Steganography Assisted Tor

Michael Freyberger
ELE 454 Spring 2015
Prof. Prucnal

What is Steganography?

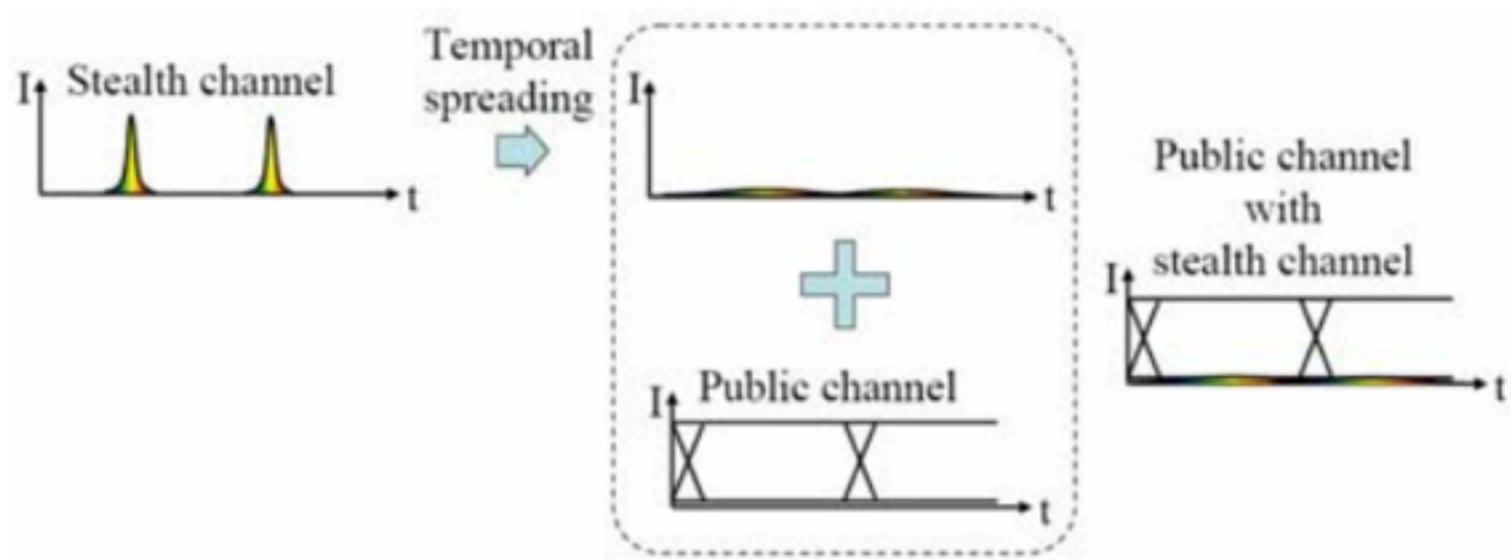


Figure 1: Schematic illustration of optical steganography using group velocity dispersion.

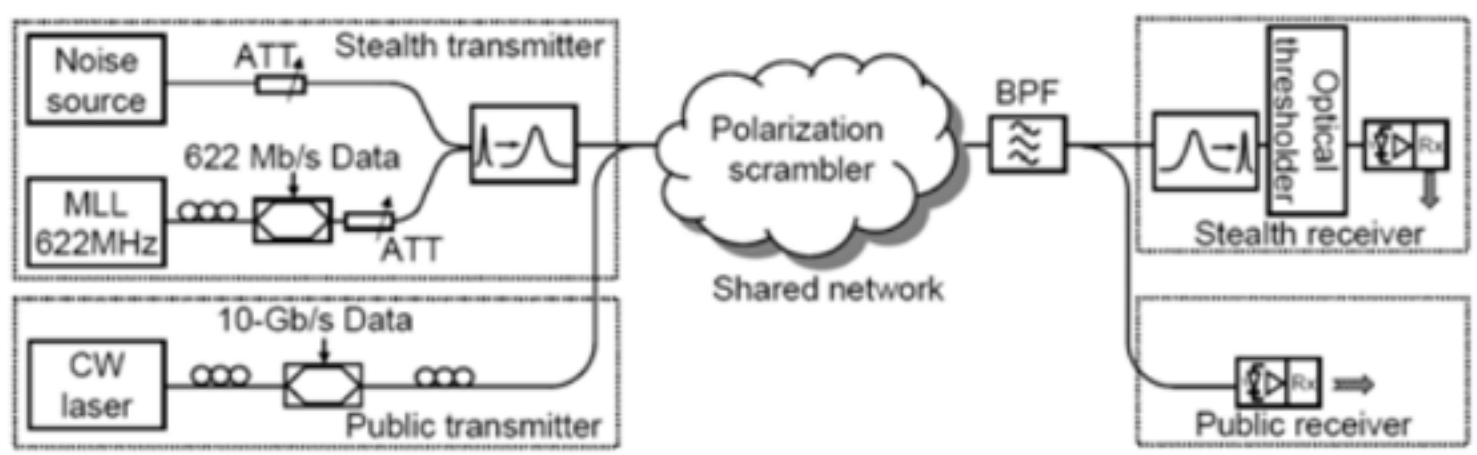
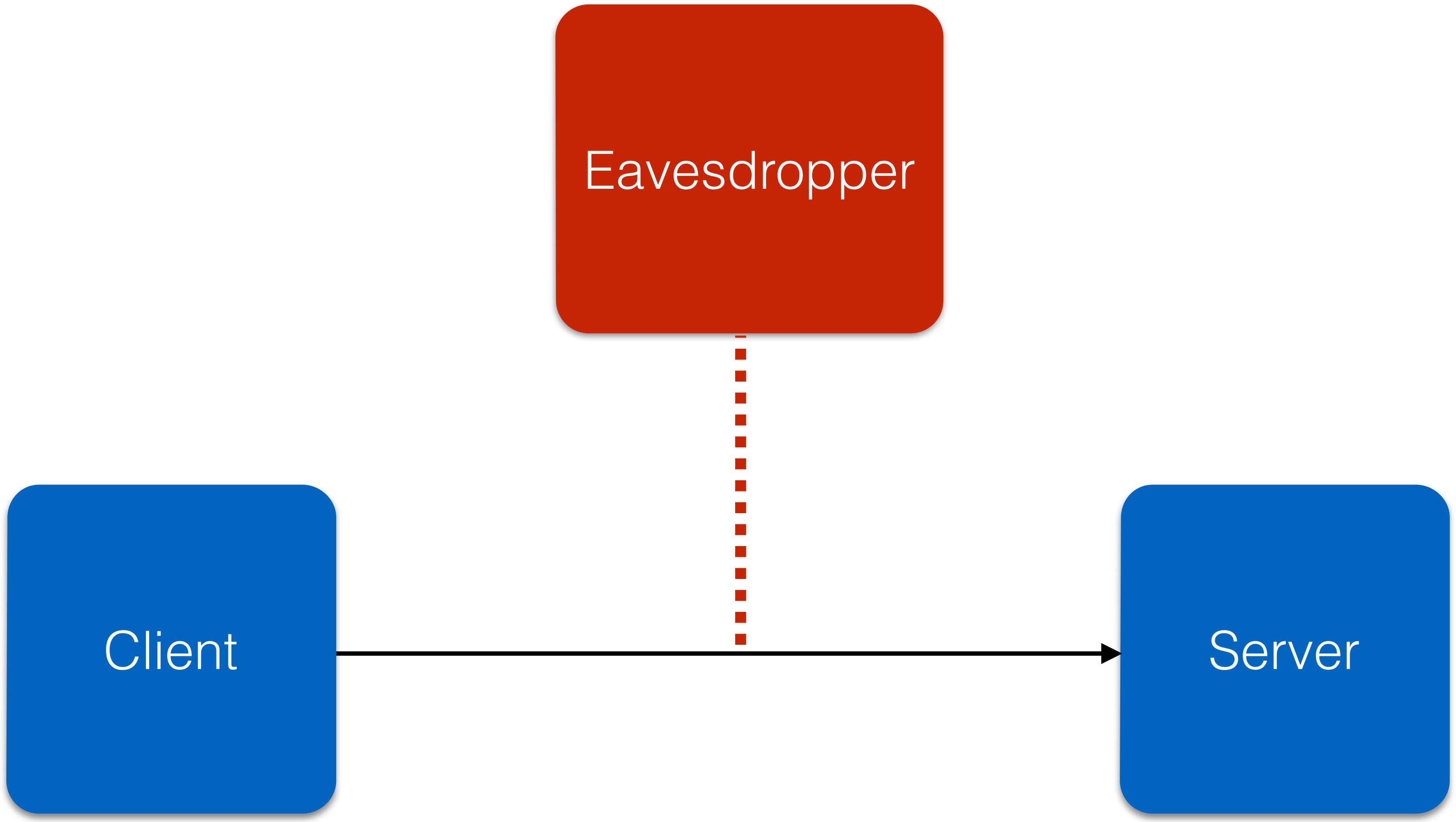
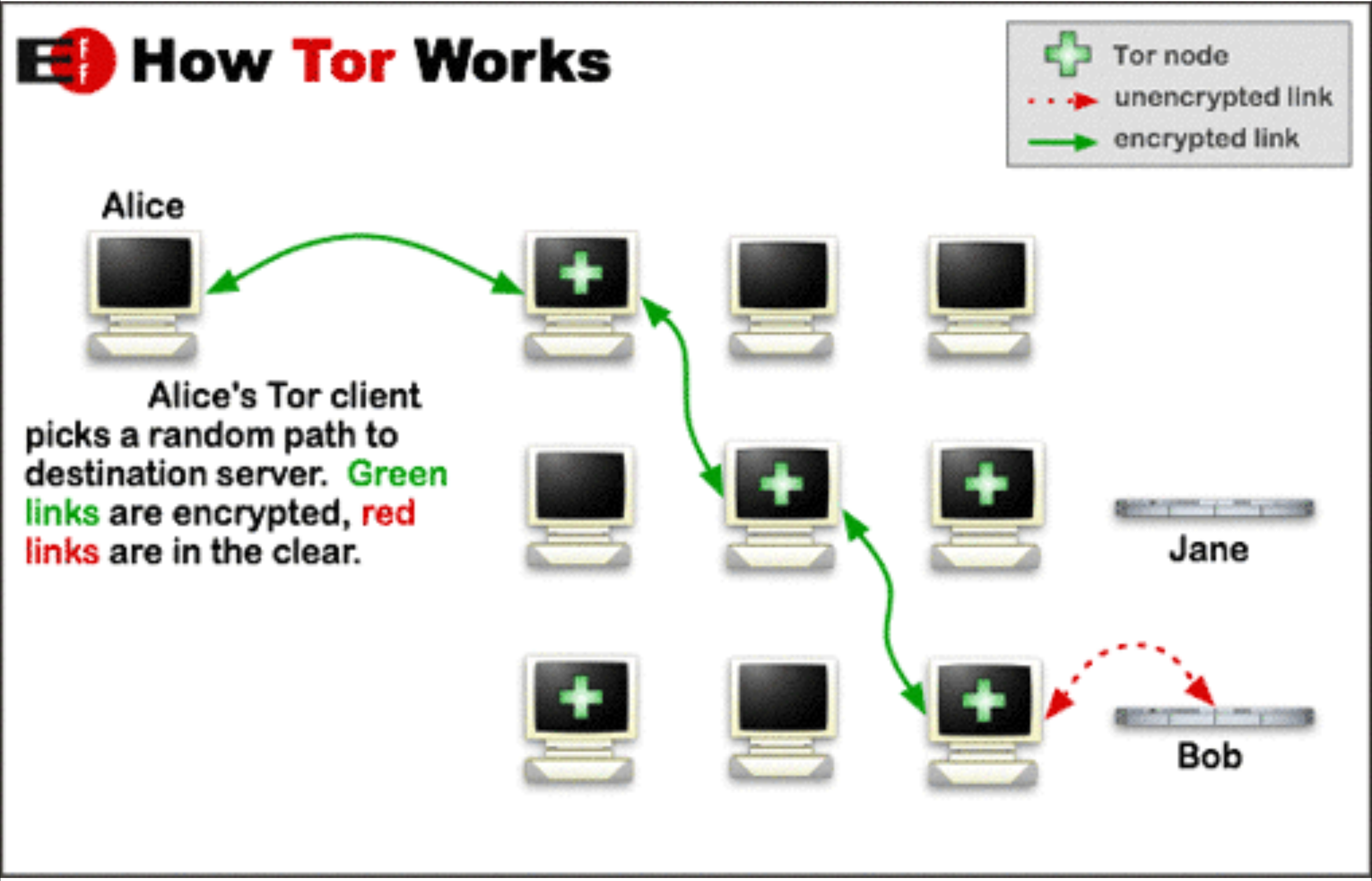


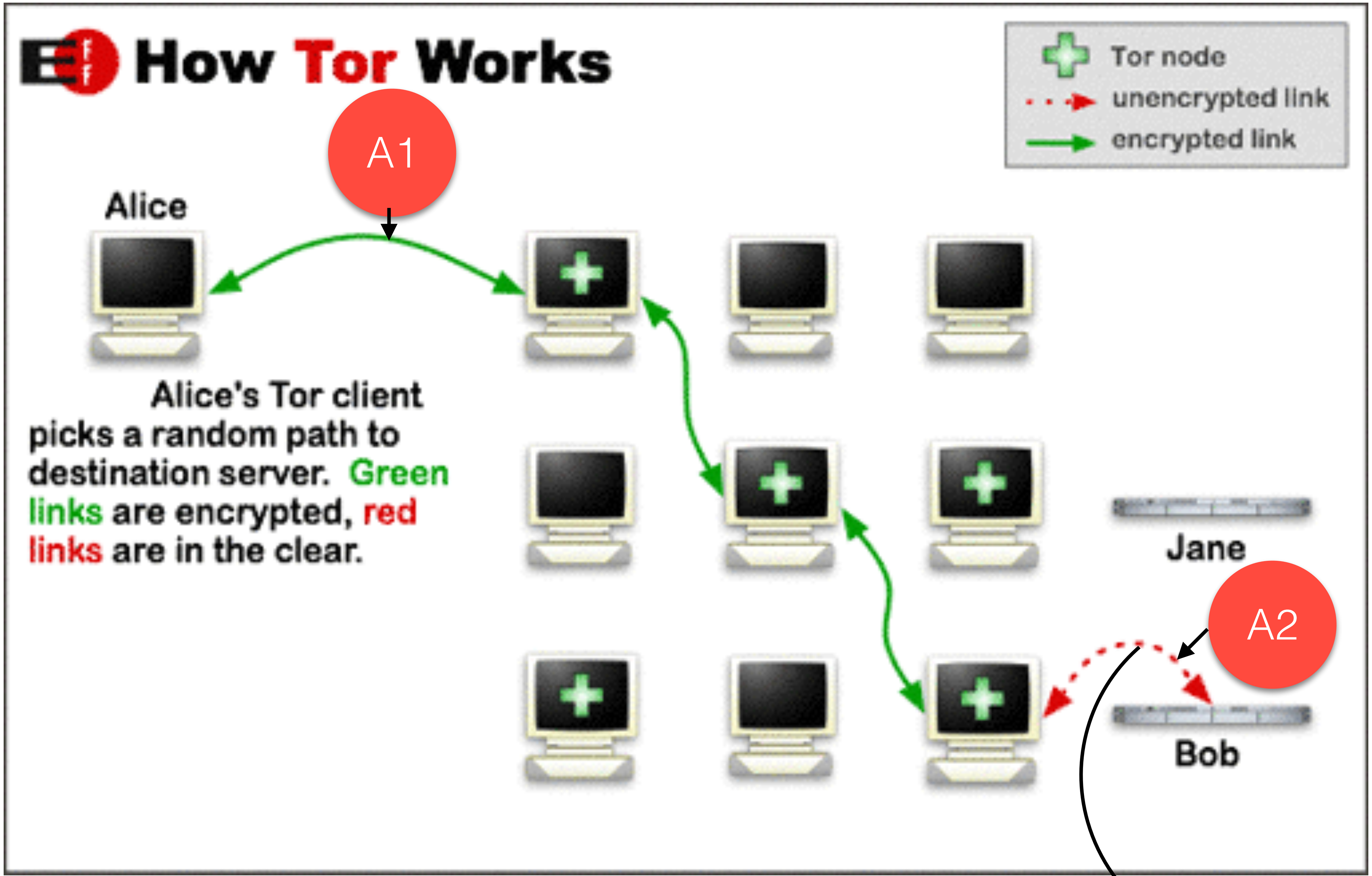
Figure 2: Schematic illustration of optical steganography. MLL: picosecond pulsed laser; ATT: variable optical attenuator; BPF: 3-nm optical band pass filter.

OPTICAL STEGANOGRAPHY FOR DATA HIDING IN OPTICAL NETWORKS
Paul R. Prucnal, Mable P. Fok, Konstantin Kravtsov, and Zhenxing Wang



The Problem Tor Solves


How Tor Works
Tor node
unencrypted link
encrypted link
Alice
Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Bob



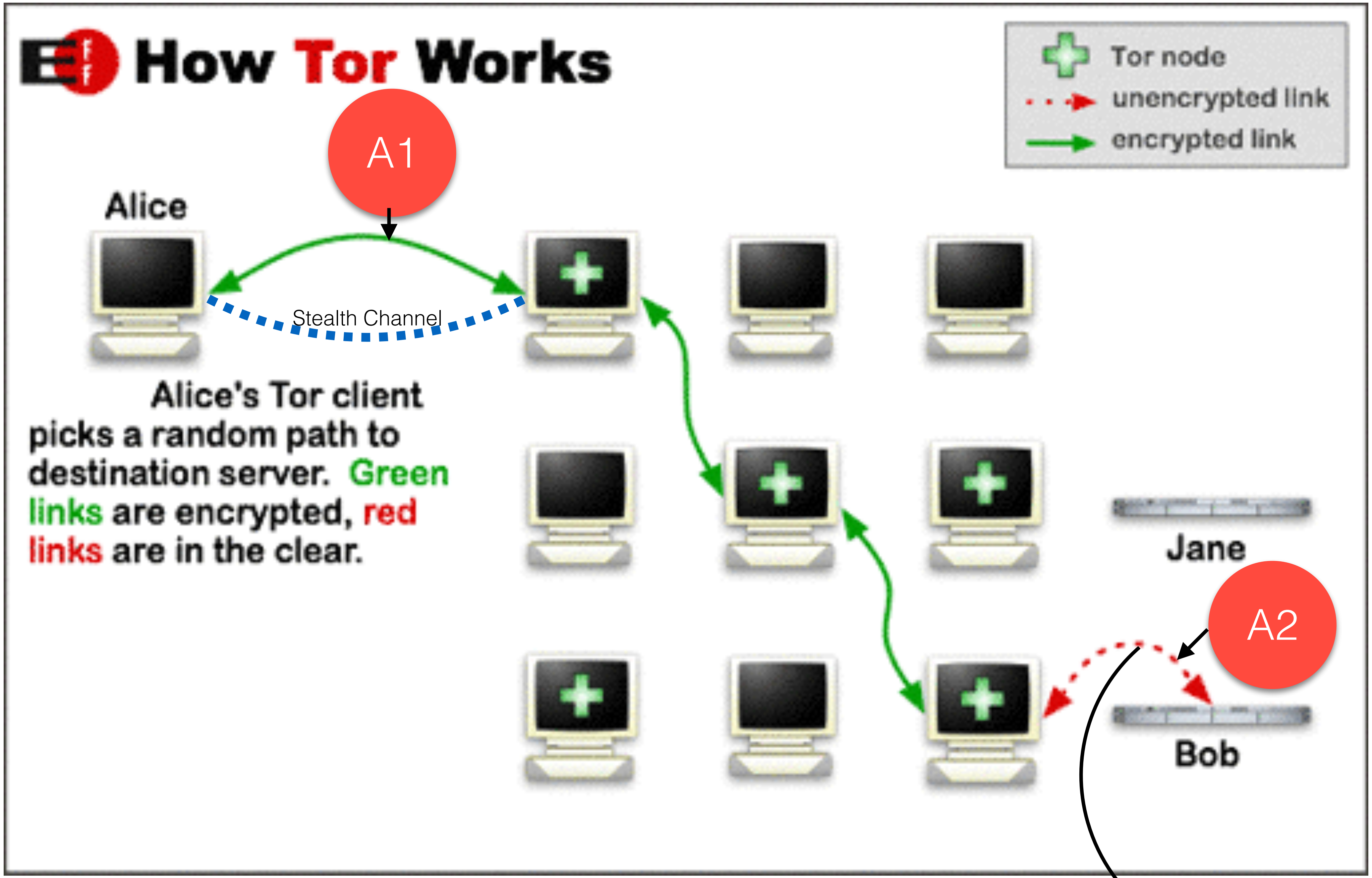
Assume this is encrypted with something like **https**

The Attack

Possible Timing Analysis Attack

1. Each attacker measures the amount of packets that occur during a time window.
2. The attackers share the information and determine the cross correlation between the two packet streams.
3. If the correlation is above a certain threshold, the attackers conclude that they are on the same path

	Number of Packets	
Time Window: (Each window is 1 Second Long)	Client Link	Server Link
0	15	15
1	40	42
2	189	187
3	18	19
4	74	76
5	50	50
6	52	49
7	74	73
8	94	95
9	112	113
10	99	97



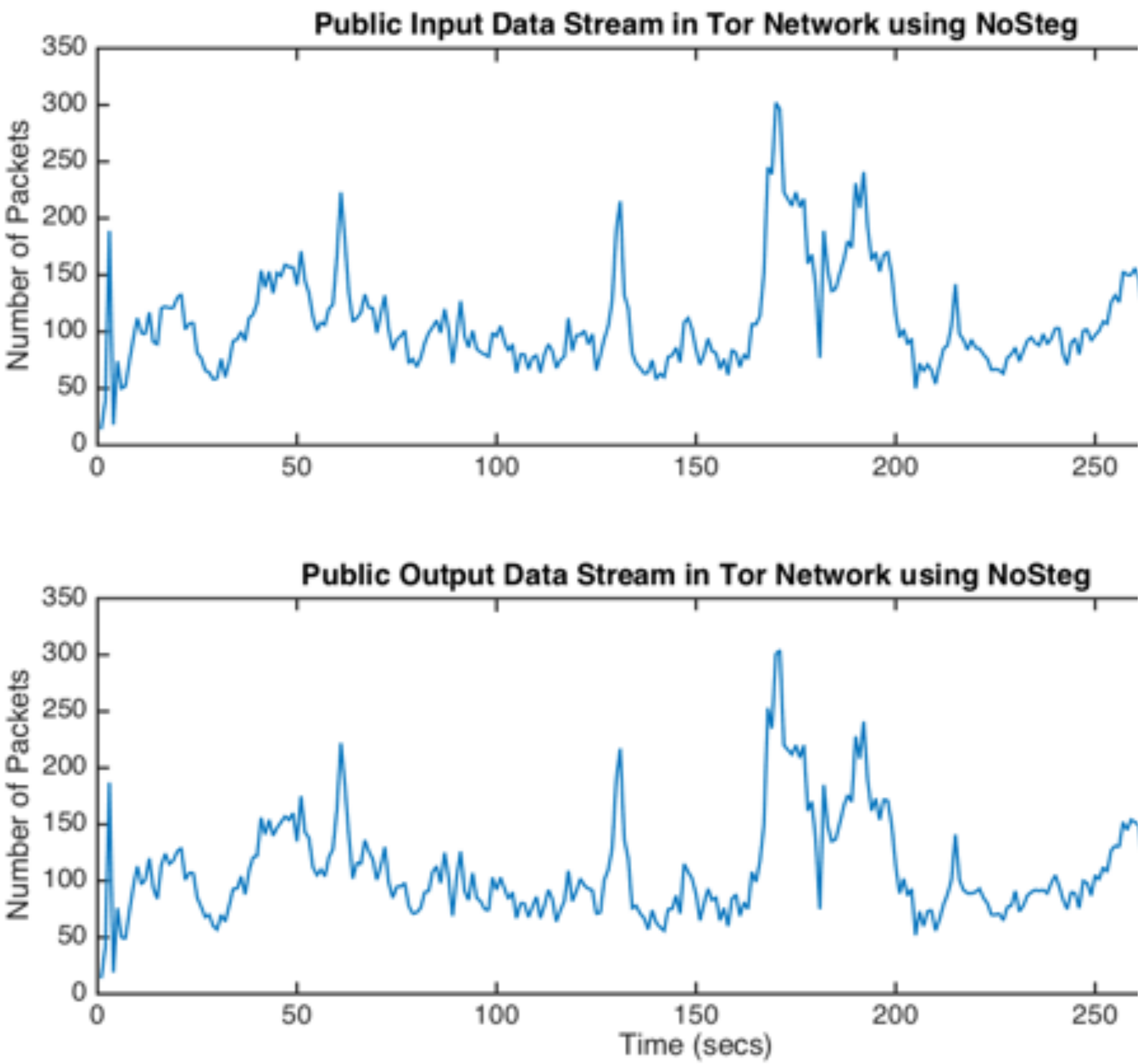
The Solution

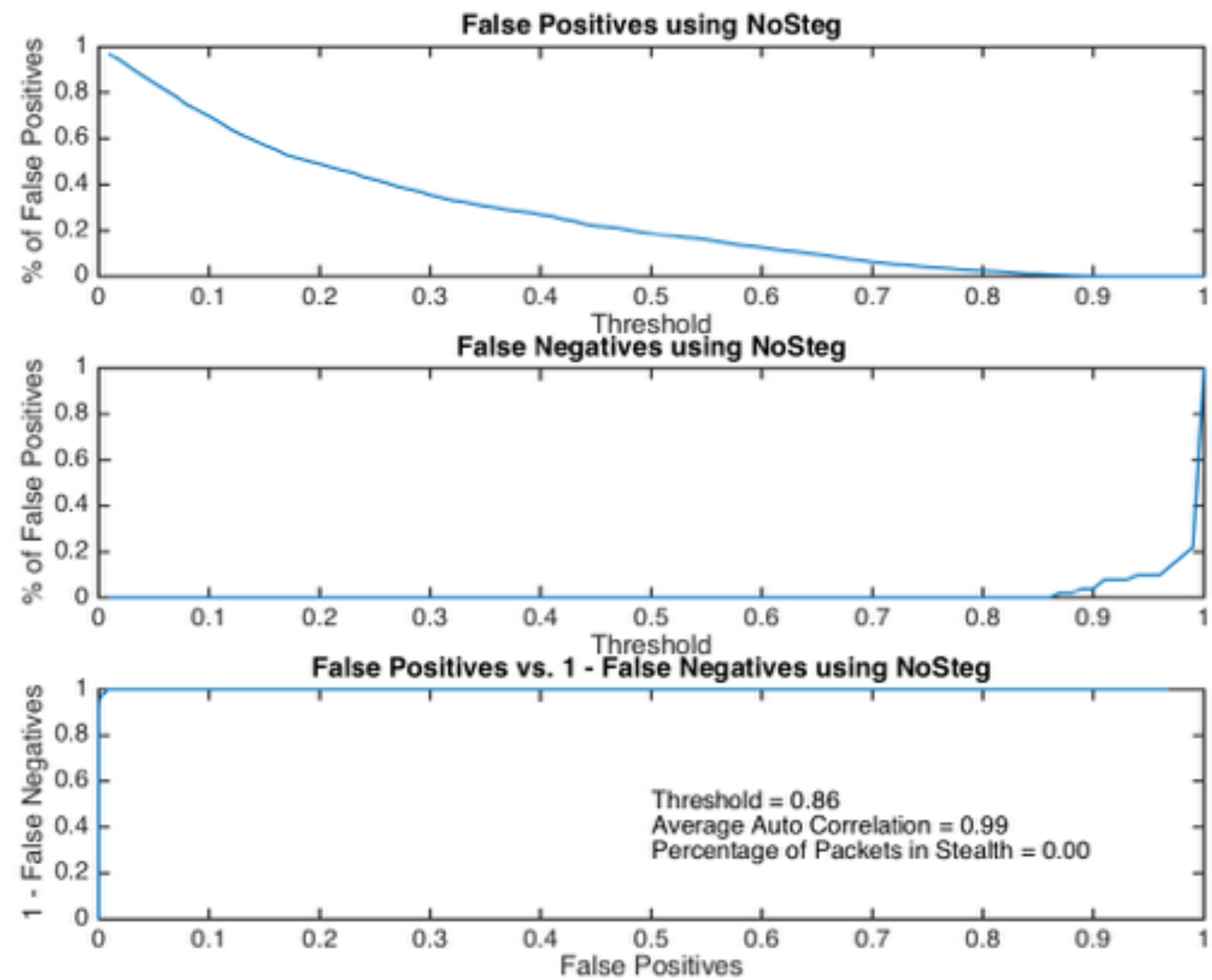
Assume this is encrypted with something like **https**

Distinguishing Characteristics

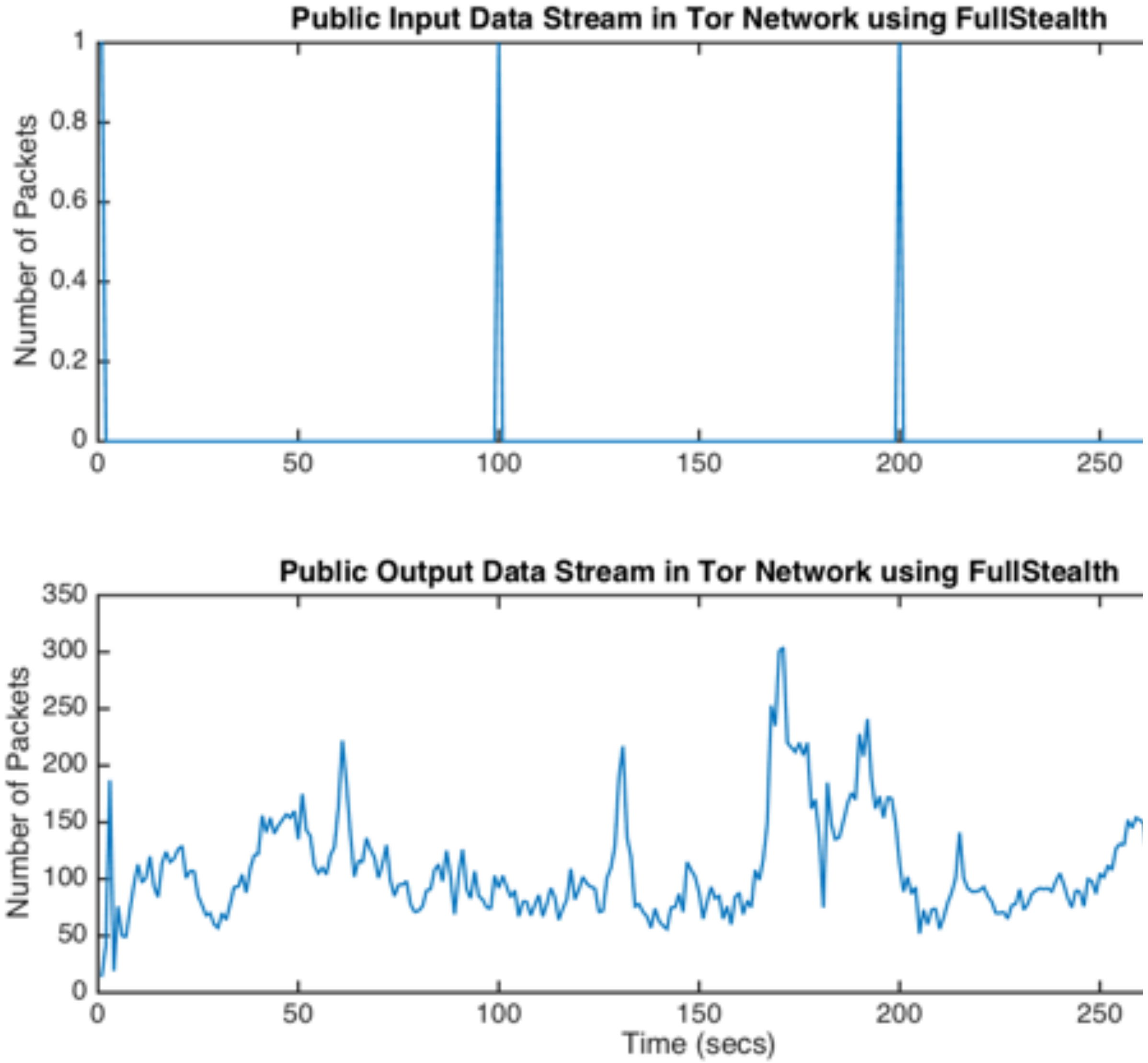
- Percentage of False Positives
- Percentage of False Negatives
- Percentage of Packets using Steganography

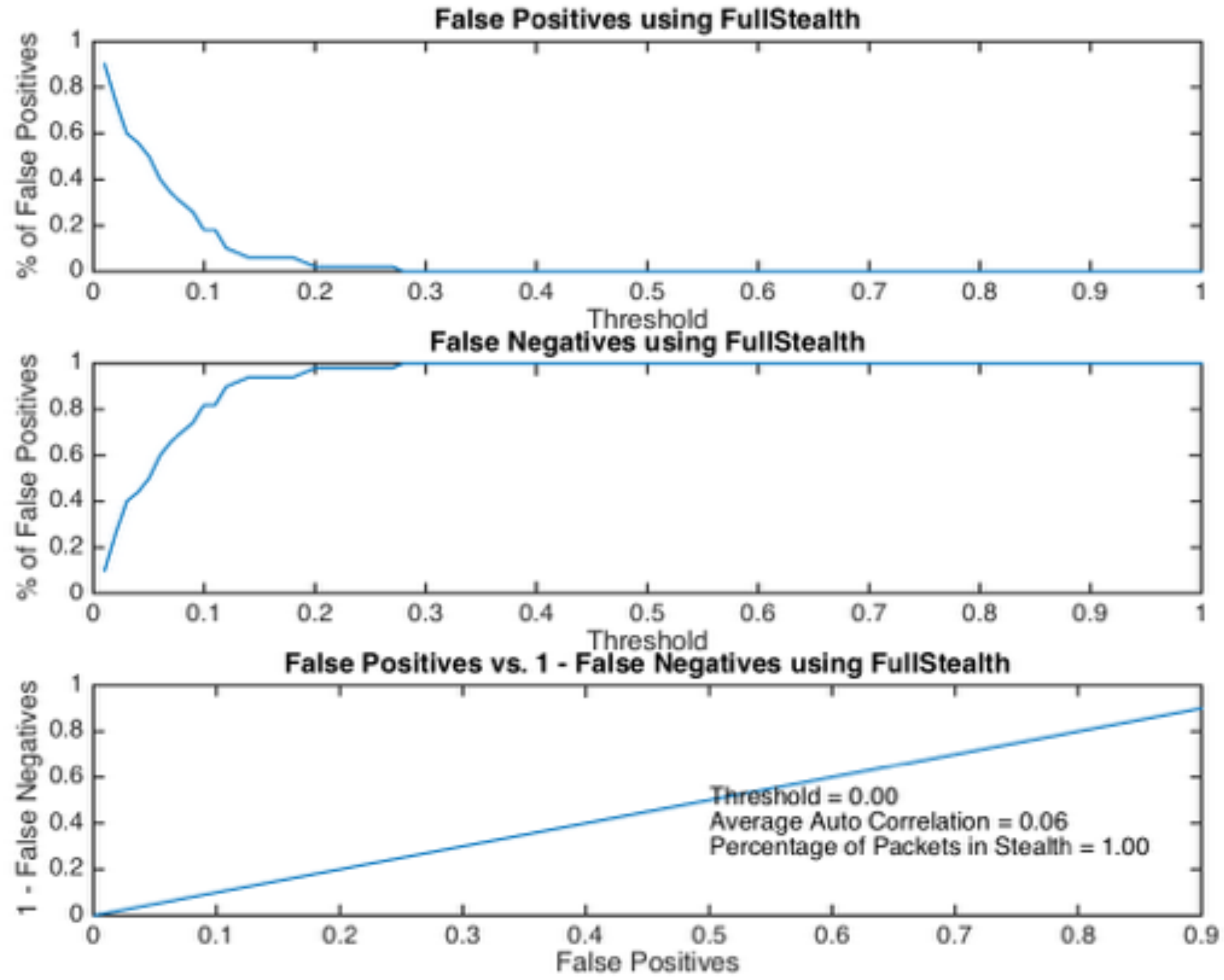
No Steganography



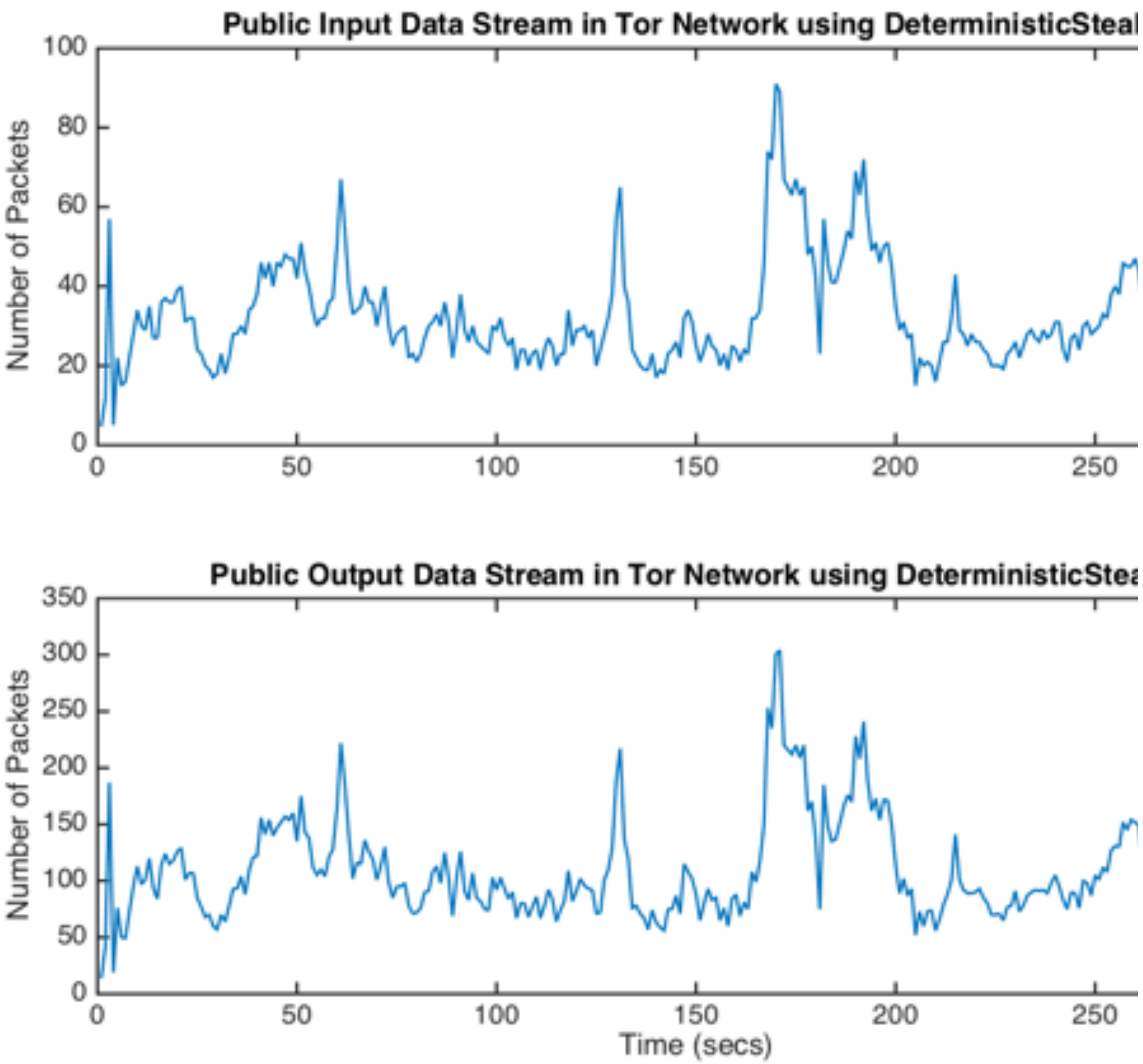


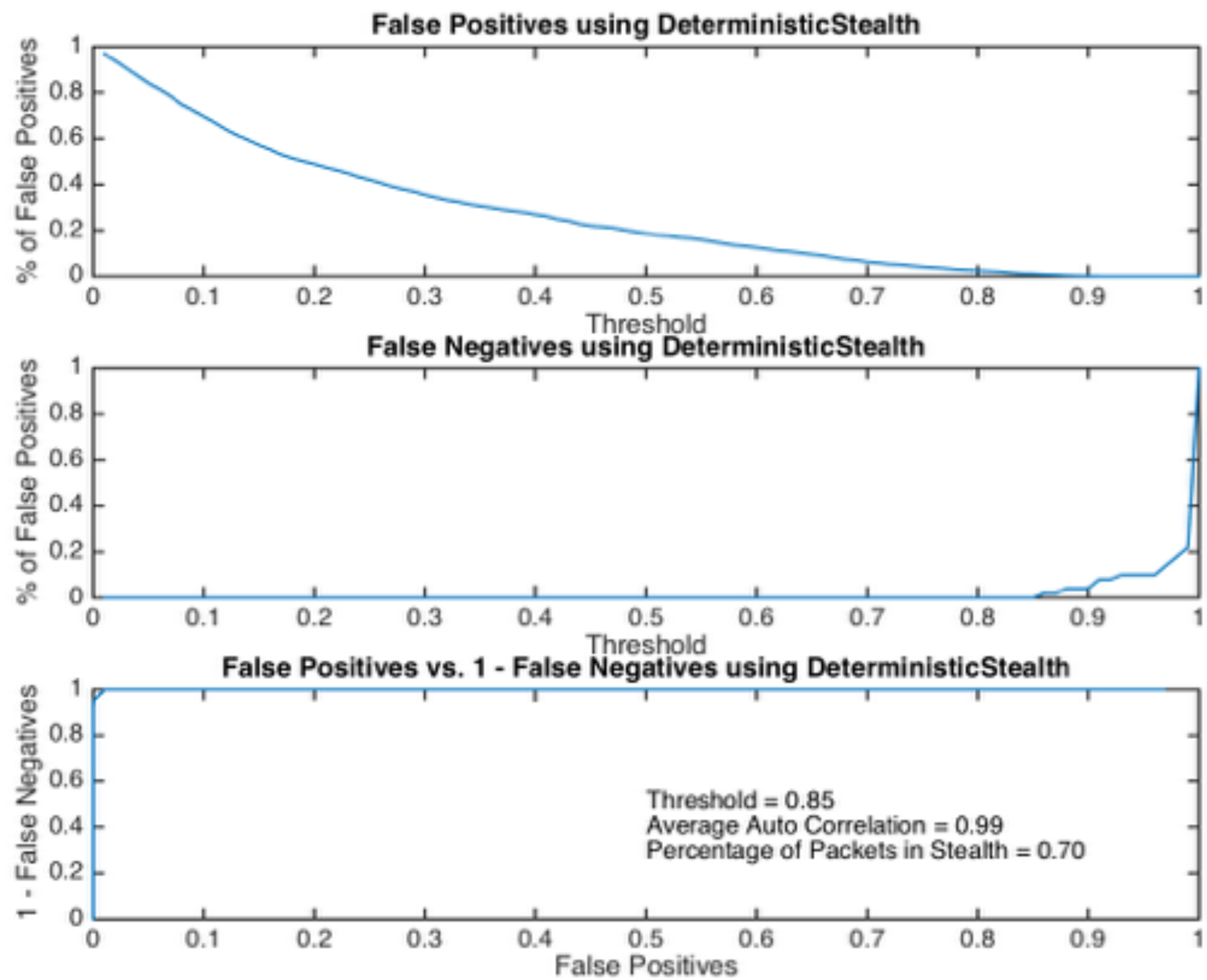
Full Steganography



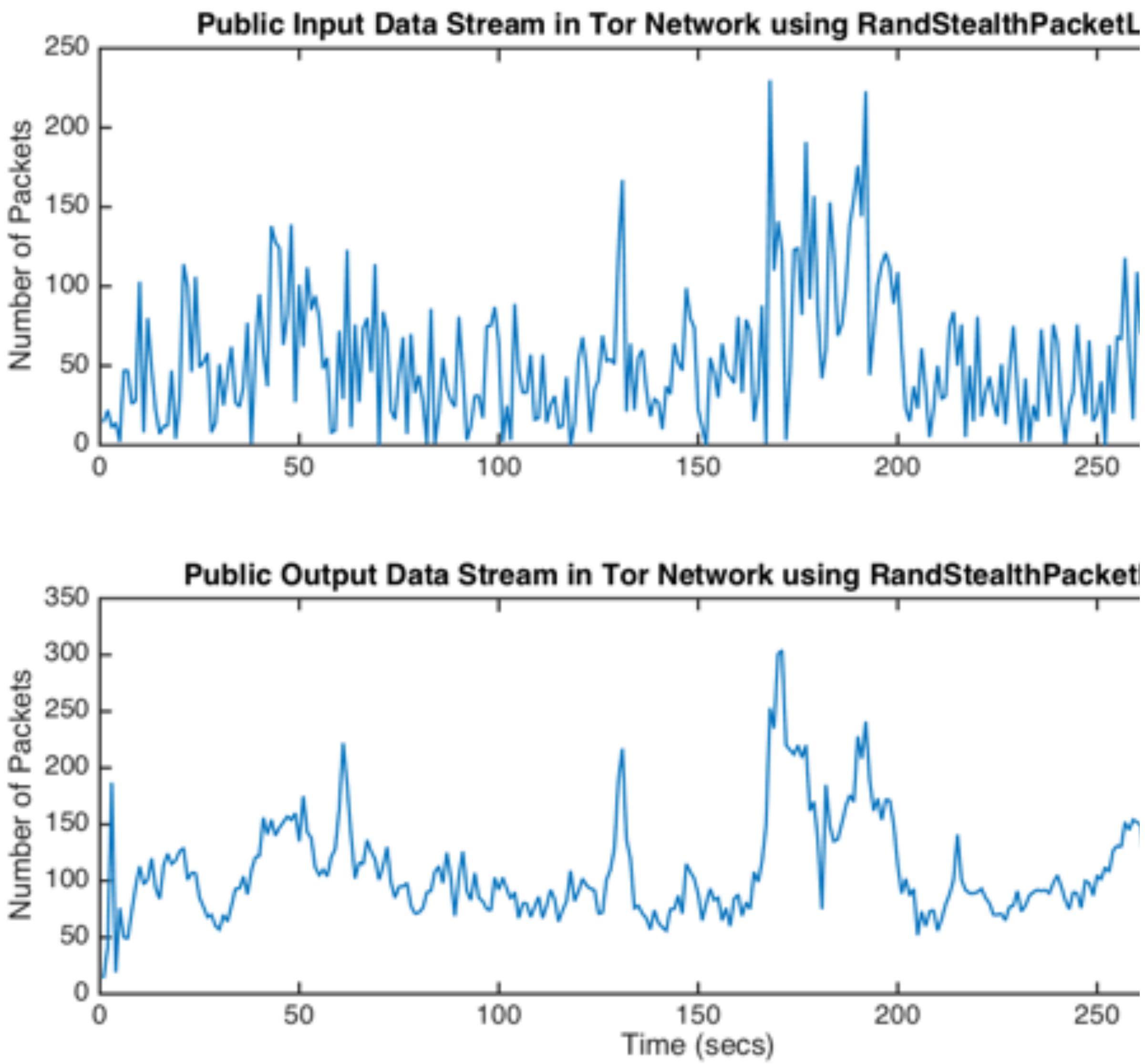


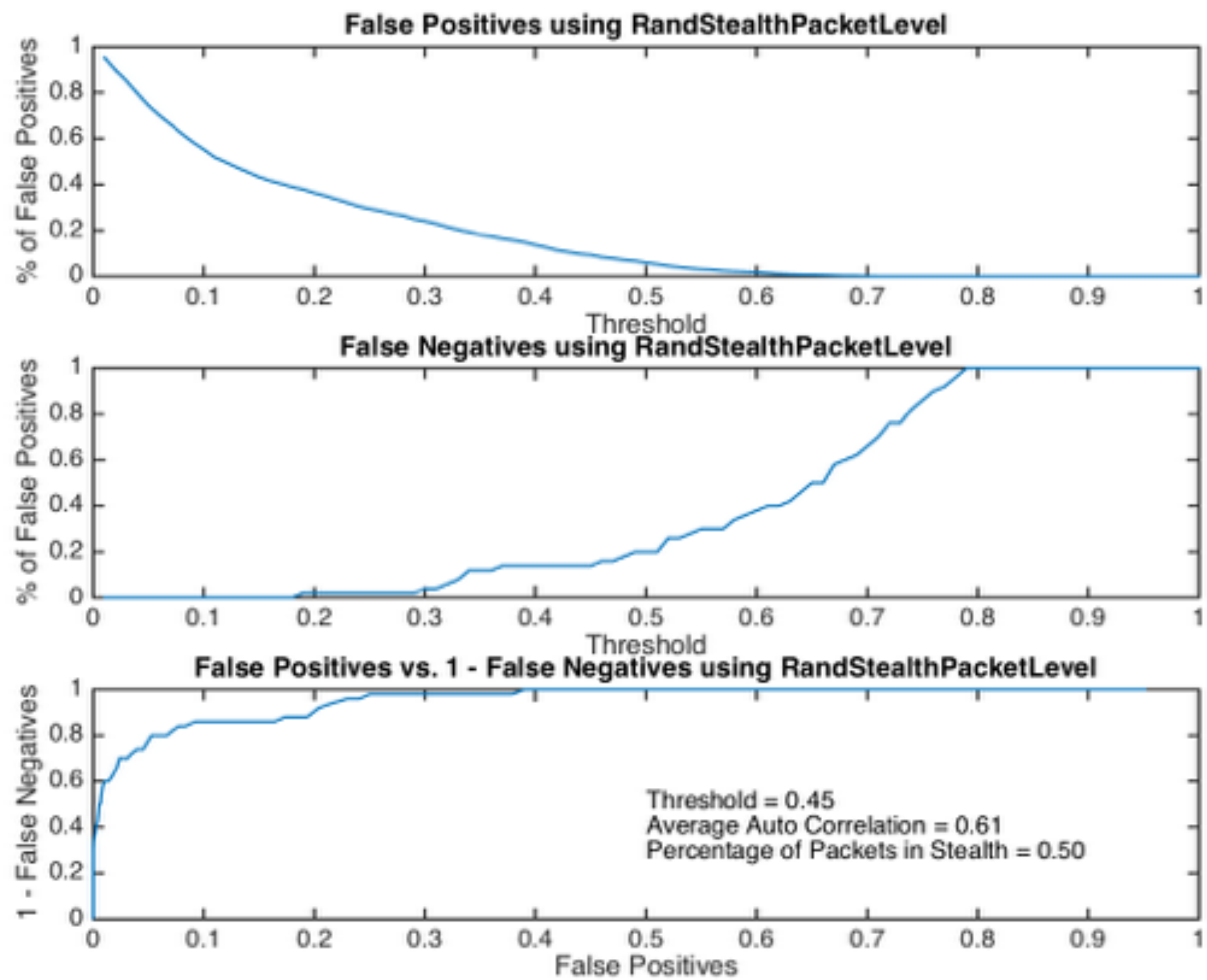
Deterministic 70% Steganography



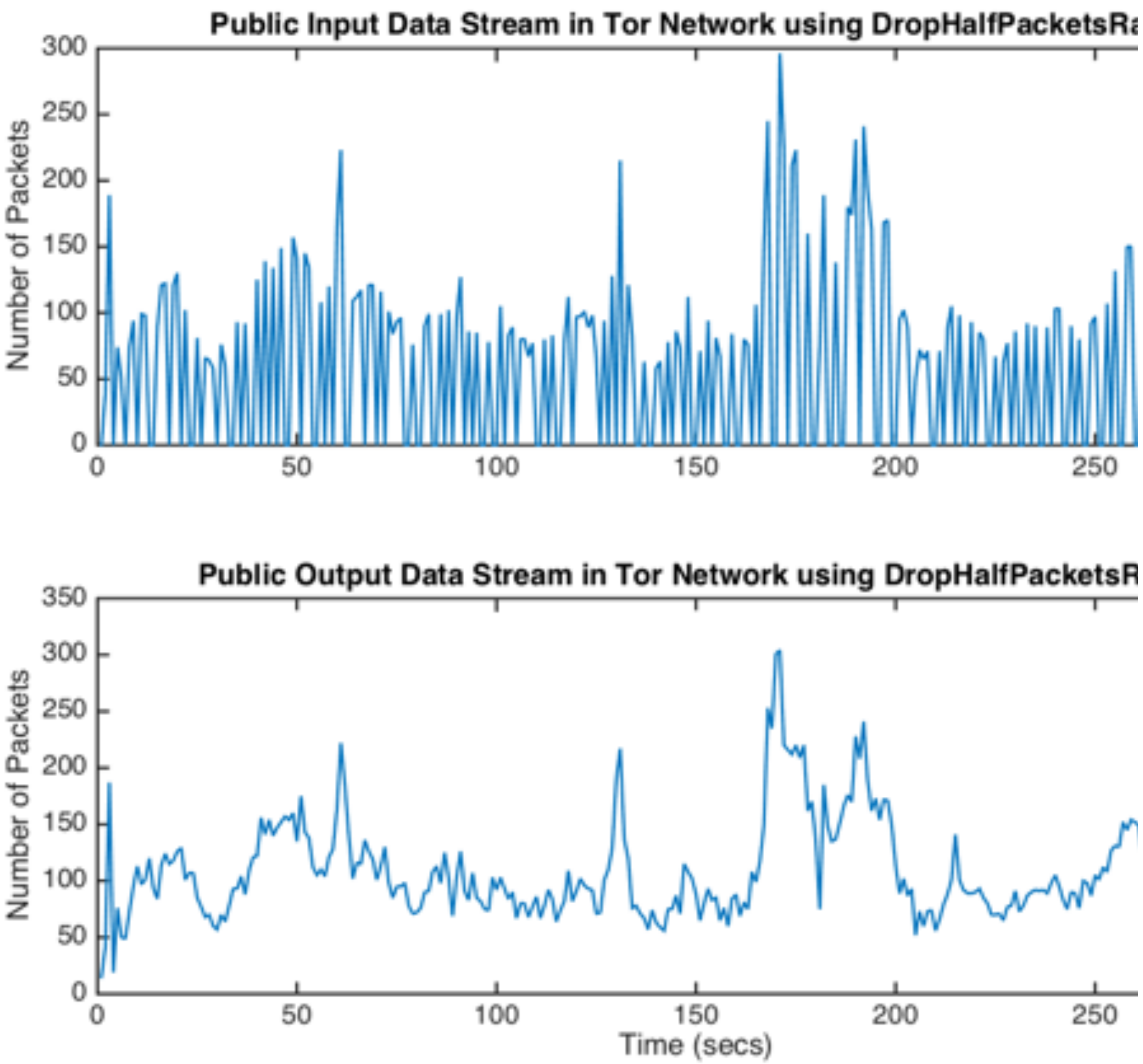


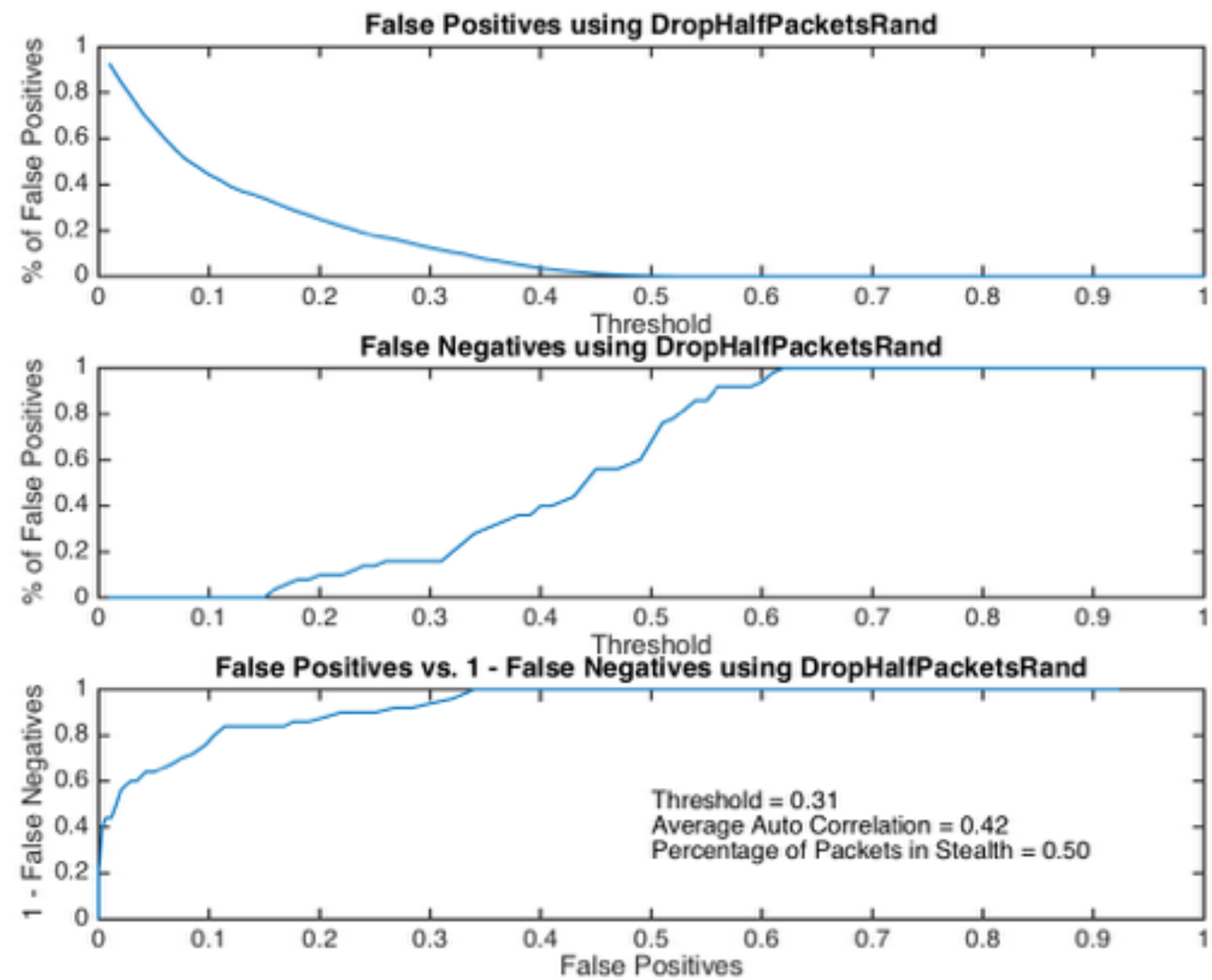
Random 50% Stealth: Limit Burst Sizes



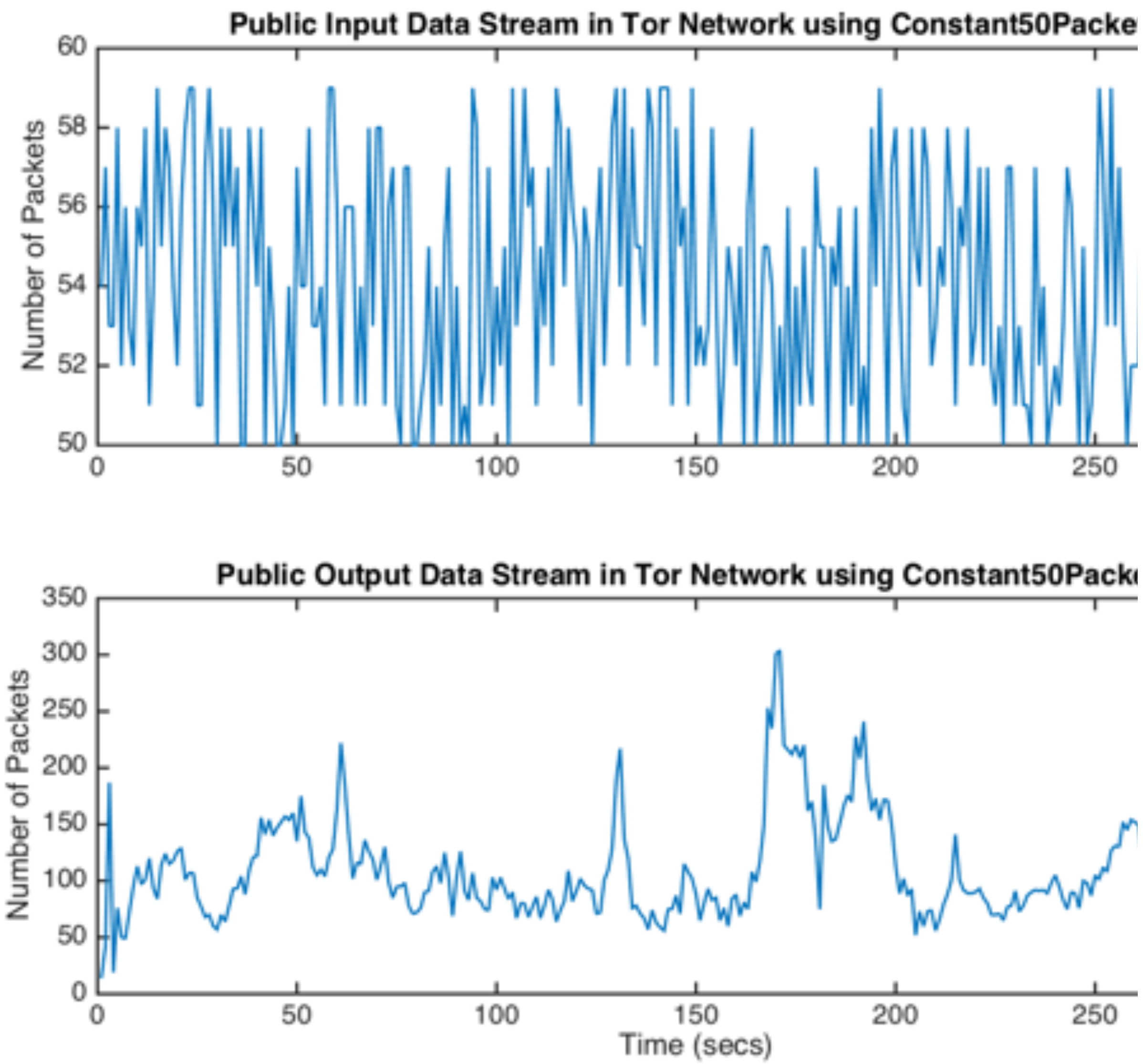


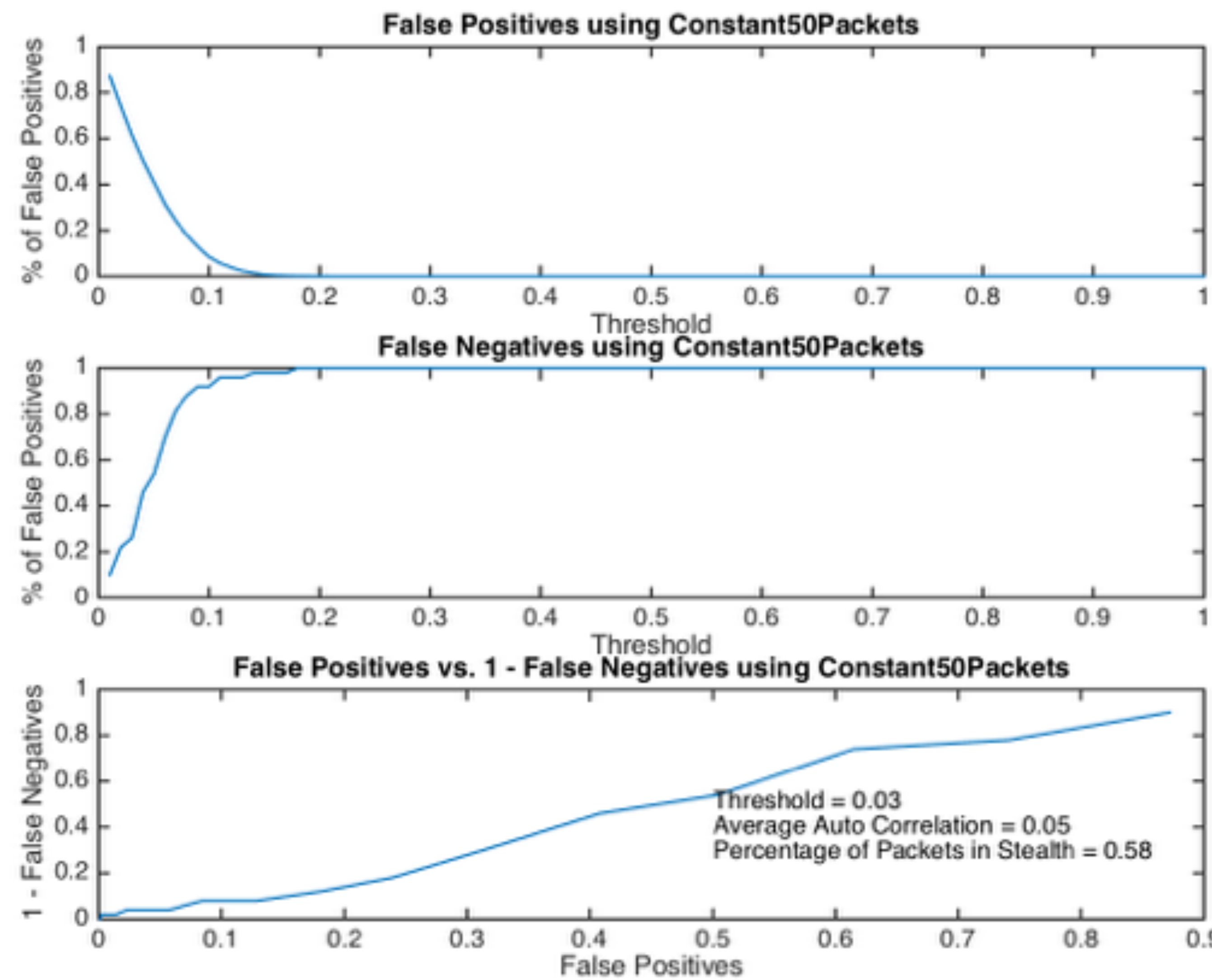
Random 50% Stealth: Drop Full Bursts



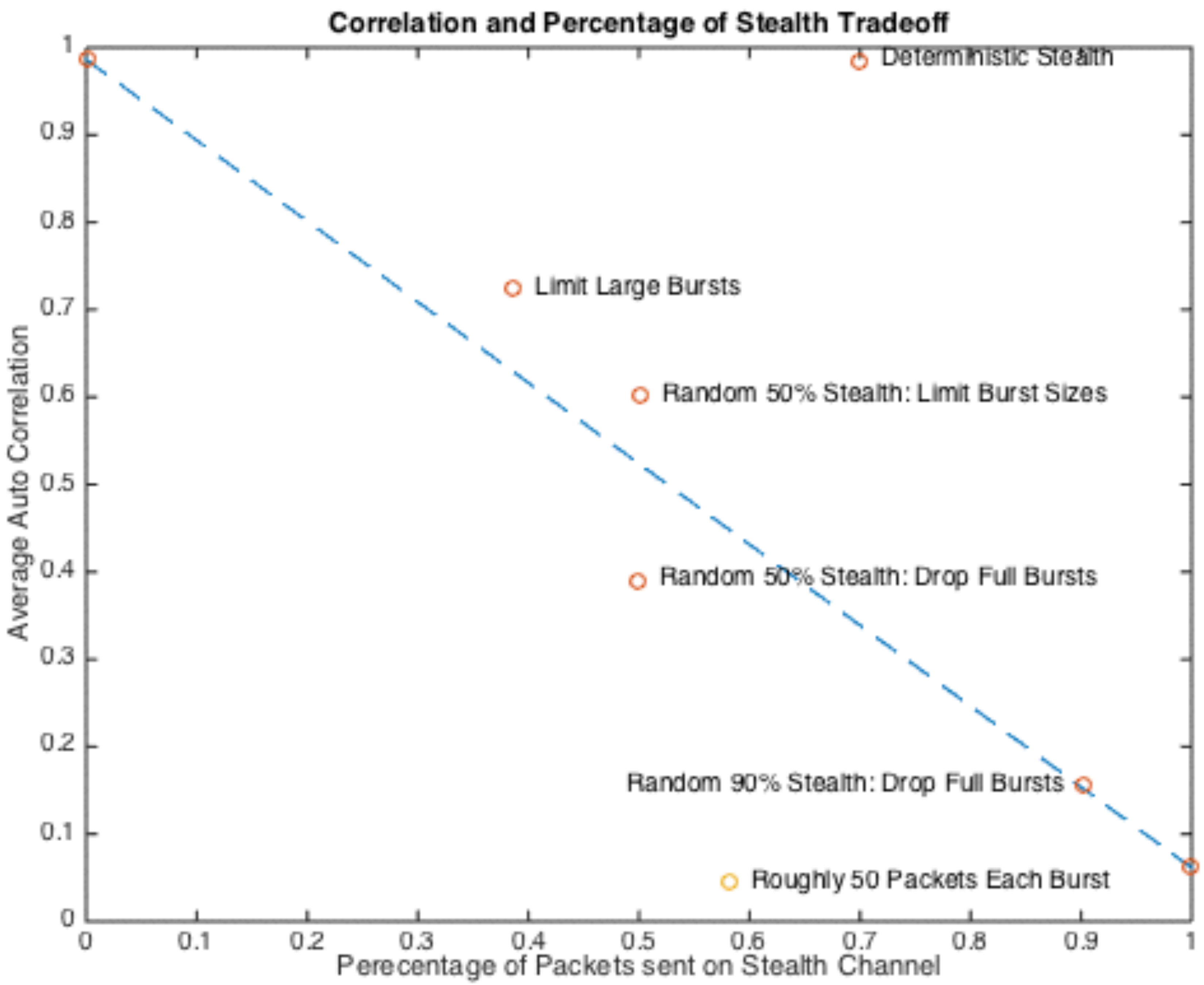


Roughly 50 Packets Each Burst





Tradeoff Curve



Conclusion

- Timing analysis attacks can be avoided with steganography, if applied correctly
- Bandwidth impact must be determined before selecting the scheme
- Implementation details TBD

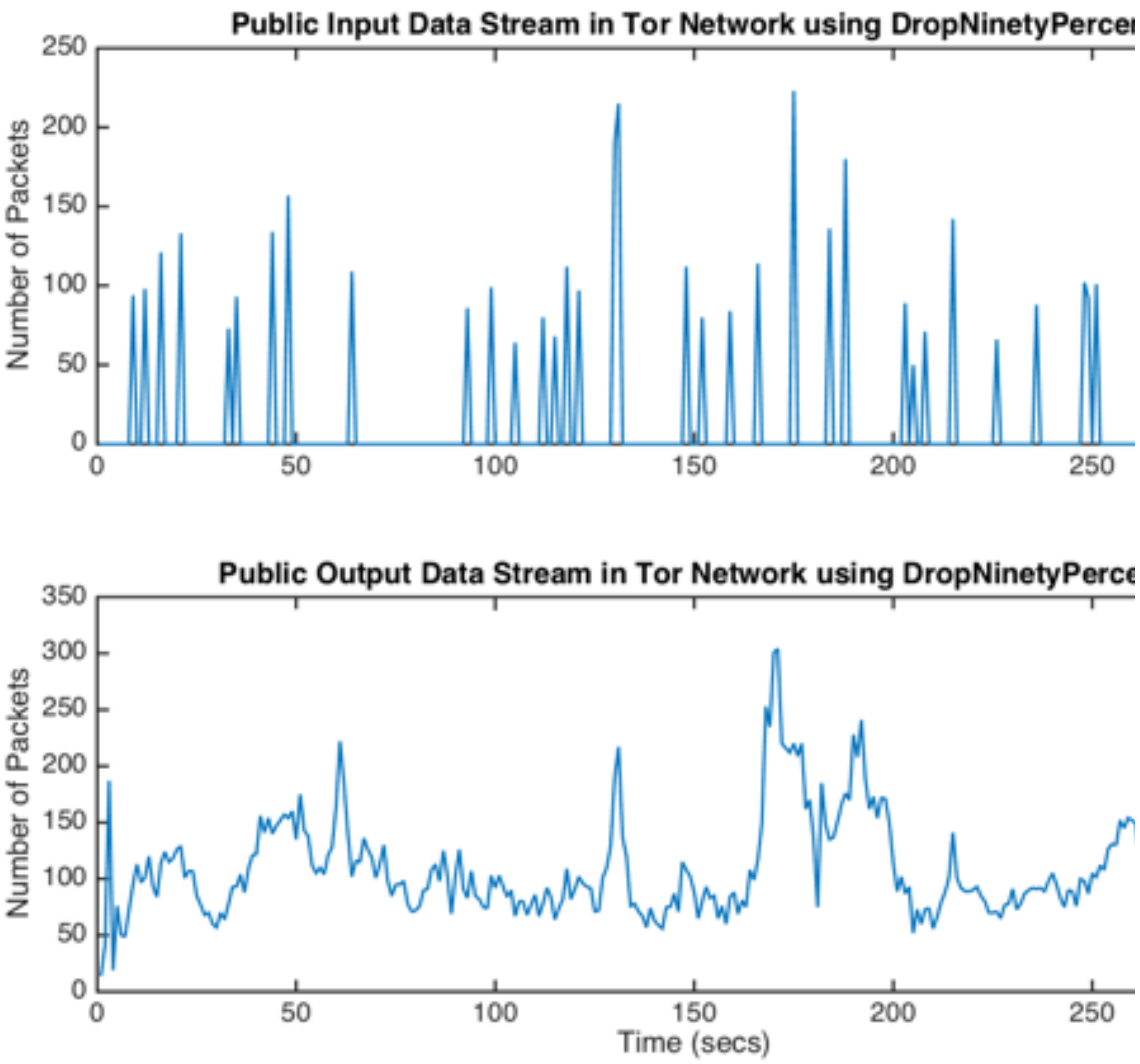
References

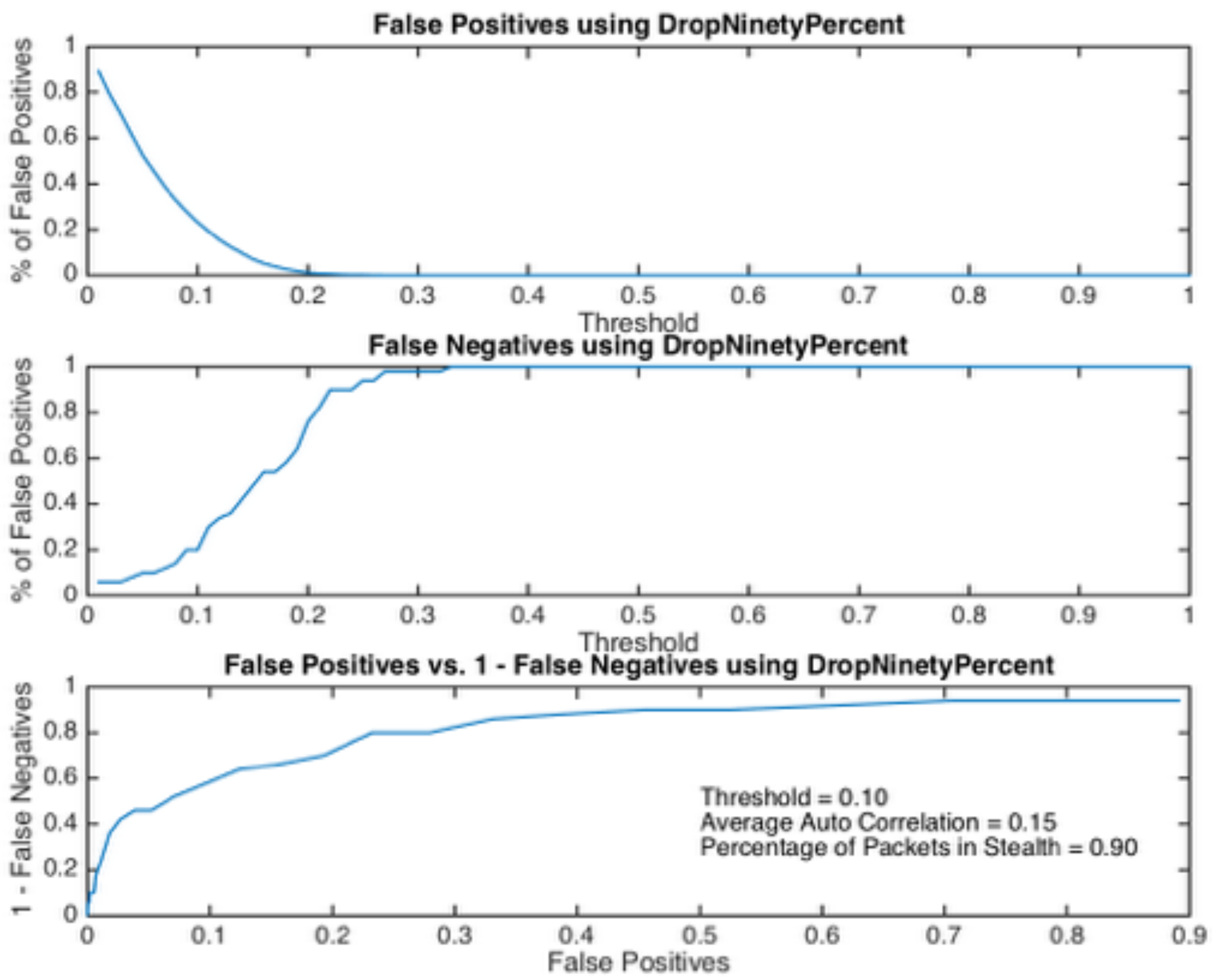
- *Physical Layer Security Based on Optical Steganography and Optical Encryption*. Ben Wu
- *Optical steganography based on amplified spontaneous emission noise*. Ben Wu,* Zhenxing Wang, Yu, Tian, Mable P. Fok, Bhavin J. Shastri, Daniel R. Kanoff, and Paul R. Prucnal.
- *Studying Timing Analysis on the Internet with SubRosa*. Hatim Daginawala and Matthew Wright
- *Timing analysis in low-latency mix networks: attacks and defenses* . Vitaly Shmatikov and Ming-Hsi. Wang
- *Timing Attacks in Low-Latency Mix Systems (Extended Abstract)*. Brian N. Levine, Michael K. Reiter. Chenxi Wang, and Matthew Wright

Questions?
Other possible schemes?

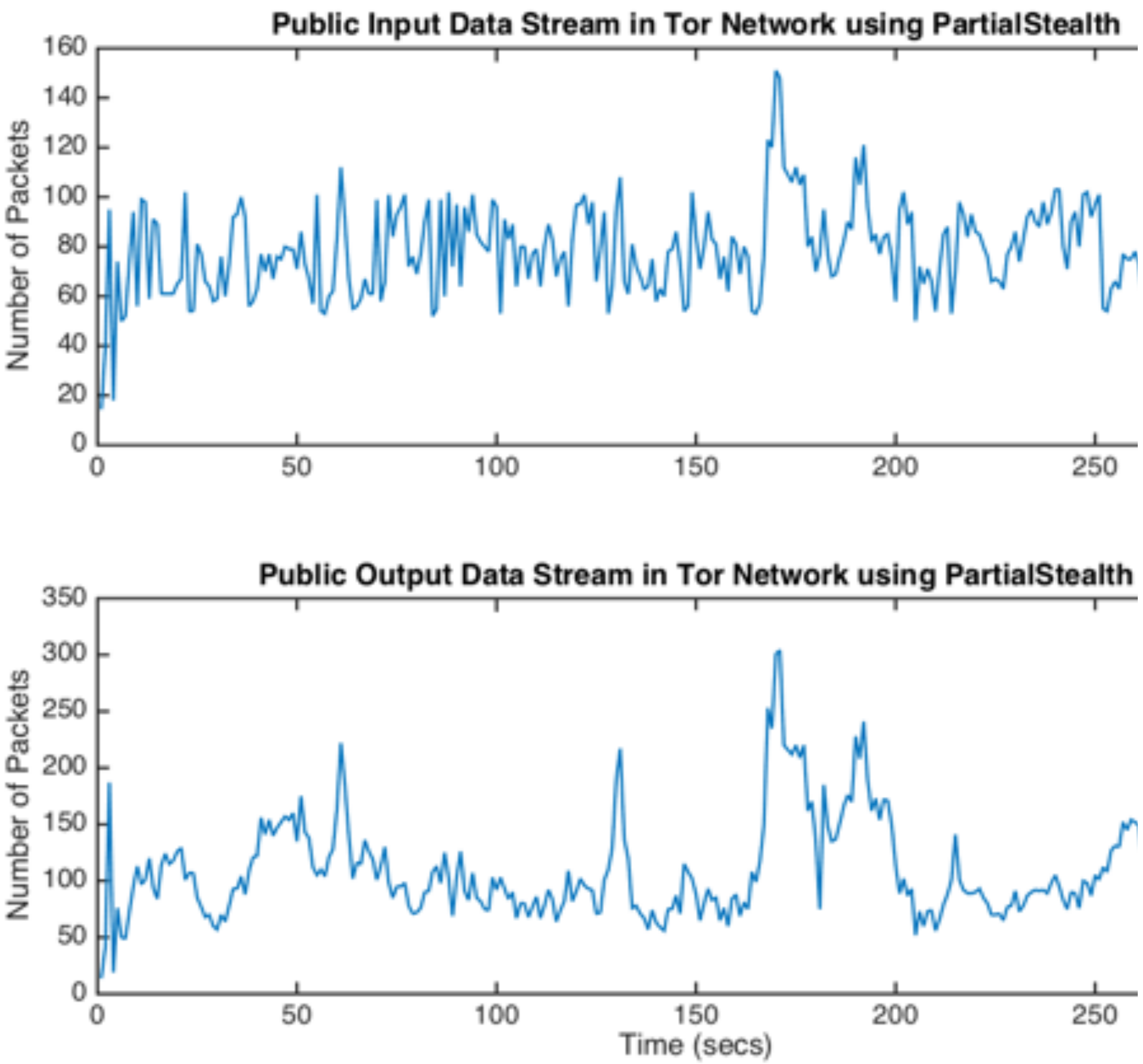
(We can demo your scheme now, if you’d like)

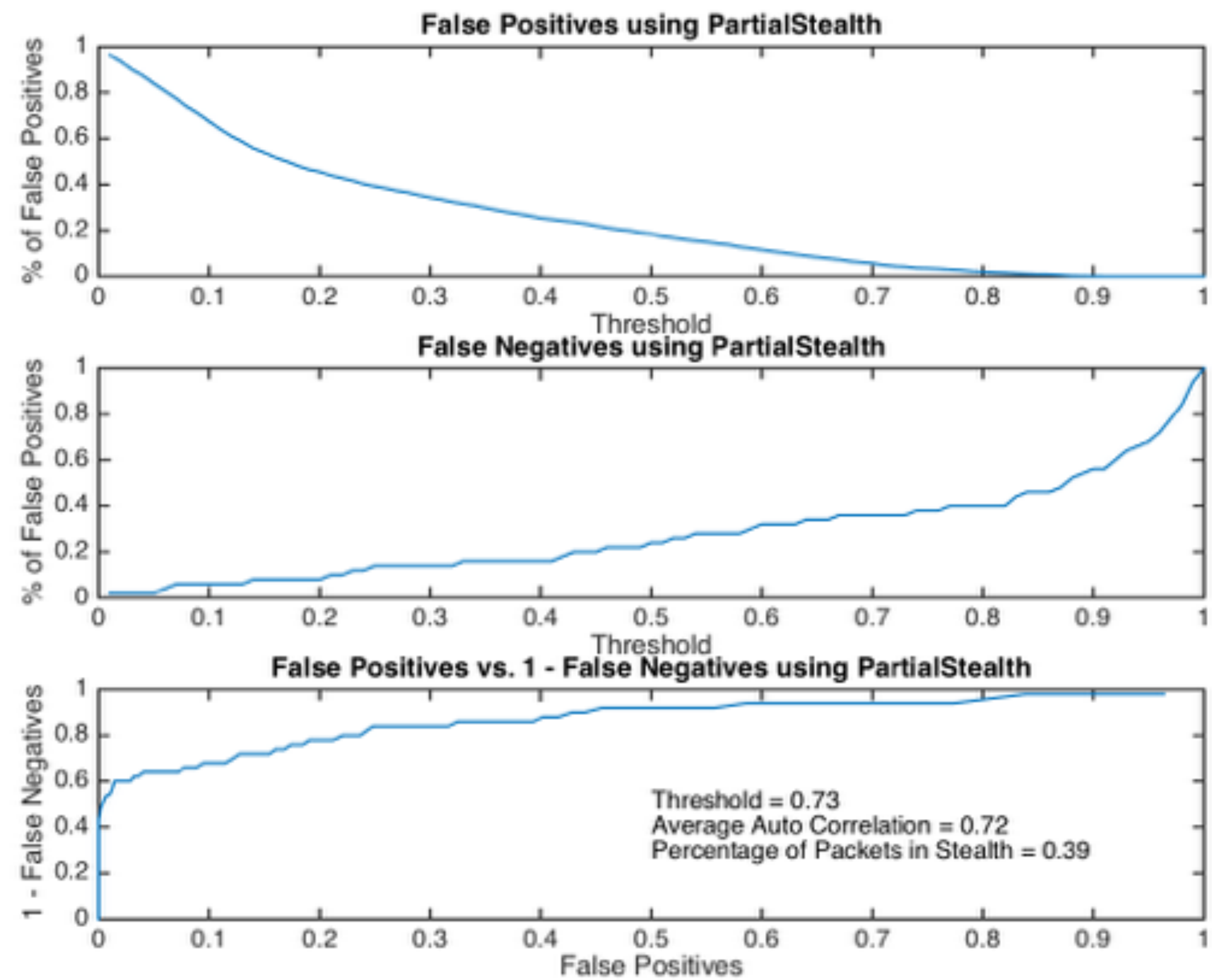
Random 90% Stealth: Drop Full Bursts





Limit Large Bursts





How does Steganography work?

- Hide the data within the noise of the signal
- Mask the information in the time domain
- Mask the information in the spectral domain

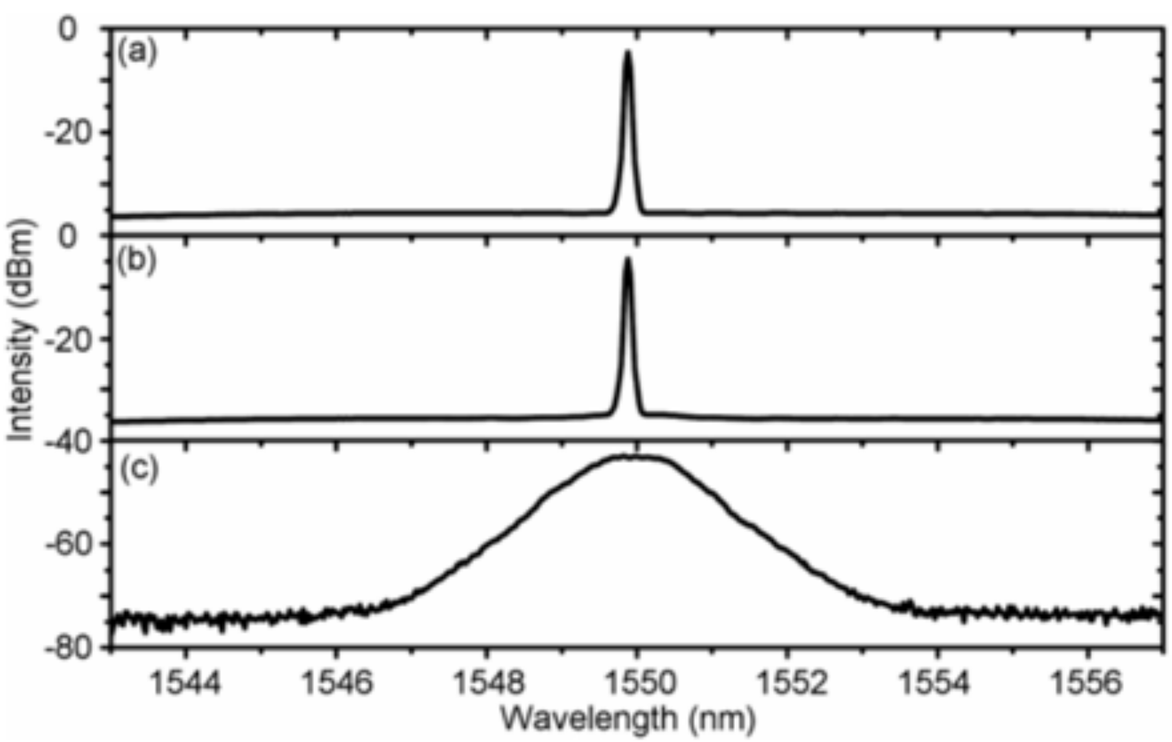


Figure 3: Optical spectra (a) public channel (b) public channel with the stealth channel (c) stealth signal alone.

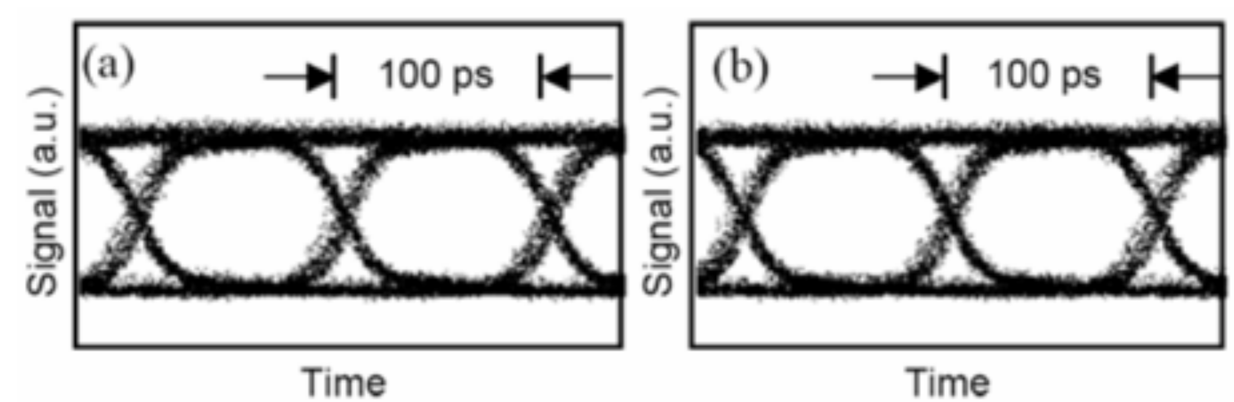
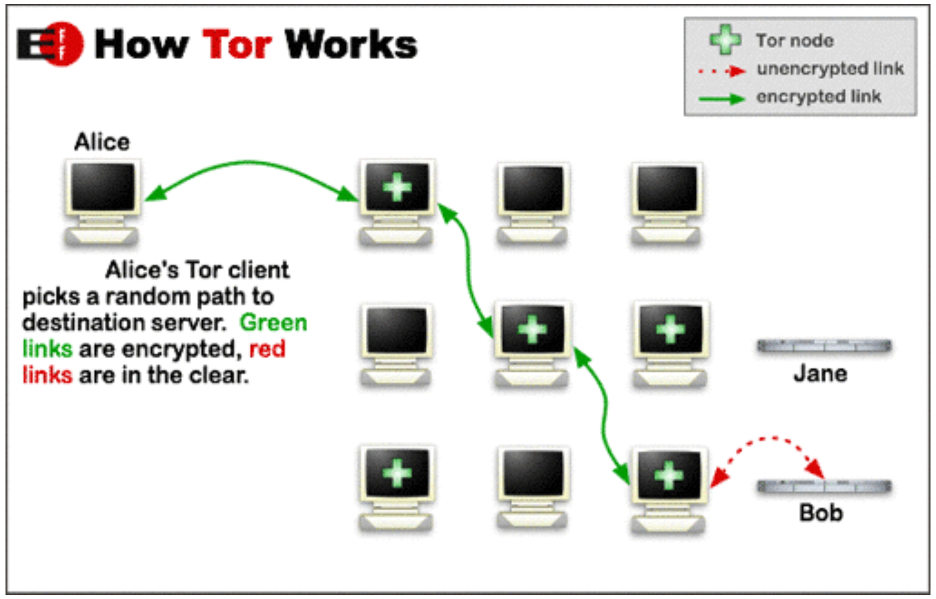


Figure 4: Eye diagrams (a) without stealth transmission (b) with stealth signal in the network.

OPTICAL STEGANOGRAPHY FOR DATA HIDING IN OPTICAL NETWORKS
Paul R. Prucnal, Mable P. Fok, Konstantin Kravtsov, and Zhenxing Wang

The Onion Router



1. Determine a path between 3 Tor nodes
2. Use asymmetric keys to determine 3 shared keys, one key for each node in the path
3. Encrypt the message with all three shared keys
4. Each node will decrypt the message with their shared key. This essentially peels off a layer of the onion.
5. Deliver the unencrypted packet to the server.
6. Use the same path for the return, but rather than peeling off a layer, add a layer. Each node encrypts the message with their shared secret.
7. Decrypt using all 3 shared secret keys in the correct order. Completely peel open the onion.

Correlation Formula

$$r(d) = \frac{\sum_i \left((x_i - \mu) \left(x'_{i+d} - \mu' \right) \right)}{\sqrt{\sum_i (x_i - \mu)^2} \sqrt{\sum_i \left(x'_{i+d} - \mu' \right)^2}}$$

X_i: The amount of input packets in the i^{th} window.

X_i': The amount of outgoing packets in the i^{th} window.

μ: The mean packet size on the input stream

μ’: The mean packet size on the output stream

d: The delay used to determine the cross correlation.

This value is typically set to 0.