INTERNET CENSORSHIP
PART II: INFORMATION HIDING

CH. 4: INTRODUCTION TO NETWORK INFORMATION HIDING

Prof. Dr. Steffen Wendzel
https://www.wendzel.de

Definition

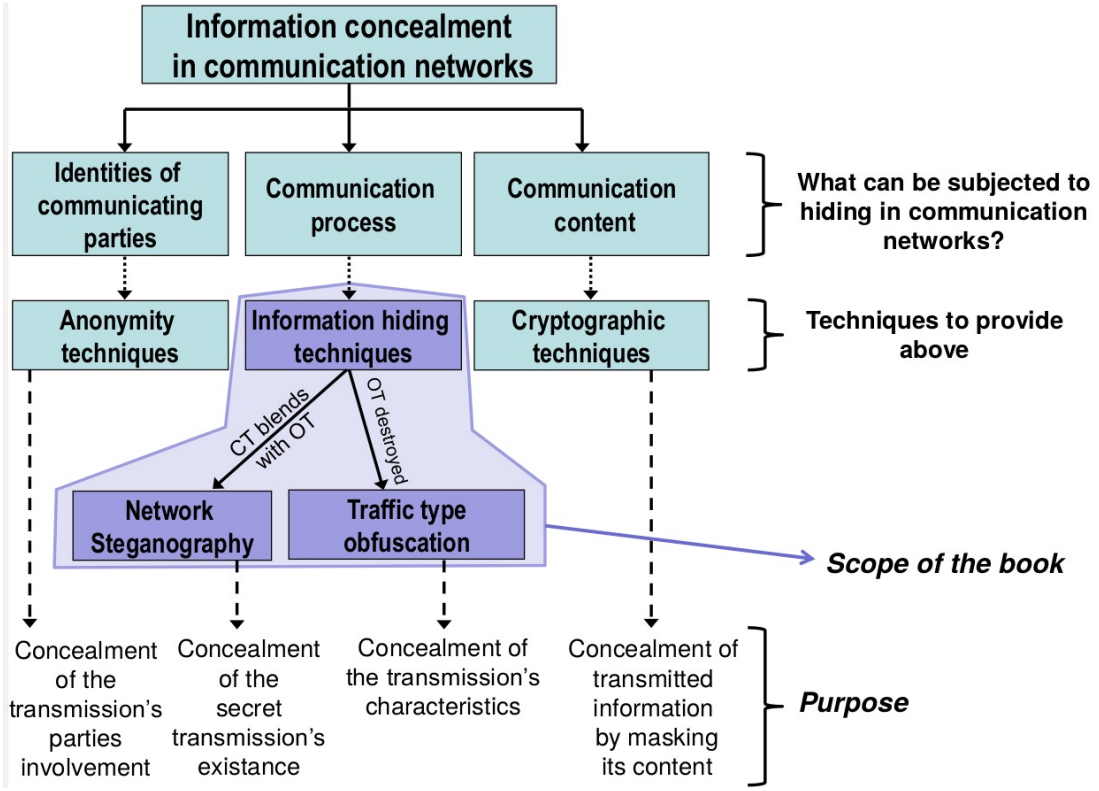


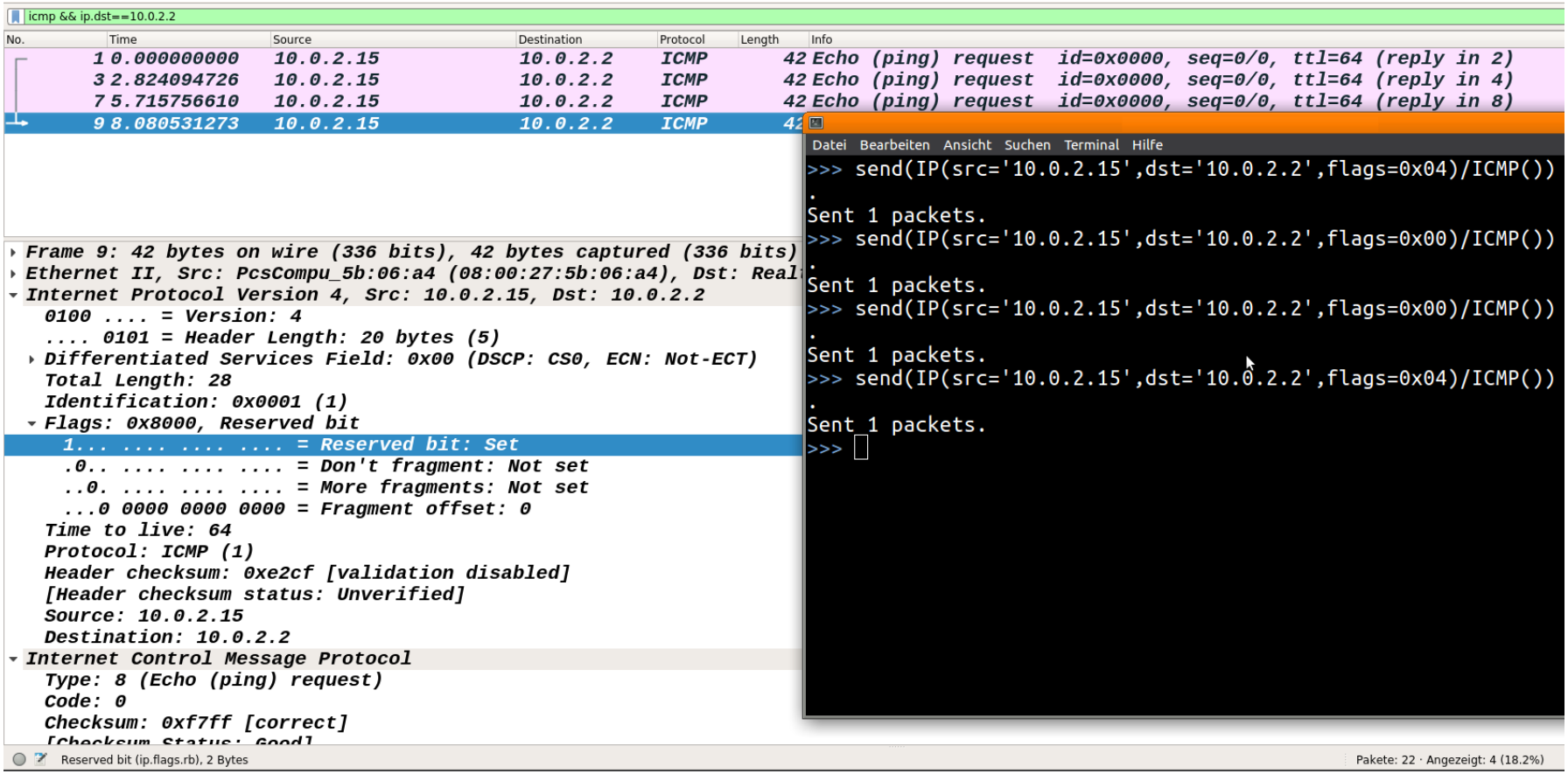
Fig.: W. Mazurczyk, S. Wendzel, S. Zander et al.: Information Hiding in Communication Networks, Wiley-IEEE, 2016

Differences to traditional digital media steganography

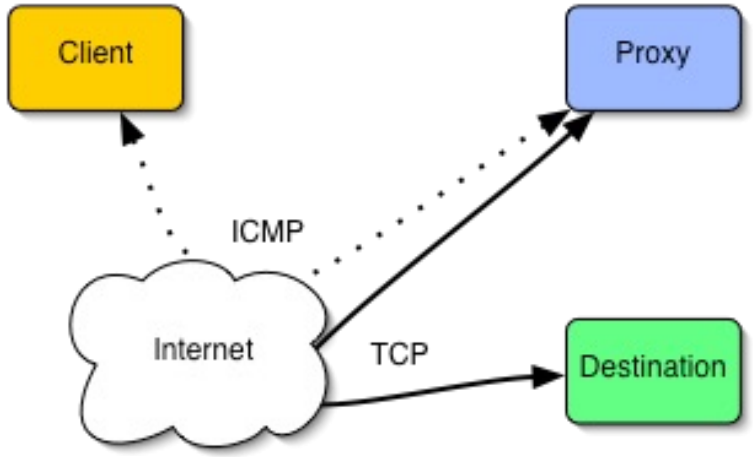
- **Inconsistent terminology**: no clear distinction between **steganography** and **covert channel**
  - See Ch. 1 for definitions of the terms steganography and covert channel and that both are considered as different research domains (covert channels in MLS context!).
  - Thus, in the network context: **network covert channel** or **network steganographic channel** handled **separately**
  - Unified: a steganographic **method** creates such a **covert channel** [1, Chapter 3]
- A bit more terminology:
  - Covert data is hidden in *overt* network transmissions
  - The „cover object“ is now called „carrier“ in the network context
  - Advantage of a constant transmission (e.g. permanent data leakage)
- Advantages:
  - Difficult to analyze **all** network data; smaller delay; with the growth of the Internet, the options for network IH grew and grow, too.

[1] W. Mazurczyk, S. Wendzel, S. Zander et al.: Information Hiding in Communication Networks, Wiley-IEEE, 2016

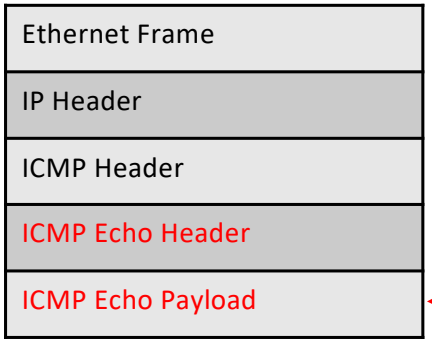
Example 1: Trivial Network Covert Channel via IPv4 Reserved Bit, sending message ``1001”



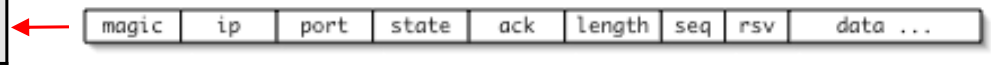
Example 2: Ping Tunnel



Analysis and improvements:
Jaspreet Kaur, Steffen Wendzel, Omar Eissa, Jernej Tonejc, Michael Meier: Covert Channel-internal Control Protocols: Attacks and Defense, *Security and Communication Networks (SCN)*, Vol. 9(15), Wiley, 2016.



Secret data is embedded into the ICMP echo payload.
In addition, a small protocol of the following format is used:



Figs.: http://www.cs.uit.no/%7Edaniels/PingTunnel/

Types of (Network) Covert Channels

- **Fundamental:**
  - **Local** and **network** covert channels
  - **Storage** and **timing** channels
  - **Noisy** and **noise-free** covert channels
  - **Direct** and **indirect** covert channels
  - **Intentional** and **unintentional** covert channels

Types of (Network) Covert Channels: Storage/Timing Cov. Channels

- Modulate **stored** information or modulate **timing** behavior

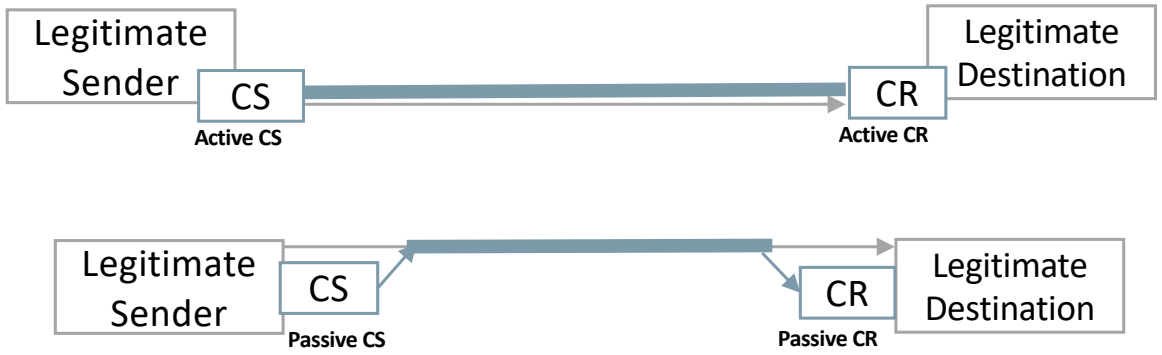
- Storage and timing are the two major categories for categorizing storage channels.

- Flawed, as we have shown in [1].
  - Example: some covert channels modify the order of network packets, such as TCP segments, which would be both, a timing operation (when to send which packet) as well as a storage operation (sequence numbers in packet headers must be written and are also interpreted by the covert channel).

[1] S. Wendzel et al.: A Generic Taxonomy for Steganography Methods, ACM Computing Surveys, 2025.

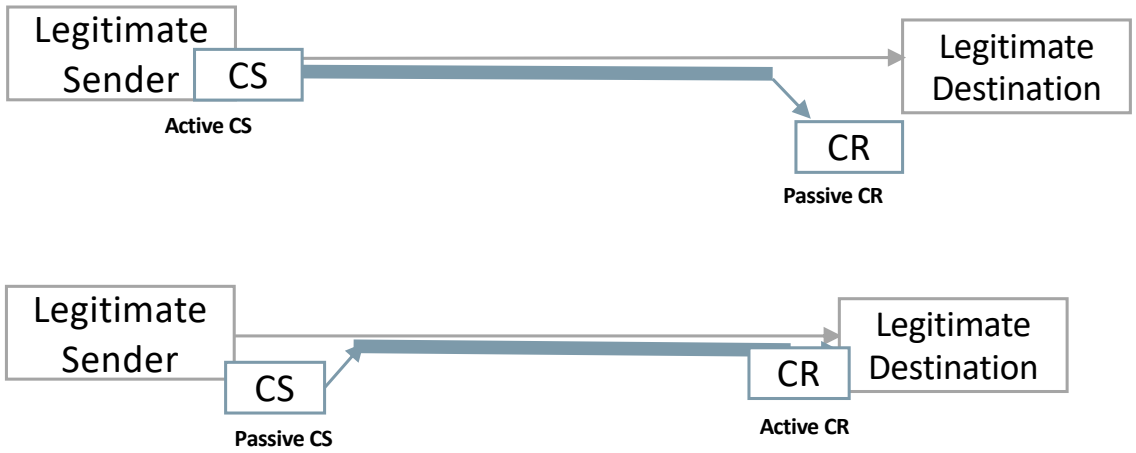
Types of (Network) Covert Channels: Active/Passive Cov. Channels

- **Active** and **passive** Covert Channels (passive elements have a different sender/receiver than the legitimate sender/receiver)



Types of (Network) Covert Channels: Semi-active/passive Cov. Channels

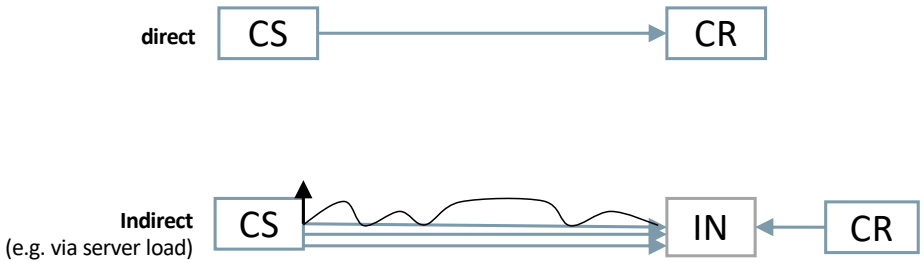
- **Semi-active** and **semi-passive** Covert Channels [1]
  - **Semi-active:**
  - **Semi-passive:**



[1] K. Lamshöft, J. Dittmann: *Assessment of Hidden Channel Attacks: Targetting Modbus/TCP*, IFAC-PapersOnLine, 53(2), 2020.

Types of (Network) Covert Channels: (In)Direct Cov. Channels

- **Direct** and **indirect** covert channels: direct channels do not rely on intermediate nodes (IN).
  - Example: via web page + server load
  - General illustration:



Further differentiation into two major patterns for the intermediate node (IN): **redirector** and **broker**.

- A broker can be a **proxy** or a **dead drop**.

⇒ **Survey:** T. Schmidbauer, S. Wendzel: *SoK A Survey of indirect network-level covert channels*, in Proc. 17th AsiaCCS, ACM, 2022. https://doi.org/10.1145/3488932.3517418

⇒ **Lets have a look into the paper and understand the patterns (broker (proxy; dead drop) and redirector.**

Types of (Network) Covert Channels: (In)Direct Cov. Channels – Case of Dead Drops with ARP [1]

- In general, **network** steganography can only be used to **transfer** secret data.
  - There are a few exceptions such as the Dead Drop (see Ch. 4).

- Illustration of the Dead Drop introduced in [1, text below is a copy from the paper]. Approach with ARP+SNMP (see Fig.):
  a) CS possesses secret information that it wants to store in the network-accessible ARP cache.
  b) CS exploits the ARP cache of a third-party system by sending a fake ARP request containing a (MAC,IP) tuple. The actual host reflected by the (MAC,IP) tuple does not exist and represents encoded secret information.
  c) The third-party host Dead Drop (D) adds the tuple to its local ARP cache …
  d) … where it can be requested by the CR for some time depending on the lifetime of ARP cache entries on the third-party host.

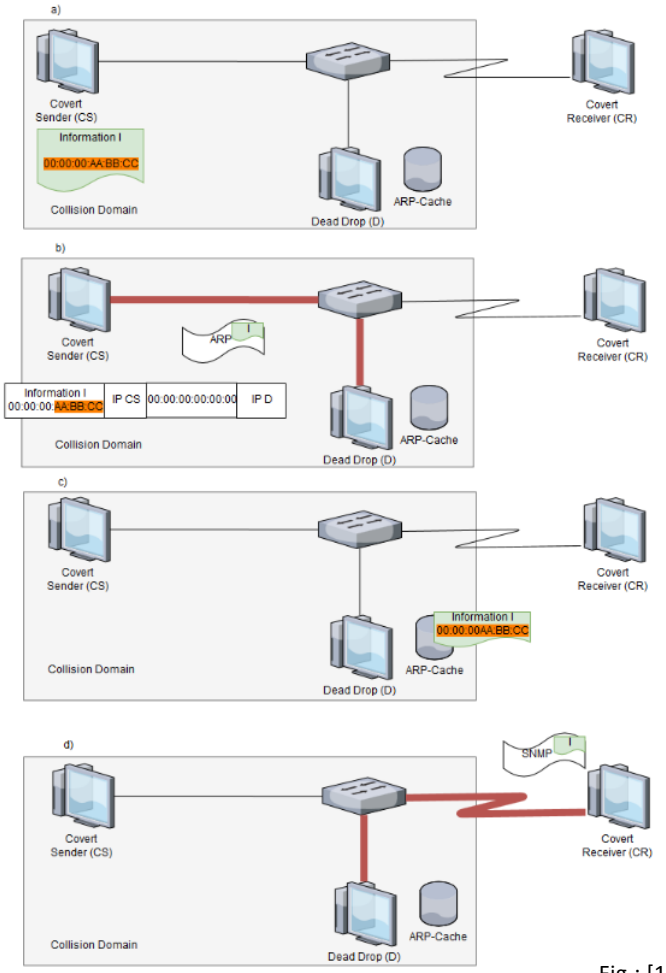


Fig.: [1]

[1] T. Schmidbauer, S. Wendzel, A. Mileva, W. Mazurczyk: Introducing Dead Drops to Network Steganography using ARP-Caches and SNMP-Walks, in Proc. ARES 2019, ACM.

Types of (Network) Covert Channels: (In)Direct Cov. Channels – Case of Dead Drops with ARP [1]

- Lifetime of entries depends on the system and caching limits (all Figures taken from [1]):

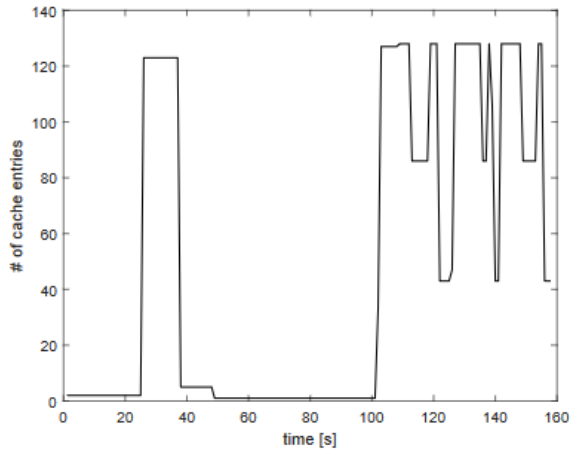


Figure 5: OpenSuSE caching behavior

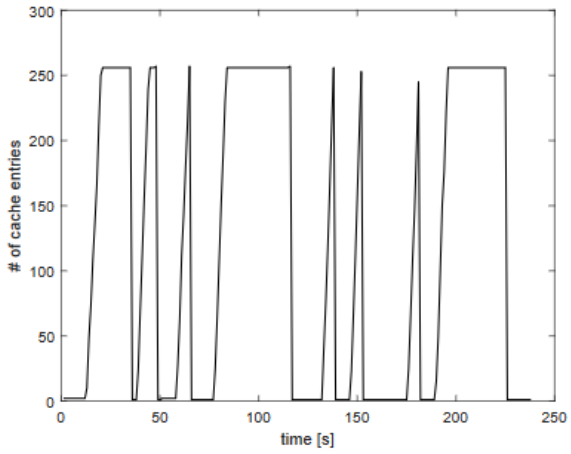


Figure 7: Windows 7 caching behavior

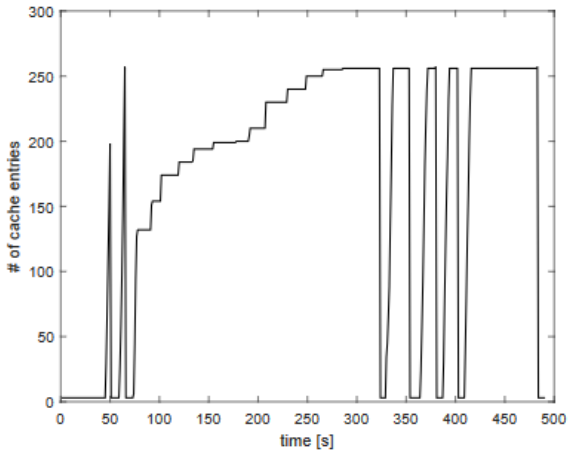


Figure 6: Windows 10 caching behavior

Figs.: [1]

[1] T. Schmidbauer, S. Wendzel, A. Mileva, W. Mazurczyk: Introducing Dead Drops to Network Steganography using ARP-Caches and SNMP-Walks, in Proc. ARES 2019, ACM.

Types of (Network) Covert Channels: (In)Direct Cov. Channels – Case of Dead Drops

- **Advantage** of Network Dead Drops: CS and CR can write/read the secret information at different times, raising fewer attention for their action.

- **Note:** Another approach is available (see a 2020-paper by Schmidbauer et al. that shows the exploitation of the NTP protocol for the purpose of creating a Dead Drop).

Types of (Network) Covert Channels: (Un)Intentional Cov. Channels

- **Intentional** (**covert**) and **unintentional** (**side**) channels
  - e.g. side channels in web applications [1]

  - Example:

Usually, traffic needs to be sent many times and measured exactly to gain any useful information out of this.

[1] S. Schinzel: An efficient mitigation method for timing side channels on the Web, in Proc. 2nd Int. Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE), 2011.

Types of (Network) Covert Channels: Cover Types

Zander categorizes covert channel carriers as follows:

- **Predictable**
- **Variable**
- **Random**

S. Zander: *Performance of Selected Noisy Covert Channels and Their Countermeasures in IP Networks*, PhD Thesis, Swinburn University of Technology, Melbourne, 2010.

History Covert Channels & Covert Channel Amplification

Institut für Organisation und Management von Informationssystemen

Types of (Network) Covert Channels: History Cov. Channels and Cov. Ch. Amplification [1]

- Most covert channels focus on the **present**, e.g., packets might contain secret stego data in their **current** payload.

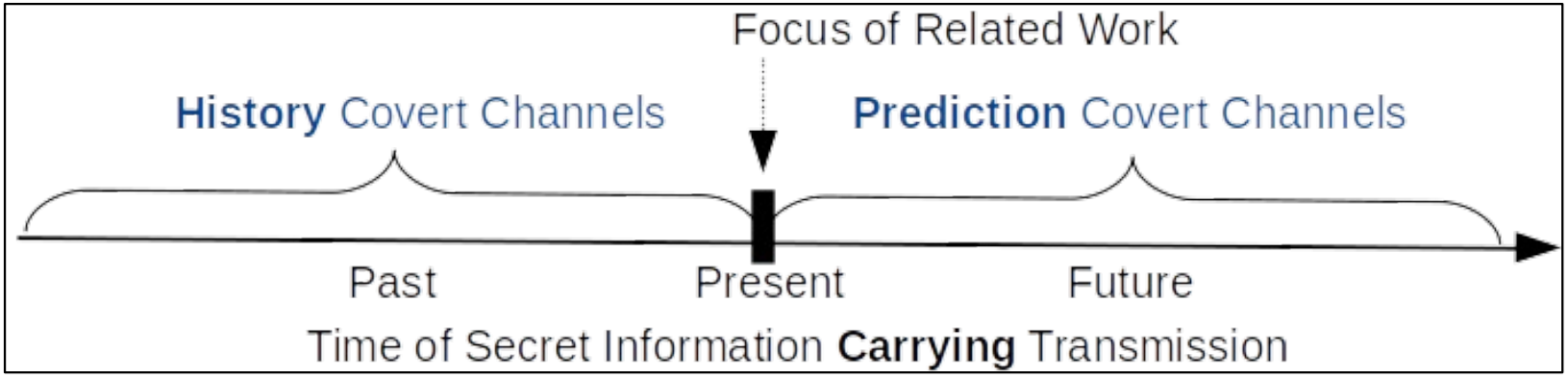
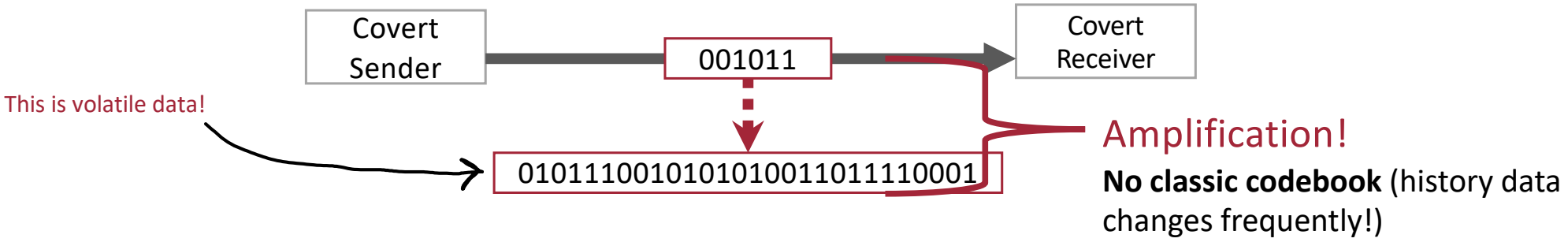


Fig.: [1]

[1] S. Wendzel, T. Schmidbauer, S. Zillien, J. Keller: DYST (Did You See That?): An Amplified Covert Channel That Points To Previously Seen Data. IEEE Transactions on Dependable and Secure Computing (TDSC), Vol. 22(1), 2025, DOI: 10.1109/TDSC.2024.3410679

Types of (Network) Covert Channels: History Cov. Channels and Cov. Ch. Amplification [1]

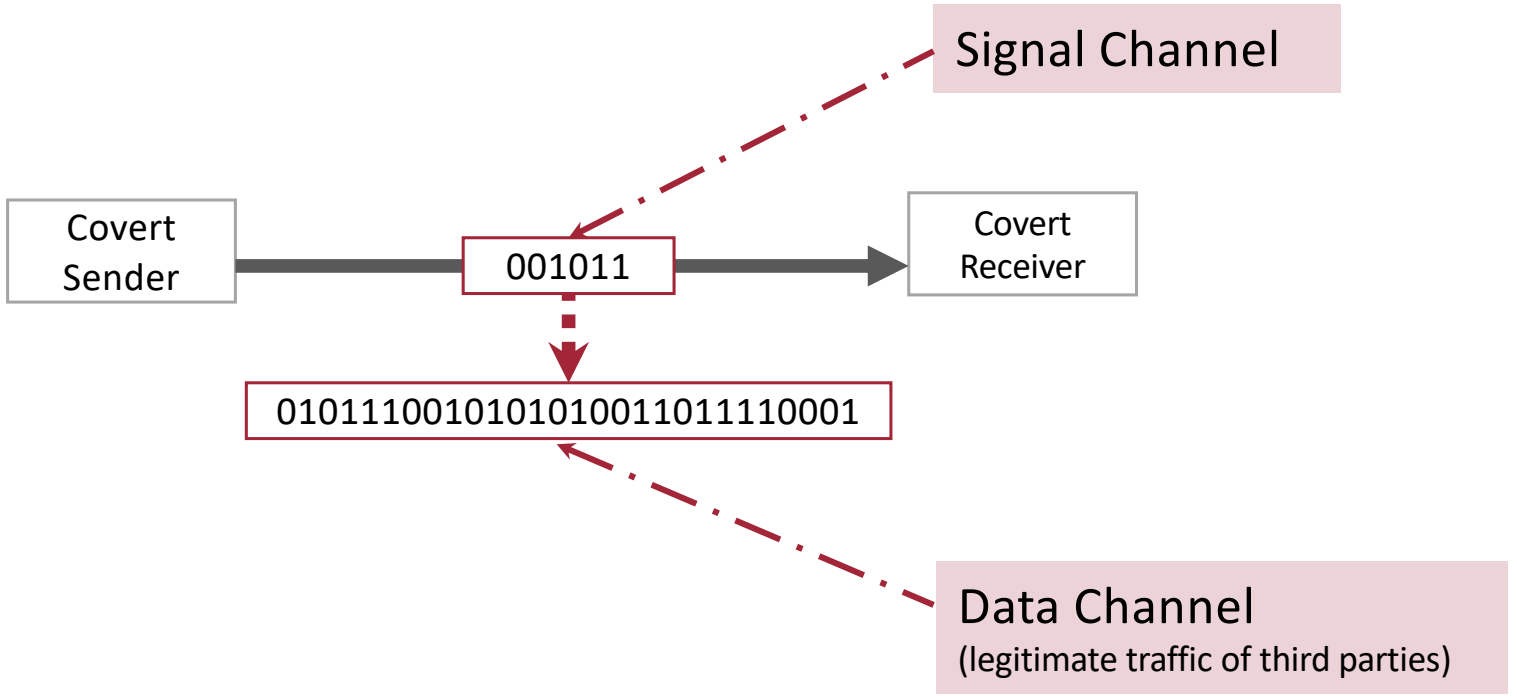
- **History** covert channels optimize transmission sizes by transferring **solely pointers to larger data chunks already seen somewhere**, e.g., in previous packets or online data [1].
- These data chunks represent the actual secret information. First implementation called "**DYST**" (*Did You See That?*). Since the pointers are smaller than the actual secret data, one achieves an **amplification**.



[1] S. Wendzel, T. Schmidbauer, S. Zillien, J. Keller: DYST (Did You See That?): An Amplified Covert Channel That Points To Previously Seen Data. IEEE Transactions on Dependable and Secure Computing (TDSC), Vol. 22(1), 2025, DOI: 10.1109/TDSC.2024.3410679

Types of (Network) Covert Channels: History
Cov. Channels and Cov. Ch. Amplification [1]

- We split our covert channel into a **signal channel** and a **data channel**.



[1] S. Wendzel, T. Schmidbauer, S. Zillien, J. Keller: DYST (Did You See That?): An Amplified Covert Channel That Points To Previously Seen Data. IEEE Transactions on Dependable and Secure Computing (TDSC), Vol. 22(1), 2025, DOI: 10.1109/TDSC.2024.3410679

Types of (Network) Covert Channels: History Cov. Channels and Cov. Ch. Amplification

- History/prediction channels enable a new category of **fully-passive covert channels** (see **figure** below), where a stego **data channel** (in this case "**DYST**") can be represented through 100% legitimate traffic – solely the **signaling channel** (containing the pointer) needs to craft new/modify existing packets [1].

		Covert **Sender**		
		Active (generates own overt traffic in which it embeds covert data)	**Passive** (embeds covert data in overt traffic of third-party nodes)	**Fully-passive** (utilizes third-party traffic without modifying it)
Covert **Receiver**	**Active** (is the destination of the overt traffic)	**Active** Covert Channel	**Semi-passive** Covert Channel	**Fully-and-semi-passive** Covert Channel
	Passive (is not the direct destination of the overt traffic, e.g., a router)	**Semi-active** Covert Channel  **DYST's Signal Channel**	**Passive** Covert Channel	**Fully-passive** Covert Channel  **DYST's Data Channel**

Fig.: [1]

[1] S. Wendzel, T. Schmidbauer, S. Zillien, J. Keller: DYST (Did You See That?): An Amplified Covert Channel That Points To Previously Seen Data. IEEE Transactions on Dependable and Secure Computing (TDSC), Vol. 22(1), 2025, DOI: 10.1109/TDSC.2024.3410679

Types of (Network) Covert Channels: History
Cov. Channels: DYST (Basic Version)

- How do history covert channels work?
  - Different approaches feasible, also outside of networks.
- Together with the concept of history covert channels, we introduced a first implementation (before-mentioned **DYST**) in [1].

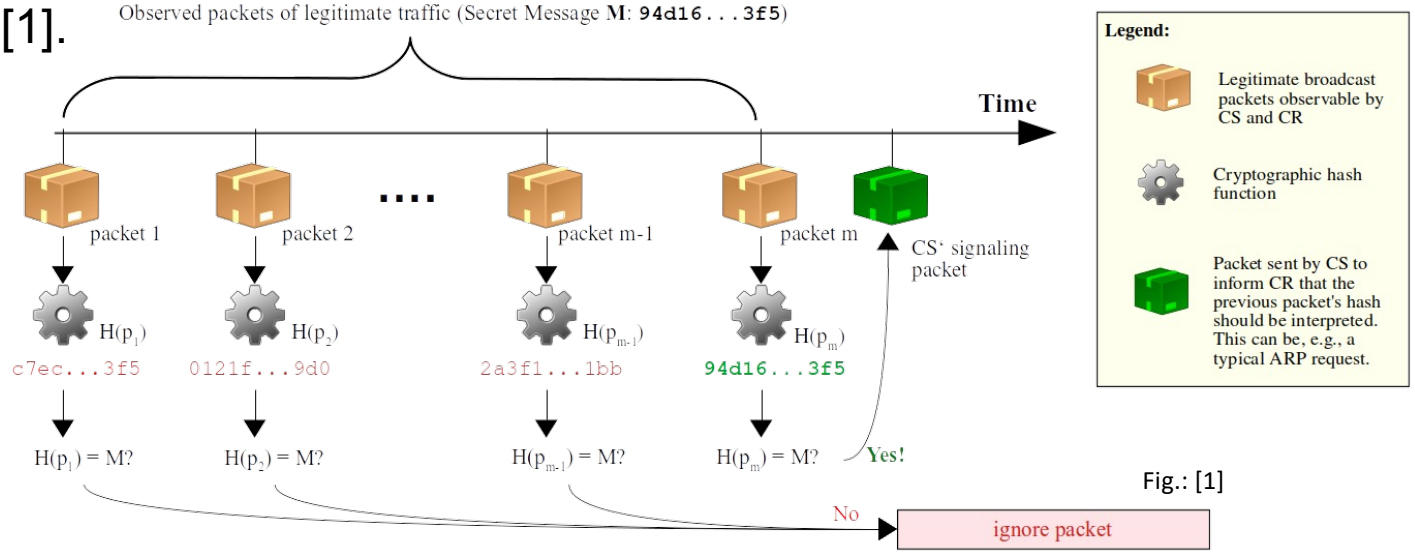
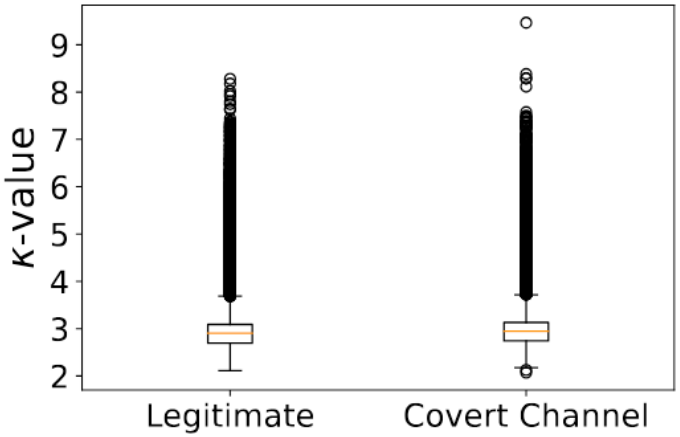


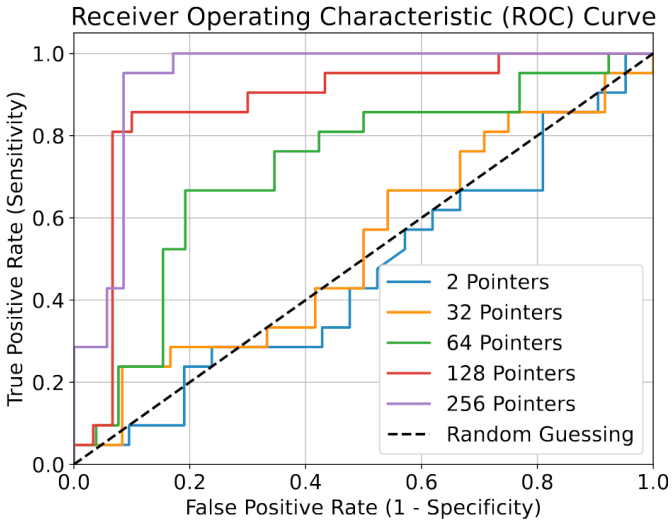
Fig.: [1]

[1] S. Wendzel, T. Schmidbauer, S. Zillien, J. Keller: DYST (Did You See That?): An Amplified Covert Channel That Points To Previously Seen Data. IEEE Transactions on Dependable and Secure Computing (TDSC), Vol. 22(1), 2025, DOI: 10.1109/TDSC.2024.3410679

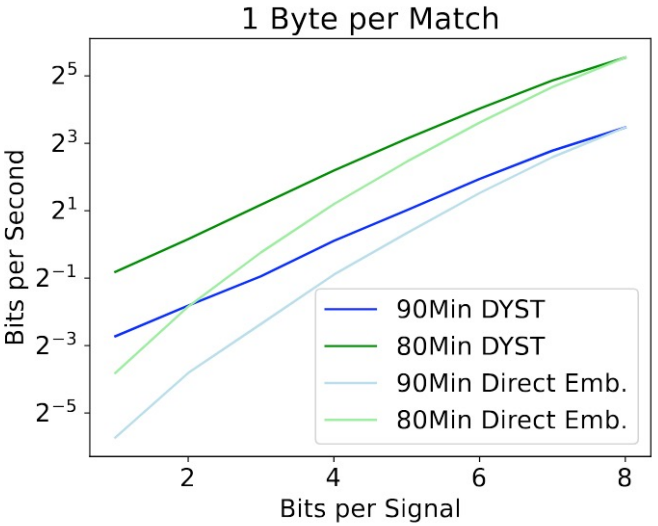
Types of (Network) Covert Channels: History
Cov. Channels: DYST (Basic Version)

Detectability and Performance

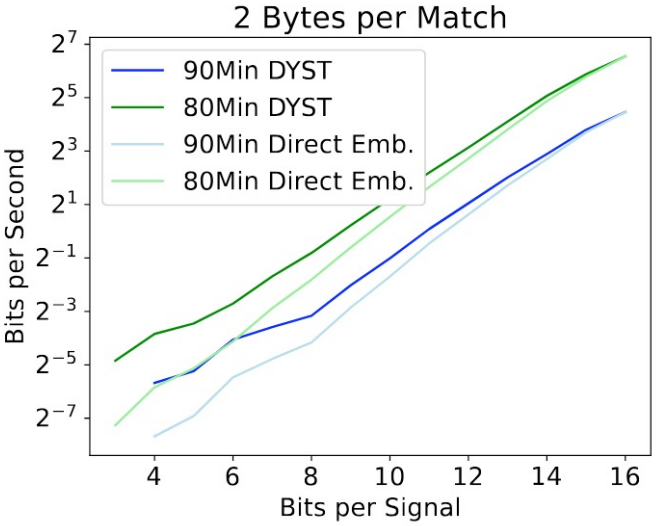




All Figures taken from [1]



(a) 1 byte/match



(b) 2 byte/match

[1] S. Wendzel, T. Schmidbauer, S. Zillien, J. Keller: DYST (Did You See That?): An Amplified Covert Channel That Points To Previously Seen Data. IEEE Transactions on Dependable and Secure Computing (TDSC), Vol. 22(1), 2025, DOI: 10.1109/TDSC.2024.3410679

universität ulm

History Covert Channels
pointing to textual data

OPPRESSION

Institut für Organisation und Management
von Informationssystemen

OPPRESSION (*Open-knowledge Compression*) [1]

- Still a **History Covert Channel**
- Still Covert Channel **Amplification**
- **But:**
  - does not point to recently observed network data
  - points to public Internet texts instead

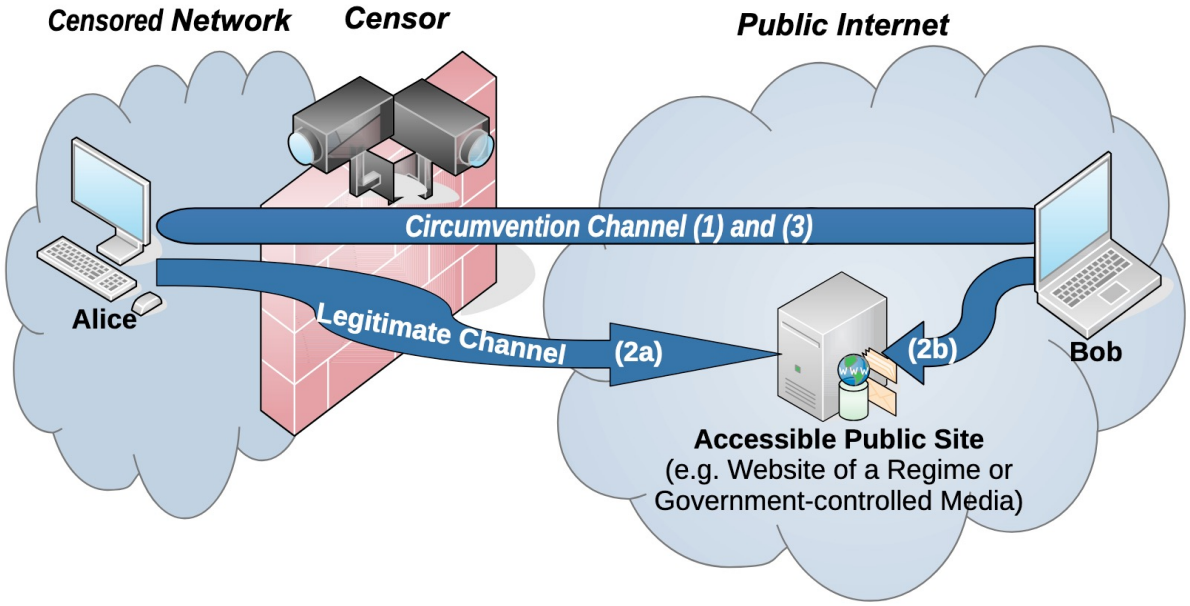


Figure 1: High-level Functioning of OPPRESSION

[1] S. Zillien, T. Schmidbauer, M. Kubek, J. Keller, S. Wendzel: Look What's There! Utilizing the Internet's Existing Data for Censorship Circumvention with OPPRESSION. ACM ASIA CCS, 2024. https://dl.acm.org/doi/pdf/10.1145/3634737.3637676

OPPRESSION (*Open-knowledge Compression*) [1]

- Sender and receiver both crawl public text repositories to create a local dictionary.

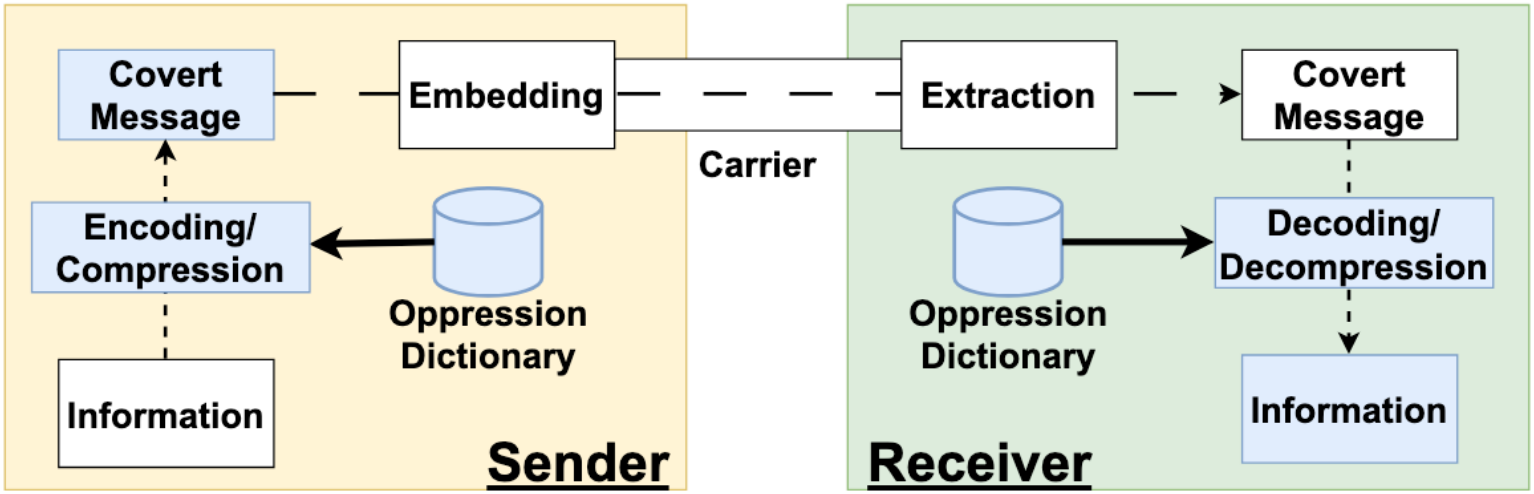


Figure 2: Contribution of OPPRESSION

[1] S. Zillien, T. Schmidbauer, M. Kubek, J. Keller, S. Wendzel: Look What's There! Utilizing the Internet's Existing Data for Censorship Circumvention with OPPRESSION. ACM ASIA CCS, 2024. https://dl.acm.org/doi/pdf/10.1145/3634737.3637676

OPPRESSION (*Open-knowledge Compression*) [1]

- In general: we are referring to a document (used to create a tree) and a particular node in that tree to represent a sentence.
- We can also spell words, if necessary (decreases compression).
- Two separate coding strategies (cf. paper)

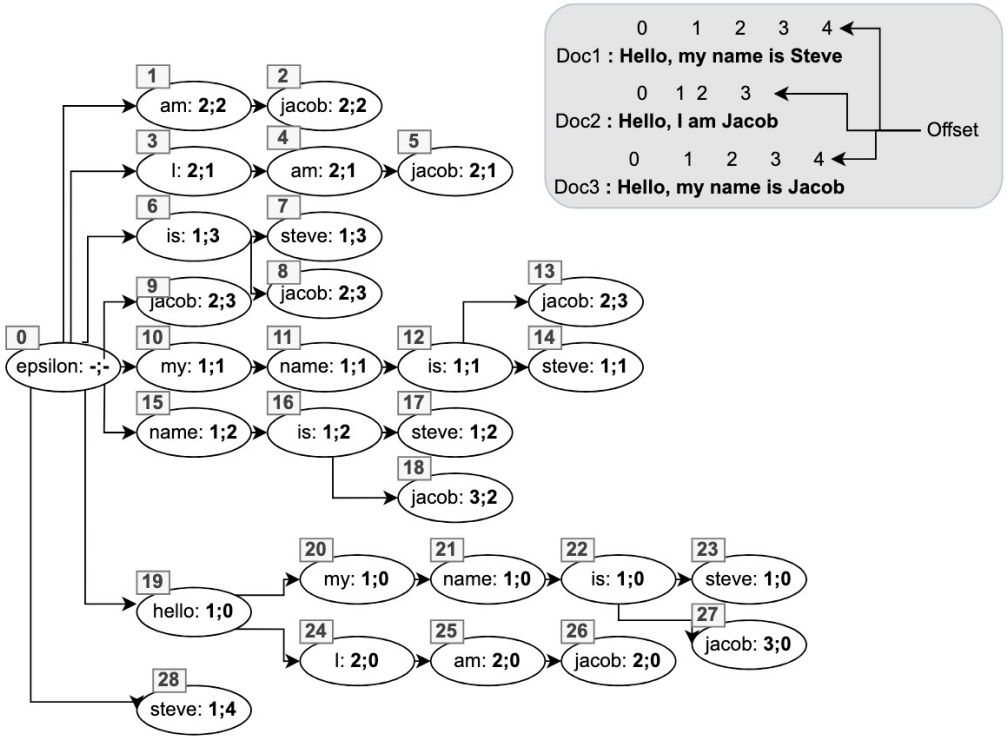


Figure 3: Document-pointer Tries

[1] S. Zillien, T. Schmidbauer, M. Kubek, J. Keller, S. Wendzel: Look What's There! Utilizing the Internet's Existing Data for Censorship Circumvention with OPPRESSION. ACM ASIA CCS, 2024. https://dl.acm.org/doi/pdf/10.1145/3634737.3637676

OPPRESSION (*Open-knowledge Compression*) [1]

- Exemplary results for one coding strategy and GZIP
- Also ran several more tests (see paper)!

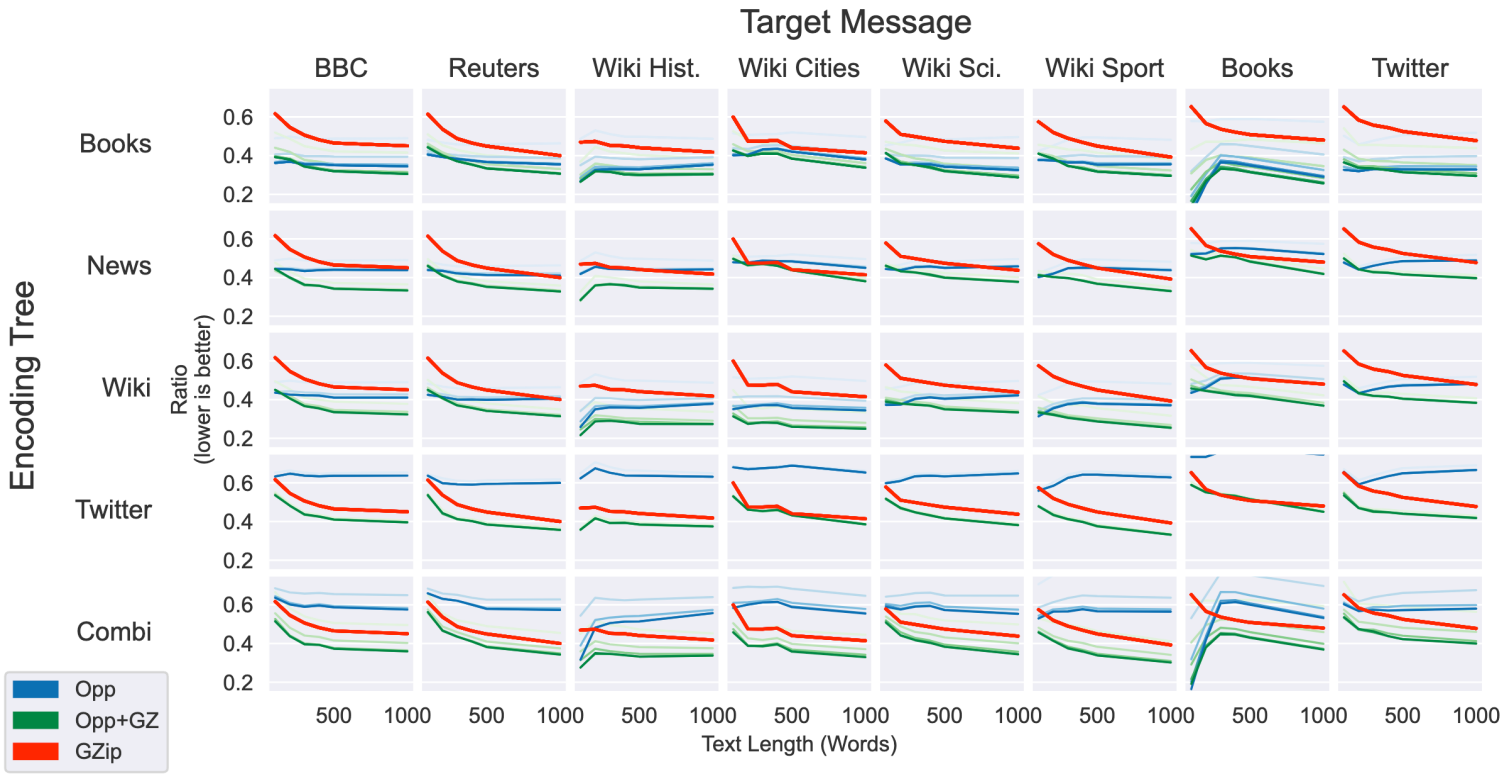


Figure 4: Evaluation Results: Doc. Pointer. Color shades indicate different tree depths (darker color signals a deeper tree).

[1] S. Zillien, T. Schmidbauer, M. Kubek, J. Keller, S. Wendzel: Look What's There! Utilizing the Internet's Existing Data for Censorship Circumvention with OPPRESSION. ACM ASIA CCS, 2024. https://dl.acm.org/doi/pdf/10.1145/3634737.3637676

OPPRESSION (*Open-knowledge Compression*) [1]

- Possible to enhance existing censorship circumvention tools:

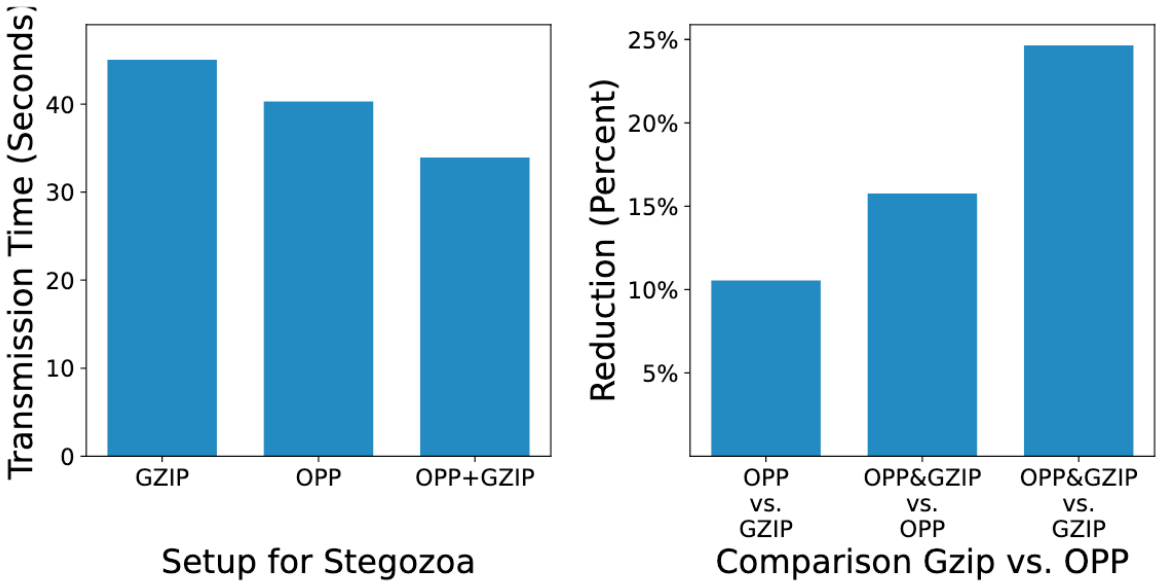


Figure 10: OPPRESSION with Stegozoa

[1] S. Zillien, T. Schmidbauer, M. Kubek, J. Keller, S. Wendzel: Look What's There! Utilizing the Internet's Existing Data for Censorship Circumvention with OPPRESSION. ACM ASIA CCS, 2024. https://dl.acm.org/doi/pdf/10.1145/3634737.3637676

universität ulm

First Aspects of Covert Channel Measurement

Institut für Organisation und Management von Informationssystemen

How to „measure“ covert channels?

- Introduction of **Covertness** by Giani et al. [1]:

  Covertness ∝ (Capacity if the medium – Transmission Rate)

  If the whole capacity of a transmission medium (e.g. network packets or an audio CD) is used, the covertness is zero, leading to a trivial detection. However, if only a tiny fraction of the capacity is used, the covertness can remain close to one.

[1] A. Giani, V. H. Berk, G. V. Cybenko: Data Exfiltration and Covert Channels, Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense V. Vol. 6201. International Society for Optics and Photonics, 2006.

Let’s have a look at Fig. 1 and 2. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=1b6cdc2dda45a3de0333be6181517417a89b9339

How to „measure“ covert channels?

- **Steganographic Cost (SC)** by Mazurczyk et al. [1]:
  - Measure of degradation or distortion of a carrier caused by the application of a steganographic method.
  - Calculation depends on context. For instance, for *LACK* steganography, which exploits packet loss, the **SC** can be calculated using the *Mean Opinion Score* (MOS) as a **difference in quality of the voice signal** (**RQ**) without and with LACK applied (**LQ**):

$$SC_{T-LACK}(t) = \Delta MOS(t) = RQ(t) - LQ(t)$$

  - For *Retransmission Steganography* (RSTEG), one can calculate the **retransmission difference** R_D instead:

$$SC_{T-RSTEG} = R_D = R_{N-RSTEG} - R_N$$

    - $R_{N-RSTEG}$ denotes retransmissions in the network with RSTEG and R_N the network's retransmissions without applying RSTEG.

[1] W. Mazurczyk, S. Wendzel, I. Azagra Villares, K. Szczypiorski: On importance of steganographic cost for network steganography, SCN, 9(8), 781-790, Wiley, 2016.