Novel Approaches for Network Covert Storage Channels

Steffen Wendzel

FernUniversität in Hagen, Germany

Verteidigung, 7. Mai 2013

Definition

Verdeckte Kanäle (*Covert Channels*).

Ursprüngliche Sicht

- Nicht vorgesehen im System
- Policy-brechend

Netzwerksicht

- **Versteckt**
- Policy-brechend

Timing Channels und *Storage Channels*

Definition

Verdeckte Kanäle (*Covert Channels*).

Ursprüngliche Sicht

- Nicht vorgesehen im System
- Policy-brechend

Netzwerksicht

- **Versteckt**
- Policy-brechend

Timing Channels und *Storage Channels*

Seitenkanal

- Verdeckter Kanal ohne beabsichtigtes Senden

Leistungen dieser Arbeit

Verdeckte Kanäle in der Gebäude-Automation

- erstmals das **Schadpotential** verdeckter Kanäle in Gebäuden entdeckt
- die **ersten drei Maßnahmen** gegen verdeckte Kanäle in Gebäuden entwickelt

Leistungen dieser Arbeit

Verdeckte Kanäle in der Gebäude-Automation

- erstmals das **Schadpotential** verdeckter Kanäle in Gebäuden entdeckt
- die **ersten drei Maßnahmen** gegen verdeckte Kanäle in Gebäuden entwickelt

Verdeckte Kanäle verbessern, bevor es Angreifer tun → Vorsprung sichern!

- bestehende **Terminologie verfeinert**
- **Feature-Reichtum** gesteigert
- **Verdecktheit** der Kanäle verbessert

Leistungen dieser Arbeit

Protokollwechselnde Kanäle können nicht völlig verhindert werden

- **Potential** der Kanäle erkannt
- Den **ersten Ansatz zur Begrenzung** der Bitrate dieser Kanäle entwickelt

Verdeckte Kanäle in der Gebäude-Automation

Gebäude-Automation

Gebäude-Automation

- Steuerung eines Gebäudes mithilfe von Sensoren, Aktoren und Controllern
- Netzwerke, verbunden mit dem Internet
- Eigene Protokoll-Standards
- Sehr unterschiedliche Konzepte (zentral/dezentral, Funk/Kabel, ...)

Gebäude-Automationssysteme sind sehr schlecht gesichert (Telnet zum Teil noch Standard für Remote-Zugriff).
Bspw. ist das **Öffnen von Türen** möglich!

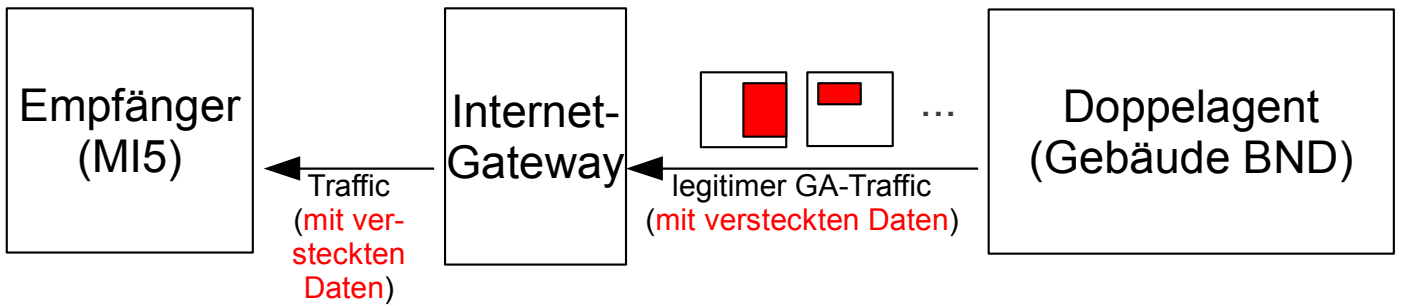
Gebäude-Automation

Fast jegliche Kommunikation ist erlaubt!

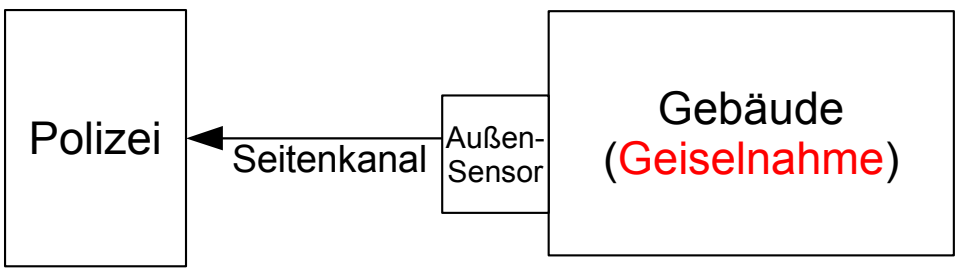
... was zu Sicherheitsproblemen führen kann.

Was passieren kann ...

Verdeckter Kanal:



Seitenkanal:



Kein Hack der Gebäudetechnik notwendig, da Außenkabel direkt verwendet werden können.

Absicherung der Gebäude-Automation

Zwei Methoden entwickelt

1. Middleware-Lösung
   - Software (Apps) greift nur über Middleware-Schnittstelle auf Gebäude zu
   - Middleware-Lösungen sind typisch zur Herstellung von Interoperabilität
   - Verhinderung verdeckter Kanäle und Seitenkanäle für Apps
2. Restrukturierung eines Gebäude-Netzes
   - Verhinderung verdeckter Kanäle und Seitenkanäle auf Protokollebene

Absicherung der Gebäude-Automation

Restrukturierung eines Gebäude-Netzes

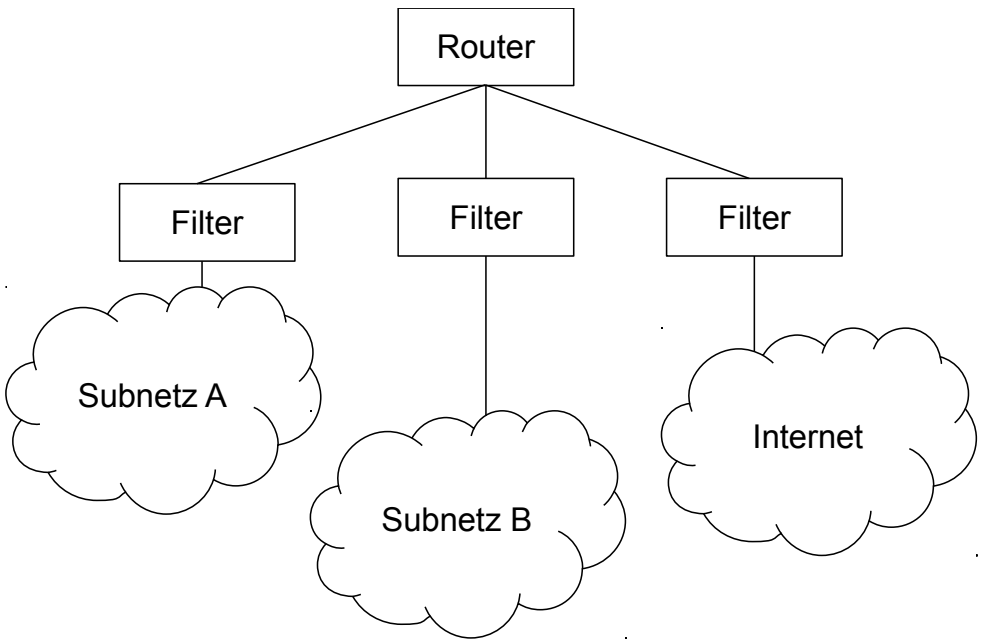
Building Automation Control Network Protocol Suite

- International verbreiteter ISO-Standard für Gebäude-Automation
- Inter-operabilität von Geräten verschiedener Hersteller
  - 651 Hersteller, davon 71 in Deutschland
- Verwendung von 4 OSI-Schichten; beinhaltet diverse Protokolle

Absicherung der Gebäude-Automation

Restrukturierung eines Gebäude-Netzes

- Policy-brechende Kommunikation verhindern:
  - Subnetze mit Geräten homogener Rechte
  - Subnetz-interne Kommunikation immer erlaubt
  - Subnetz-überschreitende Kommunikation nur über Filter
- *Beispiel: Exfiltration von Daten in öffentliches Netz*

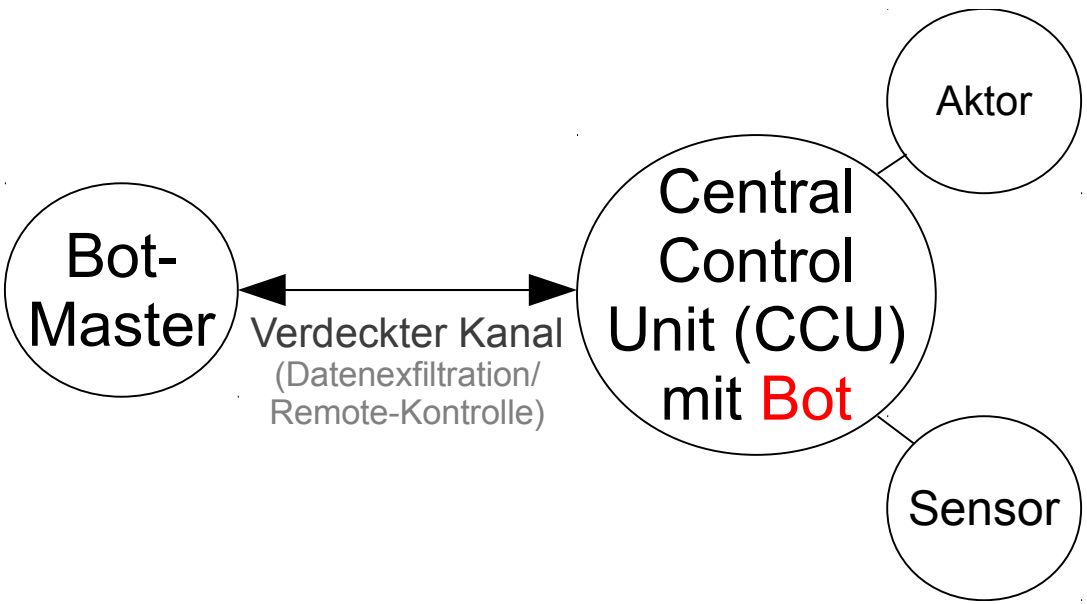


Weitere Szenarien sind denkbar.

Eines davon sind Botnetze

Szenario: Botnetz im Gebäude

Beispiel: Hack der Centrol Control Unit (CCU) einer Gebäude-Automation:



Ein Botnetz kann über die Gebäudetechnik Events/Personen überwachen und das Gebäude fernsteuern!

Botnetze der Zukunft

Weiter gedacht:

1. Wir müssen zukünftige Botnetz-Techniken verstehen, *bevor* sie *ohne unser Wissen* zum Einsatz kommen!
2. Covert Channels sind ein Dual-Use-Gut!
   → Bei Risiko einer Inhaftierung oder gar Tod [HBS13]

- Insbesondere im Internet verbreitet

Daher:

- Einführung neuer Features
- Verbesserung der Verdecktheit

Botnetze der Zukunft

Weiter gedacht:

1. Wir müssen zukünftige Botnetz-Techniken verstehen, *bevor* sie *ohne unser Wissen* zum Einsatz kommen!
2. Covert Channels sind ein Dual-Use-Gut!
   → Bei Risiko einer Inhaftierung oder gar Tod [HBS13]

- Insbesondere im Internet verbreitet

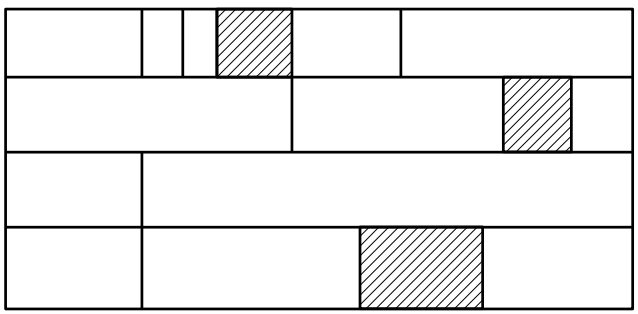
Daher:

- Einführung neuer Features
- Verbesserung der Verdecktheit

Lösung?

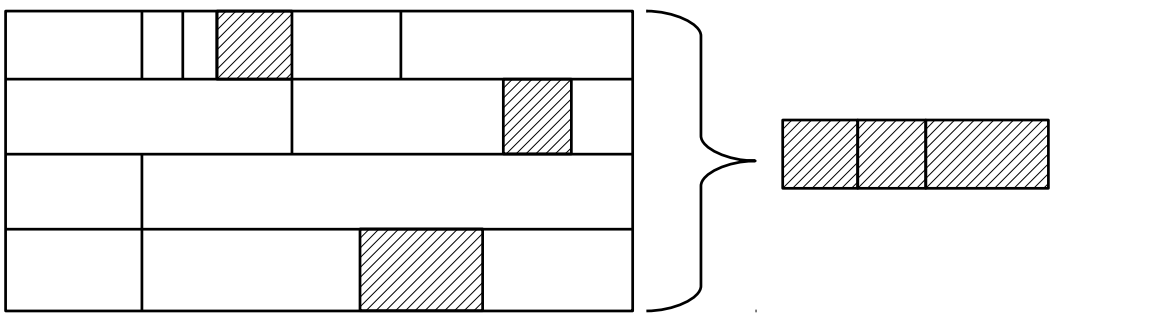
Terminologie

Feinere Terminologie, denn "Protocol" ist ungenau!



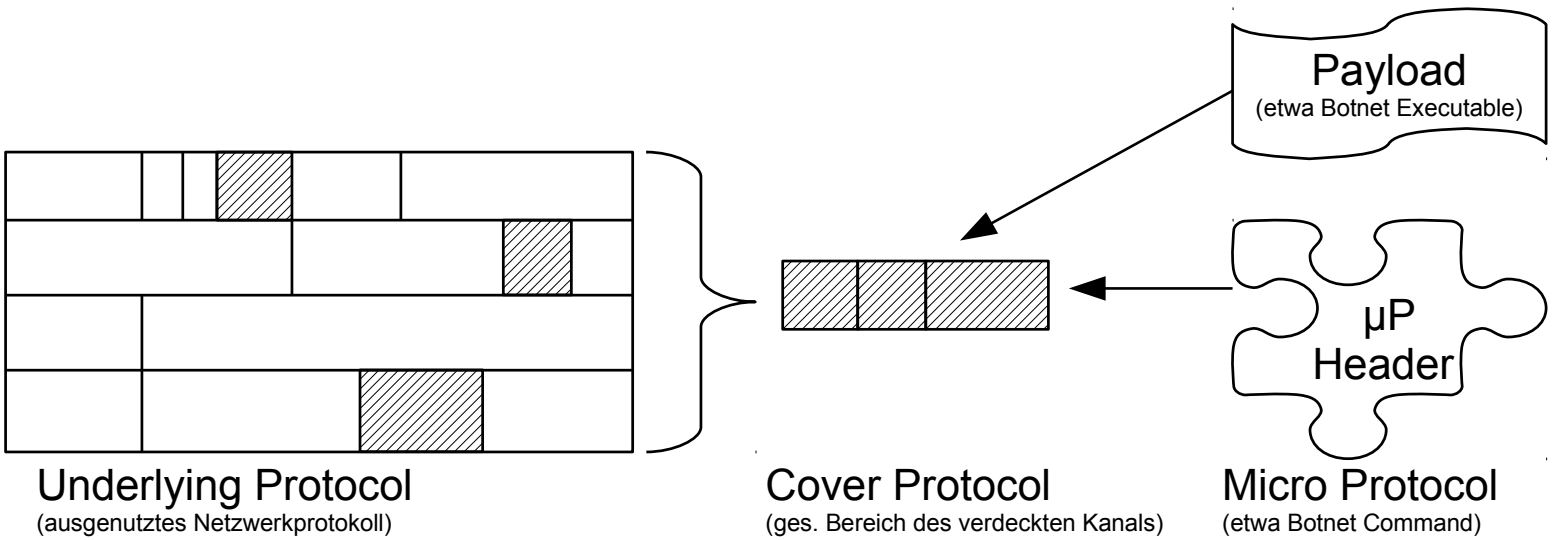
Terminologie

Feinere Terminologie, denn "Protocol" ist ungenau!



Terminologie

Feinere Terminologie, denn "Protocol" ist ungenau!



Micro Protocol

Ein Micro Protocol besteht aus einem Header. Es steuert den verdeckten Kanal und spezifiziert den Payload.

Kanal-interne Protokolle (Mikroprotokolle)

Wozu Mikroprotokolle? – Was geht nicht ohne Mikroprotokoll?

- Mobile (Bot-)Overlay-Netze (Zugriff mit verschiedenen Techniken)
- Robustheit/Reliability [RM08]
- Dynamisches Routing (zwischen Bots)
- Schrittweise Infrastruktur-Upgrades (Bot-Software aktualisieren)
- ...

Stand der Forschung

Erste Mikroprotokolle existieren:

- Statischer Header (keine dynamischen Felder) [RM08,Sto09]
- Nicht oder nur wenig für verdeckte Kommunikation geeignet

Stand der Forschung

Erste Mikroprotokolle existieren:

- Statischer Header (keine dynamischen Felder) [RM08,Sto09]
- Nicht oder nur wenig für verdeckte Kommunikation geeignet

Daher: Einführung von Ansätzen zur Optimierung

- *Status Updates*: Minimale Aufmerksamkeit durch Platzeinsparung → bestehendes Forschungsprotokoll effizienter gestaltet
- *Konformitäts-Ansatz*: Minimale Aufmerksamkeit durch konformes Verhalten

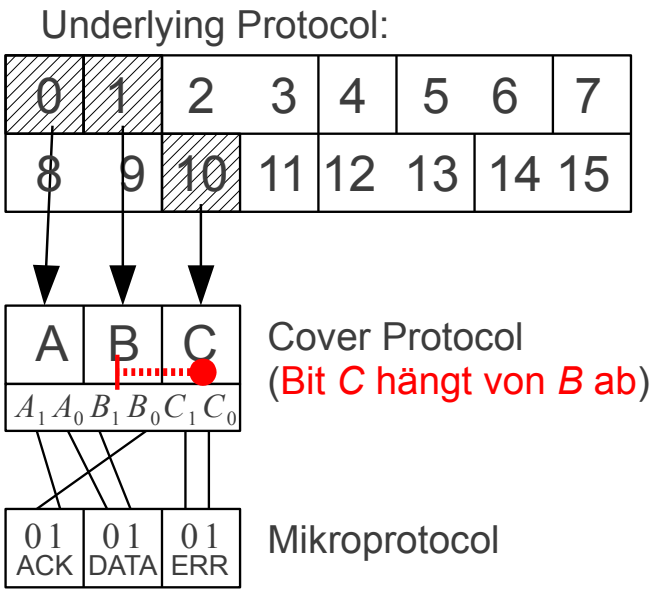
Anforderungen an Mikroprotokolle

Konformitäts-Ansatz:

- Minimale Aufmerksamkeit erzeugen:
  - Konformität zum Verhalten des Underlying Protocols
  - Angepasste Auftrittswahrscheinlichkeiten von Bits
- Anwendbarkeit für alle binären Underlying Protocols
- Praxistauglichkeit
- Klare Anwendung der verbesserten Terminologie
- Output sollte ein μP sein, das implementiert werden kann
- μP sollte dynamisch re-designed bzw. optimiert werden können
- Support für verbindungsorientierte Protokolle

Konformitäts-Ansatz

Vorbereitungsarbeiten:



- Cover Protocol und Mikroprotokoll definieren
- sizeof(μP) $\leq$ sizeof(Cover Prot.)
- Bitmapping: 1er/0er-Bits unterschiedlich behandelt; Auftrittswahrscheinlichkeiten hängen von Protokollstatus (etwa *Verbindungsaufbau*) ab

Konformitäts-Ansatz

Konformitätstest:

L(μP):	**L(CP):**
A	A
AB	AB
AC	
ABC	ABC

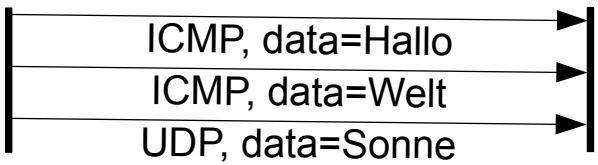
- Modellierung von zwei Grammatiken (Mikroprotokoll und Cover Protocol) mit gleichen Terminalsymbolen für gleiche Bitwerte
- Sprachinklusion: Test nur dann automatisch möglich, wenn Grammatik des μP regulär oder kontext-frei ist und Grammatik des Cover Protocols regulär ist.
- *Ähnlicher Ansatz:* Implementierungsfehler [HBS13]
  $\rightarrow$ Unser Ansatz kann es bereits!

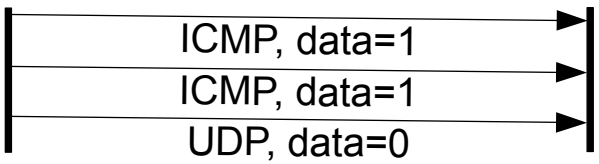
Wir wechseln zur Verteidiger-Seite:

Bitraten-Begrenzung protokollwechselnder Kanäle

Protokollwechselnde Kanäle

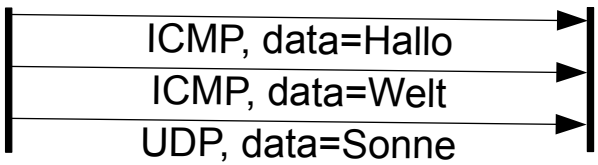
Protocol Hopping Covert Channel bzw. *Protocol Channel*:

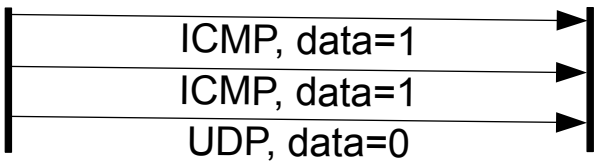




Protokollwechselnde Kanäle

Protocol Hopping Covert Channel bzw. *Protocol Channel*:





Wir kennen noch kein Gegenmittel!

- Anpassungsfähig für Änderungen der Netzwerkkonfiguration (nur Protocol *Hopping Covert* Channels *mit Mikroprotokollen*)
- Forensische Traffic-Analyse wird erschwert

Lösungsansatz:

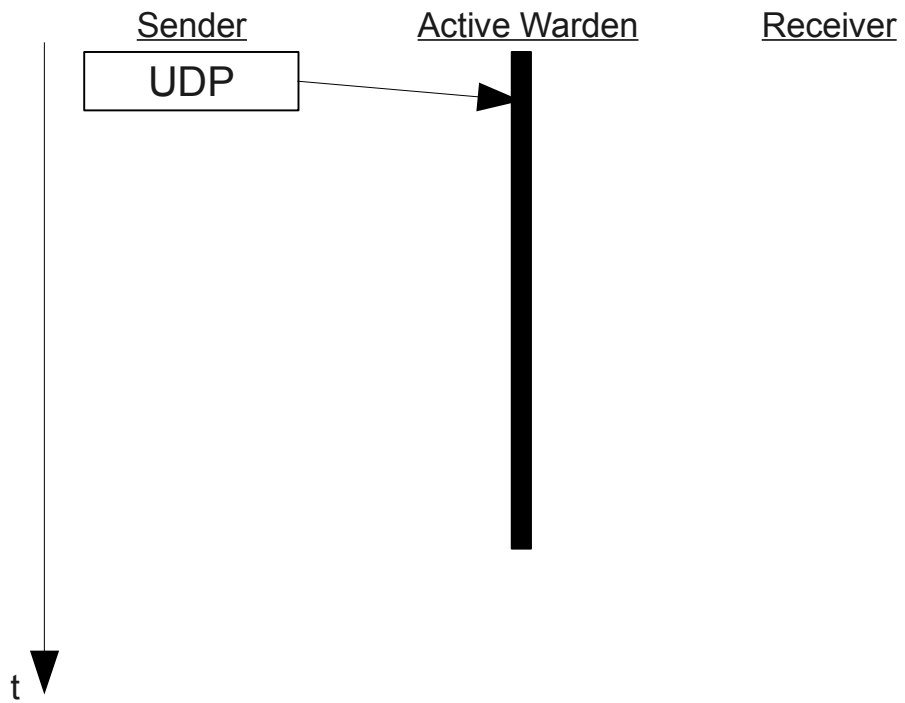
- Protocol Channels und Protocol Hopping Covert Channels benötigen *Protokollwechsel*
- **Protokollwechsel müssen immer stattfinden**, weshalb wir die Kanäle nicht verhindern können.
- **Aber:** Wir können Protokollwechsel verzögern! → Bitrate des Kanals limitieren
- Verzögerung konfigurierbar → Limitierung konfigurierbar

Beispiel:

- Protocol Channel mit ICMP (1) und UDP (0)
- Übertragung der Nachricht “01100”

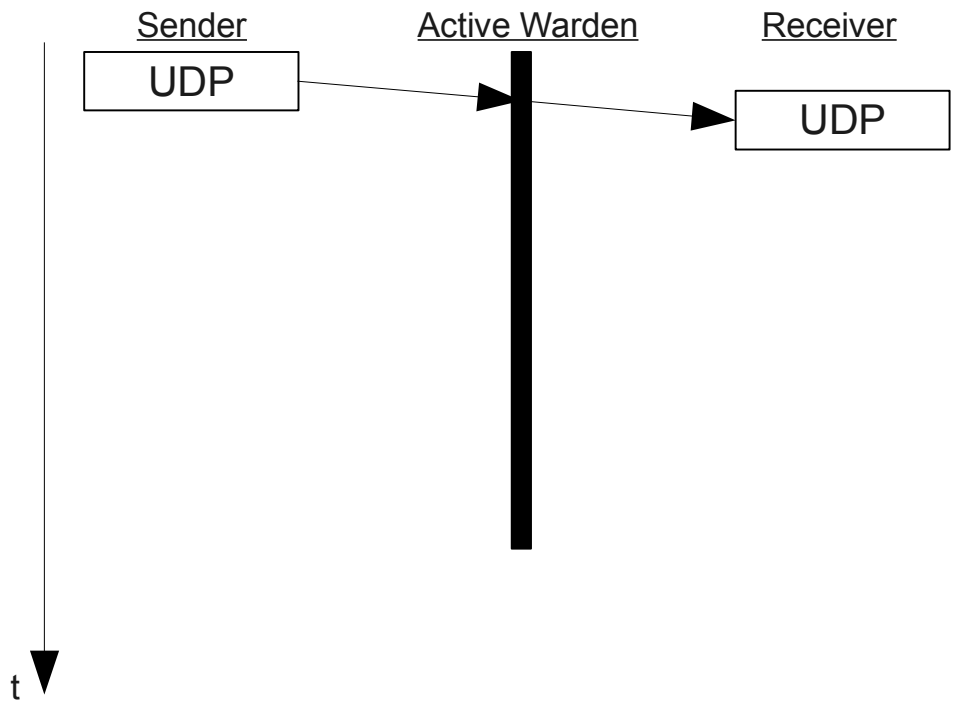
Beispiel:

- Protocol Channel mit ICMP (1) und UDP (0)
- Übertragung der Nachricht “01100”



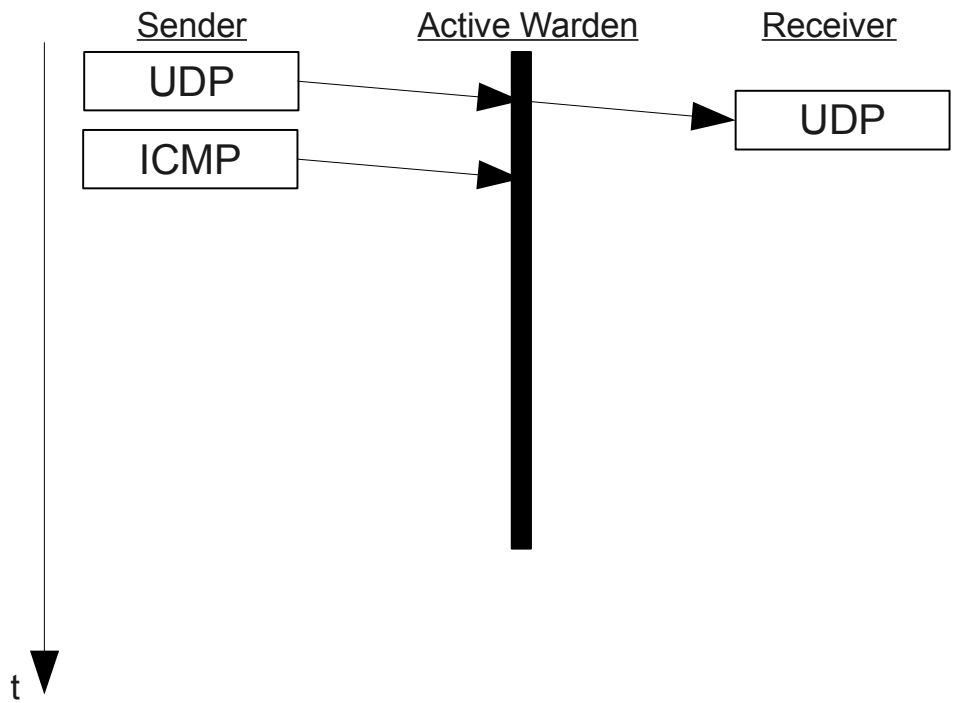
Beispiel:

- Protocol Channel mit ICMP (1) und UDP (0)
- Übertragung der Nachricht “01100”



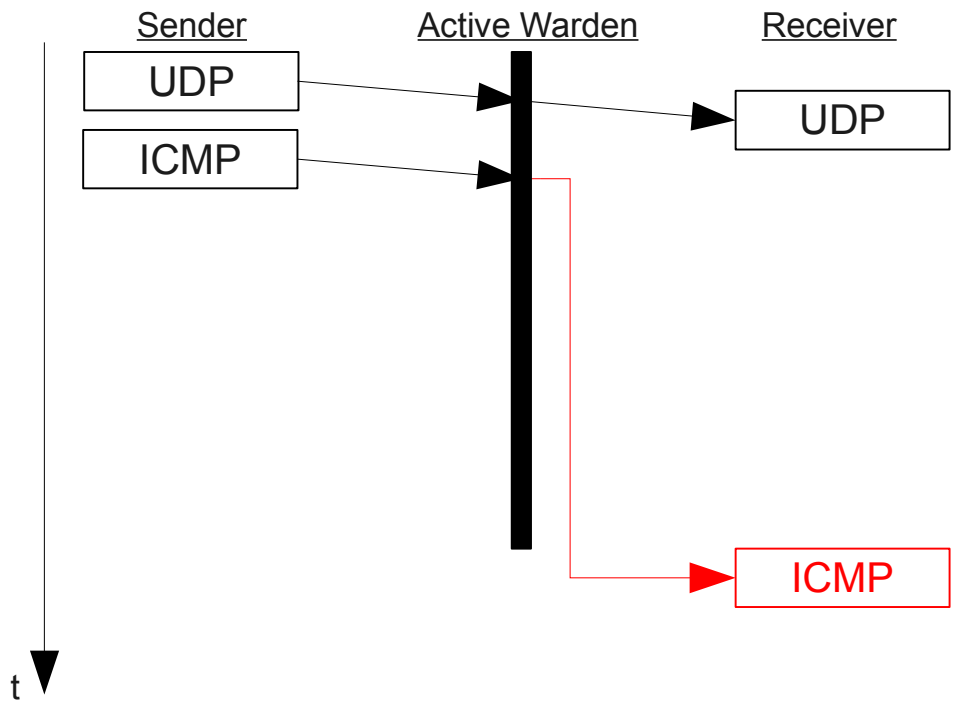
Beispiel:

- Protocol Channel mit ICMP (1) und UDP (0)
- Übertragung der Nachricht “01100”



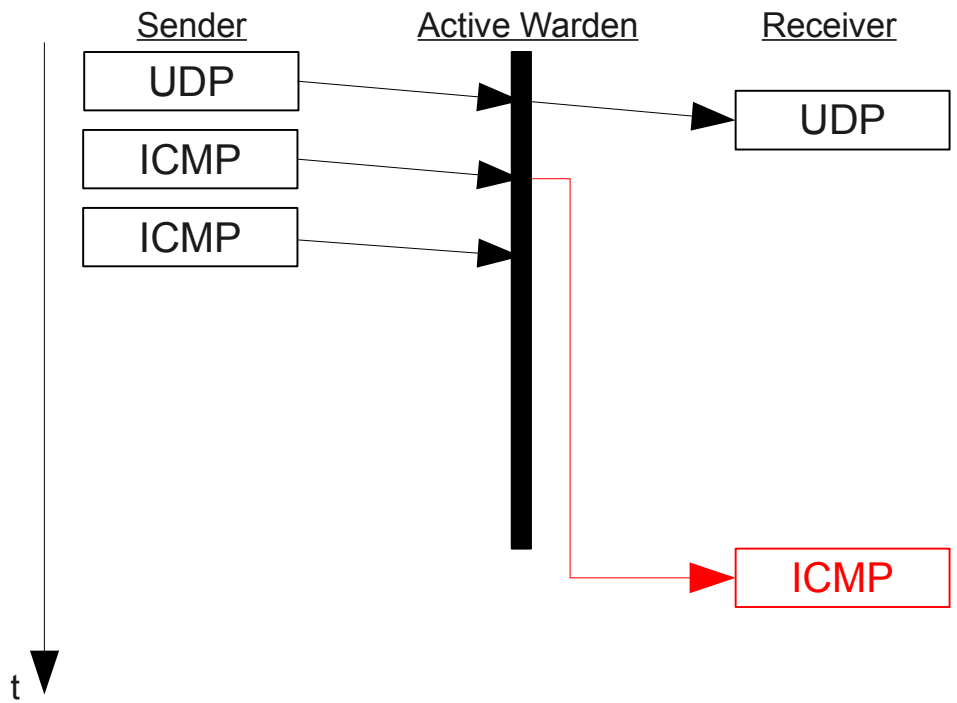
Beispiel:

- Protocol Channel mit ICMP (1) und UDP (0)
- Übertragung der Nachricht “01100”



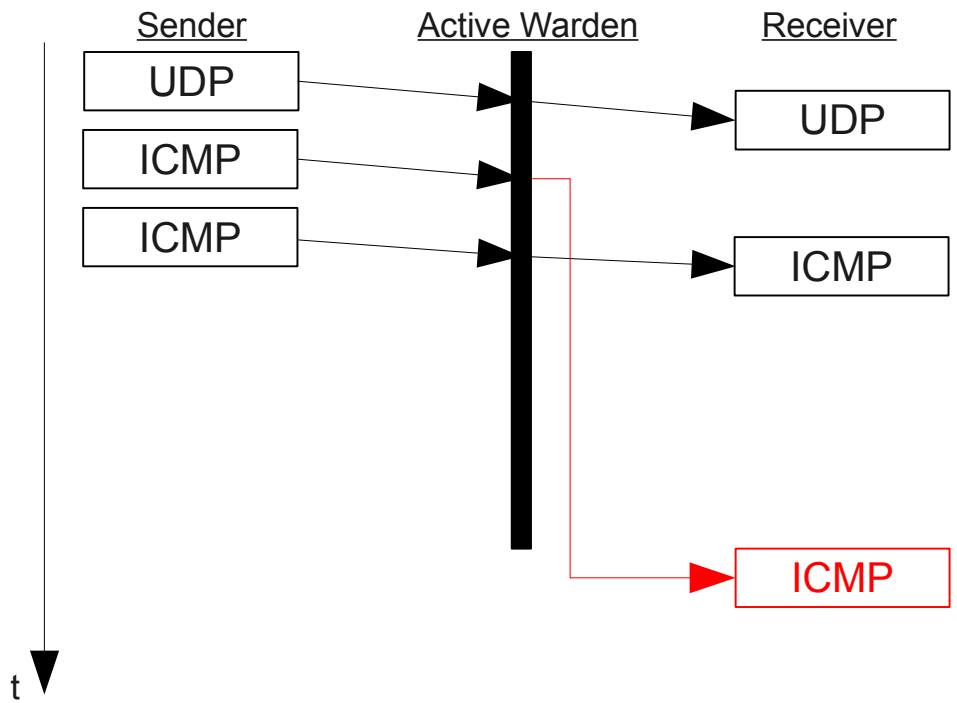
Beispiel:

- Protocol Channel mit ICMP (1) und UDP (0)
- Übertragung der Nachricht “01100”



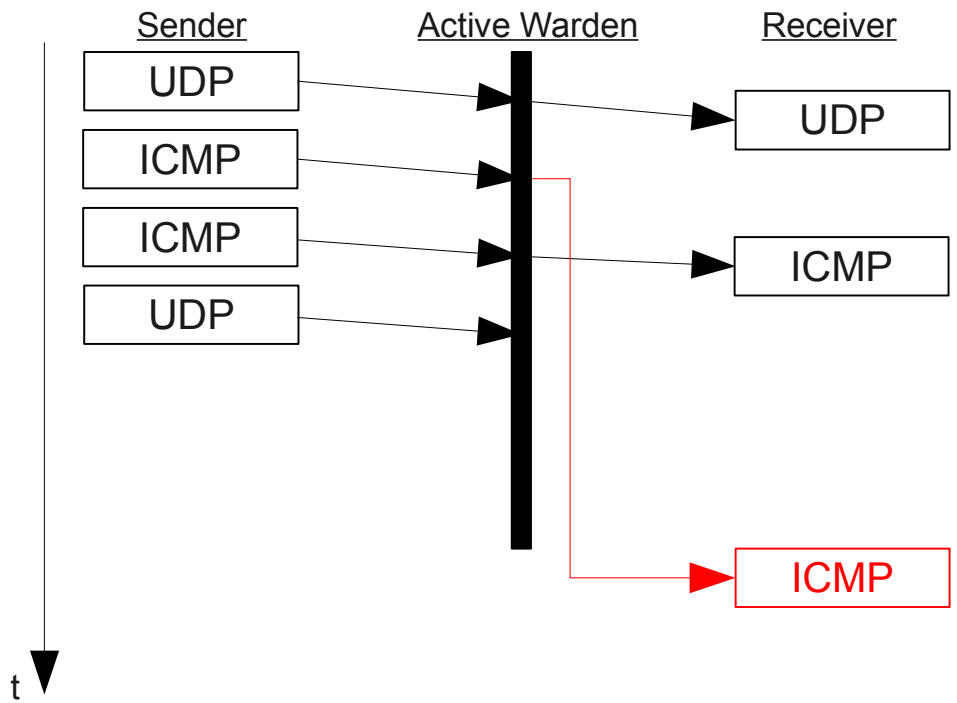
Beispiel:

- Protocol Channel mit ICMP (1) und UDP (0)
- Übertragung der Nachricht “01100”



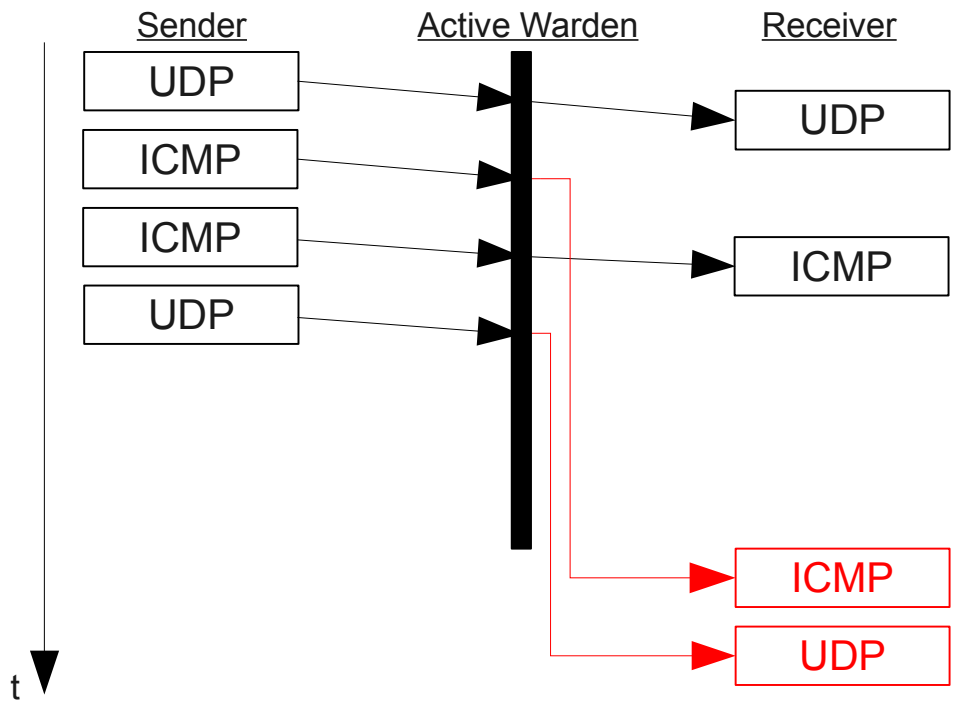
Beispiel:

- Protocol Channel mit ICMP (1) und UDP (0)
- Übertragung der Nachricht “01100”



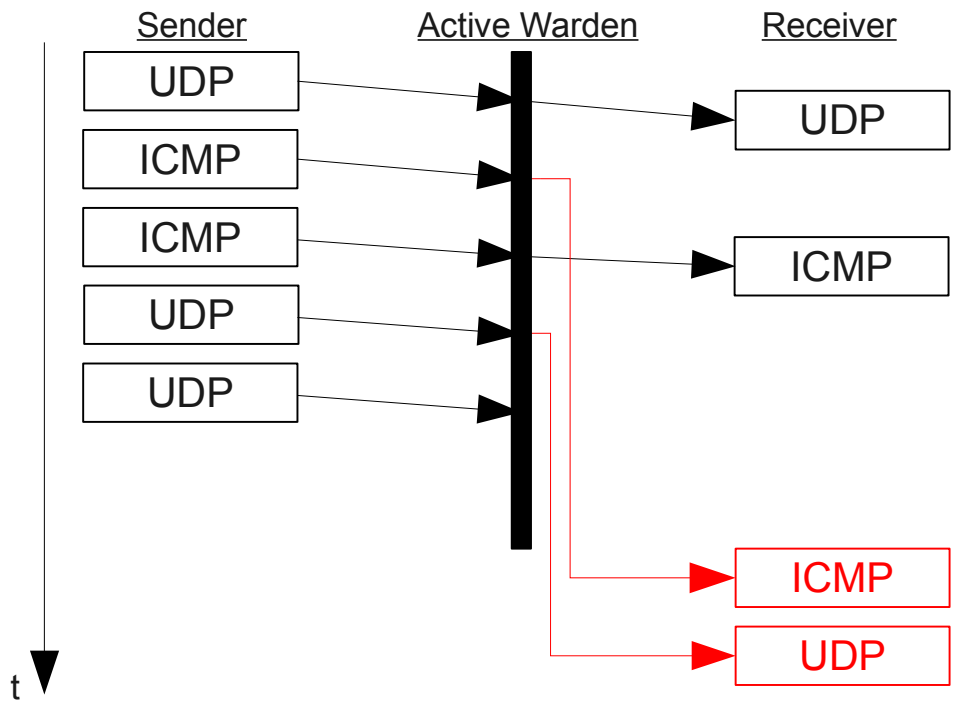
Beispiel:

- Protocol Channel mit ICMP (1) und UDP (0)
- Übertragung der Nachricht “01100”



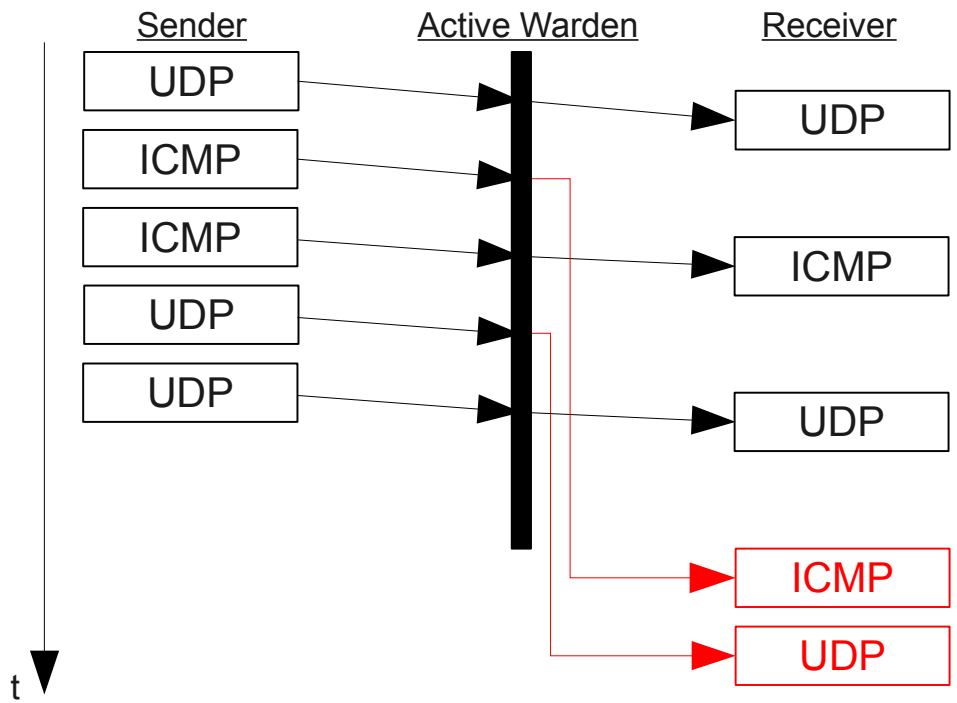
Beispiel:

- Protocol Channel mit ICMP (1) und UDP (0)
- Übertragung der Nachricht “01100”



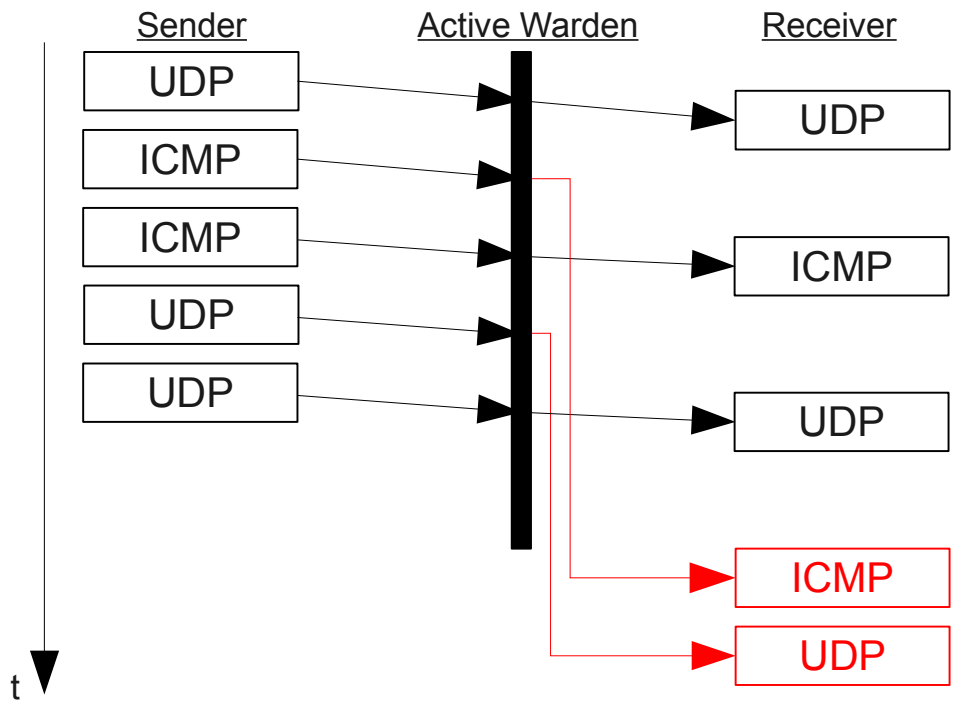
Beispiel:

- Protocol Channel mit ICMP (1) und UDP (0)
- Übertragung der Nachricht “01100”



Beispiel:

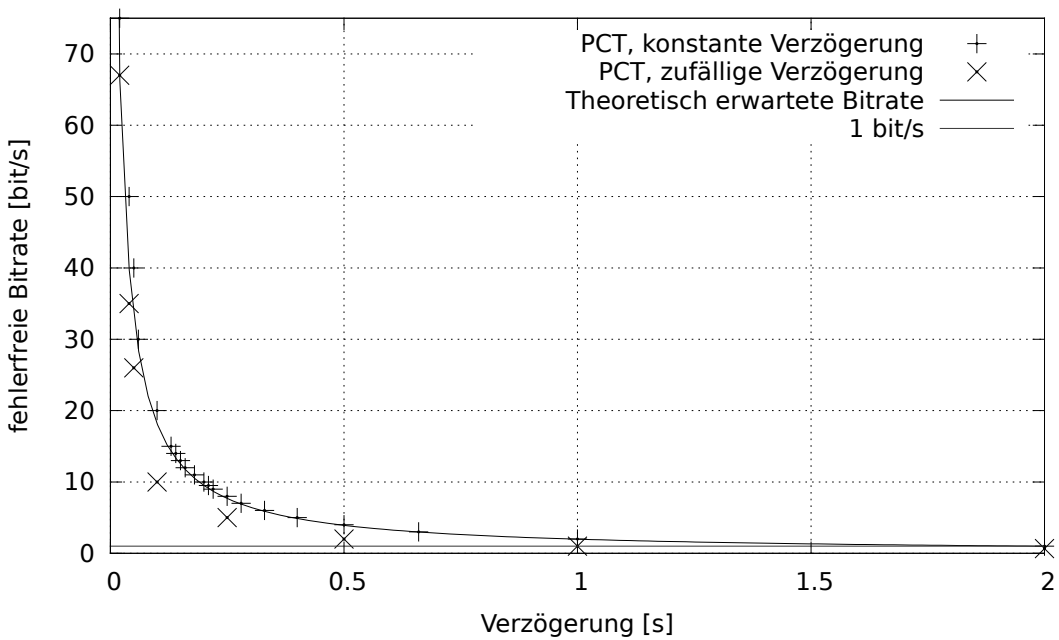
- Protocol Channel mit ICMP (1) und UDP (0)
- Übertragung der Nachricht “01100”



- Empfangene Nachricht: “01**01**0”

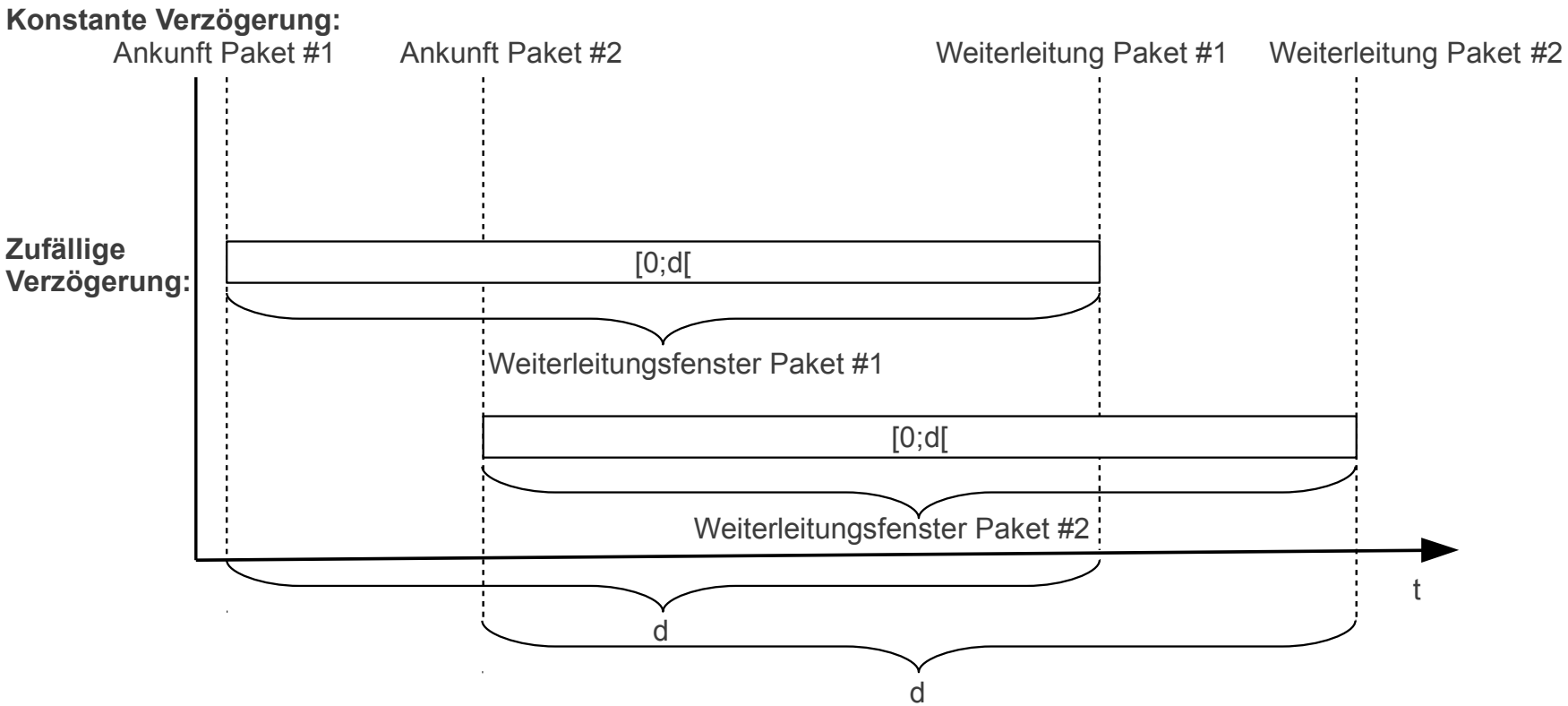
Resultate

- Abhängig von Kanaltyp, Anzahl der Protokolle, Kodierung, Verzögerung und Transferzeit
- Beispielresultat:



Konstanter und zufälliger Verzögerung

- Zufällige Verzögerung ist effektiver, denn:



Anwendbarkeit in der Praxis

- Bei jeglichem Protokollwechsel
- Getestet für Protocol Channel (UDP/ICMP)
- Getestet für Protocol Hopping Covert Channel (versch. Anwendungsprotokolle)
- Getestet für Protocol Channel in BACnet
  - Anwendbar in der Gebäude-Automation
- Verzögert Peer Discovery-Phase (*Network Environment Learning Phase*)

Anwendbarkeit in der Praxis

- Verzögerung sind selten und gering:
  - Verzögerung *ausschließlich* bei Protokollwechsel
  - Verzögerung von 1 s resultiert für PC mit 2 Protokollen bereits in einer Bitrate von 1 bit/s
- Verzögerungen und Vertauschungen der Paketreihenfolgen sind üblich
- Whitelisting für erlaubte Protokollwechsel zu entsprechenden IPs (etwa DNS zum Nameserver mit anschließendem $\rightarrow$ HTTP(S))
- Problematisch: Mikroprotokolle mit Sequenznummern $\rightarrow$ Zwang zur Nutzung bei PHCC

Zusammenfassung

Zusammenfassung (1/2)

Verdeckte Kanäle in der Gebäude-Automation

- Schadpotential wurde zuvor nicht erkannt
- Die ersten drei Protektionsmaßnahmen eingeführt

Zusammenfassung (1/2)

Verdeckte Kanäle in der Gebäude-Automation

- Schadpotential wurde zuvor nicht erkannt
- Die ersten drei Protektionsmaßnahmen eingeführt

Mikroprotokolle

- Terminologie verfeinert
- Mikroprotokolle hinsichtlich ihrer Versteckheit verbessert:
  - Konformitäts-Ansatz
  - Minimierung der Headergröße

Zusammenfassung (2/2)

Verdeckte Kanäle mit Protokollwechsel-Funktion

- U.a. für Botnets der Zukunft hochgradig nützlich
- Den ersten Ansatz zur Limitierung entwickelt
- Für BACnet getestet und somit in Gebäude-Automation anwendbar

Ich danke Ihnen für Ihre Aufmerksamkeit!

Quellen

HBS13 A. Houmansadr, C. Brubaker, V. Shmatikov: *The Parrot is Dead: Observing Unobservable Network Communications*, In: IEEE S&P 2013, IEEE, 2013 *(to appear)*.

RM08 Ray, B., Mishra, S.: *A protocol for building secure and reliable covert channel*. In: PST 2008, IEEE, pp. 246-253, 2008.

Sto09 Stødle, D.: *Ping tunnel – for those times when everything else is blocked*, verfügbar unter: *http://www.cs.uit.no/~daniels/PingTunnel/*, 2009.