THE FUTURE OF DATA EXFILTRATION & MALICIOUS COMMUNICATION

Steffen Wendzel
http://www.wendzel.de

- Steffen Wendzel
  - PhD student @University of Hagen
  - Researcher @Augsburg University of Applied Sciences
  - Author of four CS-related books

  http://www.wendzel.de | Twitter: @cdp_xe

Prediction

Malware communication will become

stealthy and **adaptive**.

Requirement

Hide communication between sender and receiver, i.e., provide a communication that raises as few attention as possible

… can be used by journalists to transfer illicit information but also by malware

Part I

The hiding techniques we already know …

… and what research did to counter network covert channels.

Typical Techniques for Covert Channels

- Packet Timings
- Packet Order
- Find something to piggyback (unused/redundant fields in ICMP, HTTP, etc.)

Typical Techniques for Covert Channels

- Many of the available hiding techniques & programs implement *crapto channels**.

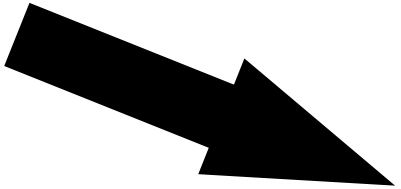
*adopted from „craptography“, i.e., crappy crypto implementations.

Shared Resource Matrix

	Operation A		
Attribut	Op1	Op2,Guard1	Op2,Guard2
a	R	-	-
b e	-	M	M
c	-	R	-
User-In	R	R	R
User-Out	M	M	M

Covert Flow Trees

```
2  procedure Lockfile(f: file);
3  begin
4     if not f.locked and empty(f.inuse) then
5       f.locked := true
6  end;
7
8
9  procedure Unlockfile(f: file);
10 begin
11    if f.locked then
12      f.locked := false
13 end;
14
15
16 function Filelocked(f: file): boolean;
17 begin
18    Filelocked := f.locked;
19 end;
```



	Lockfile	Unlockfile	Filelocked
reference	locked,inuse	locked	locked
modify	locked	locked	-
return	-	-	locked

Covert Flow Trees

	Lockfile	Unlockfile	Filelocked
reference	locked,inuse	locked	locked
modify	locked	locked	-
return	-	-	locked

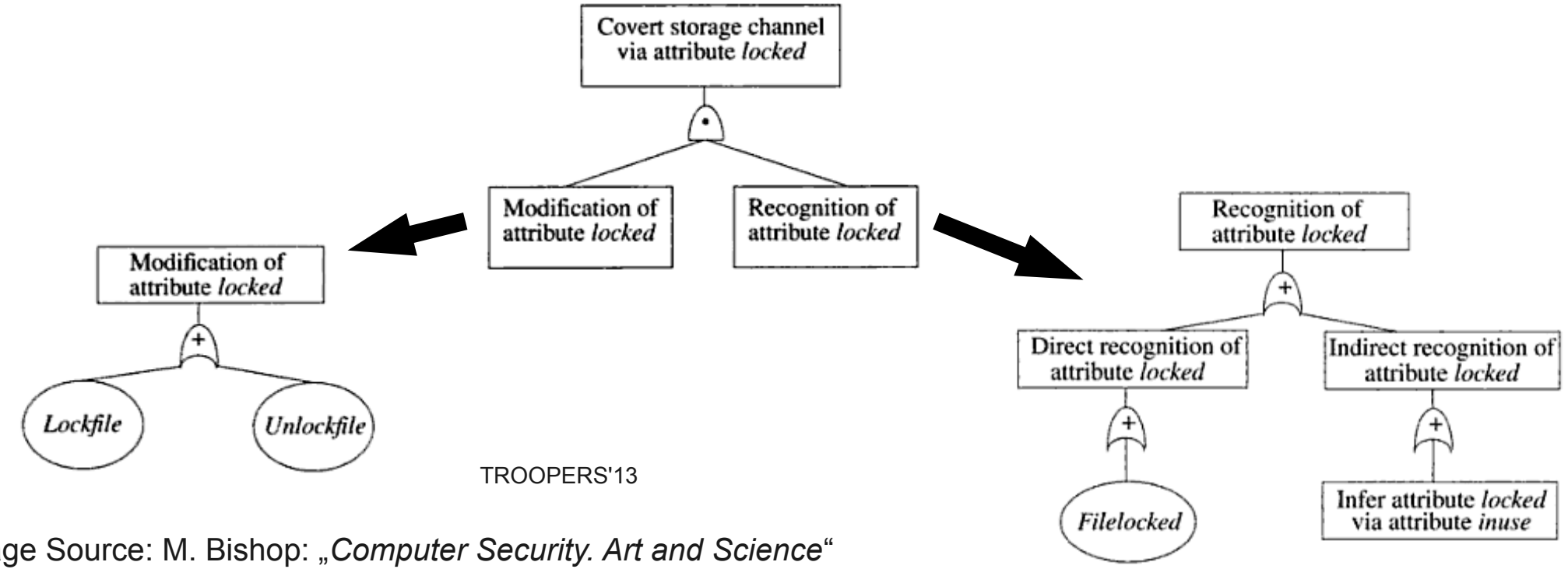


Image Source: M. Bishop: „*Computer Security. Art and Science*“

The Pump and Similar Approaches

Traffic Normalization

- Clear/Unify/Modify selected areas in network packet headers
- Cold Start Problem
- Inconsistent TCP retransmissions

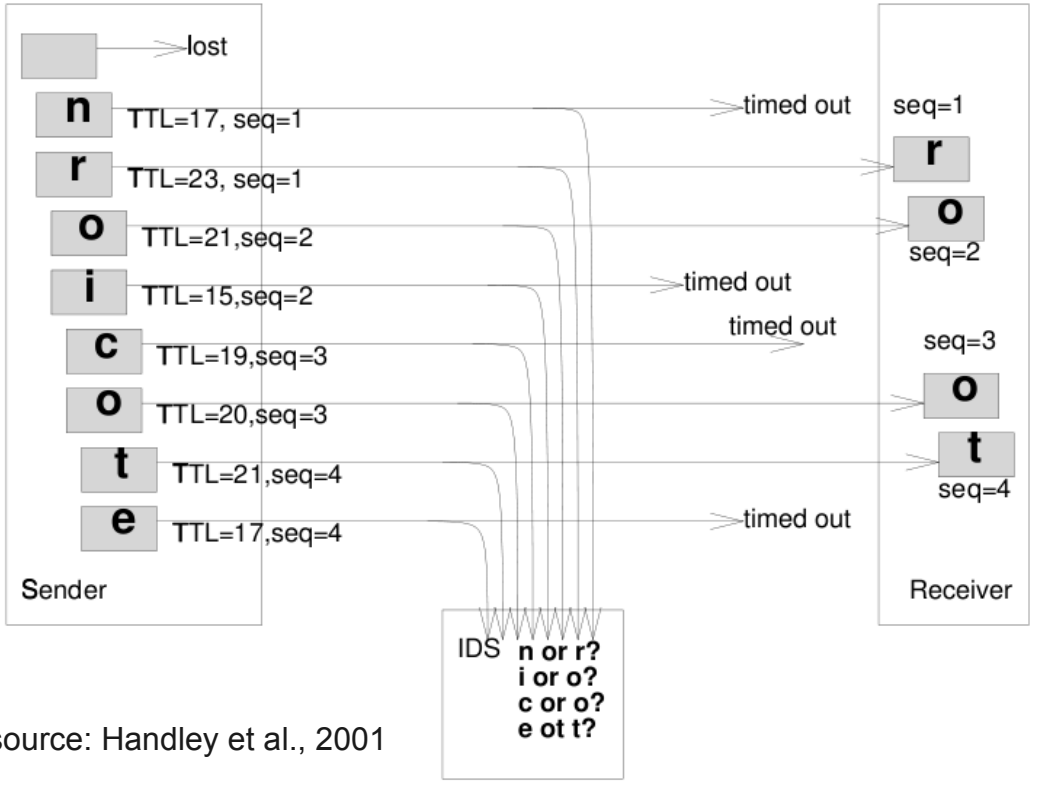
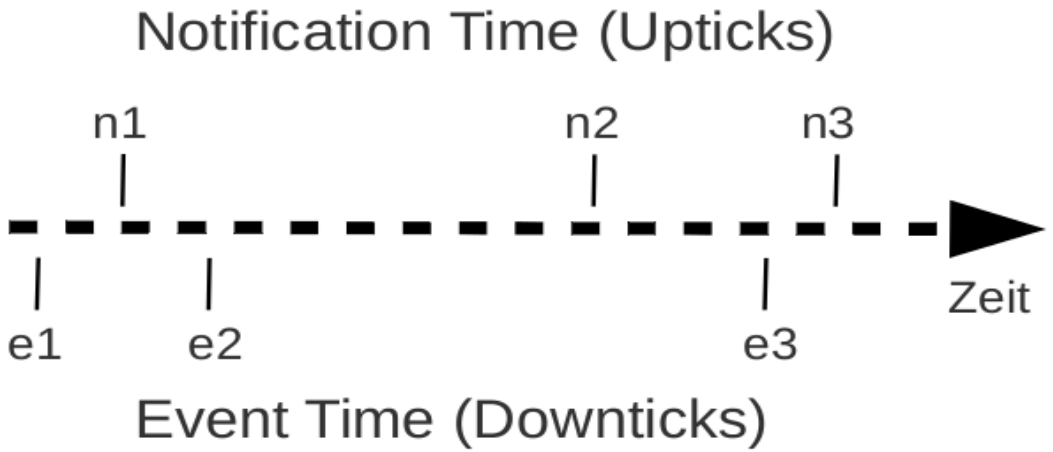


Image source: Handley et al., 2001

Fuzzy Time

- 1991 (VAX Security Kernel)



Other Approaches

- Statistical approaches
- Machine learning
- Various active wardens
- Business process evaluation
- Spurious processes approach
- Code modifications to prevent covert channels based on timing leaks
- … and quite many other academic approaches (cf. my latest book)

Summary (pt. 1)

Many means exist to

- … embed hidden information into network packets
- … to detect, limit, and prevent such embeddings
  - … some of them are ooold!
  - … but we cannot detect all techniques.

Part II

Novel Approaches for Network Covert Storage Channels

[selected aspects of a thesis]

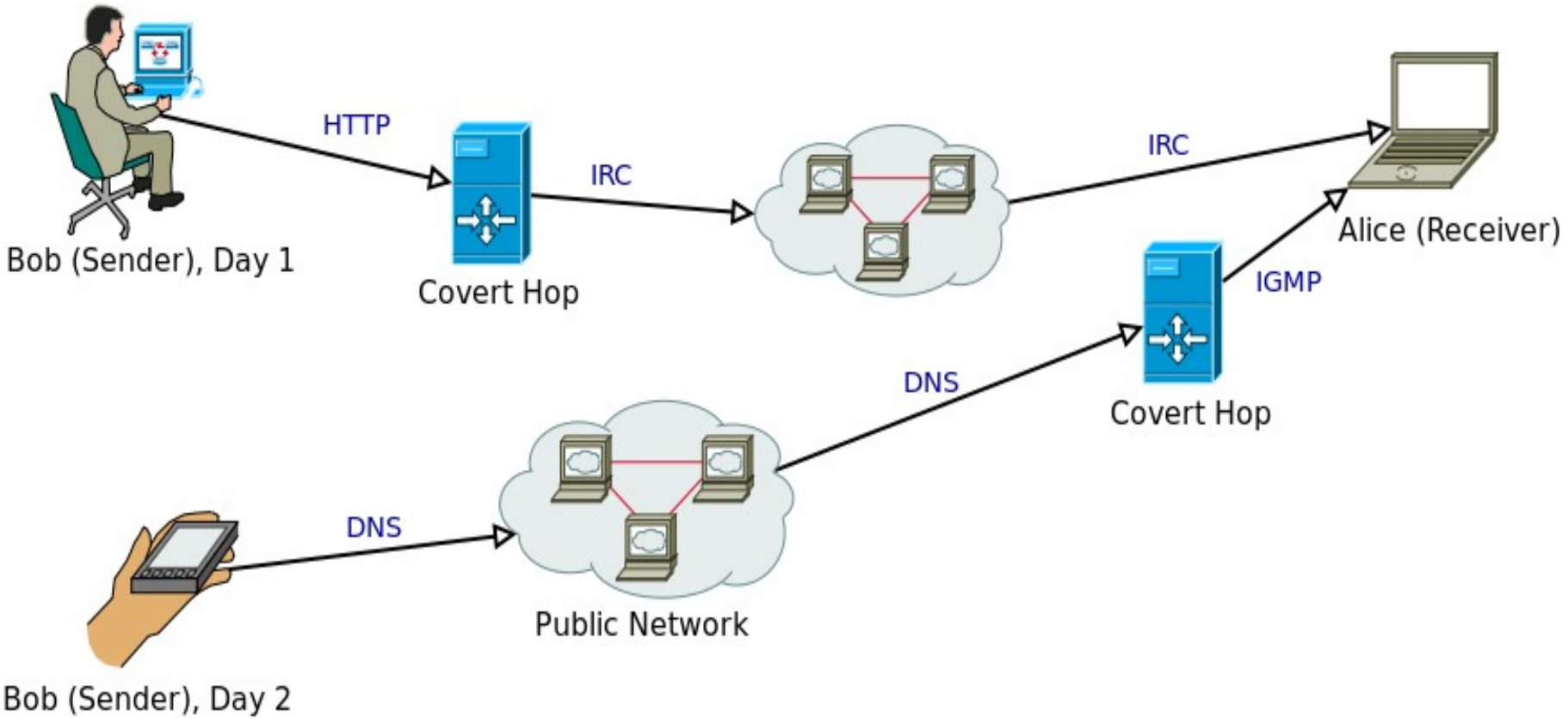
Related Work

- Existing CC-internal Control Protocols (Ray/Mishra, pingtunnel)
- Natural Selection for Network Protocols (Li et al.)
- Adaptive Network Covert Channels (Yarochkin et al.)
- Covert channels optimized for raising low attention

  using CC-internal Control Protocols

  … and Protocol Hopping Covert Channels

  … able to bypass normalizers.
- Protocol Channels

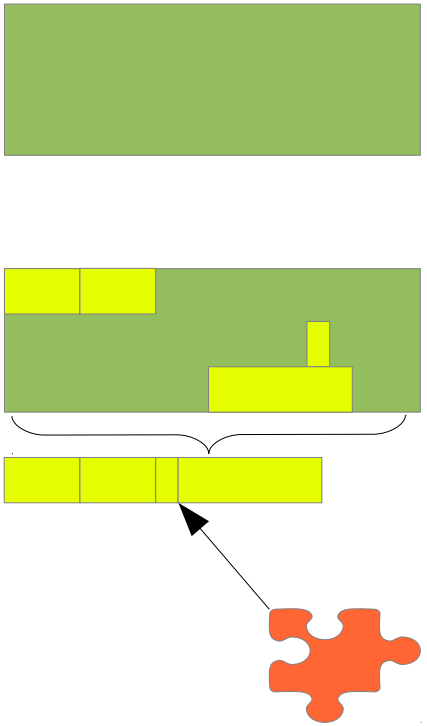

HTTP
IRC
IRC
Bob (Sender), Day 1
Covert Hop
Alice (Receiver)
IGMP
DNS
Covert Hop
DNS
Public Network
Bob (Sender), Day 2

Features

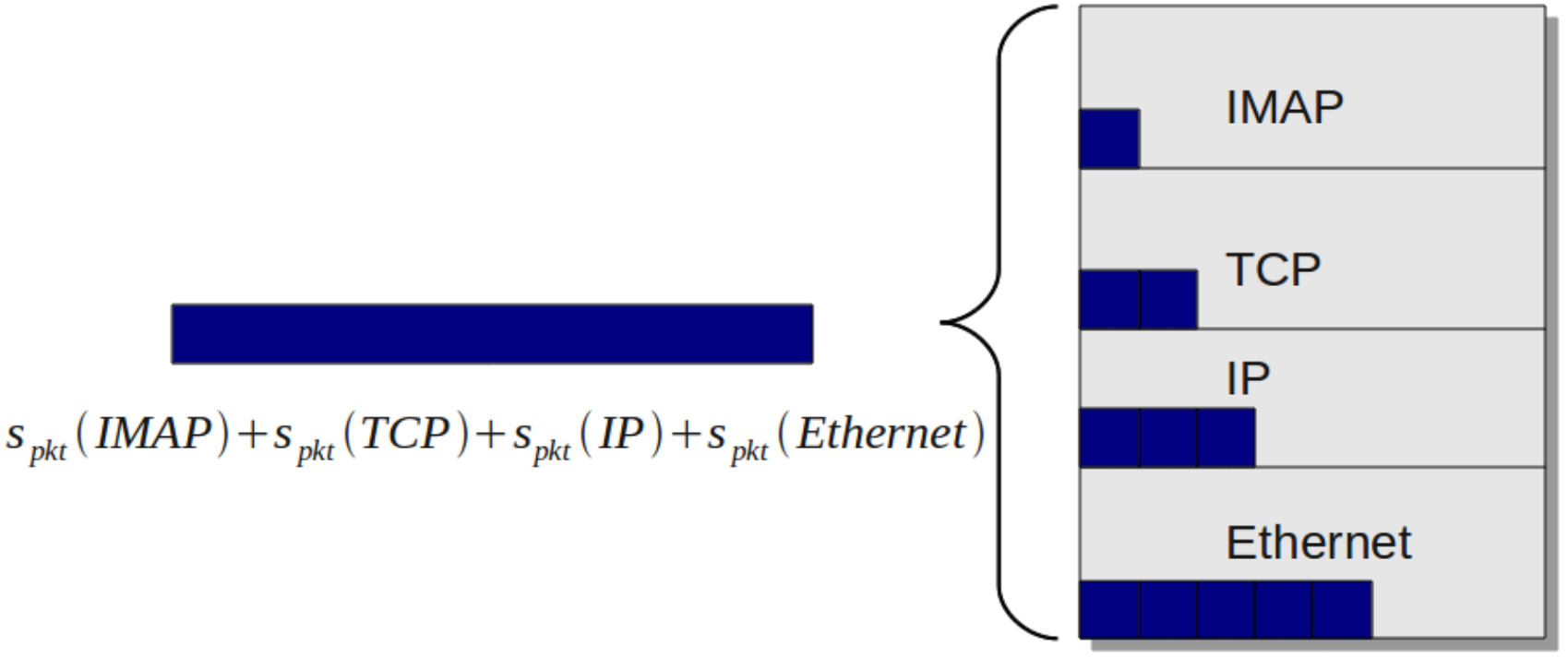
- Protocol Switching
  - Adaptive Covert Channels
  - Network Environment Learning Phase (NEL)
  - Mobile Environments
- Version-dependent protocol sets
  - Step-by-step Upgradability
- Space-efficiency and dynamic headers

Terminology

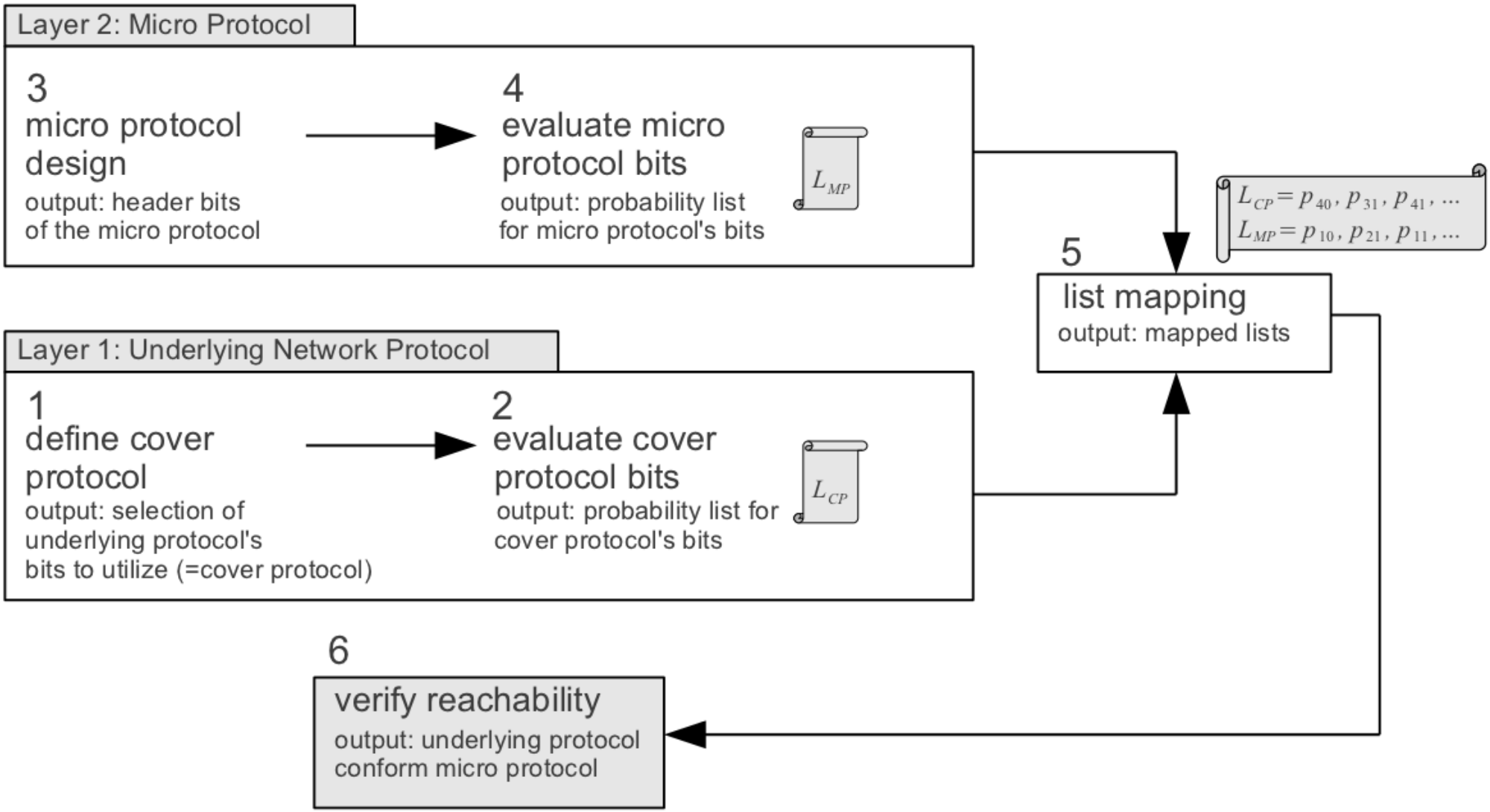
- **Terminology** as a means to provide finer distinctions between different points of view.
- **Underlying Protocol**
  - e.g. IPv4, TCP, ICMPv4, IPv6, …
- **Cover Protocol**
  - utilized area within the underlying protocol
  - e.g., 2 least significant bits of TTL + DF flag
- **Micro Protocol**
  - control protocol placed within cover protocol
  - shares cover protocol space with the covert channel's payload



Combining Multiple Layers



Micro Prot. Engineering Approach



Status Update Approach

- We tried to adopt existing protocol engineering means
- IPv6 „Next Header“, IP „Options“
- Compressed SLIP (CSLIP)
- Status Updates are is like a mix of „Next Header“, „IP Options“, and „CSLIP“.

Status Updates

- We link a communication between two CC peers to *statuses*.
- A connection can comprise different statuses, e.g.:
  - Source address
  - Destination address
  - Transaction state
- Status Updates indicate the update of a status.

Status Updates

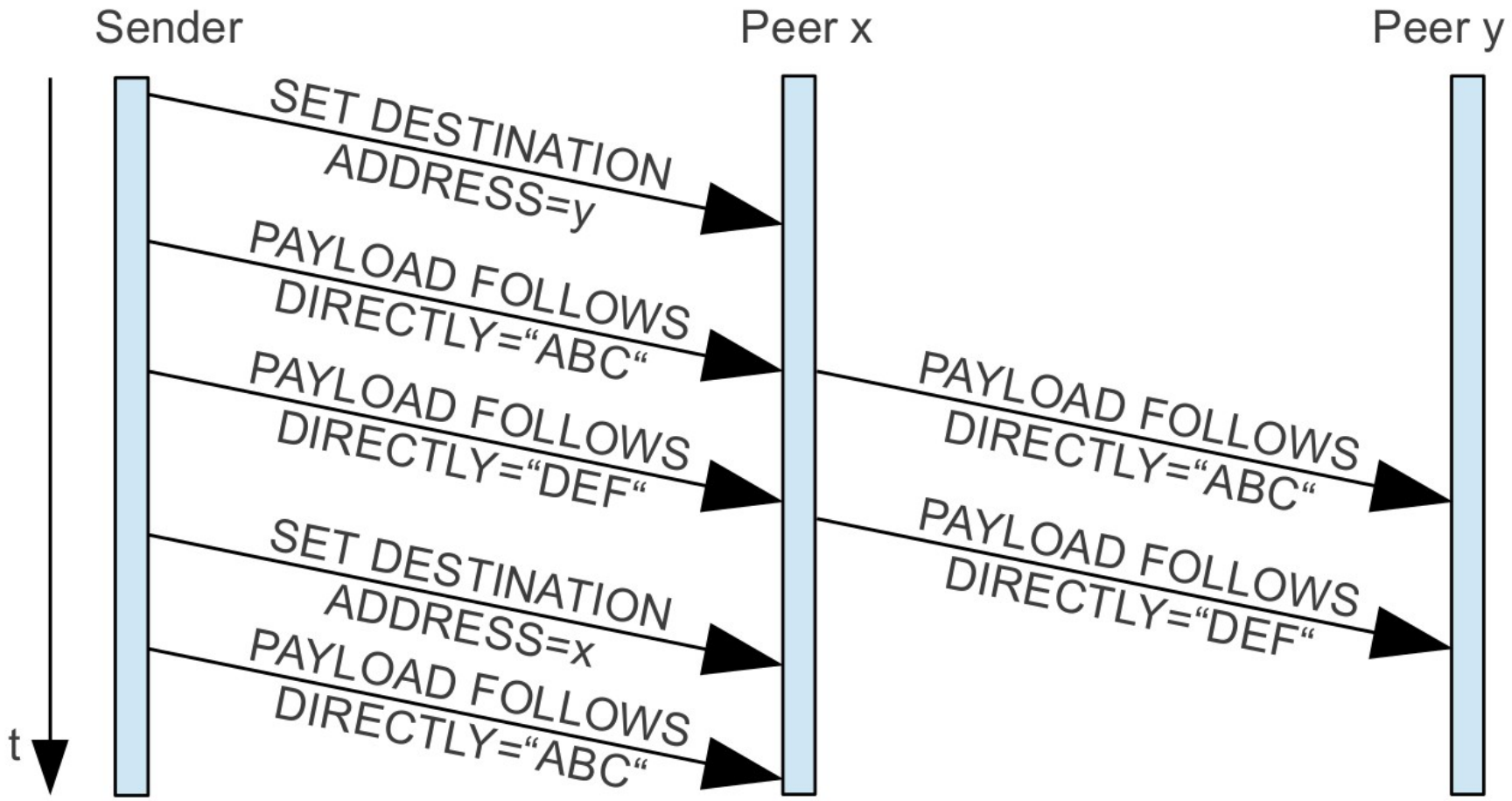
- One status update comprises
  - A „Type of Update“ value
  - The value for the update
- Therefore, sender and receiver share a ToU table, e.g.:
  - 00 SET SOURCE ADDRESS
  - 01 SET DESTINATION ADDRESS
  - 10 END OF UPDATES
  - 11 PAYLOAD FOLLOWS DIRECTLY

Status Updates

- For instance, to change the source address of a connection (e.g., on a proxy):

00 (SET SRC ADDR.)	**NEW SOURCE ADDRESS FOR THE CONNECTION (e.g., a small n bit overlay address or an underlay network's address)**

Example: Packet Forwarding



Combining ToUs to Sequences

Re-Design of Ray/Mishra'08

- Designed a status update-based version of a CC micro protocol developed by Ray and Mishra.

a) unmodified header (8 bits):

seq. number	data flag	ack flag	exp. seq. no.	start flag	end flag

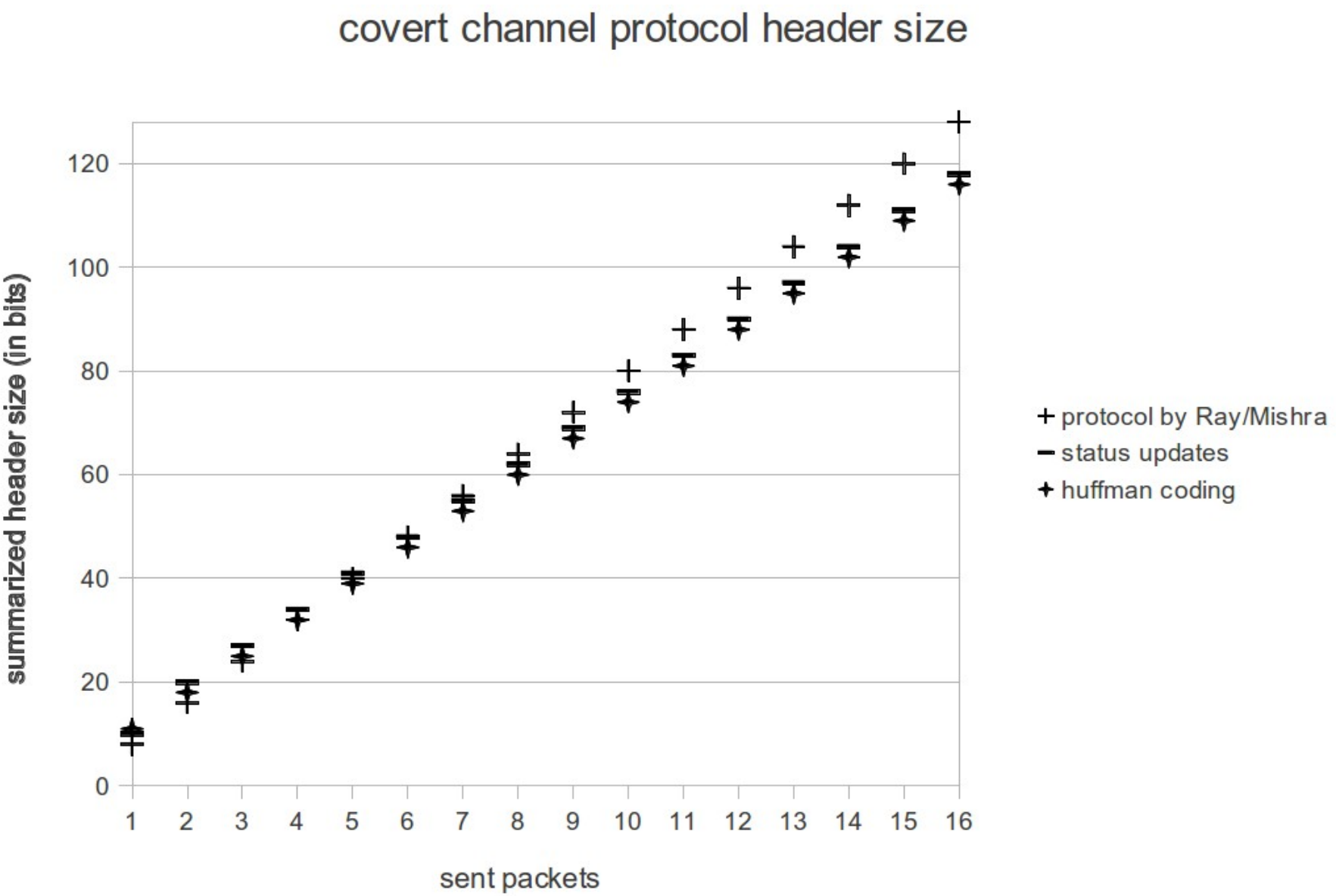
b) re-designed header, default ToU (7 bits):

ToU	seq. number	data flag	ack flg.	exp. seq. no.

c) re-designed header, start/stop ToU (3 bits):

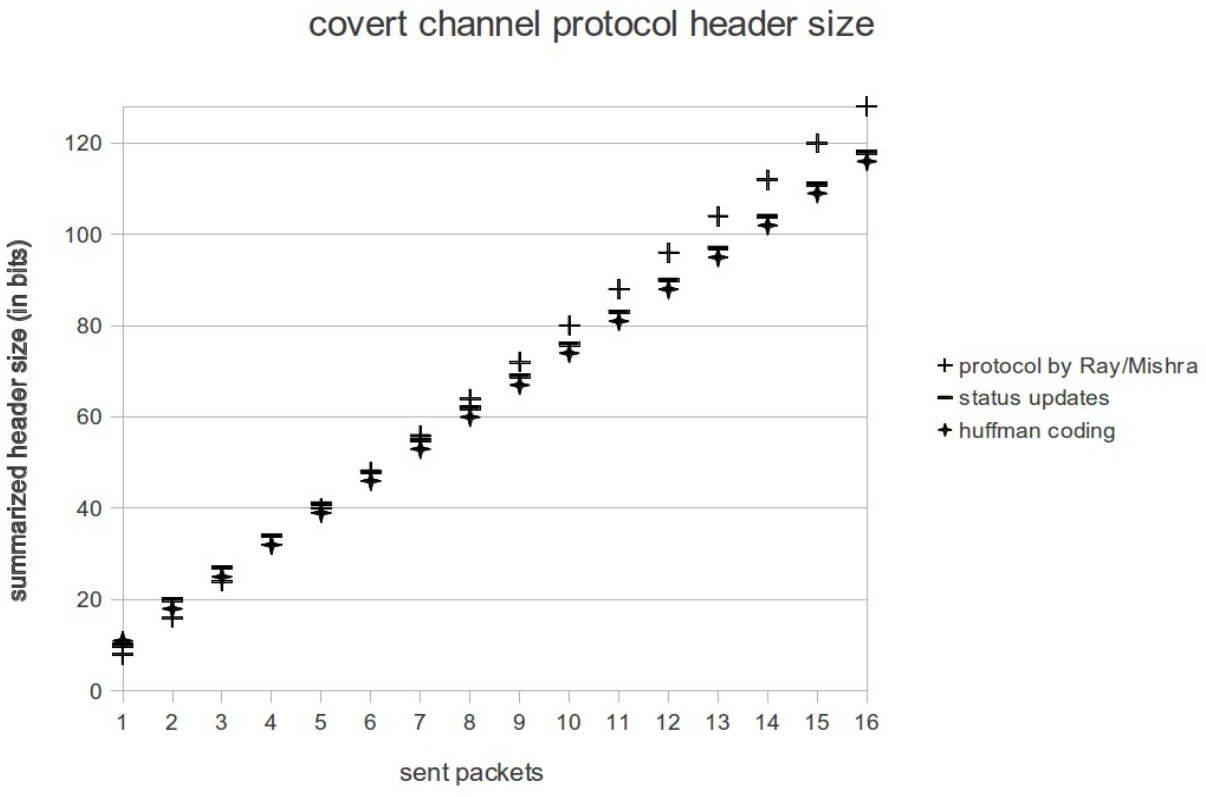
ToU	start flag	end flag

Re-Design of Ray/Mishra'08



Re-Design of Ray/Mishra'08

- Initial connection inefficiency problem
  - Many ToUs are required to initially configure a connection
  - These ToUs require more space than a normal header
  - SU perform better if a transaction requires >= 5 packets



Dynamic Routing in CC Overlays

- CC networks are overlay networks
- Similar to Ad-Hoc networks (changing components, changing topology)
- Existing approach for dynamic routing in steganographic networks was presented by Szczypiorski et al. and was based on the random-walk algorithm.

Requirements for CC Routing

- Routing overhead should be small
  - Status updates
- Must be capable to adapt quickly to topology changes since underlay network can change at any time.
  - Only small routing overhead should be produced for propagating updates.
- Overlay network addresses can differ to underlay addresses and a routing approach must support overlay addresses.

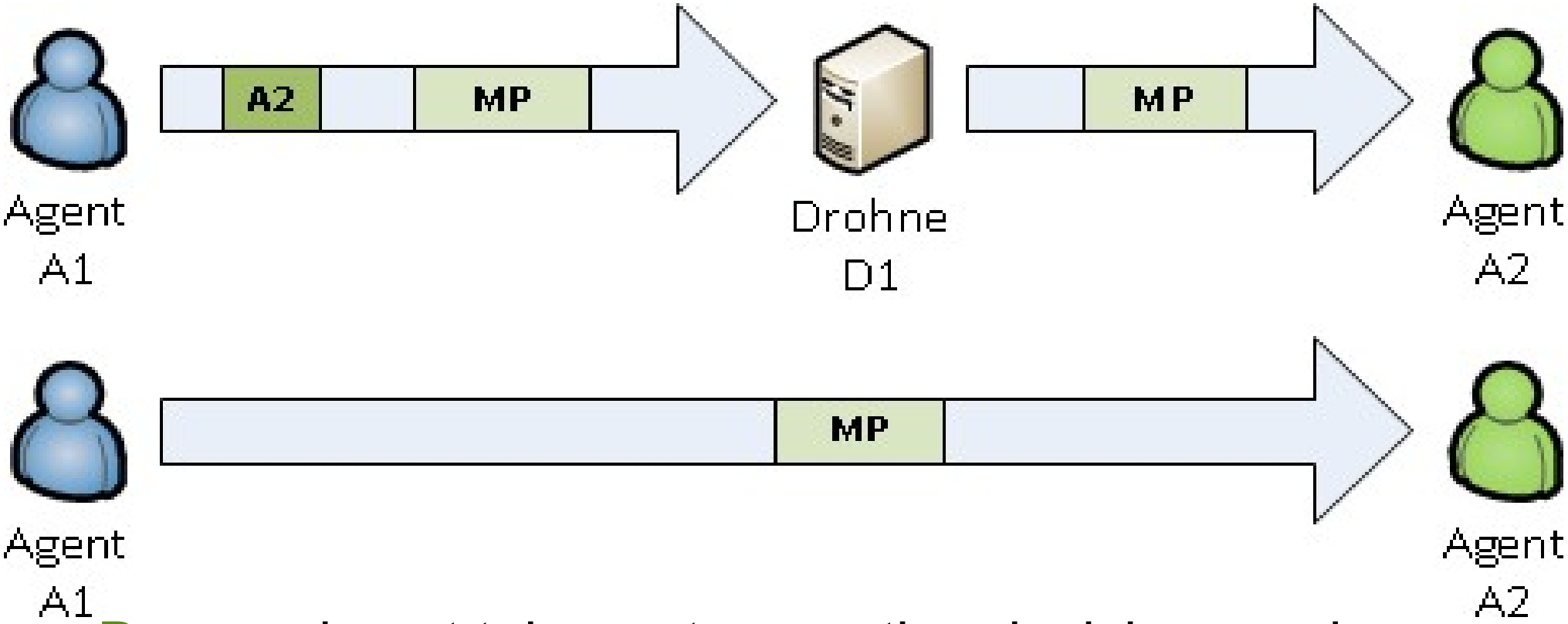
Our Approach

- Sender is responsible for route plotting (source routing).
- We implemented optimized link state routing (OLSR)
  - OLSR was designed for mobile Ad-Hoc networks
  - … with the goal of a small routing overhead
  - Multi-Point Relays (MPR)
    - A peer floods updates only to peers of his MPR set (similar like OLSR).
  - Status Update-based realization to achieve minimal micro protocol overhead

Dynamic Routing in CC Overlays

- Introducing **Quality of Covertness**
- Extendable Architecture
- Dynamic Cover Protocol Switching
  - Protocol Hopping Covert Channels
- Network Environment Learning Phase
  - Peers determine possible communication options between each other

Agents and Drones for Overlay Routing



Drones do not take part on routing decisions and are never a routing path's destination

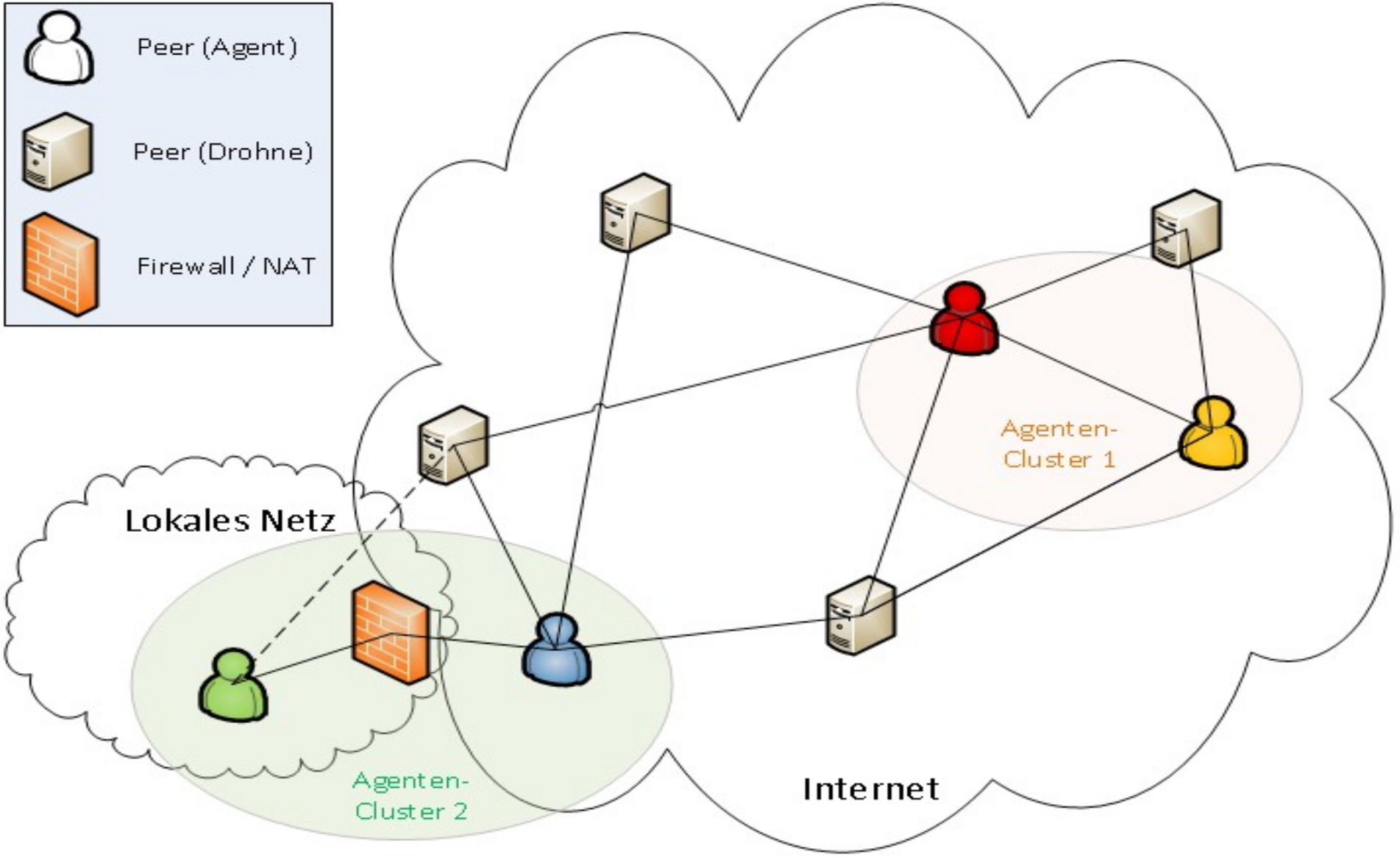
Drones are not aware of a covert communication.

Agents and Drones for Overlay Routing

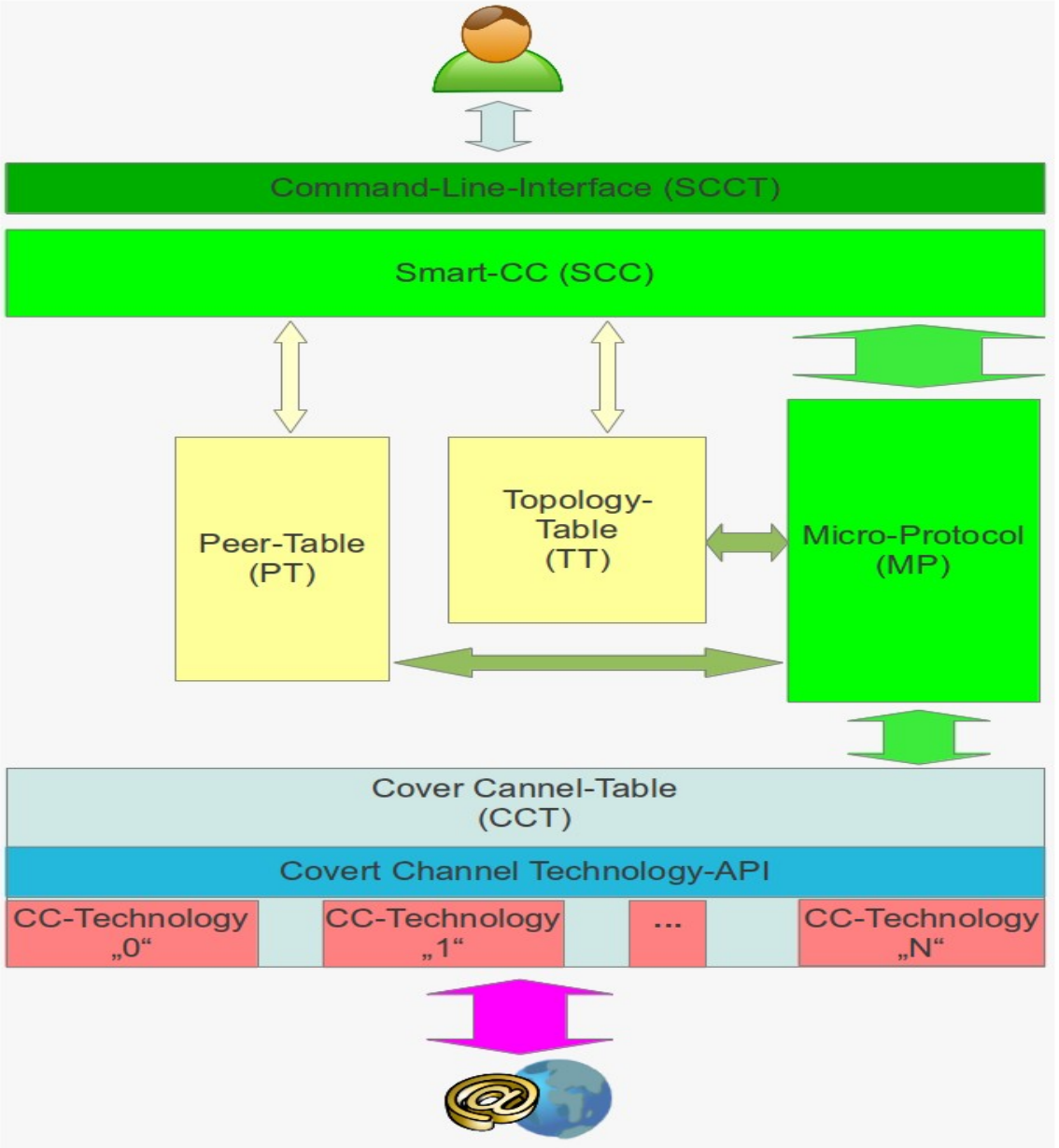
- Our approach comprises a CC network topology table
  - A graph of the paths between peers as well as their capabilities (supported CC techniques)
  - Is propagated between the peers
  - New ToUs for routing propagation were required:

Type of Update	**Meaning**
REQUEST_PT_TT	Used by a peer to request the full peer table and topology table while bootstrapping.
RESPONSE_PT_TT	Response to REQUEST_PT_TT.
TT_LIST	A sequence of edges of the topology graph. Send on topology changes. Propagated according to MPRsel.
PT_ENTRY	A new or updated entry to the peer table. Send when a peer crashes, goes off, or joins the network, or changes CC capabilities. Propagated according to MPRsel.

Agent Clusters

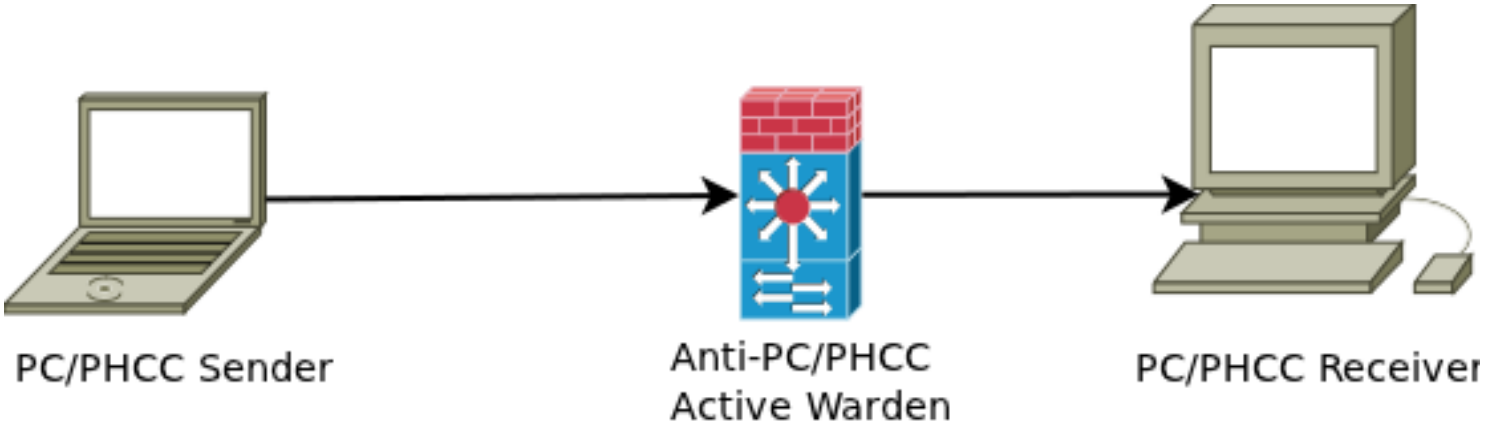


SCCT


Command-Line-Interface (SCCT)
Smart-CC (SCC)
Peer-Table
(PT)
Topology-
Table
(TT)
Micro-Protocol
(MP)
Cover Cannel-Table
(CCT)
Covert Channel Technology-API
CC-Technology
„0“
CC-Technology
„1“
...
CC-Technology
„N“

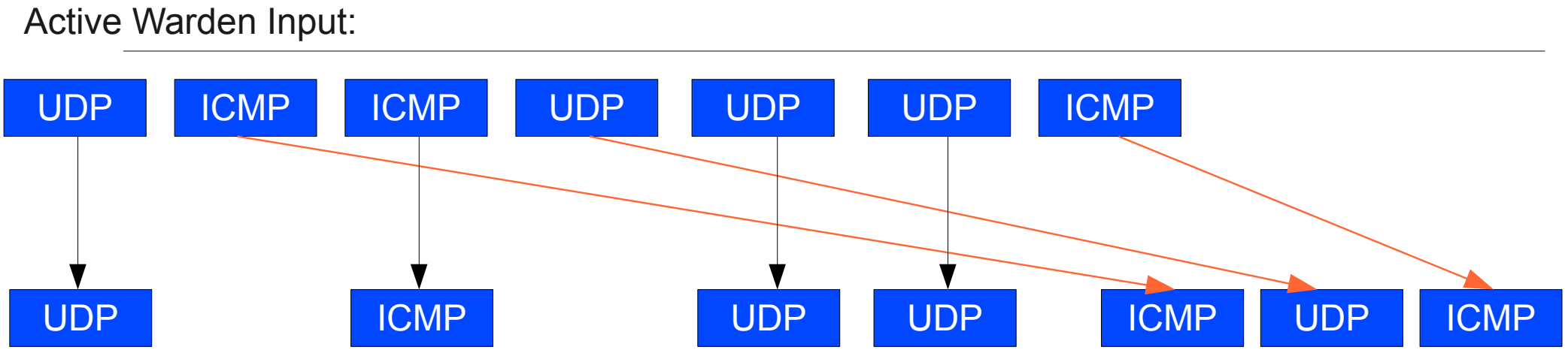
What can we do to counter PSCCs?

- By introducing delays on protocol switches
- PoC code based on **delay-net/IPQueue** and **iptables**



Example

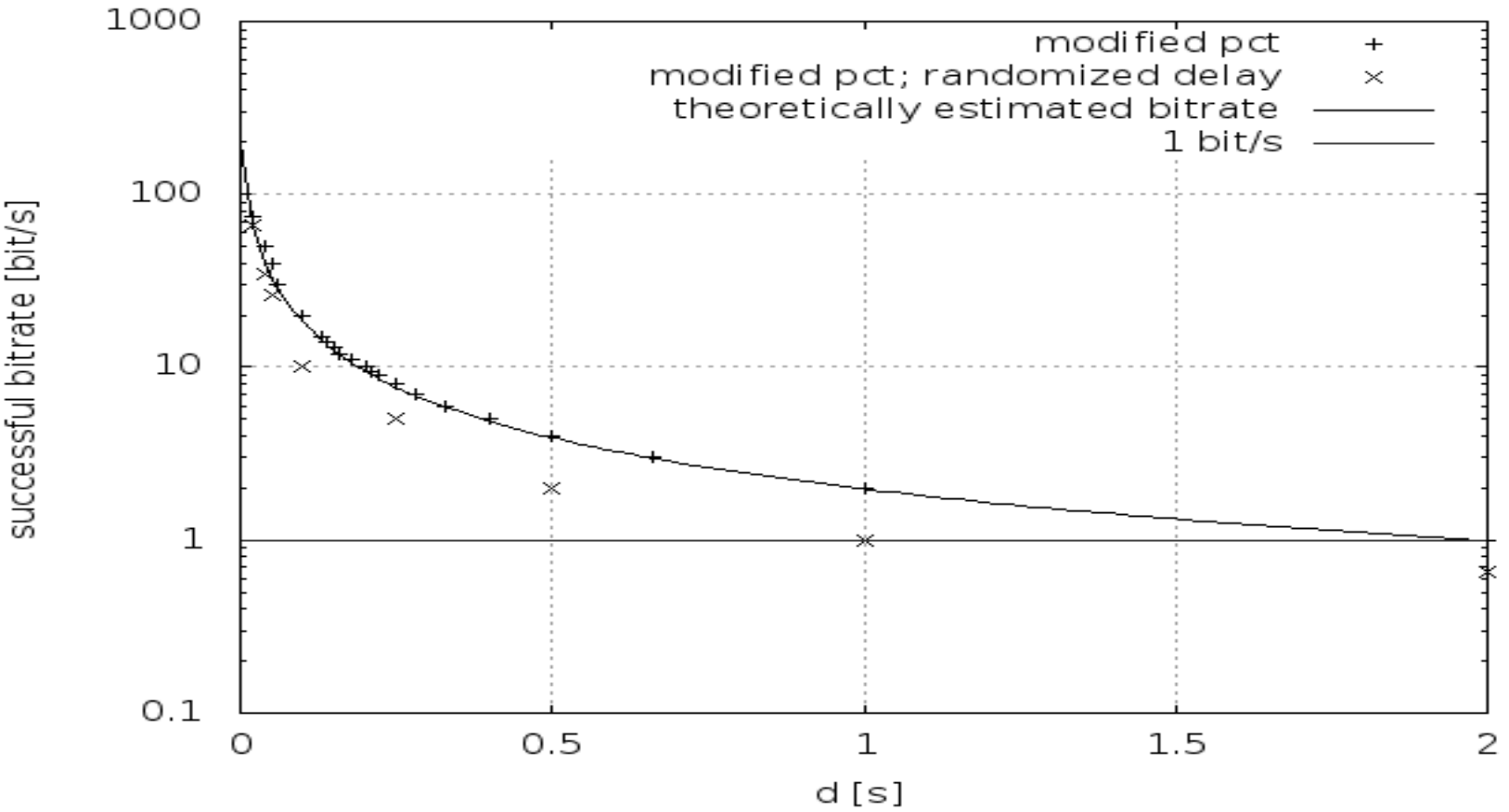
- Protocol Channel based on ICMP (1) & UDP (0)
- Message „0110001“ with high *d* (e.g. *1s*)



Output: U,I,U,U,I,U,I or 0100101

Results

- Pretty useful to counter **protocol channels**!
- Can counter **protocol hopping covert channels** without sequence numbers in their micro protocols!



Summary (pt. 2)

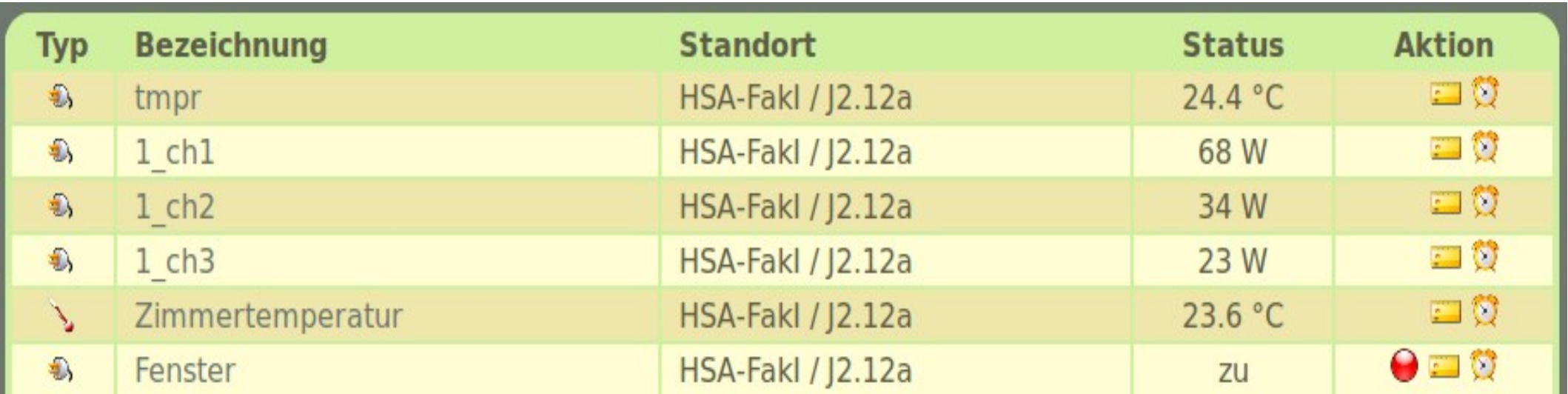
- Improved CCs with **protocol hopping**
- CC **overlays** with **dynamic routing** capability
  - Agents and Drones
  - **Upgradable** Infrastructure
  - **Mobile Access**
- Internal control protocols (**micro protocols**)
  - Optimized for a low-attention raising operation
  - Utilization of **multiple layers** for **cover protocols**
- **Active warden** to counter protocol switches

Part III

Covert and Side Channels in Building Automation Systems

Side Channels in BAS

- **Side channels** are covert channels without intentional sender
- A side channel in a BAS leaks information about **events** taking place within a building
- Examples:
  - Employee uses a side channel to detect the presence of his boss in his office in order to steal a document.
  - Observing healthiness / Ambient Assisted Living



Typ	Bezeichnung	Standort	Status	Aktion
	tmpr	HSA-FakI / J2.12a	24.4 °C	
	1_ch1	HSA-FakI / J2.12a	68 W	
	1_ch2	HSA-FakI / J2.12a	34 W	
	1_ch3	HSA-FakI / J2.12a	23 W	
	Zimmertemperatur	HSA-FakI / J2.12a	23.6 °C	
	Fenster	HSA-FakI / J2.12a	zu	

Covert Channels in BAS

Enterprise network could be highly protected

→ data leakage will be difficult

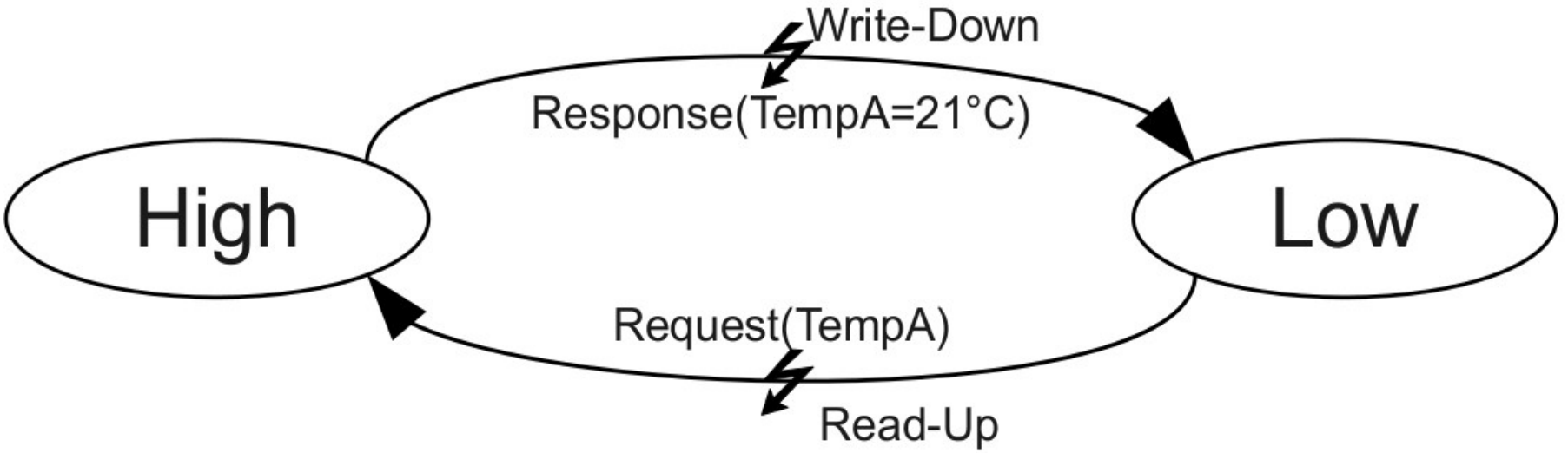
Solution:

Exfiltrate confidential information using a **covert channel** (e.g., BAS broadcasting).

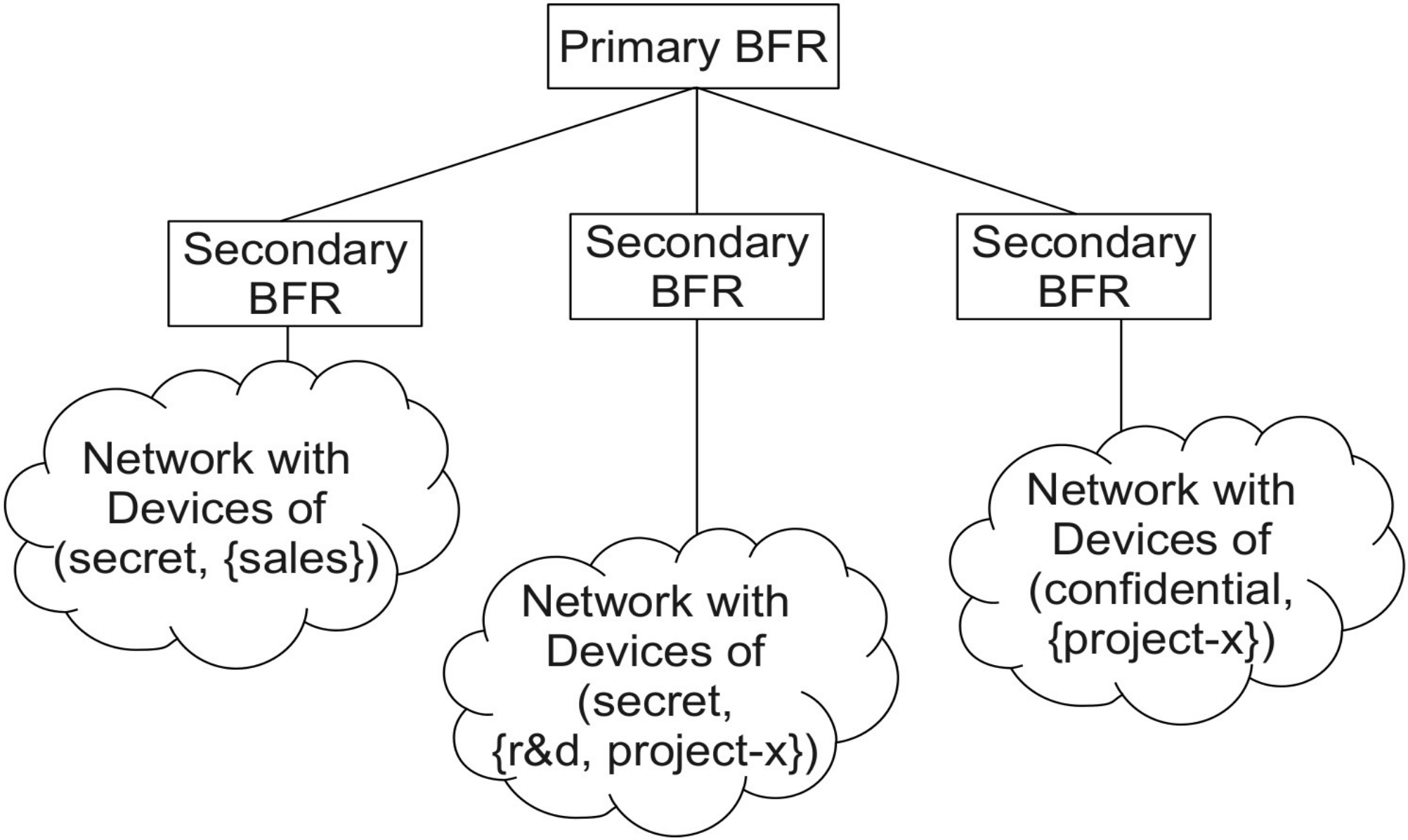
The receiver can either be connected to the BA network or can sniff a tunneled BA connection between multiple buildings.

- e.g., BACnet/IP (encapsulated in UDP)

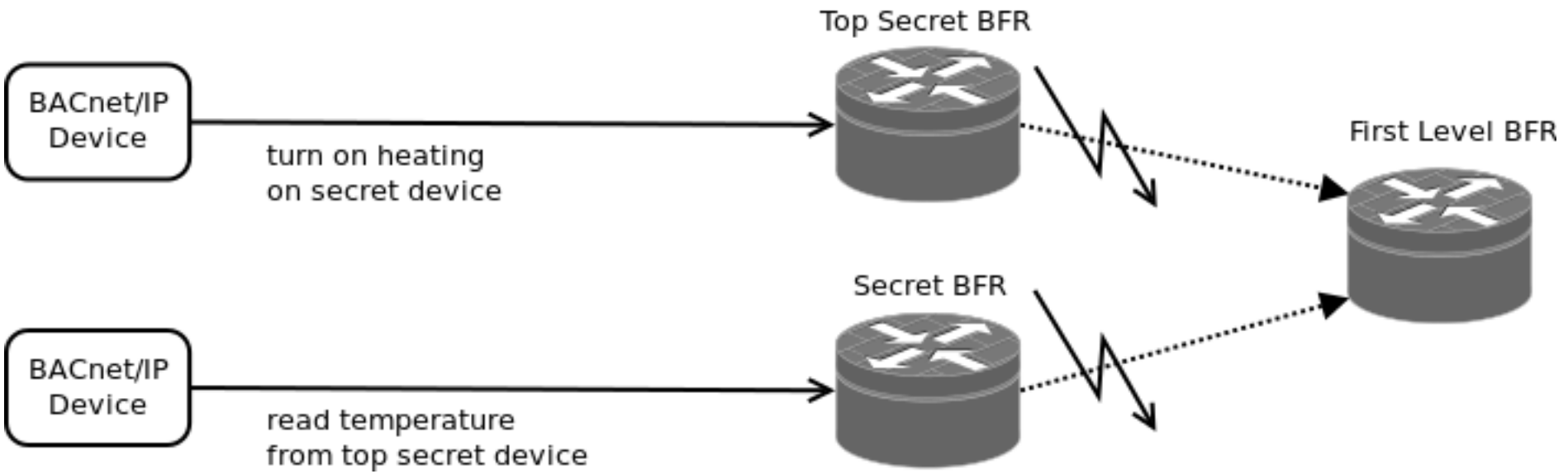
BACnet Protection



Introducing MLS using the Open Source BACnet Firewall Router



MLS+BFR = Protection!



Summary (pt. 3)

- We presented the first **side** channels and **covert** channels in BAS, and especially in BACnet.
- We presented a means to protect BACnet environments based on the **BACnet Firewall Router**.
  - … not really stable,
  - … bad documentation,
  - … over-engineered (configurable via „stacks“).
- We need a stable and usable BACnet firewall!
  - Any volunteers?

What can we conclude?

There are various means to establish covert channels and various (theoretical) means to counter covert channels.

Novel approaches enable covert channels to become **pretty valuable for malware** …

… but *should* become valuable for the „good guys“.

Covert (and Side) Channels exist in Building Automation Systems …

… but can be prevented.

However, the important thing is …

You can

… enable covert channels to become useful in practice (journalists).

… create real systems to counter the botnets of the future.


END
1
FLEMING ST.
LOVE RUM?
MILE
0
FLEMING
WHITEHEAD
ST
ATM

Related Publications

- Books:
  - Steffen Wendzel: Tunnel und verdeckte Kanäle im Netz, Springer-Vieweg, 2012. (in German)
- Scientific Papers (Selection):
  - Steffen Wendzel, Jörg Keller: Preventing Protocol Switching Covert Channels, In: International Journal On Advances in Security, vol. 5 no. 3&4, pp. 81-93, 2012.
  - Steffen Wendzel, Benjamin Kahler, Thomas Rist: Covert Channels and their Prevention in Building Automation Protocols -- A Prototype Exemplified Using BACnet, in Proc. 2nd Workshop on Security of Systems and Software Resiliency, pp. 731-736, Besançon, France, IEEE, 2012.
  - Steffen Wendzel, Sebastian Zander: Detecting Protocol Switching Covert Channels, 37th IEEE Conf. on Local Computer Networks (LCN), pp. 280-283, Clearwater, Florida, IEEE, 2012.
  - Steffen Wendzel, Jörg Keller: Systematic Engineering of Control Protocols for Covert Channels, In Proc. 13th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security (CMS 2012), LNCS 7394, pp. 131-144, Canterbury, Springer, 2012.
  - Steffen Wendzel: Covert and Side Channels in Buildings and the Prototype of a Building-aware Active Warden, First IEEE International Workshop on Security and Forensics in Communication Systems (SFCS 2012) of the 2012 IEEE ICC, pp. 6753-6758, Ottawa, Canada, IEEE, 2012.
  - Steffen Wendzel, Jörg Keller: Low-attention forwarding for mobile network covert channels, in Proc. 12th Conference on Communications and Multimedia Security (CMS 2011), IFIP, LNCS vol. 7025, pp. 122-133, Ghent, Belgium, Springer, 2011.
  - More available here: http://www.wendzel.de/publications/index.html
- Professional Articles:
  - Benjamin Kahler, Steffen Wendzel: How to own a Building? Wardriving gegen die Gebäude-Automation, in Proc. 20. DFN Workshop ``Sicherheit in vernetzten Systemen'', pp. H1-H13, 2013. (in German)