# Micro protocols and dynamic protocol switches for network covert channels

Guest Talk at Swinburne University of Technology, Melbourne

Steffen Wendzel
University of Hagen /
Augsburg University of Applied Sciences

- Steffen Wendzel
  - Ph.D. student (University of Hagen, Germany)
    - internal protocols for network covert storage channels
  - IT4SE project (Augsburg University of Applied Sciences, Germany)
    - reducing energy consumption in smart homes
    - www.it4se.net („IT for Smart renewable Energy generation and use“)

# Outline

- Single-Slide BAS Security Overview
- Covert channel overlay networks
- Micro protocols
- Dynamic protocol switches
- Optimized forwarding

# BAS Security (IT4SE)

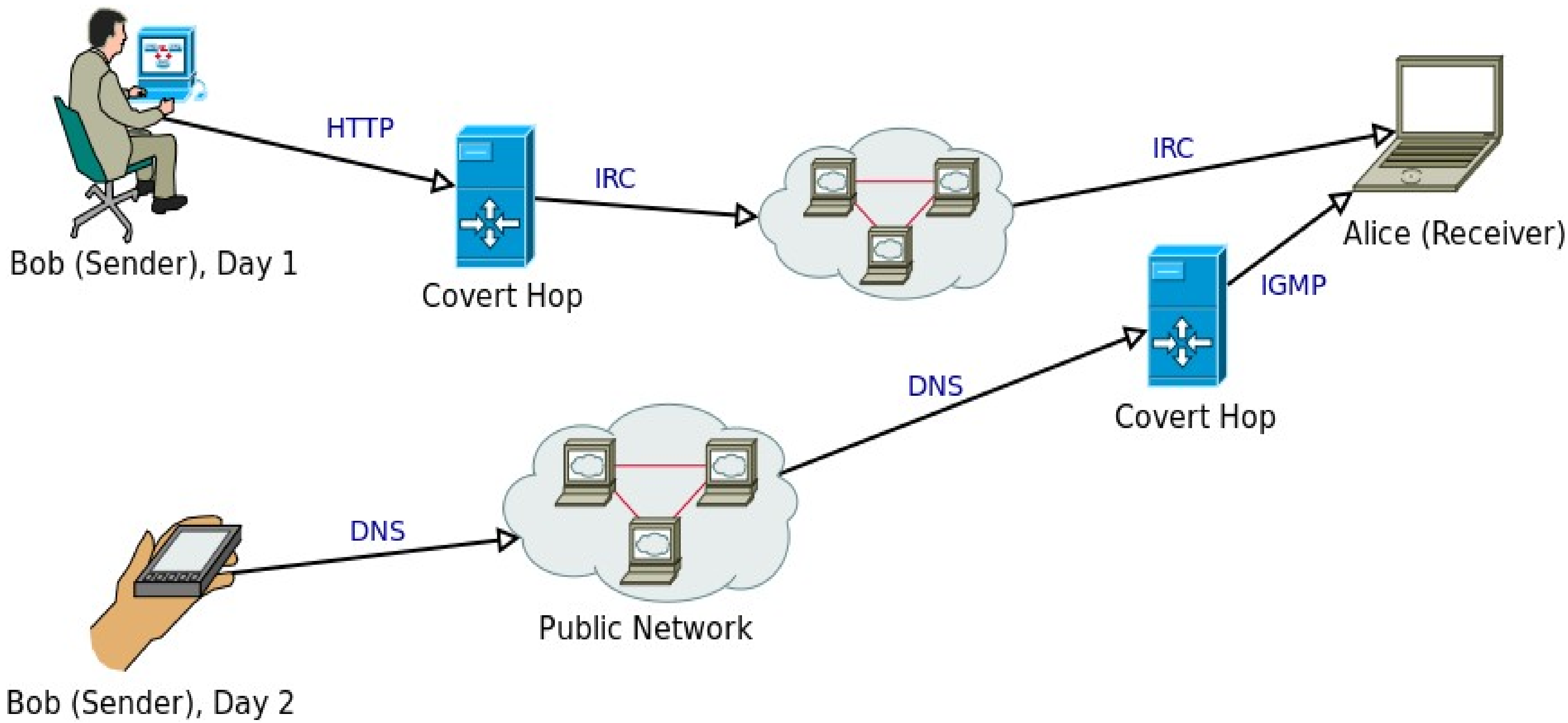
- Missing basic security features (e.g. encryption) and very old hardware
- Unpublished communication protocols (e.g. HomeMatic Home Automation System)
- Security middleware „HASI“
  - Goal: Privacy + Reducing Energy Consumption
  - Usability Aspects (e.g. energy advisor)
    - Visit www.it4se.net to find out more :-)

Advisor Rabit and „CurrentCost“

# covert storage channels based on micro protocols

# Scenario (pt. 1)

Auto-configuration within covert channel overlay network for mobile users:



# Scenario (pt. 2)

- Multiple users/devices/access points for the covert channel overlay network

  → various covert channel software versions with

  → different supported protocols
- Step-by-step infrastructure upgrade (backward-compatibility)
- Enabling version-independent covert channel communication for peers

  → passive NEL is not sufficient

  → active NEL: Exchange covert channel

  protocol information using micro protocols

# Related Work (hacking community)

- LOKI2 („daemon9“, Phrack Mag. Vol. 7/51, 1997)

  *”Swapping protocols is broken in everything but Linux. (...) This is why this feature is 'beta'.*” → /swapt

- Protocol Hopping Covert Channels (2007)
  - Transparent protocol switching
- Covert channel-internal protocols
  - ACK flags, seq. numbers, various flags, …
  - e.g. Pingtunnel by Stodle

# Related Work (scientific part)

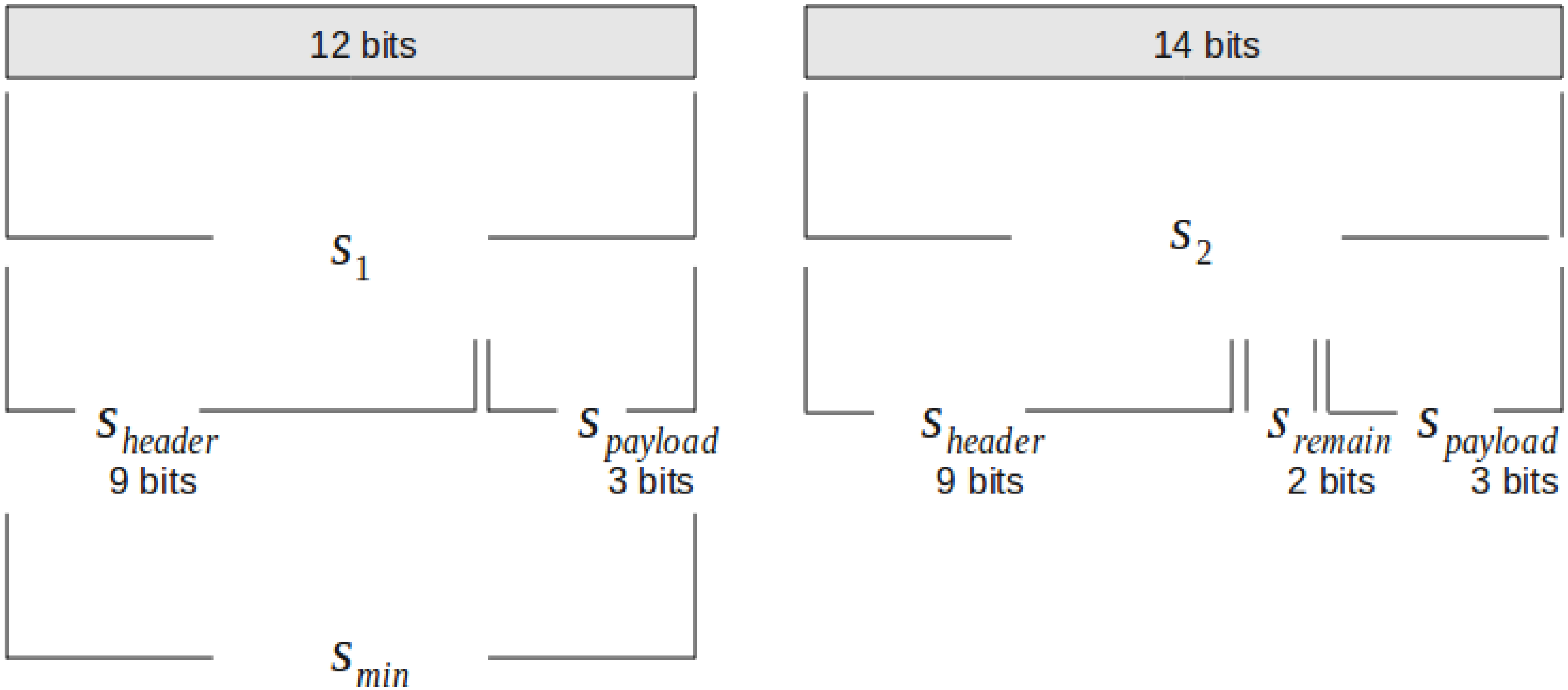
- Ray and Mishra: *A Protocol for Building Secure and Reliable Covert Channel* (2008):

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

- Yarochkin et. al.: *Towards Adaptive Covert Communication System* (2008)
  - Network Environment Learning Phase (NEL)
  - Communication Phase

# „Initiator Protocol“

- Unified base for covert communication (support is mandatory at the beginning of each new connection between peers)

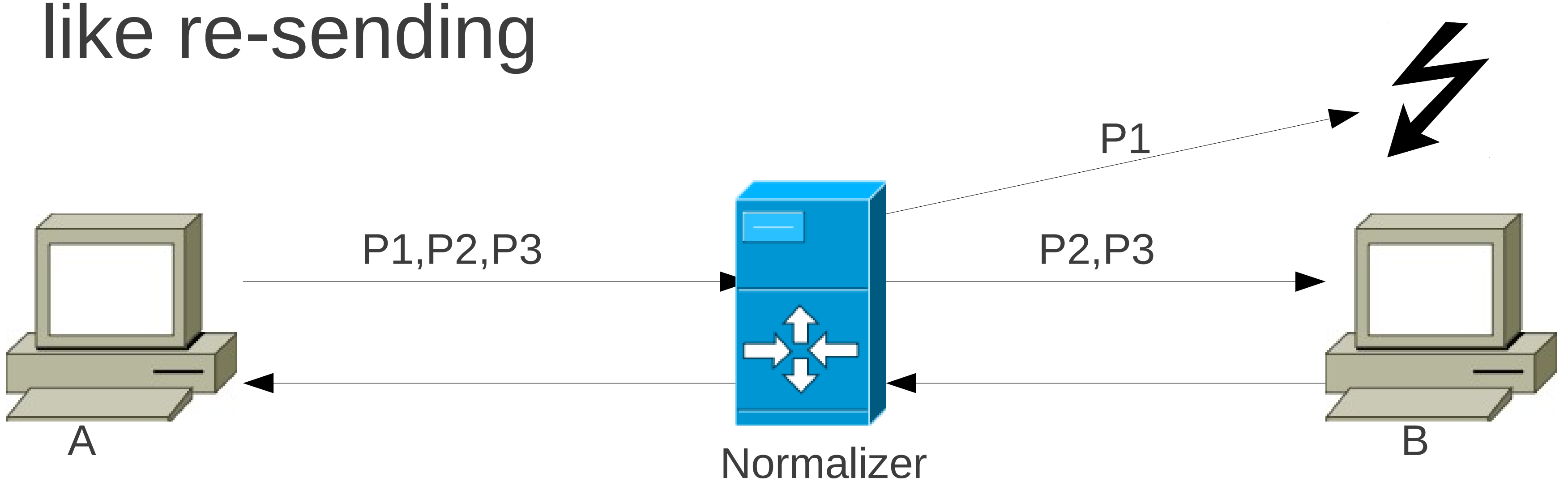


# Choosing Protocols

- Using more bits of a packet's header → raise more attention
- Using LSB of the TTL or using MSB of the TTL results in different raised attention
- HTTP URL or HTTP User Agent
- We cannot define values for single protocols
  - Raised attention always depends on the network's monitoring infrastructure
  - Exotic protocols raise more attention (e.g. EGRP in a BGP network)
- Possible solution: Linking protocols to attention classes (Low, Avg, High)

# Normalizer Problem

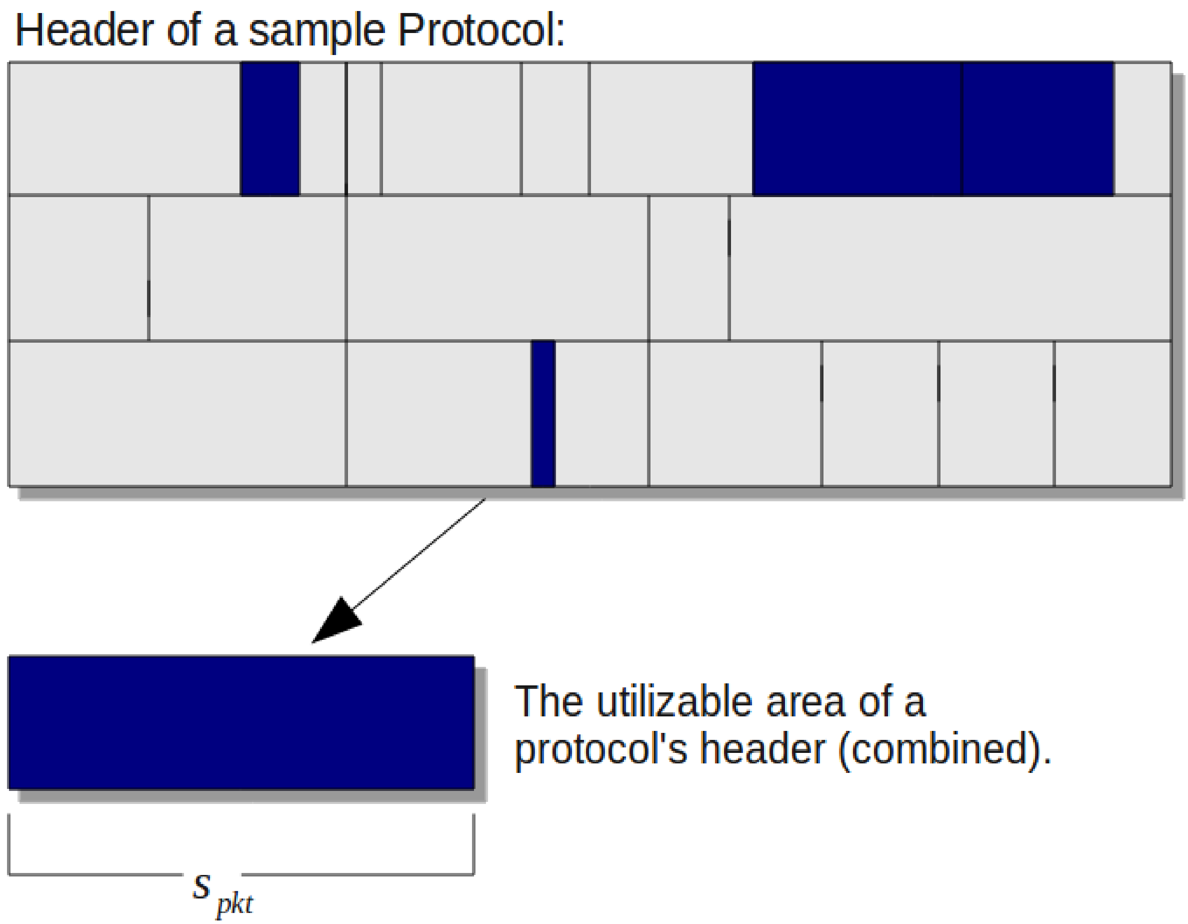
- Yarochkin et. al. as well as Wendzel/Keller: Two-army problem within NEL
- Problem: A and B cannot determine whether some <u>cover</u> protocols are blocked, cleared or modified by an active warden
- Two solutions: temporary participant C or TCP-like re-sending



# Space Requirements

- Combining a header's areas: $s_{pkt} := \sum_{i=1}^{n} s_i$
- #packets per unidirect. transaction:

$$N := \lceil \frac{s_{overall}}{s_{pkt}} \rceil$$



# Space Requirements (2)

- Average data per covert channel packet

  Round robin:

  $$s_{pkt} := \frac{\sum_{i=1}^{n} s_i}{n}$$

  different prob(p):

  $$s_{pkt} := \sum_{i=1}^{n} p_i \cdot s_i$$

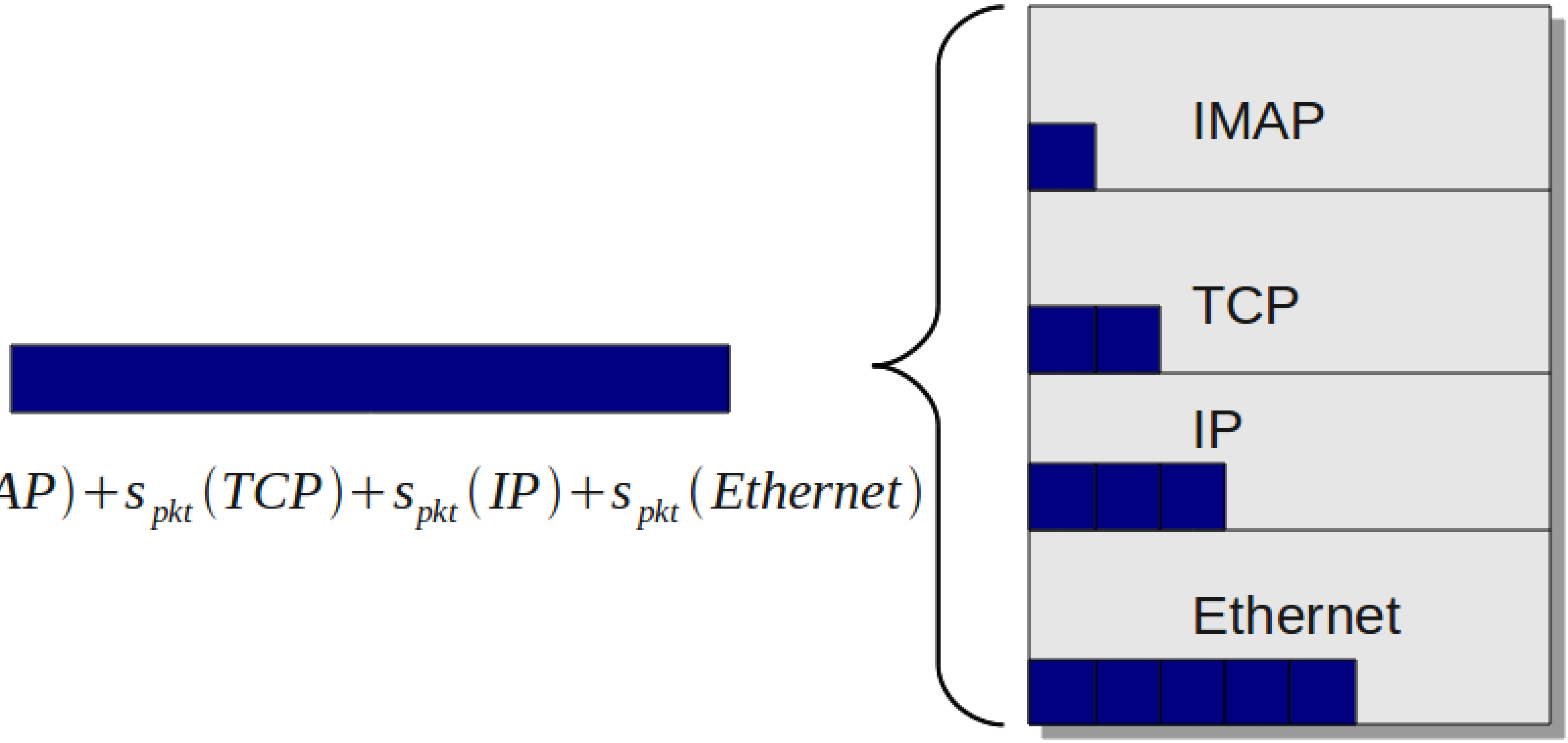
- A single protocol can result in multiple elements in P (the set of supported protocols of a peer):
  - E.g.: uncombinable elements

    $$P = \{ HTTP_{POST}, HTTP_{CONNECT} \}$$
  - But: redundant elements:

    $$P = \{ ICMP_{echo} \}, p_{ICMP_{ECHO}} = p_{ICMP_0} + p_{ICMP_8}$$

# Space Requirements (3)

Combining multiple layers




$$s_{pkt}(IMAP)+s_{pkt}(TCP)+s_{pkt}(IP)+s_{pkt}(Ethernet)$$

# Use-case dependent optimization

- Two use-cases:
  - Protesters: fast mobile upload of videos of harmed other protesters → high throughput, small attention.
  - Automatic password cracker (1 password/h)

    → small throughput, minimized attention.

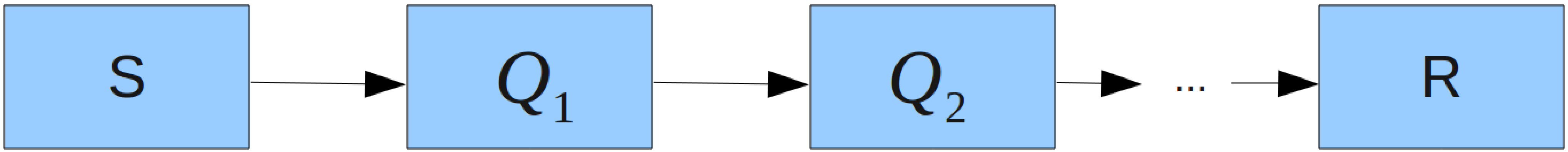
$$f_1 = \sum_{i=1}^{n} p_i \cdot s_i$$ maximize for minimal packet count

$$q_i := \frac{sizeof(P_i)}{s_{pkt}(P_i)}$$

$$f_2 = \sum_{i=1}^{n} p_i \cdot q_i$$ minimize for small overhead

#bits required to
transfer 1 covert bit

# Low-attention Forwarding using Covert Channel Proxies




- Shared Protocols between two proxies:

$$SP_{i,i+1} = P_i \cap P_{i+1}$$

- Provided Spaces for elements in SP:

$$S_{i,i+1} = \{s_{pkt}(p_1), s_{pkt}(p_2), \ldots, s_{pkt}(p_n)\}, p_1, \ldots, p_n \in SP$$

- Max. available space per protocol:

$$s_{max}(Q_i, Q_{i+1}) = max\, S_{i,i+1}$$

# Low-attention Forwarding using Covert Channel Proxies (2)

- **Goal:**
  - Transfer as few packets as possible to keep a low profile
- **Simple solution by using S and SP:**
  - IF $s_{max}(Q_i, Q_{i+1}) = s_{max}(Q_{i+1}, Q_{i+2})$ OR transaction complete THEN forward
  - ELSE
    - Forward as many packets of size $s_{max}(Q_{i+1}, Q_{i+2})$ as possible
    - cache remaining data
    - Wait time *t* for new data
      - IF no new data in interval *t* THEN forward remaining data
      - ELSE recursive call

# Summary

- We propose upgradeable and mobile covert channel software for overlay networks.
- Covert channel software should be capable of using different cover protocols for robustness (blocking) and mobility.
- Goal-dependent utilization of different protocols (small overhead or minimized attention)
- Optimize forwarding for multiple protocols within the covert channel overlay network → low attention

# Thank you for your attention!

Web: http://www.wendzel.de
Mail: STEFFEN @ PLOETNER-IT . DE

Are there any questions?

Image source: Amazon

# New Slide for the PDF Web Publication: Background Material

- Our publications serving as a base for this talk:
  - Wendzel, S., Keller J.: *Low-attention forwarding for mobile network covert channels*, In Proc. 12th IFIP CMS, Ghent, pp. 122-133, 2011.
  - Wendzel, S.: *The problem of traffic normalization within a covert channel's network environment learning phase*, In Proc. SICHERHEIT, 2012. (*to appear*)
  - Rist, T., Wendzel, S., Masoodian, M., Monigatti, P., André, E.: *Creating Awareness for Efficient Energy Use in Smart Homes*, In Proc. Intelligent Wohnen. Zusammenfassung der Beiträge zum Usability Day IX, pp. 162-168, 2011.