Unobservable Covert Streaming for Internet Censorship Circumvention

Síntese de Vídeo para Evasão de Censura na Internet

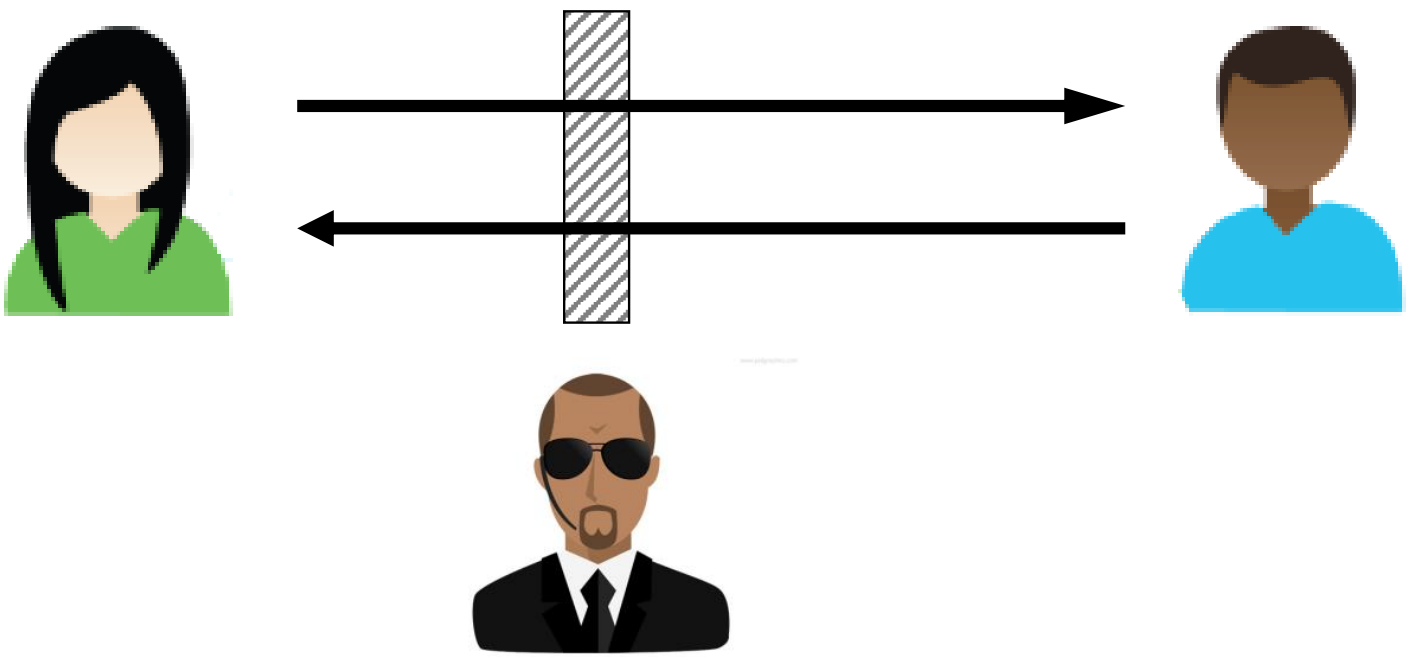
Diogo Barradas Nuno Santos Luís Rodrigues

INESC-ID / Instituto Superior Técnico, Universidade de Lisboa

September, 2016

Repressive regimes monitor Internet access

Diogo Barradas, Nuno Santos, Luís Rodrigues

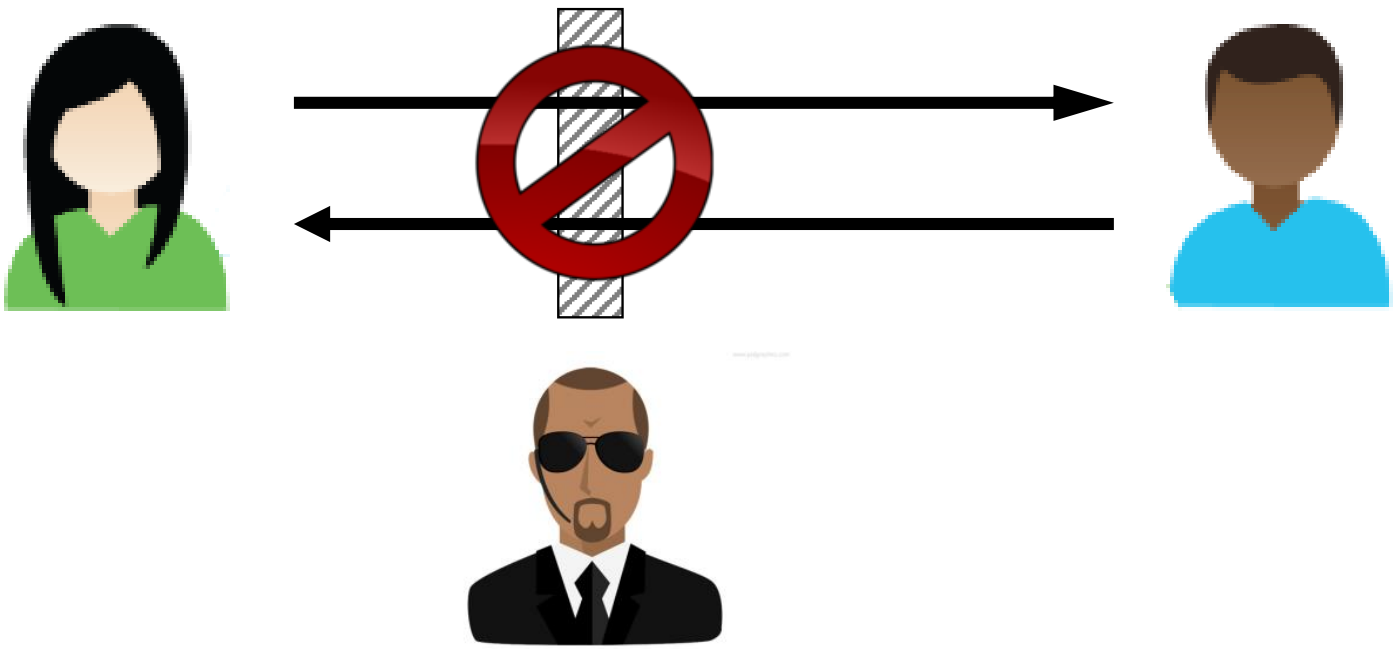


Repressive regimes monitor Internet access

Diogo Barradas, Nuno Santos, Luís Rodrigues

Censors monitor tra□c flows

- Citizens may be prevented from accessing/publishing information

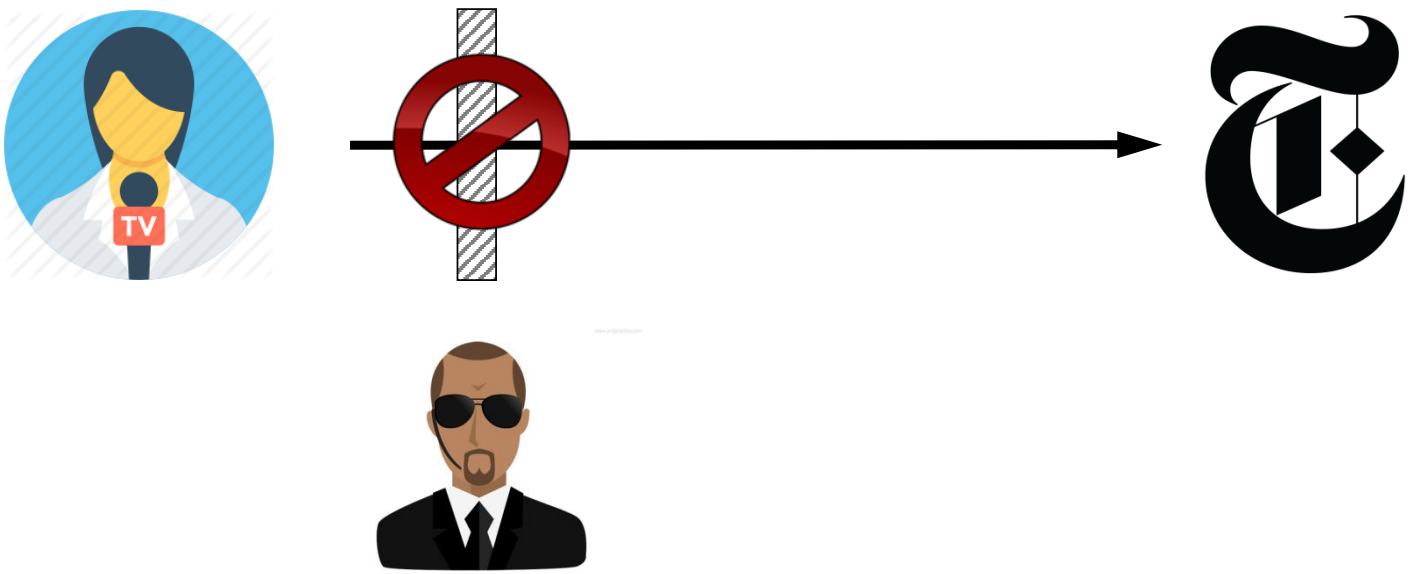


Repressive regimes monitor Internet access

Diogo Barradas, Nuno Santos, Luís Rodrigues

Censors monitor tra□c flows

- Citizens may be prevented from accessing/publishing information

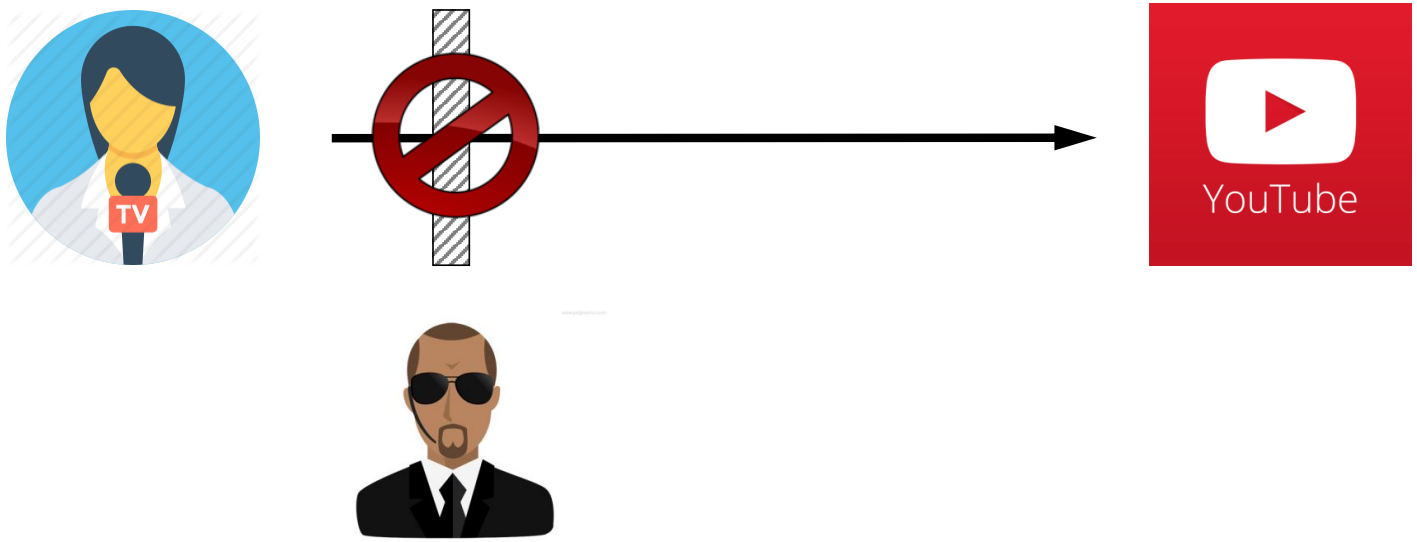


Repressive regimes monitor Internet access

Diogo Barradas, Nuno Santos, Luís Rodrigues

Censors monitor tra□c flows

- Citizens may be prevented from accessing/publishing information

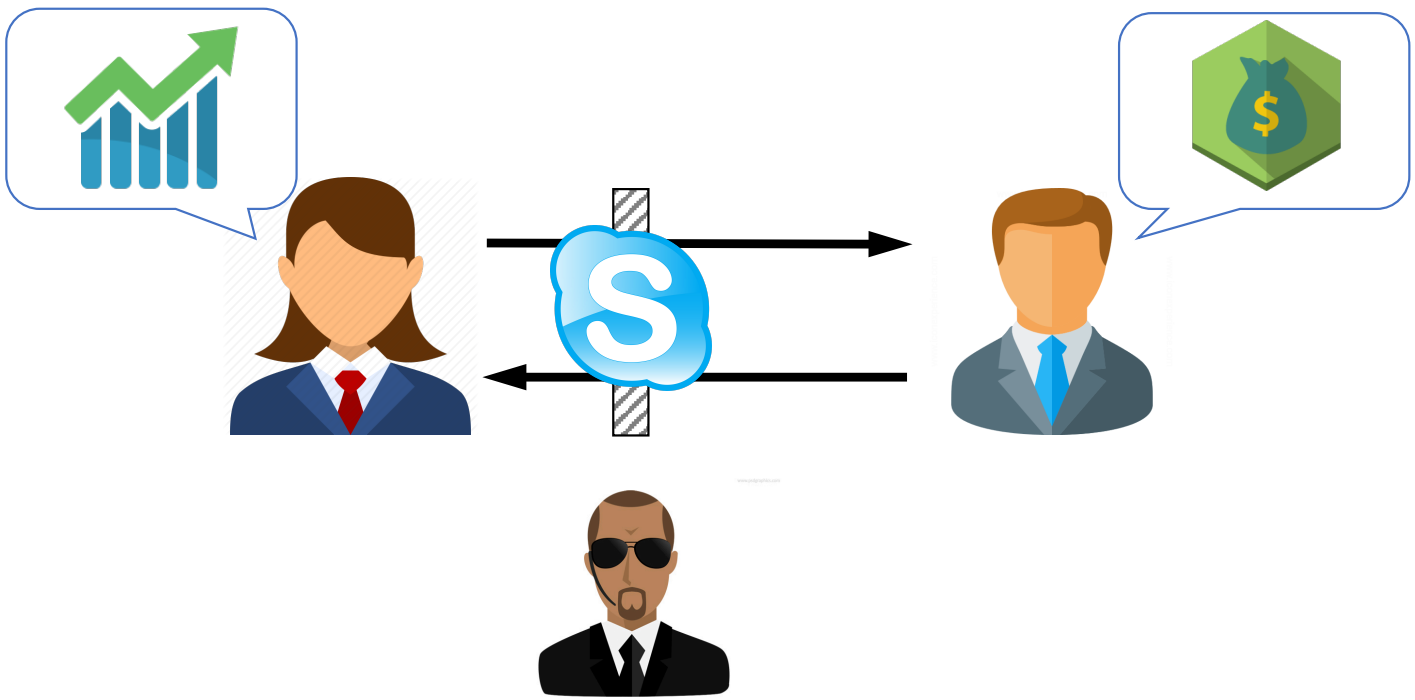


The censor avoids blocking all communication channels

Diogo Barradas, Nuno Santos, Luís Rodrigues

Preservation of critical communication services

- Important to assure the regime's sustainability



How does the censor block rightful information?

Several techniques:

- HTTP requests filtering
- DNS Hijacking
- Blocking of IP ranges

How does the censor block rightful information?

Diogo Barradas, Nuno Santos, Luís Rodrigues

Several techniques:

- HTTP requests filtering
- DNS Hijacking
- Blocking of IP ranges

Detection / blocking of covert channels

- Network Perturbations (Active Attacks)
- Statistical Tra□c Analysis (Passive Attacks)

Tunneling data through multimedia protocols

Diogo Barradas, Nuno Santos, Luís Rodrigues

Desirable characteristics:

- Resistance to active/passive attacks
- Arbitrary data transmission
- Interactive communication
- Reasonable throughput

Paper contributions

This paper proposes a censorship resistant communication system which o□ers the transmission of data:

- Through TCP/IP
- Without the need to change client/server applications
- Resistant against active attacks
- Resistant against *state-of-the-art* tra□c analysis

Agenda

1. Introduction
2. Our solution
   - Threat Model
   - Design
   - Implementation
3. Evaluation
4. Conclusions

Threat Model

Diogo Barradas, Nuno Santos, Luís Rodrigues

Hypothesis

- The video-conferencing application encrypts the content of the packets carrying multimedia data (ex: Skype)

Threat Model

Diogo Barradas, Nuno Santos, Luís Rodrigues

Hypothesis

- The video-conferencing application encrypts the content of the packets carrying multimedia data (ex: Skype)

Censor's Capabilities:

- *Deep Packet Inspection*
- Observe, store and analyze tra□c flows
- Apply artifical constraints on the network

Threat Model

Diogo Barradas, Nuno Santos, Luís Rodrigues

Hypothesis

- The video-conferencing application encrypts the content of the packets carrying multimedia data (ex: Skype)

Censor's Capabilities:

- *Deep Packet Inspection*
- Observe, store and analyze tra□c flows
- Apply artifical constraints on the network

Censor's Limitations:

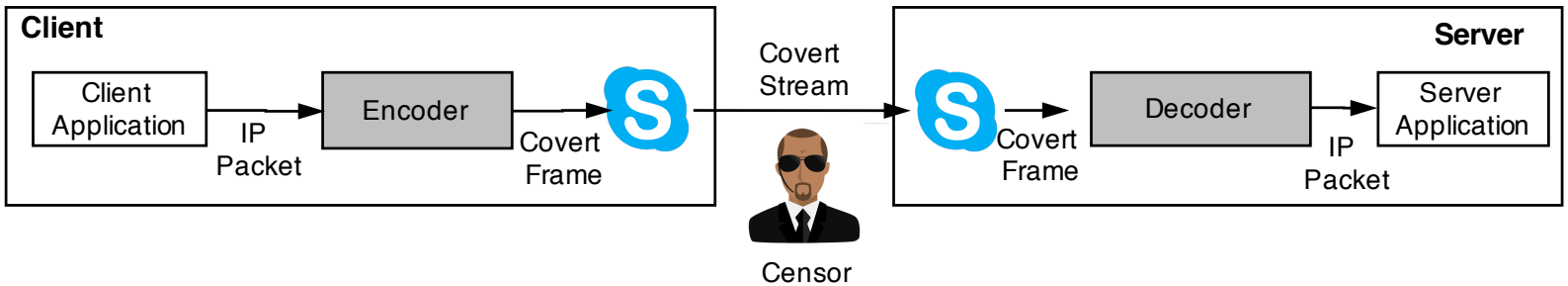
- Unable to decipher the content of Skype packets
- Not in collusion with the video-conferencing service provider
- Attempts to minimize collateral damage

TÉCNICO LISBOA

Agenda

Communication Model

Diogo Barradas, Nuno Santos, Luís Rodrigues



Allow the communication between client/server applications:

- through TCP/IP
- modulating data into video-frames
- sending the modified frames through Skype

Design Challenges

1. Conflicting encoding requirements
   - Data tunneling changes the patterns of Skype streams
2. Preserve the signature of legitimate Skype tra□c
   - Characterize Skype streams
3. Periodic adaptation
   - Skype streams' patterns are a□ected by network conditions
4. Synchronization resistant to active attacks
   - The censor may attempt to prevent the channel's synchronization

Design Challenges

1. Conflicting encoding requirements
   - Data tunneling changes the patterns of Skype streams
2. Preserve the signature of legitimate Skype tra□c
   - Characterize Skype streams
3. Periodic adaptation
   - Skype streams' patterns are a□ected by network conditions
4. Synchronization resistant to active attacks
   - The censor may attempt to prevent the channel's synchronization

Design Challenges

1. Conflicting encoding requirements
   - Data tunneling changes the patterns of Skype streams
2. Preserve the signature of legitimate Skype tra□c
   - Characterize Skype streams
3. Periodic adaptation
   - Skype streams' patterns are a□ected by network conditions
4. Synchronization resistant to active attacks
   - The censor may attempt to prevent the channel's synchronization

Design Challenges

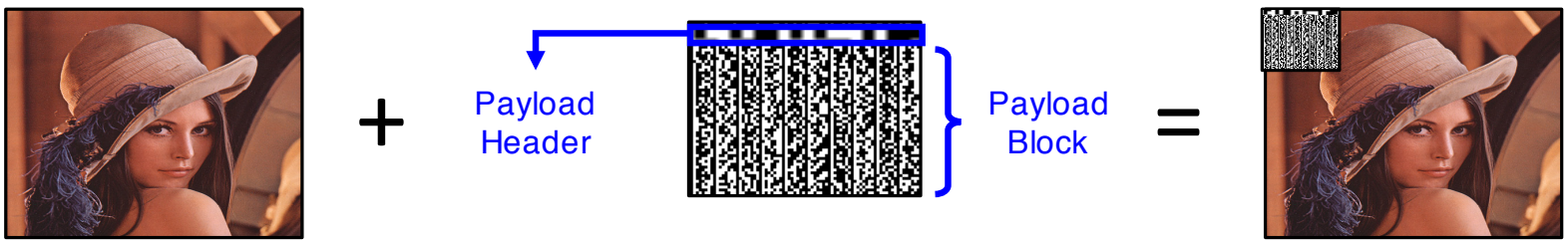
1. Conflicting encoding requirements
   - Data tunneling changes the patterns of Skype streams
2. Preserve the signature of legitimate Skype tra□c
   - Characterize Skype streams
3. Periodic adaptation
   - Skype streams' patterns are a□ected by network conditions
4. Synchronization resistant to active attacks
   - The censor may attempt to prevent the channel's synchronization

How to encode IP packets into video?

Diogo Barradas, Nuno Santos, Luís Rodrigues

1 - Conflicting encoding requirements

Encoding of IP packets in pixels



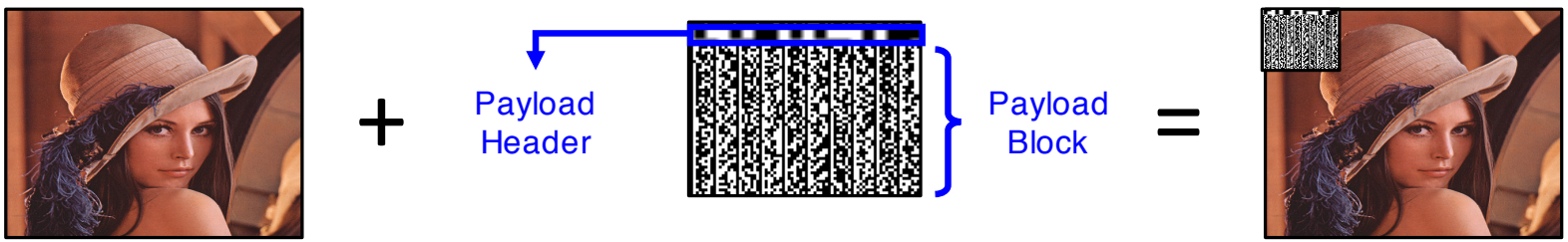
(a) Carrier Frame (b) Payload Frame (c) Covert Frame

How to encode IP packets into video?

Diogo Barradas, Nuno Santos, Luís Rodrigues

1 - Conflicting encoding requirements

Encoding of IP packets in pixels

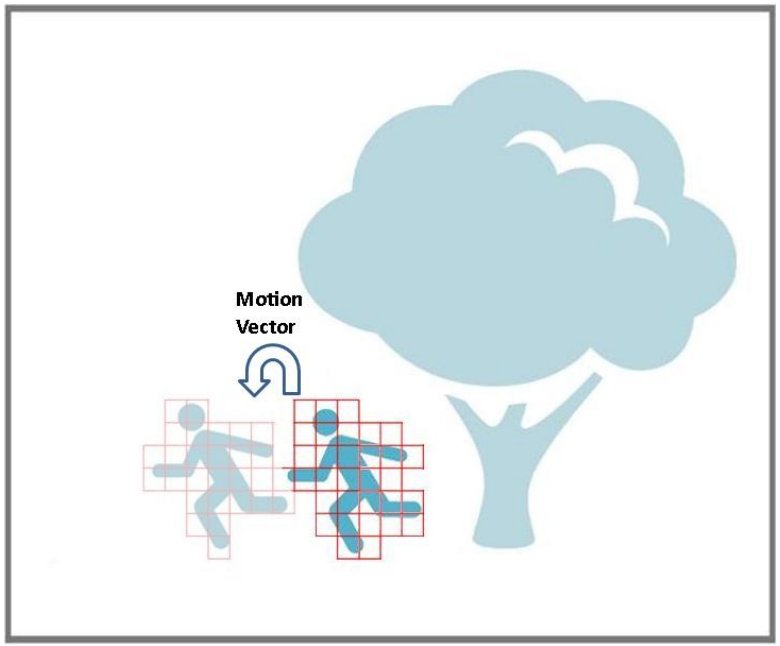


(a) Carrier Frame (b) Payload Frame (c) Covert Frame

Name	Description
s_p	payload frame area (pixel$\times$pixel)
s_c	cell size (pixel$\times$pixel)
b_c	color encoding (bits)
r_p	payload frame rate (frames/s)

How to find a balance between observability and throughput?

Diogo Barradas, Nuno Santos, Luís Rodrigues



1 - Conflicting encoding requirements

- Compression leverages similarities between frames
- "Irregular" frames change tra□c patterns
- Data encoding must be adjusted

How to create unobservable streams?

Diogo Barradas, Nuno Santos, Luís Rodrigues

2 - Preserve the signature of legitimate Skype traffic

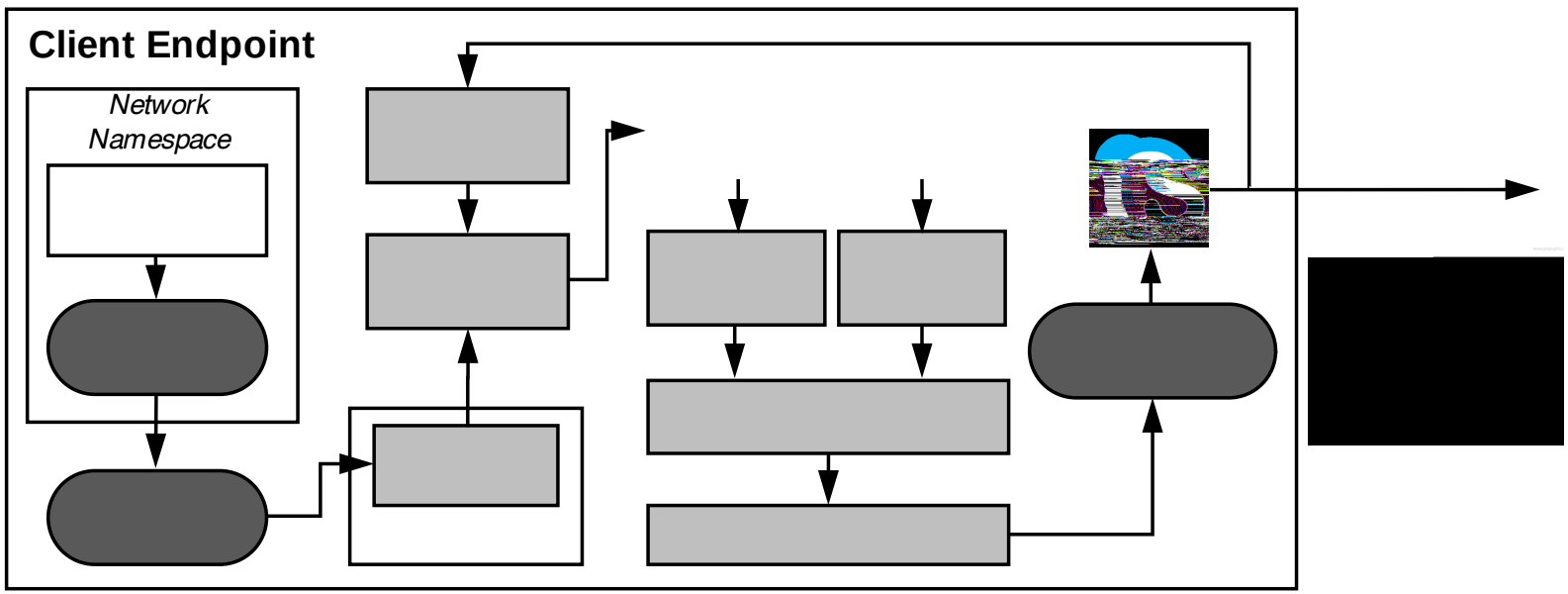
- Quantitatively characterize Skype streams
  - Packet length frequency distribution
- Quantify the differences between Skype streams
  - *Earth Mover's Distance*

Implementation Challenges

- Network Interaction
  - How to make TCP/IP communication possible?
- Video Processing
  - How to combine frames?
- Skype Interaction
  - How to send covert frames without modifying Skype?

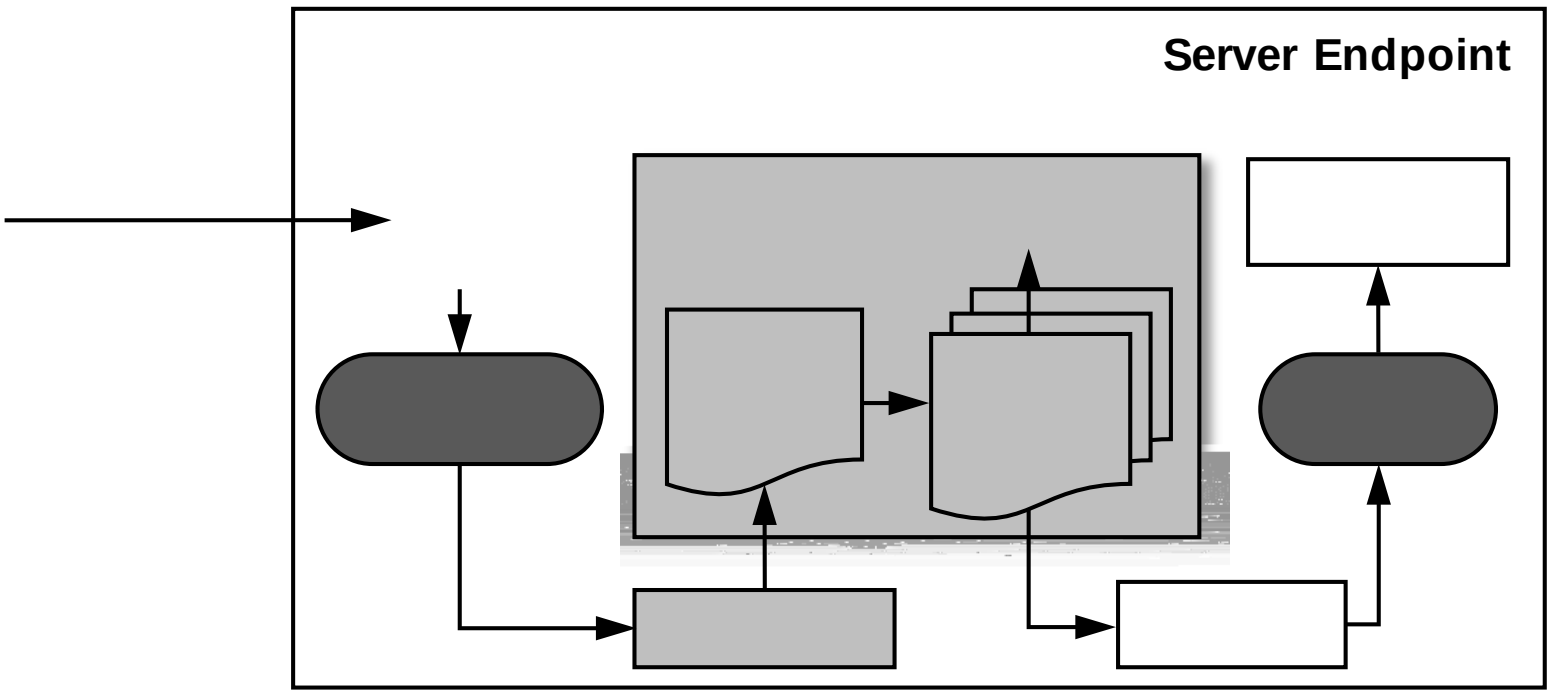
Implementation - Client

Diogo Barradas, Nuno Santos, Luís Rodrigues



Implementation - Server

Diogo Barradas, Nuno Santos, Luís Rodrigues



Aditional Implementation Features

Diogo Barradas, Nuno Santos, Luís Rodrigues

- IP packets fragmentation / reconstruction
- Error correction
- Encoding parameters calibration
- Attack resistant parameter negotiation

Agenda

Evaluation Steps

1. Definition of observability metrics
2. Verification of di□erences between streams
3. Stability of Skype streams' tra□c patterns
4. Skype streams classification
5. Generation of unobservable channels
6. Performance of the obtained channels

Experiments Configuration

Diogo Barradas, Nuno Santos, Luís Rodrigues

Experiments Configuration

- 2 VMs 32bit Linux Ubuntu 14.04.3 LTS - 2GB RAM - 4 virtual CPUs
- Skype v4.3.0.37

Streams Datasets

- 30 videos representing legitimate Skype calls
- 30 videos extracted from Youtube

Definition of observability metrics

Diogo Barradas, Nuno Santos, Luís Rodrigues

Characteristic Function - Create a stream signature

- Frequency distribution of packet lengths

Definition of observability metrics

Characteristic Function - Create a stream signature

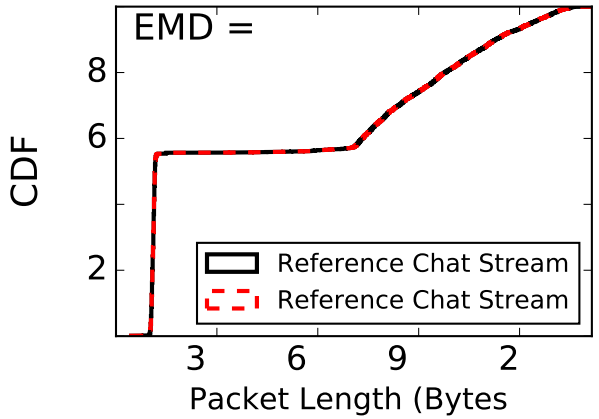
- Frequency distribution of packet lengths

Similarity Function - Quantify differences among streams

- *Earth Mover's Distance*
  - Cost of transforming signature f_1 on signature f_2

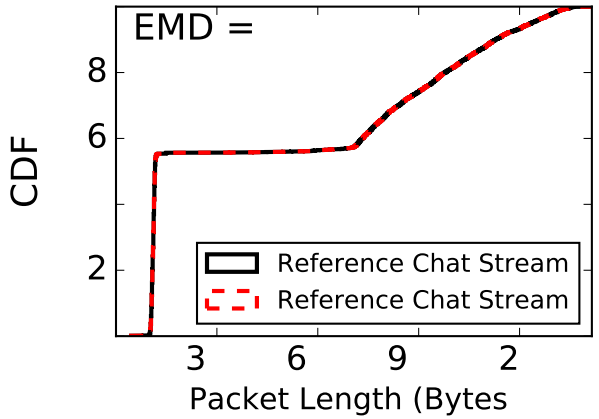
Are there differences among regular/irregular streams?

Diogo Barradas, Nuno Santos, Luís Rodrigues



Are there differences among regular/irregular streams?

Diogo Barradas, Nuno Santos, Luís Rodrigues

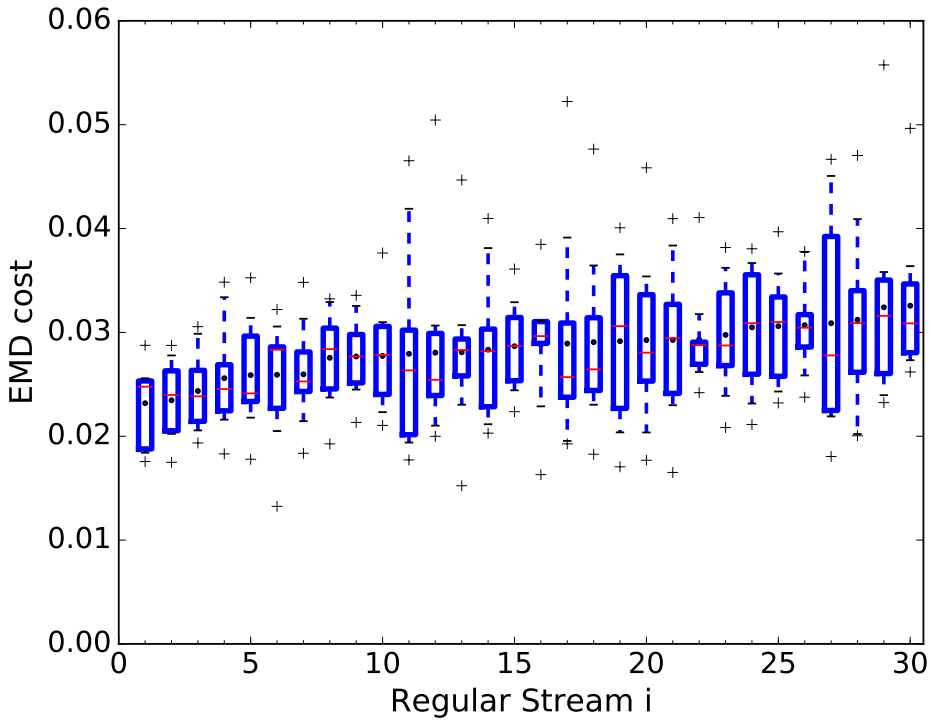


Characterization of Skype streams

- Regular/irregular streams exhibit distinct patterns

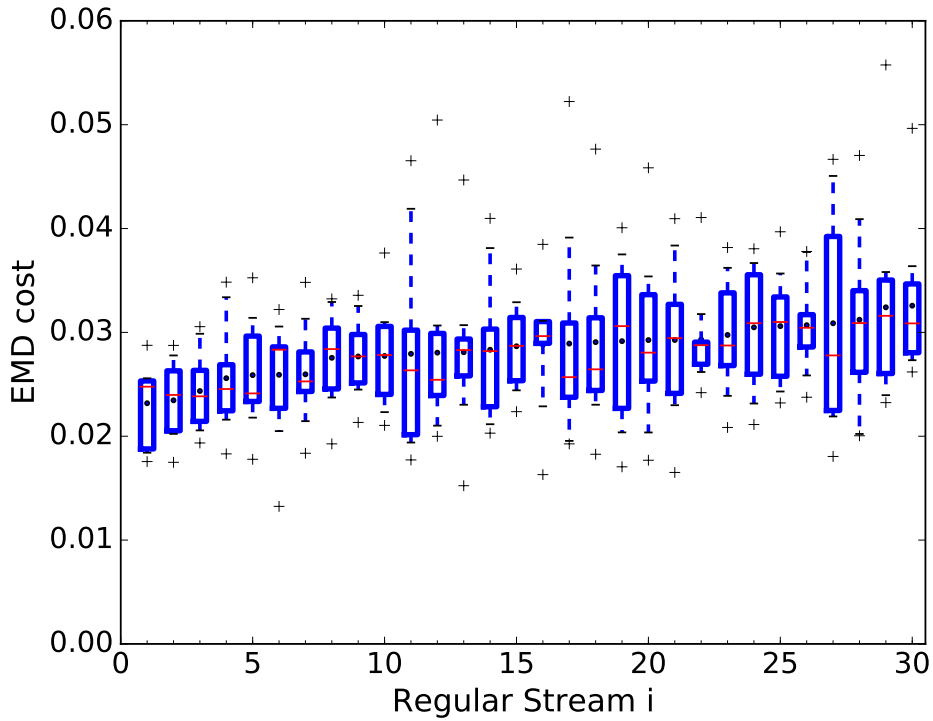
Are these patterns reliable for stream classification?

Diogo Barradas, Nuno Santos, Luís Rodrigues



Are these patterns reliable for stream classification?

Diogo Barradas, Nuno Santos, Luís Rodrigues

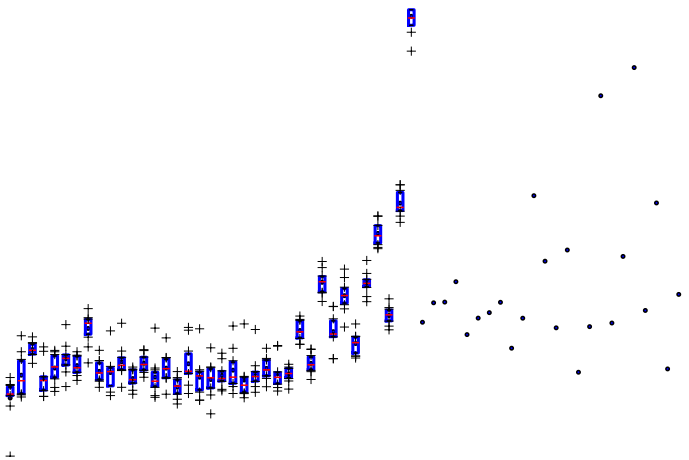


Characterization of Skype streams

- These patterns appear to be stable
  - Max. di□erence of 2% (between 25% and 75% quartiles)

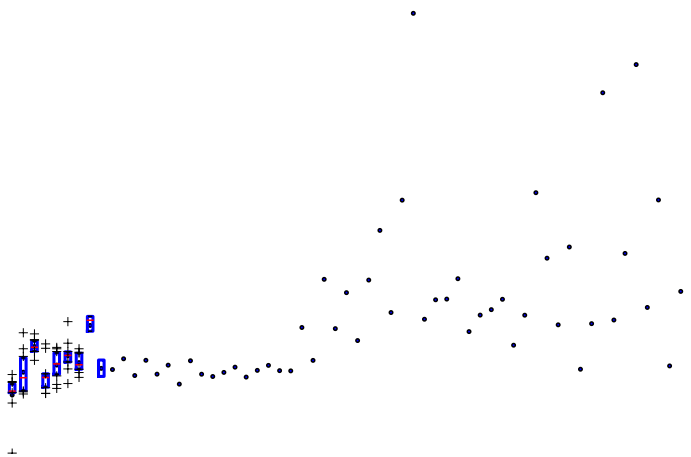
Is it possible to accurately distinguish Skype streams?

Diogo Barradas, Nuno Santos, Luís Rodrigues



Is it possible to accurately distinguish Skype streams?

Diogo Barradas, Nuno Santos, Luís Rodrigues



Is it possible to accurately distinguish Skype streams?

Diogo Barradas, Nuno Santos, Luís Rodrigues

Is it possible to create unobservable streams?

Diogo Barradas, Nuno Santos, Luís Rodrigues

Recall the encoding parameters

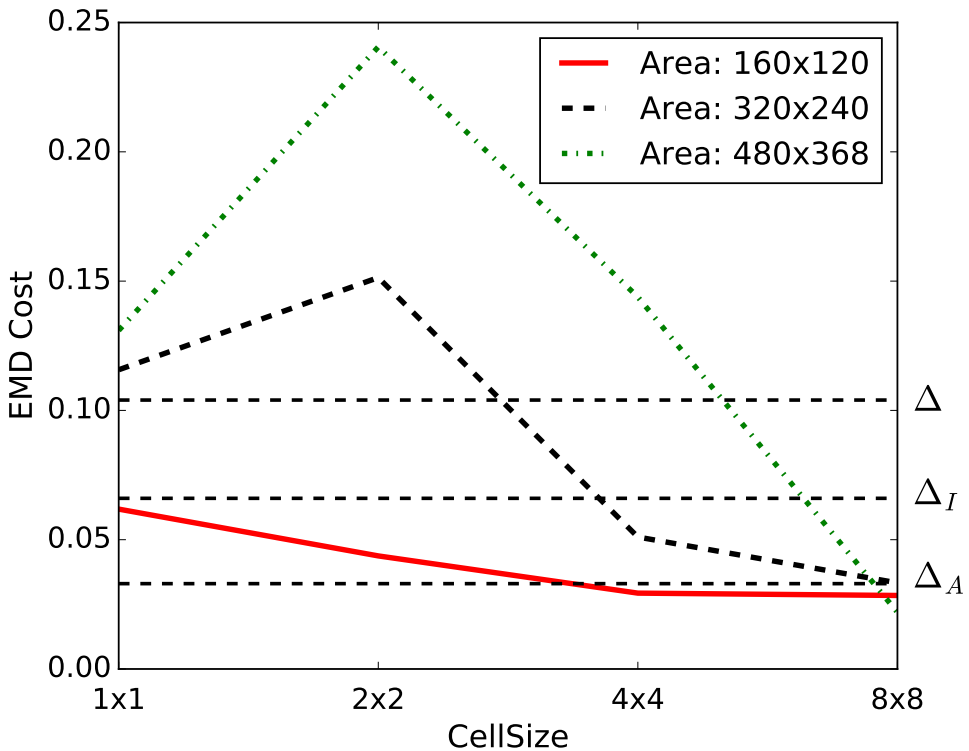
Name	Description
s_p	payload frame area (pixel$\times$pixel)
s_c	cell size (pixel$\times$pixel)
b_c	color encoding (bits)
r_p	payload frame rate (frames/s)

Is it possible to create unobservable streams?

Diogo Barradas, Nuno Santos, Luís Rodrigues

1 - Payload area VS Cell Size

- Bits p/Cell = 1



What is the performance of this channel?

Diogo Barradas, Nuno Santos, Luís Rodrigues

Can we support the execution of typical applications?

Use cases

- Comparison of execution time
  - System use vs Open channels
- Interactive sessions
  - 10x - 20x time overhead

Case	W/ System	W/o System	Overhead
A. Wget	1m 9s 830ms	7ms	9,975.7×
B. FTP	2m 45s	8s 528ms	19×
C. SMTP	2m 42s	37s 913ms	4.3×
D. SSH	1m 51s 493ms	6s 485ms	17.2×
E. Telnet	1m 17s 471ms	7s 670ms	10.1×
F. Chat Netcat	1s 147ms	11ms	133×
G. Tunel SSH	3m 46s 55ms	21s 940ms	10.3×

Results

This paper o□ers the following results:

- Implementation of the system
  - Linux / Skype
- An empirical demonstration of the transfer of arbitrary data in an unobservable way
- An experimental study of the system's performance

TÉCNICO LISBOA

Agenda