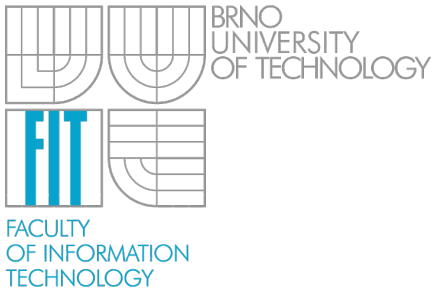
# Hiding TCP Traffic: Threats and Countermeasures

Libor Polčák, Radek Hranický, Petr Matoušek

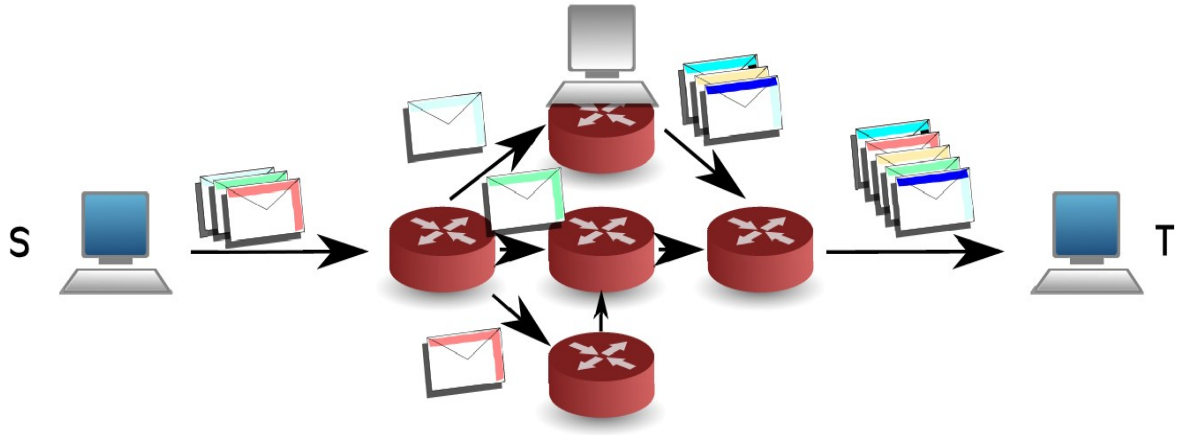
Brno University of Technology, Fakulty of information technology
Božetěchova 2, 612 66 Brno
ipolcak@fit.vutbr.cz
xhrani00@stud.fit.vutbr.cz
matousp@fit.vutbr.cz




24.5.2013

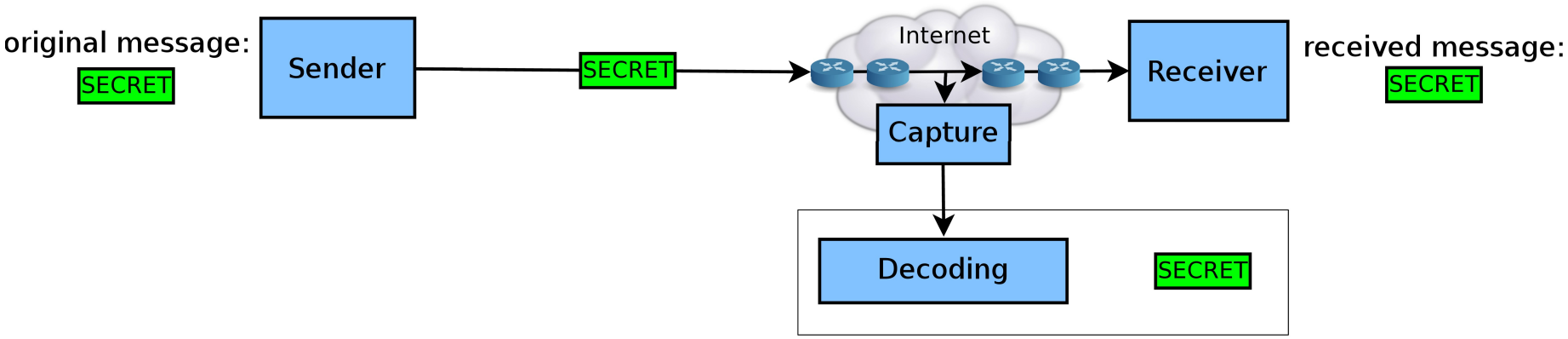
# Motivation

- Detection of traffic hiding in IP networks
  - Completness of lawful interceptions
- Focus on a specific attack
  - Confusion of packet decoding
  - Misleading information



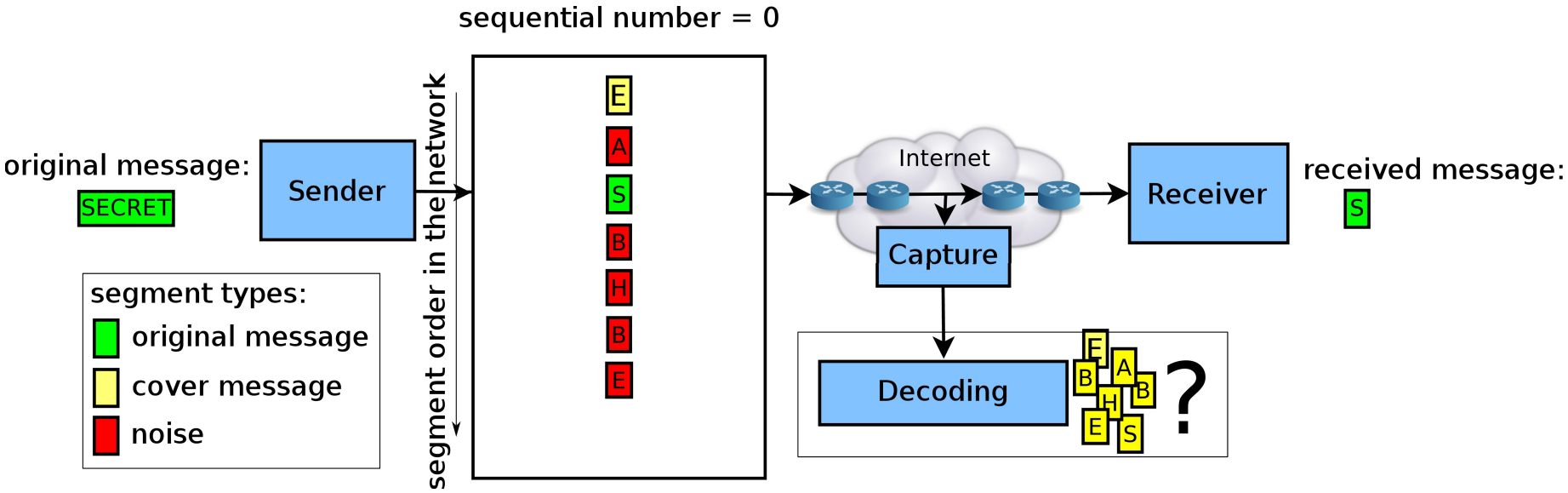
# Attack description

# Normal TCP communication

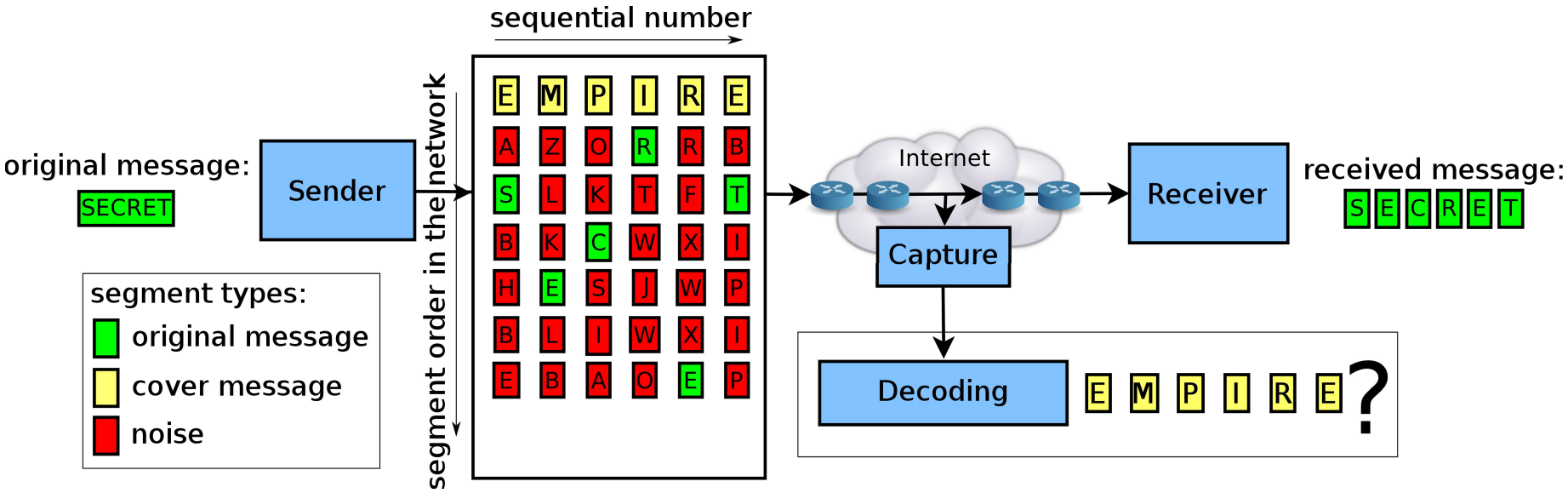



- Decoding software
  - Firewall, IDS/IPS
  - Wireshark, TCP session decoding
  - Proprietary e-investigation software

# Attack description

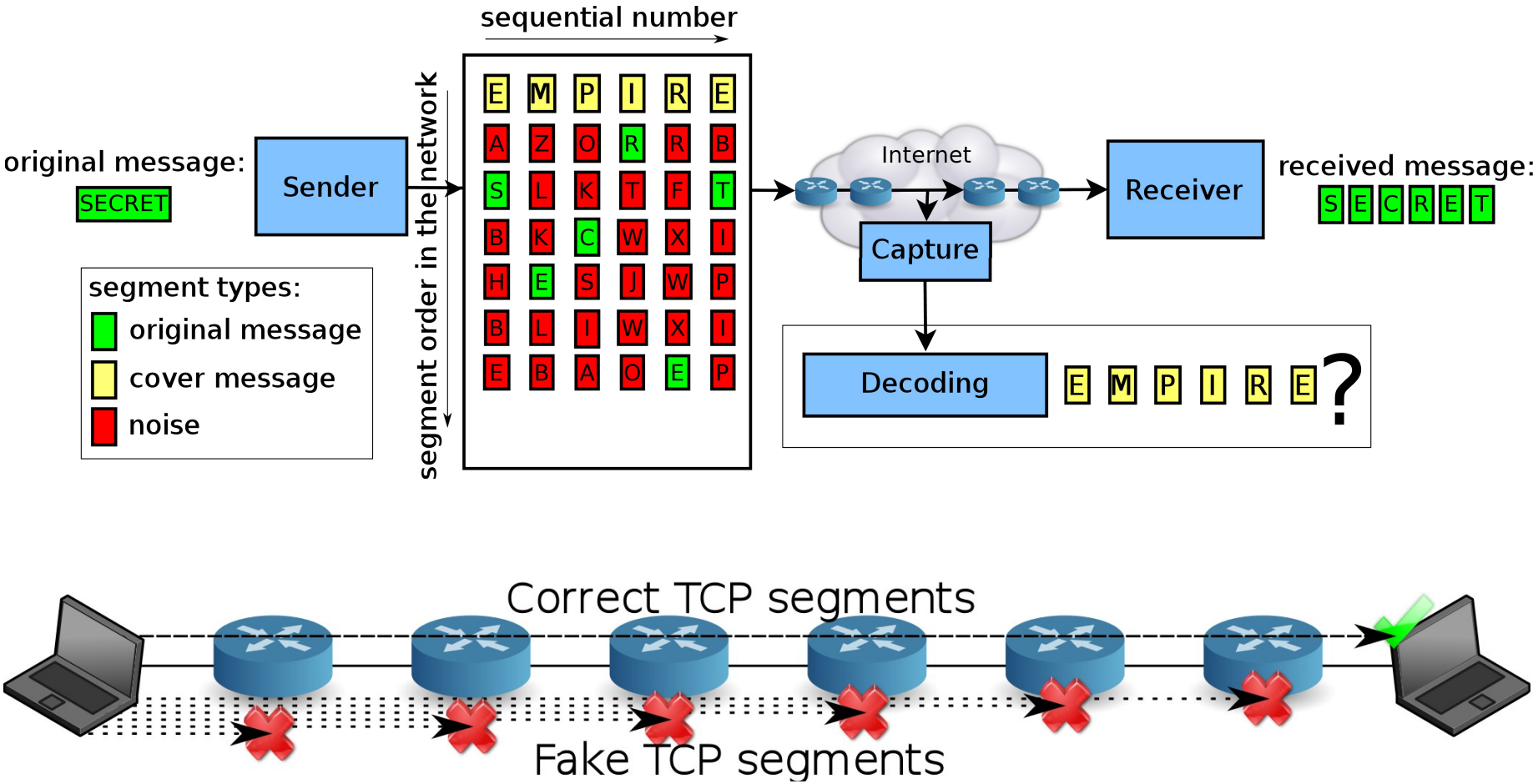


# Attack description



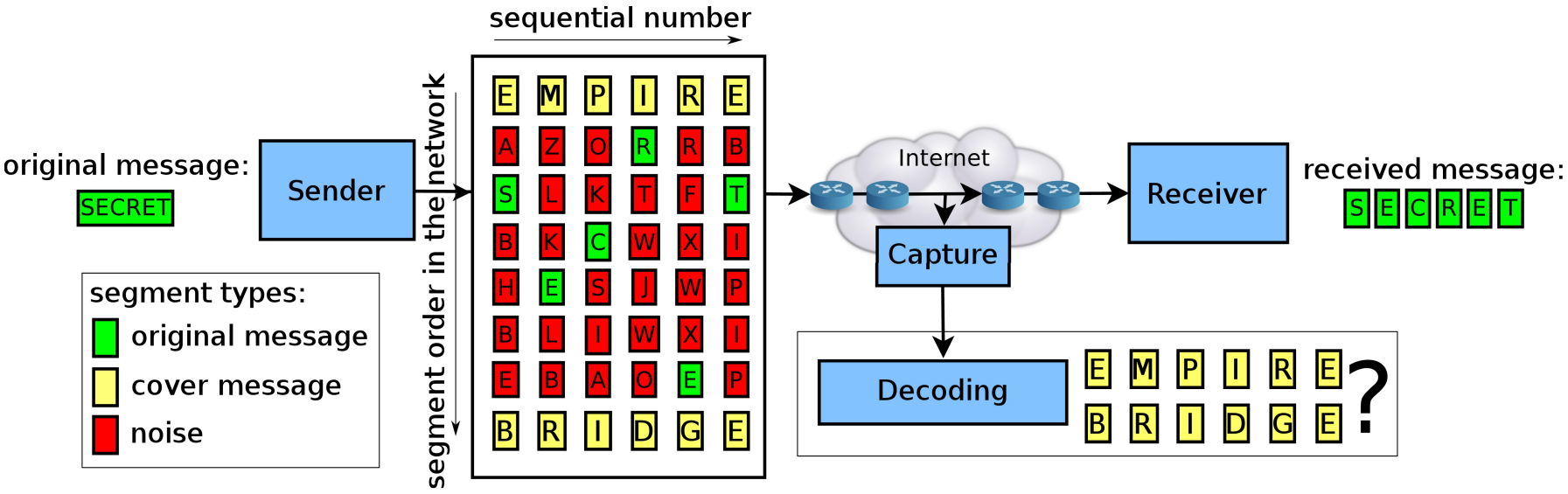

- Main advantage: data hiding without cooperation of the other side
- Receiver uses standard TCP without any modification

# Attack description

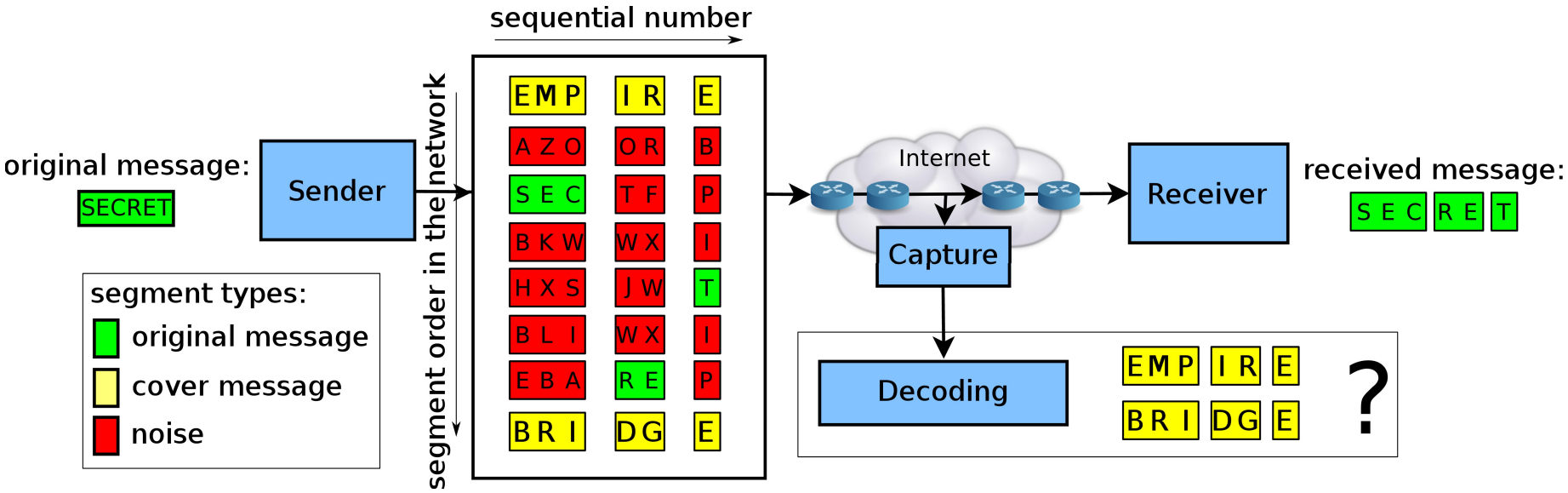


# Extensions to the attack

# Cover message in the last segments

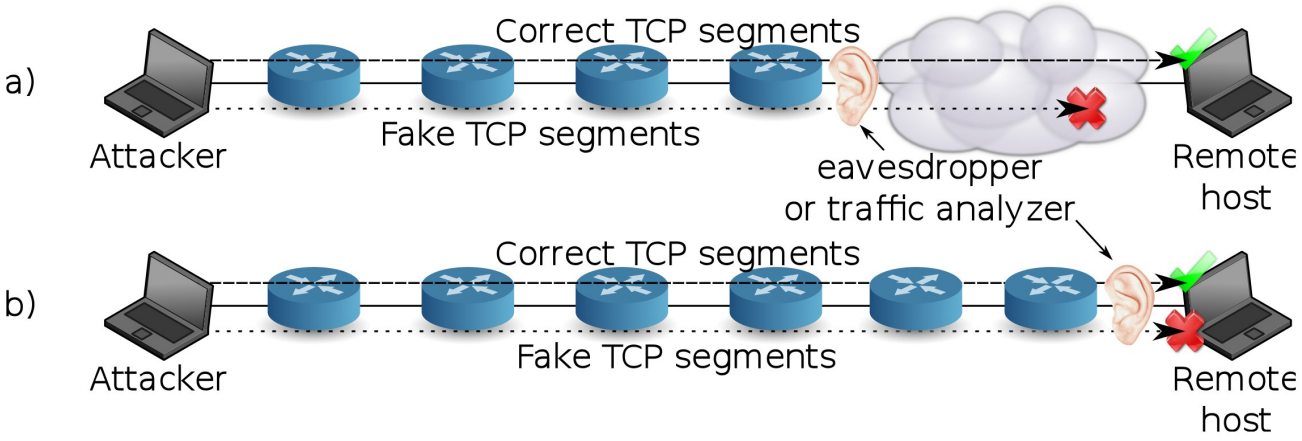


# Configurable-sized segments

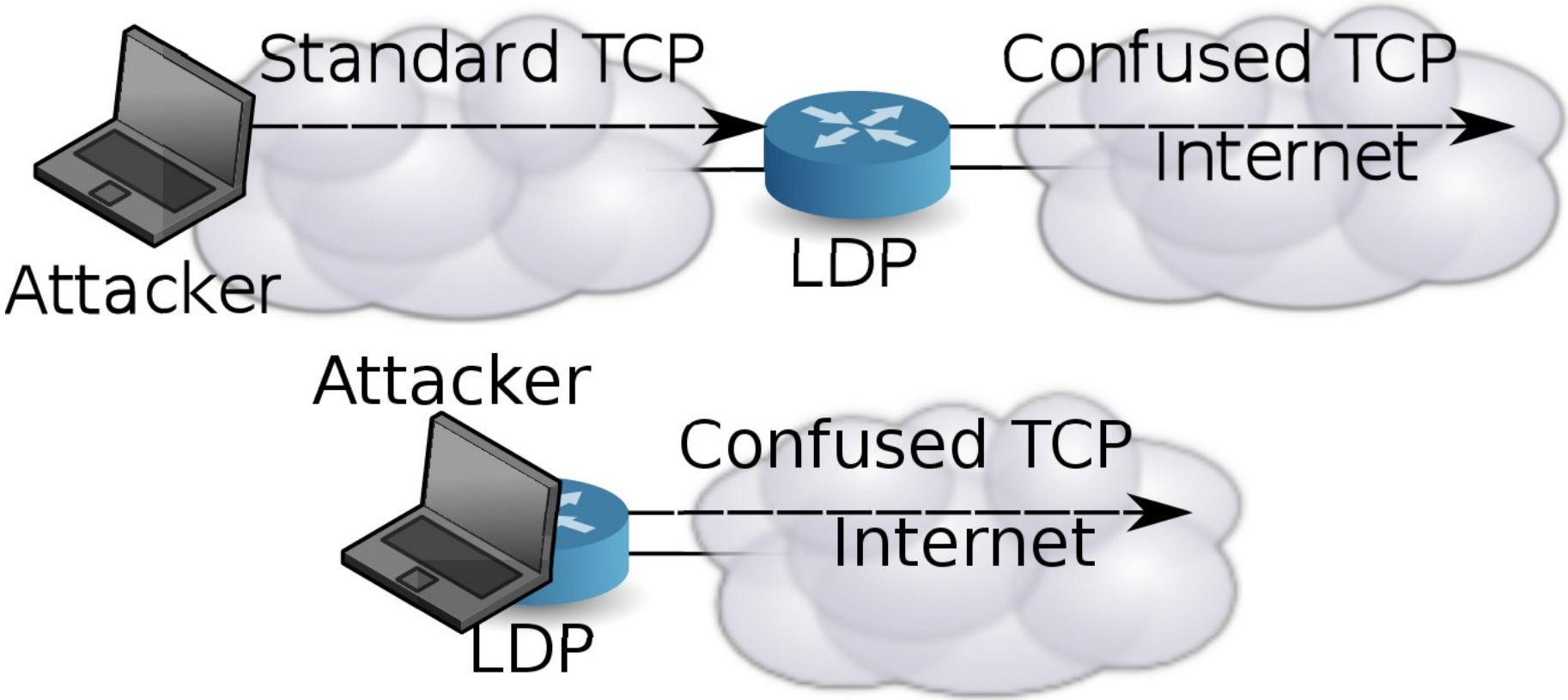


# Datagram drops in IPv6

- Hop Limit (HL)
- Middleboxes (e.g. firewalls, IDS/IPS, routers etc.) may drop some packets
  - Flow label, traffic class
  - Extension headers
  - IPSec (AH, unencrypted ESP)
  - Hop-by-hop headers options



# LDP – proxy for the attack



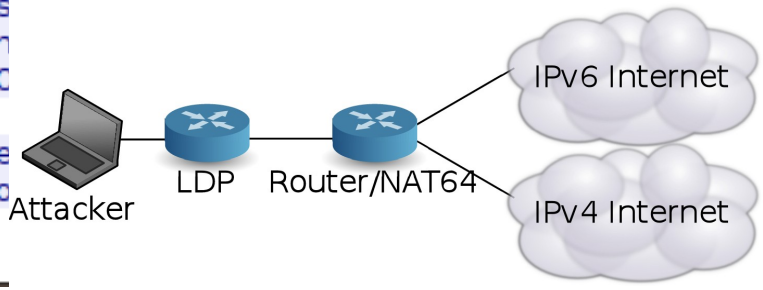

- Source code available at http://www.fit.vutbr.cz/~ipolcak/prods.php
- Automatically detects number of hops to the destination

# Attack analysis

# Attack analysis – Wireshark/IRC

Stream Content

```
:kriminalnik!~kriminaln@dhcpz158.fit.vutbr.cz MODE kriminalnik +i
Podvrzena zprav:kriminalnik!~kriminaln@dhcpz158.fit.vutbr.cz JOIN #sec6net
:underworld1.no.quakenet.org 332 kriminalnik #sec6net :Demo 7.3.2013
:underworld1.no.quakenet.org 333 kriminalnik #sec6net Komplic 1362567085
:underworld1.no.quakenet.org 353 kriminalnik = #sec6net :kriminalnik @Komplic
:underworld1.no.quakenet.org 366 kriminalnik #sec6net :End of /NAMES list.
Podvrzena zprav:underworld1.no.quakenet.org 324 kriminalnik #sec6net +tnCN
:underworld1.no.quakenet.org 329 kriminalnik #sec6net 1362566987
Podvrzena zpra:underworld1.no.quakenet.org 352 kriminalnik #sec6net ~kriminaln
dhcpz158.fit.vutbr.cz *.quakenet.org kriminalnik H :0 kriminalnik
:underworld1.no.quakenet.org 352 kriminalnik #sec6net ~Komplic
pcpolcak.fit.vutbr.cz *.quakenet.org Komplic H@ :3 Sec6Net
:underworld1.no.quakenet.org 315 kriminalnik #sec6net :End of /WHO list.
:Komplic!~Komplic@pcpolcak.fit.vutbr.cz PRIVMSG #sec6net :ahoj
Podvrzena zprava.... b
a:Komplic!~Komplic@pcpolcak.fit.vutbr.cz PRIVMSG #sec6net :tak co noveho?
Podvrzena zprava....:underworld1.no.quakenet.org PONG
underworld1.no.quakenet.org :LAG1834516297
Podvrzena zprava.... bla bla bla bl^ bla bla bla bla bla bPodvrzena zprava....
bla bla :Komplic!~Komplic@pcpolcak.fit.vutbr.cz PRIVMSG #sec6net :ok
Podvrzena zprava.... bla bla bla bla bla bla bla bPodvrzena zpravai... bla bla
bla:Komplic!~Komplic@pcpolcak.fit.vutbr.cz PRIVMSG #sec6net :ano
P6dvrzena zprava.... bla bla bla bla bla bla bla bla blPodvrzena zprava....
bla:underworld1.no.quakenet.org 354 kriminalnik 152 #sec6net kriminalnik H
:underworld1.no.quakenet.org 354 kriminalnik 152 #s
:underworld1.no.quakenet.org 315 kriminalnik #sec6n
Podvrzena zprava....:underworld1.no.quakenet.org PO
underworld1.no.quakenet.org :LAG1864668051
:Komplic!~Komplic@pcpolcak.fit.vutbr.cz PRIVMSG #se
Podvrzena zprava.... blPodvrzena zprava..k.:underwo
underworld1.no.quakenet.org :LAG1894689943
```

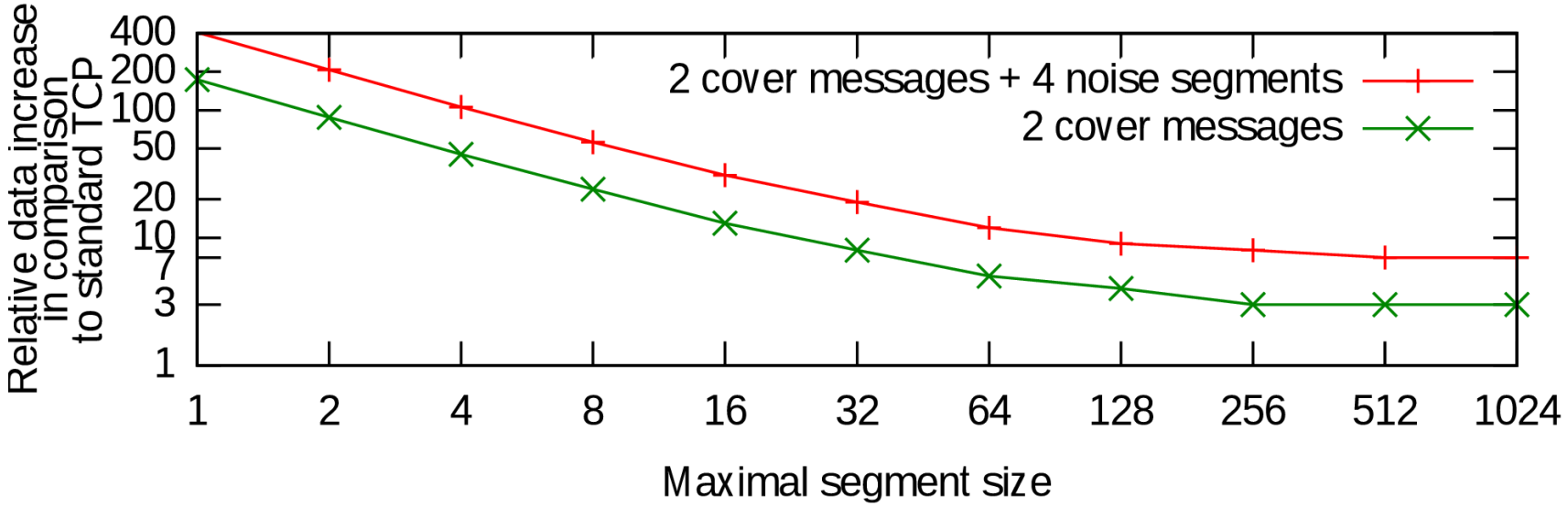


# Downside of the attack

- Information leakage from the opposite directions of the TCP stream (indirect clue)
  - Incoming IRC messages
  - Preview of the message send to a discussion forum
- Consequence: The attack might be misused only in a specific scenario
  - Opposite direction unavailable to the interceptor
  - No valuable data in the opposite direction

# Attack characteristic: overhead

- Very big overhead for short-sized segments
  - Overhead for 16 KB data transfer

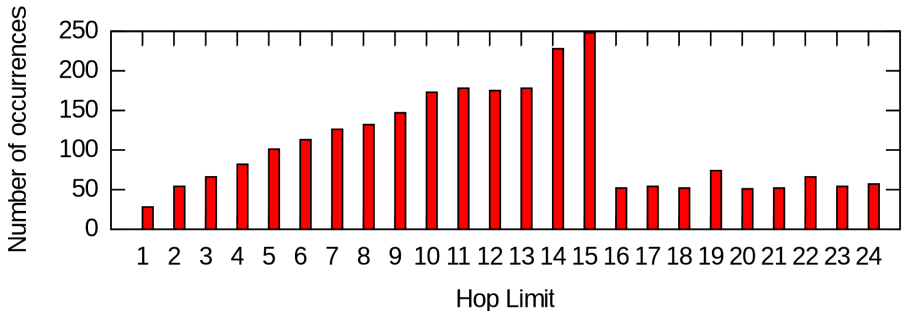



- What can an attacker do?
  - Big segments → easier reconstruction
  - Hide only a specific part of communication

# Countermeasures and attack detection

# Attack detection

- Hop Limit variation

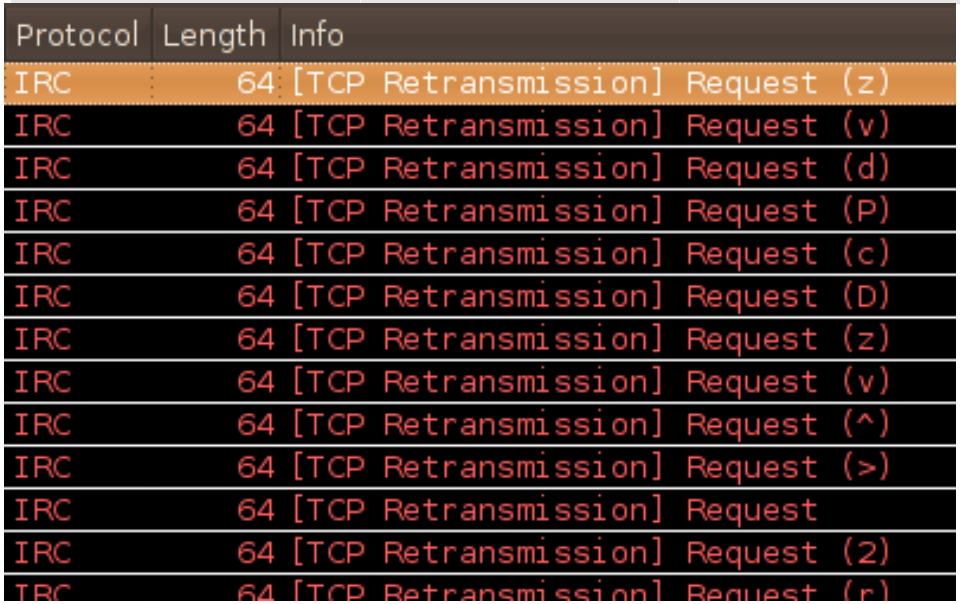


- NetFlow

| Duration | Direction | Packets | Bytes | Bpp |
|---|---|---|---|---|
| 3.502 s | Attacker -> Server | 8467 | 521056 | 61 |
| 3.502 s | Server -> Attacker | 1016 | 79352 | 78 |

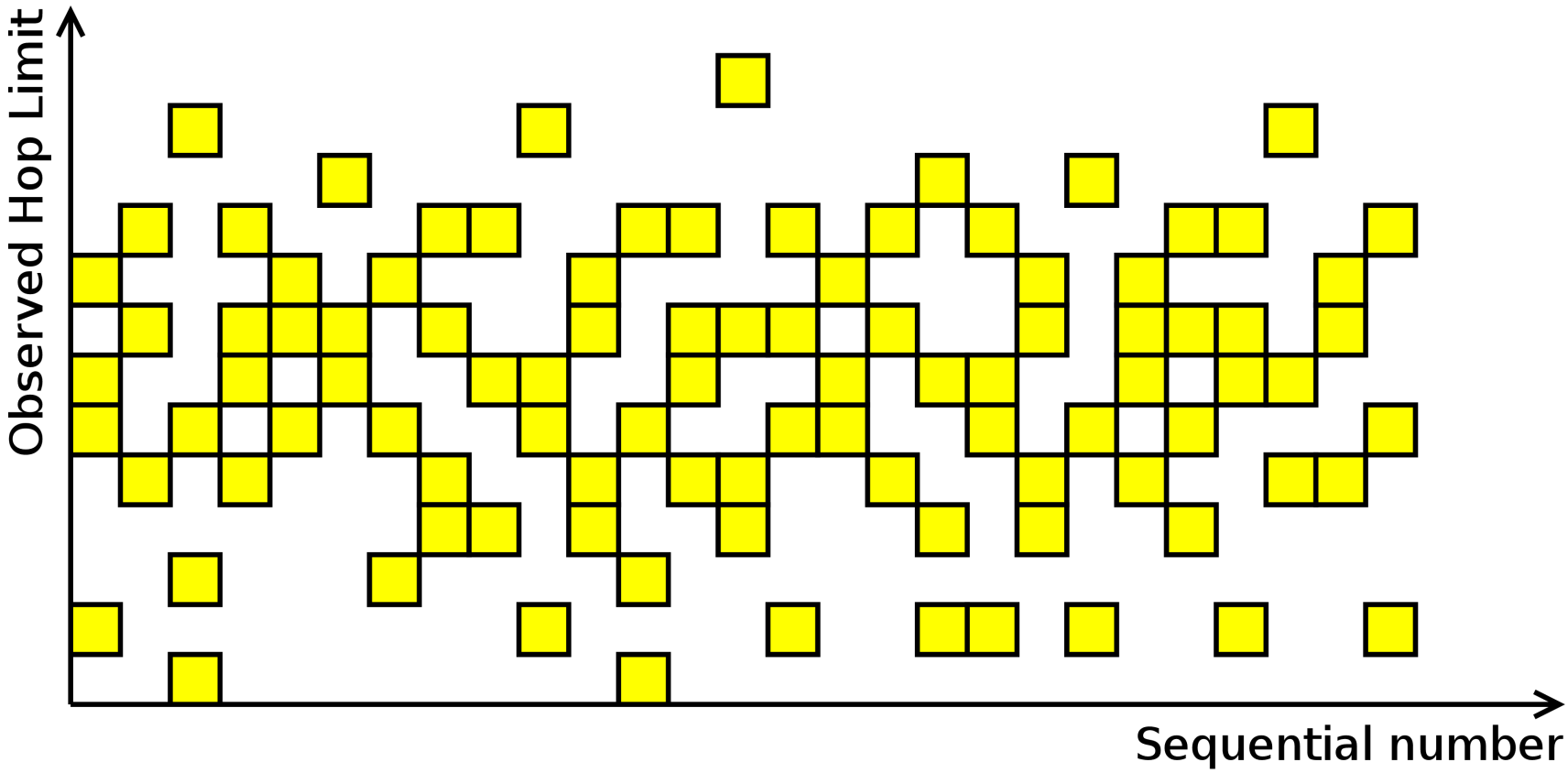
# Decoding software

| Decoding SW | IPv6 support | Interpretation | Detected anomalies |
|---|---|---|---|
| Wireshark | Yes | First cover message | High number of TCP retransmittions |
| Chaosreader | Yes | Random noise | None |
| tcpflow | Yes | Last cover message | None |
| tcptrace | Yes | Last cover message | High number of segments with the same sequential number (rexmt) |



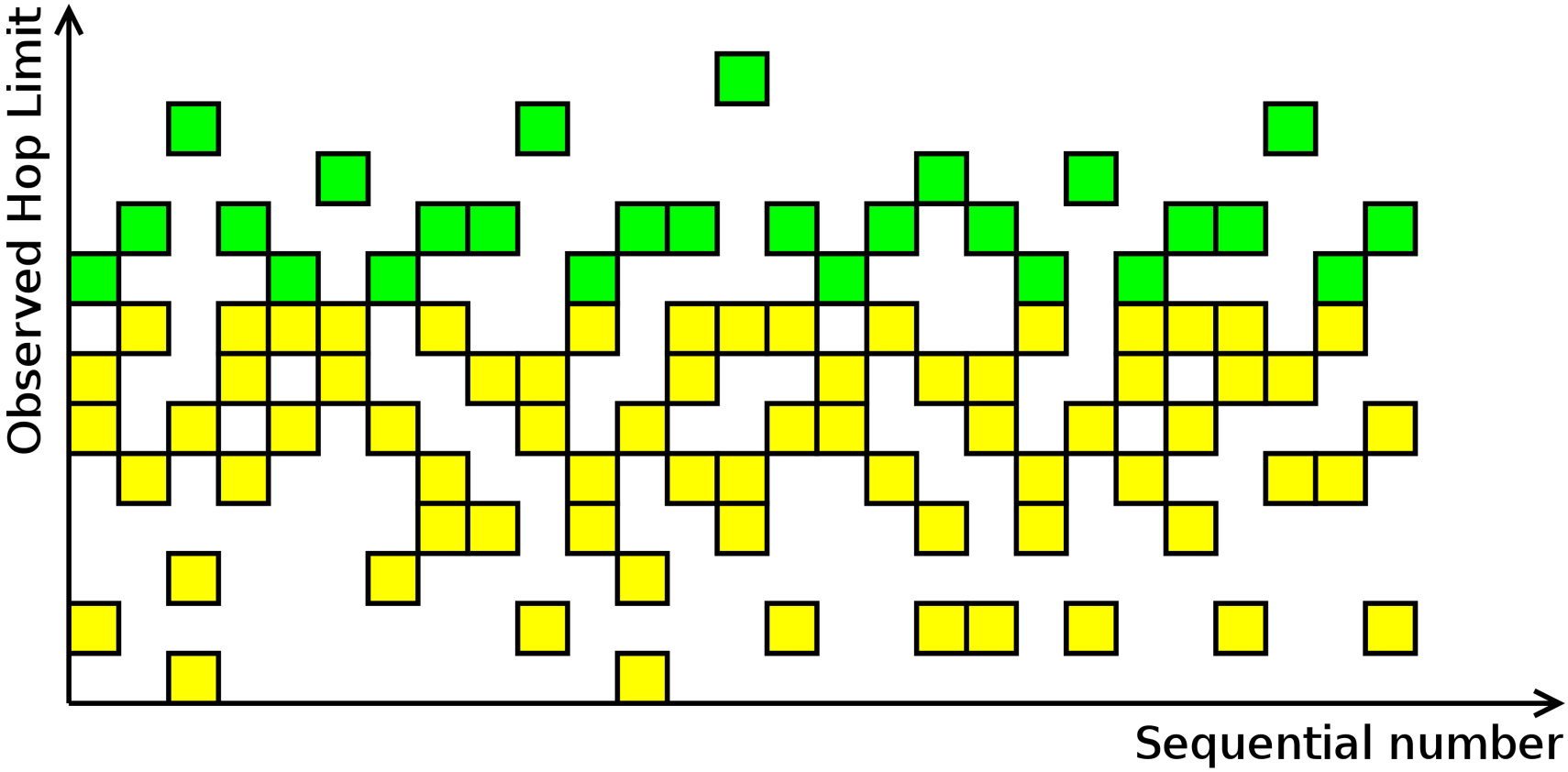

```
…
TCP connection 1:
…
           total packets: 3051
…
    a->b:                          b->a:
      total packets:     2565      486
      ack pkts sent:     2564      486
…
      unique bytes sent: 504     8826
…
      rexmt data pkts:   2037       9
      rexmt data bytes:  2037    4759
```

# LNC – Fake data removal

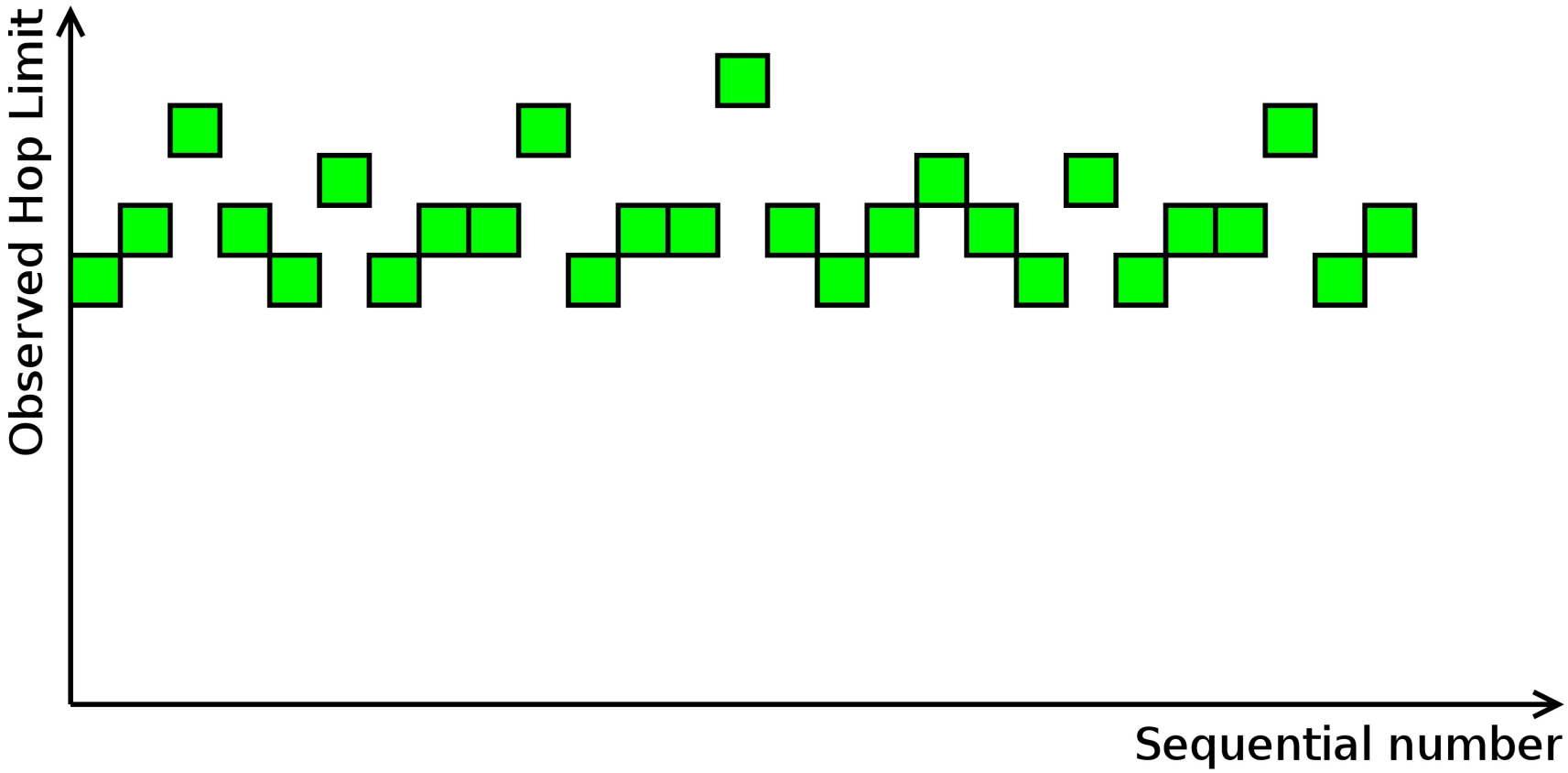



- Filters fake packets in a PCAP file

# LNC – Fake data removal



# LNC – Fake data removal




- Source code available at http://www.fit.vutbr.cz/~ipolcak/prods.php

# Fake data removal

- What can go wrong?
  - Packets are not dropped due to HL/TTL
  - If the destination receives overlapping segments with distinct content → the behaviour differs
  - Fake packets send when the correct were already processed

# Conclusion

# Conclusion

- The attack has dozens of modifications
  - Segment length
  - Noise, cover messages
  - Packet dropping
  - Etc.
- Some forms easy to detect, some harder
  - Suspicious retransimitions
  - Unusual metadata
- Limited usability due to leakage of data in the opposite direction

# Conclusion

- http://www.fit.vutbr.cz/~ipolcak/prods.php
  - LDP – proxy, LNC – PCAP cleaner
- Cooperation with Ministry of Interior and Czech police
  - Project Modern Tools for Detection and Mitigation of Cyber Criminality on the New Generation Internet (http://www.fit.vutbr.cz/~ipolcak/grants.php?id=517)
  - Lawful Interception System

Thank you for your attention.