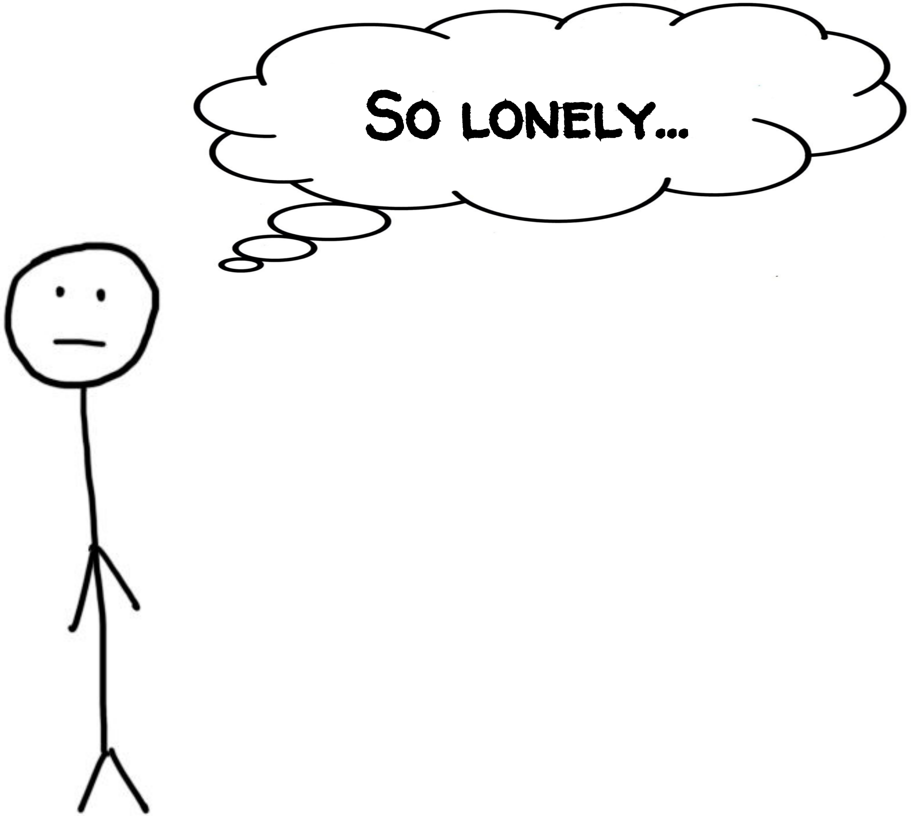
Deniable Liaisons

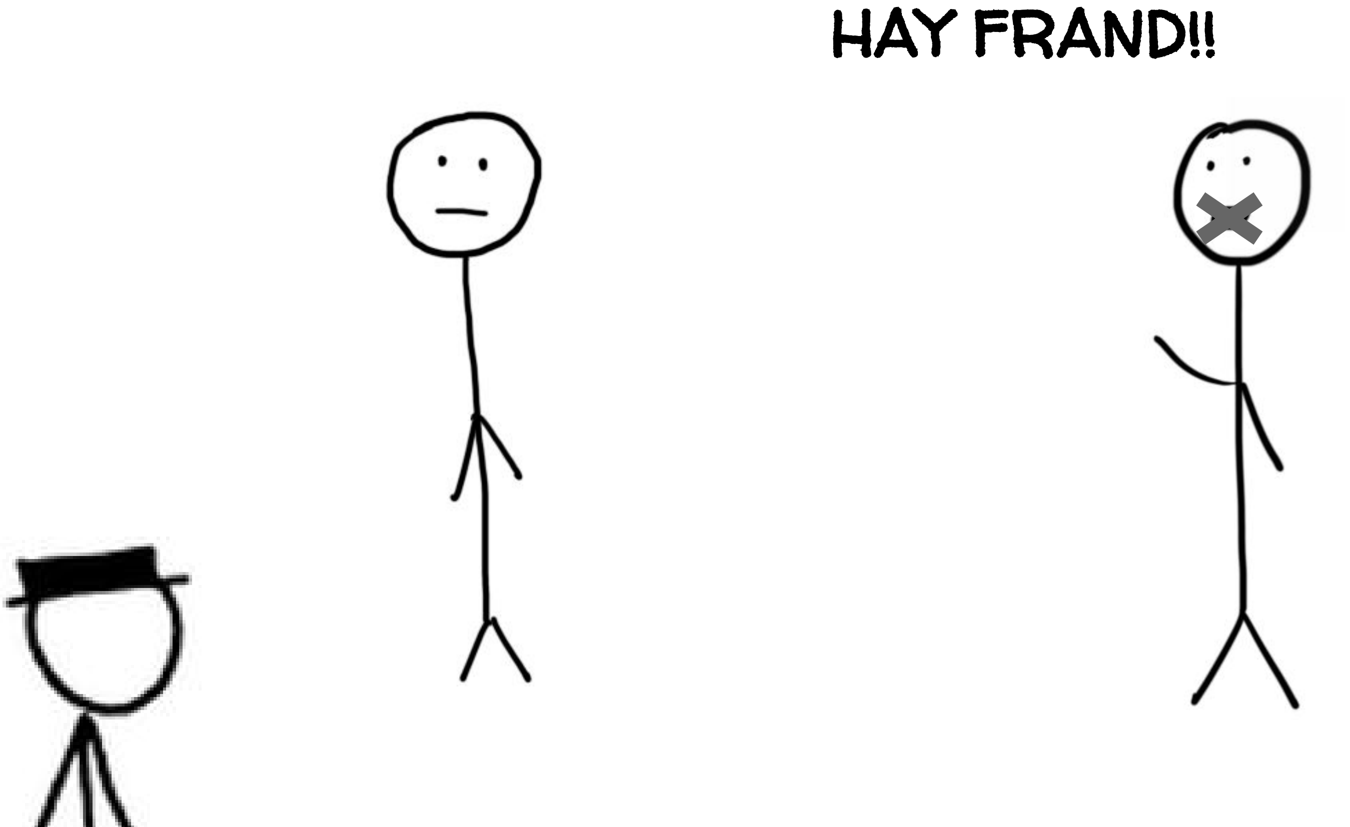
Abhinav Narain, Nick Feamster, Alex C. Snoeren
Presented by: Daniel Suo

Background

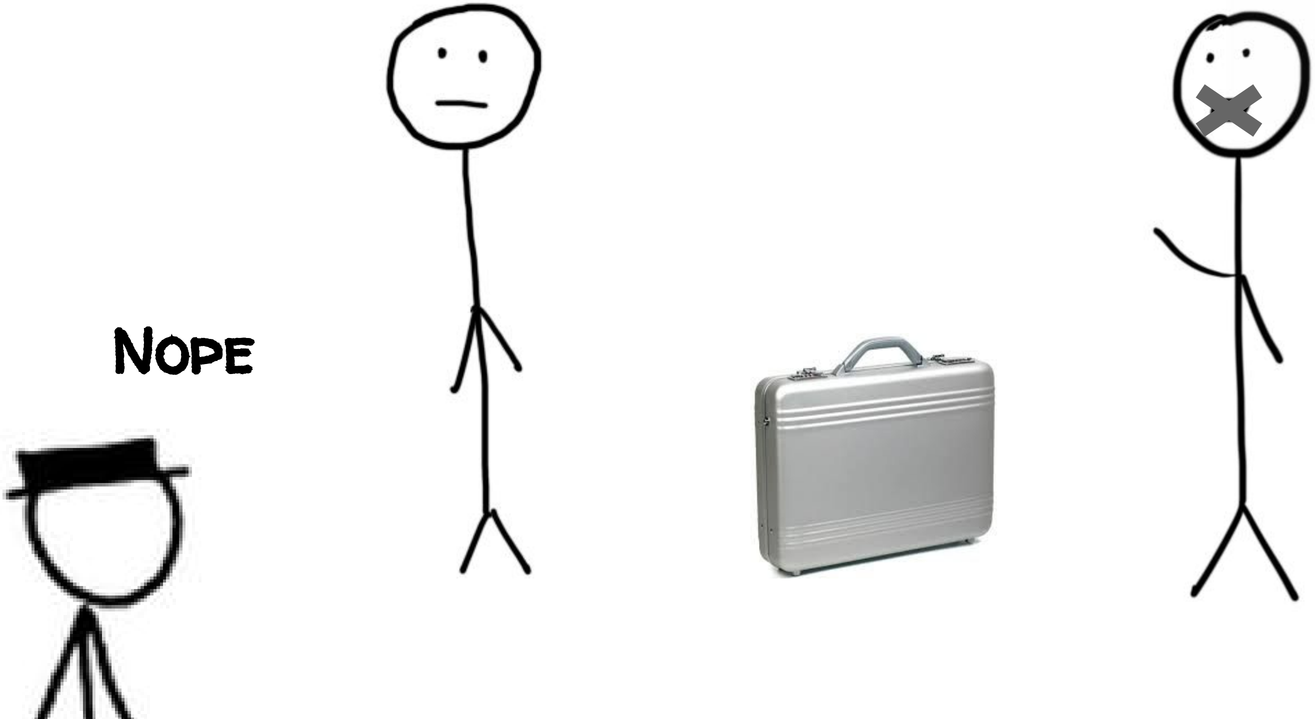
User scenario



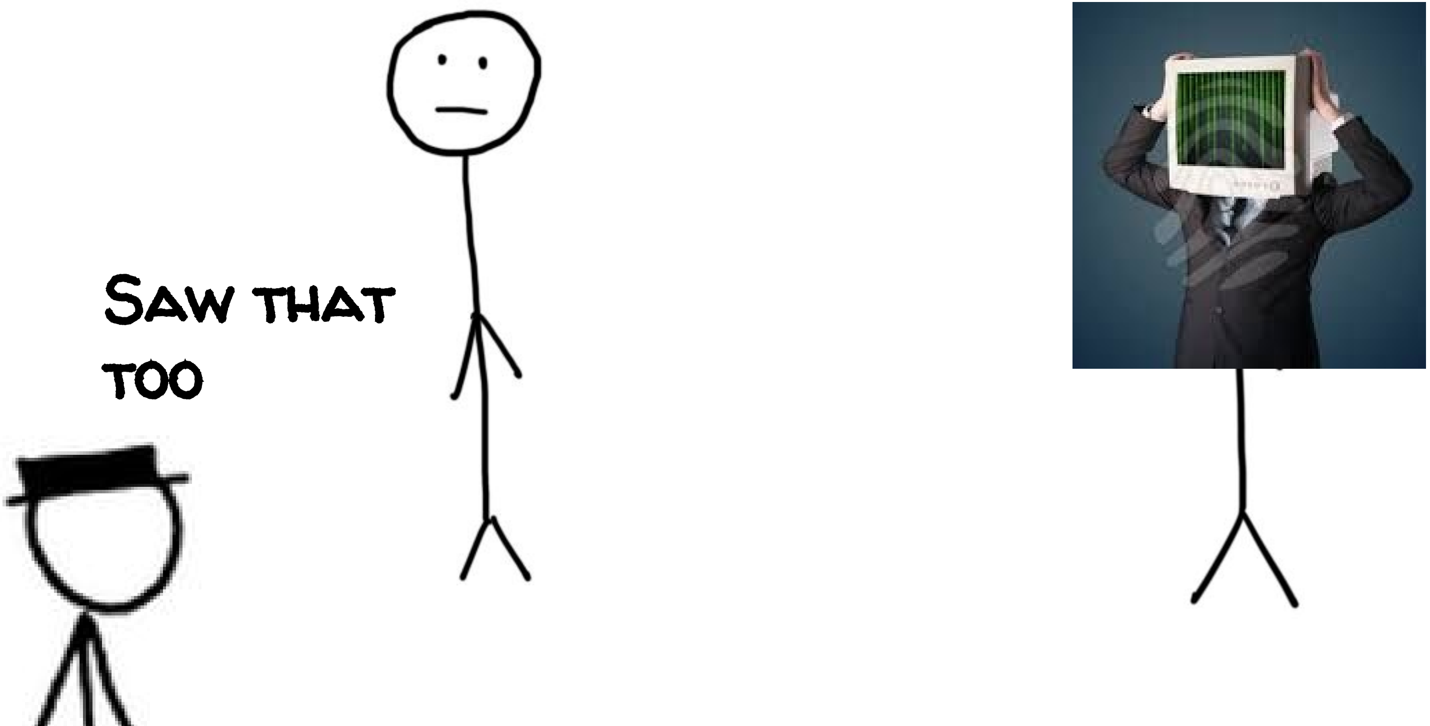
User scenario



User scenario



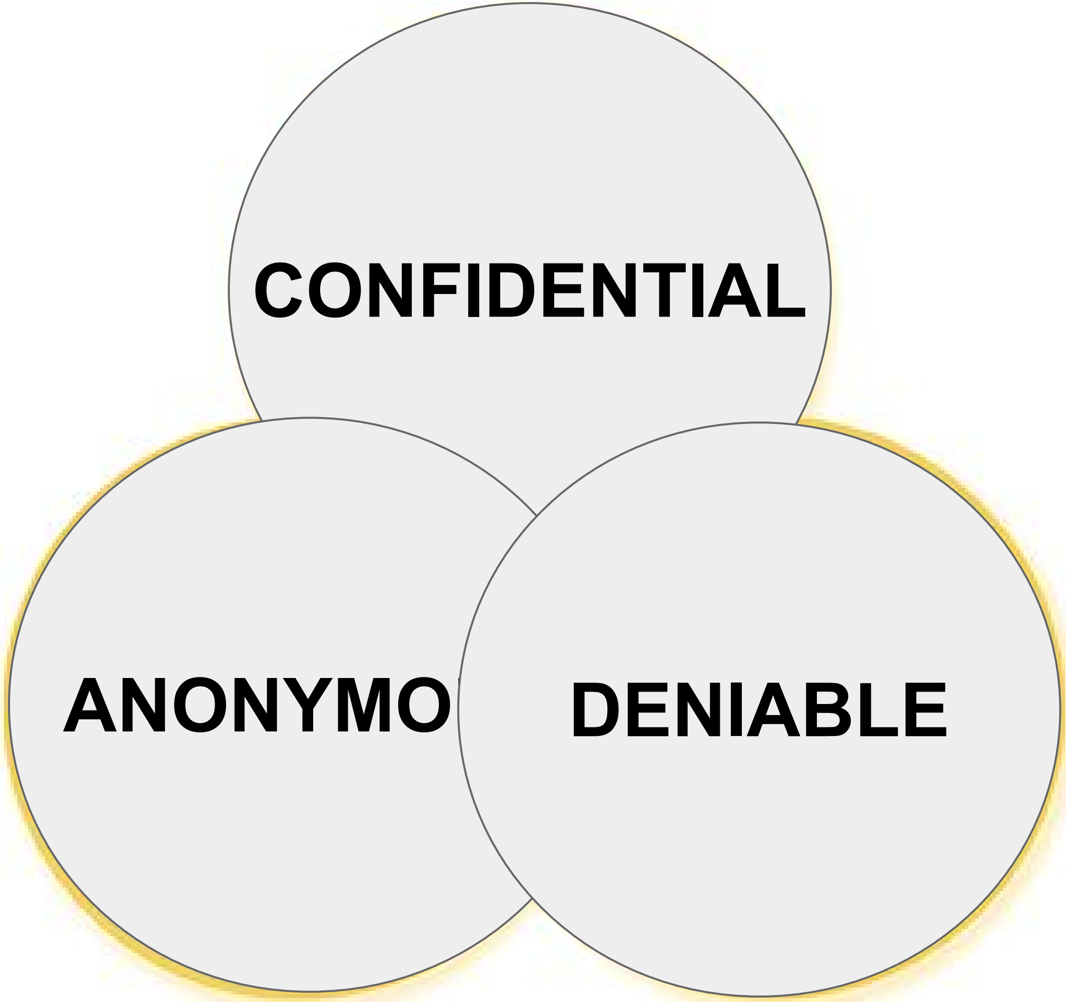
User scenario



Sorry, bro

That's Philipp Winter ->


MSNBC
MAY 31, 2011
NATION
TAMRON HALL
NAS 2792.69
msnbc
MOMENTS AGO
DEVELOPING NOW
REP. WEINER: LEWD PHOTO TWEETED WAS FROM HACKER
TOP STORIES


CONFIDENTIAL
ANONYMOU
DENIABLE

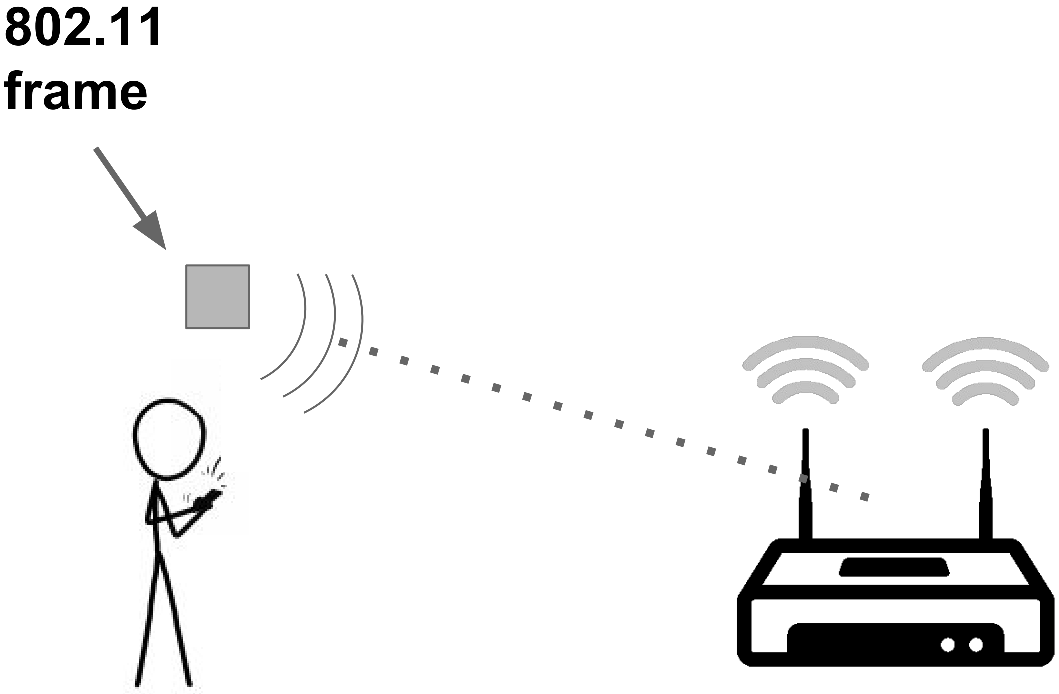
This one's too easy... Use your imagination.

DenaLi (Get it?) Overview

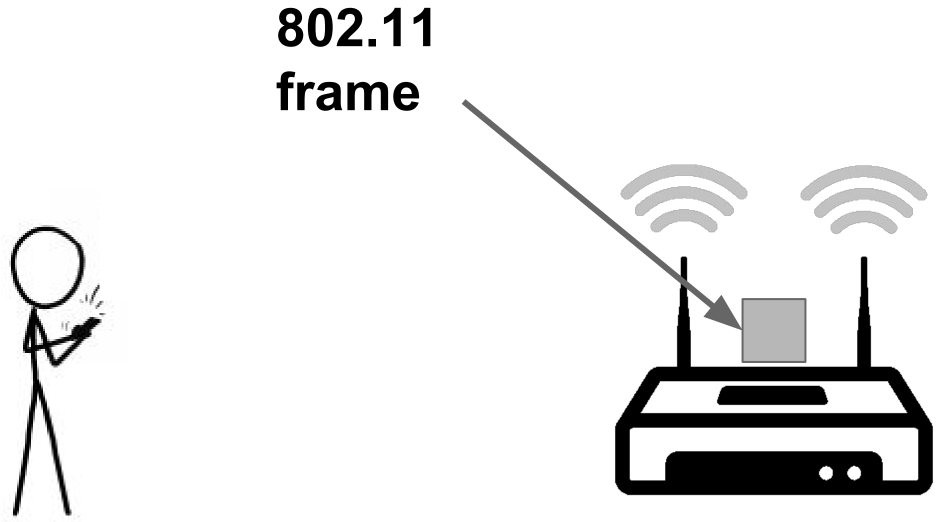
Deniable Liaisons: insights

1. Wireless everywhere
2. Wireless frames are often corrupted
3. Can hide messages in corrupted frames

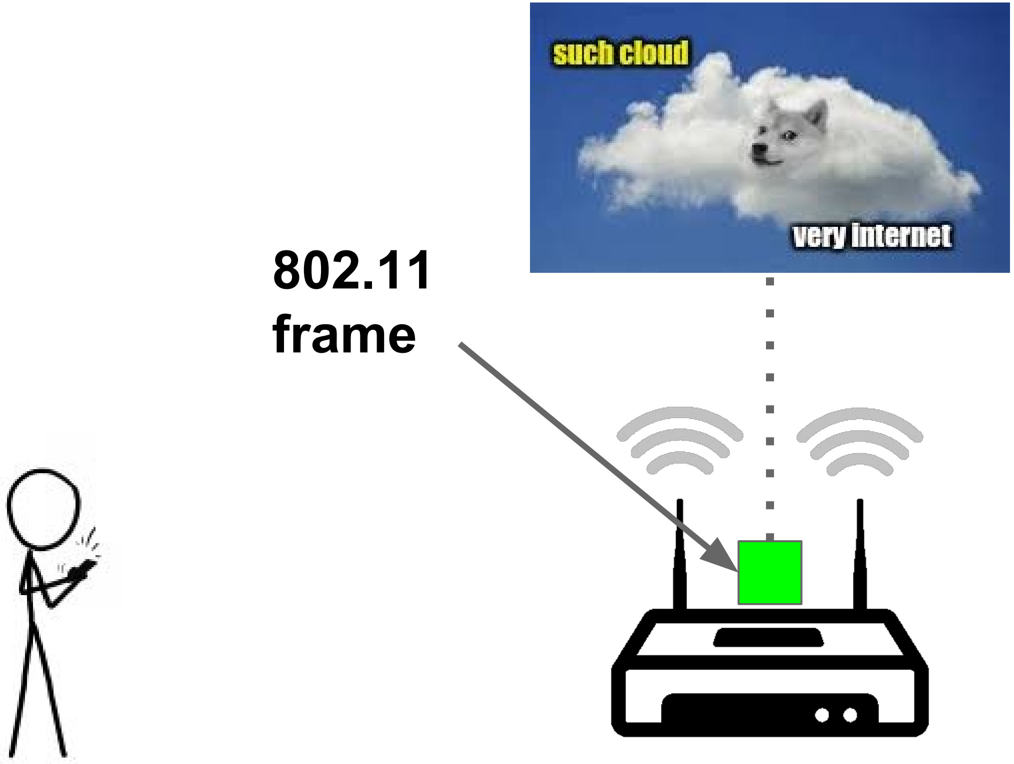
Deniable Liaisons: basic approach



Deniable Liaisons: basic approach

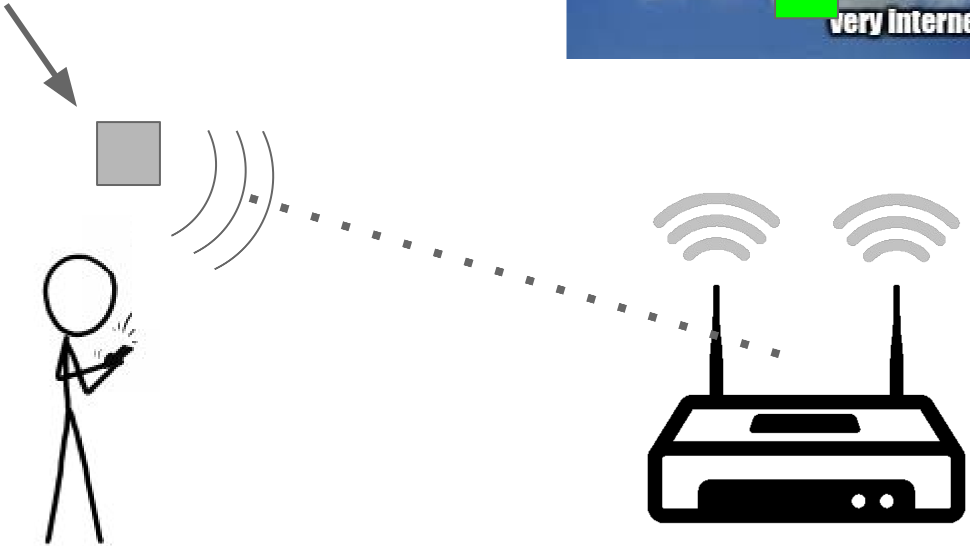


Deniable Liaisons: basic approach



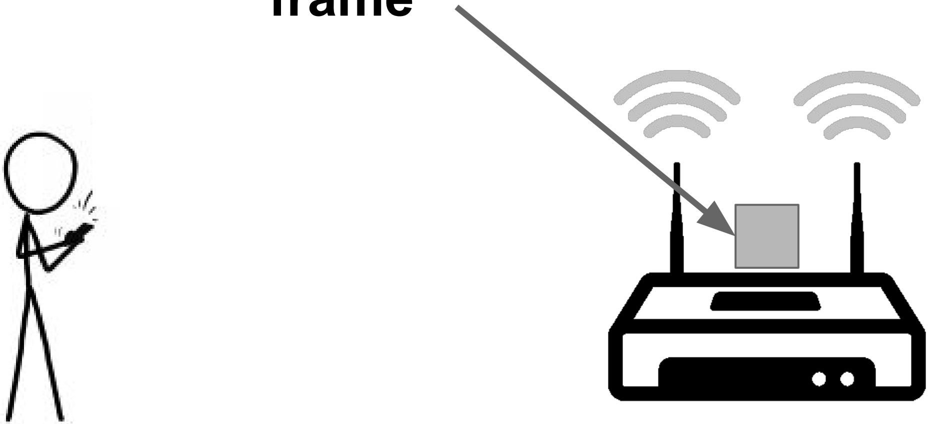
Deniable Liaisons: basic approach

802.11 frame

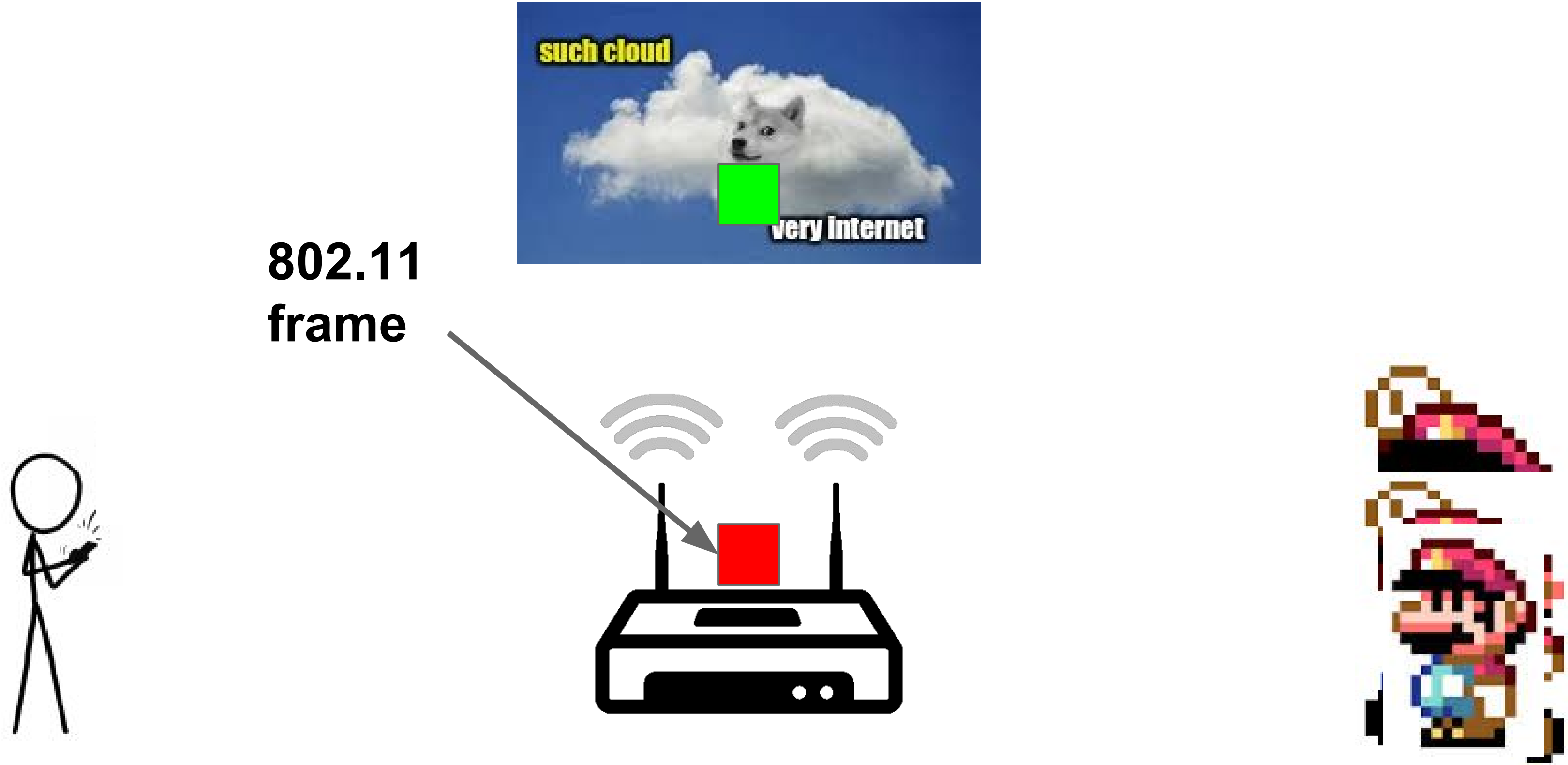


Deniable Liaisons: basic approach

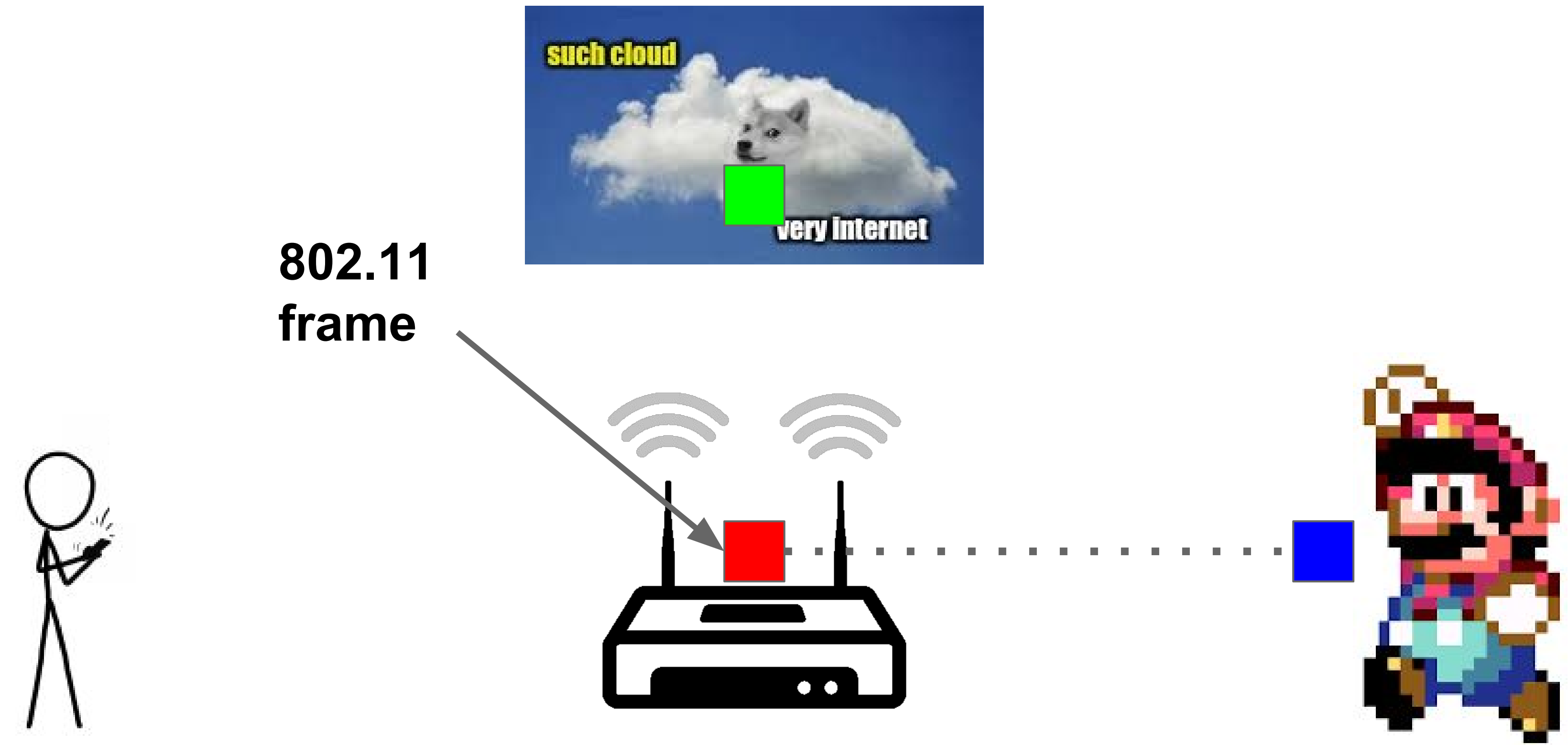
802.11 frame



Deniable Liaisons: basic approach



Deniable Liaisons: basic approach



Deniable Liaisons: Challenges

- Anonymity and confidentiality are easy
- Deniability is hard; have to make resulting stream deniable
  - Frequency of corrupt frames
  - Bit positions within the frames that are corrupted

Deniable Liaisons: Threat model

- Goal: detect presence of hidden communication on shared wireless medium
- Capabilities
  - Listen to wireless frames within radio range
  - Finite computational resources (prototype uses one laptop)
  - May know user’s identity, but not MAC address
  - May also monitor from multiple points

The Nitty Gritty

Injecting corrupt frames

- Injecting frames
- Establishing a shared session
- Encoding and transmitting
- Receiving and decoding

Injecting corrupt frames

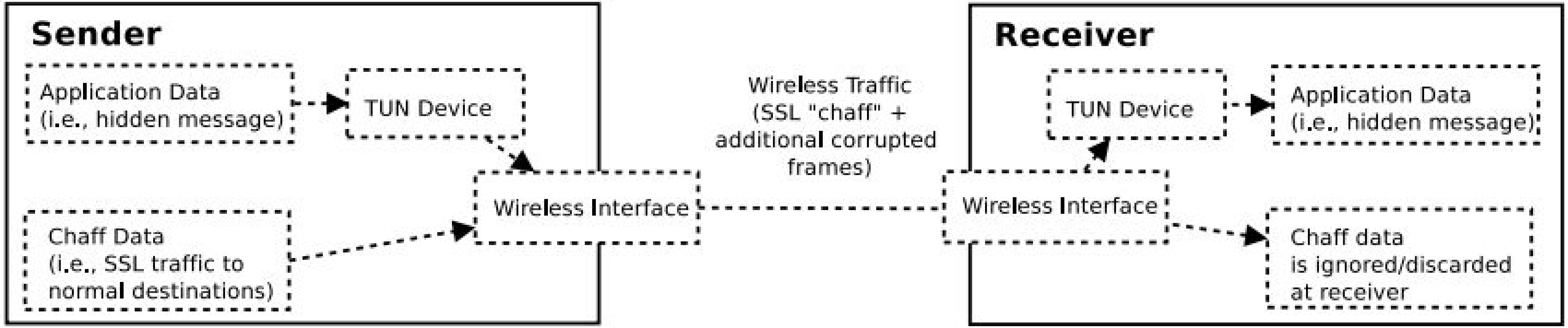


Figure 2: *Injection of additional corrupted frames via a virutal network interface (implemented as a Linux TUN device).*

Injecting corrupt frames

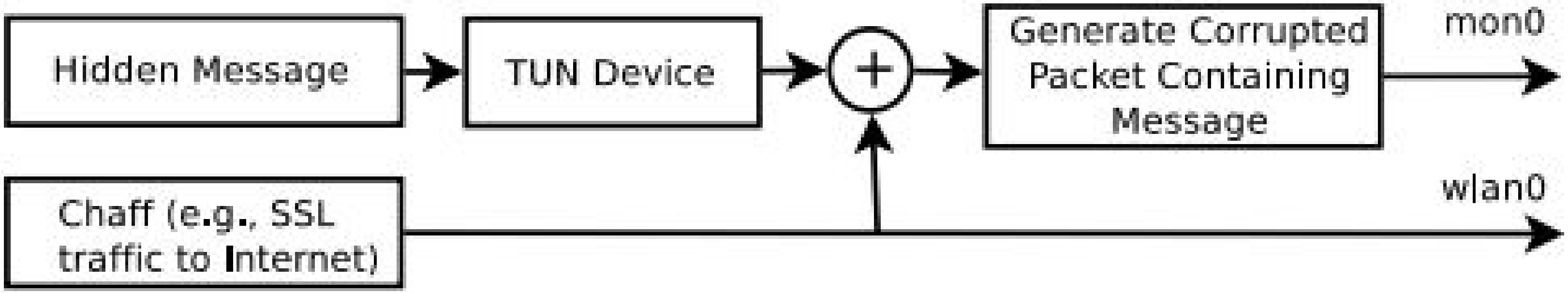


Figure 3: *Process of injecting corrupted frames at the sender; the receiver performs the reverse of this process.*

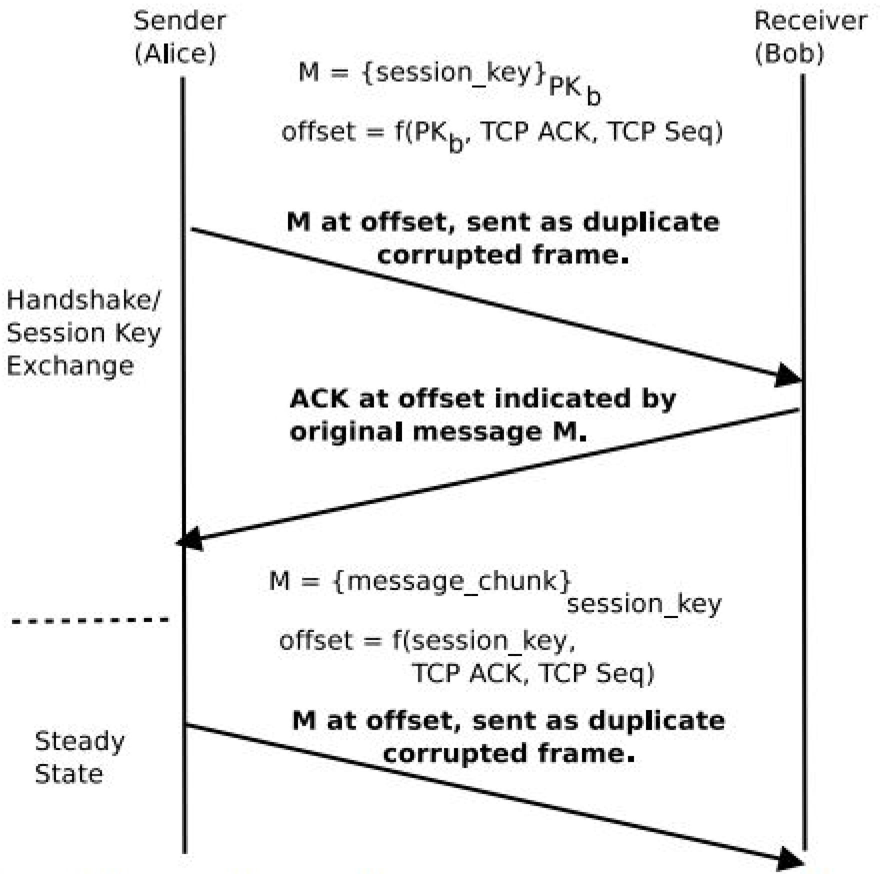


Figure 4: *Steps involved in exchanging messages using corrupted frames.*

Protocol: Encoding and transmitting data

- When message is ready, duplicate a frame
- Encrypt message with session key
- Compute offset in frame
- Compute HMAC on ciphertext

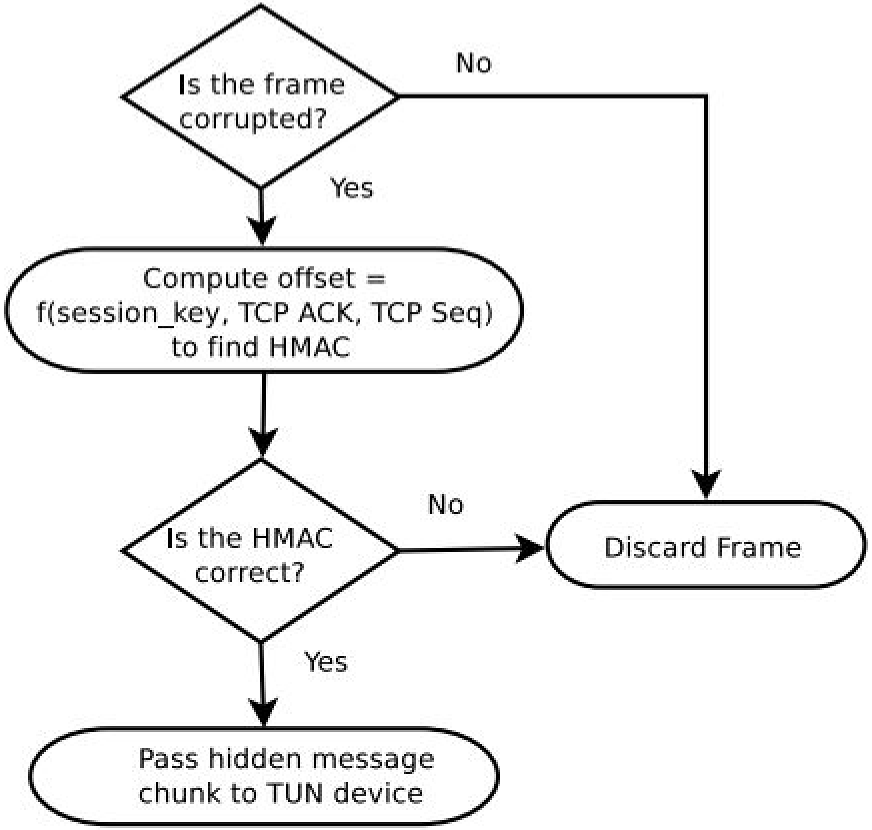


Figure 5: *Checking the integrity of received hidden messages.*

The Prototype

Main things

- TUN interface
- Disable FCS checksum (calculate ourselves)
- Disable retransmission

Evaluation

Data an attacker can collect

- Frame sequence
- Bit patterns within each frame
- Shady activity

Definition of deniability

$$P(tell\ difference) = 1/2 + \varepsilon$$

Definition of deniability

Pearson's coefficient (aka that *r* thing that goes from -1 to 1)

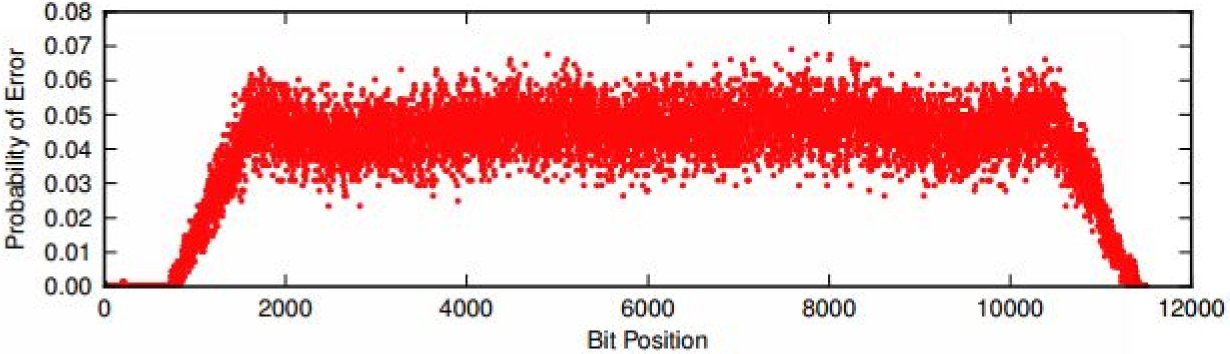
$$\varepsilon = 1/2 - \frac{cov(f(x), f'(x))}{2\sigma_{f(x)}\sigma_{f'(x)}}$$

Definition of deniability

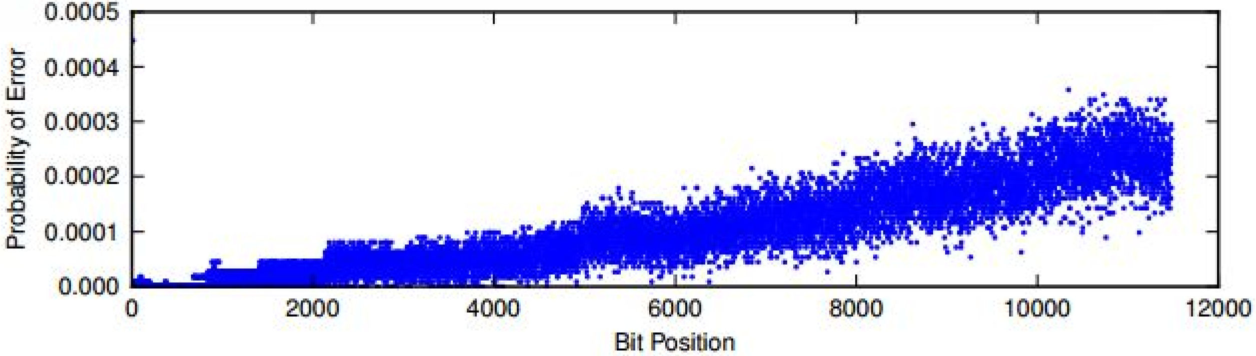
Correlation (r)	Epsilon (½ - r)	P(gotcha) (½ + e)
1	-½	0
0	½	1
-1	1 ½	2

Definition of deniability

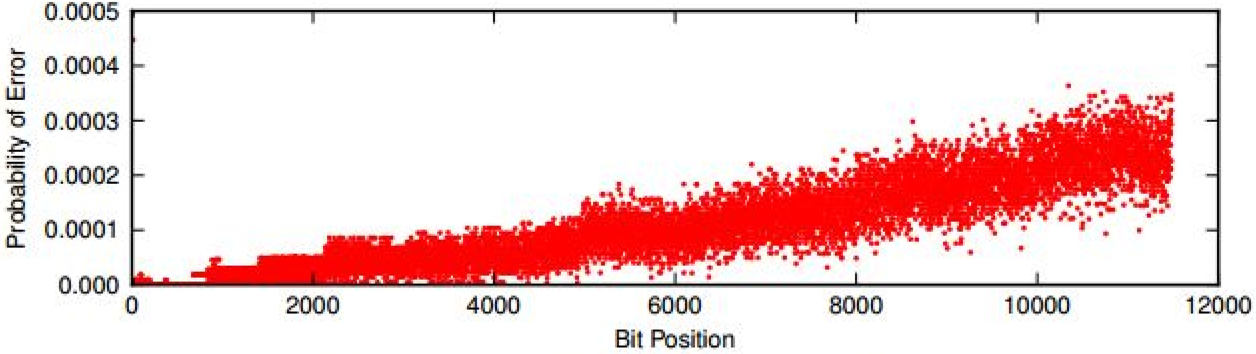
- For packet error rate
  - Actually, just make this constant. Derp?
- For bit error distribution
  - Calculate correlation on where bit errors within a frame occur over a sequence of frames



(a) *The bit-error distribution from the perspective of the DenaLi sender, given a 23 KB message and a 70-byte TUN MTU.*



(b) *Natural bit error distribution.*



(c) *The bit error distribution after the DenaLi perturbation from (a) is added.*

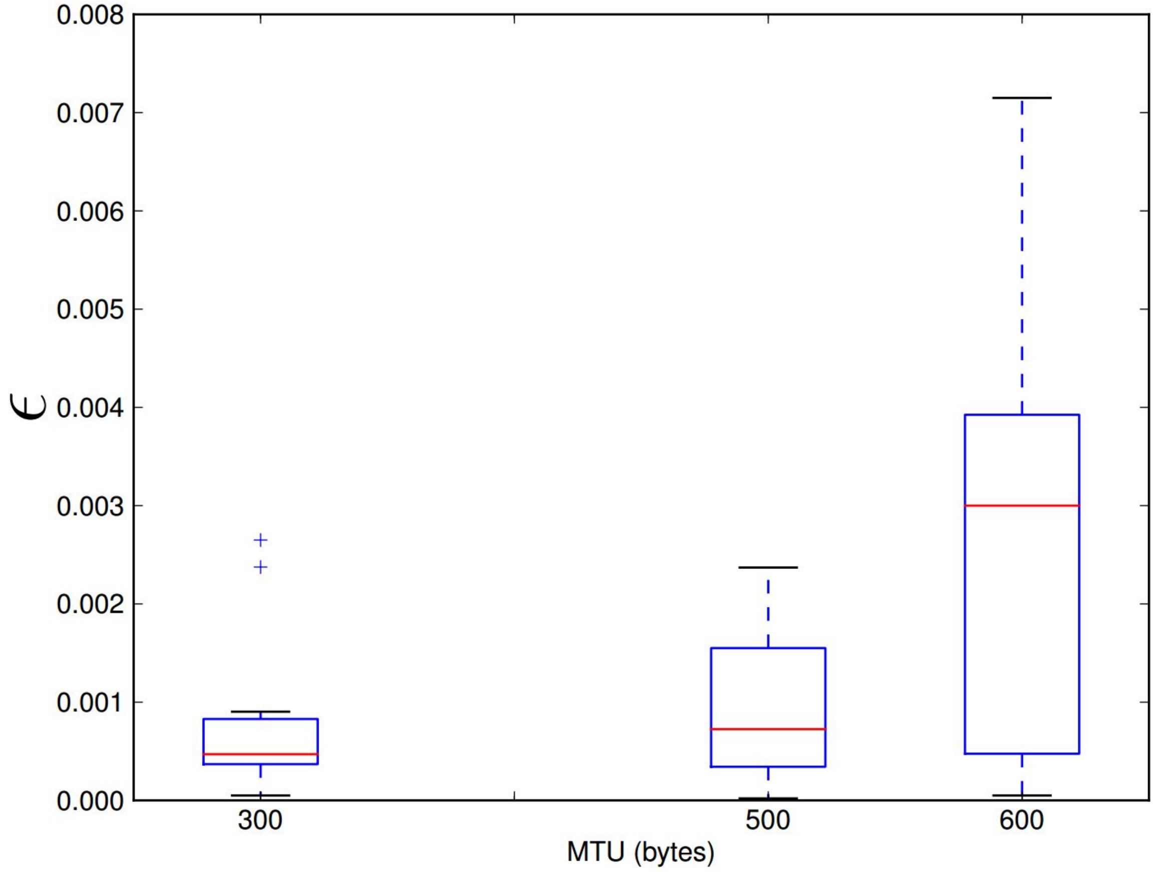


Figure 8: ε *vs. TUN MTU* (i.e., *injected frame size). We varied MTU sizes to achieve different throughput. Large TUN MTU values result in larger* ε *values and are less deniable.*

BER	PER	Throughput (bps)
10^{-4}	0.7	427.4
10^{-5}	0.1	103.6
10^{-6}	0.05	42.98

Table 1: *Bit error rates, approximate corresponding packet error rates assuming 1500-byte packets, and the resulting DenaLi throughput given a 70-byte TUN MTU. We test a range of bit error rates that are observed in practice [14].*

Future Work

The future

- Coping with limited bandwidth
- Analyzing adaptive bitrate algorithms (aka another observations we need to counteract)
- Timing attacks
- Transport layer (TCP on top of DenaLi)
- Mobile devices
- Multi-hop networks

Unsolicited Opinions

Strengths

- Doesn’t require special equipment (sort of)
- Takes advantage of environment
- Decoupled

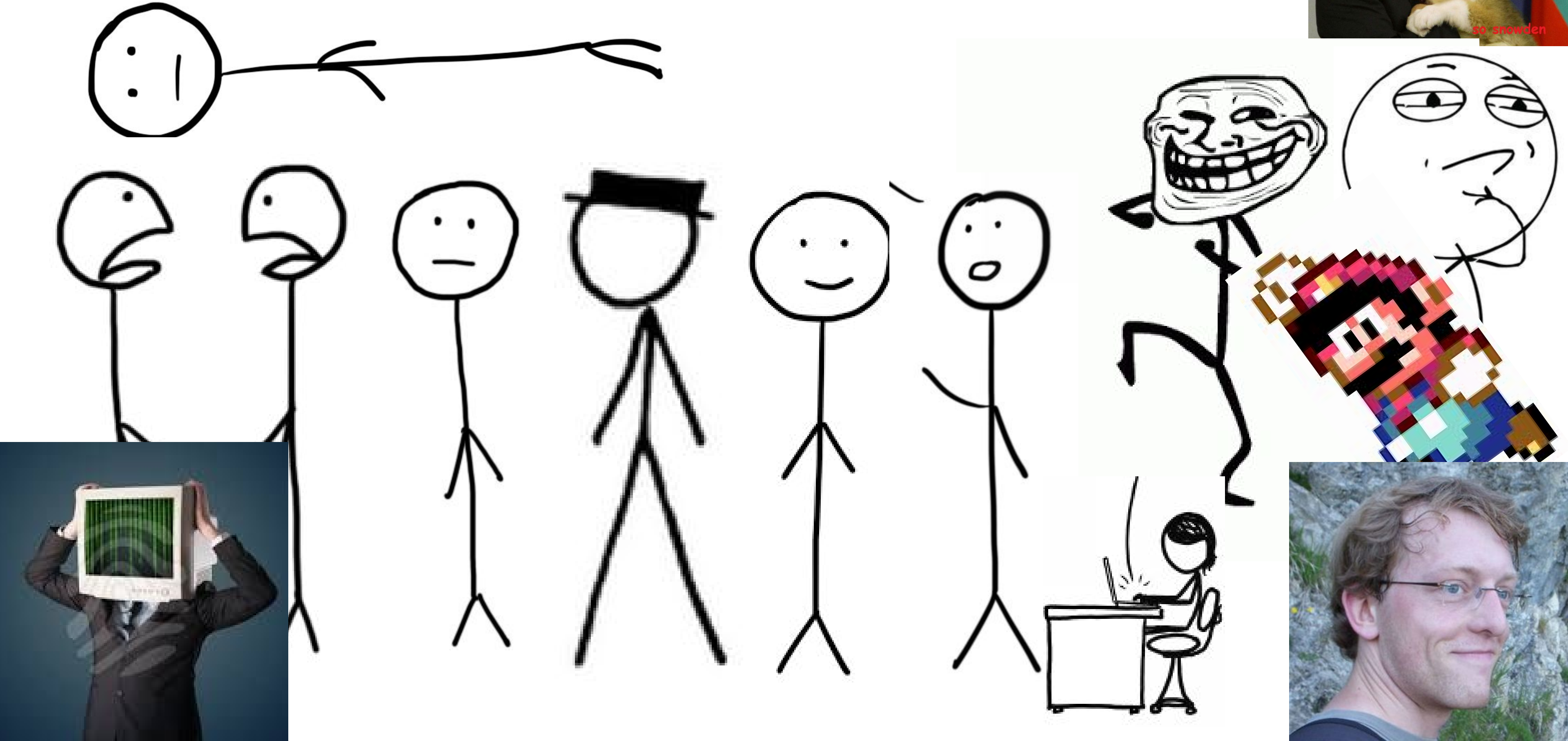
Possible weaknesses

- Have to be physically close
- Attacker can’t be too close
- Relies on 802.11
- What about other patterns / attacks?

Unsolicited opinion: A lot of things have to go right

- Dude, just log on to StarBucksCheepInternet
- What was your public key again?
- Can you hear me now?
- Stop looking at me!

Cast (Courtesy of Wait but Why, XKCD, and The Internet)



Brought to you by: The NSF