
CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia
CyCon
International Conference
on Cyber Conflict

CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence
Tallinn, Estonia

CyCon
International Conference on Cyber Conflict
30 MAY - 2 JUNE 2017, TALLINN, ESTONIA

SDN-based Network Obfuscation

Roland Meier
PhD Student
ETH Zürich

CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia

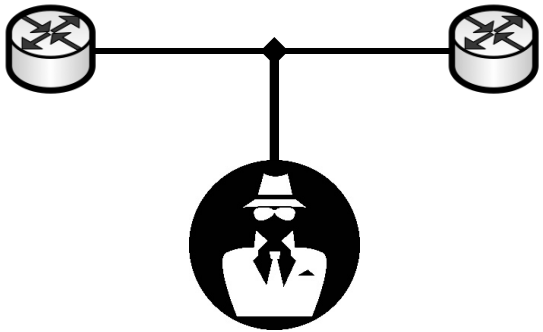
CyCON

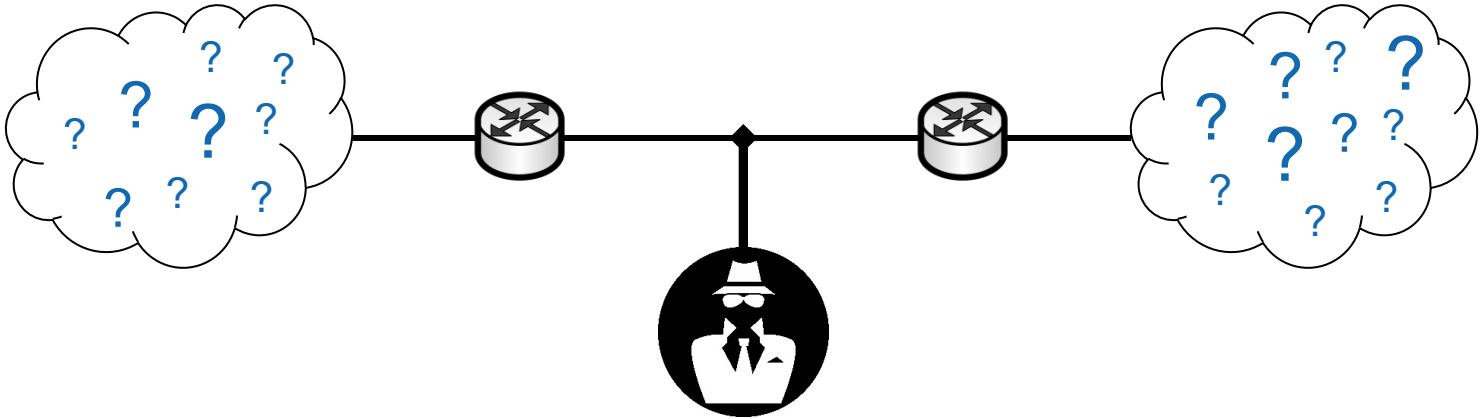
International Conference
on Cyber Conflict

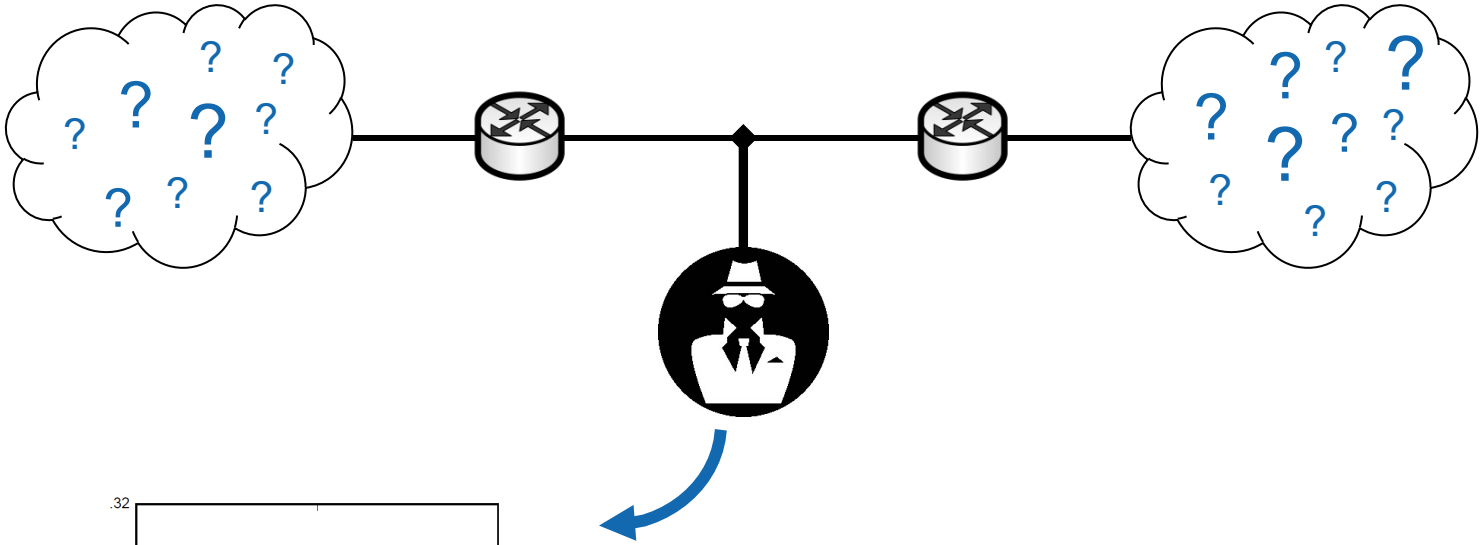
30 MAY - 2 JUNE 2017, TALLINN, ESTONIA

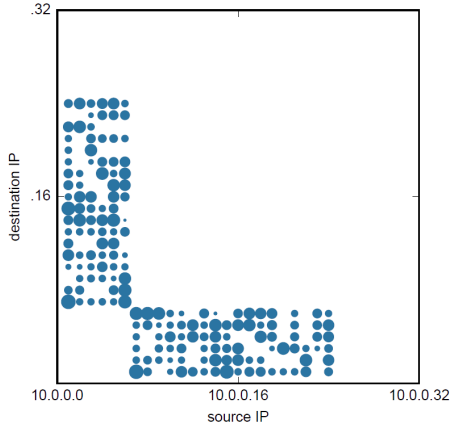
CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia

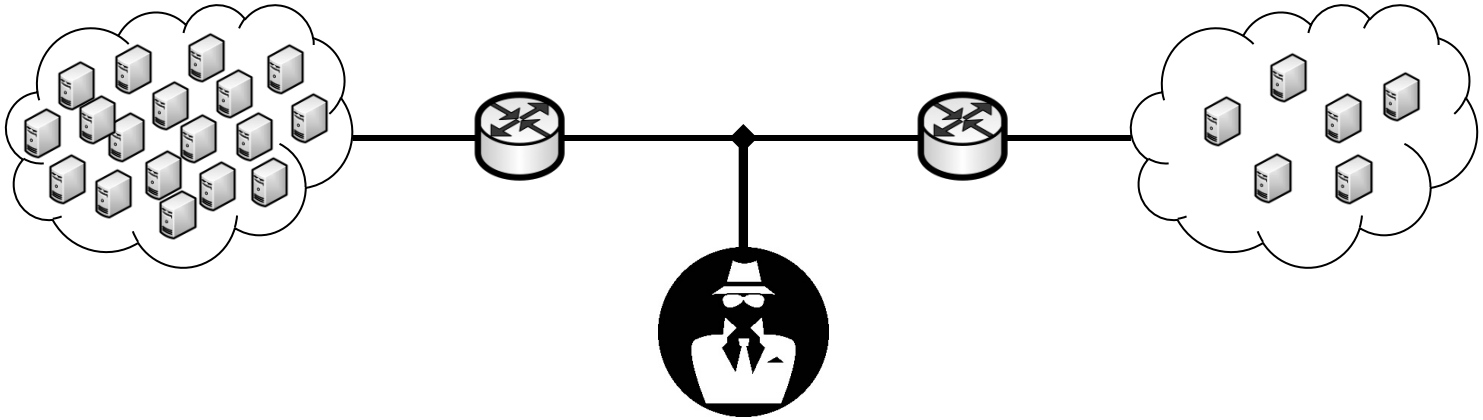
CyCON
International Conference
on Cyber Conflict
30 MAY - 2 JUNE 2017, TALLINN, ESTONIA

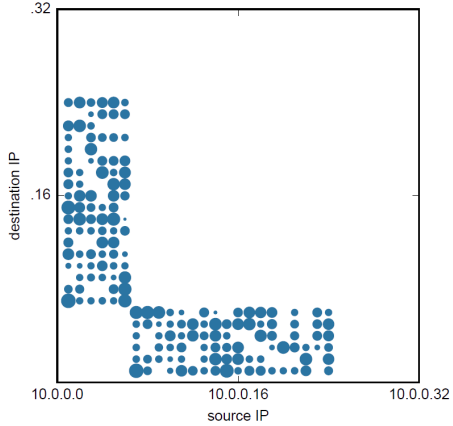


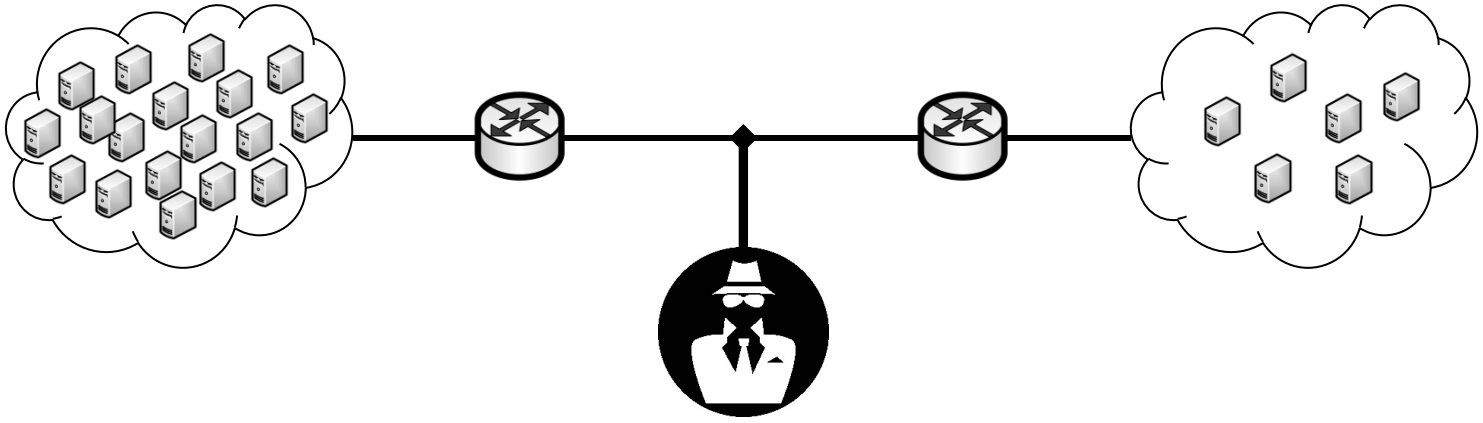


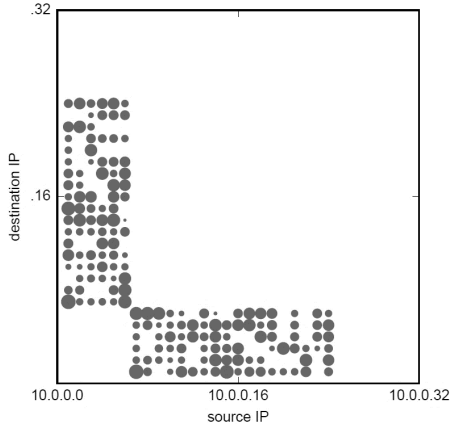


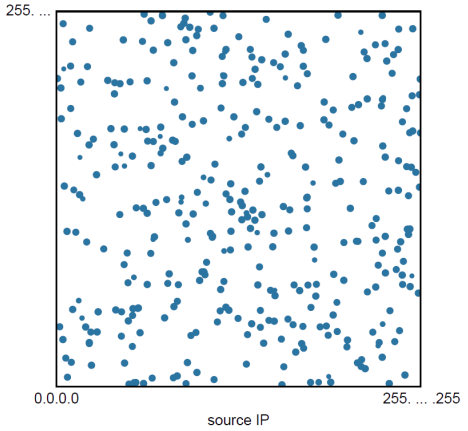


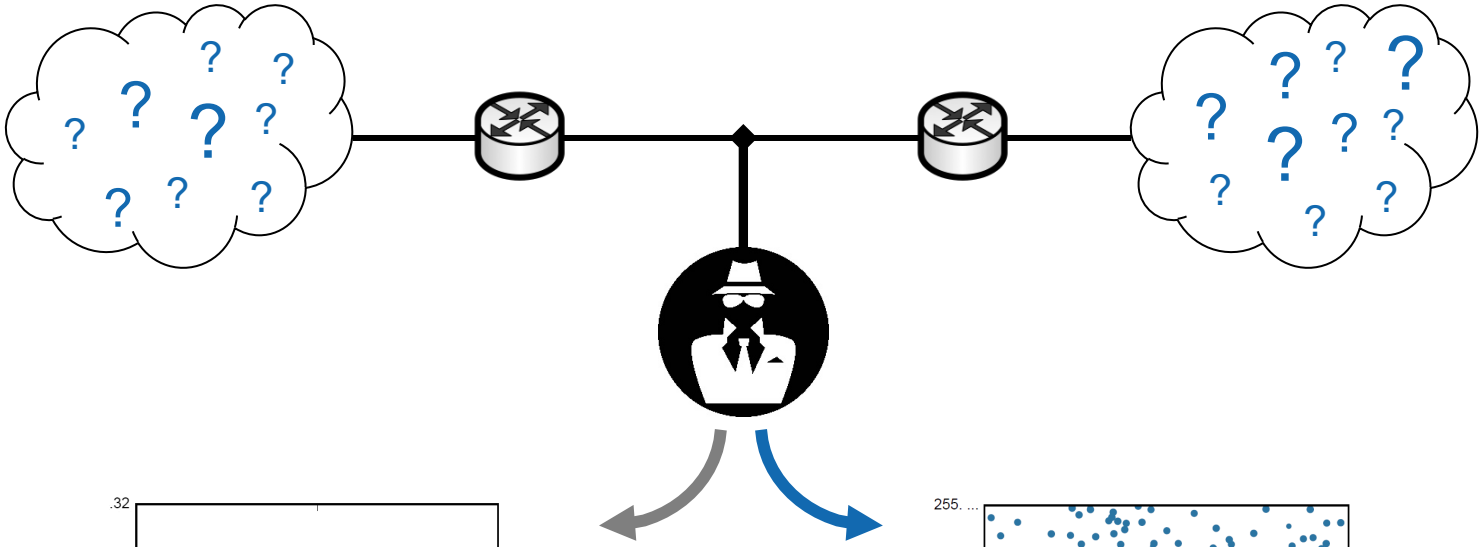


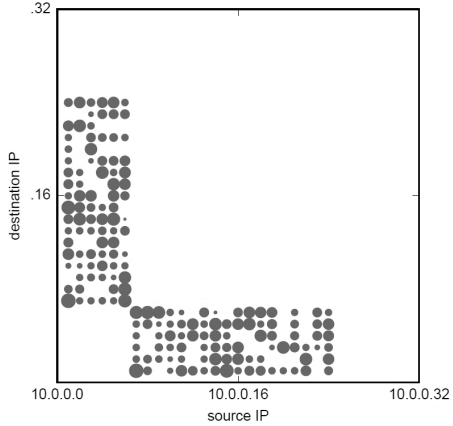

.32
.16
destination IP
10.0.0.0
10.0.0.16
10.0.0.32
source IP

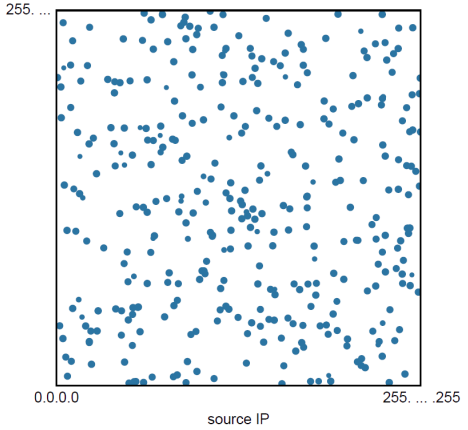


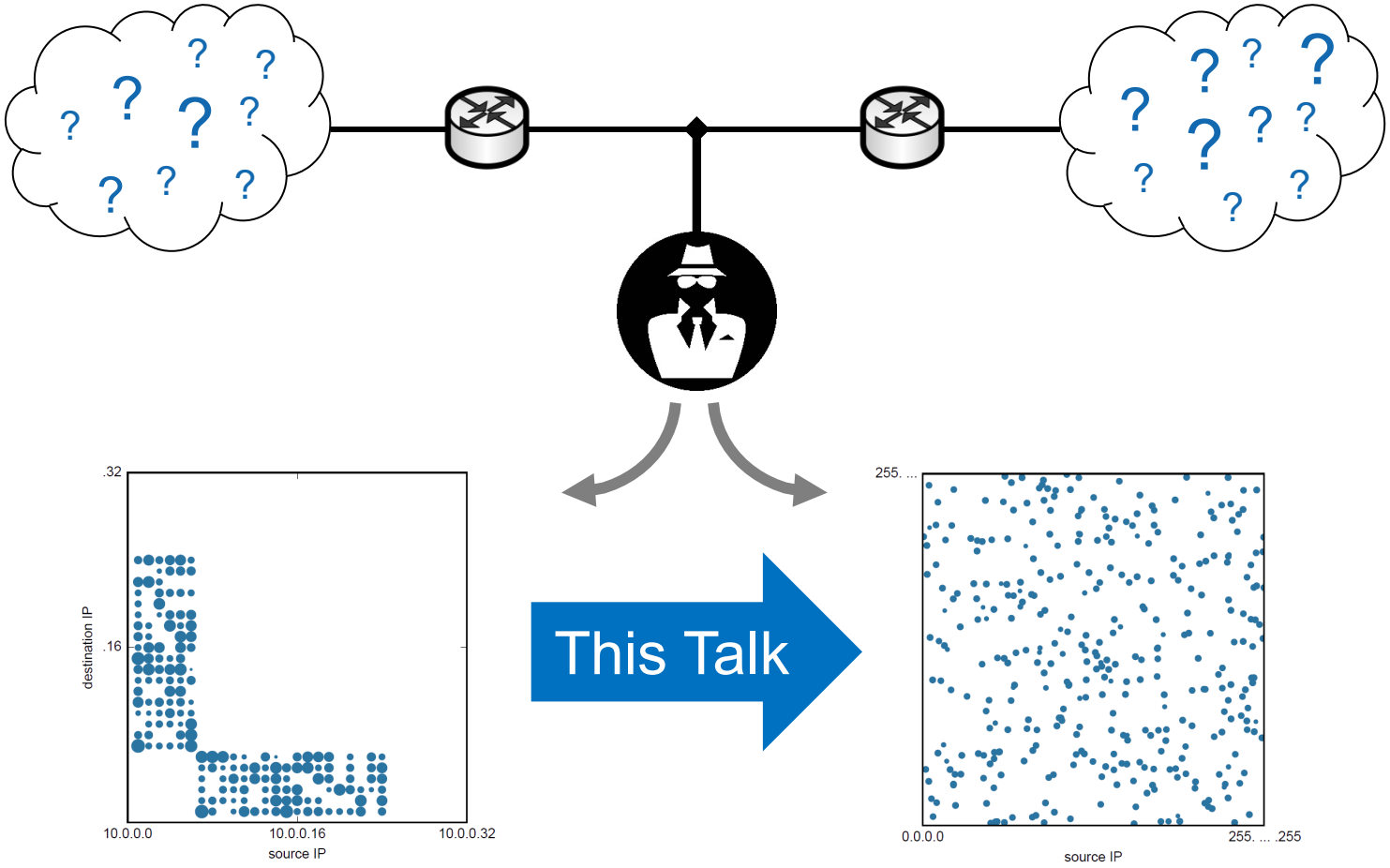

.32
.16
destination IP
10.0.0.0
10.0.0.16
10.0.0.32
source IP


255. ...
0.0.0.0
255. ... .255
source IP




.32
.16
destination IP
10.0.0.0
10.0.0.16
10.0.0.32
source IP


255. ...
0.0.0.0
255. ... .255
source IP



CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence
Tallinn, Estonia

CyCON
International Conference On Cyber Conflict
30 MAY - 2 JUNE 2017, TALLINN, ESTONIA

N.S.A. May Have Hit Internet Companies at a Weak Spot

The Internet companies' data centers are locked down with full-time security […]. But *between the data centers […] information was unencrypted and an easier target for government intercept efforts*,

…

- The New York Times, Nov. 25, 2013

The Atlantic SUBSCRIBE SEARCH MENU

GLOBAL

The Creepy, Long-Standing Practice of Undersea Cable Tapping

The newest NSA leaks reveal that governments are probing "the Internet's backbone." How does that work?

1.8k 808

OLGA KHAZAN | JUL 16, 2013

The Washington Post

Technology

Google encrypts data amid backlash against NSA spying

By Craig Timberg September 6, 2013

Google is racing to encrypt the torrents of information that flow among its data centers around the world in a bid to thwart snooping by the NSA and the intelligence agencies of foreign governments, company officials said Friday.

The move by Google is among the most concrete signs yet that recent revelations about the National Security Agency's sweeping surveillance efforts have provoked significant backlash within an American technology industry that U.S. government officials long courted as a potential partner in spying programs.

Google's encryption initiative, initially approved last year, was accelerated in June as the tech giant struggled to guard its reputation as a reliable steward of user information amid controversy about the NSA's PRISM program, first reported in The Washington Post and the Guardian that month. PRISM obtains data from American technology companies, including Google, under various legal authorities.

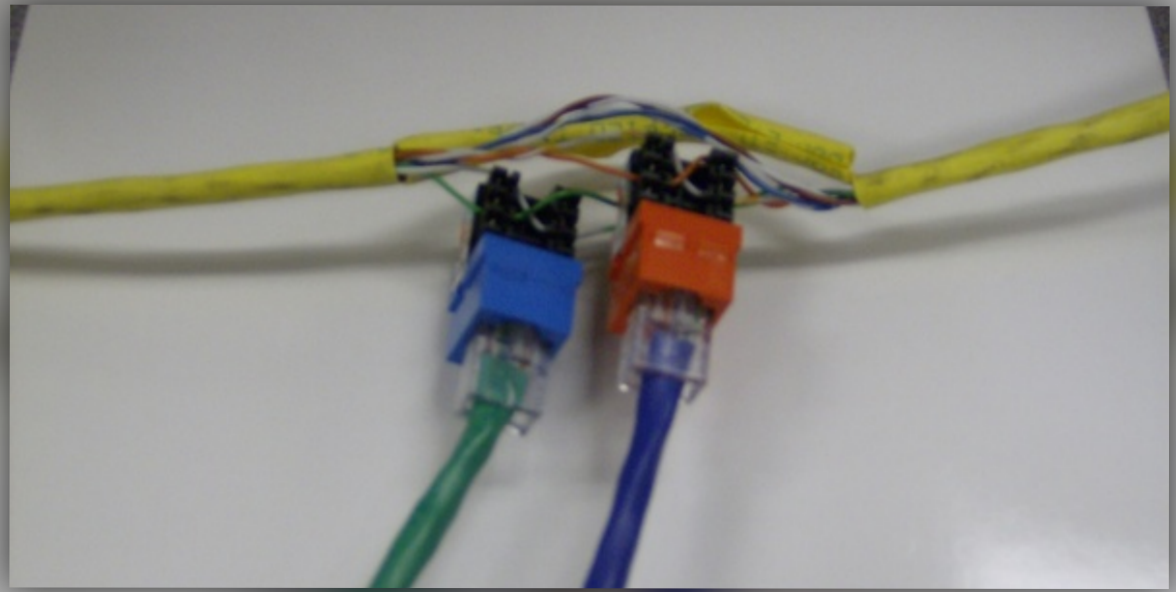
CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia

CyCON

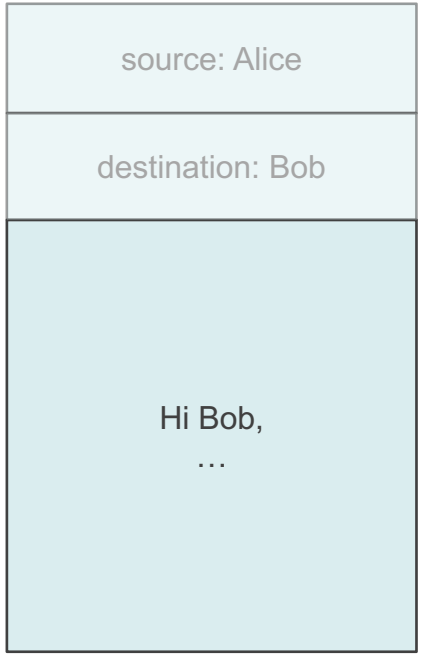
International Conference
on Cyber Conflict

30 MAY - 2 JUNE 2017, TALLINN, ESTONIA



[janitha.com]

This thesis vs. existing solutions

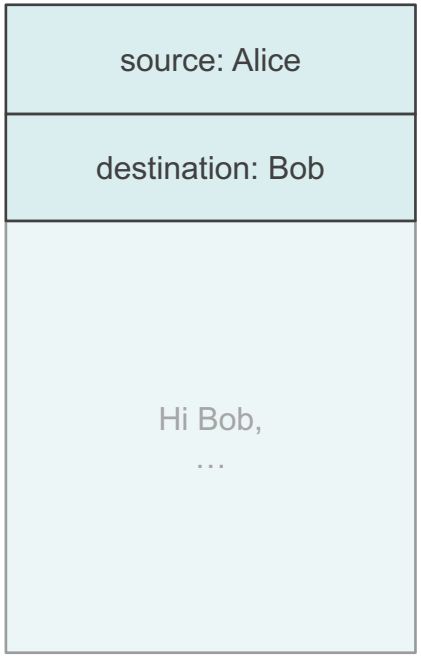


Payload encryption

CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

CyCON
International Conference On Cyber Conflict
30 MAY - 2 JUNE 2017, TALLINN, ESTONIA

This thesis vs. existing solutions



Header obfuscation

Payload encryption

This thesis

SDN-based Network Obfuscation

This thesis

SDN-based Network Obfuscation

- Communication anonymity
  who is communicating with whom?
- Volume anonymity
  how much traffic flows between host X and Y?
- Topology anonymity
  how many hosts are in the network?

This thesis

SDN-based Network Obfuscation

- Software-Defined Network
  New network architecture
- Network-based approach
  No modifications at end-hosts

Software-Defined Networking

Traditional network

[Cisco]

closed
software

closed
hardware

Software-Defined Networking

Traditional network

[Cisco]

closed
software

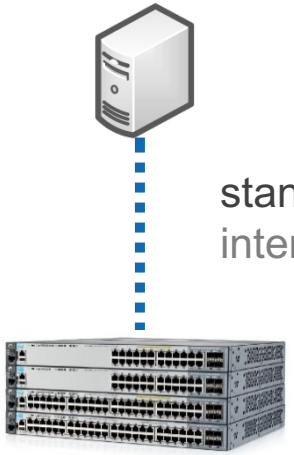
closed
hardware

SDN

open
software

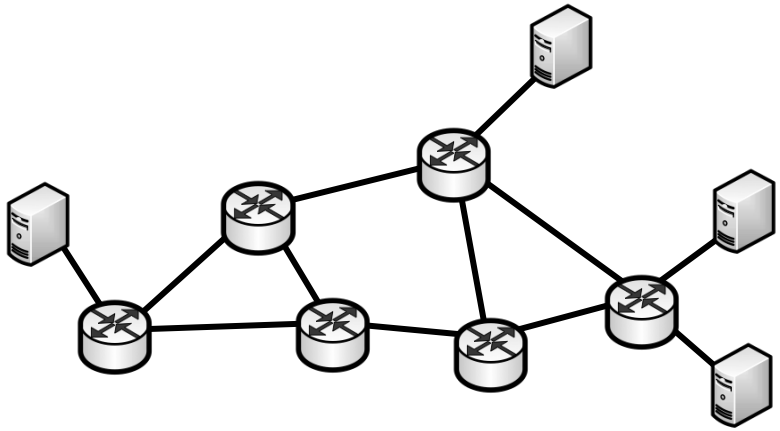
standardized
interface

standardized
hardware



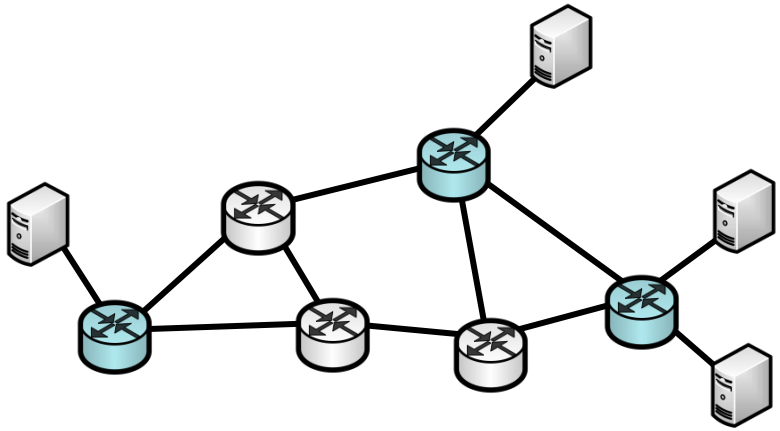
[HP]

Architecture



Layer 2 network

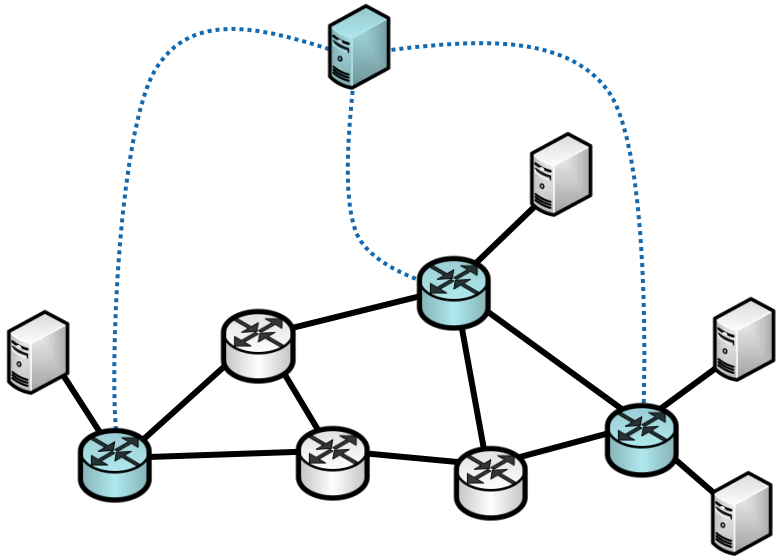
Architecture



Layer 2 network

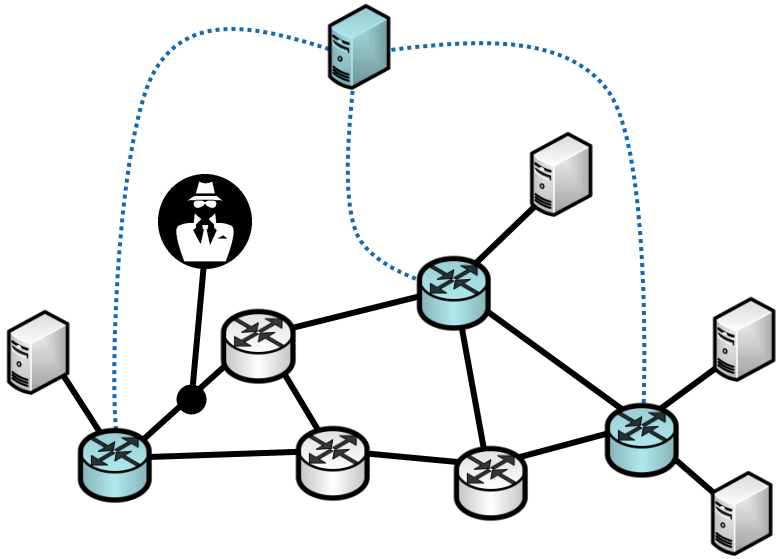
With some SDN switches

Architecture



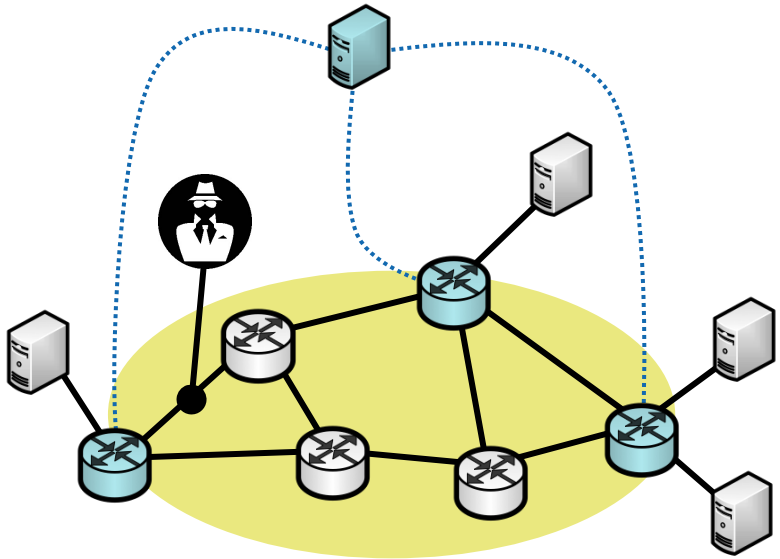
- Layer 2 network
- With some SDN switches
- And a central controller

Architecture



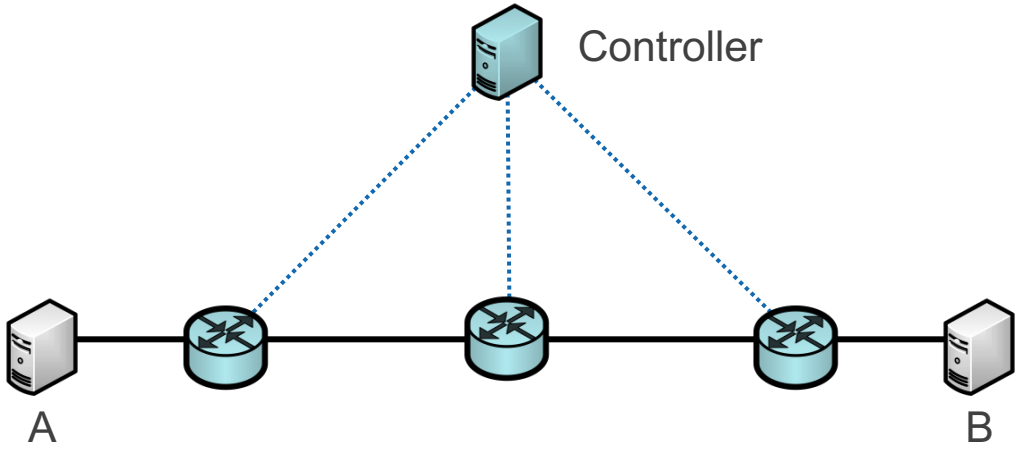
- Layer 2 network
- With some SDN switches
- And a central controller
- Attacked by an eavesdropper

Architecture

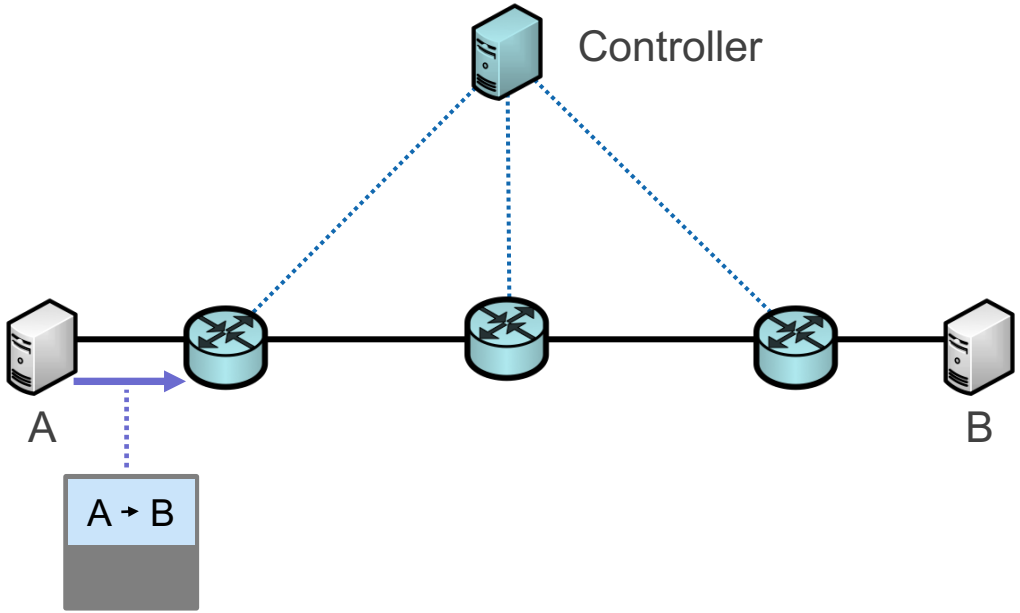


- Layer 2 network
- With some SDN switches
- And a central controller
- Attacked by an eavesdropper
- Protected by our system

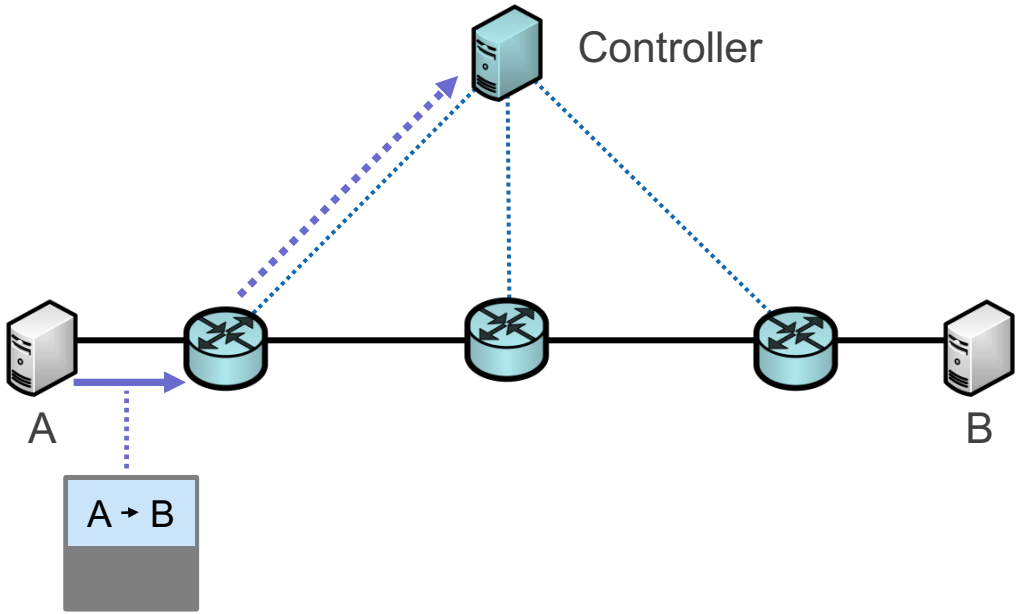
Example



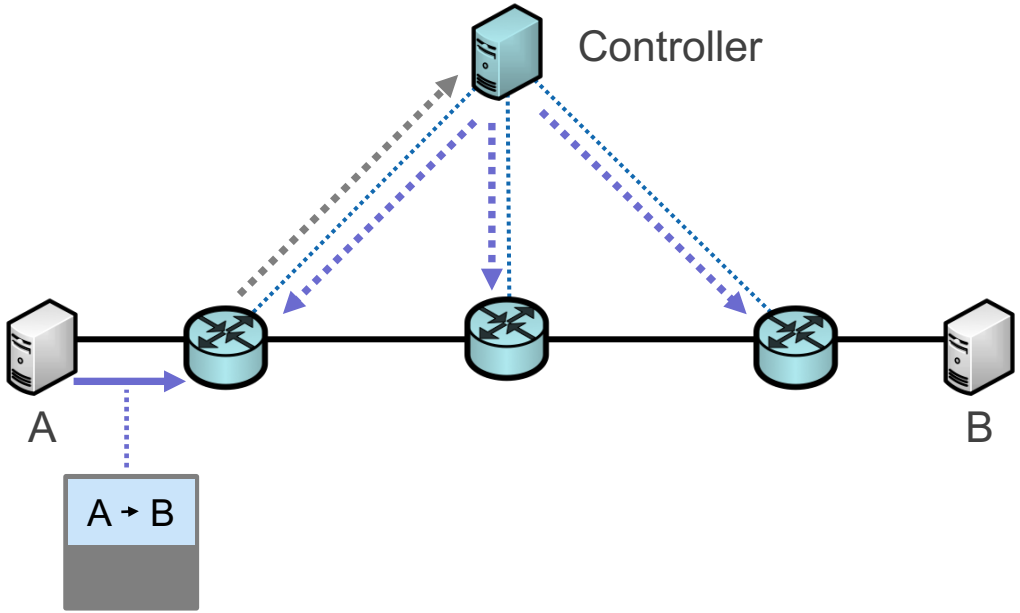
Packet from A to B enters the network



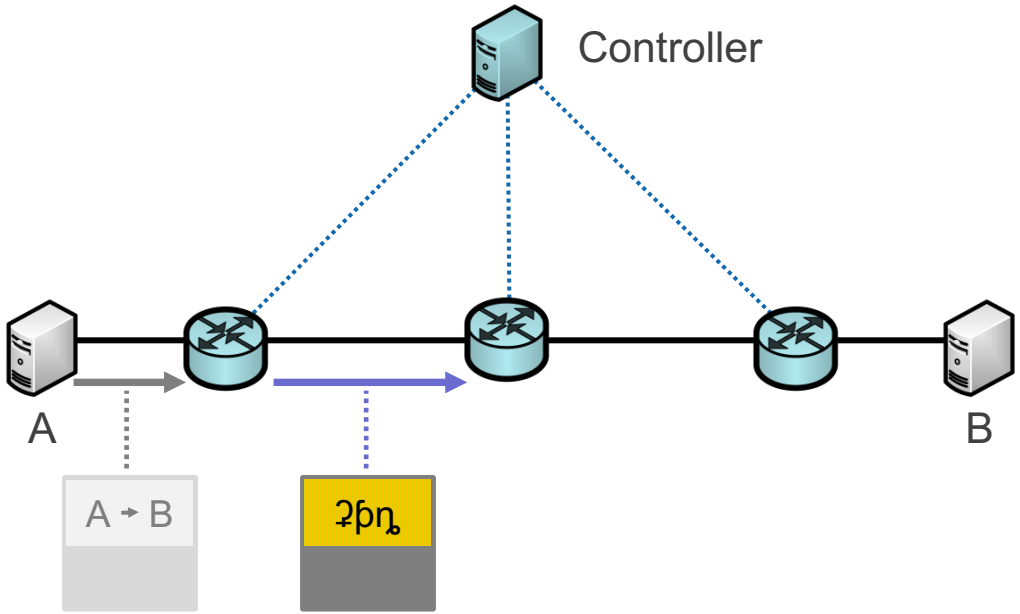
Ingress switch notifies controller



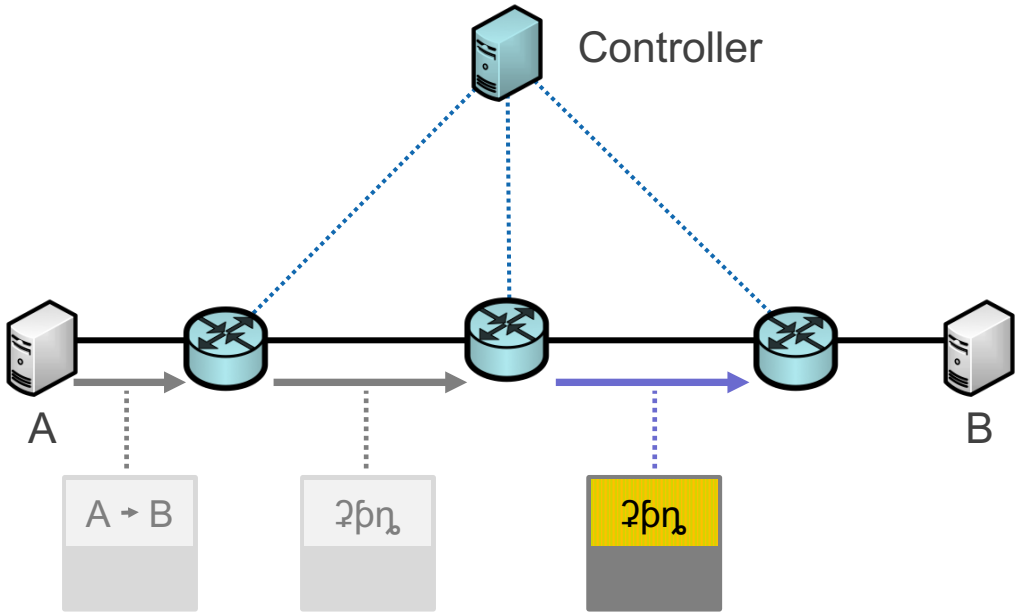
Controller computes & installs flow rules



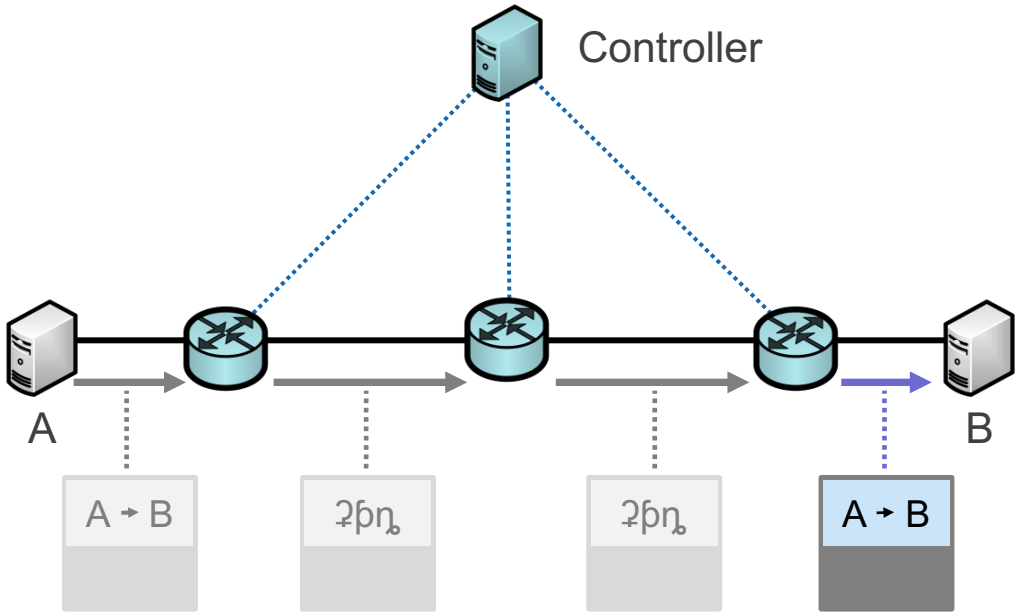
Ingress switch obfuscates source and destination



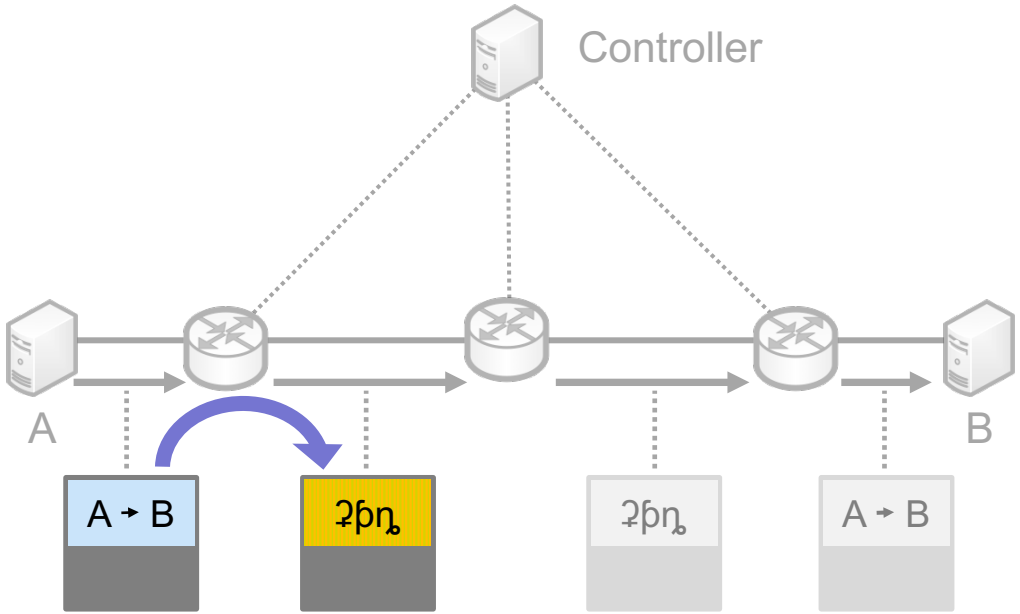
Core switch forwards obfuscated packet



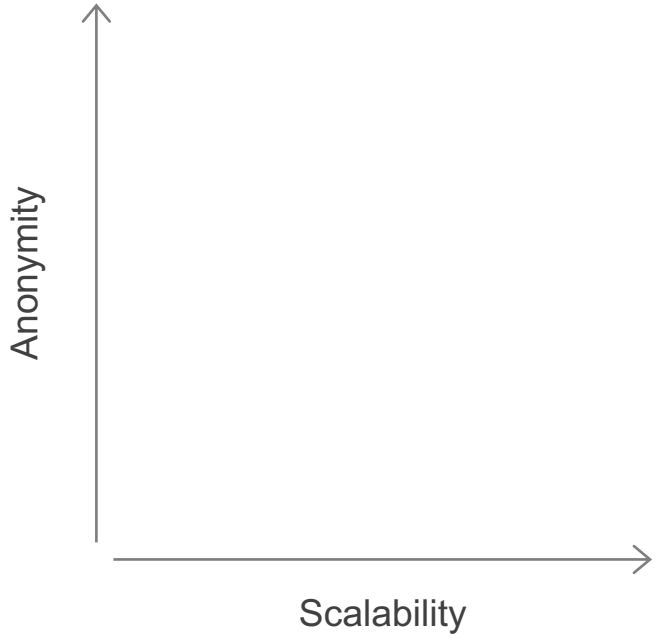
Egress switch de-obfuscates source and destination



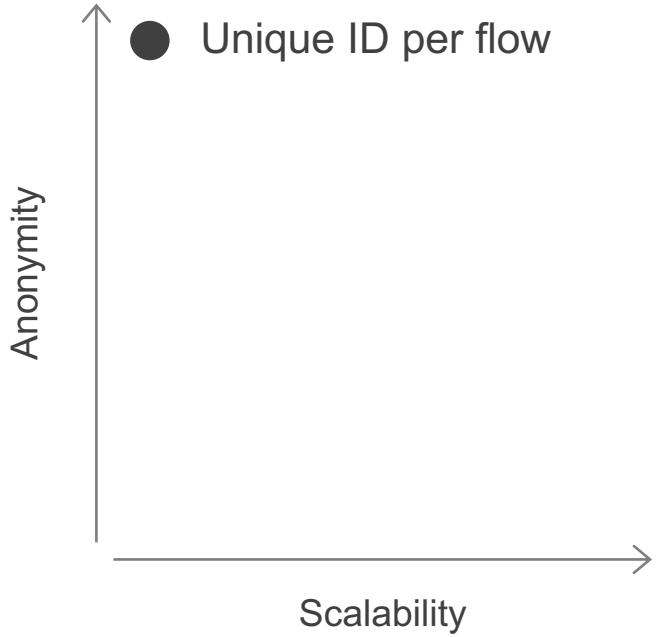
How does the rewriting work?



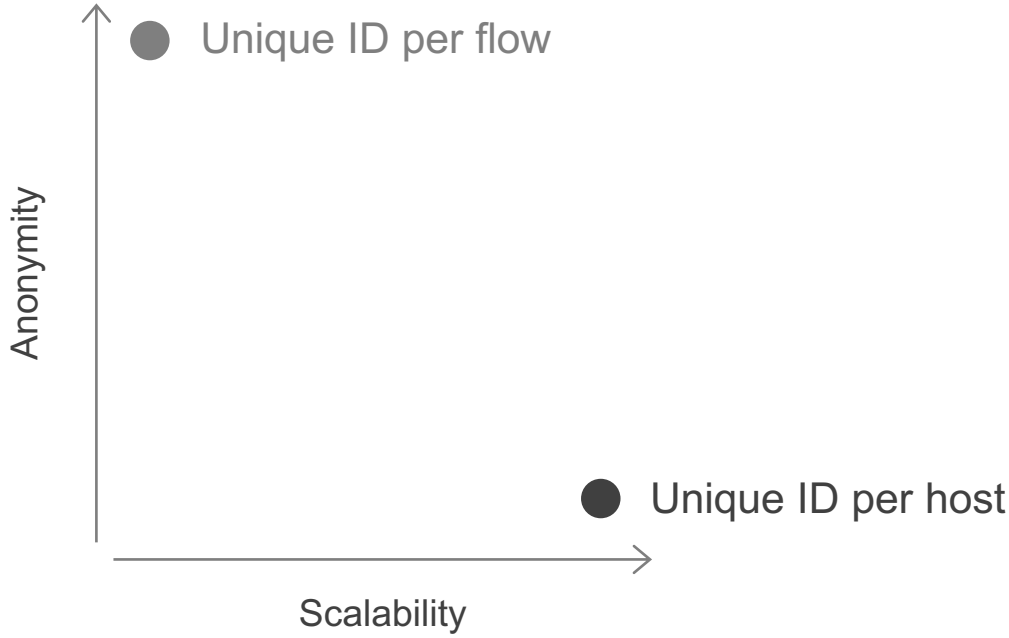
Rewriting as a trade-off between anonymity and scalability



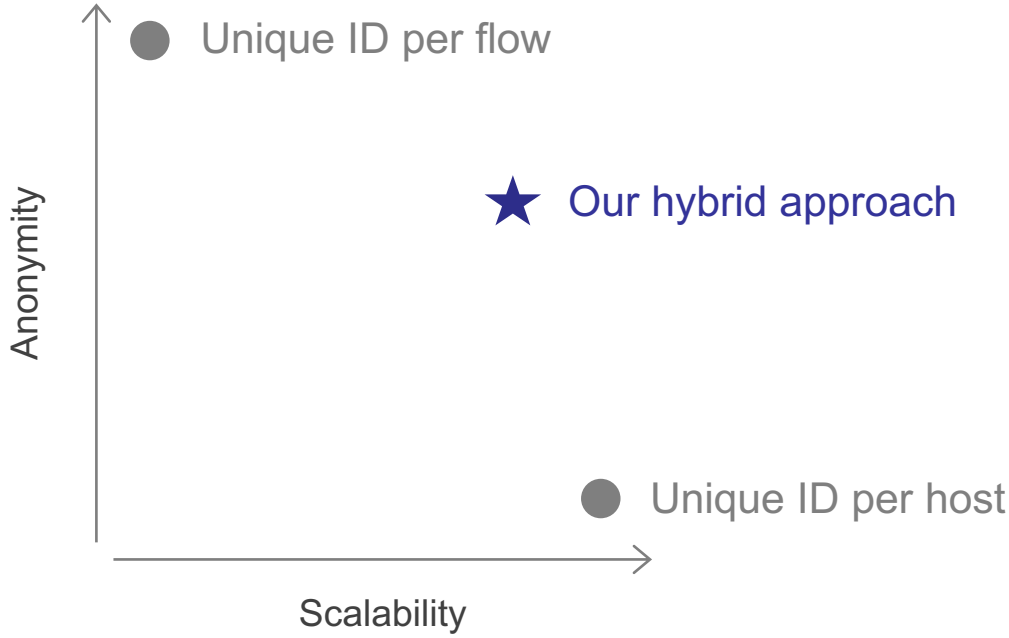
Rewriting as a trade-off between anonymity and scalability



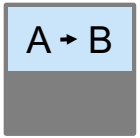
Rewriting as a trade-off between anonymity and scalability



Rewriting as a trade-off between anonymity and scalability

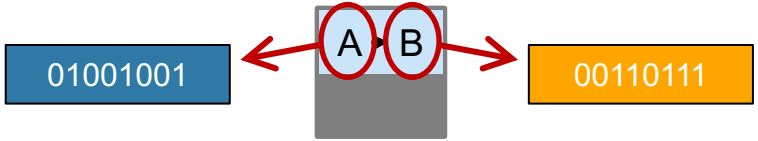


Rewriting scheme



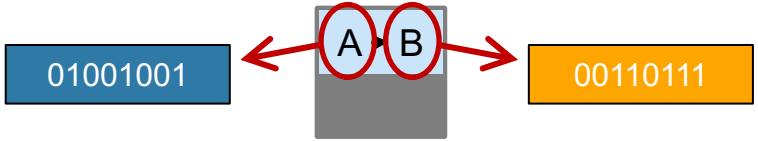
Rewriting scheme

Map source and destination to IDs



Rewriting scheme

Map source and destination to IDs

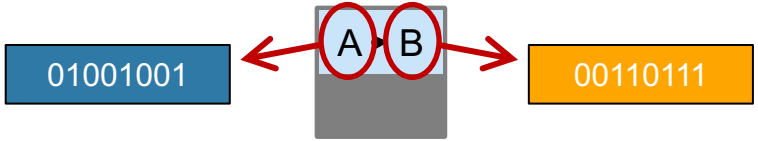


Match-fields with arbitrary bitmasks

MAC src	MAC dst	IP src	IP dst

Rewriting scheme

Map source and destination to IDs

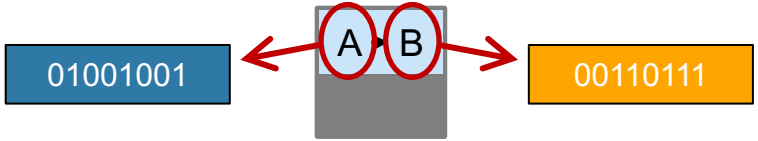


Match-fields with arbitrary bitmasks

Interpret as bit-string of 160 bits

Rewriting scheme

Map source and destination to IDs



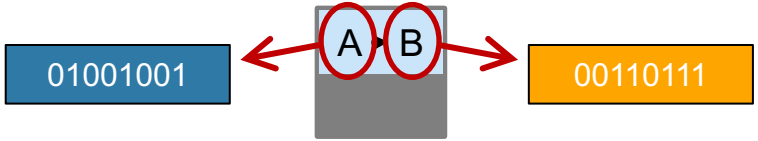
Match-fields with arbitrary bitmasks

Interpret as bit-string of 160 bits

Randomly select bits that are used for source and destination ID

Rewriting scheme

Map source and destination to IDs



Match-fields with arbitrary bitmasks

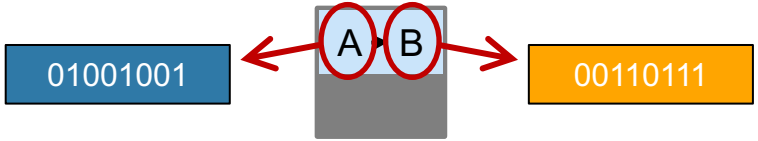
Interpret as bit-string of 160 bits

Randomly select bits that are used for source and destination ID

Add source and destination ID

Rewriting scheme

Map source and destination to IDs



Match-fields with arbitrary bitmasks

Interpret as bit-string of 160 bits

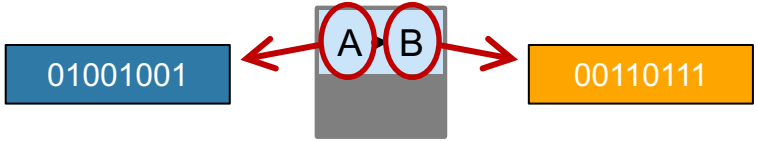
Randomly select bits that are used for source and destination ID

Add source and destination ID

Set other bits to random values

Rewriting scheme

Map source and destination to IDs



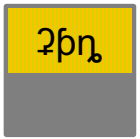
Match-fields with arbitrary bitmasks

Interpret as bit-string of 160 bits

Randomly select bits that are used for source and destination ID

Add source and destination ID

Set other bits to random values



Evaluation

Obfuscation controller compared with Floodlight in default configuration

Resource usage in switches
flow table entries

Switch load
flow table updates / s

Controller load
flows / s

Network performance
RTT and bandwidth

Evaluation

Obfuscation controller compared with Floodlight in default configuration

- ↘ Resource usage in switches
  # flow table entries
- ↘ Switch load
  # flow table updates / s
- → Controller load
  # flows / s
- → Network performance
  RTT and bandwidth

Follow-up work

iTAP: In-network Traffic Analysis Prevention using Software-Defined Networks

https://itap.ethz.ch

Roland Meier
ETH Zürich
meierrol@ethz.ch

David Gugelmann
ETH Zürich
gugelmann@tik.ee.ethz.ch

Laurent Vanbever
ETH Zürich
lvanbever@ethz.ch

ABSTRACT

Advances in layer 2 networking technologies have fostered the deployment of large, geographically distributed LANs. Due to their large diameter, such LANs provide many vantage points for wiretapping. As an example, Google's internal network was reportedly tapped by governmental agencies, forcing the Web giant to encrypt its internal traffic. While using encryption certainly helps, eavesdroppers can still access traffic metadata which often reveals sensitive information, such as who communicates with whom and which are the critical hubs in the infrastructure.

This paper presents iTAP, a system for providing strong anonymity guarantees *within* a network. iTAP is network-based and can be partially deployed. Akin to onion routing, iTAP rewrites packet headers at the network edges by leveraging SDN devices. As large LANs can see millions of flows, the key challenge is to rewrite headers in a way that guarantees strong anonymity while, at the same time, scaling the control-plane (number of events) and the data-plane (number of flow rules). iTAP addresses these challenges by adopting a hybrid rewriting scheme. Specifically, iTAP scales by reusing rewriting rules across distinct flows and by distributing them on multiple switches. As reusing headers leaks information, iTAP monitors this leakage and adapts the rewriting rules before any eavesdropper could provably de-anonymize any host.

We implemented iTAP and evaluated it using real network traffic traces. We show that iTAP works in practice, on existing hardware, and that deploying few SDN switches is enough to protect a large share of the network traffic.

SOSR '17, April 03-04, 2017, Santa Clara, CA, USA

DOI: http://dx.doi.org/10.1145/3050220.3050232

CCS Concepts

•**Security and privacy** → **Pseudonymity, anonymity and untraceability;** *Network security;* •**Networks** → **Network privacy and anonymity; Programmable networks;**

Keywords

Anonymous communication; wiretapping; SDN

1. INTRODUCTION

Since the Snowden revelations, it is well-known that network eavesdropping was (and probably still is) performed in the Internet core, particularly on undersea cables [22]. While worrying, these threats can be mitigated to a large degree by hiding connection metadata (e.g., using Tor [14]) and by relying on pervasive encryption (e.g., using VPNs).

However, network eavesdropping is not limited to the Internet backbone. As enterprise networks become bigger in terms of users and physical reach, they, too, become susceptible to wiretapping. Indeed the advent of new layer 2 technologies such as TRILL [7], Shortest Path Bridging [30], or SDN-based solutions [34] enables network administrators to build large LAN zones that can easily span several thousand devices and users. Due to their large physical diameter, such networks inevitably exhibit many vantage points for wiretapping. Actually, the majority of the attacks is now performed by insiders, *i.e.* malicious insiders or inadvertent actors [4] that act from within the network, rather than by remote attackers. As an example, Google's Wide-Area Network (WAN) – the private network connecting Google's data centers – was reportedly tapped by governmental agencies, forcing the Web giant to encrypt its internal traffic [36].

While encrypting internal traffic protects the payload of connections, an in-network attacker can still monitor and analyze the unencrypted packet headers, i.e., the *metadata*. In particular, the MAC addresses and, in case of SSL/TLS application layer encryption, also the IP addresses of the source and destination hosts along with the source and destination ports used for the communication.

By analyzing these unencrypted header fields, an attacker can gain useful information about: *i)* which hosts communicate; *ii)* the topology of the network; *iii)* the addresses of

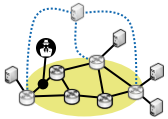
This thesis

+ Partial deployment
+ Improved scalability at network edge
+ Evaluation based on real user traffic

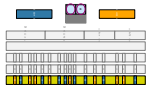
https://itap.ethz.ch

Contributions

https://itap.ethz.ch

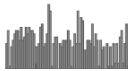


Network-based design



Scalable & anonymity-providing header rewriting scheme

Prototype implementation (open source)



Evaluation

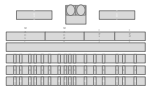
CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

CyCON
International Conference On Cyber Conflict
30 MAY - 2 JUNE 2017, TALLINN, ESTONIA

Contributions

https://itap.ethz.ch

Network-based design



Scalable & anonymity-providing header rewriting scheme

Prototype implementation (open source)

Evaluation

Thank you! Questions?