Obfuskierte und versteckte Datenkommunikation: Subdomänen und Forschungstrends

Steffen Wendzel[1,2]

[1] Zentrum für Technologie und Transfer | ZTT, Hochschule Worms
[2] Fakultät für Mathematik und Informatik, FernUniversität in Hagen

Cyberagentur-Talks – Cyberagentur meets Cyber-Scientists, 5. April 2023

Hochschule Worms
University of Applied Sciences

"In my own field, for example, it once was possible for a grad student to learn just about everything there was to know about computer science. […] Nowadays the subject is so enormous, nobody can hope to cover more than a tiny portion of it."

- Donald Knuth (2001)

Information Hiding: What is it?

What is „Information Hiding“? Two different examples:

All figures taken from Wikipedia articles on ‚Steganography‘ and ‚Watermarking‘

History of Information Hiding

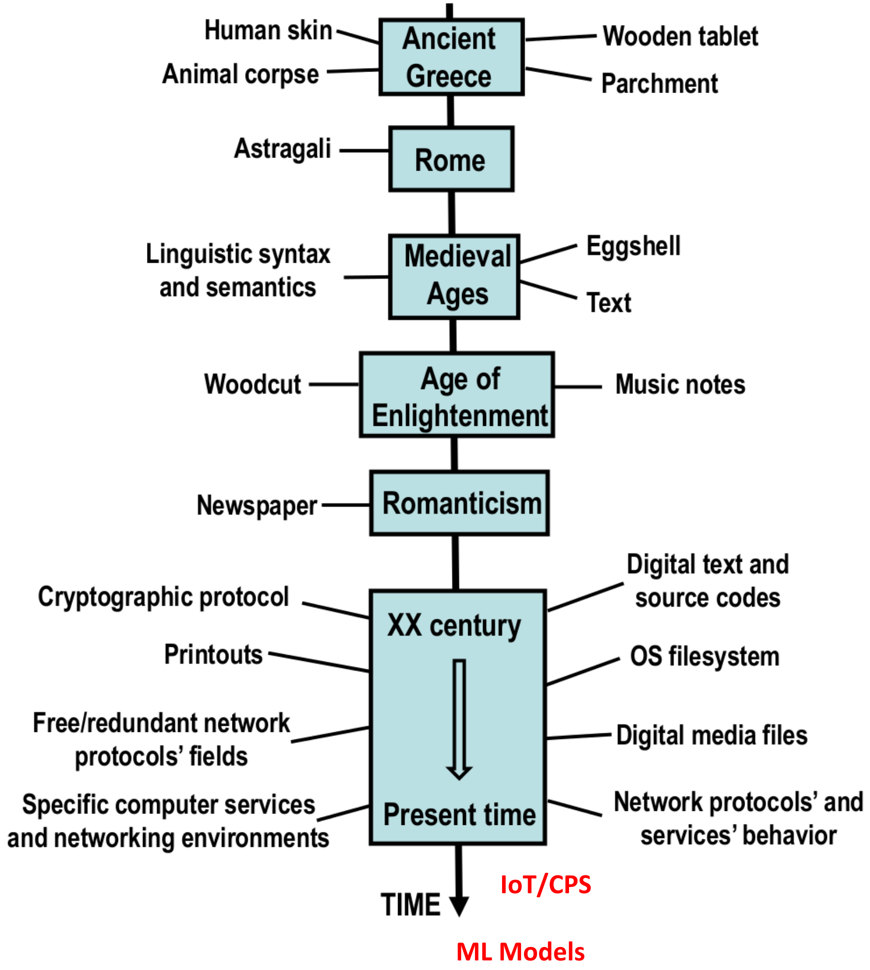


Fig.: W. Mazurczyk, S. Wendzel, S. Zander et al.: Information Hiding in Communication Networks, Wiley-IEEE, 2016

History of Information Hiding

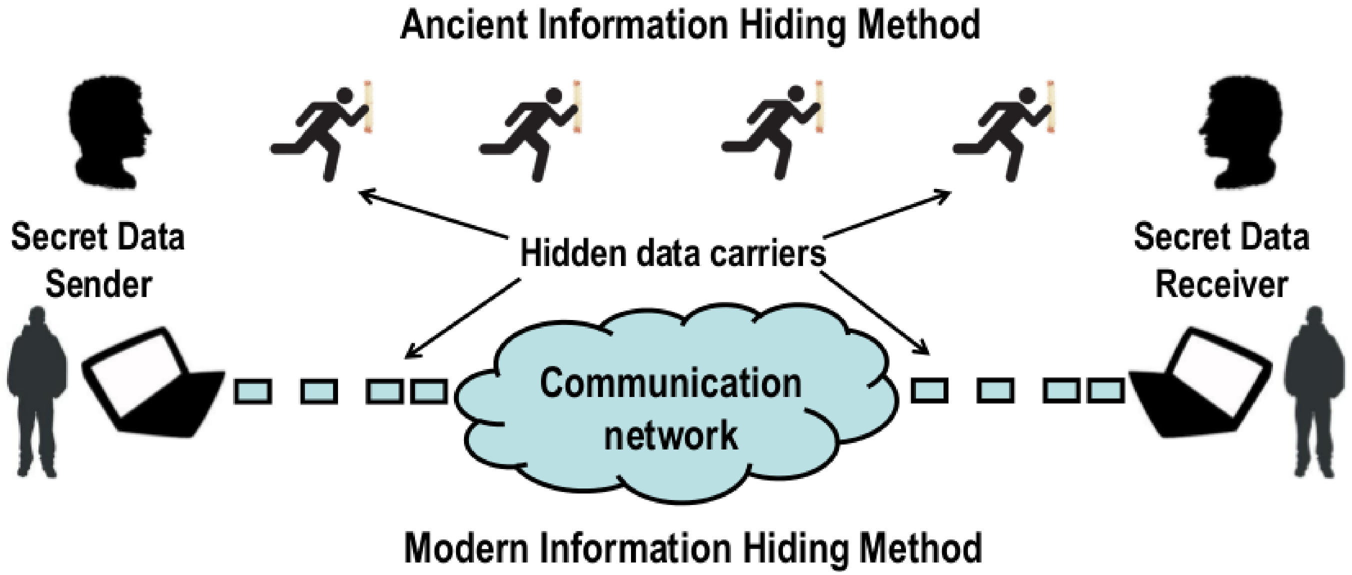


Fig.: W. Mazurczyk, S. Wendzel, S. Zander et al.: Information Hiding in Communication Networks, Wiley-IEEE, 2016

Related Disciplines

Change **characteristics** of traffic, e.g., let Tor traffic appear as Skype traffic.

- Censorship Circumvention
  (Traffic Morphing, **Traffic Obfuscation**)

Hide the **fact** of a secret communication, e.g., by hiding it in some legitimate traffic.

- Traffic Flow Watermarking
  (Flow Linking)

- Network Information Hiding
  (Network Steganography, Covert Channels, Traffic **Concealment**, ``Tunneling'')

- Network Side Channels
  (e.g., Network Protocol Cache Exploitation)

„Don‘t People Just Use Tor?“

- Censorship Circumvention **uses** Tor.
  But: **Tor needs adjustments to prevent being filtered!**

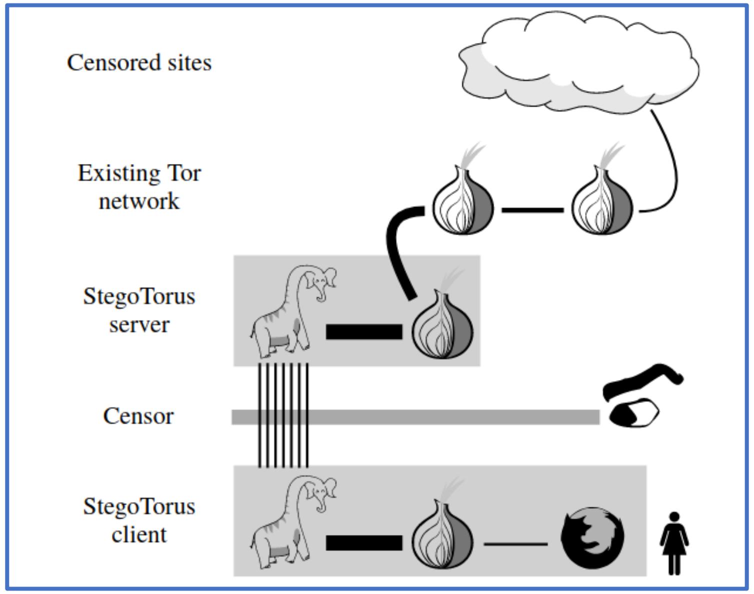


Fig.: Weinberg et al. "Stegotorus: A camouflage proxy for the Tor anonymity system." *Proc. ACM CCS 20212.*

Example: Packet Size Padding as proposed by Dyer et al.: *Peek-a-boo, I still see you: Why efficient traffic analysis countermeasures fail*, in Proc. IEEE Symposium on Security and Privacy (S&P), 2012.

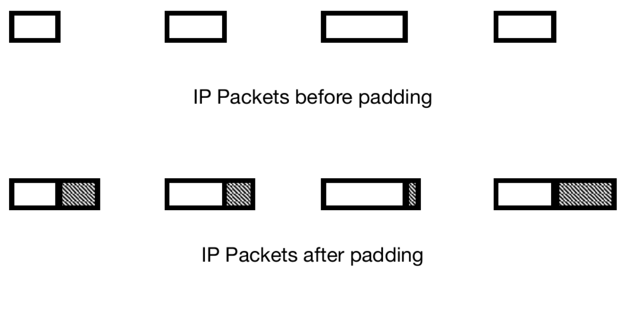


Figure 5.2: Padding network packets to de-identify packet sizes.

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

Basic Mimicry System [1]

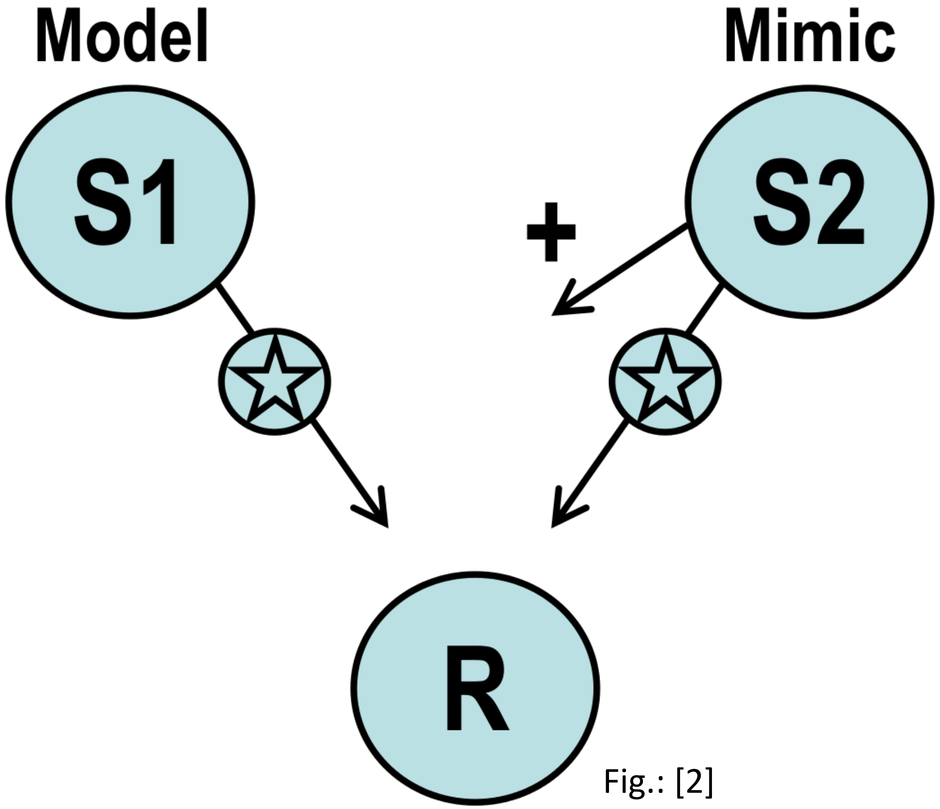


Fig.: [2]

[1] R. I. Vane-Wright: A unified classification of mimetic resemblances, Biological Journal of the Linnean Society, 1976.
[2] W. Mazurczyk, S. Wendzel, S. Zander et al.: Information Hiding in Communication Networks, Wiley-IEEE, 2016

Scientific Re-inventions in Cybersecurity

- **Scientific Re-inventions** are common, and cybersecurity is no exception [1].

- Thousands of methods to conceal, circumvent, obfuscate and hide data available.
  - Several redundancies!

- Started to derive commonalities in 2013 (Steganography, Covert Channels) and widened focus in 2022 (Censorship, Traffic Obfuscation etc.)

[1] S. Wendzel, L. Caviglione, W. Mazurczyk: Avoiding Research Tribal Wars Using Taxonomies, in: IEEE Computer, Vol. 56(1), 2023.

"In my own field, for example, it once was possible for a grad student to learn just about everything there was to know about computer science. […] Nowadays the subject is so enormous, nobody can hope to cover more than a tiny portion of it."

*- Donald Knuth (**2001**)*

Let‘s add 22 years to Knuth‘s Words …

Figs.: DukeNukeIt/Wikipedia

2023 … in a network security research lab far, far away:

"In ~~my own field~~ network concealment research, for example, it once was possible for a grad student to learn just about everything there was to know. […] Nowadays the subject is so enormous, nobody can hope to cover more than a tiny portion of it."

- Knuth didn't say that.

Hochschule Worms University of Applied Sciences

Low-level Methods

- There **are hundreds data hiding/concealment methods** available.
- Organization of these methods is beneficial to **keep an overview** and to find similar works.
- Organization also **prevents scientific re-inventions**.

Lecture will present new taxonomy that covers essentially all steganography domains and unifies terminology in the domain.

How things started …

- 2013 – no state-of-the-art detail-level survey for network steganography was available.

- Formation of team working on a first paper because **multiple** terms were used for **same** hiding concepts.
  - w/ **Sebastian Zander** (Murdoch Univ., Perth/Swinburne Univ. Techn., Melbourne), **Bernhard Fechner** (Univ. Augsburg/Hagen) and **Christian Herdin** (TH Augsburg).

Development Over Time

- First taxonomy for NetSteg
- Definition of hiding patterns
- Methodology & concepts

- Added new timing channel categorization (protocol-agnostic/aware)
- New patterns
- Advanced general terminology

- Introduction of **hybrid patterns** (combination of two or more patterns)
- **Distributed** hiding patterns

- First taxonomy application to **ICS/CPS**
- Based on the network-level taxonomy

- Entirely new taxonomy, **for all domains of steganography**
- Differentiation between **embedding** and **representation** process
- Still mostly limited to network steganography

- First pattern-based taxonomy of **indirect** network CCs
- Uses the 2021-taxonomy

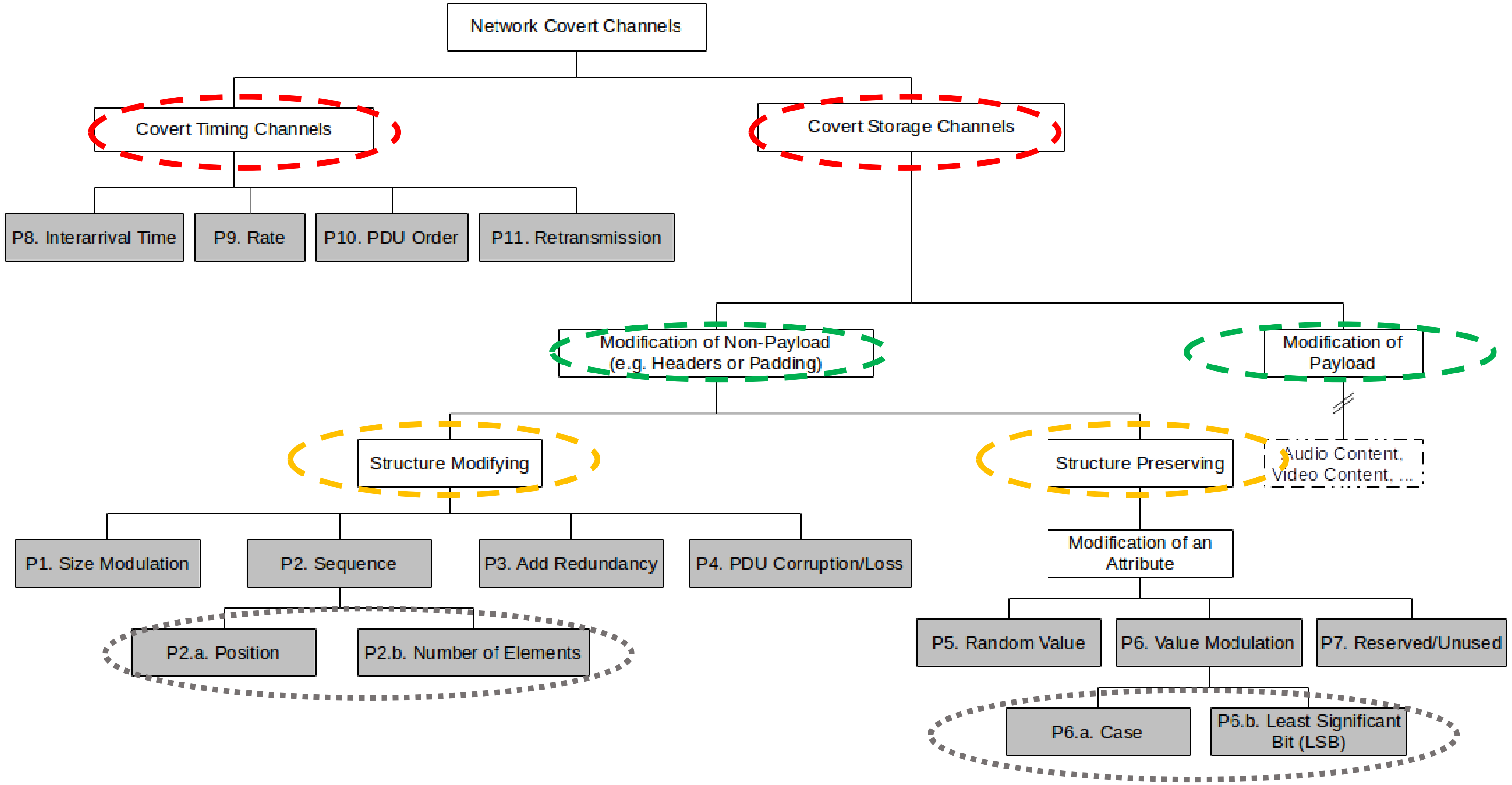
- First draft of a *complete* taxonomy for all steganography domains
- Fixes several issues with the 2021-taxonomy
- Comes with a tutorial/unified description method

Key publications

Publications adding new patterns

Introduction of ``Hiding Patterns“ in 2015

Patterns were set in relation to other patterns to introduce a **new taxonomy** of patterns. The 109 hiding techniques could be described by only 11 patterns.



S. Wendzel, S. Zander et al.: [Pattern-based Survey and Taxonomy for Network Covert Channels](), ACM Comp. Surv. (CSUR), Vol. 47(3), 2015.

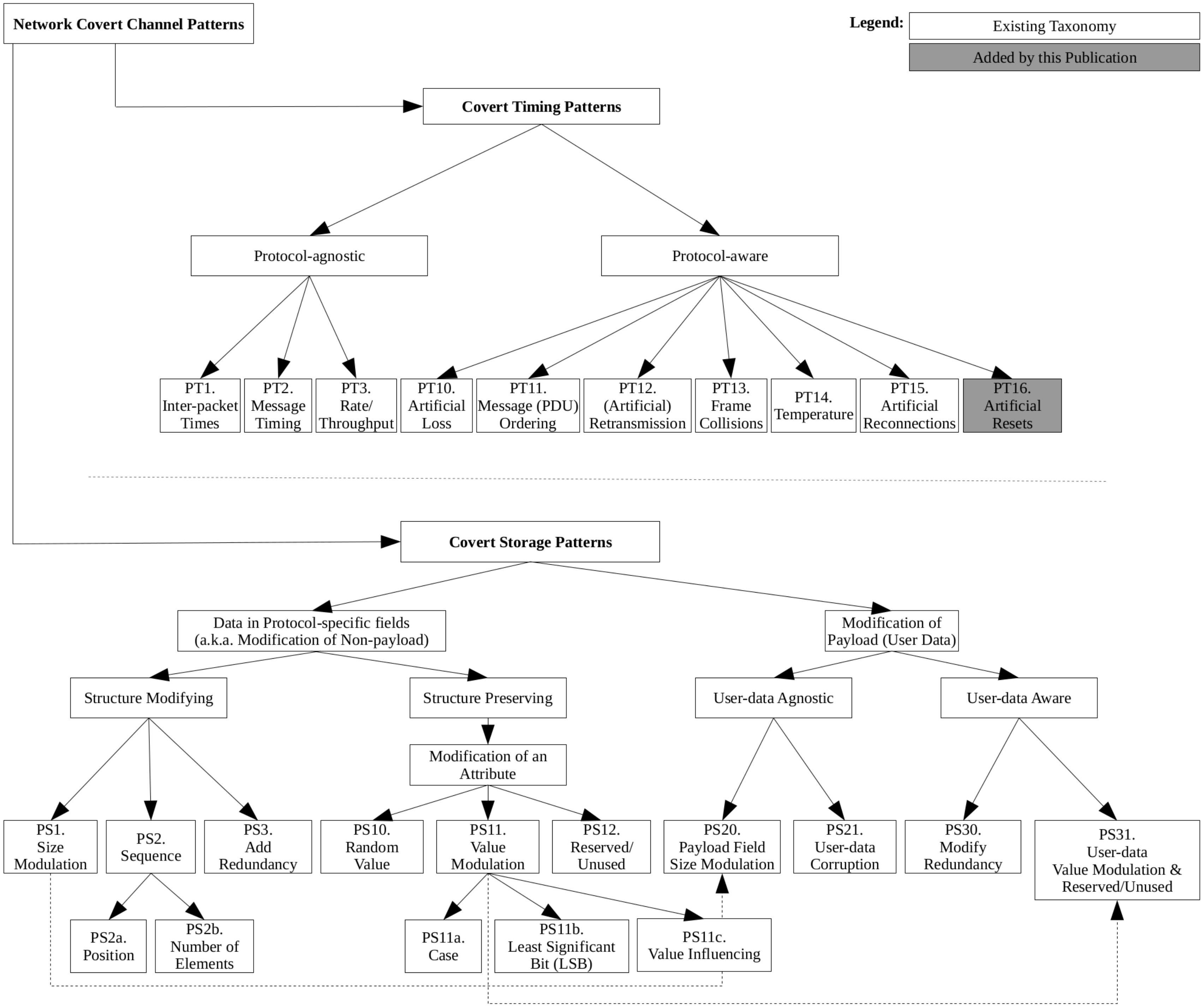
Hochschule Worms
University of Applied Sciences

Latest Network-specific Taxonomy

Hiding techniques categorized into 20 main timing and multiple sub-patterns. Pattern names and their numbers were updated and extended in 2016, 2018, 2019, (2020) and 2021 by several papers (small refs. below).

S. Wendzel, S. Zander, B. Fechner, C. Herdin: Pattern-based Survey and Taxonomy for Network Covert Channels, ACM CSUR, Vol. 47(3), 2015.
W. Mazurczyk, S. Wendzel, S. Zander et al.: Information Hiding in Communication Networks, WILEY-IEEE, 2016, Chapter 3.
W. Mazurczyk, S. Wendzel, K. Cabaj: Towards Deriving Insights into Data Hiding Methods Using Pattern-based Approach, in Proc. ARES, pp. 10:1-10:10, ACM, 2018.
A. Velinov, A. Mileva, S. Wendzel, W. Mazurczyk: Covert Channels in MQTT-based Internet of Things, IEEE ACCESS, Vol. 7, pp. 161899-161915, 2019.
A. Mileva, A. Velinov, L. Hartmann, S. Wendzel, W. Mazurczyk: *Comprehensive Analysis of MQTT 5.0 Susceptibility to Network Covert Channels*, Computers & Security, Elsevier, 2021.
L. Hartmann, S. Zillien, S. Wendzel: Analysis of New Covert Channels in CoAP, in: Proc. DETONATOR workshop (part of Proc. EICC 2021), ACM, 2021.

Fig.: reference L. Hartmann et al. (2021) above



How does such a *hiding pattern* look like?

E2.2 Element Positioning (PT1. Inter-packet Times)

Illustration: Secret message is represented by the spatial/temporal position of an element, e.g., network packets with a temporal position create inter-packet times.

Examples: (see [1,2,3] for more)

- Alter timings between Ethernet frames
- Alter timings between IP packets

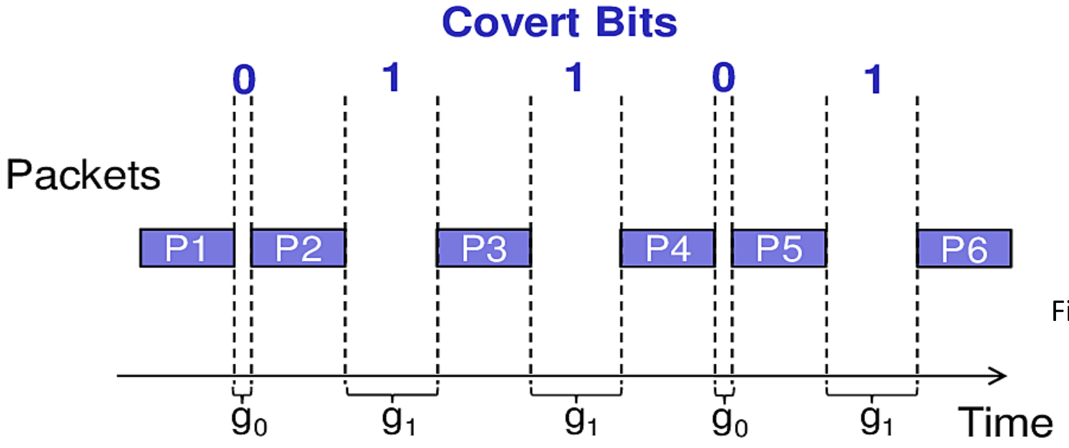


Fig.: [2]

Pattern was introduced in [1], originally variant in [2], updated by [3].

[1] S. Wendzel et al.: A Generic Taxonomy for Steganography Methods, pre-print, 2022.
[2] S. Wendzel, S. Zander, B. Fechner, C. Herdin: Pattern-based Survey and Taxonomy for Network Covert Channels, ACM CSUR, Vol. 47(3), 2015.
[3] W. Mazurczyk, S. Wendzel, S. Zander et al.: Information Hiding in Communication Networks, WILEY-IEEE, 2016, Chapter 3.

Toward Hiding Patterns for **Steganography**

Remaining slides of this paper are all based on
S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann, C. Krätzer, K. Lamshöft, C. Vielhauer, L. Hartmann, J. Keller, T. Neubert, S. Zillien (2022): *A Generic Taxonomy for Steganography Methods*, pre-print
https://www.techrxiv.org/articles/preprint/A_Generic_Taxonomy_for_Steganography_Methods/20215373
(If not explicitly indicated, figures of the following slides are taken from this paper.)

Hochschule Worms
University of Applied Sciences

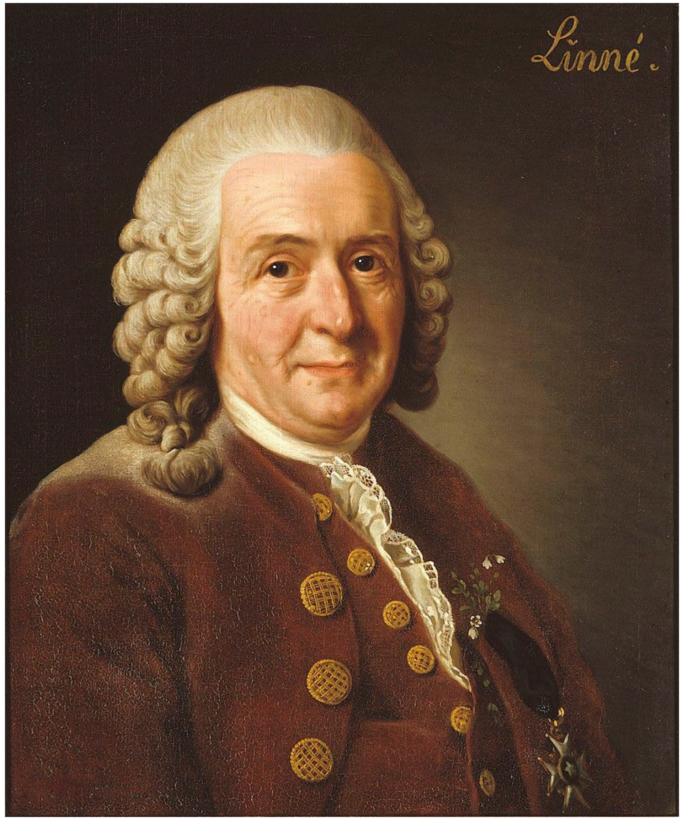
Let‘s start with the …

… **Problems**.

Problem 1: Different Names for the Same Thing

If the names are unknown knowledge of the things also perishes.

– Carl Linnaeus



Img.: Wikipedia, public domain

S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2022.

Problem 1: Different Names for the Same Thing

- **What‘s the Problem:**
  - Size-based Covert Channel
  - Packet Length/Size Covert Channel
  - Field Length Covert Channel
  - Padding Size Covert Channel
  - …
- **Solution:**
  - allow **aliases** when patterns are defined, so that people can connect terms easily (can be done using a pattern language, such as PLML).

S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2022.

Problem 2: Who cares about yet another taxonomy?

- New taxonomies in infosec are published on a regular basis!
- **Fact:** when you publish yet another one, it is likely getting ignored, like many other scientific inventions.

Solution: Involve the community!

- You found a new pattern? Contact us and we will integrate it; **you** will be named as the inventor!
- You published work that matches some pattern? We are happy to reference your work (paper/code/…) in our taxonomy so that you get some visibility!
- You plan to contribute something fundamental to the taxonomy? Contact us and take part at our working group meetings.

S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2022.

Problem 3: People need to understand a taxonomy!

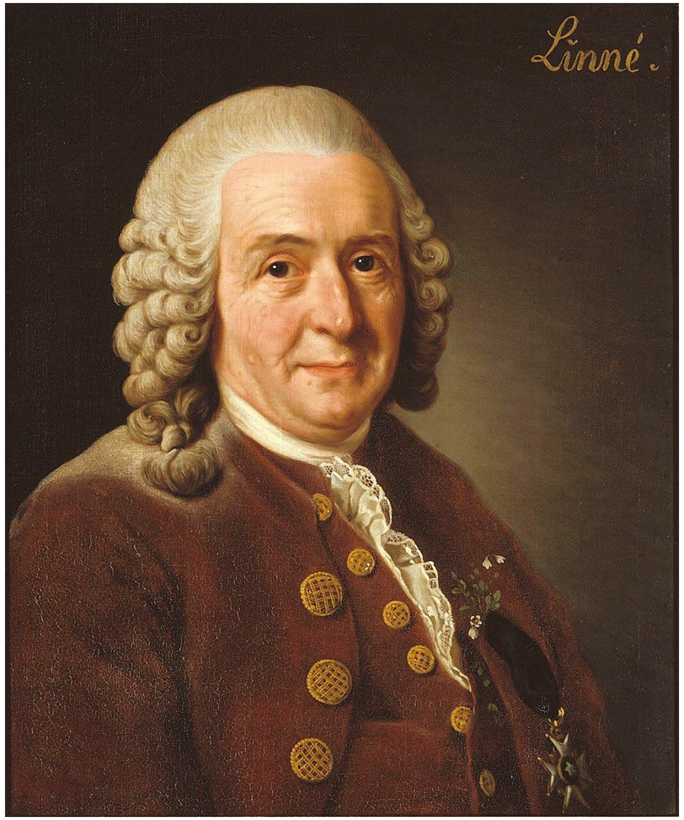
Let’s come back to Linnaeus.

His taxonomy was a success because of its **binomial nomenclature**!

Canis lupus (grey wolf)

Add more words for more detail:

Canis lupus ***dingo*** (austr. dingo)



Img.: Wikipedia, public domain

S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2022.

Problem 3: People need to understand a taxonomy!

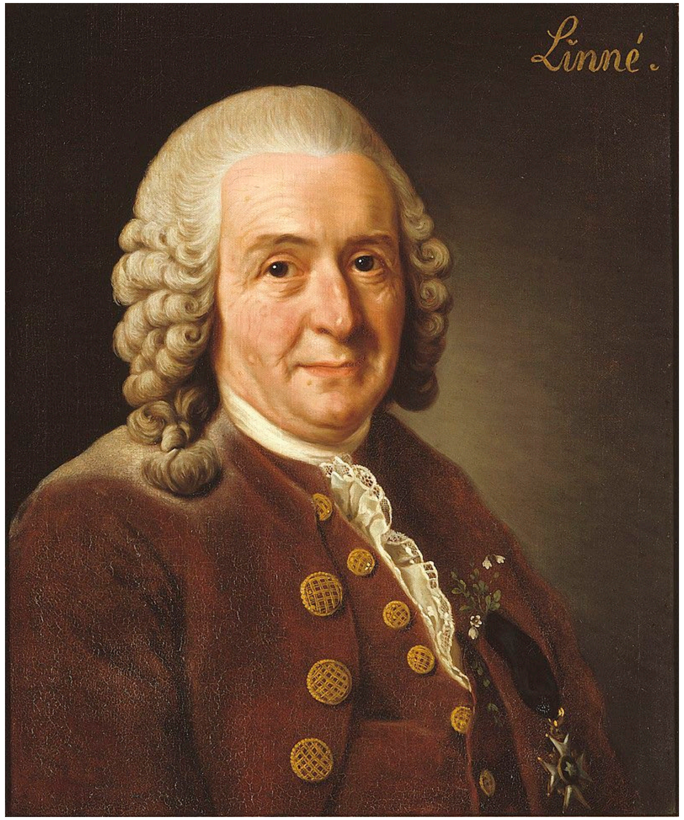
Essential terms of our steganography taxonomy are **bi-nomial**, more detailed terms can contain more words.

Our naming and enumeration conventions for patterns are easy to apply:

E1. State/Value Modulation

E1.3. LSB State/Value Modulation

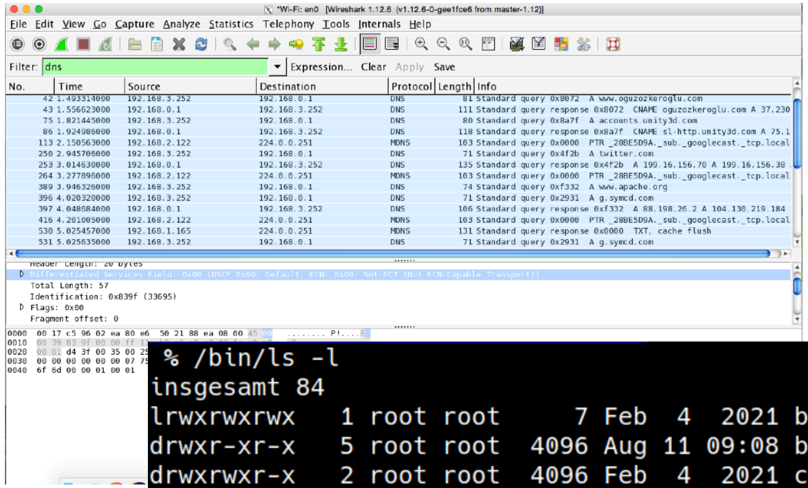
E1.3n1. Network LSB State/Value Modulation

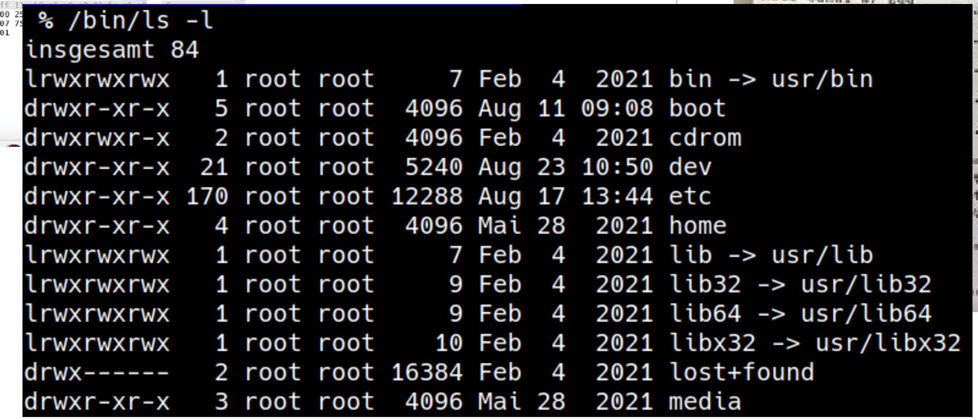


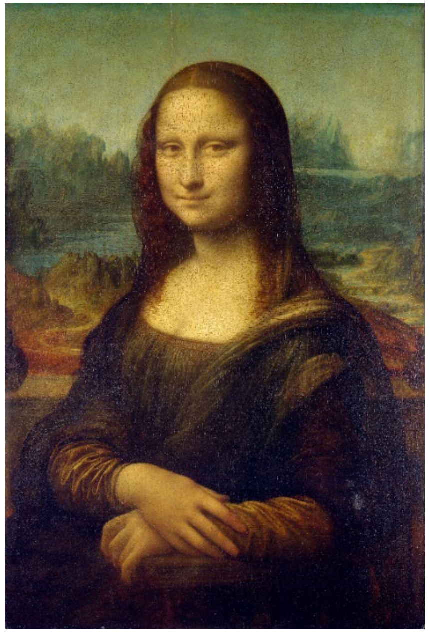
Img.: Wikipedia, public domain

S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2022.

Problem 4: Heterogenous Stego Objects

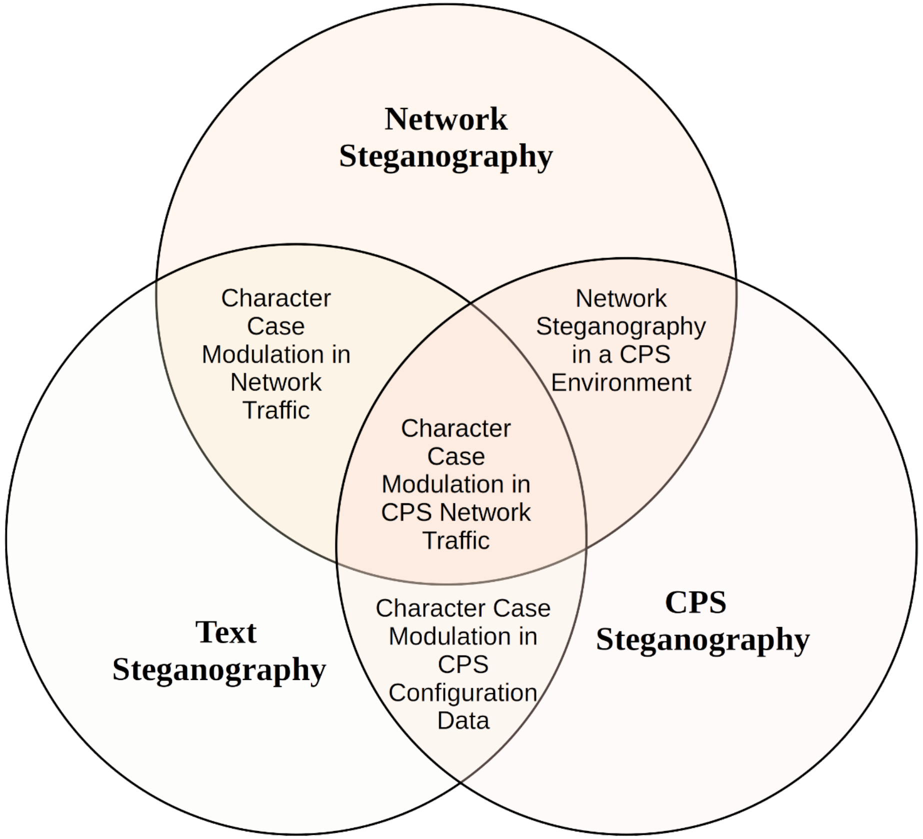






Taxonomies should be **exhaustive** and **mutually exclusive** [1], i.e., every object should be classifiable and should only belong to exactly one class. [1] K. D. Bailey: Typologies and Taxonomies. An Introduction to Classification Techniques, Sage Publications, 1994.

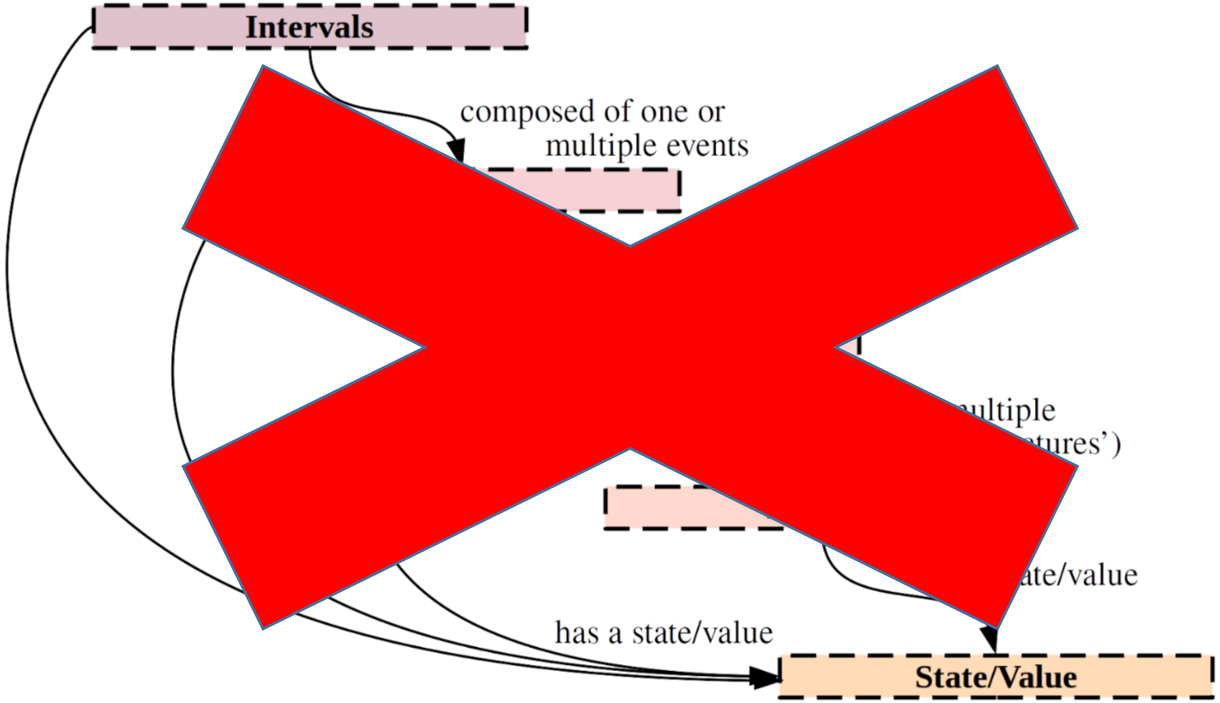
Problem 4: Heterogenous Stego Objects



S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2022.

Problem 4: Heterogenous Stego Objects

Solution (version 1): **Object-oriented** approach:

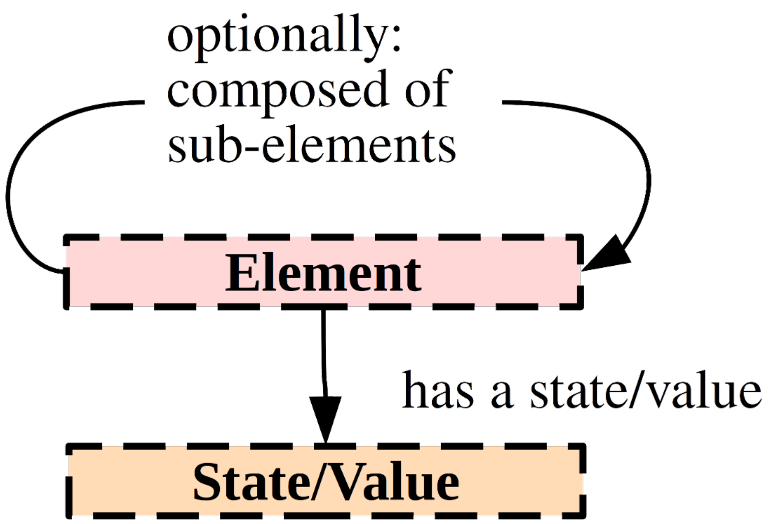


S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2022.

Problem 4: Heterogenous Stego Objects

Solution (v2): keep-it-simple-and-stupid (**KISS**)

Object-oriented approach, but simple:



S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2022.

Problem 4: Heterogenous Stego Objects

Solution (v2): keep-it-simple-and-stupid (**KISS**)

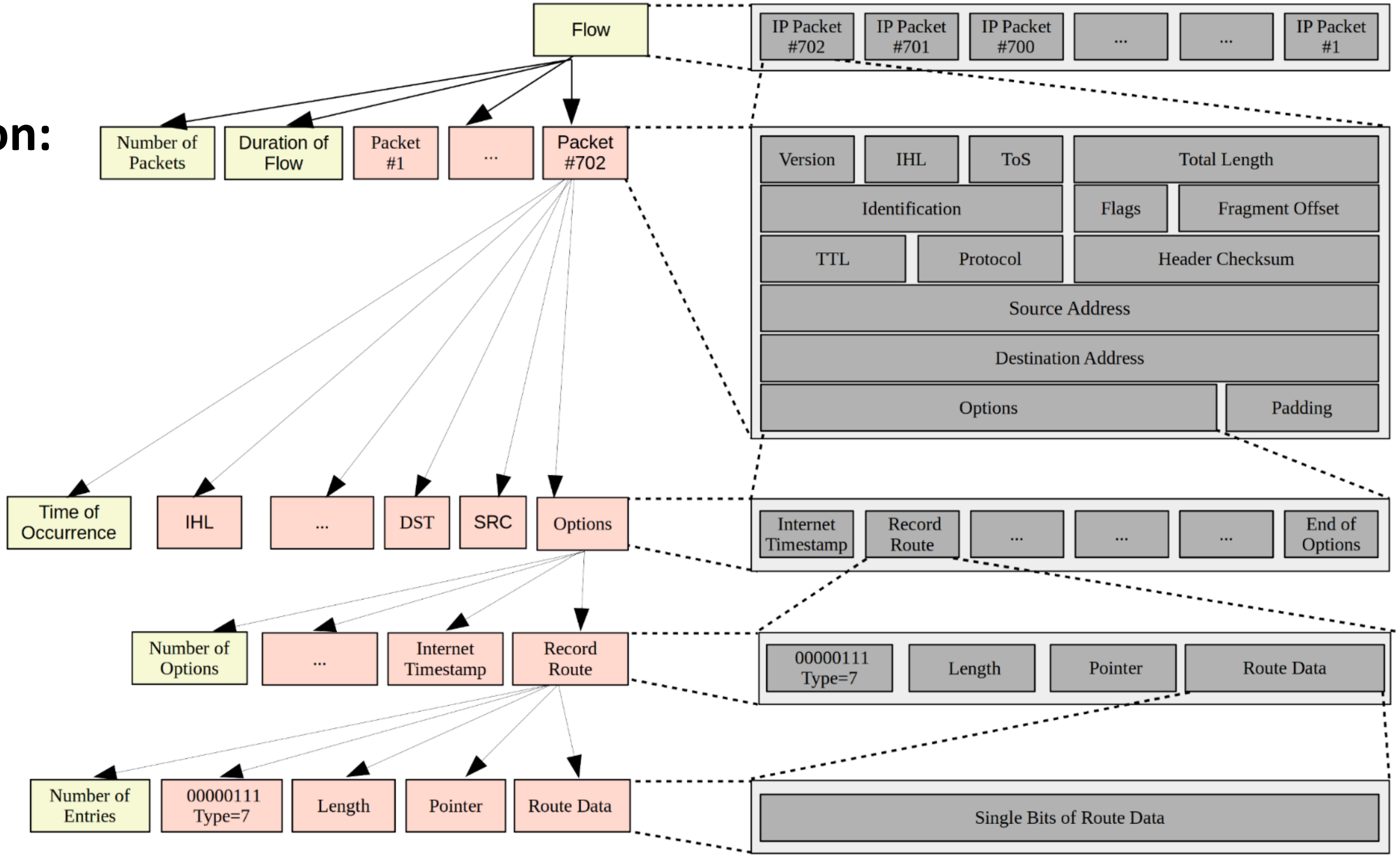
Table 1. Differentiation between the types of *objects* used in this paper.

Domain	Element Examples	State/Value Examples
network steg.	network packet (e.g., IP packet); header field (e.g., TCP seq. no.); packet size property; time of occurrence property of a packet	actual packet size in bytes; actual TCP sequence number; time of sending/arrival
text steg.	a text; a paragraph; a character; line spacing; font of a character; size of a character; text length	actual color value; actual font name; actual length of text
digital media steg.	pixel of an image; PNG file header attributes; color attribute of a pixel; image size property	actual color value; actual image size value
CPS steg.	a sensor; an actuator; control command (e.g., BACnet *ReadProperty*); temperature value of a sensor; status of an actuator	actual state of an actuator (open/closed); actual temperature value of a sensor
filesystem steg.	file; inode; file creation/deletion timestamp attributes; file size attribute; file header attribute; inode attribute (e.g., inode number field)	file's actual status (e.g., existent/deleted); actual inode number's value

S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2022.

Problem 4: Heterogenous Stego Objects

Illustration:



S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2022.

Problem 5: Hiding methods are often hybrid

For instance: “Artificial Reconnections”

1. Value Modulation (set certain header bits that trigger reconnects)
2. Element Positioning (position a packet in time)

Solution: following [1]: allow hybrid definitions, combined of atomic elements.

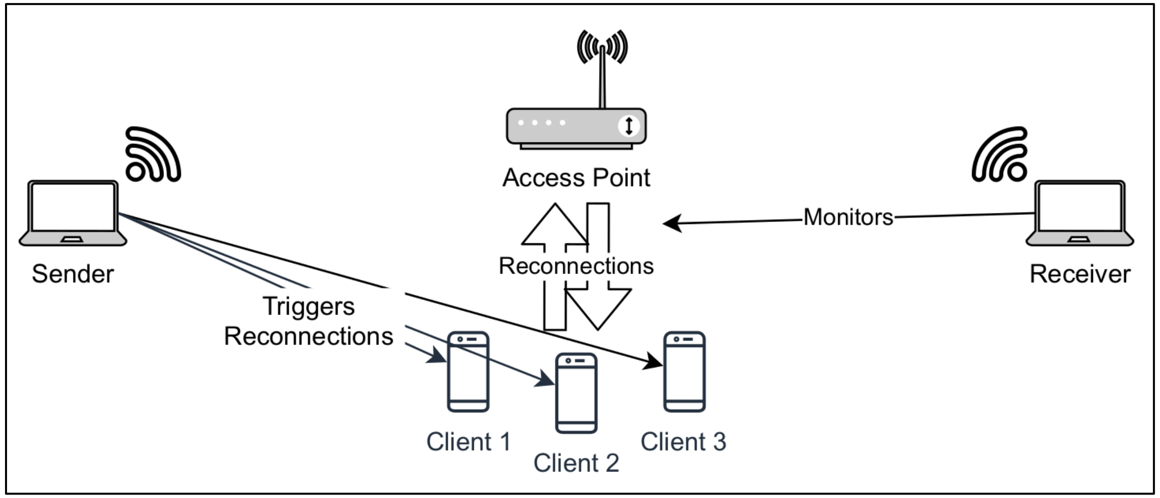


Fig.: S. Zillien, S. Wendzel: *Reconnection-based Covert Channels in Wireless Networks*, in Proc. 36th IFIP SEC, Springer, 2021.

[1] W. Mazurczyk, S. Wendzel, K. Cabaj: *Towards Deriving Insights into Data Hiding Methods Using Pattern-based Approach*, Proc. ARES'18 (CUING Workshop), 2018.

Problem 6: Embedding ≠ Extraction

Example: Spiekermann et al. [1]:

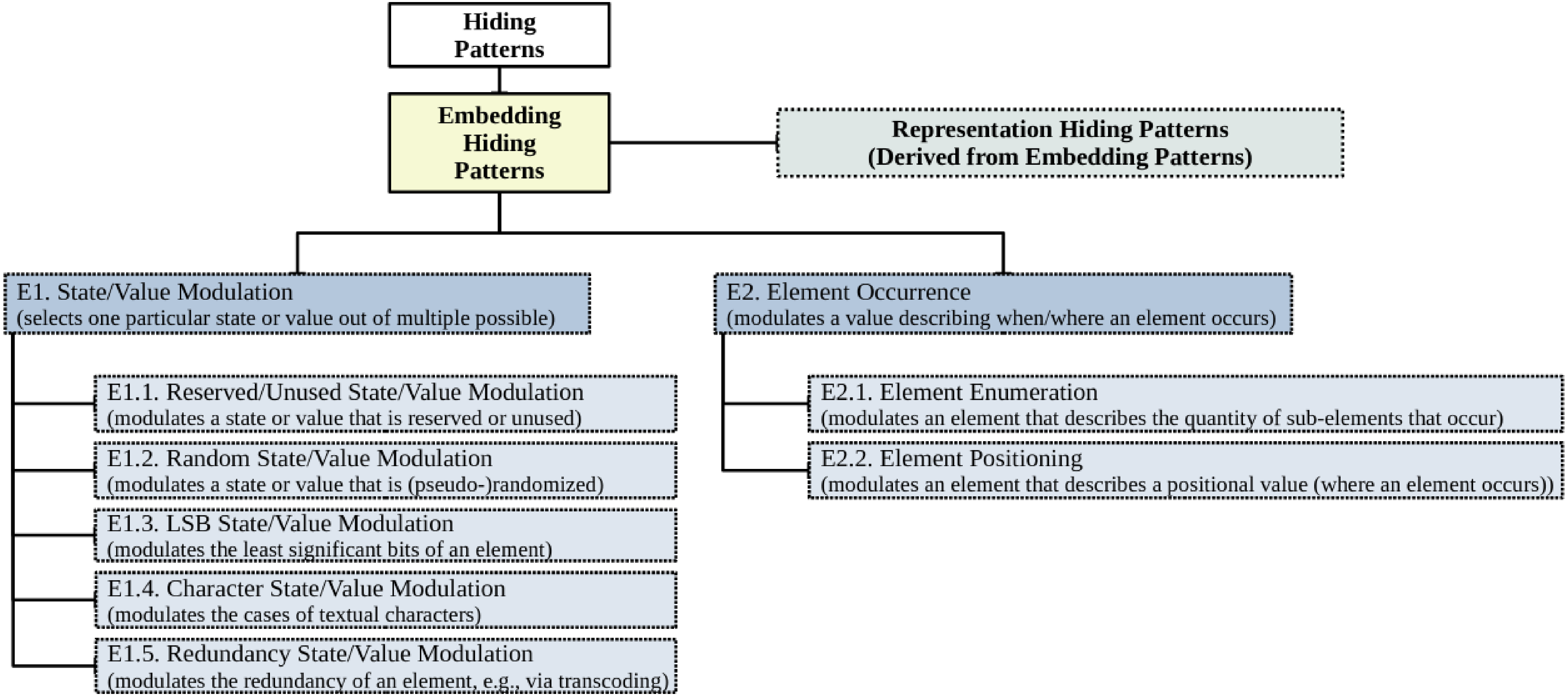
1. Sender **relocates a VM** (e.g., from Europe to Australia, using commands sent through the State/Value Modulation pattern).
2. Receiver **observes the RTT to the VM**, i.e., measures the temporal location (i.e., temporal position) of packets (Element Positioning pattern).

Solution: Differentiate between **Embedding** and **Representation** (Extraction) patterns.

- **Embedding Patterns** describe how secret information is embedded into a cover object, such as an image file or a network packet.
- **Representation Patterns** describe how the secret information is represented in the cover object.

[1] D. Spiekermann, J. Keller, T. Eggendorfer: Towards Covert Channels in Cloud Environments, Proc. IWDW, Springer, 2017.

Generic Taxonomy



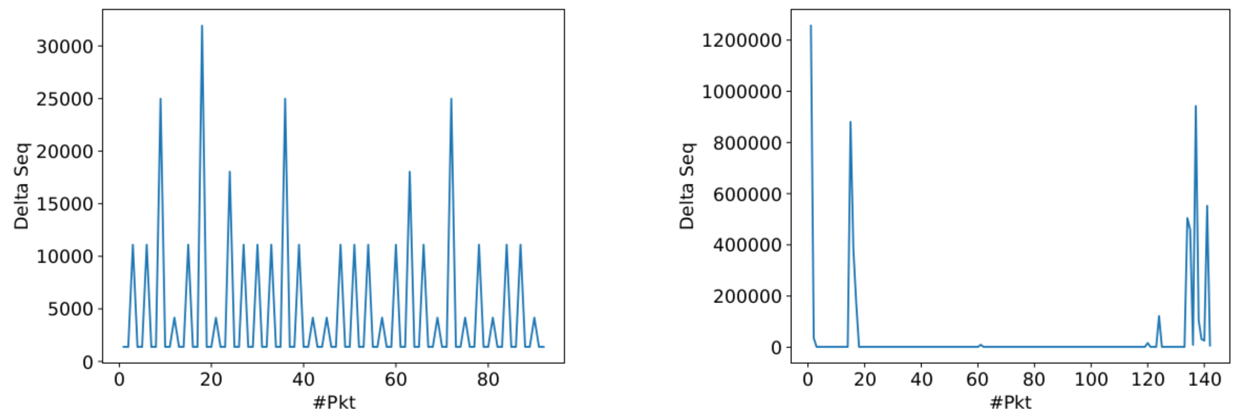
S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2022.

Example 1: Network Steganography

Sample Method: Encode secret signal by mimicking TCP retransmissions (doubling selected packets).

<u>Hiding Pattern:</u>

E2.1n1. Network Element Enumeration
(we modulate the number of duplicate packets)



(a) Typical Covert channel traffic (b) Regular traffic (Germany 2)

Fig. 3: Comparison: covert - regular: Δ values between retransmissions

Fig.: S. Zillien, S. Wendzel: Detection of Covert Channels in TCP Retransmission, in Proc. NordSec, Springer, 2018.

S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2022.

Example 2: CPS Steganography

Sample Method: Encode secret signal by influencing response time of a CPS actuator [1].

Hiding Pattern:

E2.2c1. CPS Element Positioning
(we "position" the actuator action in time)

[1] A. Herzberg, Y. Kfir: *The Leaky Actuator: A Provably-covert Channel in Cyber Physical Systems*, in Proc. ACM CPS-SPC 2019.

S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2022.

Example 3: Filesystem Steganography

Sample Method: Placing secret data in bytes of unused filesystem blocks.

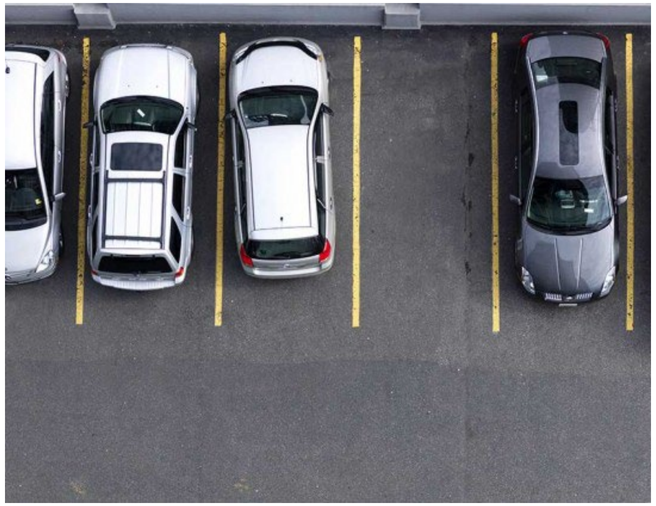


Fig: bloomberg.com/Getty Images

Hiding Pattern:

E1.1f1. Filesystem Reserved/Unused State/Value Modulation
(we modulate the content of unused blocks)

S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2022.

Example 4: Text Steganography

Sample Method: Modifying the features of characters in text (e.g., underlining, font type, color).

Hiding Pattern:

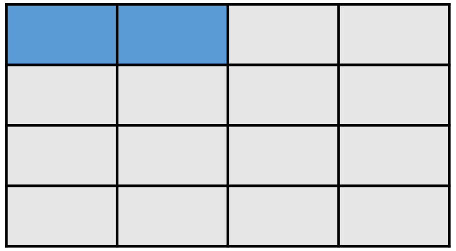
E1.4t1. Text Character State/Value Modulation
(we modulate the features (but not the position, case or number) of characters)

S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2022.

Example 5: Digital Media Steganography

Initial sub-taxonomy available (requires multiple follow-up publications).

Sample Method: Inserting a blue screen or blue pixel at some location in a video or image file.



<u>Hiding Pattern:</u>

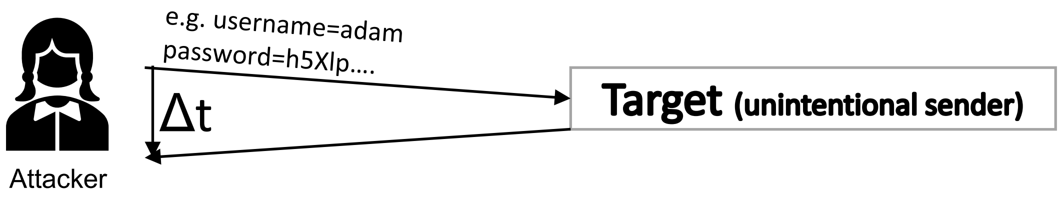
E2.2d1. Digital Media Element Positioning
(we modulate the position of the element (blue screen/pixel) in a temporal or spatial way)

S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2022.

Example 6: Side Channels

A **side** channel is nothing else but a **passive covert** channel **without sending-intention**.

We can describe them through **representation patterns**.



Sample Method: A side channel might leak secret data through the response time for web-based requests [1].

Pattern: **R2.2n1. Network Element Positioning**.

[1] S. Schinzel: *An Efficient Mitigation Method for Timing Side Channels on the Web*, in Proc. COSADE 2011.

S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2022.

Example 7: Traffic Obfuscation

Sample Method: Packet Size Padding [1]

Pattern: **E2.1n1. Network Element Enumeration**

(we simply add more byte elements to the padding)

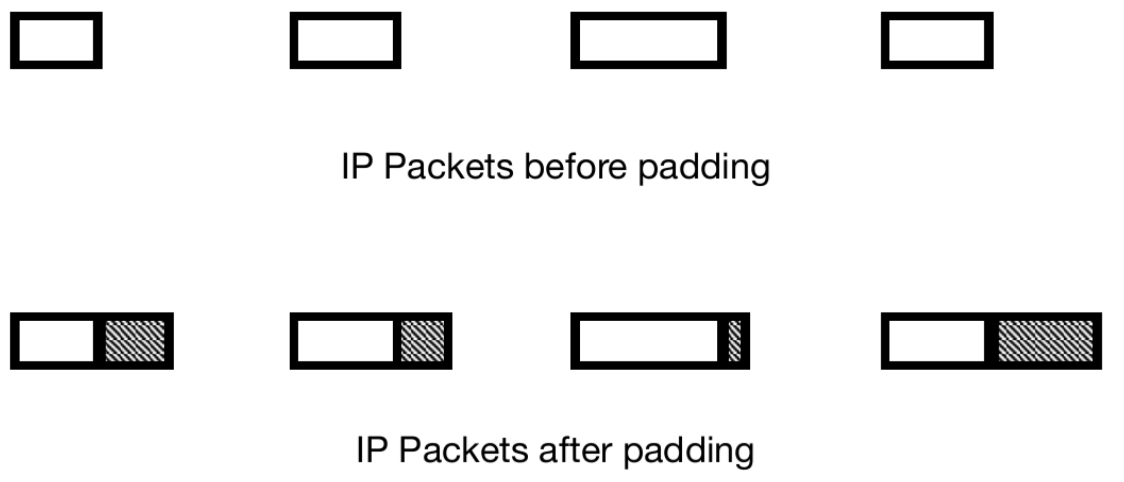


Figure 5.2: Padding network packets to de-identify packet sizes.

Fig.: W. Mazurczyk et al.: *Information Hiding in Communnication Networks*, Wiley-IEEE, 2016.

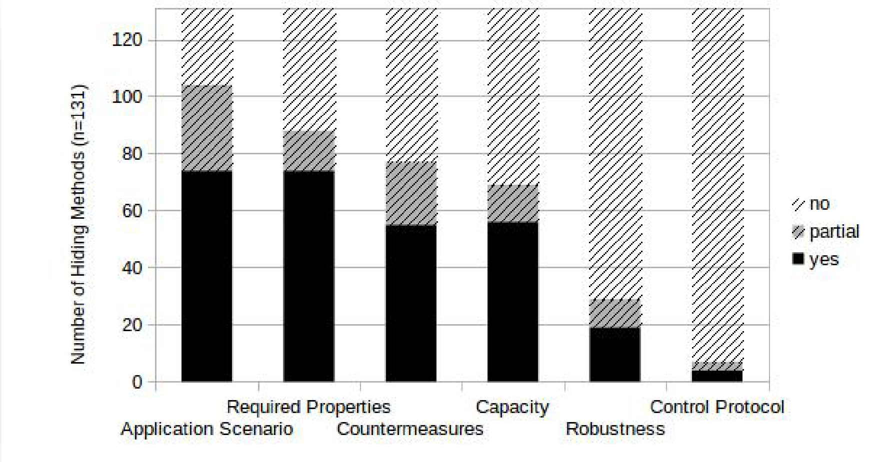
[1] K. P. Dyer et al.: *Peek-a-boo, I still see you: Why efficient traffic analysis countermeasures fail,* 2012 IEEE Symposium on Security and Privacy. IEEE, 2012.

S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2022.

Hochschule Worms
University of Applied Sciences

Problem 7: Where do all the details go?

Fig.: S. Wendzel, W. Mazurczyk, S. Zander: [Unified Description for Network Information Hiding Methods](), in: Journal of Universal Computer Science, 2016.



- There is no „One-Size-Fits-All“ Solution!
- You can optimize a taxonomy either to cover a **broad** spectrum or to cover **details**, but both is almost infeasible.
- Our **multi-stage approach**:

Generic Taxonomy → **Domain-specific Taxonomy** → **Unified Description Method**

(clarify the **general idea behind a hiding method**)

(subsume a hiding method in a **particular domain**)

(**describe details of a hiding method** in a publication using **patterns** and a **unified structure** to aid **replicability** and **comparability** of research)

S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2022.

Problem 8: Will people really use it the right way?

Design Rules!

S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2022.

Problem 9: Backwards Compatibility

All hiding patterns defined since 2015 (mostly network steganography) can be represented in the new taxonomy (see paper for details)!

TABLE II
INTEGRATION OF THE ORIGINAL **TIMING** PATTERNS INTO THE NEW TAXONOMY. **P**: PATTERN, **HP**: HYBRID P

Pattern of Existing Taxonomy	Ref.	Short Description	Generic / Sub-tax. Emb. Pattern	Type	Comments
PT1. Inter-packet Times (former: Inter-arrival Times)	[2], [5]	The CS alters the timing intervals between network PDUs (inter-packet times) to encode hidden data.	**E2.2. Element Positioning / E2.2n1.**	**P**	Inter-packet times are represen occurrences in time.Instead of directly, each element is placed
PT2. Message Sequence Timing	[2]	The CS encodes secret symbols through the timing of message sequences.	**E2.1. Element Enumeration / E2n1.**	**P**	The number of occurrences of a secret symbol (usually follow
PT3. Rate/Throughput	[5]	The CS alters the data rate of traffic.	**E2.2. Element Positioning / E2.2n1.**	**P**	Elements (packets) are position other, or not (similar to PT1).
PT10. Artificial Loss	[2]	The CS signals secret symbols through artificial loss of transmitted PDUs.	**E2. Element Occurrence / E2n1.**	**P**	Which message is lost depend lost, i.e., which elements occur
PT11. Message Ordering (former: PDU Order/ Manipulated Message Ordering)	[2], [5], [52]	The CS encodes data using a synthetic PDU order.	**E2.2 Element Pos.** (& **E1. State/Value Modul.**) / **E2.2n1** (& **E1n1.**)	**P / HP**	The PDUs are located at spe packets are emitted by CS (in CS-router), their sequence num
PT12. Retransmission	[5]	The CS re-transmits previously sent or received PDUs.	**E2.1. Element Enumeration / E2.1n1.**	**P**	An element (packet) occurs mu
PT13. Frame Collisions (former: PDU Corruption/Loss)	[2], [5]	The CS causes artificial frame collisions to embed secret symbols by letting two packets occur closely behind each other.	**E2.2. Element Positioning / E2.1n1.**	**P**	Two elements (packets) are pos slot, thus, causing a collision.
PT14. Temperature	[2]	The CS influences a third-party node's clock skew, e.g., using burst traffic.	-	-	Specific indirect and hybrid hi aspects of an embedding and ther mixes network steganogra (CPU temperature).
PT15. Artificial Reconnections	[54]	The CS employs artificial (forced) reconnections to transfer secret messages.	**E1. State/Value Modulation & E2.2 Element Positioning**	-	Reconnects are hybrid events a (e.g., TCP FIN) or commands a timing (element positioning as the time of reconnection is together with a sender's addr represents an indirect covert ch the reconnections of third-party
PT16. Artificial Resets	[55]	The CS causes a connection reset of third-party nodes, whose connection states are observed by one or more CRs.	**E1. State/Value Modulation & E2.2 Element Positioning**	-	See PT15, above. Resets are c

TABLE III
INTEGRATION OF THE ORIGINAL **STORAGE** PATTERNS INTO THE NEW TAXONOMY. **P**: PATTERN, **HP**: HYBRID PATTERN.

Pattern of Existing Taxonomy	Ref.	Short Description	Generic / Sub-tax. Emb. Pattern	Type	Comments
PS1. Size Modulation	[5]	The CS uses the size of a header element or a PDU to encode a hidden message.	**E2.1. Element Enumeration / E2.1n1.**	**P**	A packet's size is increased by adding more sub-elements
PS2. Sequence	[5]	The CS alters the sequence of header/PDU elements to encode hidden information.	**E2.2. Element Positioning / E2.2n1.**	**P**	
PS2.a. Position	[5]	The CS alters the position of a given (single) header/PDU element to encode hidden information.	**E2.2. Element Positioning / E2.2n1.**	**P**	
PS2.b. Number of Elements	[5]	The CS encodes the hidden information by the number of header/PDU elements transferred.	**E2.1. Element Enumeration / E2n1.**	**P**	
PS3. Add Redundancy	[5]	The CS creates a new space within a given header element or within a PDU to hide data into.	**E2.1. Element Enum. & E1.1. Reserved/Unused State/Value Modul. / E2.1n1. & E1.1n1.**	**HP**	
PS10. Random Value	[5]	The CS embeds hidden data in a header element containing a (pseudo) random value.	**E1.2. Random State/Value Modulation / E1.2n1.**	**P**	
PS11. Value Modulation	[5]	The CS selects one of the *n* values that a header element can contain to encode a hidden message.	**E1. State/Value Modulation / E1n1.**	**P**	
PS11.a. Case Modulation	[5]	The CS uses case-modification of letters in header elements to encode hidden data.	**E1.4. Character State/Value Modulation / E1.4n1.**	**P**	
PS11.b. LSB Modulation	[5]	The CS uses the LSB of header elements to encode the hidden data.	**E1.3. LSB State/Value Modulation / E1.3n1.**	**P**	
PS11.c. Value Influencing	[53]	The CS (directly or indirectly) influences values so that a CR can determine the value. The value is influenced by altering another value or surrounding networking conditions.	Depends on the implementation (temporal and spatial actions necessary).	-	
PS12. Reserved/ Unused	[5]	The CS encodes hidden data into a reserved or unused header/PDU element.	**E1.1 Reserved/ Unused State/Value Modul. / E1.1n1.**	**P**	

TABLE IV
INTEGRATION OF THE ORIGINAL **STORAGE** PATTERNS FOR **PAYLOAD-BASED METHODS** INTO THE NEW TAXONOMY. [*] INDICATES PATTERNS WHICH WERE ADDED FOR COMPLETENESS BUT WERE NOT OFFICIALLY DEFINED. **P**: PATTERN, **HP**: HYBRID PATTERN.

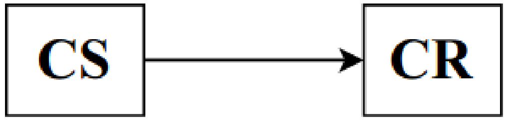
Pattern of Existing Taxonomy	Ref.	Short Description	Generic / Sub-tax. Emb. Pattern	Type	Comments
PS20. Payload Field Size Modulation (derived from PS1)	[52]	The CS uses the payload size to encode a hidden message.	**E2.1. Element Enumeration / E2n1.**	**P**	Equals original pattern PS1. Size Modulation, but with a focus on payload.
PS21. User-data Corruption	[52]	The CS blindly overwrites a packet's payload.	**E1. State/Value Modulation / E1n1.**	**P**	Special case of **E1** being applied to network payload; the fact that the overwriting is *blind* does not make it an own pattern (in comparison to, e.g., **E1.1.** or **E1.2.** that focus on specific types of cover data). Moreover, example cases of [52] represent hybrid methods.
PS30. Modify Redundancy	[52]	The CS exploits the redundancy of user-data by transcoding them so that a free space for secret data is obtained (and then filled).	**E1.5. Redundancy State/Value Modul. & E1.1. Reserved/Unused State/Value Modul. / E1.5n1. & E1.1n1.**	**HP**	First, an element's values are modified (e.g., by transcoding or compression) so that free space is created in a packet (**E1.5**); the space is then filled with secret data (**E1.1**).
PS31. User-data Value Modulation and Reserved/Unused	[52]	The CS performs a modulation of payload values.	**E1. State/Value Modul. / E1.1. Reserved/Unused State/Value Modul. / E1n1. & E1.1n1.**	**P**	Special case of **E1./E1.1.** being applied to payload elements.
PS32. User-data Sequence Modulation (plus sub-patterns)	[*]	The CS performs a PS2/PS2.a/PS2.b-like sequence modulation of payload fields.	**E2.1. Element Enumeration** *-or-* **E2.2. Element Positioning / E2.2n1.** *-or-* **E2.1n1.** *-or-* **E2.1n1.**	**P**	Special case of the original patterns PS2/PS2.a/PS2.b being applied to payload elements.
PS33. User-data Random Value Modulation	[*]	The CS performs a PS10-like random value modulation of payload fields.	**E1.2. Random State/Value Modulation / E1.2n1.**	**P**	Special case of the original pattern PS10 being applied to payload elements.

S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2022.

Alright, but some hiding techniques are famous indirect/side channels!

We worked out a taxonomy for such techniques too!

- Patterns to describe the **architecture** of **indirect/side** channels.
- Utilize the generic taxonomy's patterns to describe the **details**.



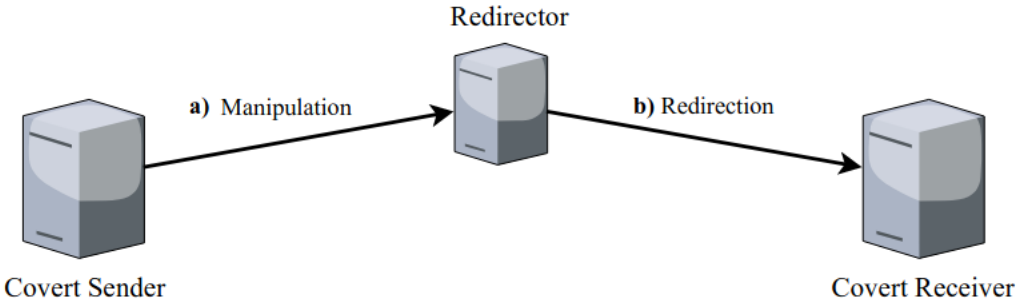
(a) Direct Covert Channel

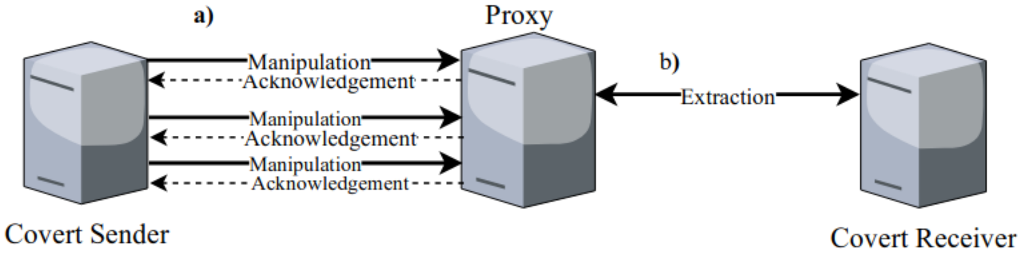
(b) Indirect Covert Channel

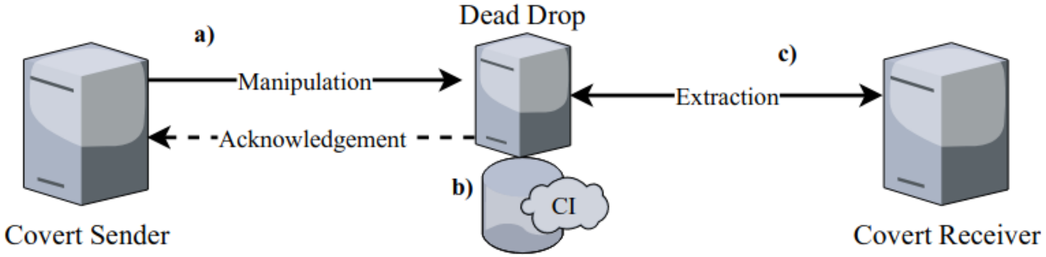
T. Schmidbauer, S. Wendzel: *SoK: A Survey on Indirect Network Covert Channels*, ASIA CCS, 2022.

Alright, but some hiding techniques are indirect!

Essentially three patterns:







T. Schmidbauer, S. Wendzel: *SoK: A Survey on Indirect Network Covert Channels*, ASIA CCS, 2022.

Hochschule Worms
University of Applied Sciences

What else can be done with the taxonomy?

- Evaluation of what’s **new** (or is there already something like that?).
- Categorization and Description of what’s **there**.
- Identification of **gaps** (esp. through the unified description method)

Now, let‘s pick a sample pattern …

E2.2 Element Positioning (PT1. Inter-packet Times)

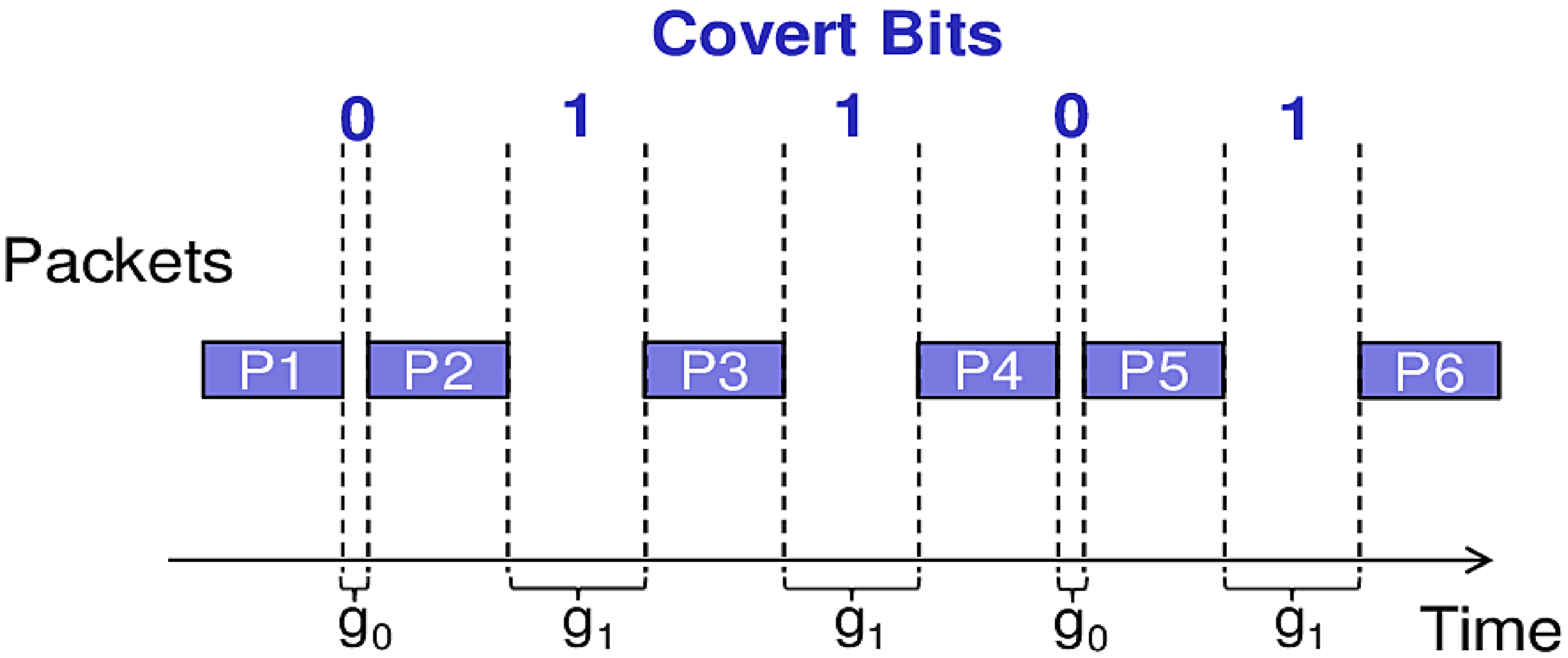
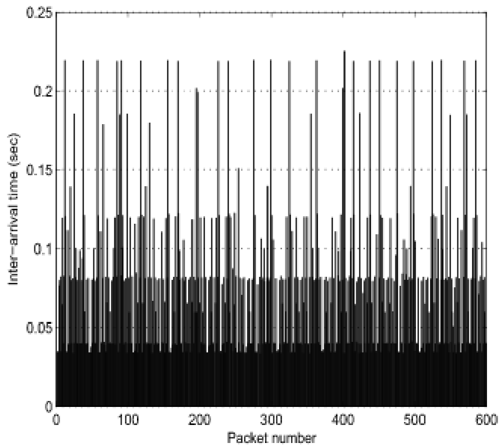
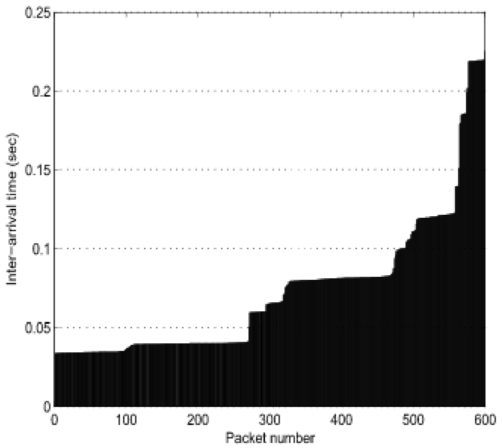


Fig.: W. Mazurczyk, S. Wendzel, S. Zander et al.: Information Hiding in Communication Networks, WILEY-IEEE, 2016, Chapter 3.

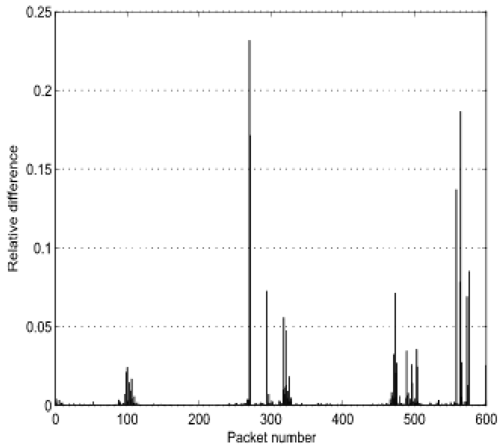
Inter-packet Times Pattern: Detection by Cabuk et al.: ε-similarity





Introduced by Cabuk et al. in [1].

1. Record all inter-packet gaps of a flow.
2. Sort all inter-packet times of a flow.
3. For consecutive values T_1 and T_2:
   calculate relative difference $\lambda_i = \frac{|T_{i+1} - T_i|}{T_i}$.
4. Calculate the percentage of λ values of a given flow that are below the threshold ε.



[1] S. Cabuk et al.: IP Covert Channel Detection, in: Transactions on Information and System Security (TISSEC), ACM, 2009.

Inter-packet Times Pattern: Detection by Cabuk et al.: Compressibility Score

Introduced by Cabuk et al. [1]:

1. Record a window of n inter-packet times of a flow $\Delta_{t_1}, \ldots, \Delta_{t_n}$.
2. Encode the IPG in an ASCII string S with *rounded* values to aid compressibility, e.g. "A20A20A19B30B29C31...", where the upper-case latter A, B, C, … indicates the number of leading zeros behind the comma (A=no zeros, B=one zero etc.)
   and the following digits represent rounded IPGs.
3. Compress S with a compressor $\mathfrak{I}$ (e.g. *gzip*): $C = \mathfrak{I}(S)$.
4. Use $\kappa = \frac{|S|}{|C|}$ as an indicator for the presence of a covert channel.

[1] S. Cabuk et al.: IP Covert Channel Detection, in: Transactions on Information and System Security (TISSEC), ACM, 2009.

Replicating Experiments

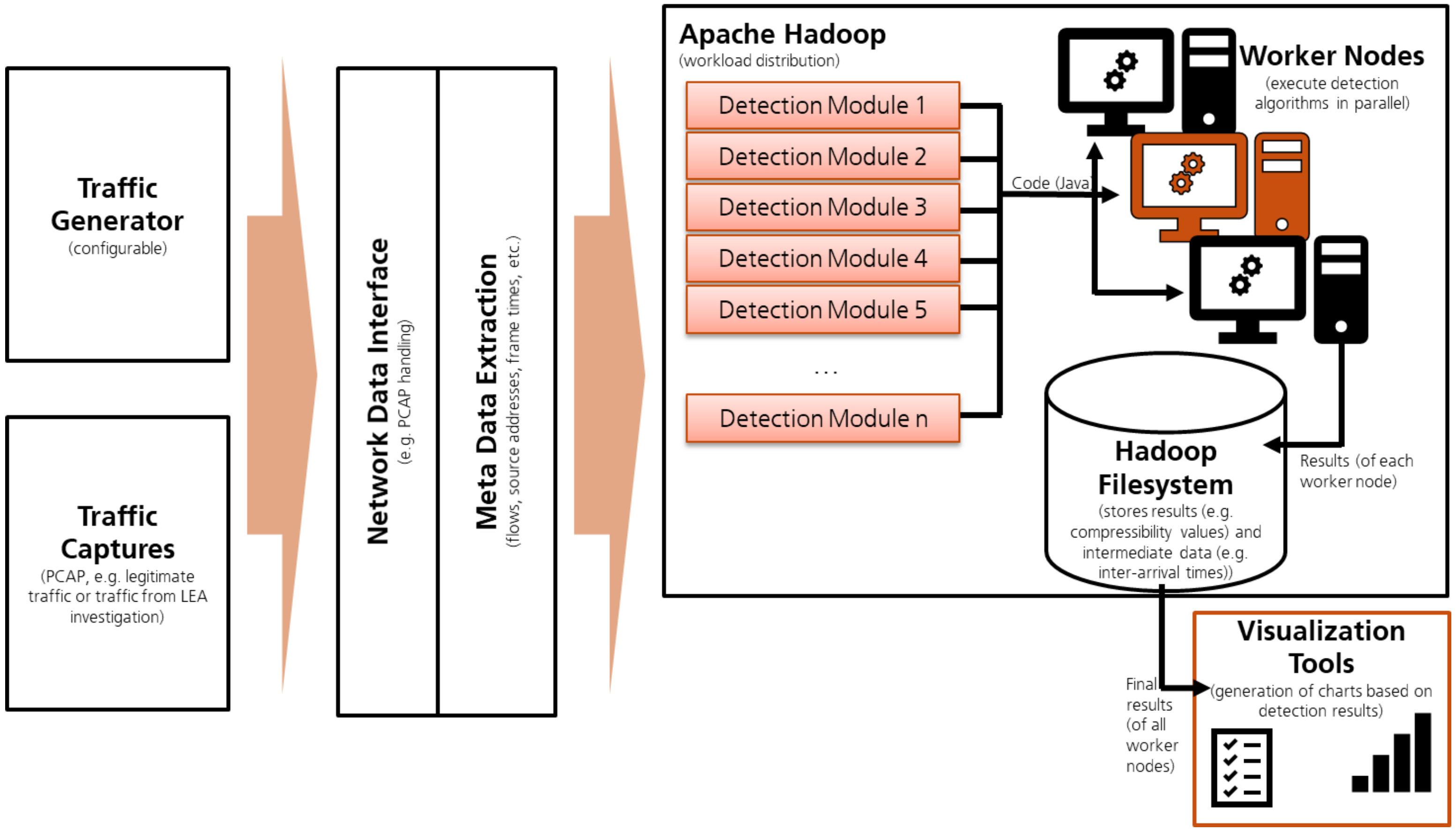
- Almost nobody seems to replicate experimental results of other researchers in the covert channel domain.
  - Manifold reasons, e.g., it is difficult to publish replication studies, no data available, no code available, no time, …

- **But:** How trustworthy are provided results during review and in papers?
  - Conference and journal quality is a good indicator, but not perfect.
  - Publisher name is not a good indicator, e.g., Springer, IEEE, ACM, … they all feature low-quality papers.

cf. S. Wendzel, L. Caviglione, W. Mazurczyk, J.-Francois Lalande: Network Information Hiding and Science 2.0: Can it be a Match?, *Int. Journal of Electronics and Telecommunications*, Vol. 63(2), pp. 217-222, 2017.

Replicating Experiments on Covert Channels

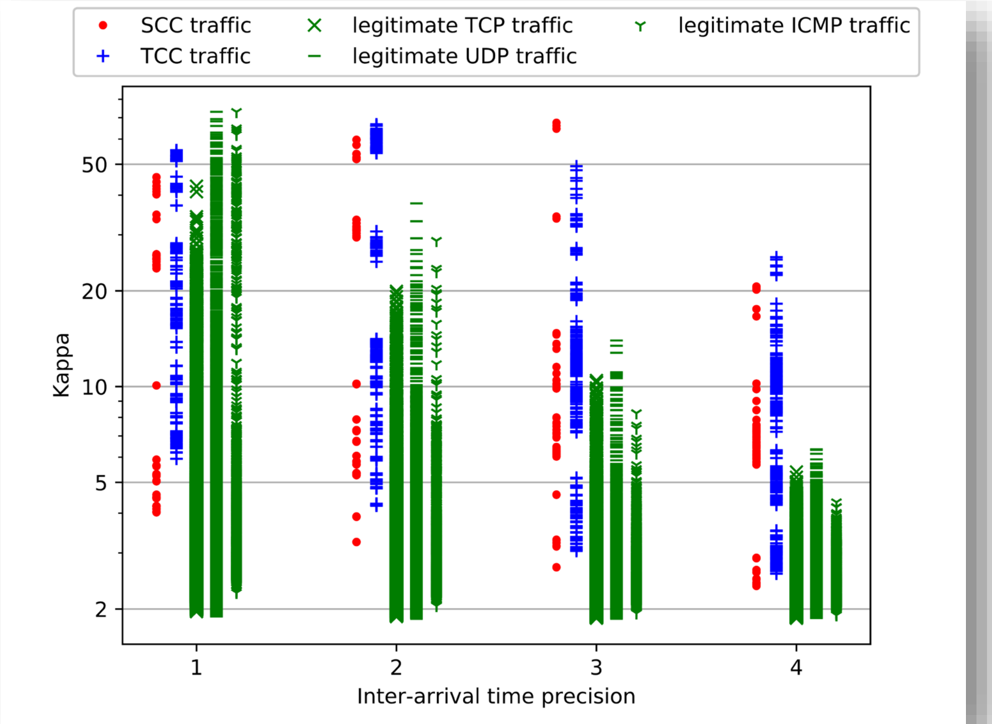
WoDiCoF (*Worms Distributed Covert Channel Detection Framework*)



R. Keidel, S. Wendzel, S. Zillien et al.: WoDiCoF - A Testbed for the Evaluation of (Parallel) Covert Channel Detection Algorithms, J.UCS, Vol. 24(5), 2018.

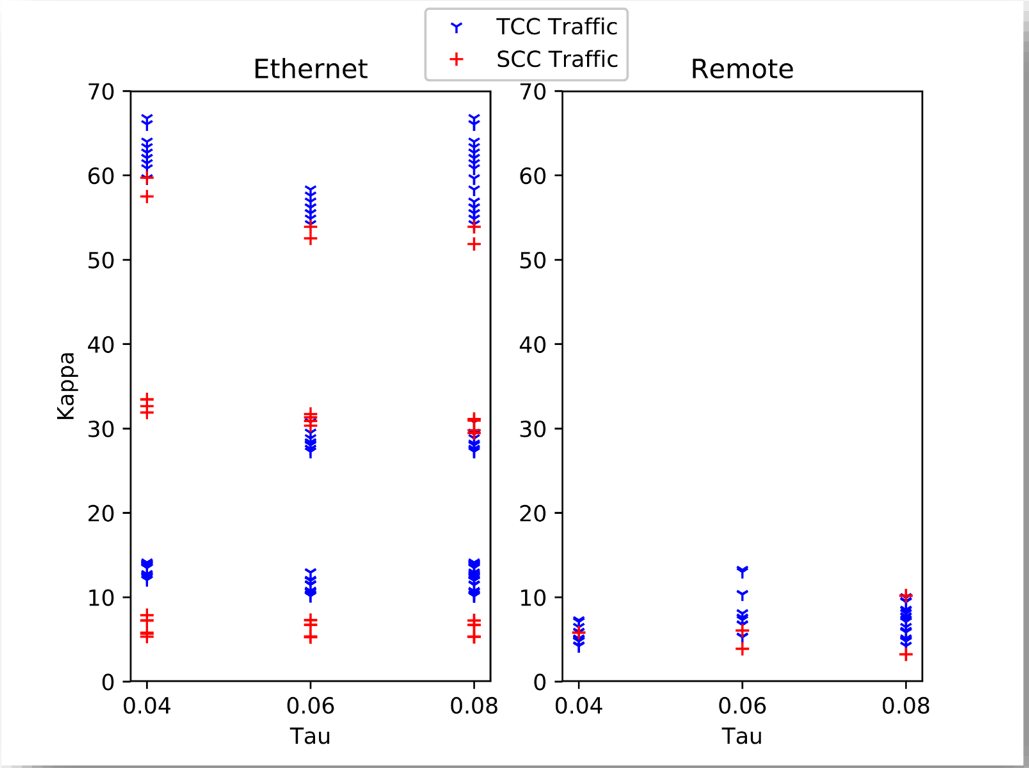
Replication Study: Compressibility of Cabuk et al.

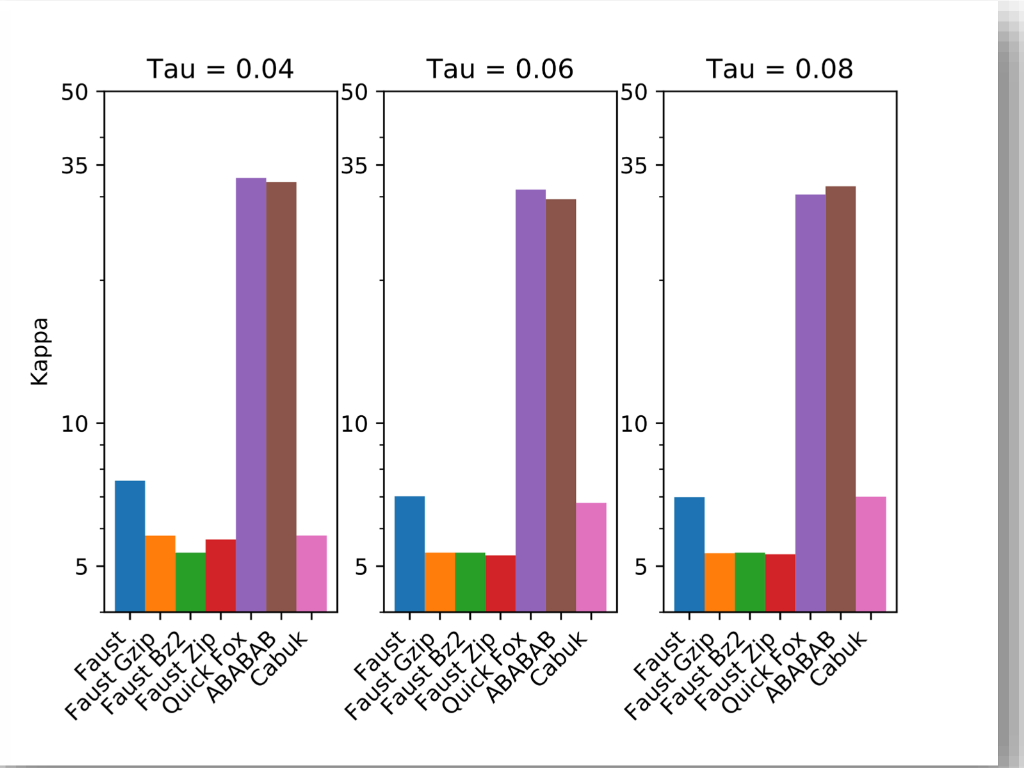
- Let’s see how the precision of the measured IAT values influences κ …



R. Keidel, S. Wendzel, S. Zillien et al.: WoDiCoF - A Testbed for the Evaluation of (Parallel) Covert Channel Detection Algorithms, J.UCS, Vol. 24(5), 2018.

Replication Study: Compressibility of Cabuk et al.





R. Keidel, S. Wendzel, S. Zillien et al.: WoDiCoF - A Testbed for the Evaluation of (Parallel) Covert Channel Detection Algorithms, J.UCS, Vol. 24(5), 2018.

Replication Study: Compressibility of Cabuk et al.

Ethernet != Ethernet

- For this reason, future evaluations should be even more precise!

Ethernet IPG[1]

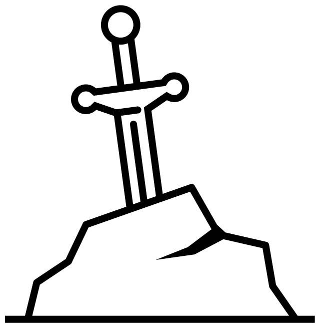
Ethernet variant	Minimum transmitted IPG	Minimum received IPG
10 Mbit/s Ethernet	9.6 µs	4.7 µs (47 bit times)
100 Mbit/s (Fast) Ethernet	0.96 µs	0.96 µs (96 bit times)[3][*dubious – discuss*]
Gigabit Ethernet	96 ns	64 ns (64 bit times)
2.5 Gigabit Ethernet	38.4 ns	16 ns (40 bit times)
5 Gigabit Ethernet	19.2 ns	8 ns (40 bit times)
10 Gigabit Ethernet	9.6 ns	4 ns (40 bit times)
25 Gigabit Ethernet	3.84 ns	1.6 ns (40 bit times)
40 Gigabit Ethernet	2.4 ns	200 ps (8 bit times)
50 Gigabit Ethernet	1.92 ns	160 ps (8 bit times)
100 Gigabit Ethernet	0.96 ns	80 ps (8 bit times)
200 Gigabit Ethernet	0.48 ns	40 ps (8 bit times)
400 Gigabit Ethernet	0.24 ns	20 ps (8 bit times)

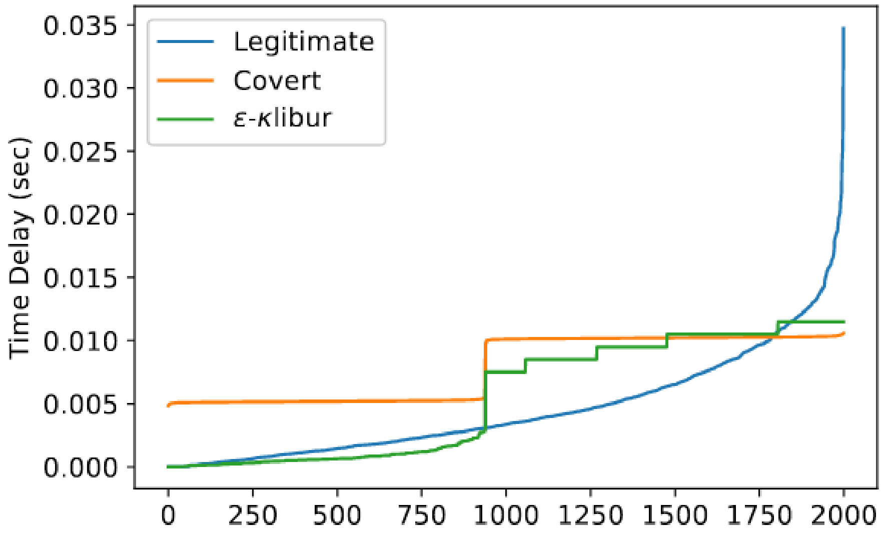
Fig.: Wikipedia (https://en.wikipedia.org/wiki/Interpacket_gap)

ε-κlibur

- Previously introduced **ε-similarity** and **compressibility score** (κ) were **cited by ca. 950 papers** so far. Thanks to *WoDiCoF* we know both methods far from perfect, so a logical next step was to **tailor a circumventing covert channel.**

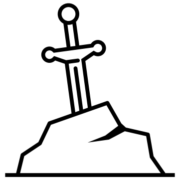
- Introduced **ε-κlibur**: more different inter-arrival times and made sure that slope is close to legitimate traffic.
- No reduced bitrate in comparison to traditional channels!





S. Zillien, S. Wendzel: Weaknesses of popular and recent covert channel detection methods and a remedy, IEEE Trans. Dependable and Secure Computing (TDSC), 2023.

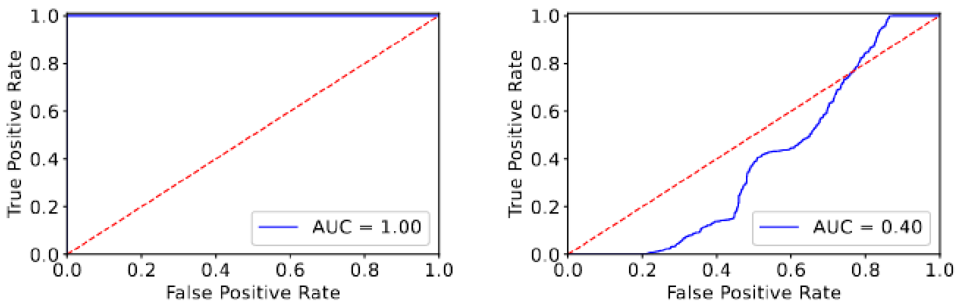
ε-κlibur (Cont.)



ε-similarity →

Compressibility

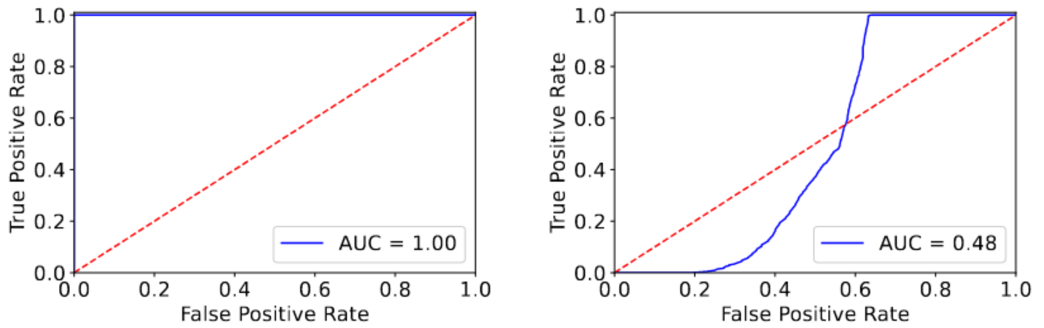
↘



(a) ROC curve of original covert channel

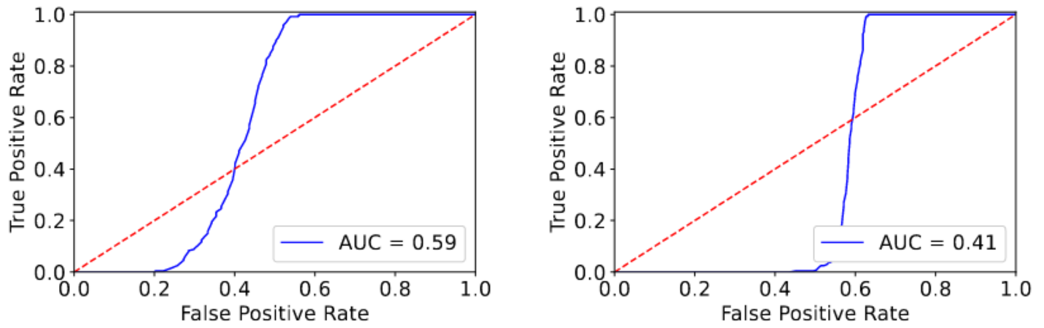
(b) ROC curve of ϵ-κlibur

Fig. 7. ROC curve comparison for the compressibility score



(a) Original covert channel (mixture of all configurations)

(b) ϵ-κlibur (mixture of all configurations)



(c) ϵ-κlibur with $\tau = 5\ ms$

(d) ϵ-κlibur with $\tau = 30\ ms$

Fig. 5. ROC curve comparison for ϵ-similarity

S. Zillien, S. Wendzel: Weaknesses of popular and recent covert channel detection methods and a remedy, IEEE Trans. Dependable and Secure Computing (TDSC), 2023.

ε-κlibur vs. GAS (Current #1) – in press!

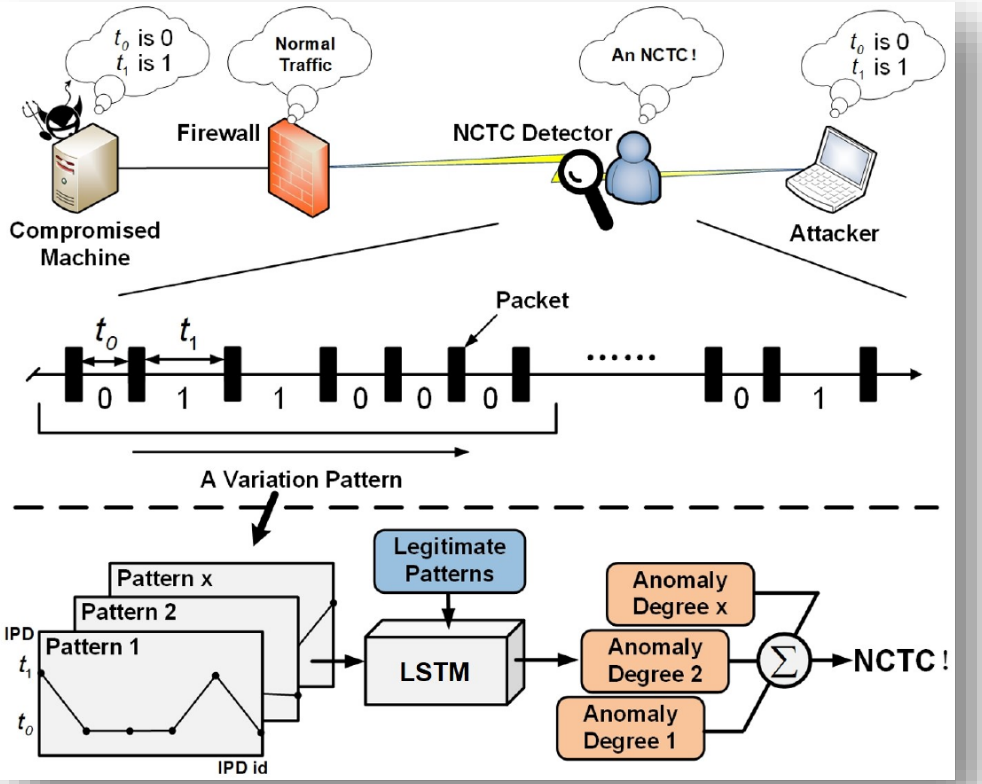


Fig.: [1]

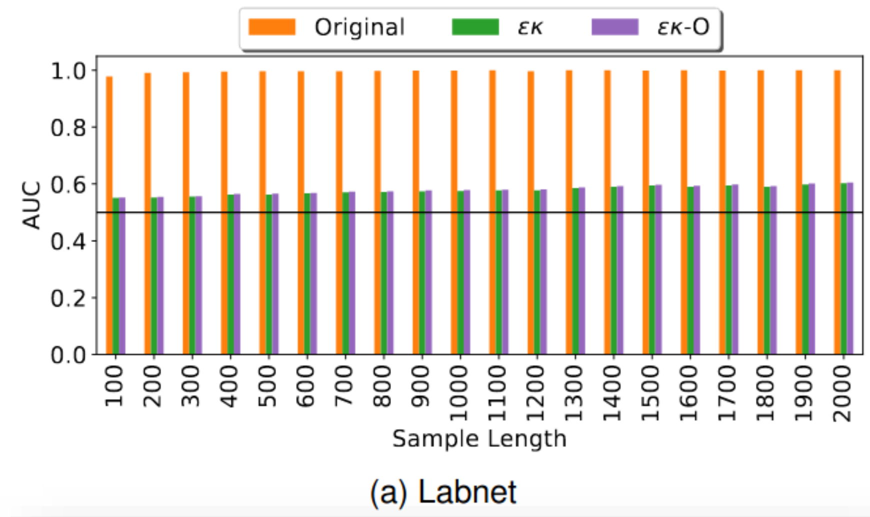


Fig.: [2]

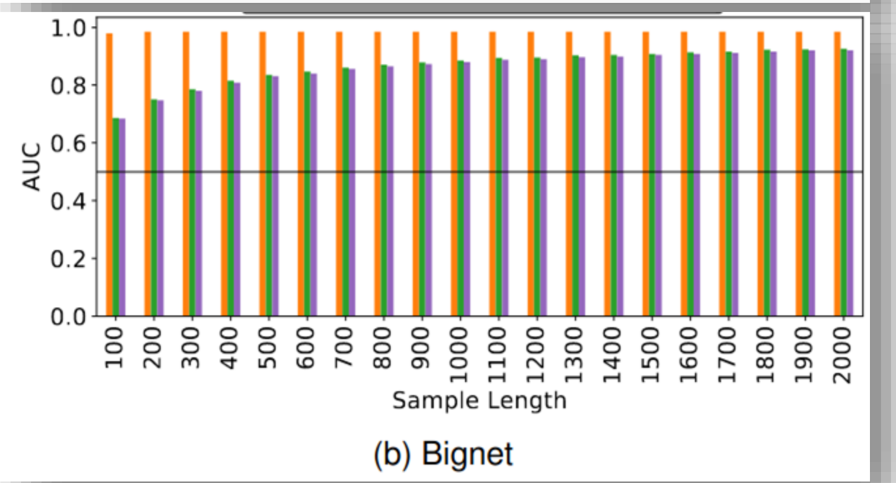


Fig.: [2]

[1] H. Li, T. Song, Y. Yang: *Generic and Sensitive Anomaly Detection of Network Covert Timing Channels*, in: IEEE Trans. Dependable & Secure Computing, 2022.

[2] S. Zillien, S. Wendzel: *Weaknesses of popular and recent covert channel detection methods and a remedy*, IEEE Trans. Dependable & Secure Computing, 2023.

ε-κlibur vs. SnapCatch

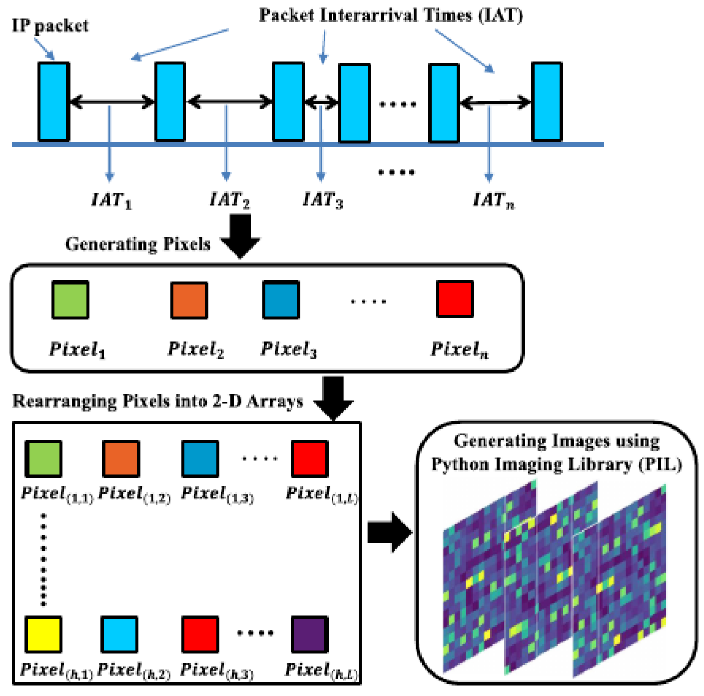


FIGURE 3. Illustration of inter-arrival time images.

Fig.: [1]

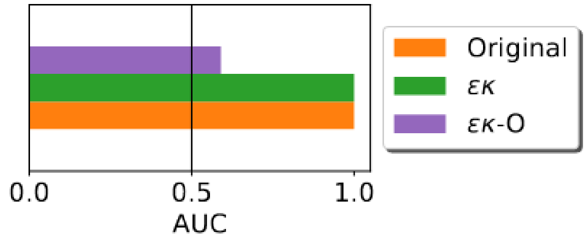


Fig. 13. AUC comparison for SnapCatch, orig. CC vs. ϵ-κlibur vs. ϵ-κlibur-O

Fig.: [2]

[1 S. Al-Eidi, O. Darwish, Y. Chen, G. Husari: SnapCatch: Automatic detection of covert channels using image processing and machine learning, in: IEEE ACCESS, 2021.
[2] S. Zillien, S. Wendzel: *Weaknesses of popular and recent covert channel detection methods and a remedy*, IEEE Trans. Dependable & Secure Computing, 2023.

What else can be done with a pattern?

Types of (Network) Covert Channels: History Covert Channels

- Known covert channels focus on the **present**, e.g., packets might contain secret data in their **current** payload.
- **History** covert channels optimize transmission sizes by transferring solely pointers to larger data chunks already seen somewhere.
- **Predictive** covert channels are a derivative of history channels but **anticipate upcoming** data they point to (e.g., anticipated regularly occurring network packets) [1].

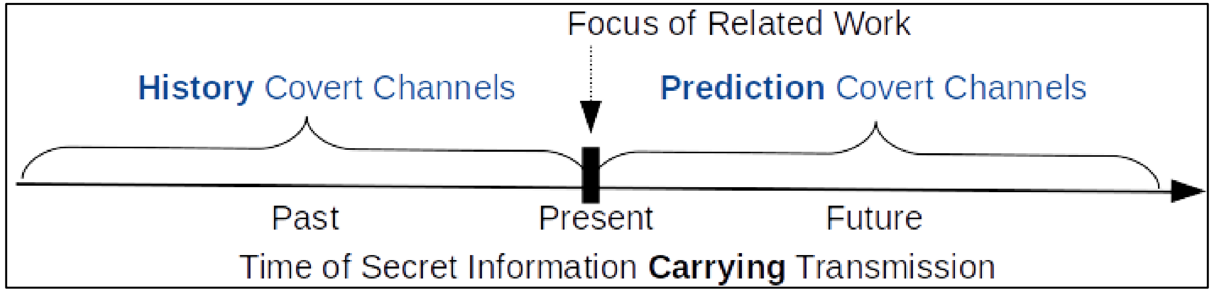


Fig.: [1]

[1] S. Wendzel, T. Schmidbauer, S. Zillien, J. Keller: *Did You See That? A Covert Channel Exploiting Recent Legitimate Traffic, ArXiv pre-print, Dec-2022. Available online: https://doi.org/10.48550/arXiv.2212.11850*

Types of (Network) Covert Channels: History Covert Channels (Cont.)

- History/prediction channels enable a new category of **fully-passive covert channels**, 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: *Did You See That? A Covert Channel Exploiting Recent Legitimate Traffic, ArXiv pre-print, Dec-2022. Available online:* https://doi.org/10.48550/arXiv.2212.11850

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

E2.2 Element Positioning (PT1. Inter-packet Times)

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].

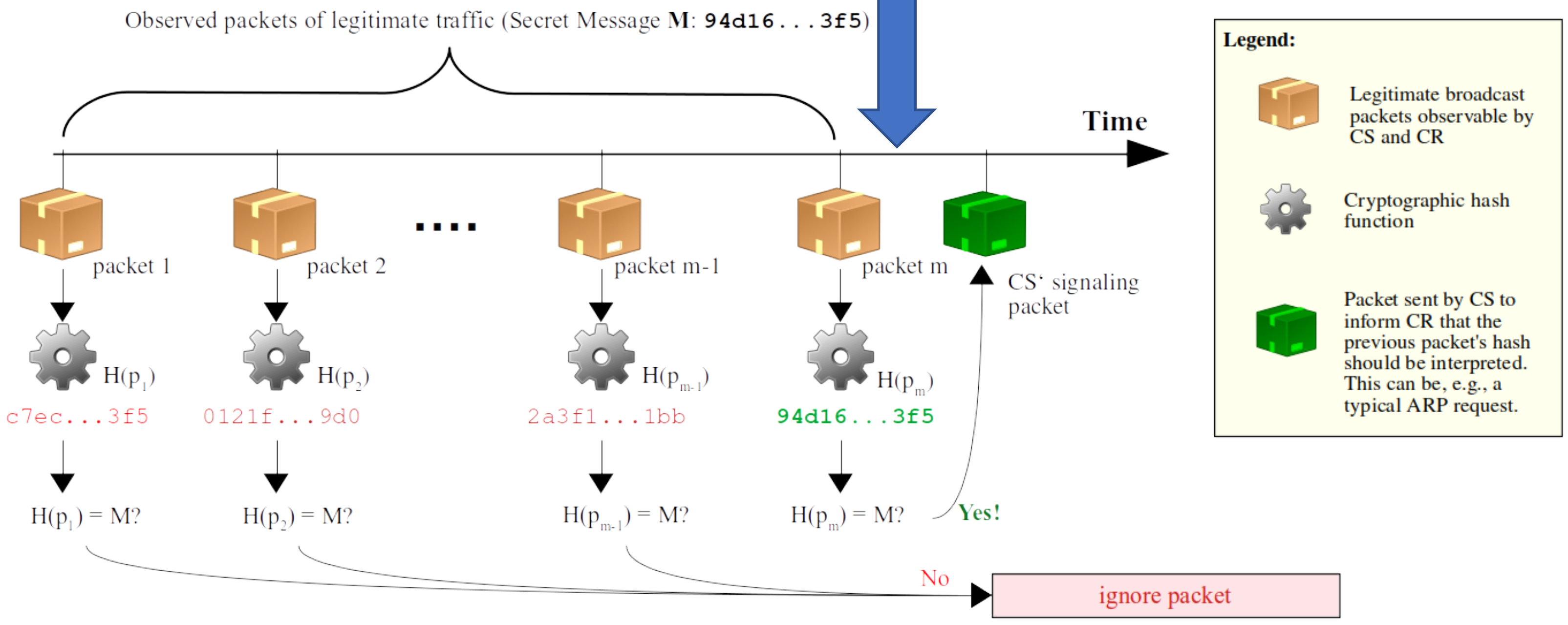
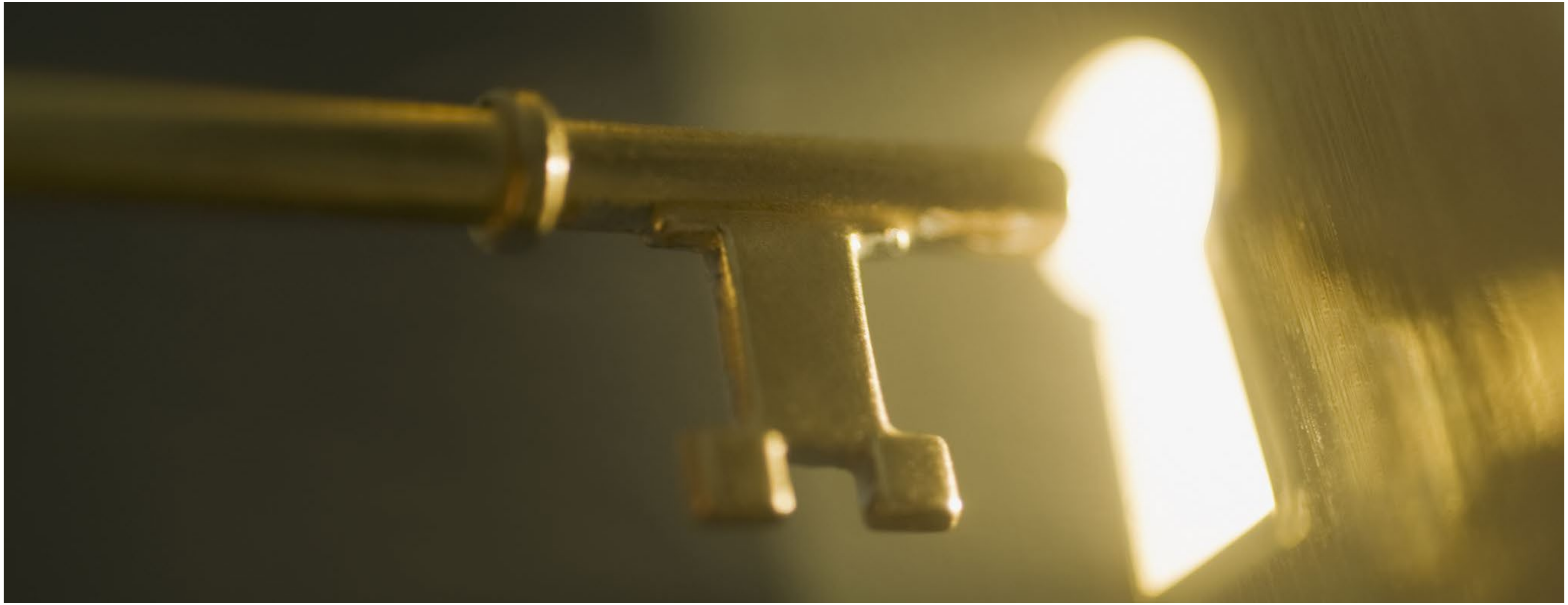


Fig.: [1]

[1] S. Wendzel, T. Schmidbauer, S. Zillien, J. Keller: *Did You See That? A Covert Channel Exploiting Recent Legitimate Traffic, ArXiv pre-print, Dec-2022. Available online:* *https://doi.org/10.48550/arXiv.2212.11850*

So What’s The Key Message?



A large fraction of information hiding research (network/text/CPS/filesystem/… steganography, side channel research, traffic flow watermarking, traffic obfuscation, censorship circumvention etc.) overlaps.

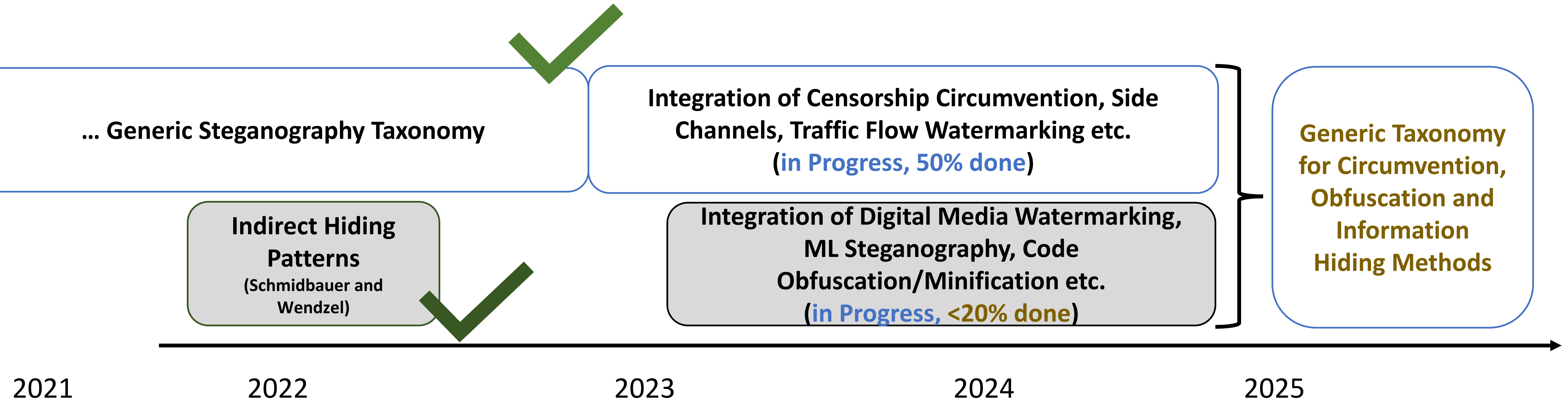
We need to find common terms to prevent scientific re-inventions.

One common taxonomy might be the solution!

Some More Take Aways

- New taxonomy allows categorizing methods of all information hiding domains (hopefully!).
- Solved several problems (applicability, provision of detail, handling of hybrid methods, design rules etc.) together with the scientific community.
- Capable of handling new variants (**ε-κlibur**) and entirely new classes of covert channels (e.g., history channels/**DYST**)!
- Multi-level approach:
  generic taxonomy → specific taxonomy → unified description method

Next Steps


… Generic Steganography Taxonomy
Integration of Censorship Circumvention, Side Channels, Traffic Flow Watermarking etc. (in Progress, 50% done)
Indirect Hiding Patterns (Schmidbauer and Wendzel)
Integration of Digital Media Watermarking, ML Steganography, Code Obfuscation/Minification etc. (in Progress, <20% done)
Generic Taxonomy for Circumvention, Obfuscation and Information Hiding Methods
2021
2022
2023
2024
2025

Interested?

Join us!

Papers are available (Open Access)

Generic Taxonomy:

S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann, C. Krätzer, K. Lamshöft, C. Vielhauer, L. Hartmann, J. Keller, T. Neubert, S. Zillien: ***A Generic Taxonomy for Steganography Methods***, pre-print, 2022.

https://PATTERNS.ZTT.HS-WORMS.DE

Other Papers: https://WWW.WENDZEL.DE

Hochschule Worms
University of Applied Sciences

Thank you for your kind attention!

wendzel@hs-worms.de
https://www.WENDZEL.de