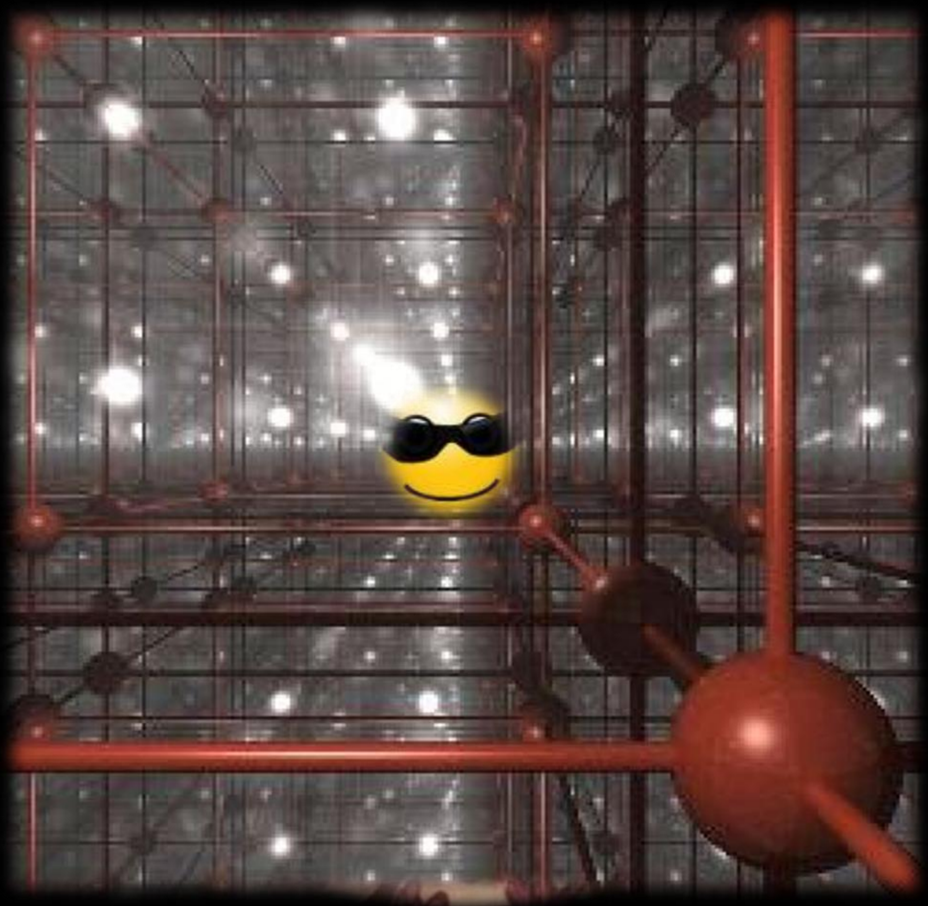
Robust and Undetectable Steganographic Timing Channels for i.i.d. Traffic

Tracy(Yali) Liu and Dipak Ghosal
Network Labs
University of California, Davis, USA

Frederik Armknecht, Ahmad-Reza Sadeghi and Steffen Schulz
System Security Lab
Ruhr-Universität Bochum, Germany

Stefan Katzenbeisser
Security Engineering Group
TU Darmstadt, Germany

Main Motivation:
Steganographic Communication over Network Traffic



Steganographic Channels

- **Common types**
  - Storage channels - communicate by modifying a stored object
  - Timing channels - transmit information by affecting the relative timing of events
- **Requirements**
  - Robustness - resilience to noise
  - Security - undetectable by the adversary

Our Focus

- **Timing channels based on inter-packet delays , i.e., the sending delays between successive packets.**
- **More concretely , independent and identically distributed (i.i.d.)**
- **Why i.i.d. traffic**
  - Extensively used in existing network analysis
  - Essential element in many advanced traffic models

Existing solutions…..

Existing Solutions and Problems

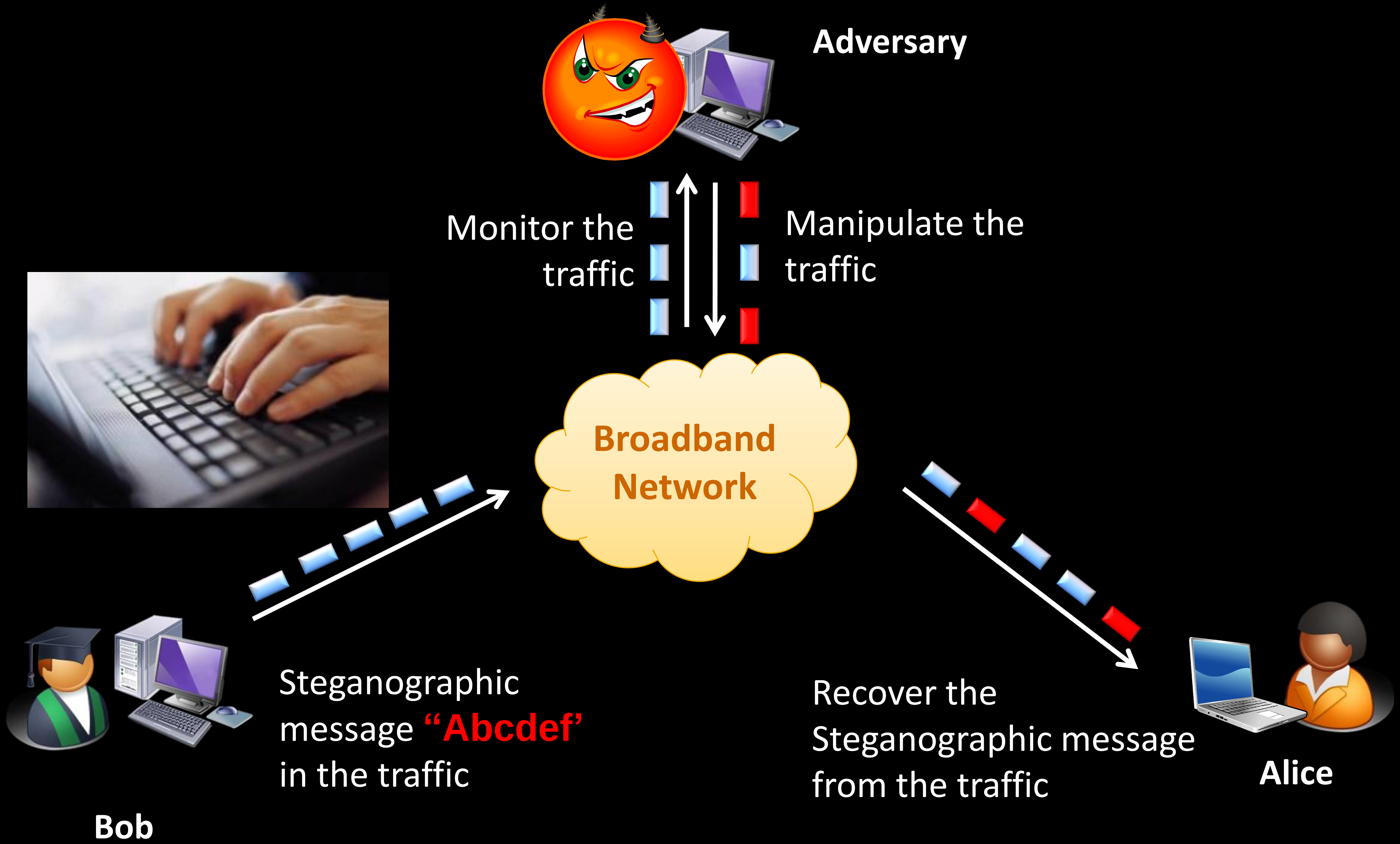
- **Common steganographic timing channels**
  - On and off
  - “small-delays” and “large-delays“
  - Perturb the inter-packet delays through small variations
  - Encoding scheme design to maximize the channel capacity – i.i.d. solution
- **Counter measures to disrupt and/or detect steganographic traffic**
  - e.g., timing jammers, statistical tests
- **Problems**
  - Security is only guaranteed under certain conditions
  - Robustness is not sufficient against noisy channels or a malicious jammer

Our Contribution

- **A novel steganographic timing channel for any legitimate traffic whose inter-packet delays are i.i.d. following an arbitrary distribution**
  - Undetectable against any (efficiently computable) statistical test
  - Robust against disruptions (caused by active adversaries and/or network noise)
- **Tunable encoding parameters allow to trade-off**
  - Robustness
  - Transmission rate
- **Validation on real telnet traffic under different network conditions**

Steganographic Channel in Telnet Traffic

- Telnet traffic: i.i.d. inter-packet delays

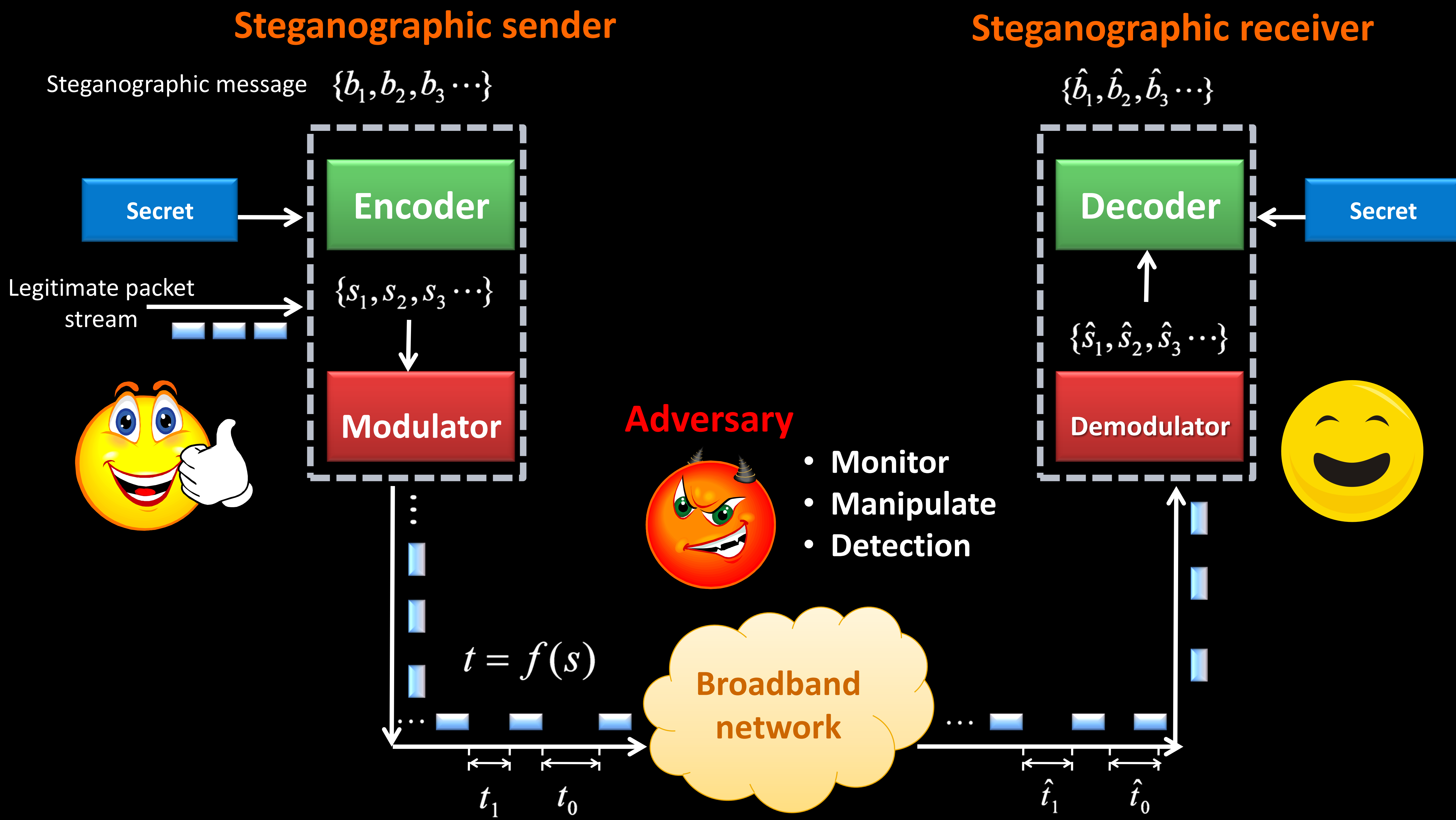


And Our Solution…..

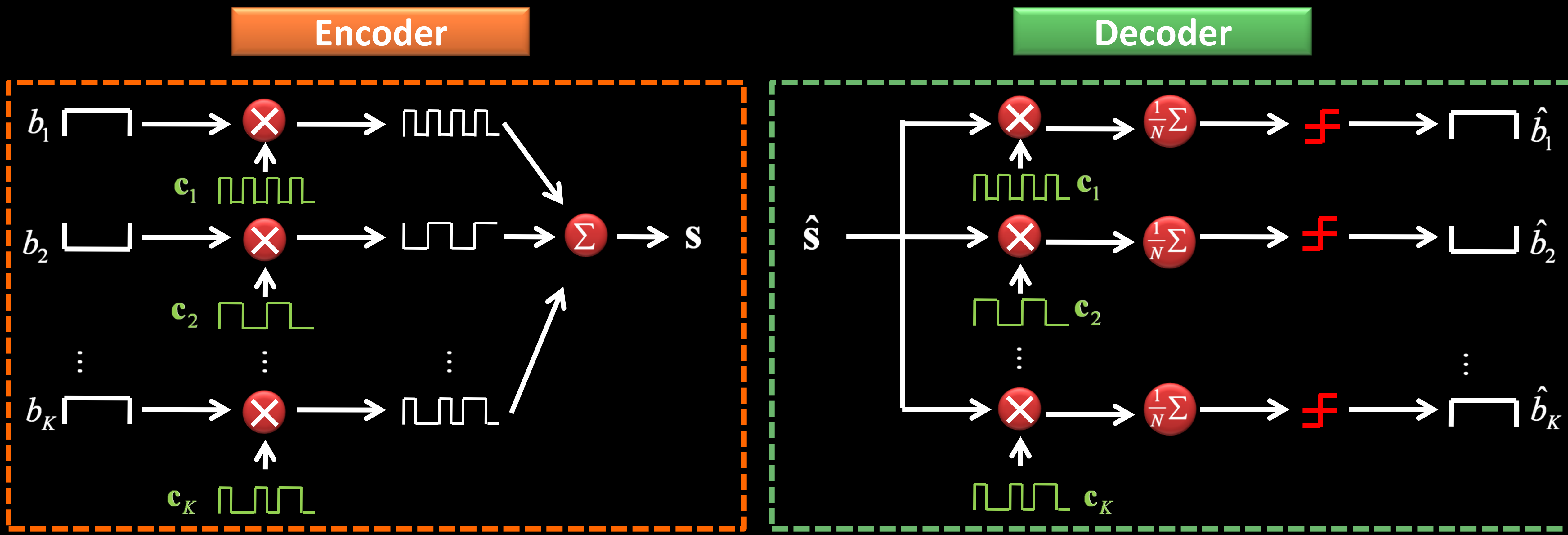
Design Objectives & Requirements

- **Undetectability**
  - Indistinguishability: adversary cannot indistinguish between the legitimate and steganographic traffic
- **Robustness**
  - Resistance to noise (malicious or non-malicious)
  - Decoding error probability: Bit Error Rate (BER) P_e
  - Robustness gain: time to increase SNR γ
    - P_e is inverse function of SNR

System Overview



Encoding with Spreading Codes



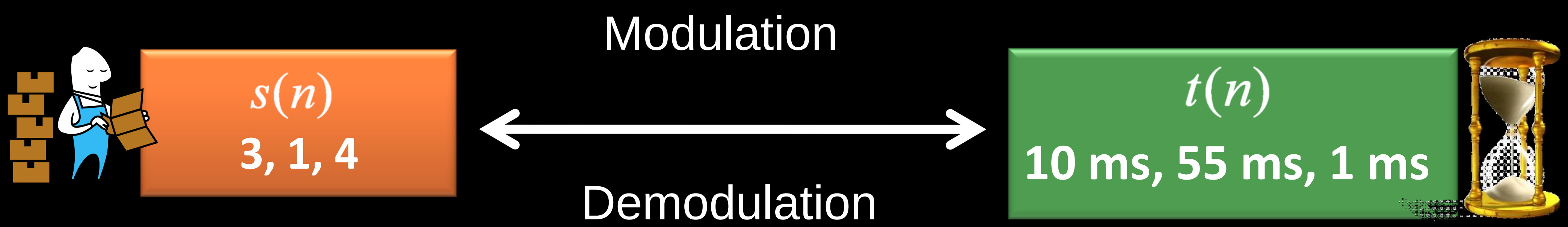
- **Uses unique spreading codes to spread the baseband data before transmission**
- **Low bit error rate (BER) – spreading gain N**
  - Noise power decreases by N
- **High transmission rate – orthogonal codes**
  - $\mathbf{s} = \sum_{k=1}^{K} b_k \cdot \mathbf{c}_k \qquad \langle \mathbf{c}_i, \mathbf{c}_j \rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$

K : total number of channel

$R_t = K/N$: transmission rate

Modulation to Address Statistical Detection

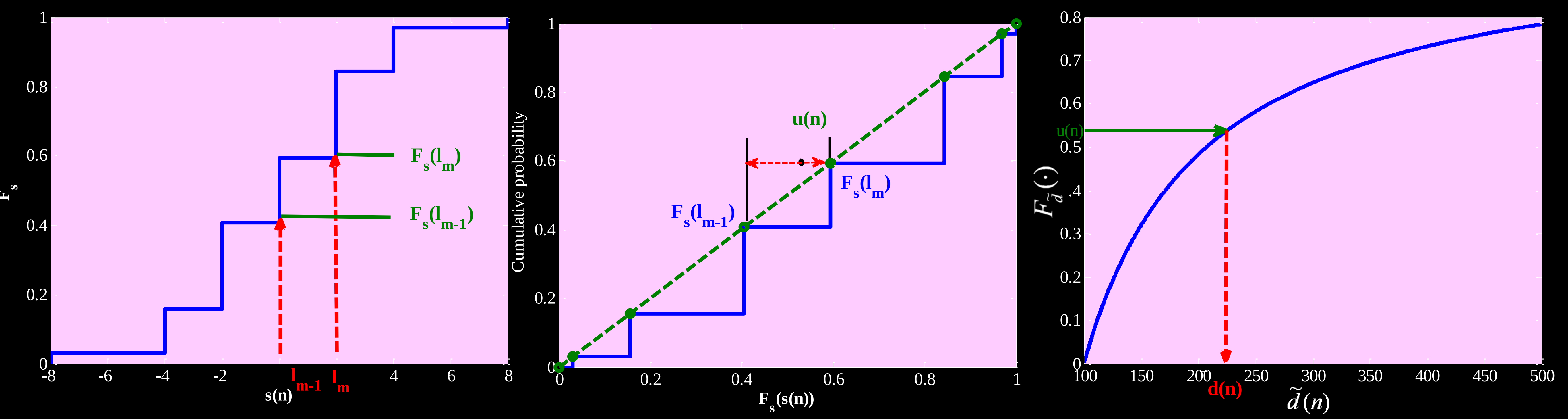
- **Function**



- **Priori knowledge**
  - Characteristics of the legitimate network traffic
- **Requirements**
  - Invertible mapping
  - Evade any statistical tests

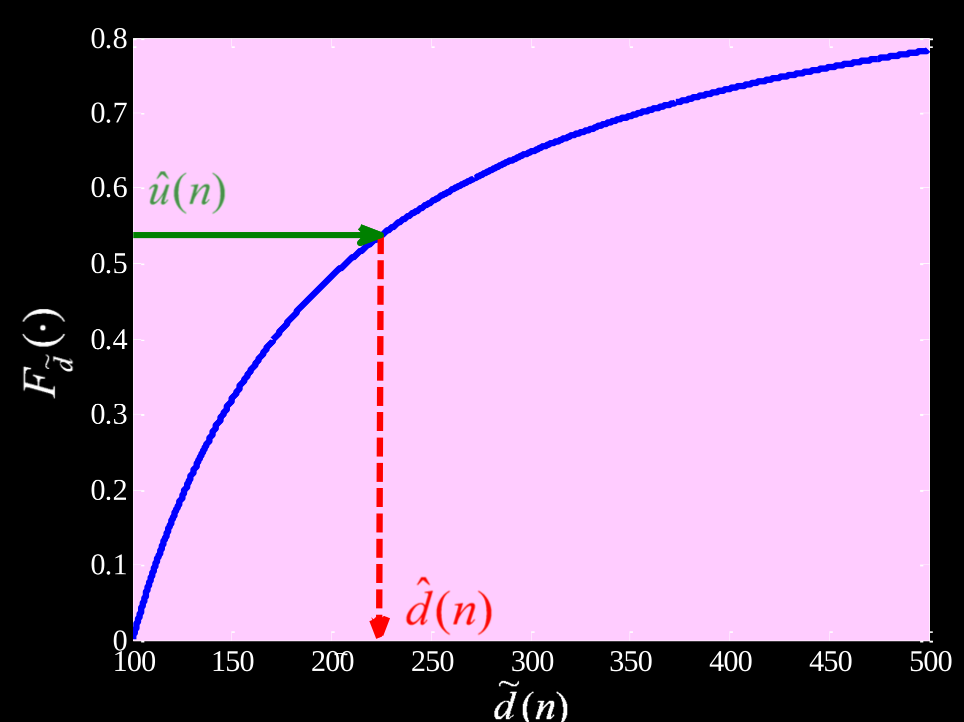
Undetectable Modulation (1)

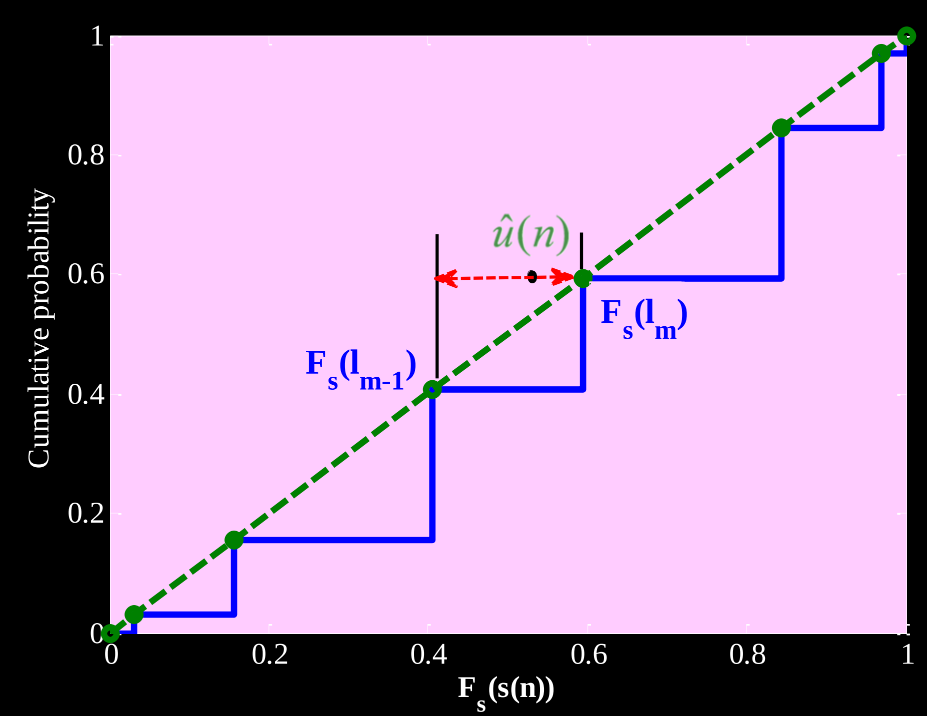
- **Inverse function based modulation scheme**
  - $u(n) = F_s(l_{m-1}) + (F_s(l_m) - F_s(l_{m-1})) \cdot v(n)$
  - $d(n) = F_{\tilde{d}}^{-1}(u(n))$
    - $F_s(\cdot)$ CDF of code symbol s(n)
    - $F_{\tilde{d}}(\cdot)$ CDF of legitimate traffic



Undetectable Demodulation (2)

- **Additive noise during transmission**
  - $\hat{d}(n) = d(n) + x(n)$
- **Inverse function based demodulation scheme**
  - $\hat{u}(n) = F_{\tilde{d}}(\hat{d}(n))$
  - $\hat{s}(n) = l_m \quad$ if $\quad \hat{u}(n) = \in (F_s(l_{m-1}), F_s(l_m)]$
  - $\hat{b}_k = \frac{1}{N}(\hat{\mathbf{s}}, \mathbf{c}_k) = b_k + \frac{1}{N}\langle \mathbf{x}, \mathbf{c}_k \rangle$

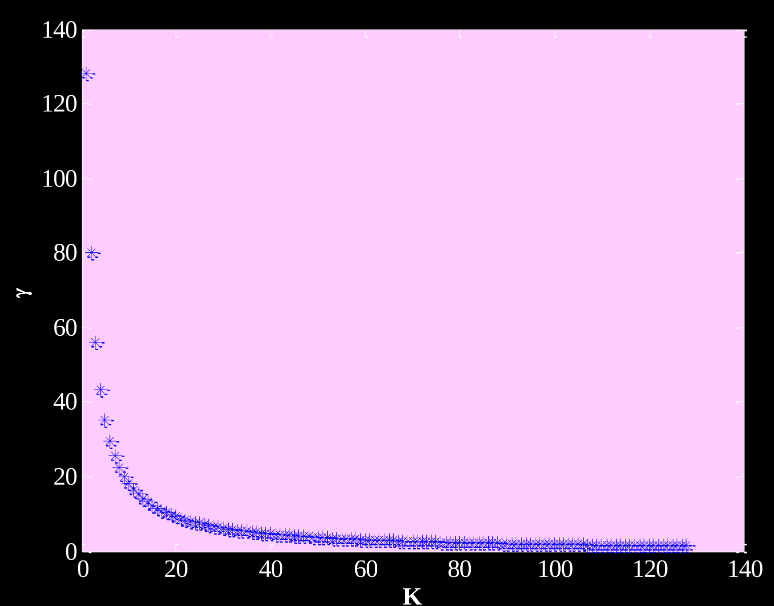


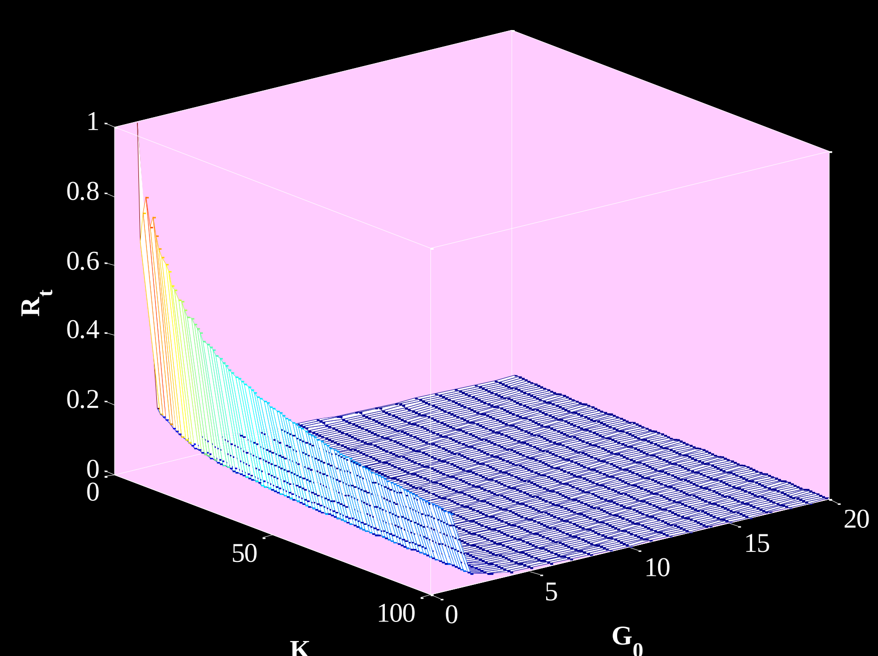


Determining Model Parameters

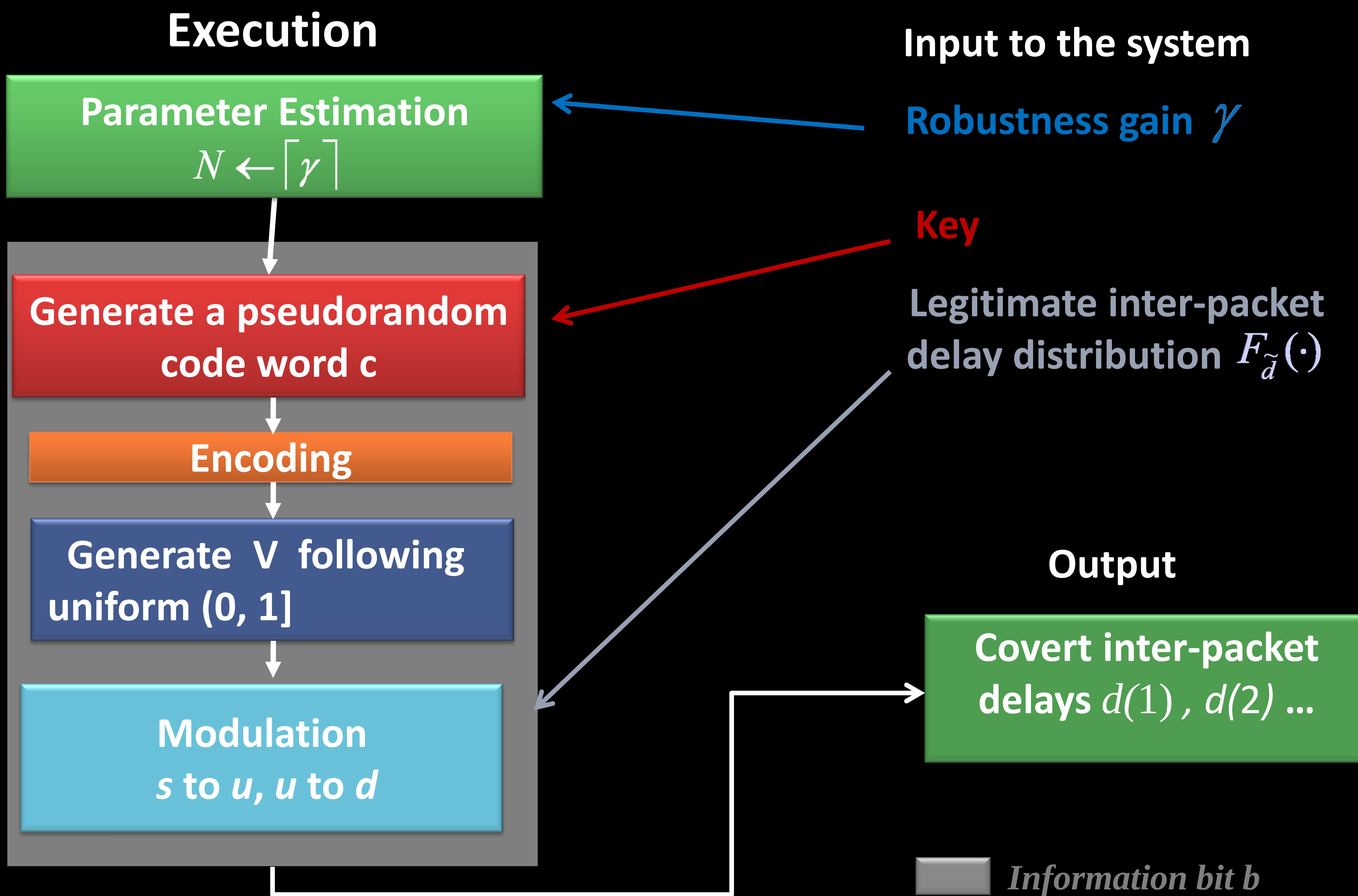
- **Modulation – compression**
- **Robustness gain – effective processing gain**
  - The SNR after performing the encoding and modulation process to the one without encoding and modulation scheme.

$$\gamma = N\frac{1}{M}\sum_{i=1}^{M}\frac{(F_s(l_i)-F_s(l_{i-1}))^2}{(\frac{1}{2})^2} = \frac{4N}{K+1}(\tfrac{1}{2})^{2K}\sum_{j=0}^{K}\binom{K}{j}^2$$





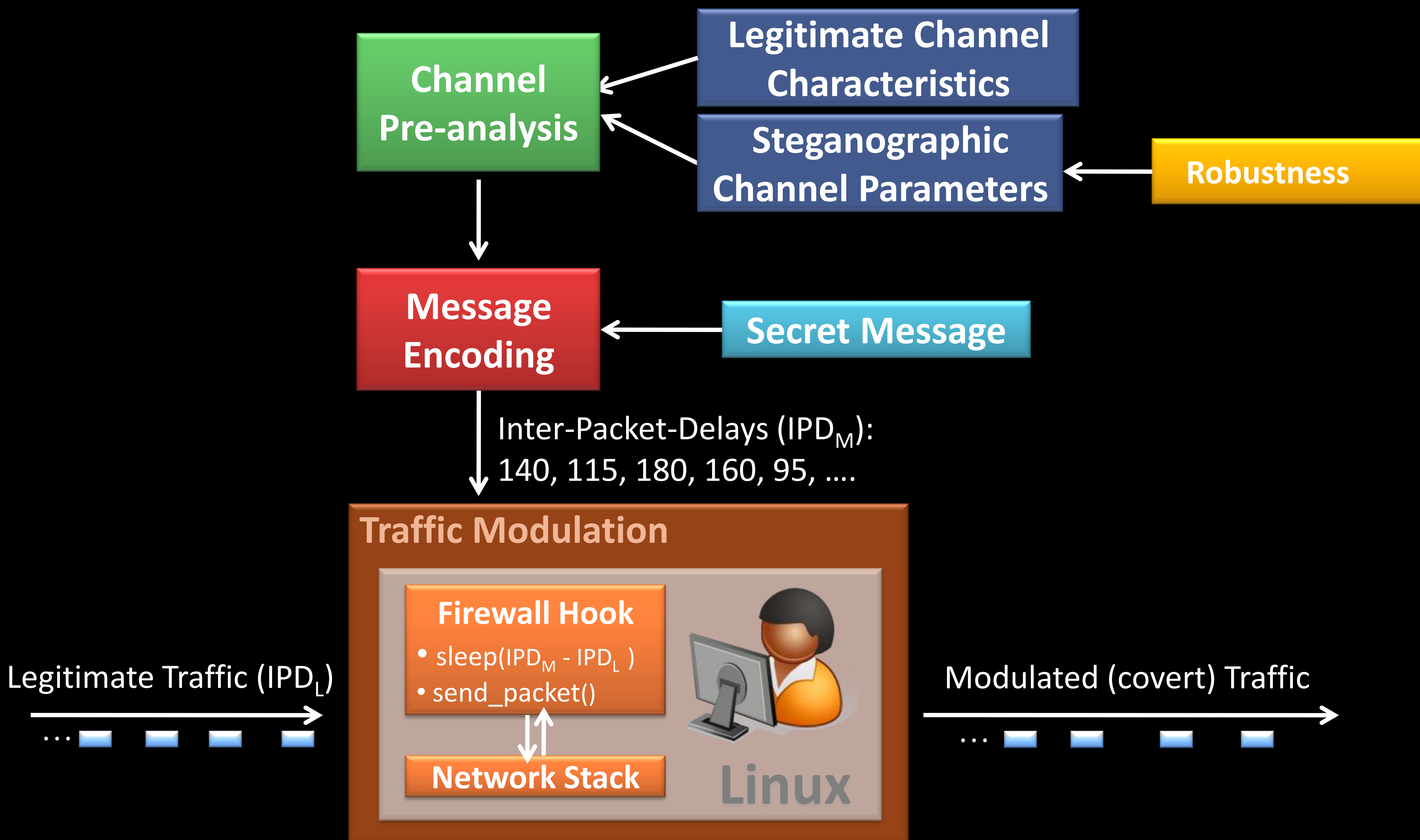
Algorithm Summary



Experimental Setup

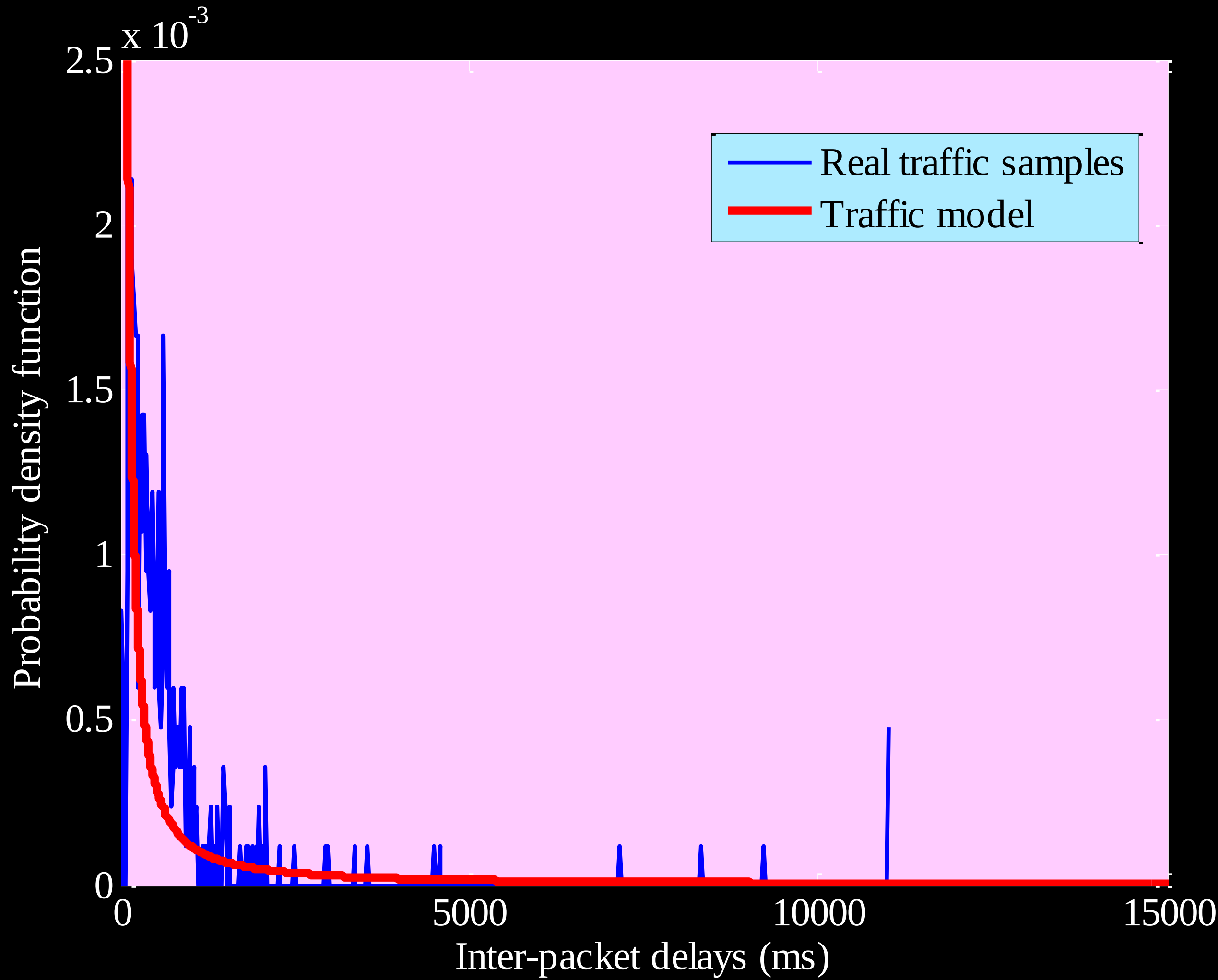
- **Simulation of the legitimate traffic**
  - Network client sends packets in exact same inter-packet delays as desired traffic
  - Content of packets is a counter to identify packet loss, dupes and order of arrival
- **Physical setup**
  - WAN: Two Linux servers at RUB and UC Davis
  - LAN: Two Linux servers at UC Davis
  - Active adversary
    - A network sniffer at the receiver
    - Injects noise at the sender
- **Real traffic traces from online archive dataset: MAWI working group traffic archive**

Implementation Architecture

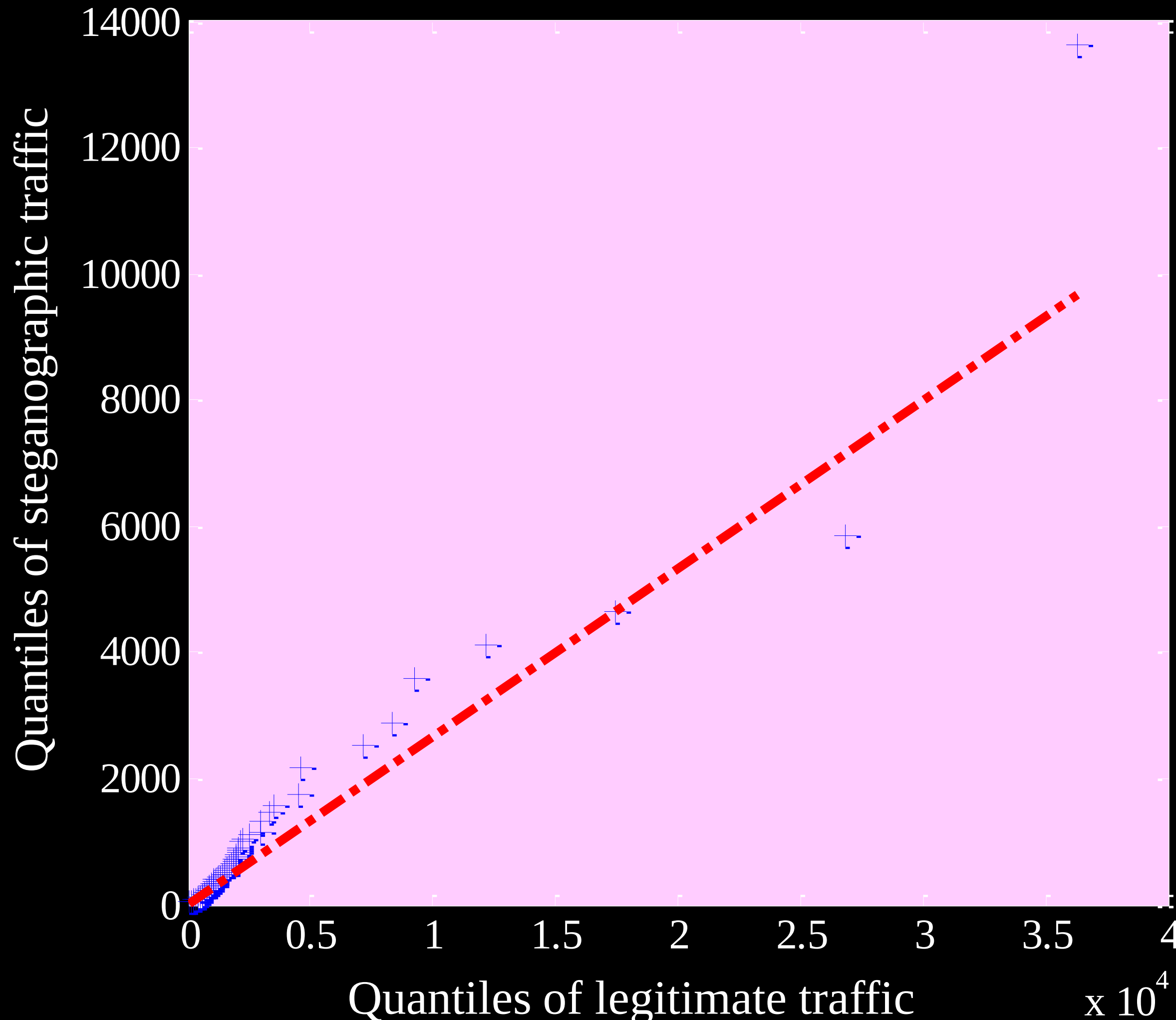


Undetectability Visualization

Telnet $F(\tilde{d}) = 1 - \left(\frac{\alpha}{\tilde{d}}\right)^{\beta}$ scale parameter α = 49 ms, shift parameter β = 0.93



Traffic Modeling



Q – Q plot

Robustness Evaluation

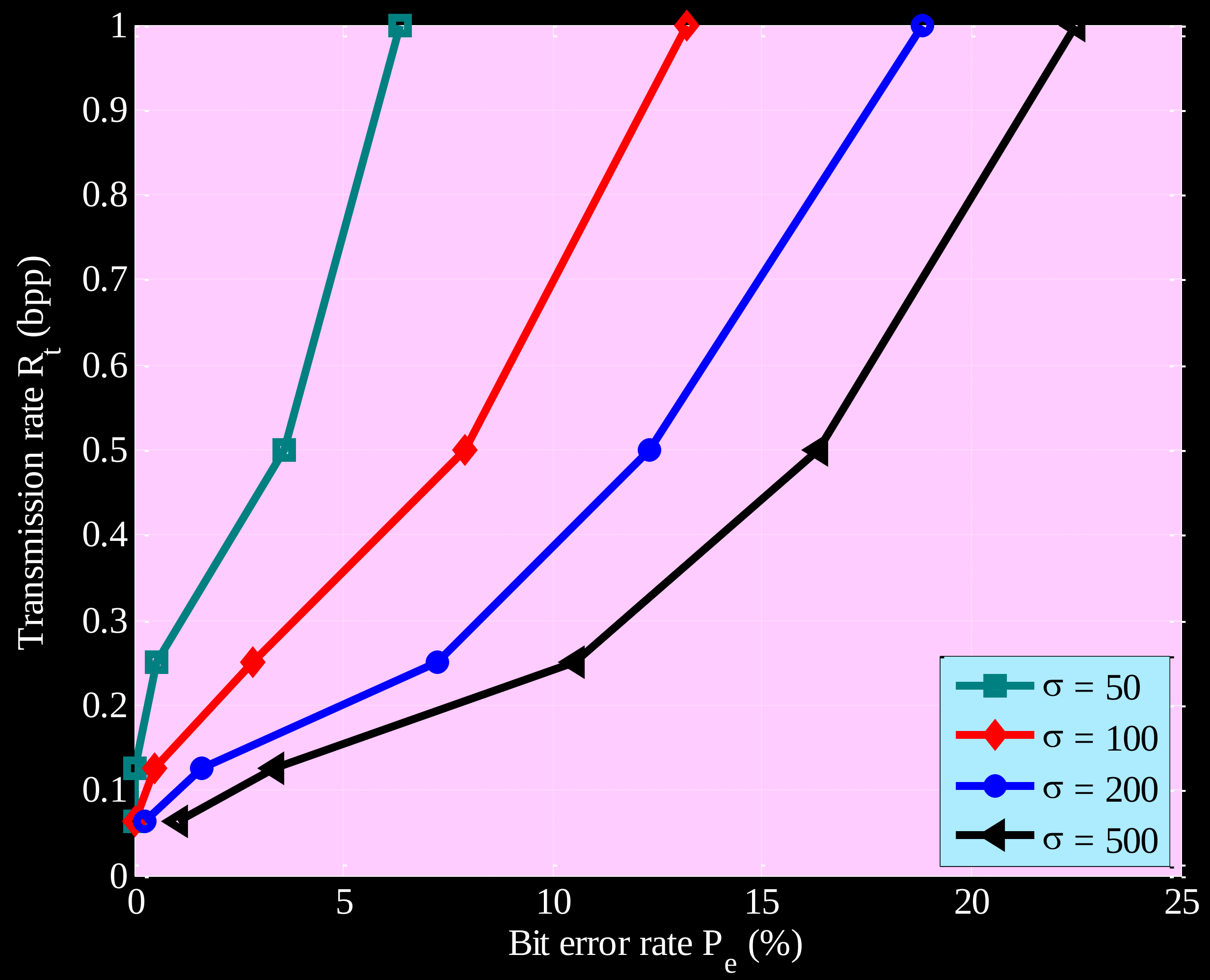
Bit error rate P_e for the experiments in the LAN

Encoding scheme		LAN	Gaussian σ^2(ms²)				Uniform $\Delta^2/12$ (ms²)			
			100	200	400	900	100	200	400	900
γ spreading	1	0	4.67	9.97	24.87	33.97	18.93	31.34	52.01	67.43
	5	0	0	0.0003	0.23	1.27	0.20	1.13	6.33	20.37
	10	0	0	0	0	3.63	0	0	0.60	4.33

Bit error rate P_e for the experiments in the WAN

Encoding scheme		WAN	Gaussian σ^2(ms²)				Uniform $\Delta^2/12$ (ms²)			
			100	200	400	900	100	200	400	900
γ spreading	1	0.02	6.01	10.22	26.93	34.98	20.10	33.23	55.89	69.87
	5	0	0.0006	0.01	0.26	1.56	0.44	1.78	8.29	23.67
	10	0.01	0	0	0.0003	4.01	0	0	1.23	5.64

Evaluation Tradeoff



The **performance trade-off** **between the** **transmission rate** R_t **and** **bit error rate** P_e (under jammed uniform noise) **.**

Conclusion, Discussion, Future Work

- **We propose a method to modulate a steganographic timing channel on network traffic with independent and identically distributed (i.i.d.) inter-packet delays.**
- **It is both robust and provably undetectable and allows to balance**
  - **Robustness against network noise**
  - **Transmission rate**
- **We experimentally validate establishing steganographic channel using real Telnet traffic**
- **Work in progress**
  - Extension of our approach for real applications such as video streaming or Voice over IP (VOIP)