Hochschule Worms
University of Applied Sciences

NETWORK INFORMATION HIDING

CH. 5: HIDING PATTERNS

A.K.A.: GUIDE ME THROUGH THE JUNGLE!

(CHAPTER MOSTLY BASED ON S. WENDZEL ET AL.: PATTERN-BASED SURVEY OF NETWORK COVERT CHANNEL TECHNIQUES, ACM CSUR, 47(3), 2015)

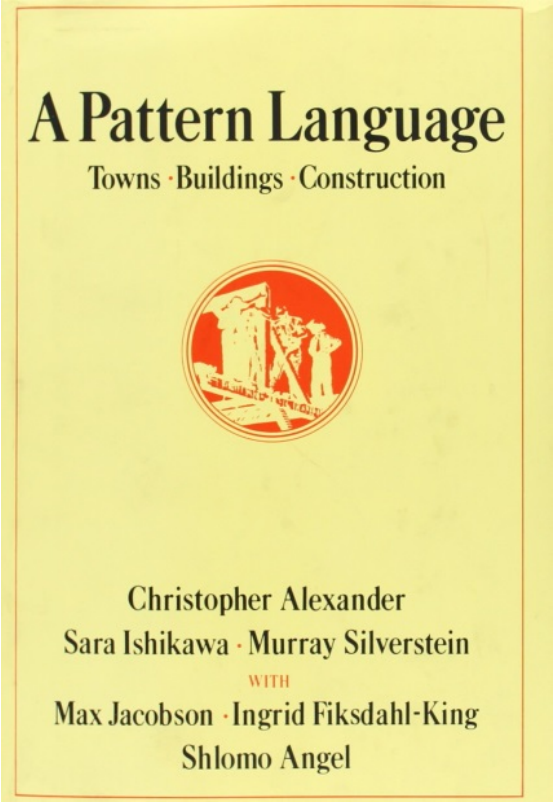
Prof. Dr. Steffen Wendzel
Worms University of Applied Sciences

https://www.wendzel.de (EN) | https://www.hs-worms.de/wendzel/ (DE)

Online Class: https://github.com/cdpxe/Network-Covert-Channels-A-University-level-Course/

Patterns

- What are „**Patterns**“?
  - A solution to a re-occurring problem in a given context
  - They are re-usable and described in an abstract way

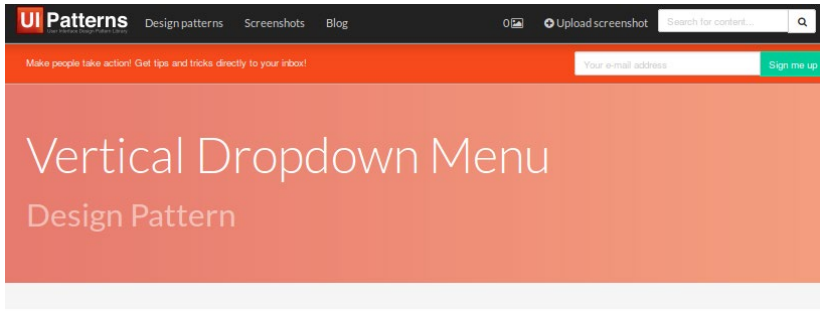


- Term introduced by Alexander *et al.* in 1977 for Architecture
- He presented a „pattern language“ comprising 253 patterns

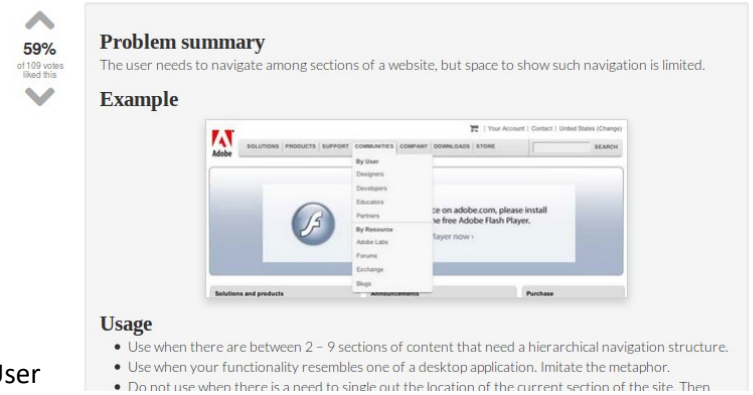
- **Example:**
  - Problem: want to minimize artificial light
  - Context: saving energy
  - Solution: build a window into a building to receive as much sunlight as possible in that room.

Patterns

- „Architectural Patterns“ discussed in Informatics are rooted in *Software Engineering*
  - introduced by the *Gang of Four* (GoF)
- Well-known are UI design patterns, cf. www.ui-patterns.com.
  - Example „Vertical Dropdown Menu“:



- Note: Patterns can even be used to generate user interfaces in a semi-automated manner (cf. [1]).



[1] Engel, J., Märtin, C., Herdin, C., Forbrig, P.: Formal Pattern Specifications to Facilitate Semi-automated User Interface Generation, in Proc. Human-Computer Interaction, Part I, HCII 2013, LNCS 8004, pp. 300-309, Springer, 2013.

Comments on Patterns

- A technique can only be a pattern **if it occurs multiple times**. In general, the scientific patterns community agrees on a minimal number of three occurrences.

- **Pattern collections** comprise patterns of a given domain. They can be understood as **pattern catalogs*** (but the latter is additionally searchable, e.g. by an index of patterns).
  - e.g., a collection of user interface patterns
  - Problematic aspect: the link-ability of patterns between collections differs due to non-unified structures in which the patterns are described.

* Terminology not unified in the literature. We can agree on collection==catalog for this lecture.

Hochschule Worms
University of Applied Sciences

Pattern Languages

- **Pattern languages** were introduced to solve the mentioned problems of pattern collections:
  - they provide a unified description for patterns
  - allow to build links/hierarchies between patterns
  - introduce aliases to prevent redundancies

- **PLML** (Pattern Language Markup Language, pronounced “Pell-Mell” [1]) is one dominating example of a pattern language.

[1] https://www.cs.kent.ac.uk/people/staff/saf/patterns/plml.html

PLML

- PLML allows the description of patterns (e.g. in XML).

- Patterns comprise various elements (attributes of PLML/1.1*):

Pattern Identifier	Name
Alias	Illustration
Description of the Problem	Description of the Context
Description of the Solution	Forces
Synopsis	Diagram
Evidence	Confidence
Literature	Implementation
Related Patterns	Pattern Links
Management Information	

* Newer version of PLML is available but the basic attributes remain. Not all attributes of the table above were used (+necessary) to describe hiding patterns.

Hiding Patterns [1]

Hiding Patterns describe they **key idea of hiding techniques**. They are kept on an **abstract, non-detailed level**, help **cleaning up terminology**, and can **form a taxonomy**.

[1] S. Wendzel, S. Zander et al.: Pattern-based Survey of Network Covert Channel Techniques, ACM CSUR, 47(3), 2015.

Patterns in Network Information Hiding

- Idea of using patterns in network information hiding was first introduced in (Wendzel et al., 2015). Please cf. http://www.ih-patterns.blogspot.com where you can also download the paper.

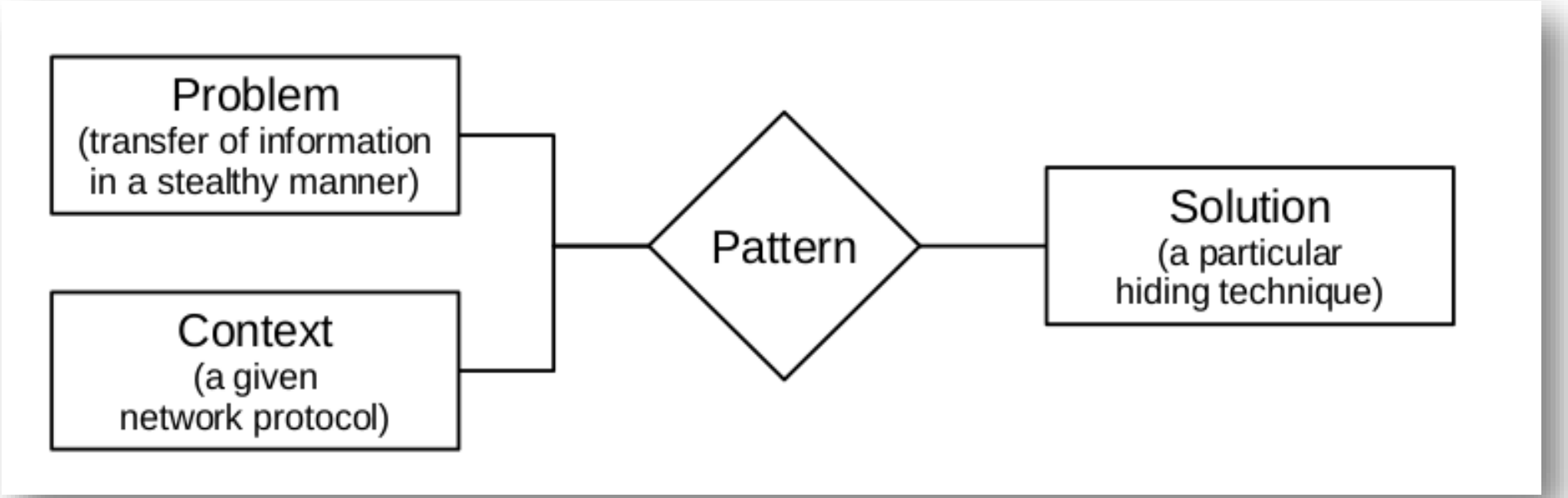


Image source: (Wendzel et al., 2015)

The following attributes were used

Table I. Used PLML/1.1 Attributes

Tag	Description
<pattern id>	Identifies a pattern within the particular catalog.
<name>	A correct assignment of a name for each pattern is important for the retrieval of a pattern when the pattern becomes part of a second catalog.
<alias>	Patterns can have different names, which are specified in the <alias> tag. The alias tag helps to find the same pattern when the pattern has different names in different catalogs.
<illustration>	An application scenario for the pattern.
<context>	Specifies the situations to which the pattern can be applied.
<solution>	Describes the solution for a problem to which the pattern can be applied. The attributes *problem* and *context* (cf. Fig. 1) are usually blurred but often not separated into two attributes.
<evidence>	Contains additional details about the pattern and its design. Moreover, the tag can contain examples for known uses of the pattern.
<literature>	Lists references to publications related to the pattern.
<implementation>	Introduces existing implementations, code fragments or implementational.

Image source: (Wendzel et al., 2015)

Hochschule Worms
University of Applied Sciences

Patterns in Network Information Hiding

- Approx. 170 network hiding techniques are known; they hide secret information in meta data of network traffic.
  - Inconsistent terminology.
  - Re-inventions very common.

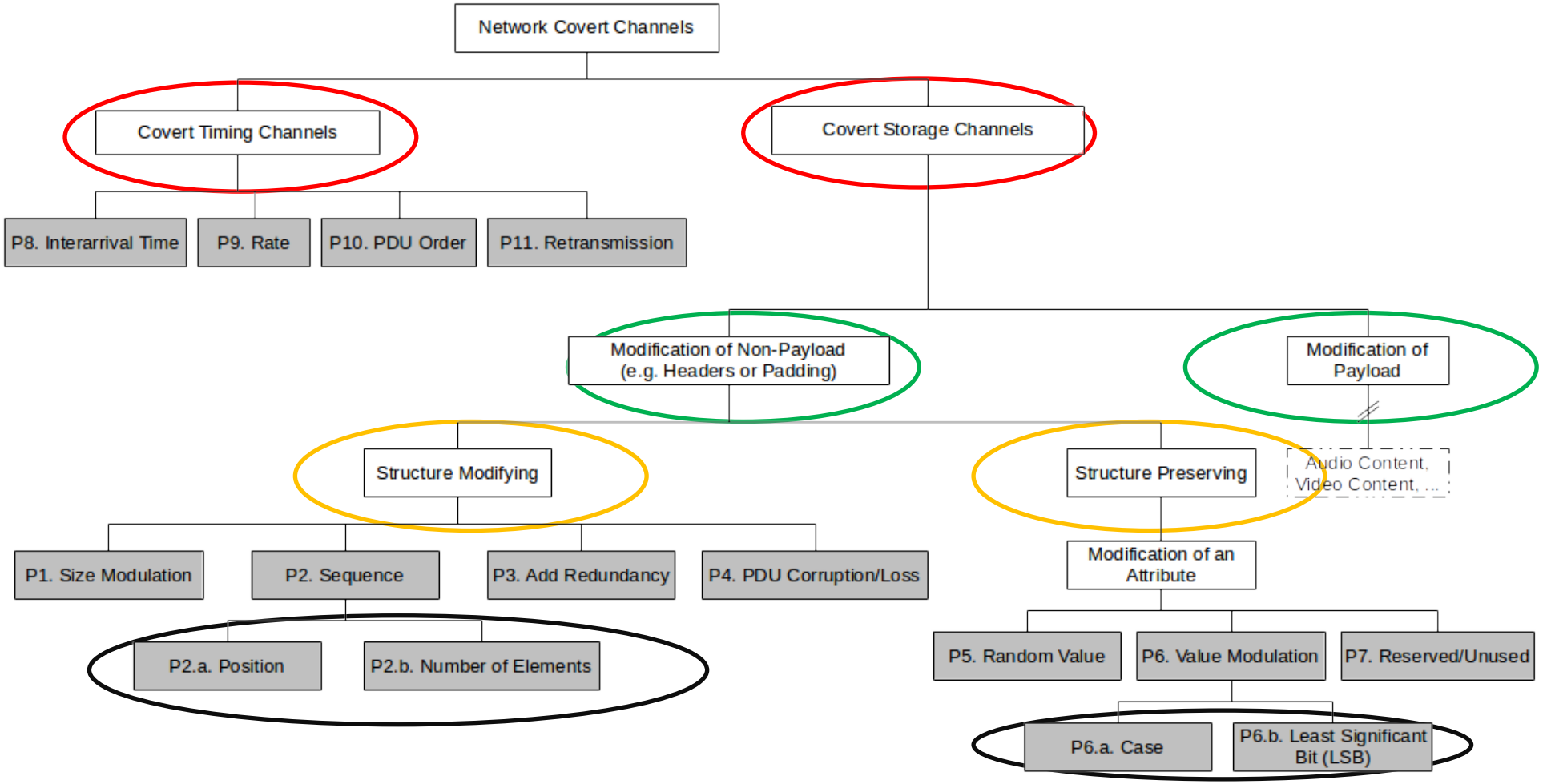
- Instead of dealing with all these hiding techniques separately, we only need to understand the few hiding patterns.

- Initially **eleven** (later a more) patterns were found to describe all analyzed hiding techniques published between 1987 and 2013.

- Also, patterns provide better taxonomies due to their several features (links and child patterns, alias handling, unified attributes, …).

Patterns in Network Information Hiding [1]

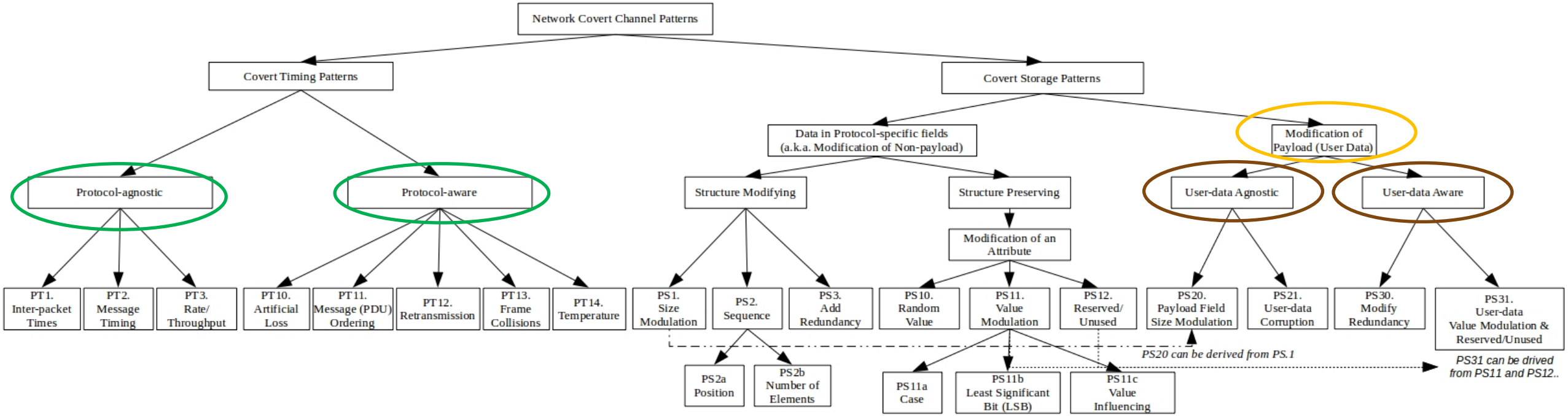
Patterns were set in relation to other patterns to introduce a **new taxonomy** of patterns. The 109 hiding techniques could be described by only 11 patterns.



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

Latest Version of Pattern Taxonomy

Currently, approx. 160 hiding techniques are categorized into 14 timing and 10 storage patterns, plus sub-patterns.
Pattern names and their numbers were updated and extended in 2016, 2018, 2019 and 2020 (in progress).



Based on:

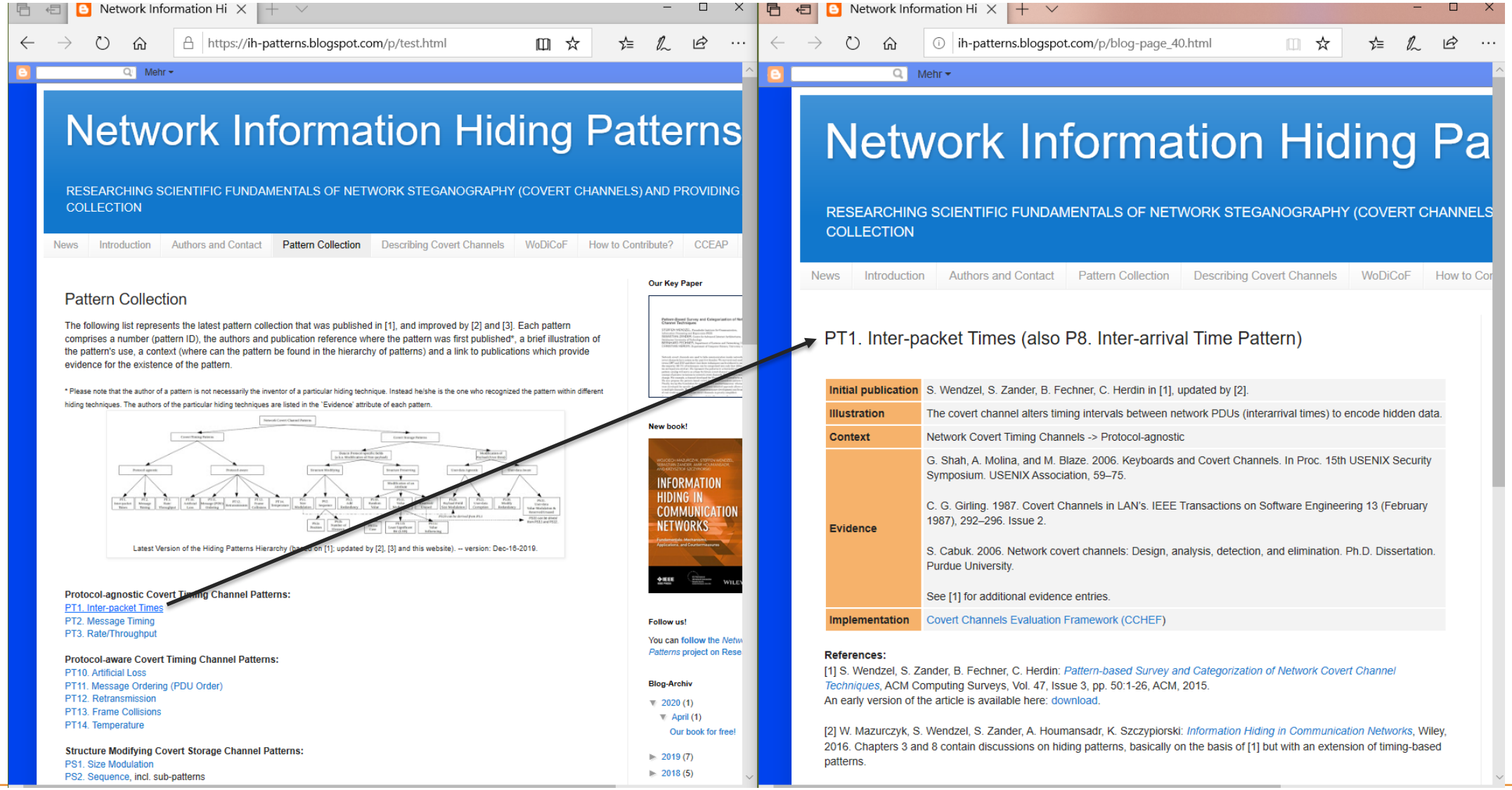
S. Wendzel, S. Zander, B. Fechner, C. Herdin: Pattern-based Survey and Taxonomy for Network Covert Channels, ACM CSUR, Vol. 47(3), 2015.

Extended by:

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://ih-patterns.blogspot.com) ← always has the latest version of the taxonomy.

Latest Version of Pattern Taxonomy

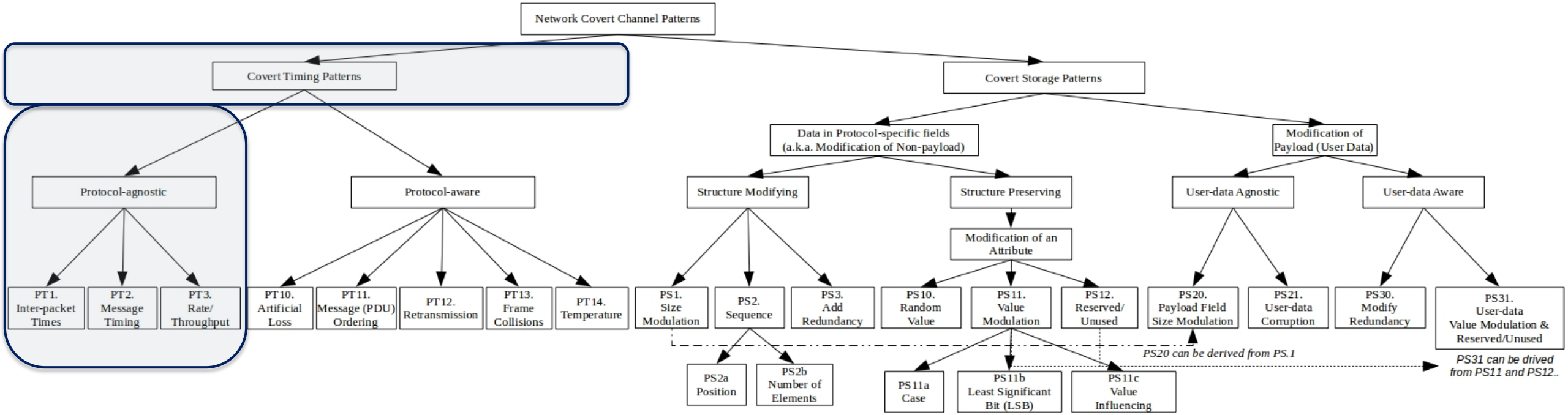
[Official Hiding Patterns Website (https://ih-patterns.blogspot.com)](https://ih-patterns.blogspot.com) ← always has the latest version of the taxonomy.



Hochschule Worms
University of Applied Sciences

Let’s go through all these patterns!

We start with the Timing Patterns: Protocol-agnostic Patterns



Based on:

S. Wendzel, S. Zander, B. Fechner, C. Herdin: Pattern-based Survey and Taxonomy for Network Covert Channels, ACM CSUR, Vol. 47(3), 2015.

Extended by:

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 (http://ih-patterns.blogspot.com) ← always has the latest version of the taxonomy.

PT1. Inter-packet Times

- **Introduced:** Wendzel et al., 2015 [1] as “P8. Inter-arrival Times”, renamed by Mazurczyk et al., 2016 [2].
- **Illustration:** The covert channel alters timing intervals between network PDUs (inter-arrival times) to encode hidden data.
- **Examples:** (see [1,2] for evidence)
  - Alter timings between Ethernet frames
  - Alter timings between IP packets

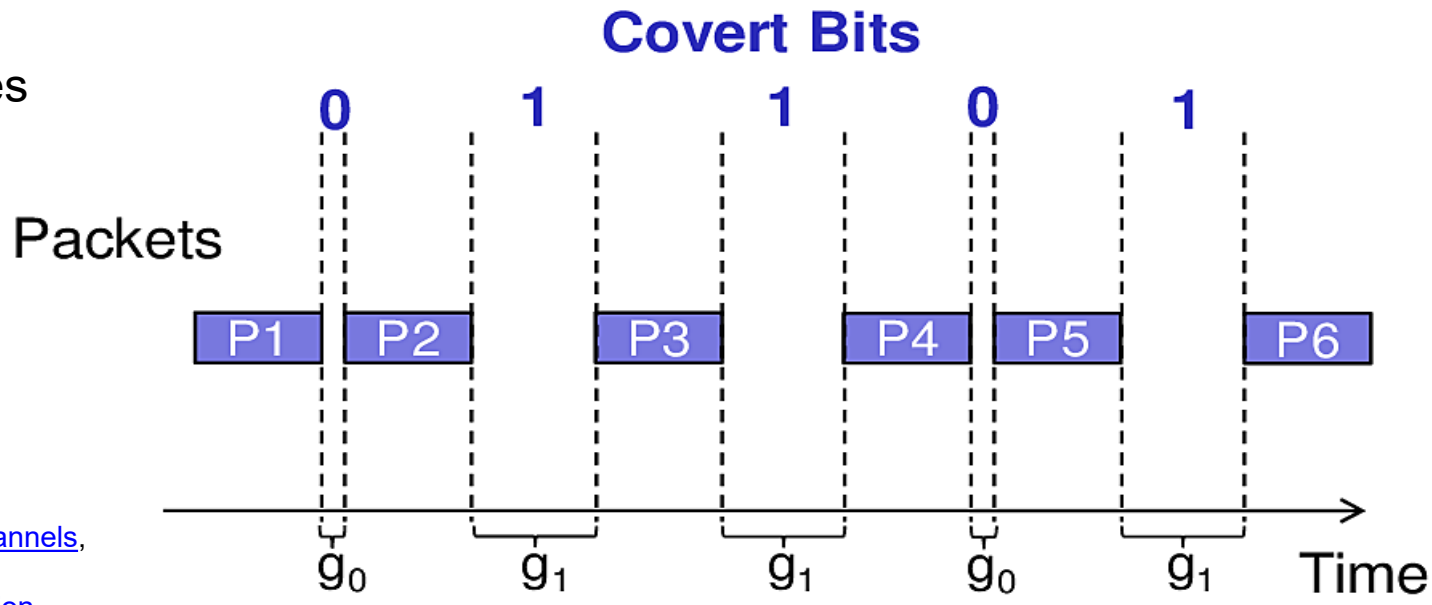
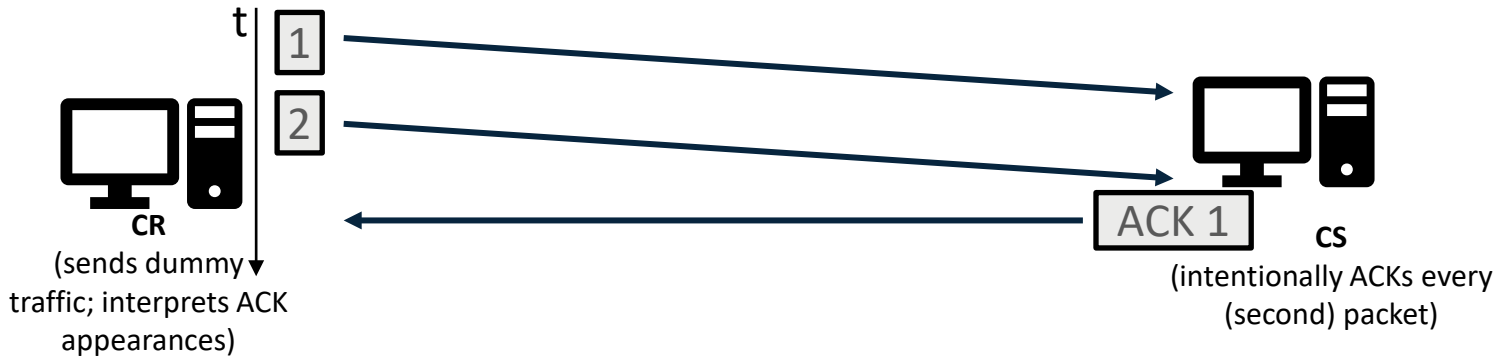


Fig.: [2]

[1] S. Wendzel et al.: Pattern-based Survey and Taxonomy for Network Covert Channels, ACM CSUR, Vol. 47(3), 2015.
[2] W. Mazurczyk, S. Wendzel, S. Zander et al.: Information Hiding in Communication Networks, WILEY-IEEE, 2016, Chapter 3.

PT2. Message Sequence Timing

- **Introduced:** Mazurczyk et al., 2016 [1].
- **Illustration:** Hidden data is encoded in the timing of message sequences, e.g. acknowledging every *n*'th received packet or sending commands *m* times.
- **Example(s):** (see [1] for evidence)
  - (Do not) wait until two frames have arrived before acknowledging the first of these frames (see below) to signal a covert (0) 1 bit.



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

PT3. Rate/Throughput Pattern

- **Introduced:** Wendzel et al., 2015 [1]
- **Illustration:** The covert channel sender alters the data rate of a traffic flow from itself or a third party to the covert channel receiver.
- **Examples:** (see [1,2] for evidence)
  - Exhaust the performance of a switch to affect the throughput of a connection from a third party to a covert channel receiver over time.
  - Directly alter the data rate of a legitimate channel between a covert channel sender and receiver.

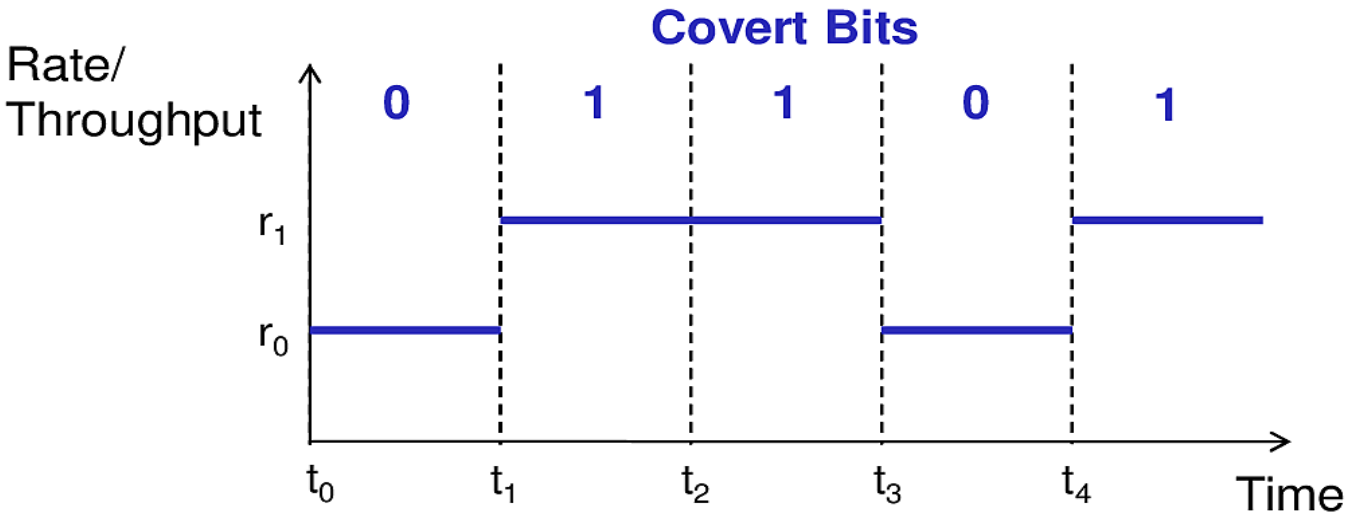
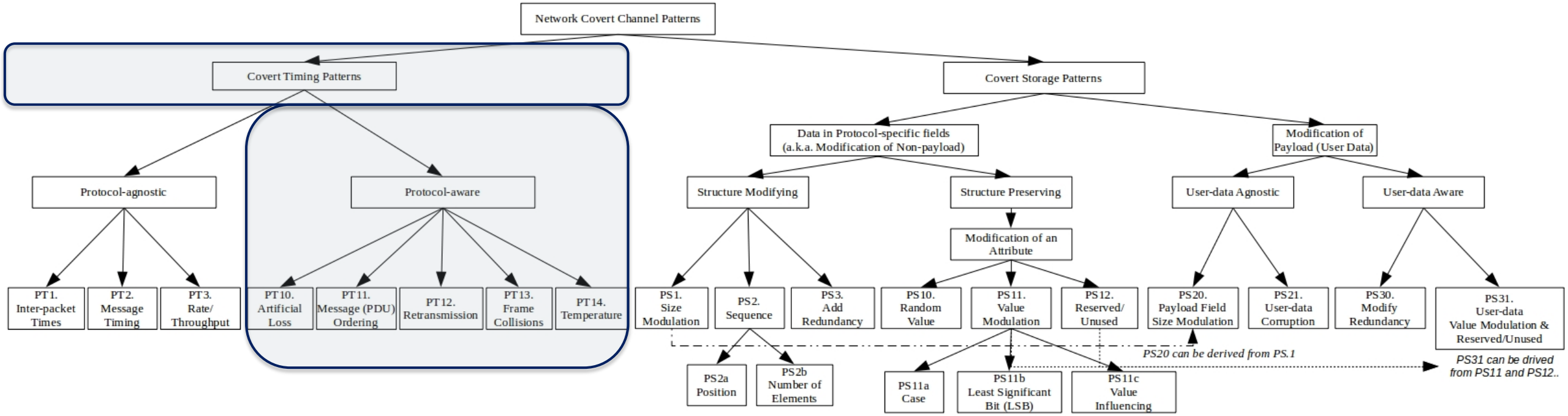


Fig.: [2]

[1] S. Wendzel et al.: Pattern-based Survey and Taxonomy for Network Covert Channels, ACM CSUR, Vol. 47(3), 2015.
[2] W. Mazurczyk, S. Wendzel, S. Zander et al.: Information Hiding in Communication Networks, WILEY-IEEE, 2016, Chapter 3.

The other Side of Timing Patterns: Protocol-ware Patterns



Based on:

S. Wendzel, S. Zander, B. Fechner, C. Herdin: Pattern-based Survey and Taxonomy for Network Covert Channels, ACM CSUR, Vol. 47(3), 2015.

Extended by:

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 (http://ih-patterns.blogspot.com) ← always has the latest version of the taxonomy.

PT10. Artificial Message/Packet Loss

- **Introduced:** Mazurczyk et al., 2016 [1], forked from and replaced former pattern “PDU Corruption” that was introduced in [2].

- **Illustration:** The covert channel signals hidden information via artificial loss of transmitted messages (PDUs).
- **Examples:** (see [2] for evidence)
  - Transfer corrupted frames in IEEE 802.11
  - MitM drops selected packets exchanged between two VPN sites to introduce covert information.

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

P11. Message Ordering (PDU Order) Pattern

- **Introduced:** Wendzel et al., 2015 [1] as “PDU Order” pattern, renamed by Mazurczyk et al., 2016 [2].

- **Illustration:** The covert channel encodes data using a synthetic PDU order for a given number of PDUs flowing between covert sender and receiver.

- **Examples:** (see [1,2] for evidence)
  - Modify the order of IPSec Authentication Header (AH) packets
  - Modify the order of TCP packets

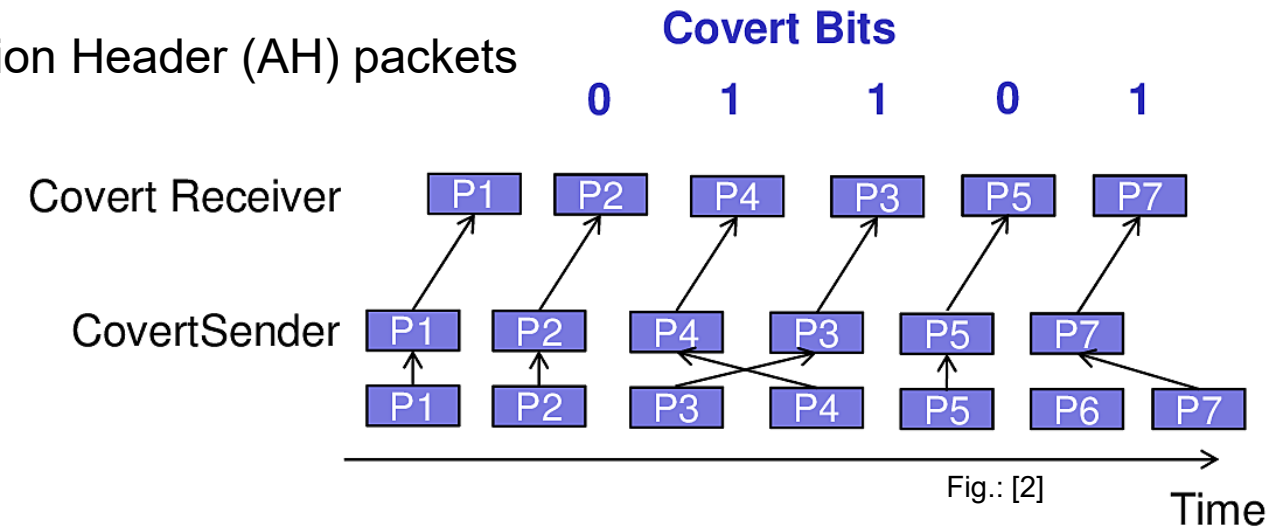
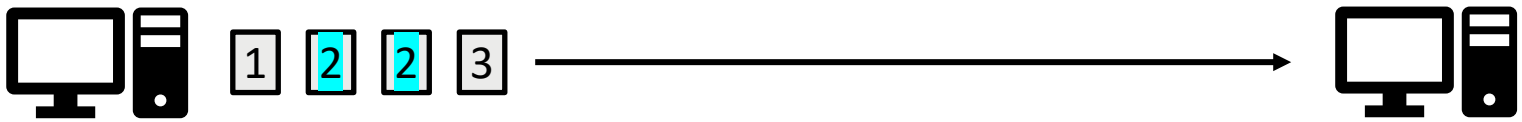


Fig.: [2]

[1] S. Wendzel et al.: Pattern-based Survey and Taxonomy for Network Covert Channels, ACM CSUR, Vol. 47(3), 2015.
[2] W. Mazurczyk, S. Wendzel, S. Zander et al.: Information Hiding in Communication Networks, WILEY-IEEE, 2016, Chapter 3.

P12. Artificial Re-transmissions Pattern

- **Introduced:** Wendzel et al., 2015 [1].
- **Illustration:** A covert channel re-transmits previously sent or received PDUs.
- **Examples:** (see [1] for evidence)
  - Transfer selected DNS requests once/twice to encode a hidden bit per request.
  - Duplicate selected IEEE 802.11 packets
  - Do not acknowledge received packets to force the sender to re-transmit a packet.



PT13. Frame Collisions

- **Introduced: Introduced:** Mazurczyk et al., 2016 [1], forked from and replaced former pattern “PDU Corruption” that was introduced in [2].

- **Illustration:** The sender causes artificial frame collisions to signal hidden information.

- **Examples:** (see [1] for evidence)
  - Ethernet CSMA/CD exploitation using jamming signals
  - Similar mechanisms for CSMA/CA

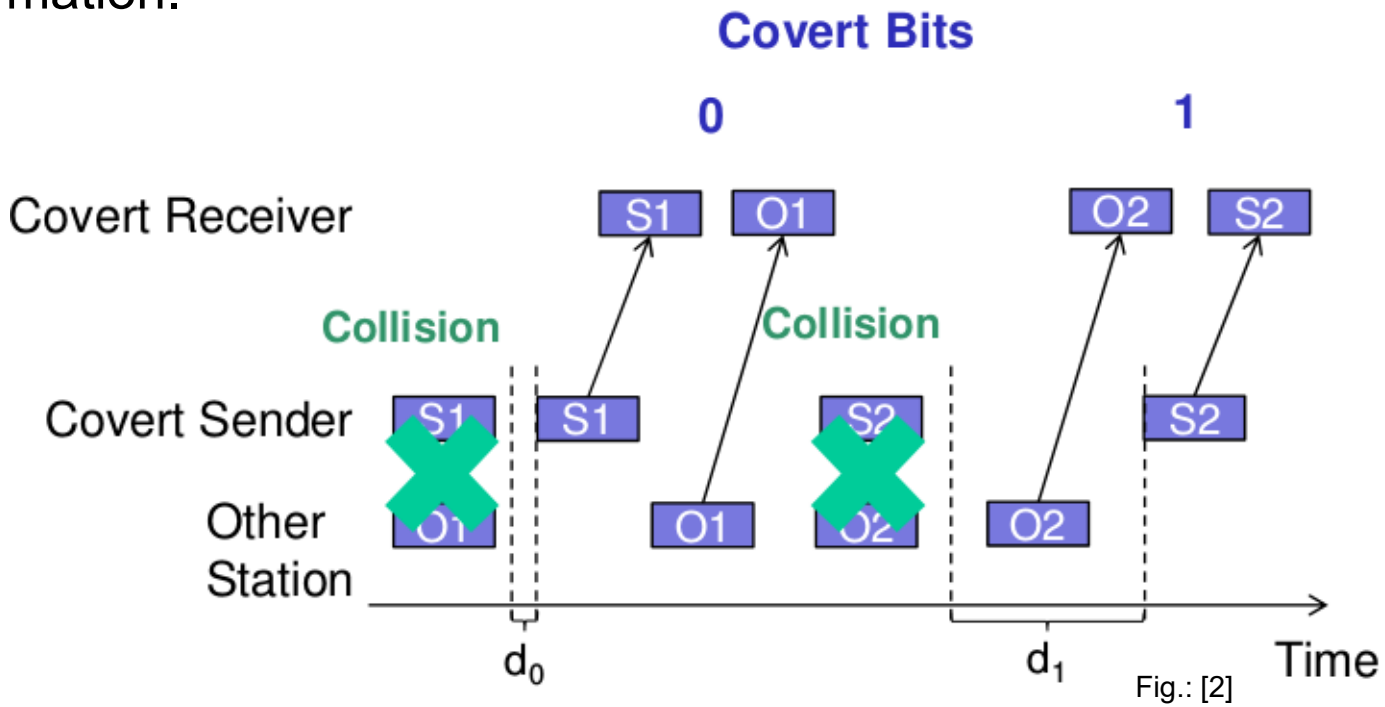


Fig.: [2]

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

PT14. Temperature

- **Introduced:** Mazurczyk et al., 2016 [1].
- **Illustration:** The sender influences a third-party node's CPU temperature, e.g. using burst traffic. This influences the node's clock skew. The clock skew can then be interpreted by the covert receiver by interacting with the node.
- **Examples:** (see [1] for evidence)
  - Few, mostly by S. Murdoch and S. Zander

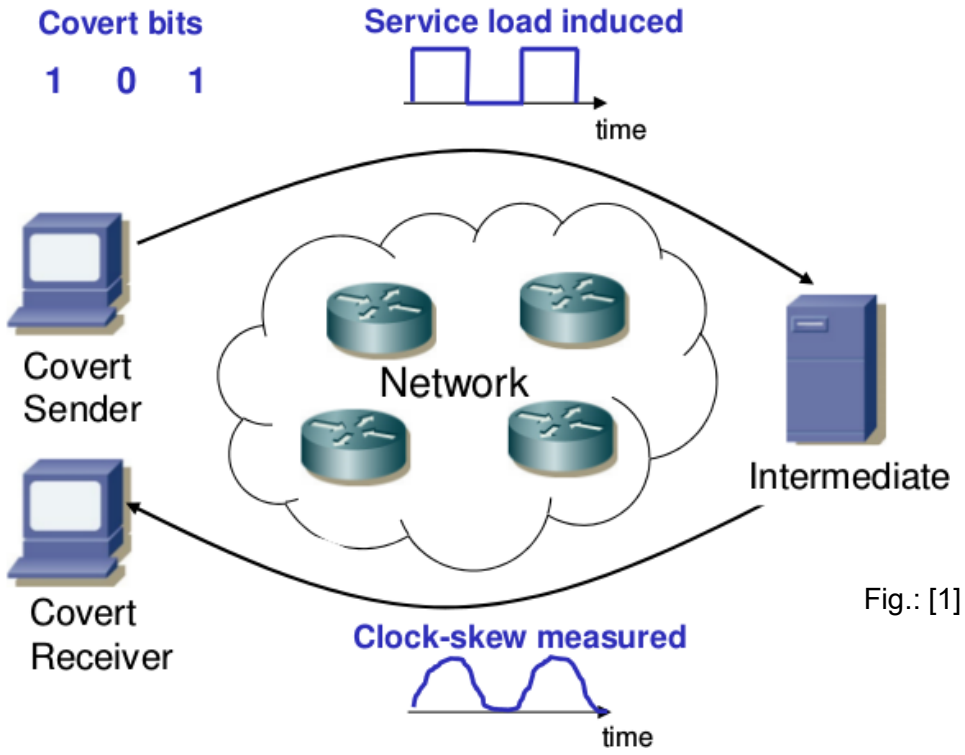
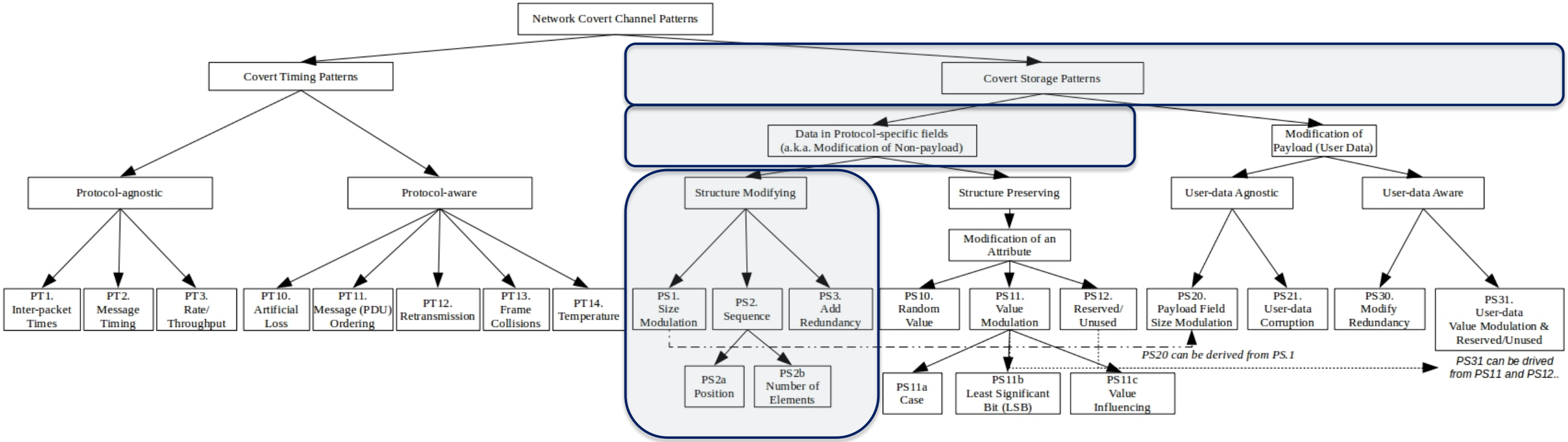


Fig.: [1]

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

Let's Switch to Storage Patterns: Protocol-specific Fields Patterns (Headers + Padding) Category: Structure Modifying Patterns



Based on:

S. Wendzel, S. Zander, B. Fechner, C. Herdin: Pattern-based Survey and Taxonomy for Network Covert Channels, ACM CSUR, Vol. 47(3), 2015.

Extended by:

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 (http://ih-patterns.blogspot.com) ← always has the latest version of the taxonomy.

PS1. Size Modulation Pattern

- **Introduced:** Wendzel et al., 2015 [1]
- **Illustration:** The overt channel uses the size of a header element or of a PDU* to encode the hidden message.
- **Examples:** (see [1] for evidence)
  - Modulation of data block length in LAN frames
  - Modulation of IP fragment sizes

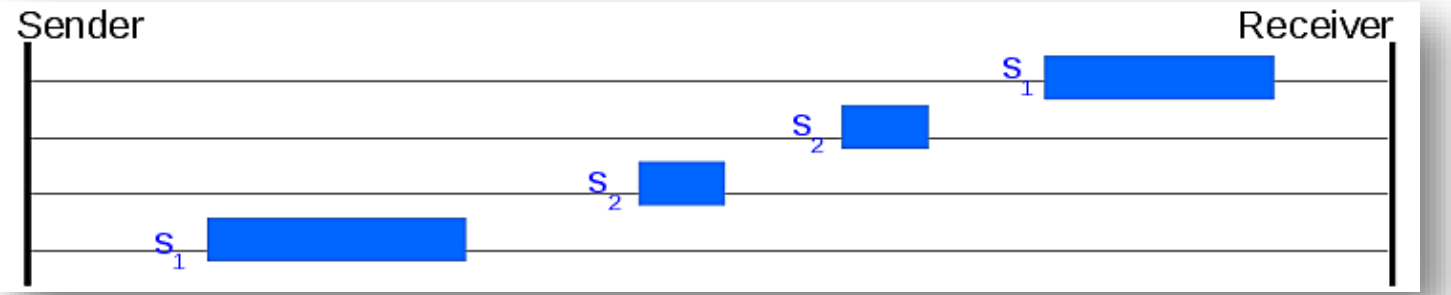


Fig.: [2]

[1] S. Wendzel et al.: Pattern-based Survey and Taxonomy for Network Covert Channels, ACM CSUR, Vol. 47(3), 2015.
[2] W. Mazurczyk, S. Wendzel, S. Zander et al.: Information Hiding in Communication Networks, WILEY-IEEE, 2016, Chapter 3.

PS2. Sequence Pattern

- **Introduced:** Wendzel et al., 2015 [1]

- **Illustration:** The covert channel alters the sequence of header/PDU elements to encode hidden information.

- **Examples:** (see [1] for evidence)
  - Sequence of DHCP options
  - Sequence of FTP commands
  - Sequence of HTTP header fields

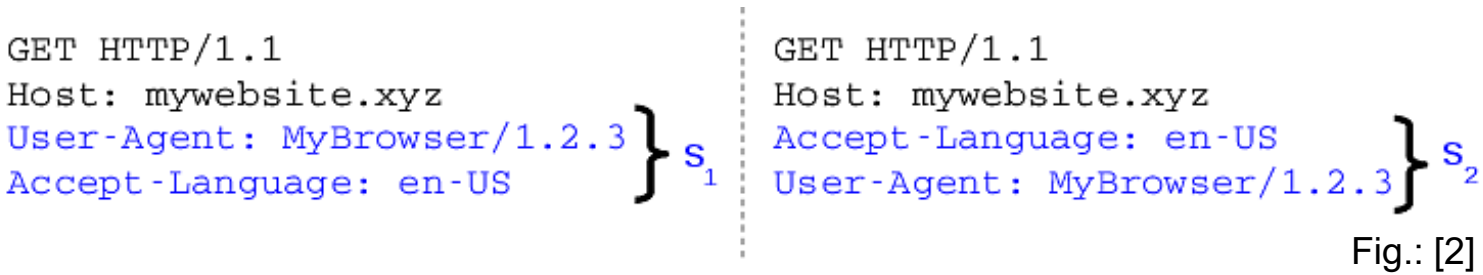


Fig.: [2]

- **Sub-patterns:**
  - PS2.a. Position Pattern (e.g. pos. of IPv4 option *x* in list of options)
  - PS2.b. Number of Elements Pattern (e.g. # of IPv4 options)

[1] S. Wendzel et al.: Pattern-based Survey and Taxonomy for Network Covert Channels, ACM CSUR, Vol. 47(3), 2015.
[2] W. Mazurczyk, S. Wendzel, S. Zander et al.: Information Hiding in Communication Networks, WILEY-IEEE, 2016, Chapter 3.

PS3. Add Redundancy Pattern

- **Introduced:** Wendzel et al., 2015 [1]

- **Illustration:** The covert channel creates new space within a given header element or within a PDU to hide data in it.

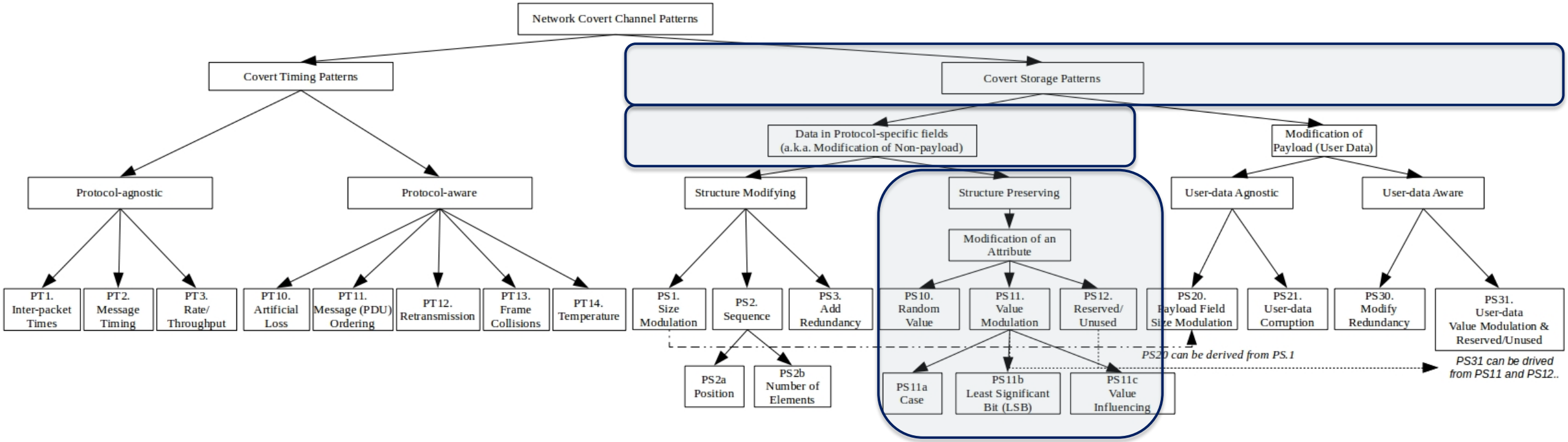
- **Examples:** (see [1] for evidence)
  - Extend HTTP headers with additional fields or extend values of existing fields

```
GET / HTTP/1.0
```

```
GET / HTTP/1.0
User-Agent: Mozilla/4.0
```

  - Create a new IPv6 destination option with embedded hidden data
  - Manipulate `pointer‘ and `length‘ values for IPv4 record route option to create space for data hiding

Let's Switch to Storage Patterns: Protocol-specific Fields Patterns (Headers + Padding) Category: Structure Preserving Patterns



Based on:

S. Wendzel, S. Zander, B. Fechner, C. Herdin: Pattern-based Survey and Taxonomy for Network Covert Channels, ACM CSUR, Vol. 47(3), 2015.

Extended by:

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 (http://ih-patterns.blogspot.com) ← always has the latest version of the taxonomy.

PS10. Random Values

- **Introduced:** Wendzel et al., 2015 [1]

- **Illustration:** The covert channel embeds hidden data in a header element containing a „random“ value.

- **Examples:** (see [1] for evidence)
  - Utilize IPv4 identifier field
  - Utilize the ISN of a TCP connection (cf. previous lecture on IH)
  - Utilize DHCP *xid* field

PS11. Value Modulation Pattern

- **Introduced:** Wendzel et al., 2015 [1]

- **Illustration:** The covert channel selects one of *n* values a header element can contain to encode a hidden message.

- **Examples:** (see [1,2] for evidence)
  - Send a frame to one of *n* available Ethernet addresses in a LAN
  - Encode information by the possible Time-to-live (TTL) values in IPv4 or in the Hop Limit values in IPv6

```
GET HTTP/1.1
Host: mywebsite.xyz
USeR-AGEnt: MyBrowser/1.2.3
```

$s_1 s_1 s_2 s_1$ $s_1 s_1 s_1 s_2 s_2$

```
GET HTTP/1.1
Host: mywebsite.xyz
user-agENt: MyBrowser/1.2.3
```

$s_2 s_2 s_2 s_2$ $s_2 s_2 s_1 s_1 s_2$

- **Sub-patterns:**
  - PS11.a. Case pattern: case modification of letters in plaintext headers (e.g. SMTP command letter cases)
  - PS11.b. LSB pattern: modify low order bits of header fields (e.g. TCP timestamp option)
  - PS11.c. Value influencing pattern: perform actions that influence some transferred value [2]

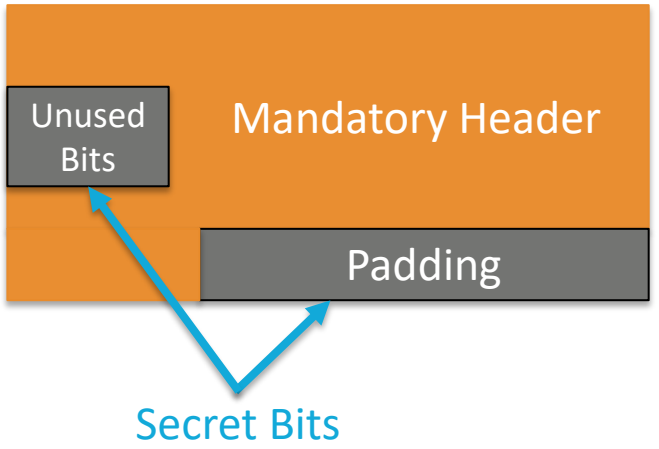
[1] S. Wendzel et al.: Pattern-based Survey and Taxonomy for Network Covert Channels, ACM CSUR, Vol. 47(3), 2015.
[2] A. Velinov, A. Mileva, S. Wendzel, W. Mazurczyk: Covert Channels in MQTT-based Internet of Things, IEEE ACCESS, Vol. 7, pp. 161899-161915, 2019.

PS12. Reserved/Unused Pattern

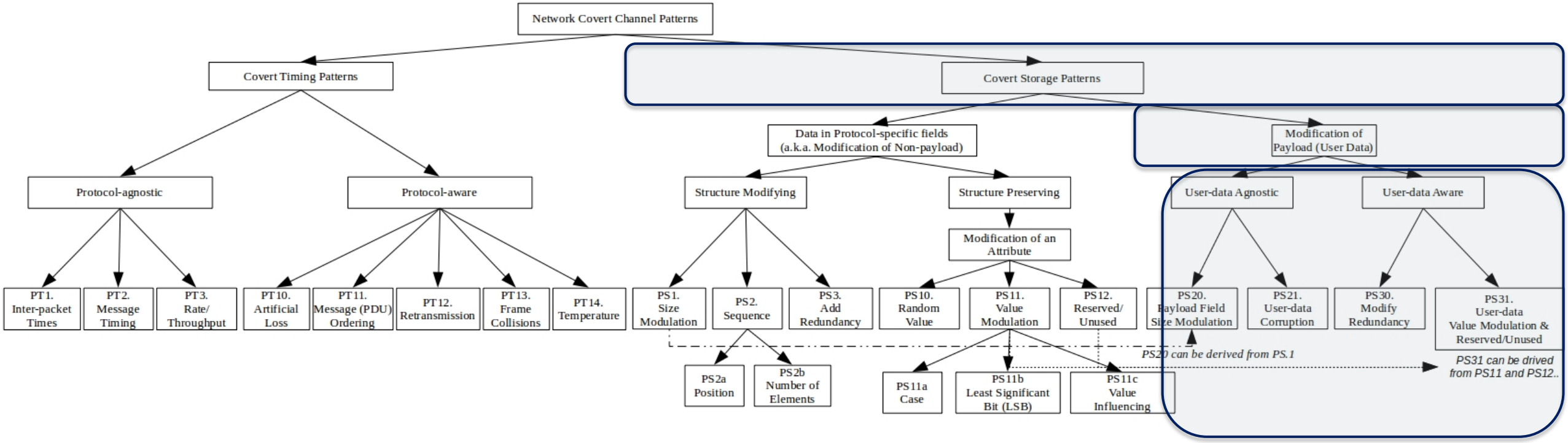
- **Introduced:** Wendzel et al., 2015 [1]

- **Illustration:** The covert channel encodes hidden data into a reserved or unused header/PDU element.

- **Examples:** (see [1] for evidence)
  - Utilize undefined/reserved bits in IEEE 802.5/data link layer frames
  - Utilize (currently) unused fields in IPv4, e.g. Identifier field, Don‘t Fragment (DF) flag or reserved flag or utilize unused fields in IP-IP encapsulation
  - Utilize the padding field of IEEE 802.3



Let's Switch to Storage Patterns: Payload Modifcation Patterns (Headers + Padding) Category: Both (User-data Agnostic & Aware) Patterns



Based on:

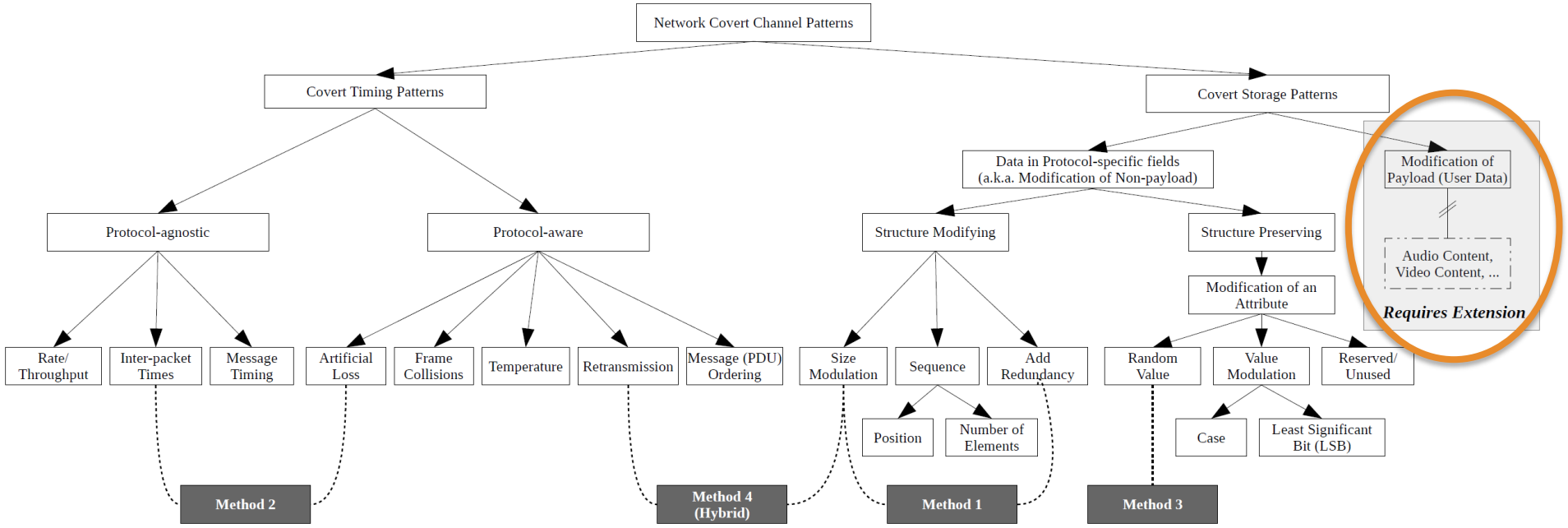
S. Wendzel, S. Zander, B. Fechner, C. Herdin: Pattern-based Survey and Taxonomy for Network Covert Channels, ACM CSUR, Vol. 47(3), 2015.

Extended by:

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 (http://ih-patterns.blogspot.com) ← always has the latest version of the taxonomy.

Why, at all? Isn't this Digital Media Steganography instead of Network Steganography??

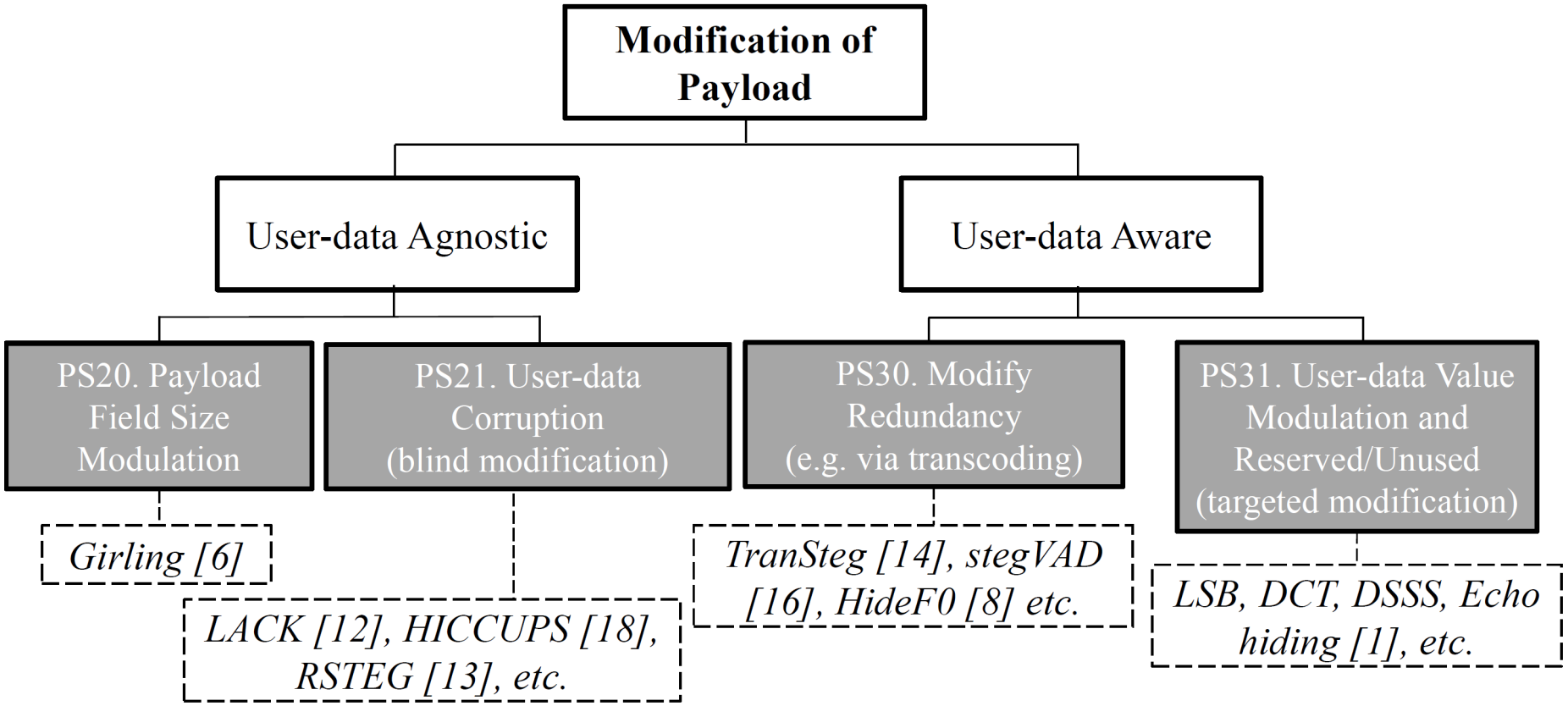
Turns out: no, it is not:



W. Mazurczyk, S. Wendzel, K. Cabaj: Towards Deriving Insights into Data Hiding Methods Using Pattern-based Approach, ARES'18.

Patterns for Payload Modification

(Network-level View, not Digital Media Steganography)

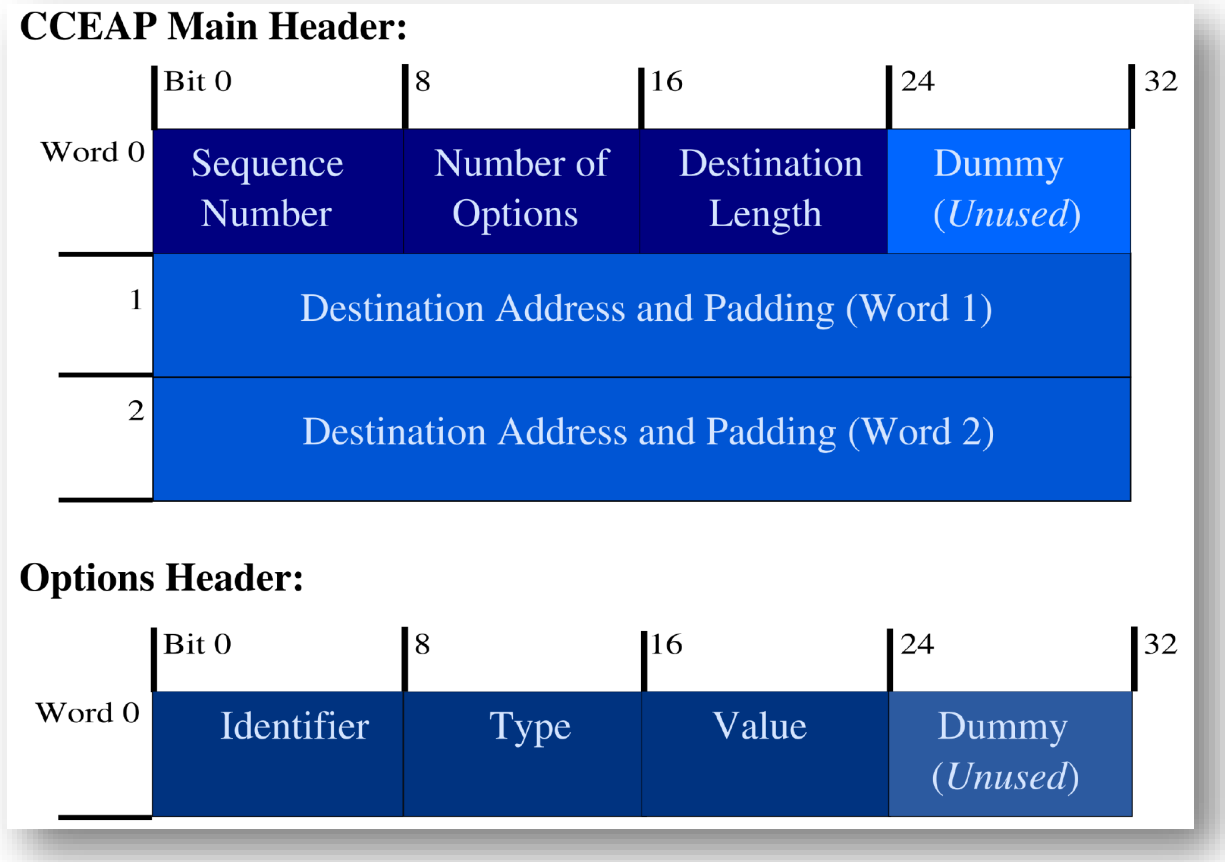


W. Mazurczyk, S. Wendzel, K. Cabaj: Towards Deriving Insights into Data Hiding Methods Using Pattern-based Approach, ARES'18.

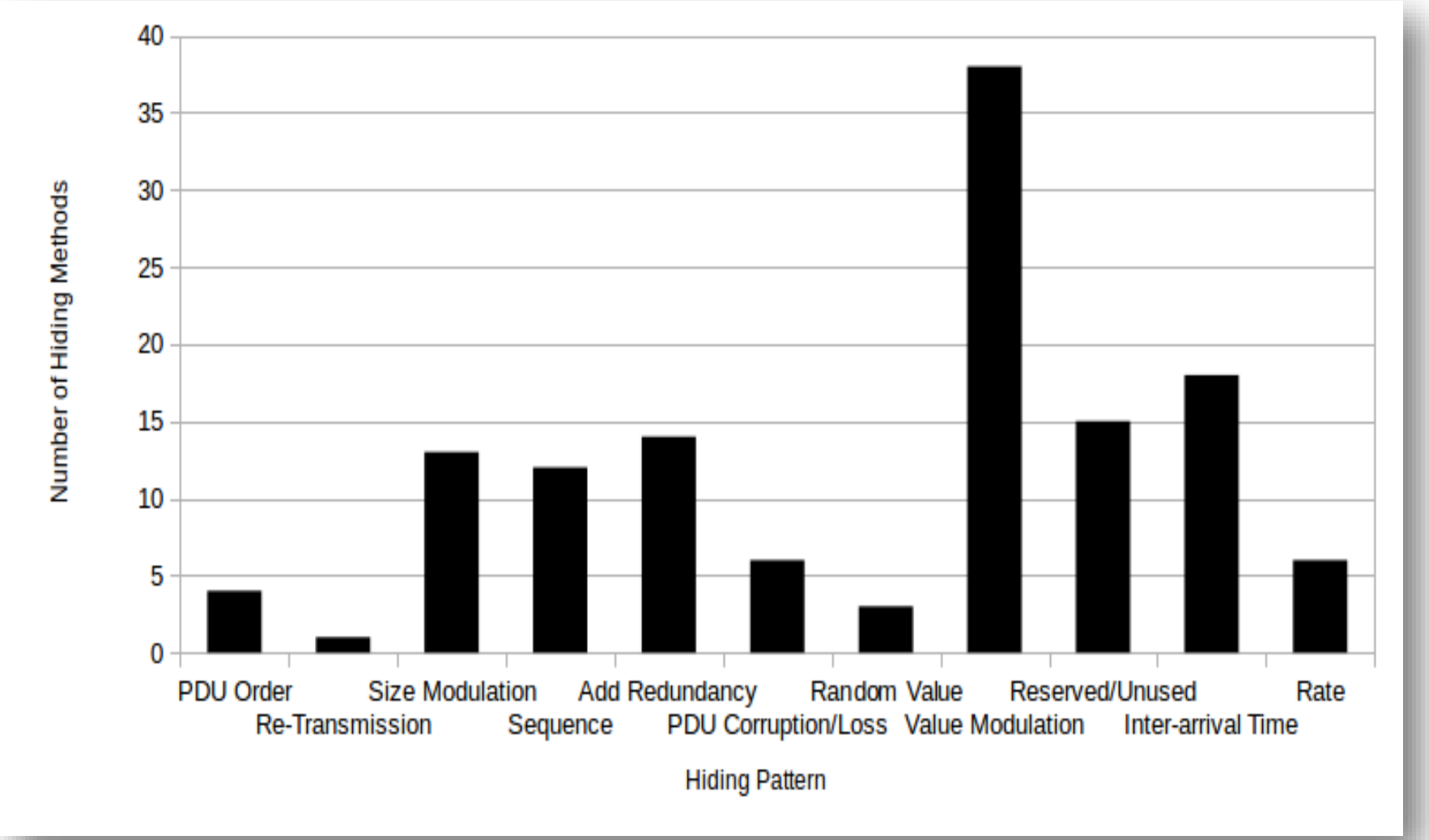
CCEAP

CCEAP is a tool for learning basic hiding patterns (not all known patterns are currently supported), available from Github.

- GUI is on the way.
- Sample exercises + solutions can be found here.
- There is also a poster.



Published Hiding Techniques [1]



[1] S. Wendzel et al. Unified Description for Network Information Hiding Methods, in: Journal of Universal Computer Science, 2016.

Final Remarks

Is it better to find new hiding **patterns** or to improve existing hiding **methods**?

Both is important and both should be done!

However, simply applying an existing method to some other network protocol (without presenting a new pattern or an improvement over existing work) is less “creative”.

See Ch. 9 „How to Describe a new Hiding Method?”, which also describes the process of finding new patterns (and ensuring the pattern is really new!).