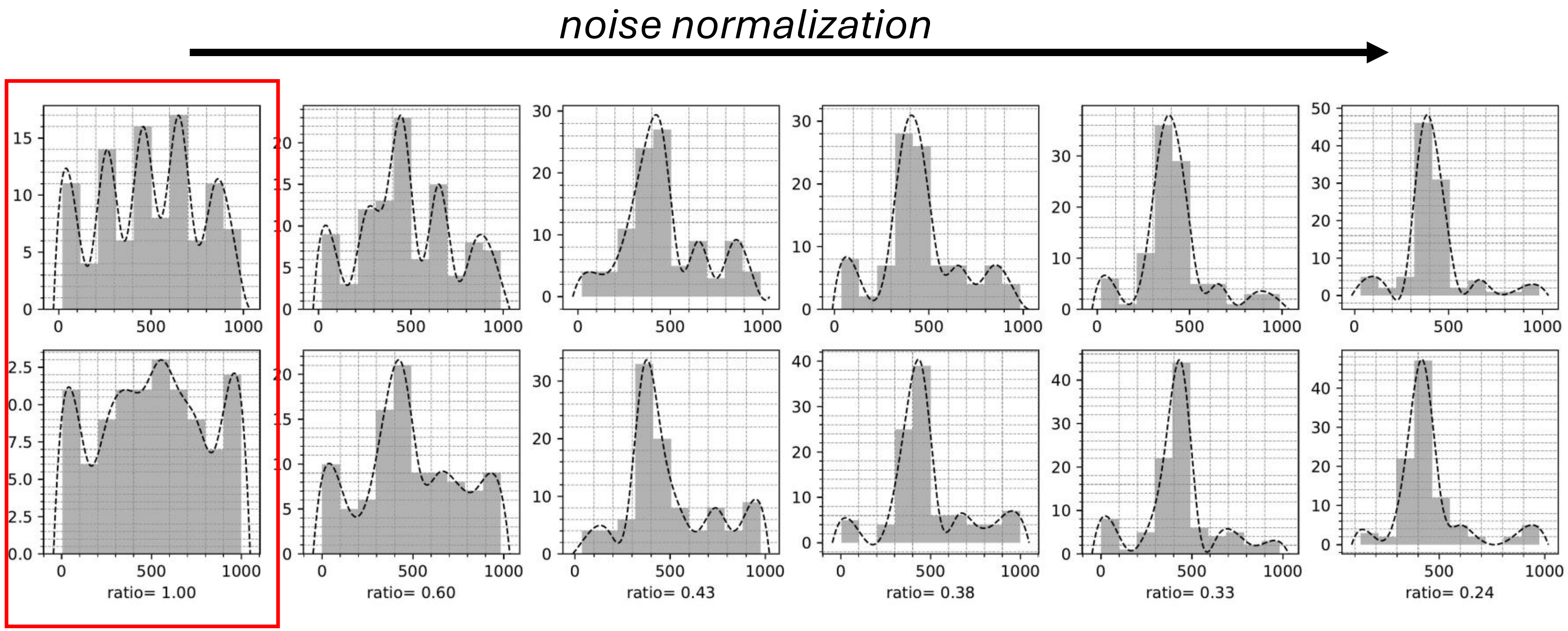
$$L = 216$$

$$|S| \simeq 73\ trillions$$

***520** bits/sec*

Experimental Results: Detection

- CHAOS employs TXAP rotation to increase costs of adversarial measurements to detect the Aps
- Noise distribution tends to project a normal distribution as seen in regular background noise
- The distribution is easily adaptable on-demand



Mitigation

- It is a design issue
- Neither TSF nor beacons can be disabled
- Not user controllable
- Any change requires firmware patches
- Potentially a different TSF synchronization strategy
- It does also have important positive uses

Other Side Effects

TSF statistical distribution is affected by environment radio traffic

TSF can be exploited to mount correlation attacks to map users to physical access points

Also See

More technical details, PoC examples:

Refer to my blog

https://bitguard.wordpress.com

Get in touch:
sirus.shahini@gmail.com

Questions?

Thank You!