ICMP Based Covert Channel

Mathieu Bangma (s1017020)
Tijn Berns (s1027659)
Bart Janssen (s4630270)

Timing Based Covert Channel

- Based on intervals between received packets
  - Sender modulates wait time between transmissions
  - In our case PING packets
- Requires agreements between sender and receiver
  - Receiver must know how to decode intervals

How do we encode a string?

String to Time-Intervals (sender)

Attack At Dawn!

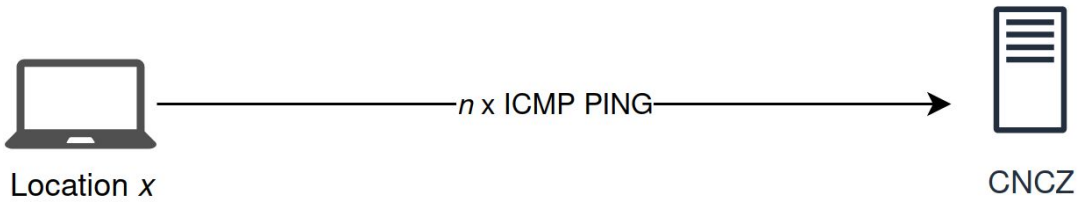
1. Convert input to lower space and remove special characters
2. Convert to ascii and subtract 97
3. Convert to given base (7)
4. Prepend 0's to ensure equal length
5. Convert strings to single integers
6. Center values around 0, multiply with delay (10), and add 1000 ms

1. attackatdawn
2. [0 19 19 0 2 10 0 19 3 0 22 13]
3. ['0' '25' ... '31' '16']
4. ['00' '25' ... '31' '16']
5. [0 0 2 5 ... 3 1 1 6]
6. [970. 970. ... 980. 1030.]

Setup & Demo

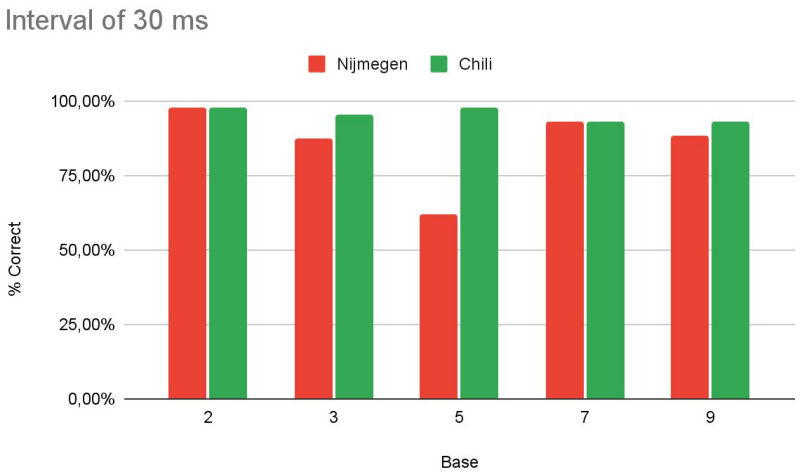
- Sender and receiver at different networks
  - **Receiver:** CNCZ server located at RU
  - **Sender:** Local terminal (15 hops from receiver)

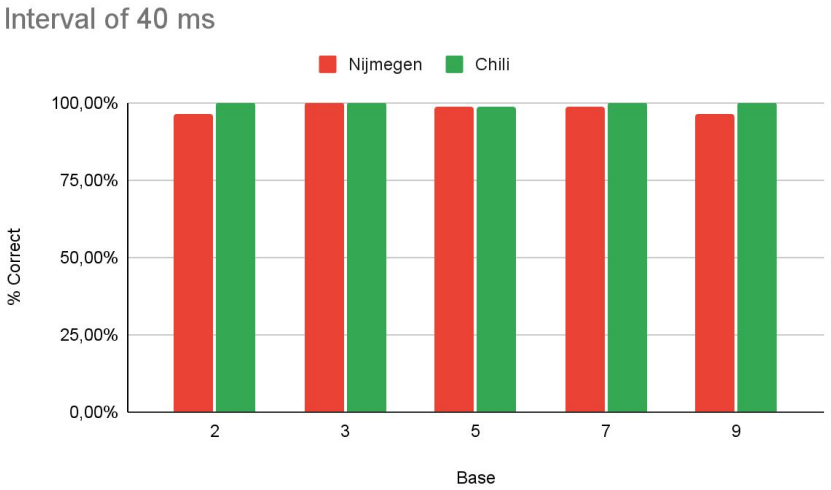
- Demo: Attack At Dawn!



Correctness

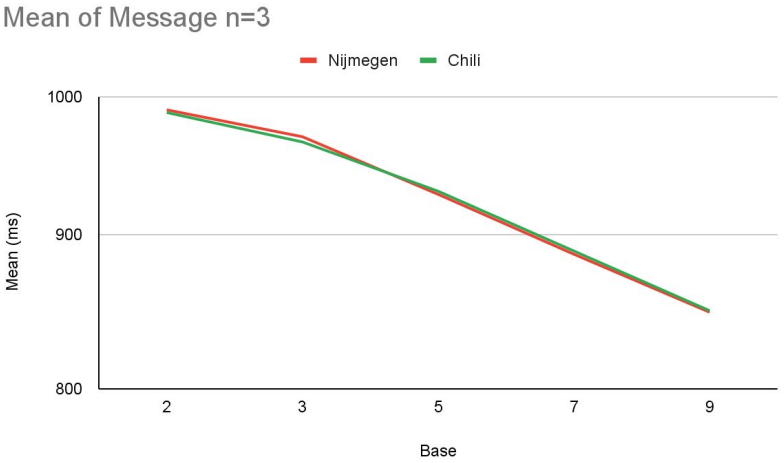
- Send from Nijmegen & Chili (VPN)

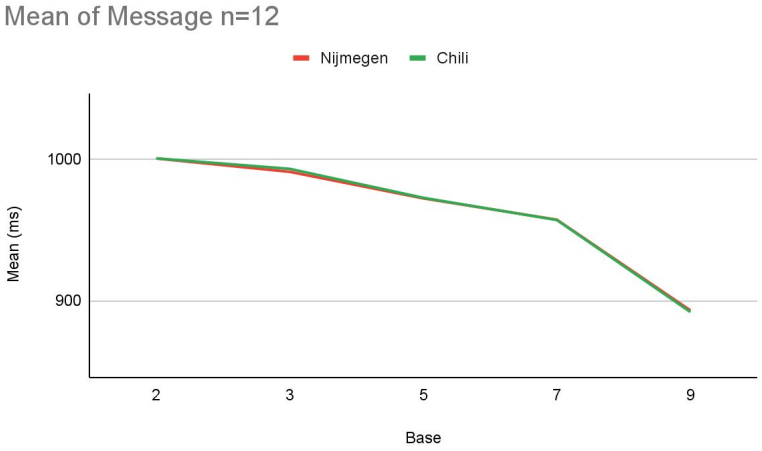


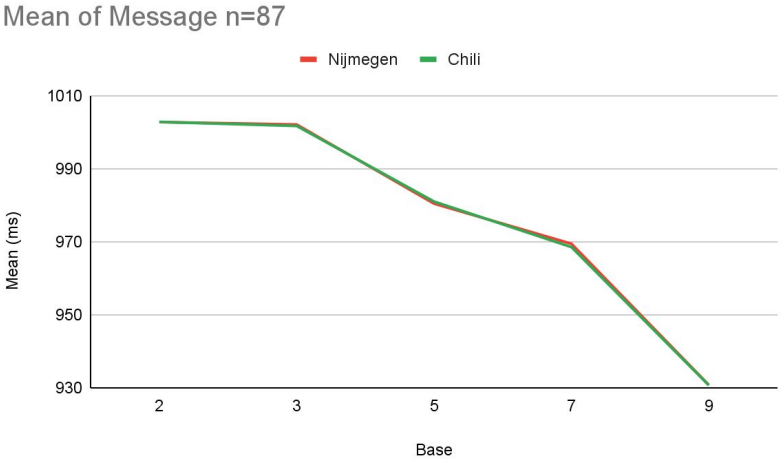


Mean Interval of the Ping Packets

Target mean ≈ 1000 ms

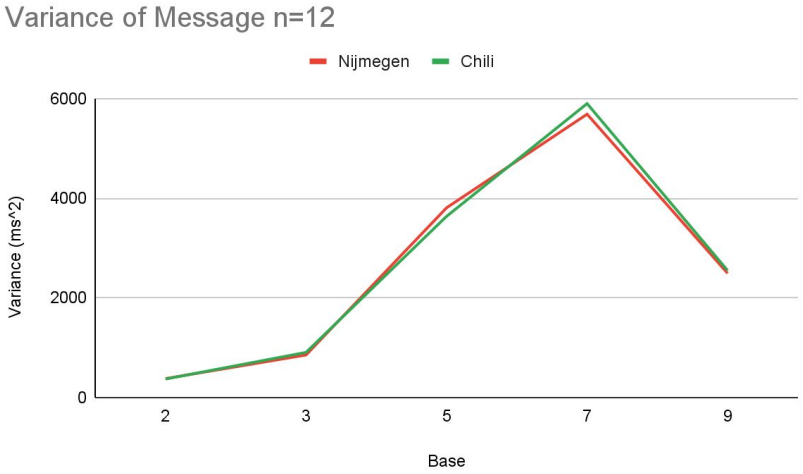


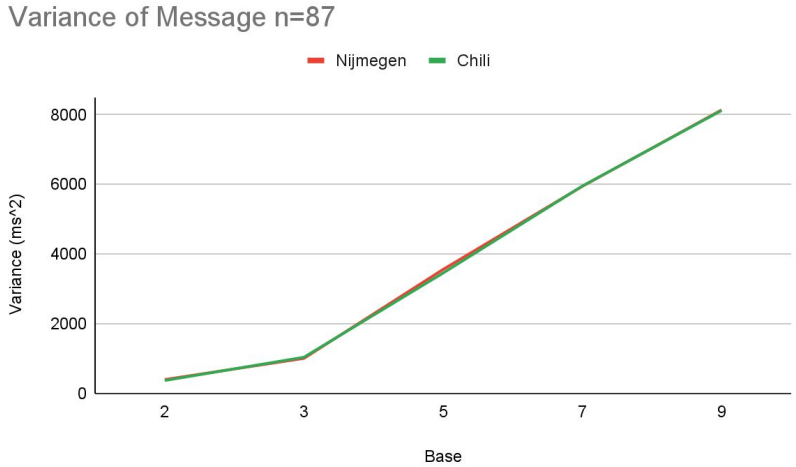




Variance of the Ping Packets

Target variance ≈ 20 ms^2





Discussion

- Detection:
  - Variance
  - Many ping packets
- Limitations:
  - Speed (1 bit / second for base 2)
- Future work:
  - Encryption to more evenly distribute the intervals
  - Checksum for correctness / validation

Questions?