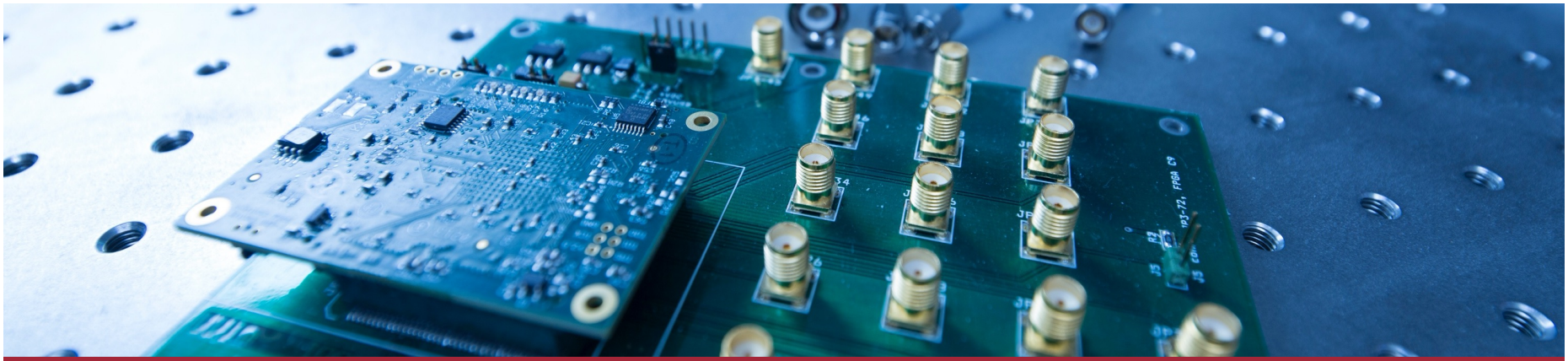
universität ulm



A Generic Taxonomy for Steganography Methods

Prof. Dr. habil. **Steffen Wendzel**

Institut für Organisation und Management
von Informationssystemen

A Generic Taxonomy for Steganography Methods (ACM Computing Surveys, 2025)

STEFFEN WENDZEL, Institute für Organisation und Management von Informationssystemen (OMI) / Kommunikations- und Informationszentrum (kiz), Ulm University Faculty of Engineering, Computer Science and Psychology, Ulm, Germany, Center for Technology & Transfer (ZTT), Hochschule Worms, Worms, Germany, and Mathematics & Computer Science, FernUniversität in Hagen, Hagen, Germany
LUCA CAVIGLIONE, IMATI CNR Genova, Genova, Italy
WOJCIECH MAZURCZYK, Warsaw University of Technology, Warszawa, Poland
ALEKSANDRA MILEVA, Goce Delcev University, Stip, North Macedonia
JANA DITTMANN, Otto von Guericke Universität Magdeburg, Magdeburg, Germany
CHRISTIAN KRÄTZER, Otto von Guericke Universität Magdeburg, Magdeburg, Germany
KEVIN LAMSHÖFT, Otto von Guericke Universität Magdeburg, Magdeburg, Germany
CLAUS VIELHAUER, University of Applied Sciences Brandenburg, Brandenburg an der Havel, Germany
LAURA HARTMANN, Center for Technology & Transfer (ZTT), Hochschule Worms, Worms, Germany and Mathematics & Computer Science, FernUniversität in Hagen, Hagen, Germany
JÖRG KELLER, Mathematics & Computer Science, FernUniversität in Hagen, Hagen, Germany
TOM NEUBERT, University of Applied Sciences Brandenburg, Brandenburg an der Havel, Germany
SEBASTIAN ZILLIEN, Ulm University Faculty of Engineering, Computer Science and Psychology, Ulm, Germany and Center for Technology & Transfer (ZTT), Hochschule Worms, Worms, Germany

Scientific Re-inventions in Cybersecurity

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

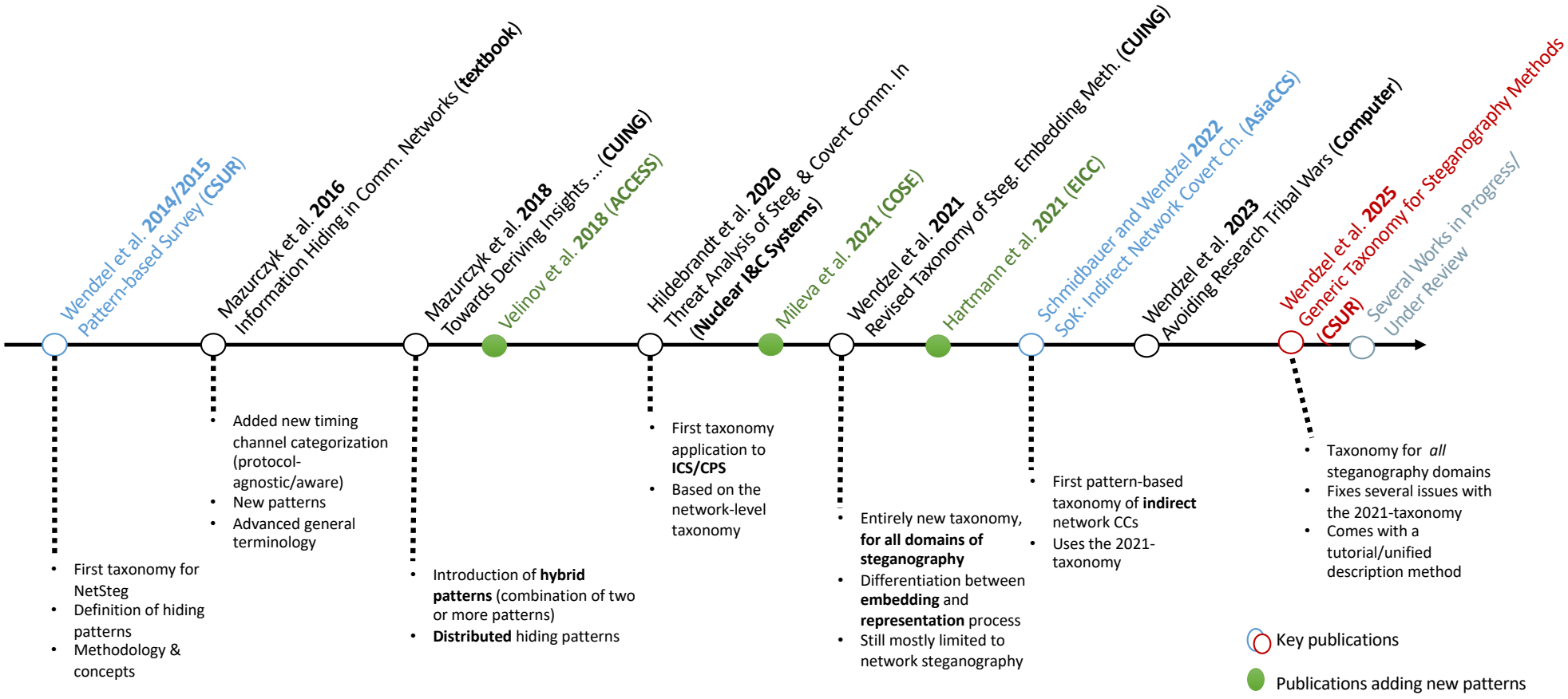
- Thousands of methods to conceal, circumvent, obfuscate and hide data available.
  - Many redundancies!

- 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**)*


Wendzel et al. 2014/2015
Pattern-based Survey (CSUR)
Mazurczyk et al. 2016
Information Hiding in Comm. Networks (textbook)
Mazurczyk et al. 2018
Towards Deriving Insights … (CUING)
Velinov et al. 2018 (ACCESS)
Hildebrandt et al. 2020
Threat Analysis of Steg. & Covert Comm. In (Nuclear I&C Systems)
Mileva et al. 2021 (COSE)
Wendzel et al. 2021
Revised Taxonomy of Steg. Embedding Meth. (CUING)
Hartmann et al. 2021 (EICC)
Schmidbauer and Wendzel 2022
SoK: Indirect Network Covert Ch. (AsiaCCS)
Wendzel et al. 2023
Avoiding Research Tribal Wars (Computer)
Wendzel et al. 2025
Generic Taxonomy for Steganography Methods (CSUR)
Several Works in Progress/ Under Review
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
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

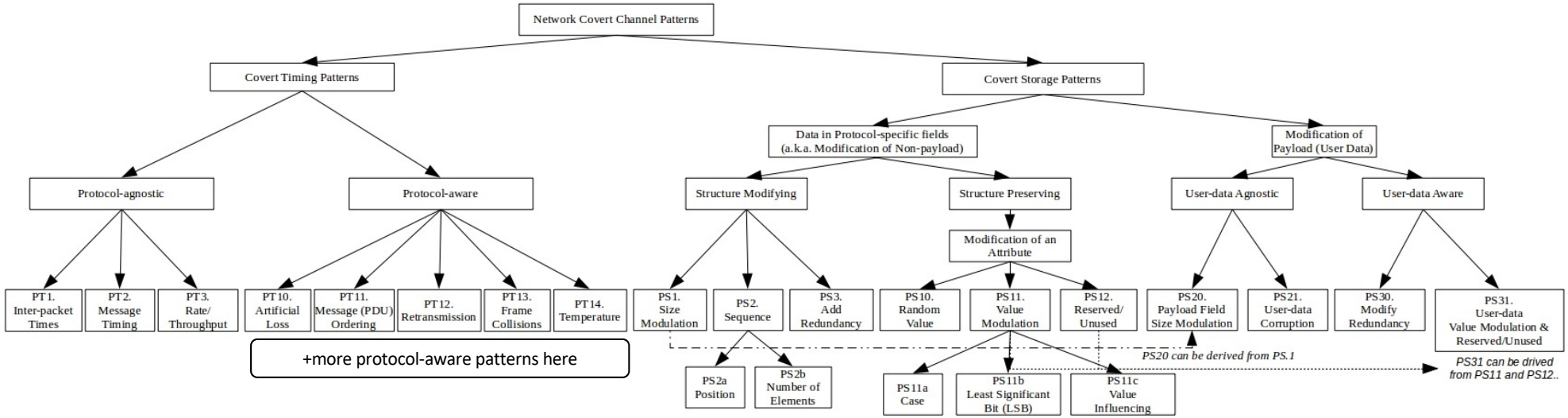
A Generic Taxonomy for Steganography

1. Drawing links between partially isolated disciplines (text steganography, image/audio steganography, filesystem steganography, network steganography etc.)

2. Finding common terms for different (but similar!) ideas

3. Aiding the development of the whole steganography research domain

2015-now: several updates on the network steganography taxonomy



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.
Official Hiding Patterns Website (https://patterns.omi.uni-ulm.de) ← always has the latest version of the taxonomy.

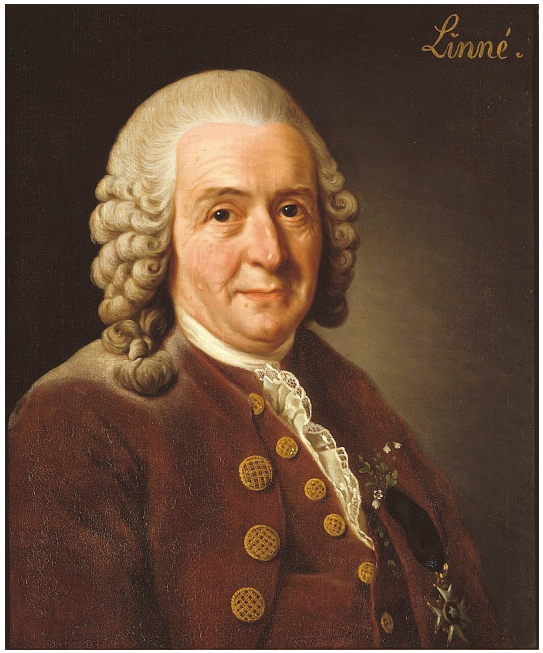
Let‘s start with the …

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*, 2025.

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*, 2025.

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.

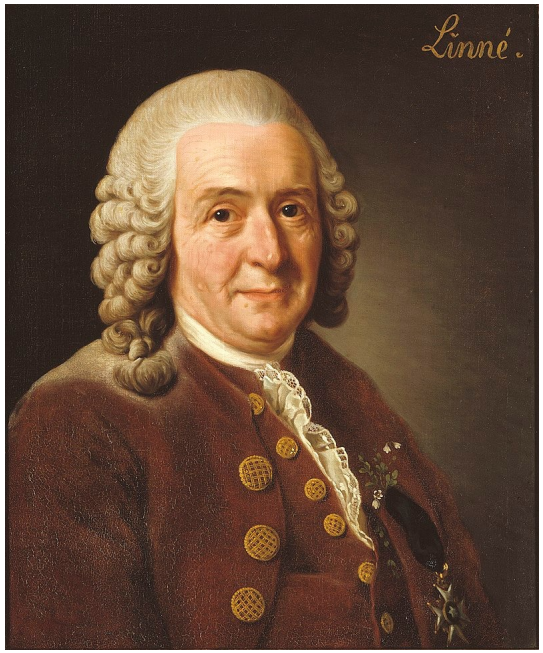
Solution: Involve the community!

- 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*, 2025.

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)



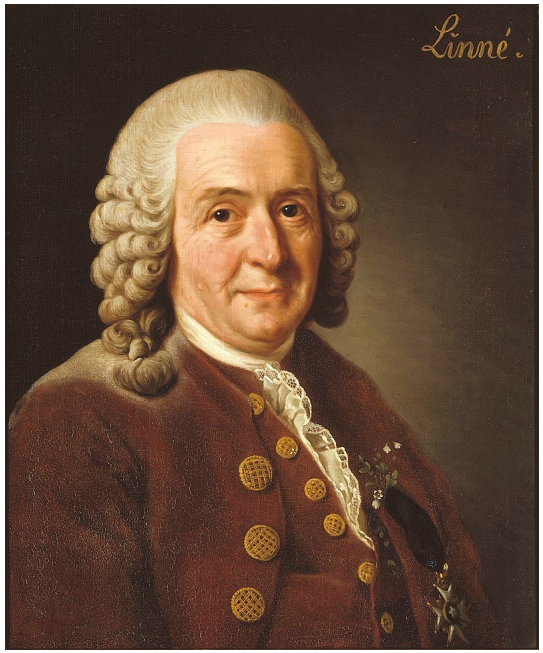
Img.: Wikipedia, public domain

S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2025.

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:

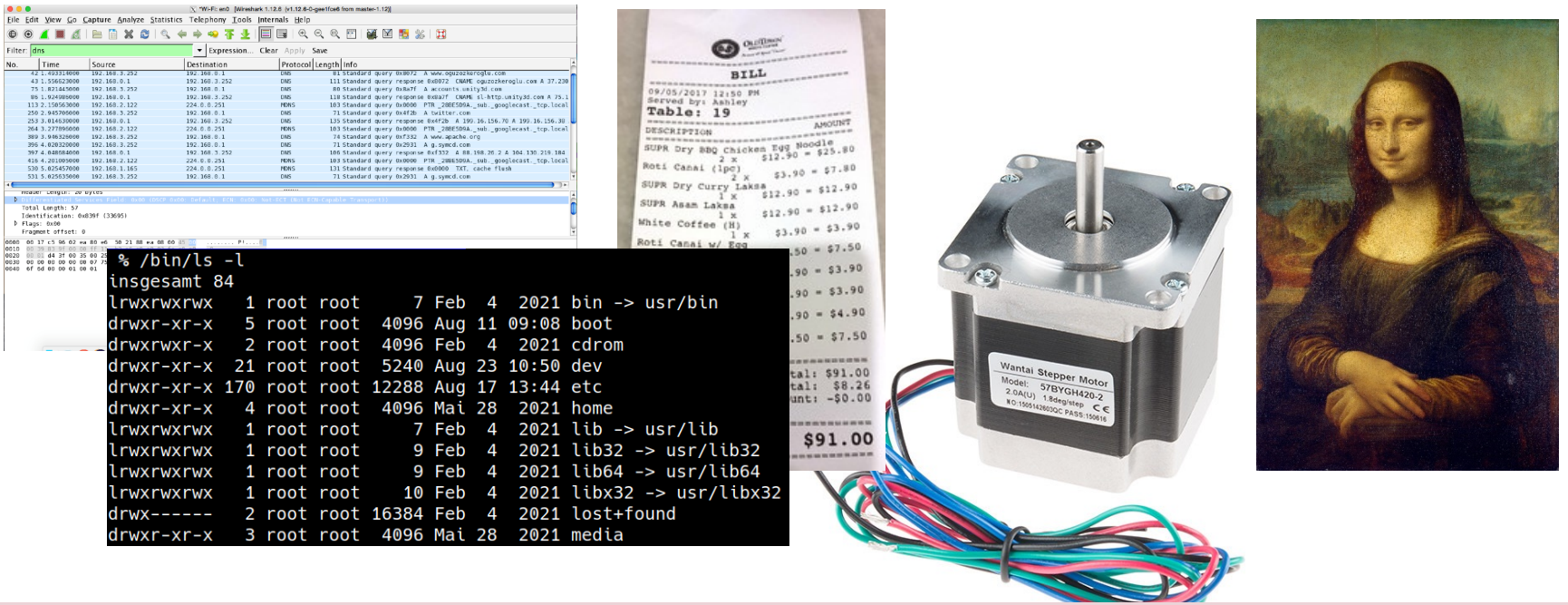
  - **E1. State/Value Modulation**
  - **E1.3. LSB State/Value Modulation**
  - **E1.3n1. Network LSB State/Value Modulation**



Img.: Wikipedia, public domain

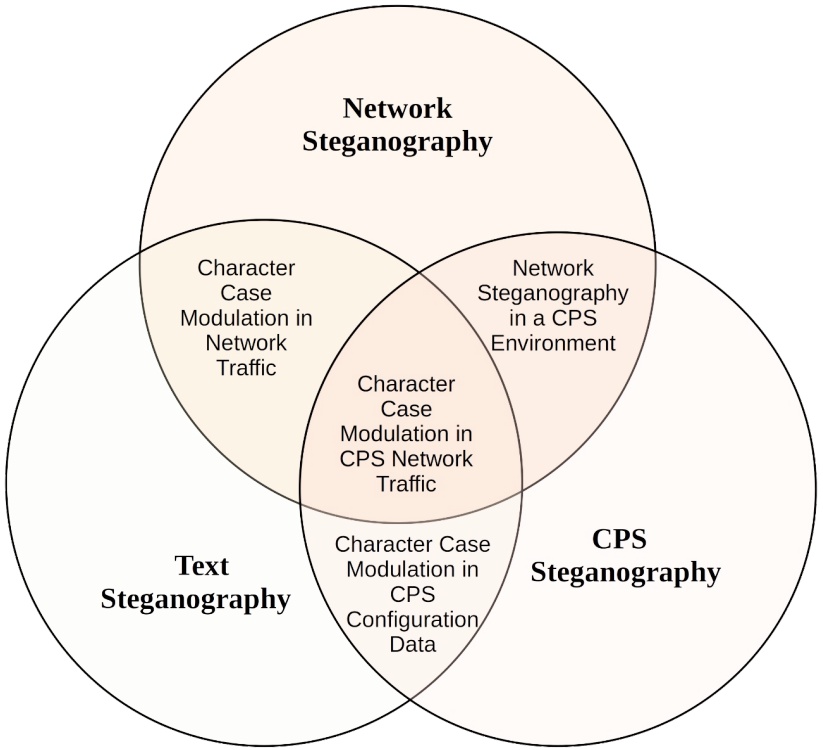
S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2025.

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.

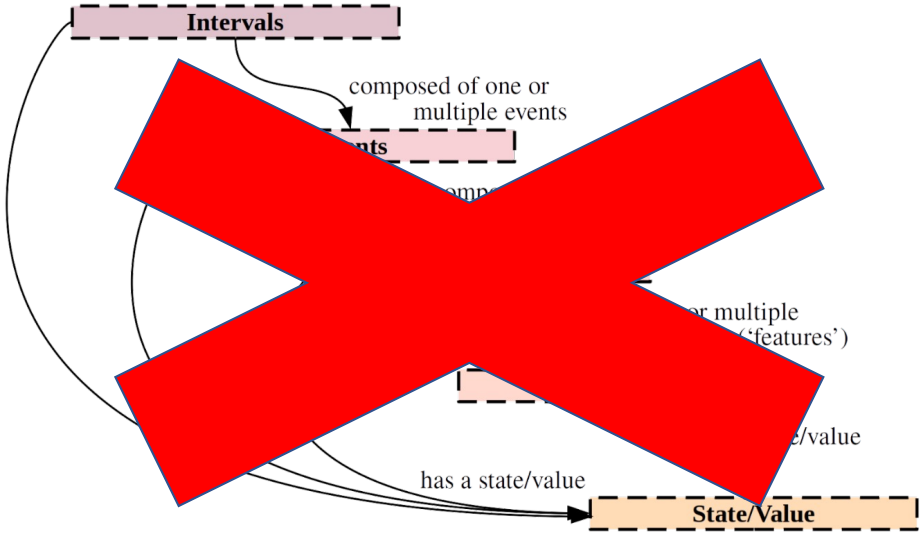
Problem 4: Heterogenous Stego Objects



S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2025.

Problem 4: Heterogenous Stego Objects

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

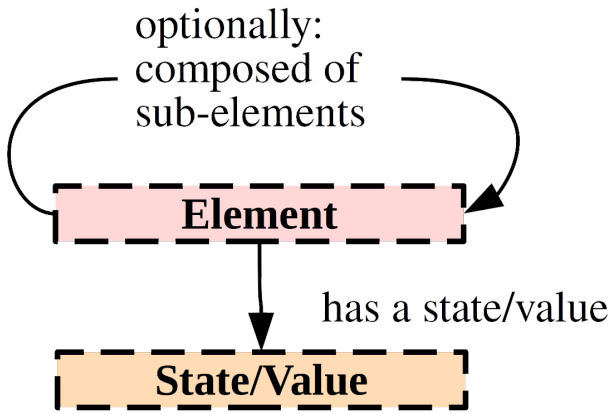


S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2025.

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*, 2025.

Problem 4: Heterogenous Stego Objects

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

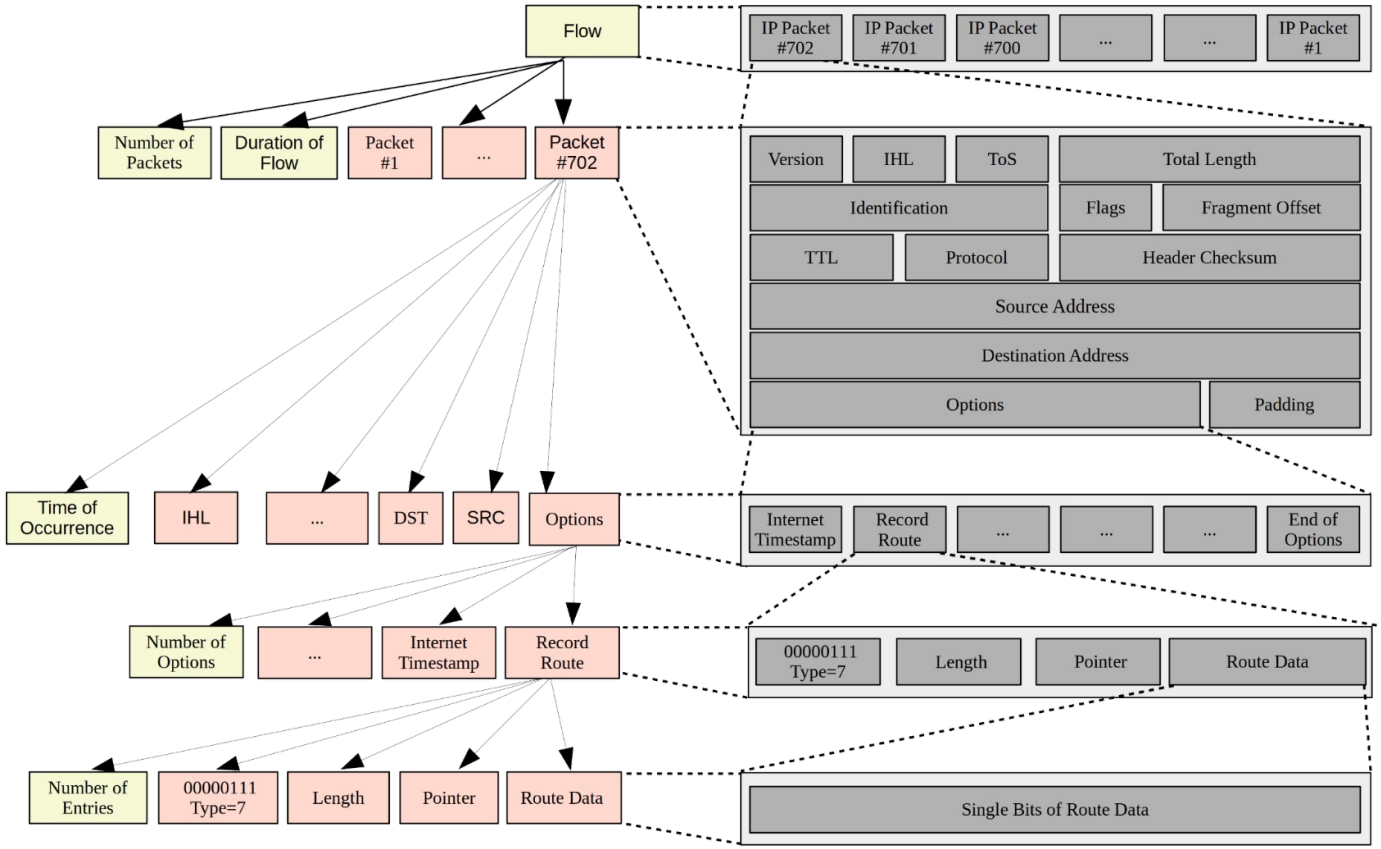
Table 1. Differentiation between the types of *objects* used in this paper.

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*, 2025.

Problem 4: Heterogenous Stego Objects

- **Illustration:**



S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2025.

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.

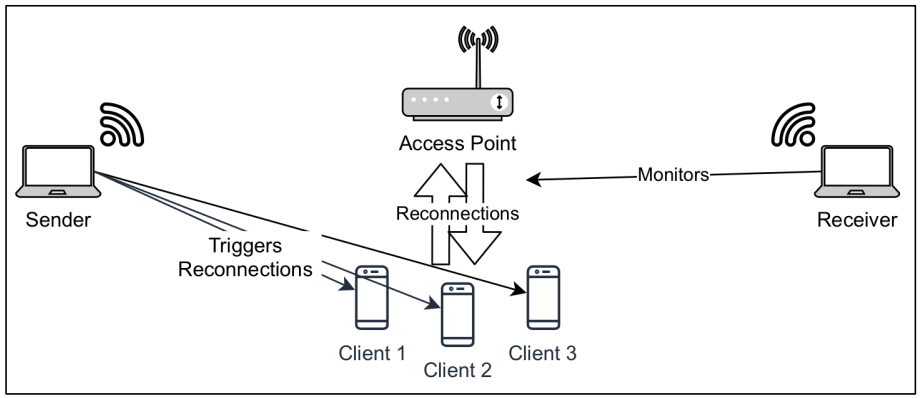


Fig.: S. Zillien, S. Wendzel: *Reconnection-based Covert Channels in Wireless Networks*, in Proc. 36th IFIP SEC, Springer, 2021.

[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]:

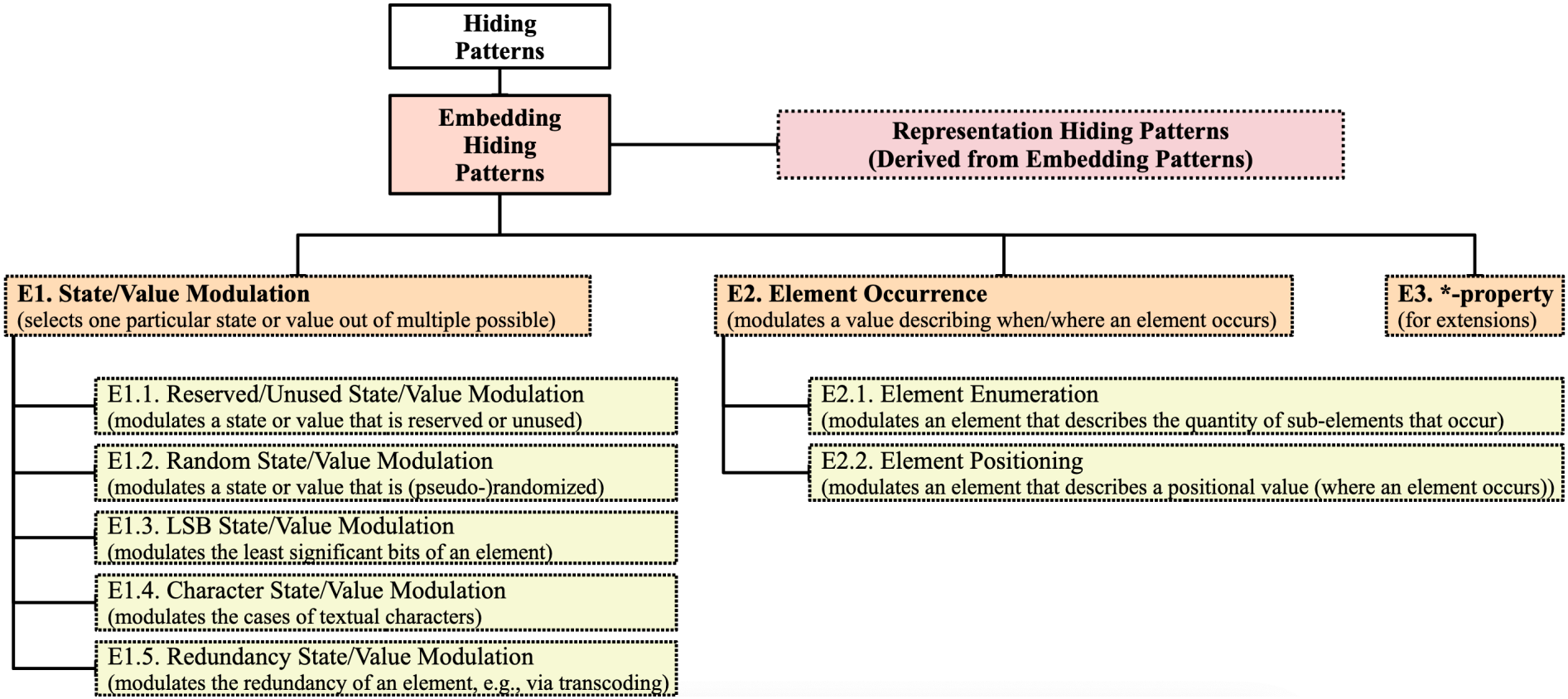
1. Sender **relocates a VM** (e.g., from Europe to Australia, using commands sent through the State/Value Modulation pattern).
2. Receiver **observes the RTT to the VM**, i.e., measures the temporal location (i.e., temporal position) of packets (Element Positioning pattern).

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.

Overview



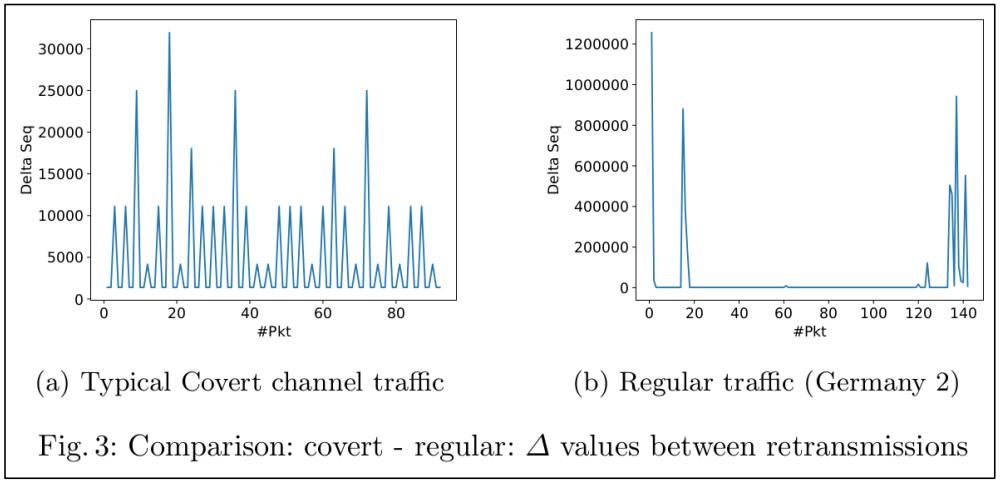
S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2025.

Example 1: Network Steganography

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

- Hiding Pattern:

  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*, 2025.

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*, 2025.

Example 3: Filesystem Steganography

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

- Hiding Pattern:

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

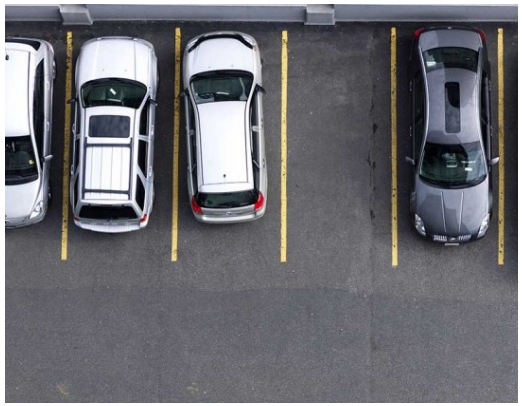


Fig: bloomberg.com/Getty Images

S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2025.

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*, 2025.

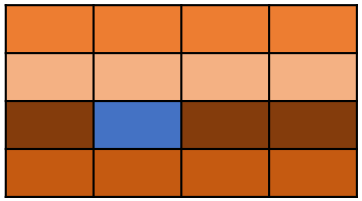
Example 5: Digital Media Steganography

- *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.

- Hiding Pattern:

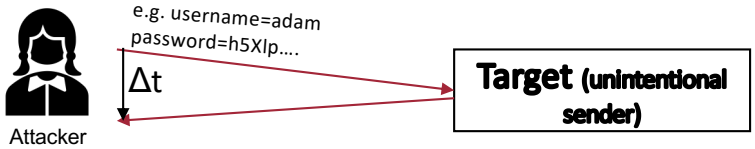
  E2.2d1. Digital Media Element Positioning
  (we modulate the position of the element (blue screen/pixel) in a temporal or spatial way)



S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2025.

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*, 2025.

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)

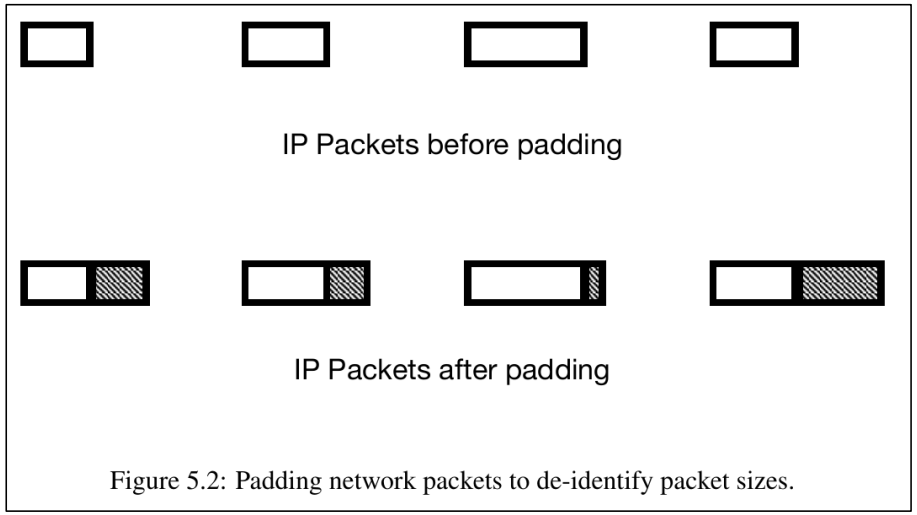


Figure 5.2: Padding network packets to de-identify packet sizes.

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*, 2025.

Problem 7: Where do all the details go?

- 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**:

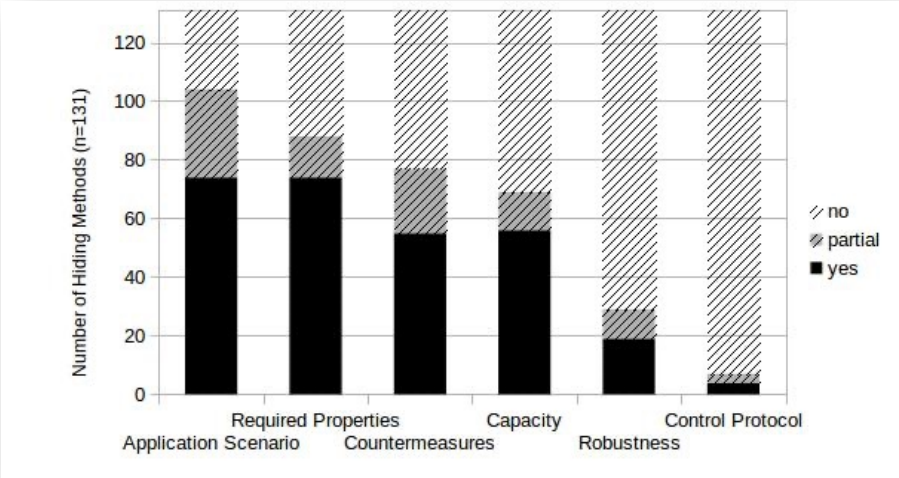


Fig.: S. Wendzel, W. Mazurczyk, S. Zander: Unified Description for Network Information Hiding Methods, in: Journal of Universal Computer Science, 2016.

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

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

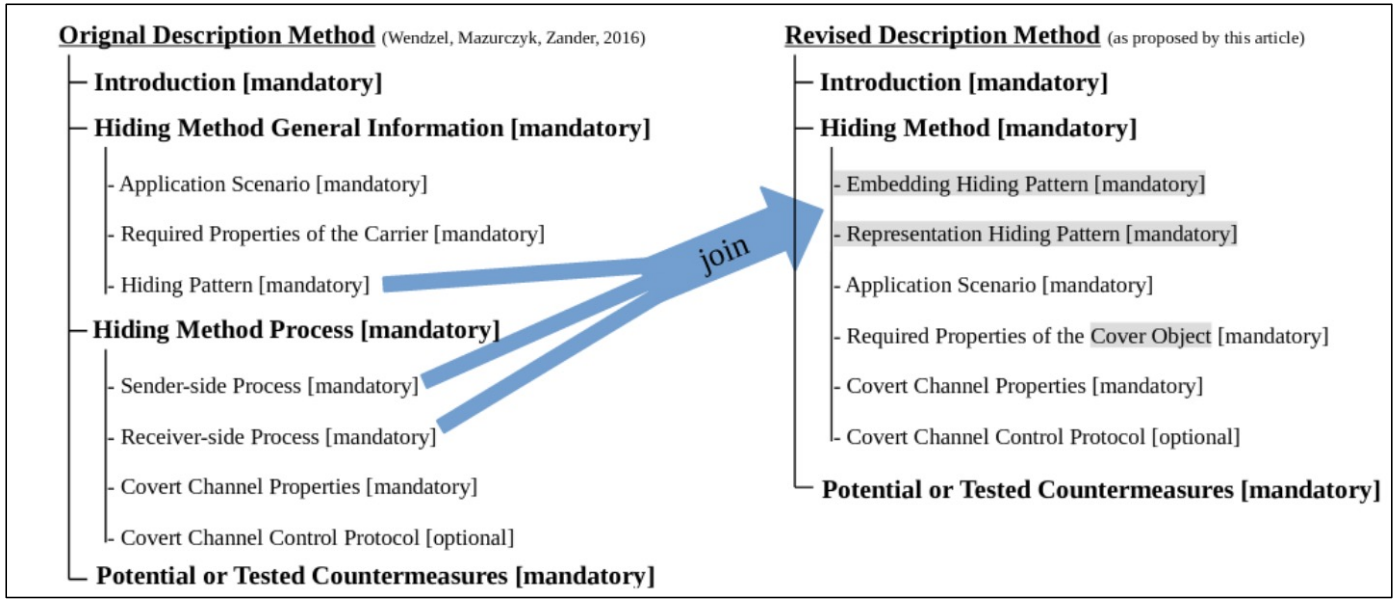
(subsume a hiding method in a **particular domain**)

(**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*, 2025.

Problem 7: Where do all the details go?

- **Unified Description Method**



S. Wendzel, L. Caviglione, W. Mazurczyk, A. Mileva, J. Dittmann et al.: *A Generic Taxonomy for Steganography Methods*, 2025.

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*, 2025.

Problem 9: Backwards Compatibility

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

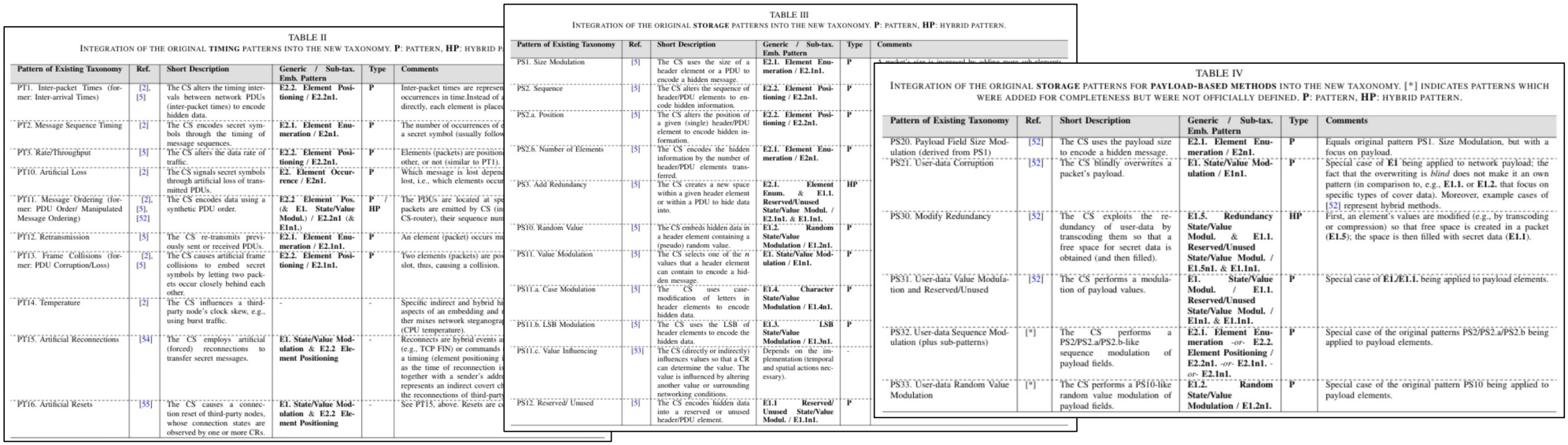


TABLE II
INTEGRATION OF THE ORIGINAL **TIMING** PATTERNS INTO THE NEW TAXONOMY. **P**: PATTERN, **HP**: HYBRID P

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 place
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 depen lost, i.e., which elements occu
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 sp 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 m
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 po 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 h aspects of an embedding and t 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	
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*, 2025.

Alright, but some hiding techniques are indirect!

- **We worked out a taxonomy for such techniques too!**
- Add patterns that the describe the **architecture** of **indirect** channels.
- Utilize the generic taxonomy's patterns to describe the **details**.

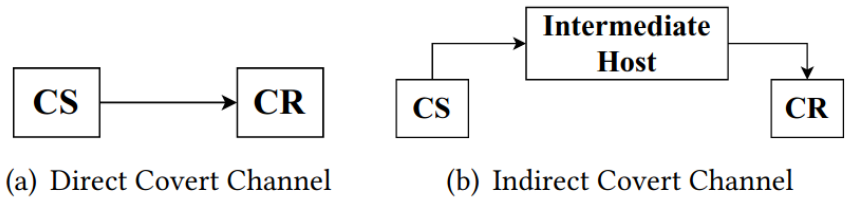


Fig.: T. Schmidbauer, S. Wendzel: *SoK: A Survey on Indirect Network Covert Channels*, Asia CCS 2022.

Alright, but some hiding techniques are indirect!

- **Essentially three patterns:**

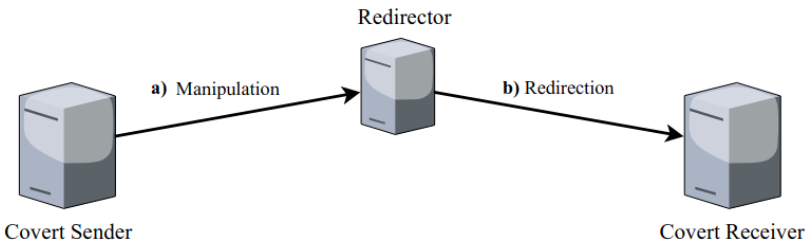


Figure 3: Redirector Pattern

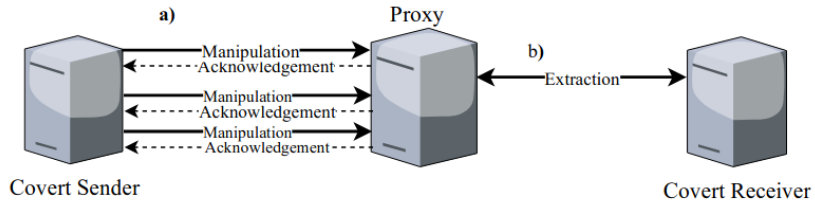
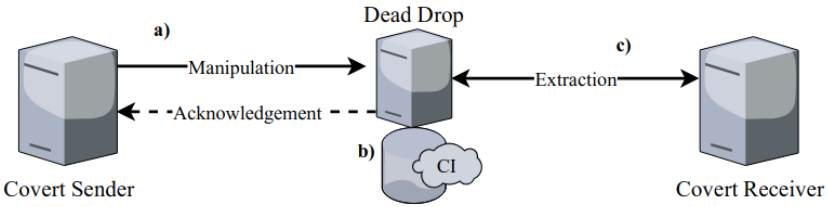


Figure 4: Proxy Pattern



(a) Dead Drop Pattern

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

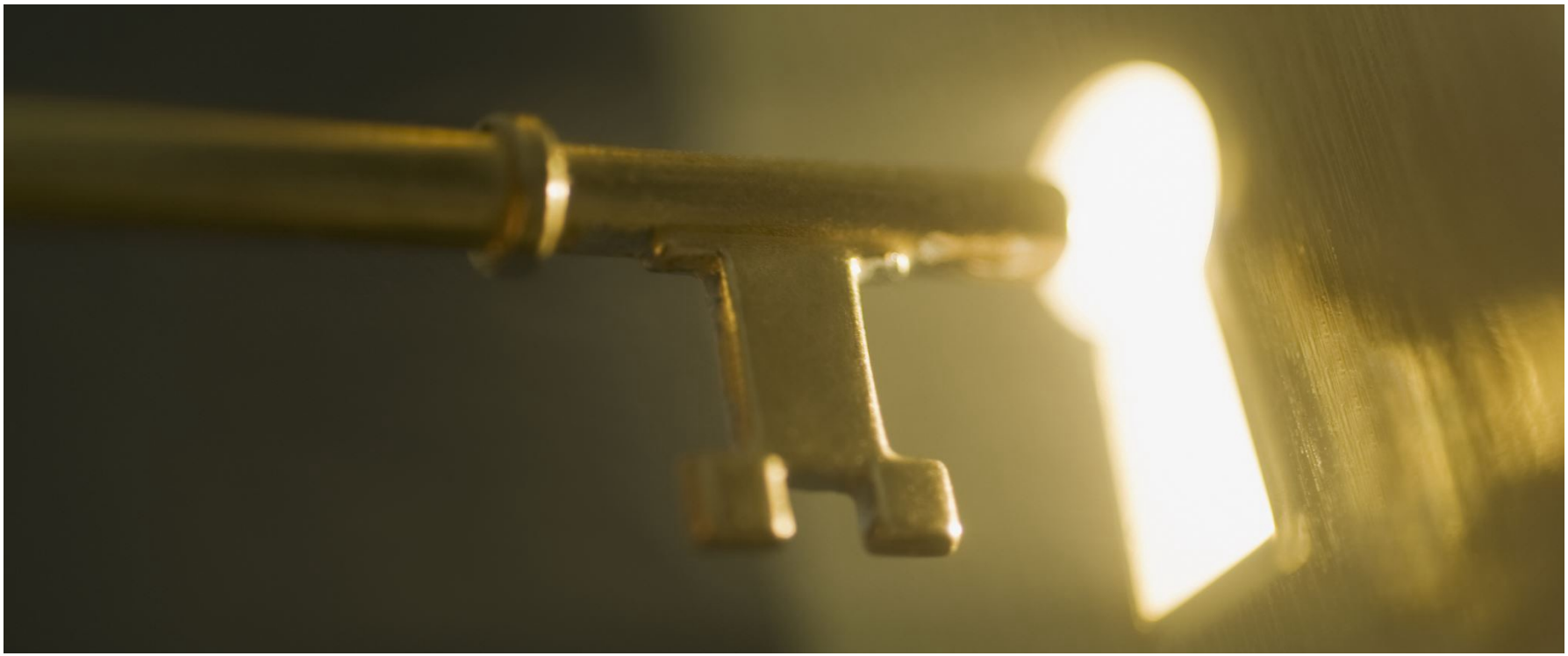
What else can be done with the taxonomy?

- 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)

Take Aways

- New taxonomy allows categorizing methods of all steganography domains (hopefully!).
- Solved several problems (applicability, hybrid techniques etc.)
- Capable of handling indirect hiding methods (additional taxonomy)
- Multi-level approach:
  generic taxonomy → specific taxonomy → unified description method
  (→ indirect covert channel taxonomy)

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, etc.) overlaps.

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

One common taxonomy might be the solution!

More Information …

https://patterns.omi.uni-ulm.de