NETWORK INFORMATION HIDING

CH. 5: HIDING PATTERNS

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

Prof. Dr. Steffen Wendzel

https://www.wendzel.de

Patterns

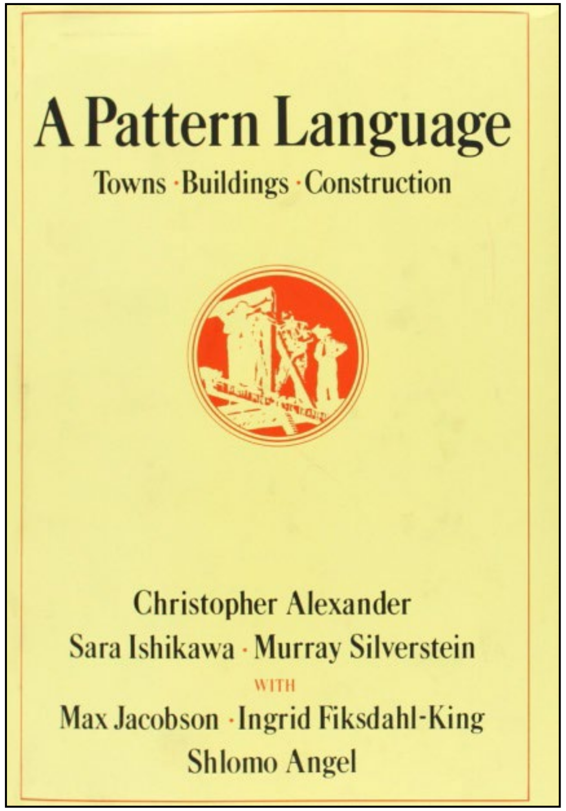
- What are „**Patterns**“?

  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
- They present 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.



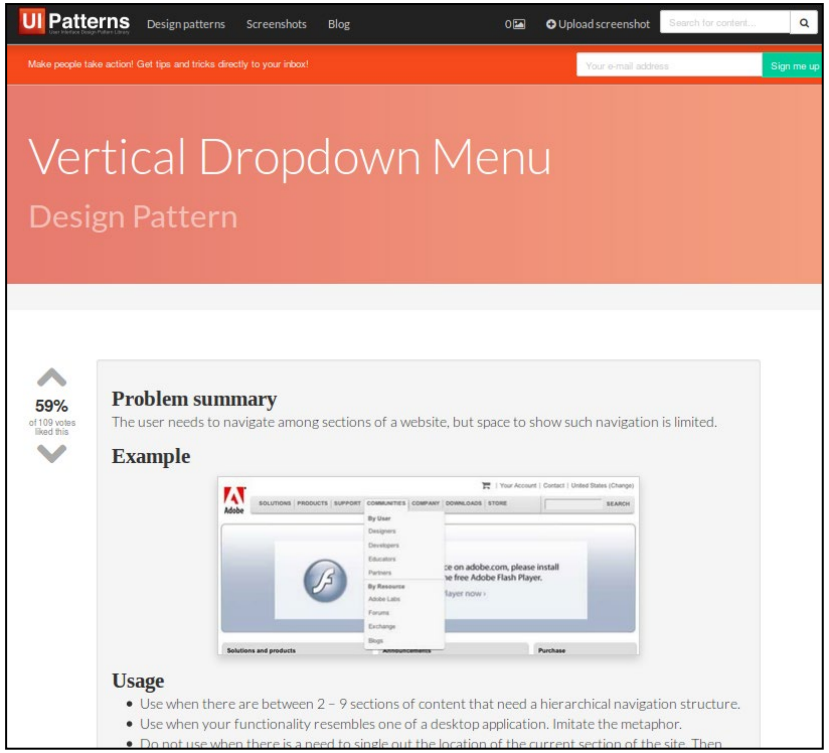
A Pattern Language

Towns · Buildings · Construction

Christopher Alexander
Sara Ishikawa · Murray Silverstein
WITH
Max Jacobson · Ingrid Fiksdahl-King
Shlomo Angel

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 (Fig.).
  - Example „Vertical Dropdown Menu“:
- <u>Note:</u> Patterns can even be used to generate user interfaces in a semi-automated manner, cf. [1].



Vertical Dropdown Menu

Design Pattern

Problem summary

The user needs to navigate among sections of a website, but space to show such navigation is limited.

Example

Usage

- Use when there are between 2 – 9 sections of content that need a hierarchical navigation structure.
- Use when your functionality resembles one of a desktop application. Imitate the metaphor.
- Do not use when there is a need to single out the location of the current section of the site. Then

[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.

Patterns

- „Security Patterns“:
  - *“Patterns are reusable packages incorporating expert knowledge. Specifically, a pattern represents a frequently recurring structure, behavior, activity, process, or “thing” during the software development process.” [1]*
  - *“A **security pattern** includes security knowledge and is reusable as a security package.”* [1]
  - These security patterns can be found at basically all levels of the software development lifecycle; they can describe knowledge, techniques and means **to improve the security** of a system/to solve a security problem but they can also describe an attack.

    Two sides of a coin: attack and defense

- “Cyber Pattern”:
  - Link between architectural pattern and security pattern.

[1] Yoshioka, N., Washizaki, H., Maruyama, K.: A survey on security patterns, Progress in Informatics, No. 5, pp. 35-47, 2008.

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 <u>three</u> 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.

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.
  - We only use a subset of PLML as it suffices for our purposes.

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

PLML

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

Hiding patterns can utilize 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

Hiding patterns were introduced in [1], the definition was slightly adjusted in [2].

Hiding Patterns describe they **key idea of hiding techniques on abstract level**.
They help **cleaning up terminology, and** can be used to form **taxonomy**.

[1] S. Wendzel, S. Zander, B. Fechner, C. Herdin: *Pattern-based Survey of Network Covert Channel Techniques*, ACM CSUR, 47(3), 2015.
[2] S. Wendzel, L. Caviglione, B. Fechner: *Poster: Steganography Hiding Patterns: A Brief Review*, in Proc. EICC'22.

Patterns in Network Information Hiding

Idea of using patterns in network information hiding was first introduced in [1]. See http://www.ih-patterns.blogspot.com where you can also download the paper.

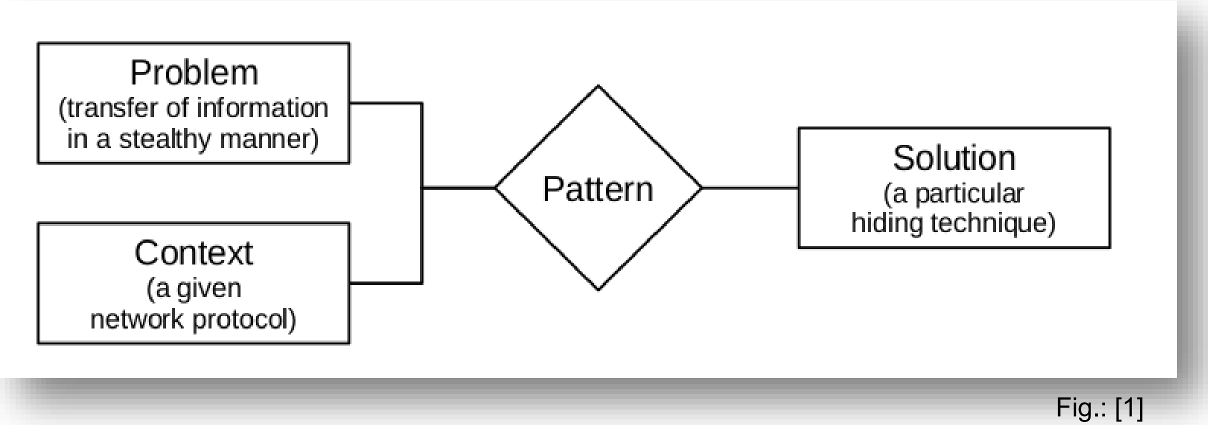

Problem
(transfer of information in a stealthy manner)
Context
(a given network protocol)
Pattern
Solution
(a particular hiding technique)

Fig.: [1]

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

The following attributes were used

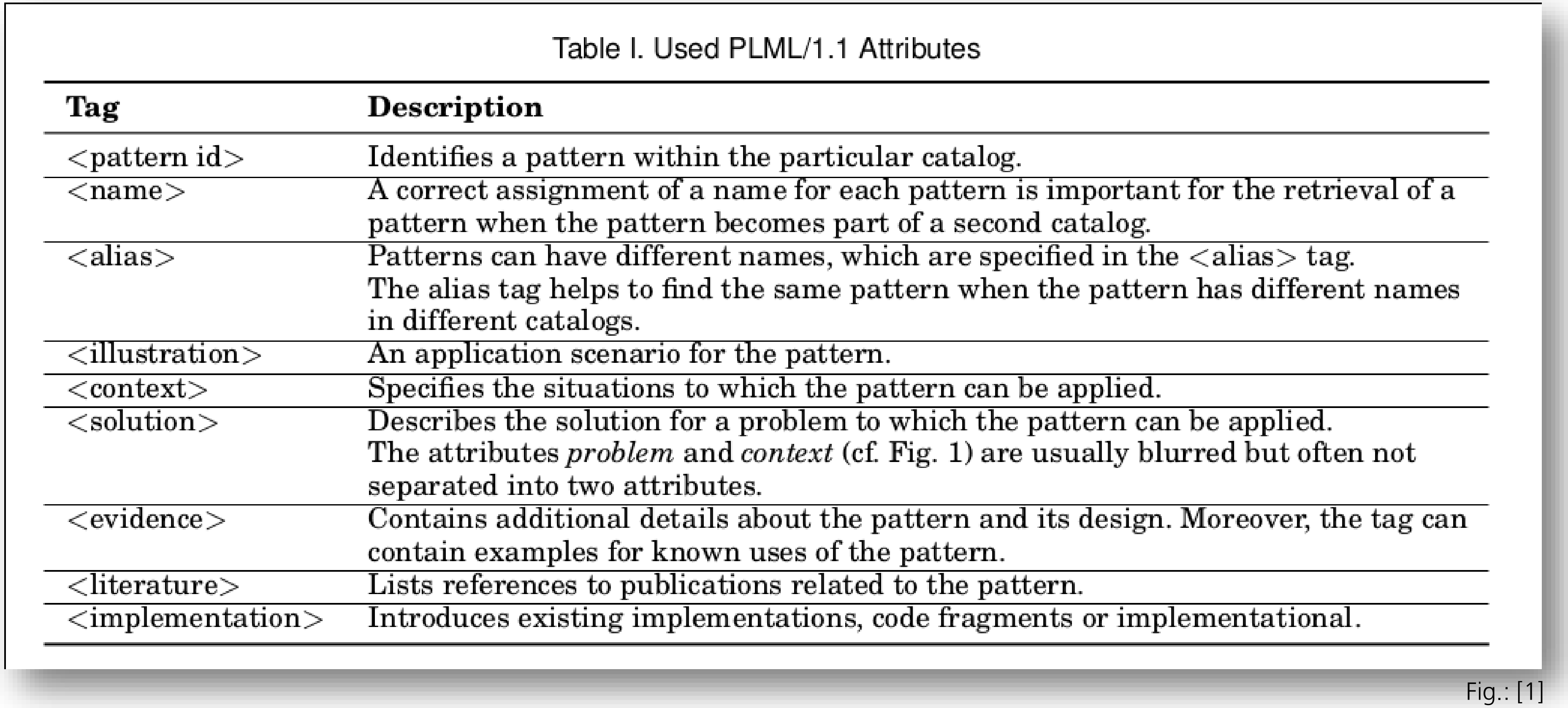


Table I. Used PLML/1.1 Attributes

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.

Fig.: [1]

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

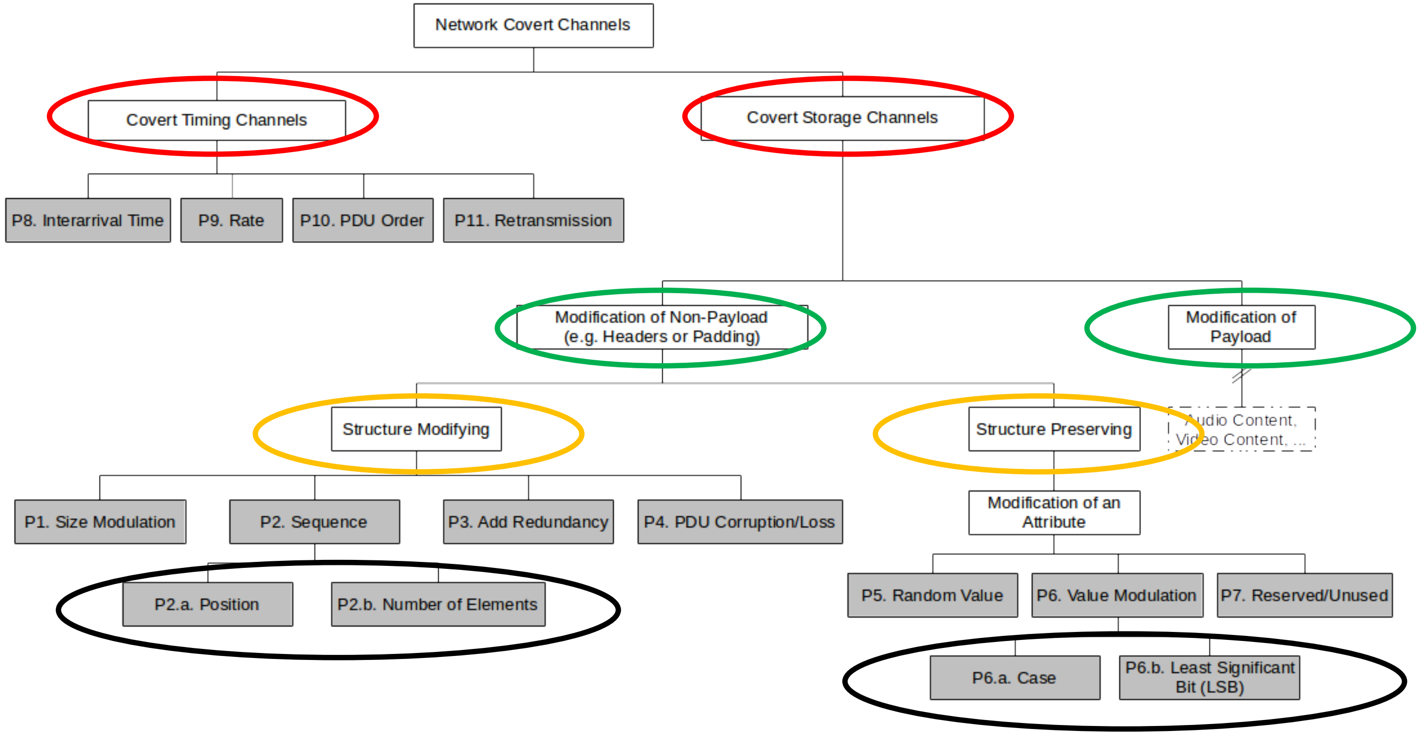
Patterns in Network Information Hiding

- A few hundred network hiding techniques are known; they hide secret information in meta data of network traffic.
  - Inconsistent terminology.
  - Scientific 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, …).

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

Patterns in Network 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.



Network Covert Channels

Covert Timing Channels

Covert Storage Channels

P8. Interarrival Time

P9. Rate

P10. PDU Order

P11. Retransmission

Modification of Non-Payload (e.g. Headers or Padding)

Modification of Payload

Structure Modifying

Structure Preserving

Audio Content, Video Content, ...

P1. Size Modulation

P2. Sequence

P3. Add Redundancy

P4. PDU Corruption/Loss

Modification of an Attribute

P2.a. Position

P2.b. Number of Elements

P5. Random Value

P6. Value Modulation

P7. Reserved/Unused

P6.a. Case

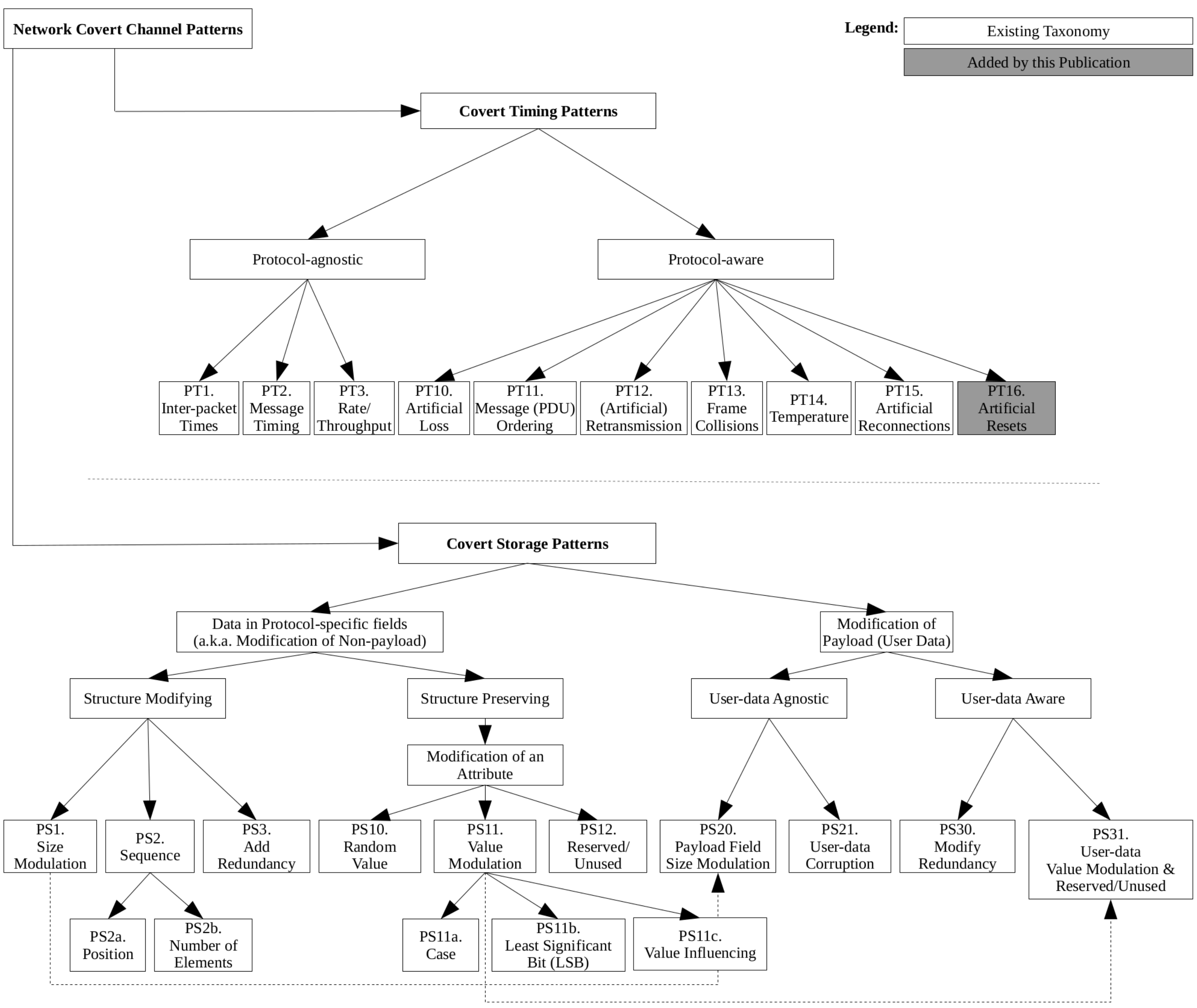
P6.b. Least Significant Bit (LSB)

Fig.: [1]

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

Latest Patterns Taxonomy Version

Hiding techniques categorized into 10 timing and 10 storage patterns, plus sub-patterns. Pattern names and their numbers were updated and extended in 2016, 2018, 2019, (2020) and 2021.



Network Covert Channel Patterns

Legend: Existing Taxonomy | Added by this Publication

Covert Timing Patterns

Protocol-agnostic

PT1. Inter-packet Times

PT2. Message Timing

PT3. Rate/ Throughput

Protocol-aware

PT10. Artificial Loss

PT11. Message (PDU) Ordering

PT12. (Artificial) Retransmission

PT13. Frame Collisions

PT14. Temperature

PT15. Artificial Reconnections

PT16. Artificial Resets

Covert Storage Patterns

Data in Protocol-specific fields (a.k.a. Modification of Non-payload)

Structure Modifying

PS1. Size Modulation

PS2. Sequence

PS2a. Position

PS2b. Number of Elements

PS3. Add Redundancy

Structure Preserving

Modification of an Attribute

PS10. Random Value

PS11. Value Modulation

PS11a. Case

PS11b. Least Significant Bit (LSB)

PS11c. Value Influencing

PS12. Reserved/ Unused

Modification of Payload (User Data)

User-data Agnostic

PS20. Payload Field Size Modulation

PS21. User-data Corruption

User-data Aware

PS30. Modify Redundancy

PS31. User-data Value Modulation & Reserved/Unused

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.

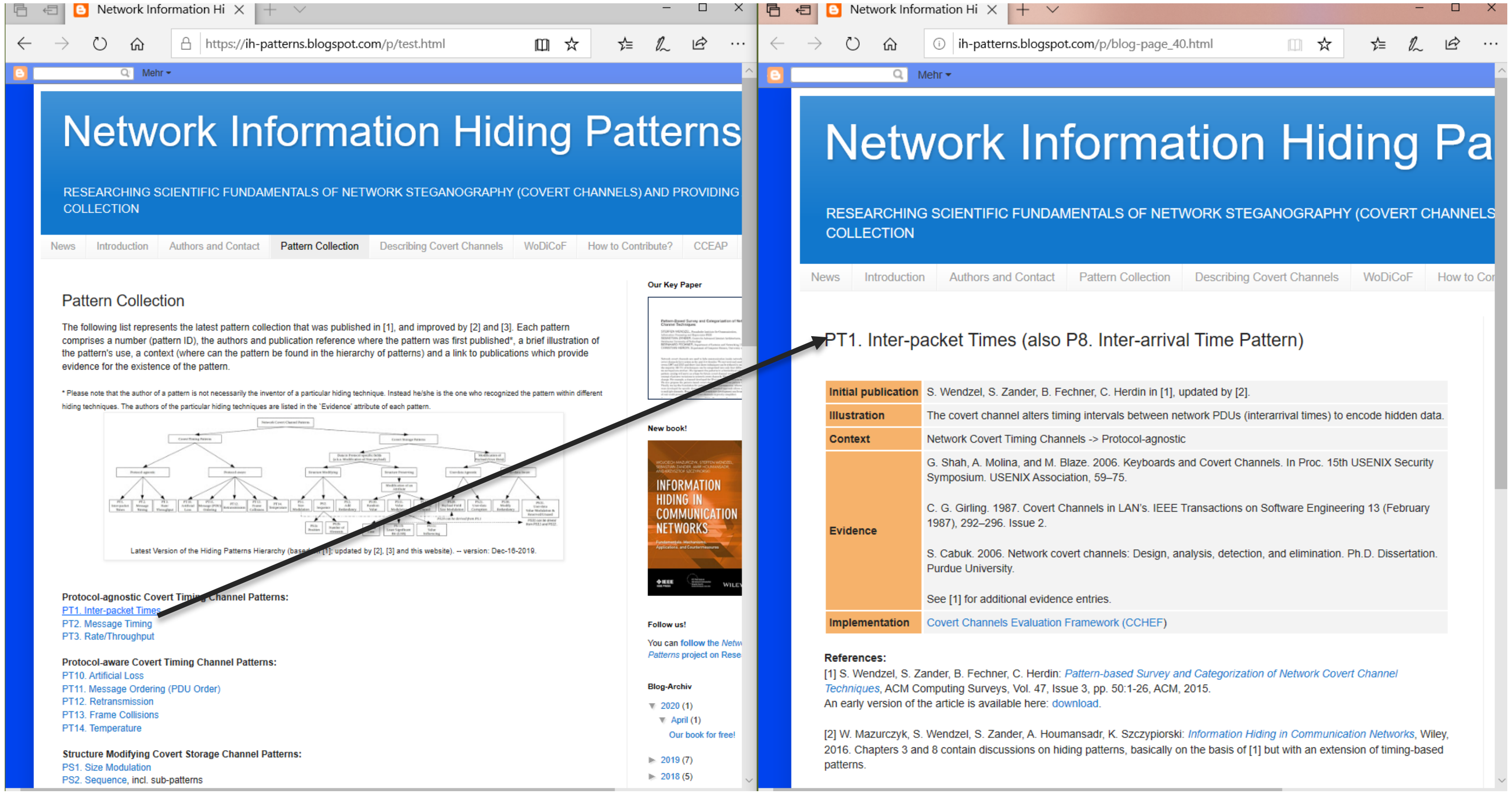
A. Mileva, A. Velinov, L. Hartmann, S. Wendzel, W. Mazurczyk: *Comprehensive Analysis of MQTT 5.0 Susceptibility to Network Covert Channels*, Computers & Security, Elsevier, 2021.

L. Hartmann, S. Zillien, S. Wendzel: Analysis of New Covert Channels in CoAP, in: Proc. DETONATOR workshop (part of Proc. EICC 2021), ACM, 2021.

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

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

Latest Version of Pattern Taxonomy


Network Information Hi
https://ih-patterns.blogspot.com/p/test.html
Mehr
Network Information Hiding Patterns
RESEARCHING SCIENTIFIC FUNDAMENTALS OF NETWORK STEGANOGRAPHY (COVERT CHANNELS) AND PROVIDING COLLECTION
News
Introduction
Authors and Contact
Pattern Collection
Describing Covert Channels
WoDiCoF
How to Contribute?
CCEAP
Our Key Paper
New book!
INFORMATION HIDING IN COMMUNICATION NETWORKS
WILEY
Follow us!
You can follow the Netw
Patterns project on Rese
Blog-Archiv
2020 (1)
April (1)
Our book for free!
2019 (7)
2018 (5)
Network Information Hi
ih-patterns.blogspot.com/p/blog-page_40.html
Mehr
Network Information Hiding Pa
RESEARCHING SCIENTIFIC FUNDAMENTALS OF NETWORK STEGANOGRAPHY (COVERT CHANNELS COLLECTION
News
Introduction
Authors and Contact
Pattern Collection
Describing Covert Channels
WoDiCoF
How to Cor

Pattern Collection

The following list represents the latest pattern collection that was published in [1], and improved by [2] and [3]. Each pattern comprises a number (pattern ID), the authors and publication reference where the pattern was first published*, a brief illustration of the pattern's use, a context (where can the pattern be found in the hierarchy of patterns) and a link to publications which provide evidence for the existence of the pattern.

* Please note that the author of a pattern is not necessarily the inventor of a particular hiding technique. Instead he/she is the one who recognized the pattern within different hiding techniques. The authors of the particular hiding techniques are listed in the `Evidence' attribute of each pattern.

Latest Version of the Hiding Patterns Hierarchy (based on [1]; updated by [2], [3] and this website). -- version: Dec-16-2019.

Protocol-agnostic Covert Timing Channel Patterns:
PT1. Inter-packet Times
PT2. Message Timing
PT3. Rate/Throughput

Protocol-aware Covert Timing Channel Patterns:
PT10. Artificial Loss
PT11. Message Ordering (PDU Order)
PT12. Retransmission
PT13. Frame Collisions
PT14. Temperature

Structure Modifying Covert Storage Channel Patterns:
PS1. Size Modulation
PS2. Sequence, incl. sub-patterns

PT1. Inter-packet Times (also P8. Inter-arrival Time Pattern)

Initial publication	S. Wendzel, S. Zander, B. Fechner, C. Herdin in [1], updated by [2].
Illustration	The covert channel alters timing intervals between network PDUs (interarrival times) to encode hidden data.
Context	Network Covert Timing Channels -> Protocol-agnostic
Evidence	G. Shah, A. Molina, and M. Blaze. 2006. Keyboards and Covert Channels. In Proc. 15th USENIX Security Symposium. USENIX Association, 59–75. C. G. Girling. 1987. Covert Channels in LAN's. IEEE Transactions on Software Engineering 13 (February 1987), 292–296. Issue 2. S. Cabuk. 2006. Network covert channels: Design, analysis, detection, and elimination. Ph.D. Dissertation. Purdue University. See [1] for additional evidence entries.
Implementation	Covert Channels Evaluation Framework (CCHEF)

References:

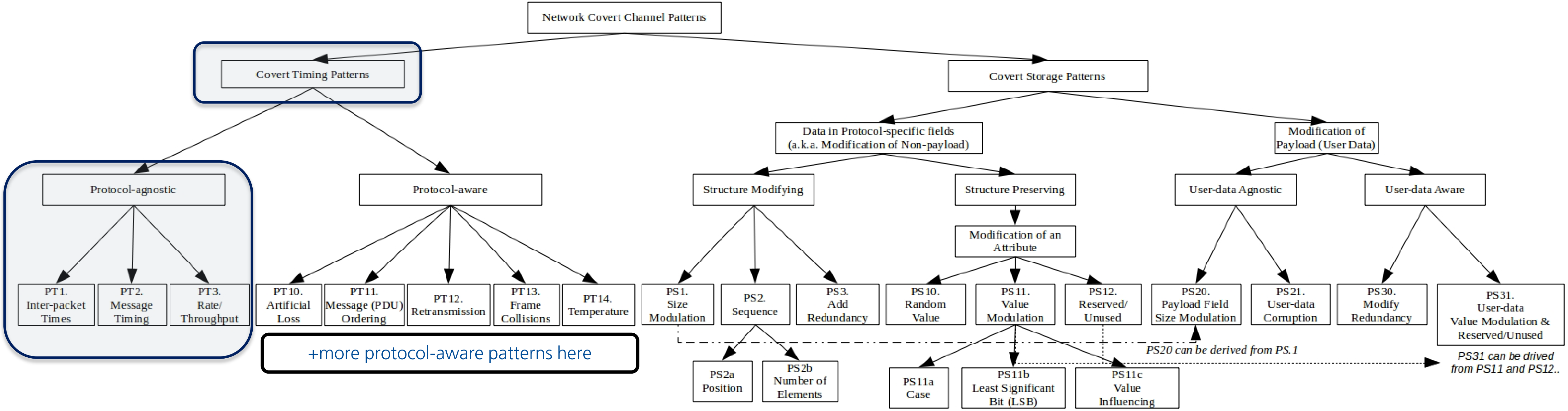
[1] S. Wendzel, S. Zander, B. Fechner, C. Herdin: *Pattern-based Survey and Categorization of Network Covert Channel Techniques*, ACM Computing Surveys, Vol. 47, Issue 3, pp. 50:1-26, ACM, 2015.
An early version of the article is available here: download.

[2] W. Mazurczyk, S. Wendzel, S. Zander, A. Houmansadr, K. Szczypiorski: *Information Hiding in Communication Networks*, Wiley, 2016. Chapters 3 and 8 contain discussions on hiding patterns, basically on the basis of [1] but with an extension of timing-based patterns.

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

Let’s go through all these patterns!

We start with the Timing Patterns: Protocol agnostic Patterns



+more protocol-aware patterns here

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://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

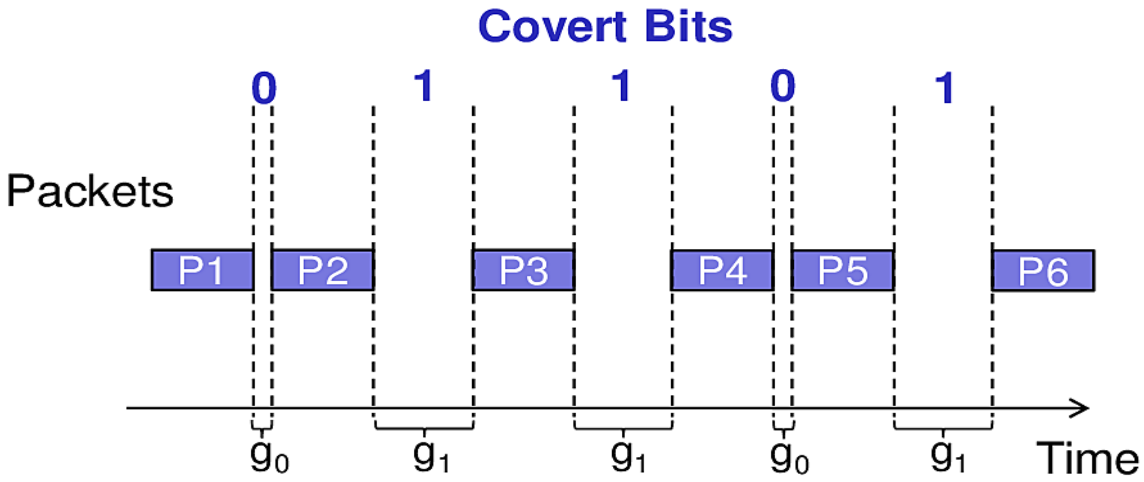
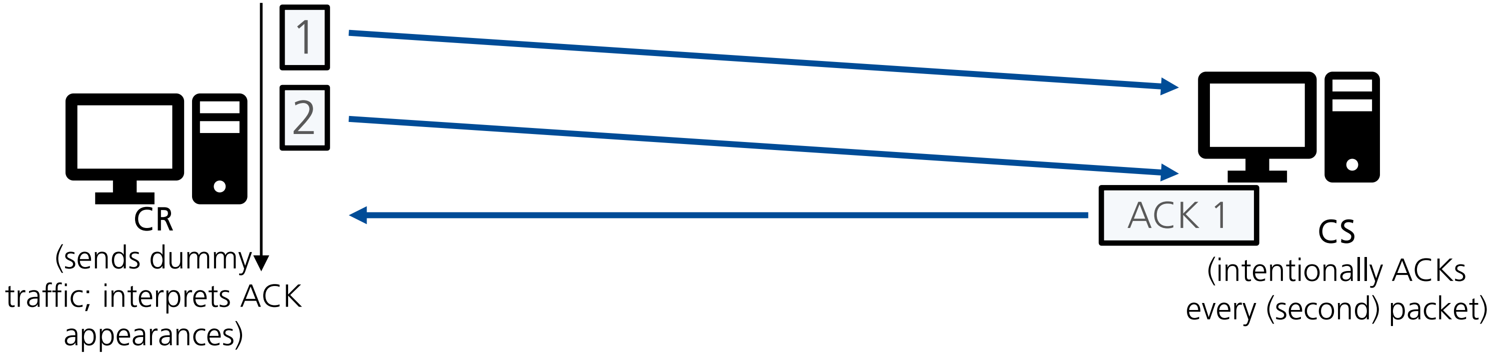


Fig.: [2]

[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
2
ACK 1
CR
(sends dummy traffic; interprets ACK appearances)
CS
(intentionally ACKs every (second) packet)

[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.

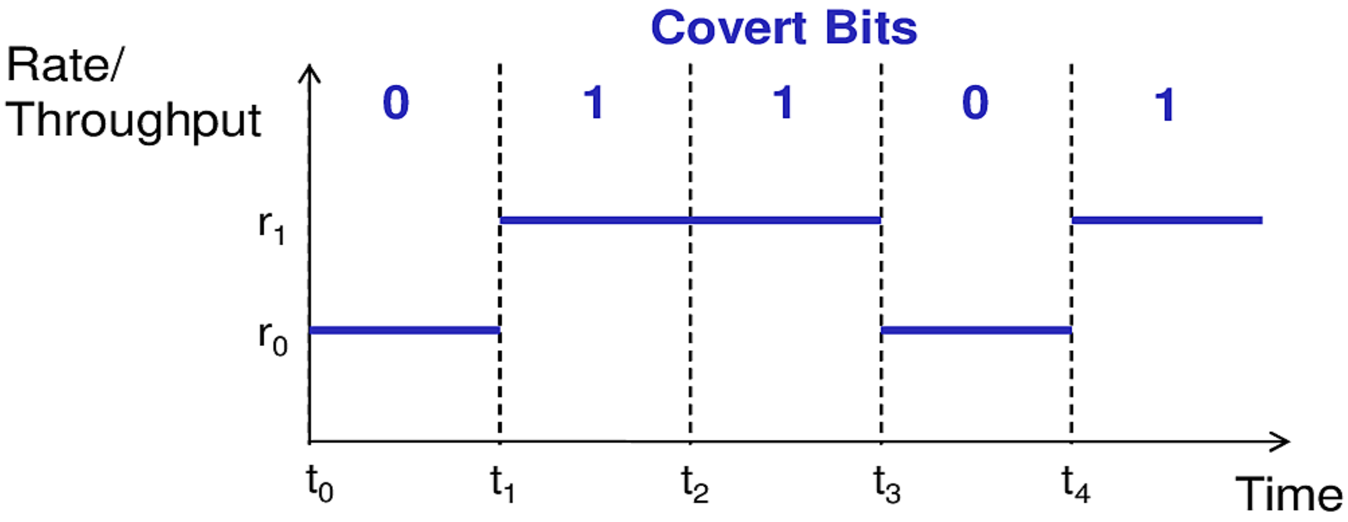
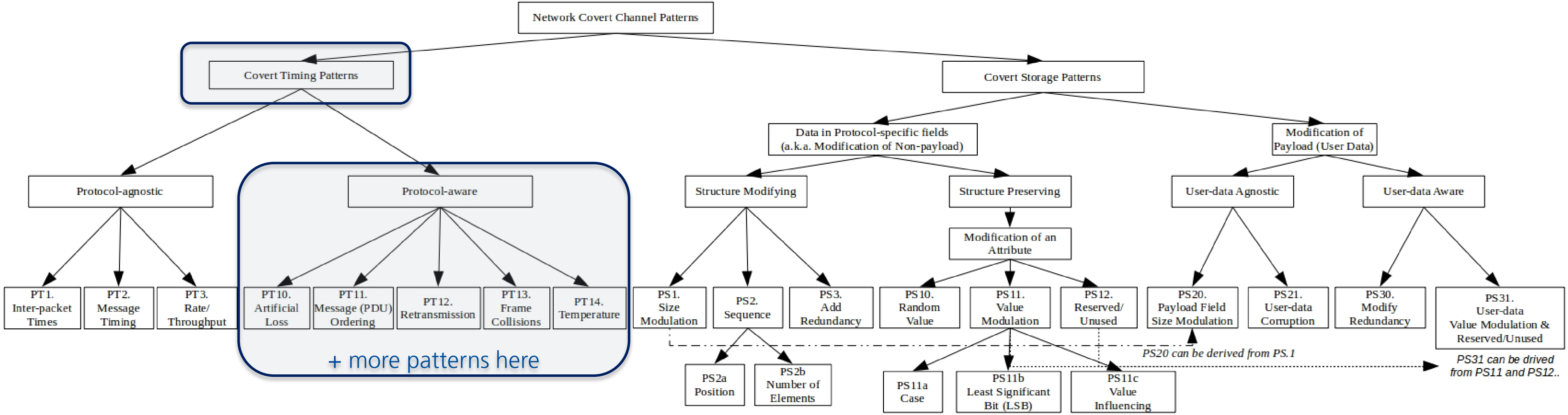


Fig.: [2]

[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:



Network Covert Channel Patterns

Covert Timing Patterns

Covert Storage Patterns

Protocol-agnostic

Protocol-aware

PT1. Inter-packet Times

PT2. Message Timing

PT3. Rate/ Throughput

PT10. Artificial Loss

PT11. Message (PDU) Ordering

PT12. Retransmission

PT13. Frame Collisions

PT14. Temperature

+ more patterns here

Data in Protocol-specific fields (a.k.a. Modification of Non-payload)

Modification of Payload (User Data)

Structure Modifying

Structure Preserving

User-data Agnostic

User-data Aware

Modification of an Attribute

PS1. Size Modulation

PS2. Sequence

PS3. Add Redundancy

PS10. Random Value

PS11. Value Modulation

PS12. Reserved/ Unused

PS20. Payload Field Size Modulation

PS21. User-data Corruption

PS30. Modify Redundancy

PS31. User-data Value Modulation & Reserved/Unused

PS2a Position

PS2b Number of Elements

PS11a Case

PS11b Least Significant Bit (LSB)

PS11c Value Influencing

PS20 can be derived from PS.1

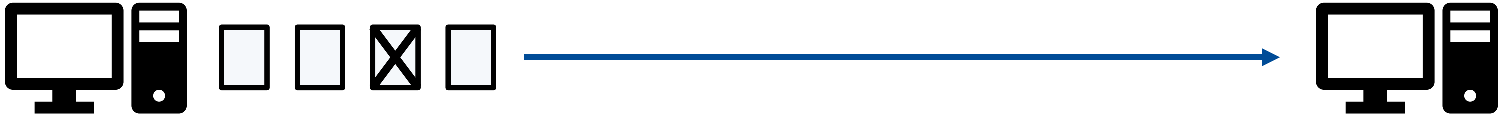
PS31 can be drived from PS11 and PS12..

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://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

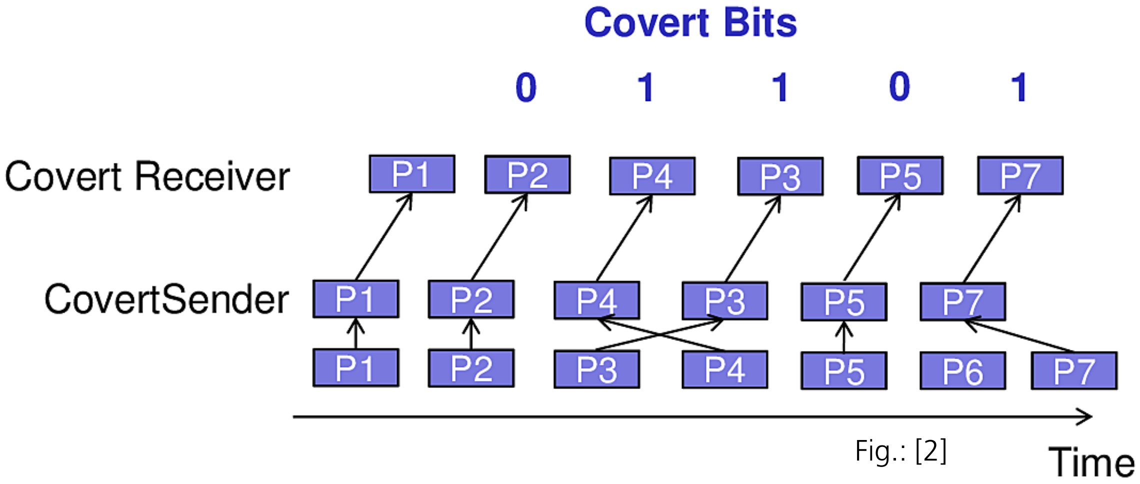
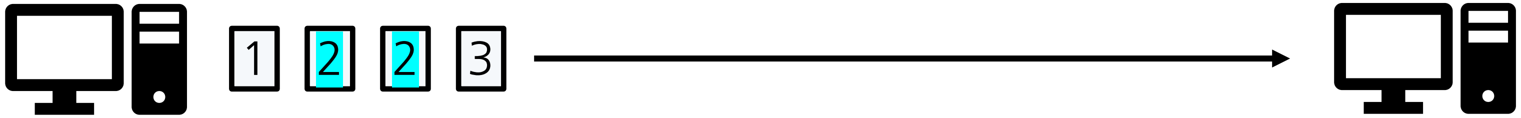


Fig.: [2]

[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.



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

PT13. Frame Collisions

- **Introduced: Introduced:** Mazurczyk et al. 2016 [1]; derived from and replaced the former "PDU Corruption" pattern that 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

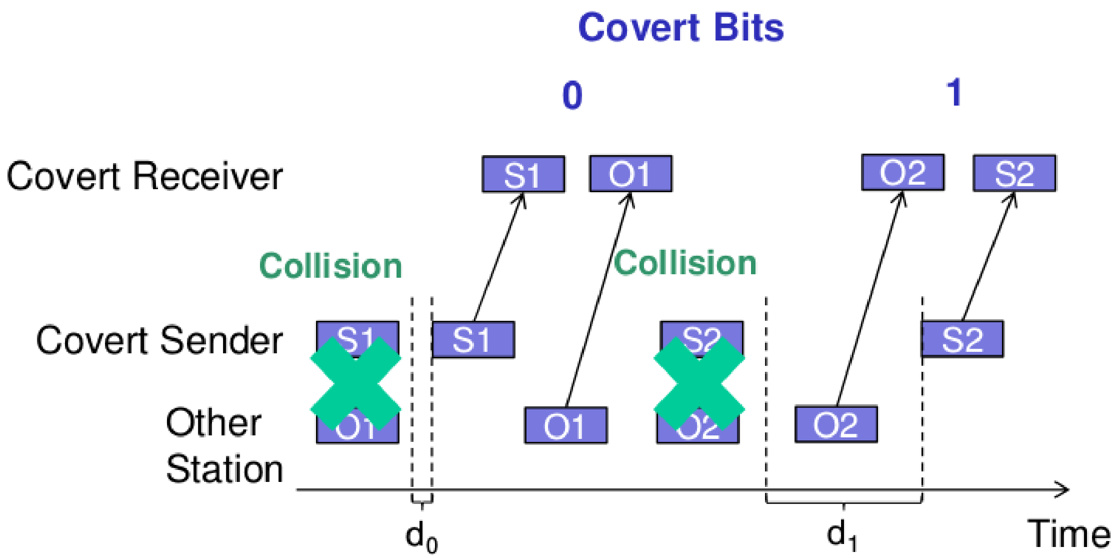


Fig.: [1]

[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

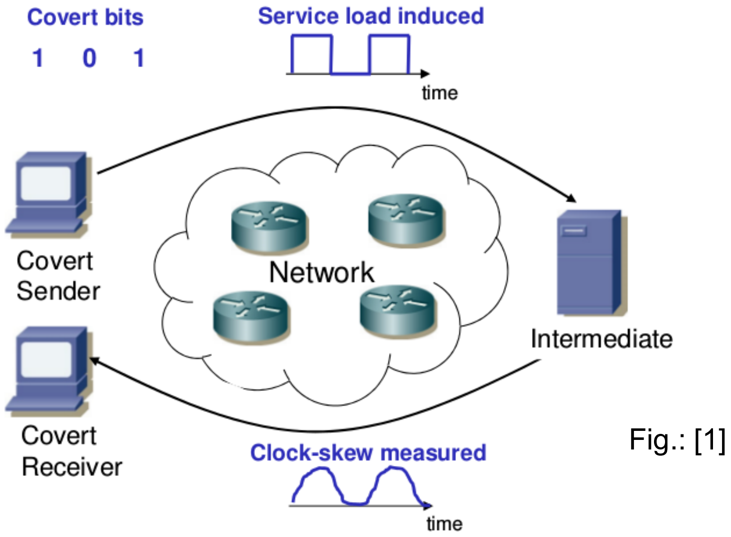


Fig.: [1]

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

PT15. Artificial Re-connections

- **Introduced:** Mileva et al., 2021 [1].

- **Illustration:** The **Artificial Re-connections** pattern employs artificial (forced) reconnections to transfer secret messages. The CS influences connections of third-party nodes in a way that **their connection states** to either a central element (e.g. MQTT broker or a server) or a peer (in a P2P network) are terminated and then re-established. The CR must be capable of monitoring these re-connections.

- **Examples:**
  - Triggered Re-connections in WiFi [2] or MQTT environments [1].

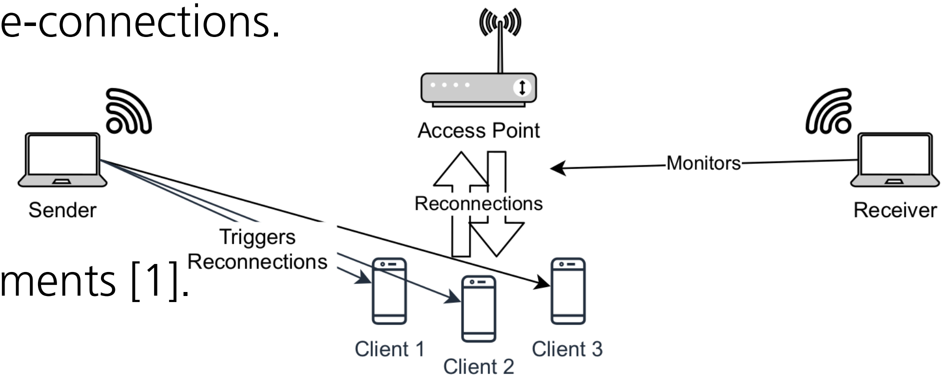


Fig.: [2]

[1] A. Mileva, A. Velinov, L. Hartmann et al.: *Comprehensive Analysis of MQTT 5.0 Susceptibility to Network Covert Channels*, Computers & Security, Elsevier, 2021.
[2] S. Zillien, S. Wendzel: *Reconnection-based Covert Channels in Wireless Networks*, in Proc. 36th IFIP SEC, Springer, 2021.

PT16. Artificial Resets

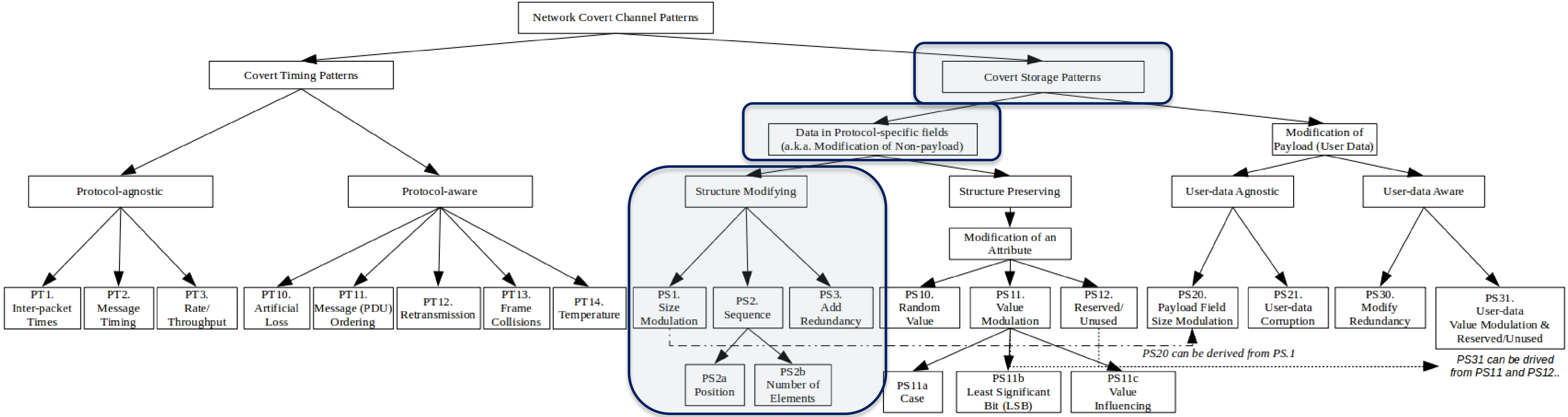
- **Introduced:** Hartmann et al., 2021 [1].

- **Illustration:** The pattern **Artificial Resets** is embedded by a covert sender that causes a connection reset of third-party nodes, whose connection states are observed by one or more covert receiver(s). The pattern is a protocol-aware timing pattern.

- **Examples [1]:**
  - CS-triggered TCP reset (using classical TCP reset attack).
  - CS-triggered resets in CoAP [1]: "[…] embedded by a) sending an empty (non-)confirmable message; b) sending a malformed packet; c) forcing a reboot of a connected node to let it forget its state, leading to a reset."

[1] L. Hartmann, S. Zillien, S. Wendzel: Analysis of New Covert Channels in CoAP, in: Proc. DETONATOR workshop (part of Proc. EICC 2021), ACM, 2021.

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



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://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

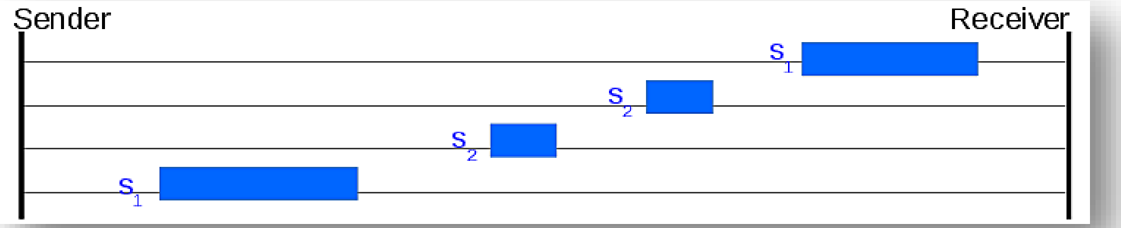
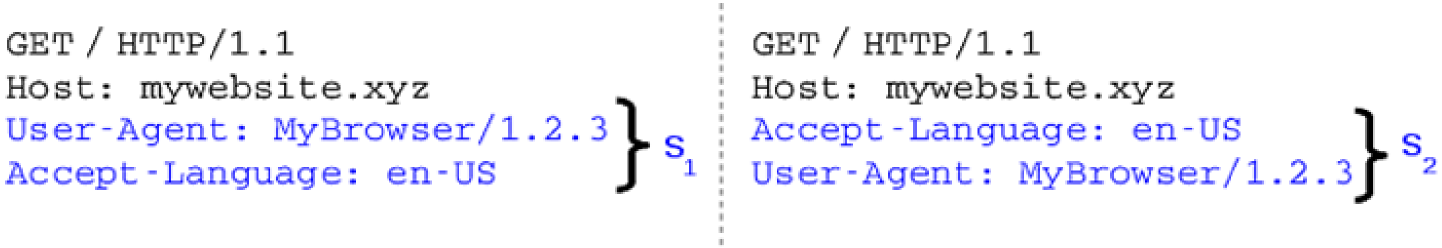


Fig.: [2]

[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



```
GET / HTTP/1.1
Host: mywebsite.xyz
User-Agent: MyBrowser/1.2.3
Accept-Language: en-US
```

```
GET / HTTP/1.1
Host: mywebsite.xyz
Accept-Language: en-US
User-Agent: MyBrowser/1.2.3
```

- **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

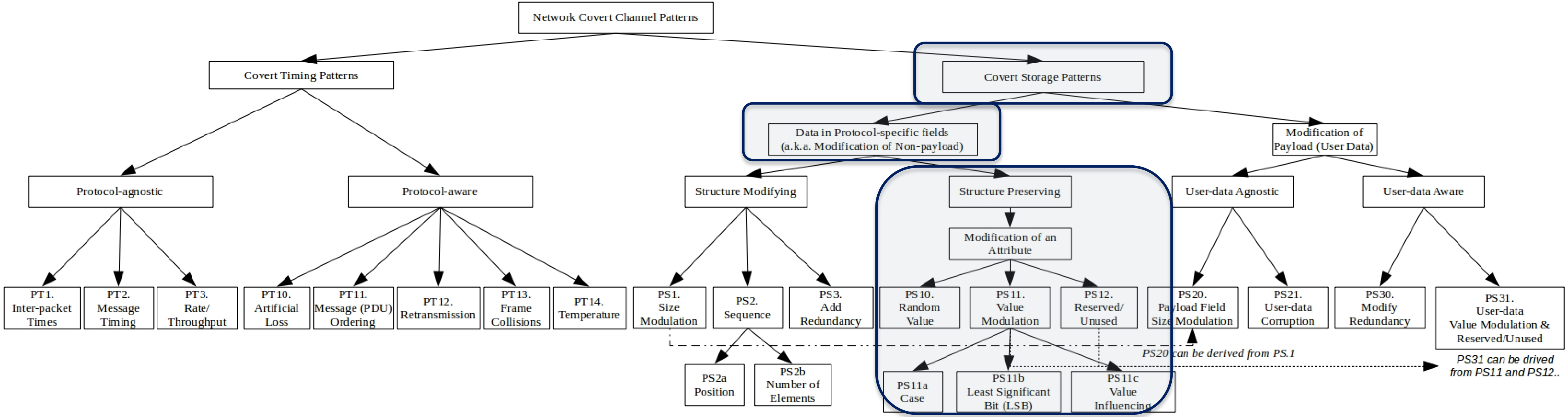
- **Introduced:** Wendzel et al., 2015 [1]
- **Illustration:** The covert channel creates new space within a given header element or within a PDU to hide data in it.
- **Examples:** (see [1] for evidence)
  - Extend HTTP headers with additional fields or extend values of existing fields

```
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

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

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



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://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.

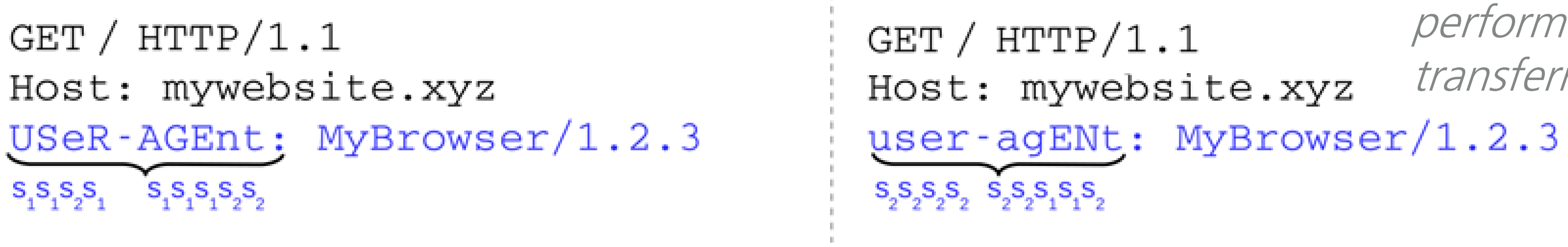
- **Examples:** (see [1] for evidence)
  - Utilize IPv4 identifier field
  - Utilize the ISN of a TCP connection
  - Utilize DHCP *xid* field

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

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

- **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]*



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

$s_1s_1s_2s_1$ $s_1s_1s_1s_2s_2$

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

$s_2s_2s_2s_2$ $s_2s_2s_1s_1s_2$

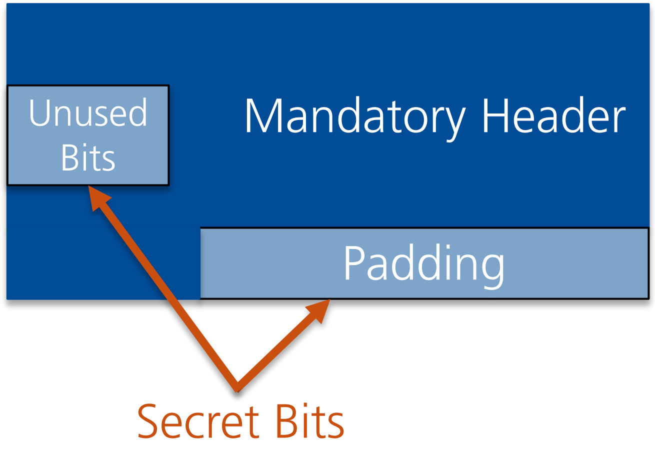
[1] S. Wendzel et al.: Pattern-based Survey and Taxonomy for Network Covert Channels, ACM CSUR, Vol. 47(3), 2015.
[2] A. Velinov, A. Mileva, S. Wendzel, W. Mazurczyk: Covert Channels in MQTT-based Internet of Things, IEEE ACCESS, Vol. 7, pp. 161899-161915, 2019.

PS12. Reserved/Unused Pattern

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

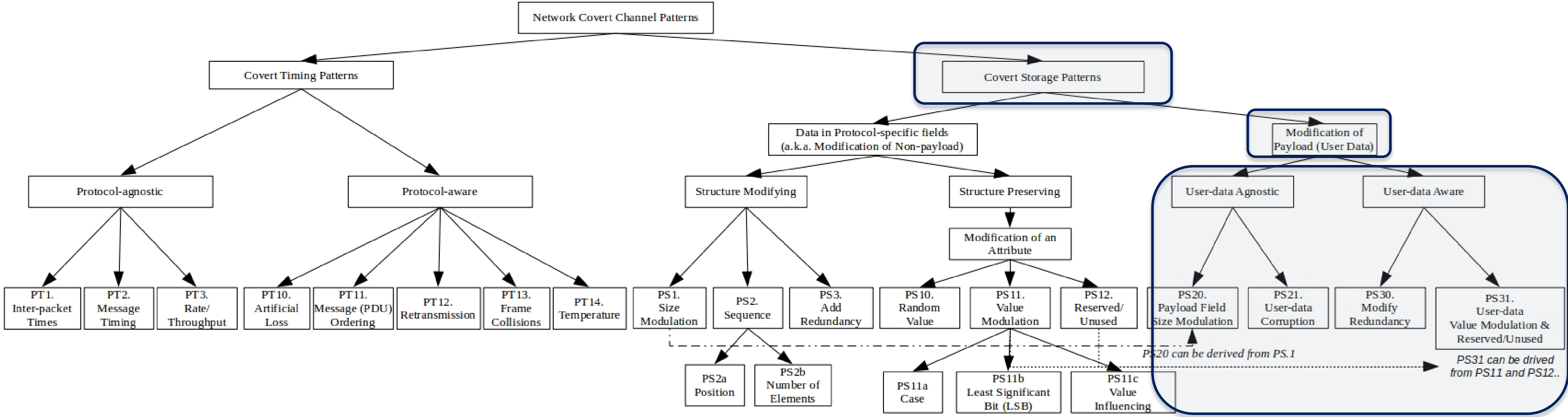
- **Illustration:** The covert channel encodes hidden data into a reserved or unused header/PDU element.

- **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



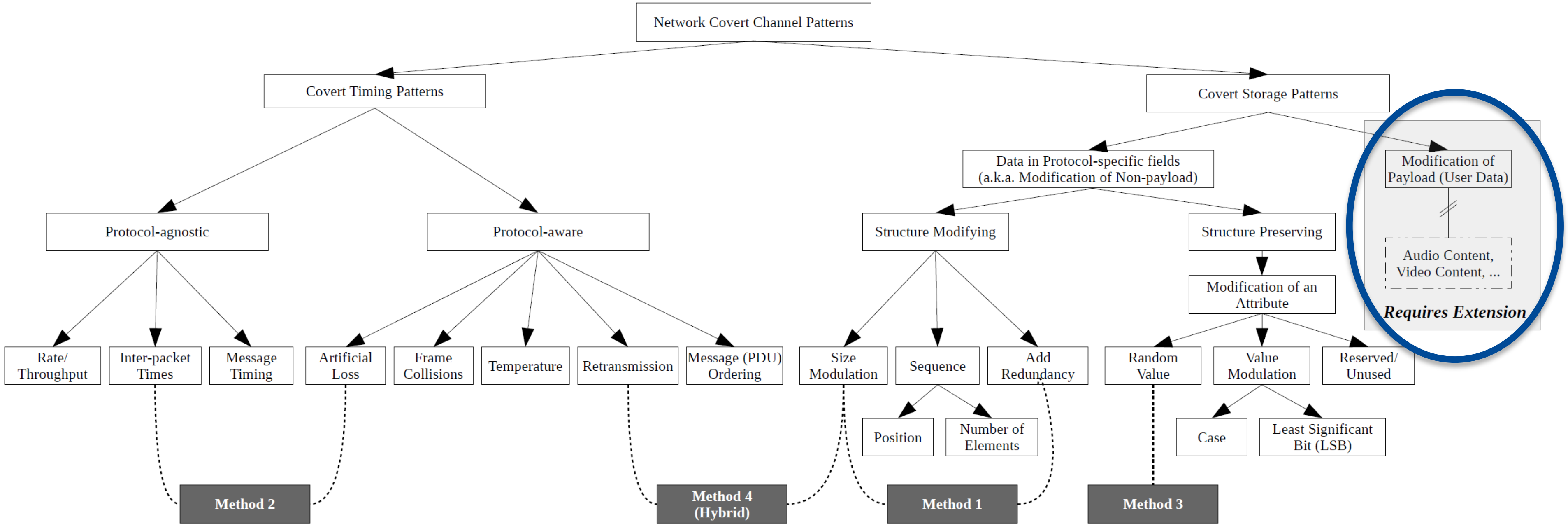
[1] S. Wendzel et al.: Pattern-based Survey and Taxonomy for Network Covert Channels, ACM CSUR, Vol. 47(3), 2015.

Let's switch to Storage Patterns: Protocol-specific Fields (Headers + Padding)
Category: Both (User-data Agnostic & Aware) Patterns



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://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)

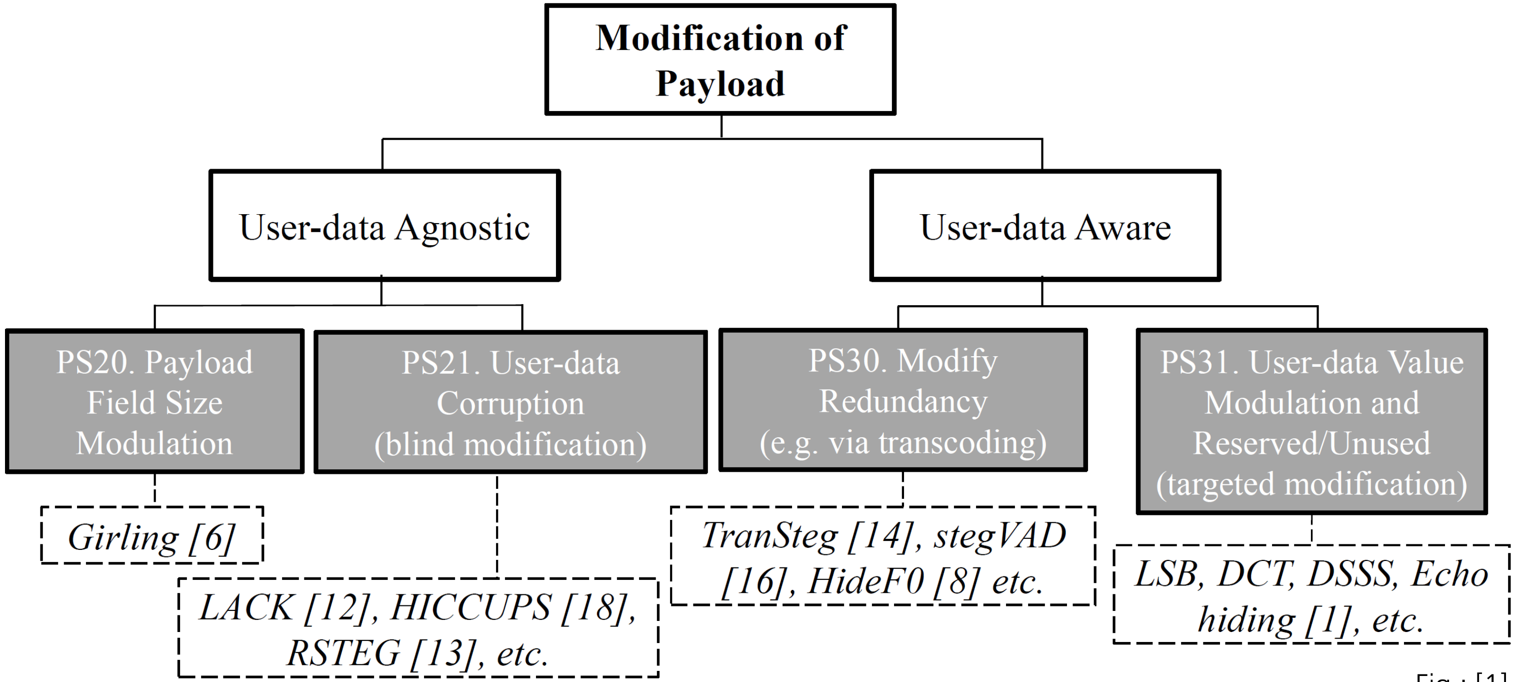

Modification of Payload
User-data Agnostic
User-data Aware
PS20. Payload Field Size Modulation
PS21. User-data Corruption (blind modification)
PS30. Modify Redundancy (e.g. via transcoding)
PS31. User-data Value Modulation and Reserved/Unused (targeted modification)
Girling [6]
LACK [12], HICCUPS [18], RSTEG [13], etc.
TranSteg [14], stegVAD [16], HideF0 [8] etc.
LSB, DCT, DSSS, Echo hiding [1], etc.

Fig.: [1]

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

Published Hiding Techniques [1]

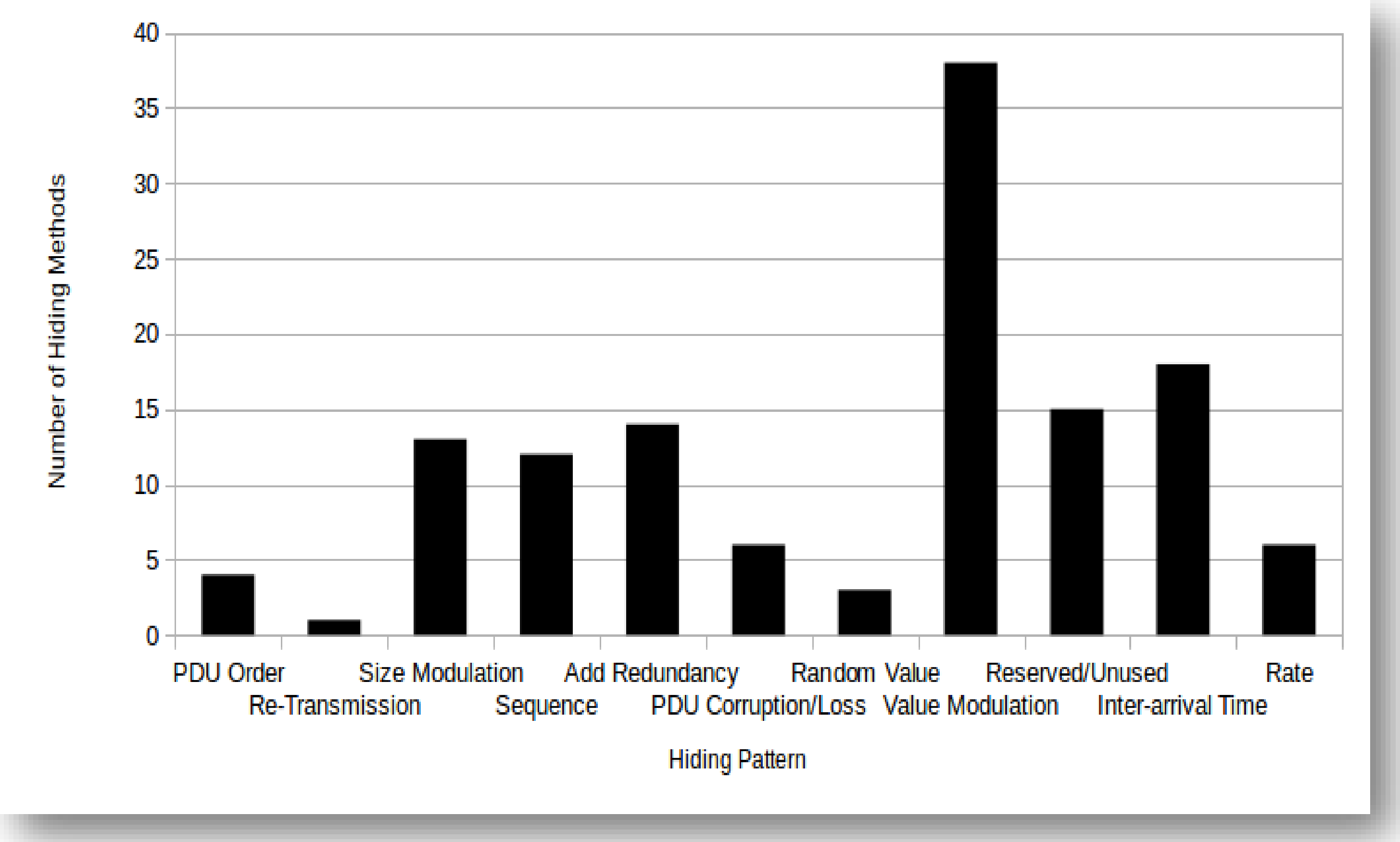


Fig.: [1]

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

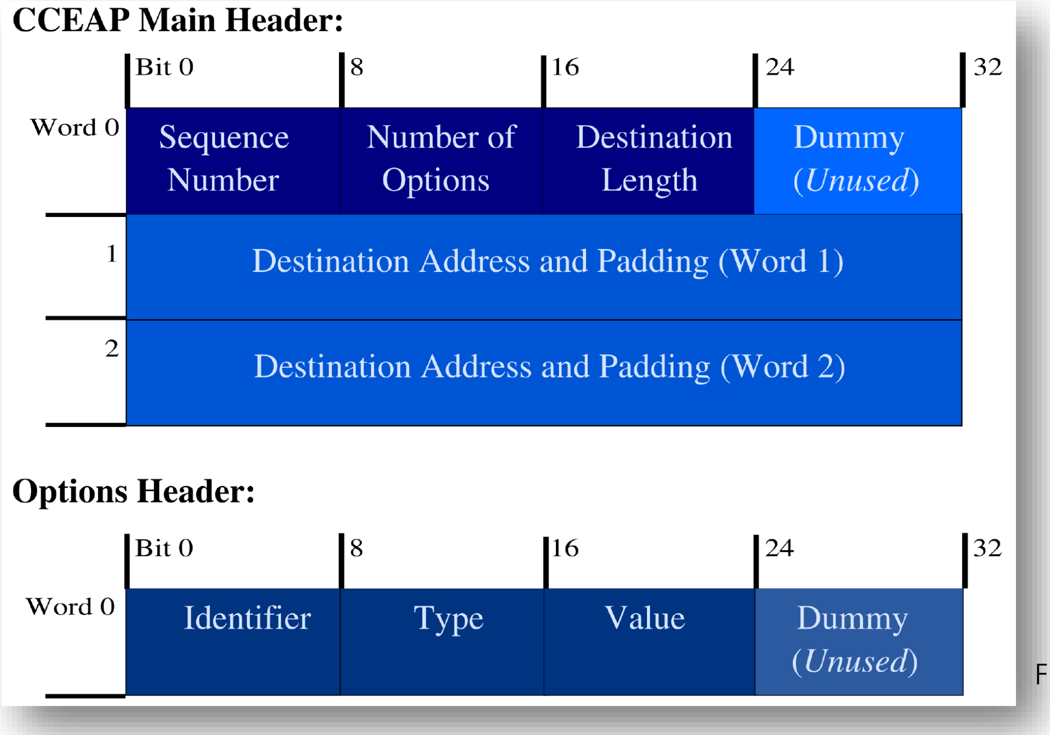
CCEAP

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.



CCEAP Main Header:

	Bit 0	8	16	24
Word 0	Sequence Number	Number of Options	Destination Length	Dummy *(Unused)*
1	Destination Address and Padding (Word 1)			
2	Destination Address and Padding (Word 2)			

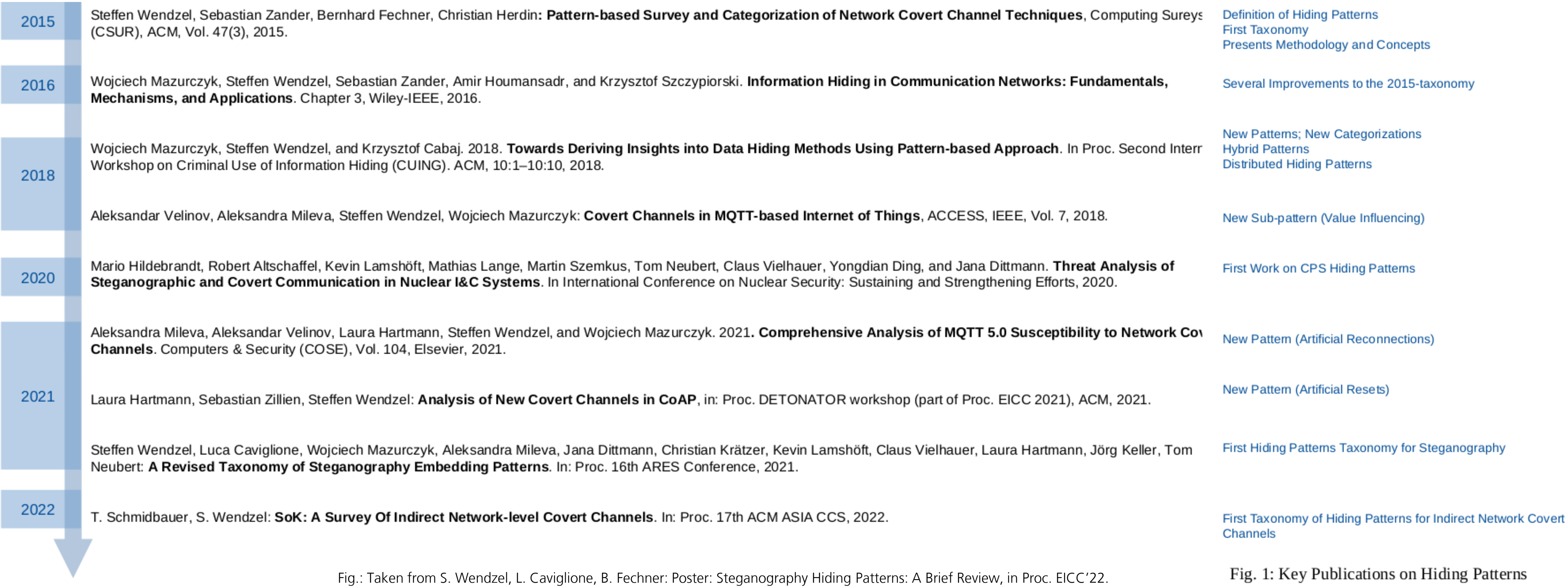
Options Header:

	Bit 0	8	16	24
Word 0	Identifier	Type	Value	Dummy *(Unused)*

Fig.: [1]

[1] S. Wendzel, W. Mazurczyk: Poster: An Educational Network Protocol for Covert Channel Analysis Using Patterns, Proc. ACM CCS, 2016.

Improvements of the Hiding Patterns Taxonomy During the Years

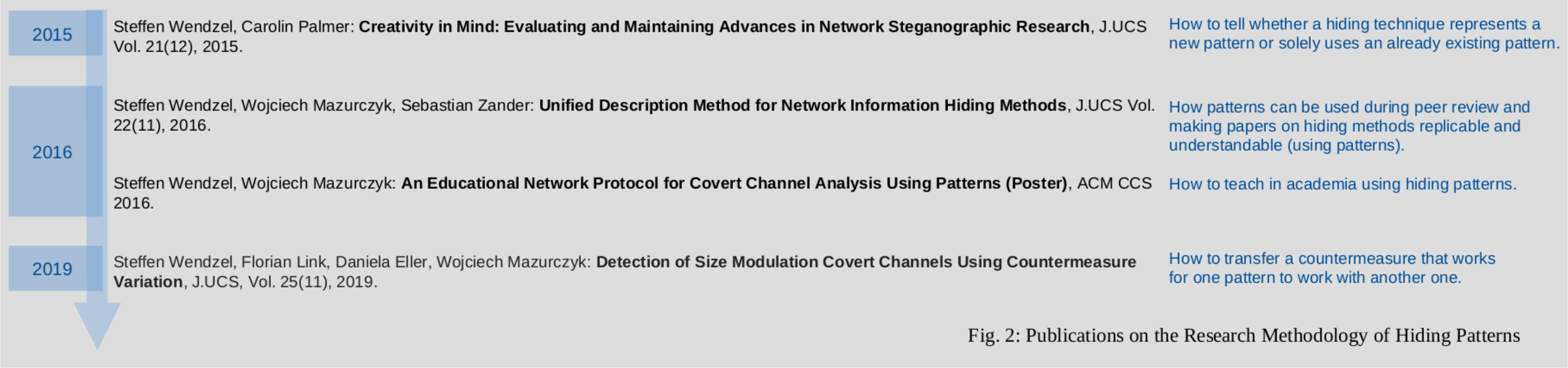


2015	Steffen Wendzel, Sebastian Zander, Bernhard Fechner, Christian Herdin**: Pattern-based Survey and Categorization of Network Covert Channel Techniques**, Computing Sureys (CSUR), ACM, Vol. 47(3), 2015.	Definition of Hiding Patterns First Taxonomy Presents Methodology and Concepts
2016	Wojciech Mazurczyk, Steffen Wendzel, Sebastian Zander, Amir Houmansadr, and Krzysztof Szczypiorski. **Information Hiding in Communication Networks: Fundamentals, Mechanisms, and Applications**. Chapter 3, Wiley-IEEE, 2016.	Several Improvements to the 2015-taxonomy
2018	Wojciech Mazurczyk, Steffen Wendzel, and Krzysztof Cabaj. 2018. **Towards Deriving Insights into Data Hiding Methods Using Pattern-based Approach**. In Proc. Second Interr Workshop on Criminal Use of Information Hiding (CUING). ACM, 10:1–10:10, 2018.	New Patterns; New Categorizations Hybrid Patterns Distributed Hiding Patterns
	Aleksandar Velinov, Aleksandra Mileva, Steffen Wendzel, Wojciech Mazurczyk: **Covert Channels in MQTT-based Internet of Things**, ACCESS, IEEE, Vol. 7, 2018.	New Sub-pattern (Value Influencing)
2020	Mario Hildebrandt, Robert Altschaffel, Kevin Lamshöft, Mathias Lange, Martin Szemkus, Tom Neubert, Claus Vielhauer, Yongdian Ding, and Jana Dittmann. **Threat Analysis of Steganographic and Covert Communication in Nuclear I&C Systems**. In International Conference on Nuclear Security: Sustaining and Strengthening Efforts, 2020.	First Work on CPS Hiding Patterns
2021	Aleksandra Mileva, Aleksandar Velinov, Laura Hartmann, Steffen Wendzel, and Wojciech Mazurczyk. 2021**. Comprehensive Analysis of MQTT 5.0 Susceptibility to Network Cov Channels**. Computers & Security (COSE), Vol. 104, Elsevier, 2021.	New Pattern (Artificial Reconnections)
	Laura Hartmann, Sebastian Zillien, Steffen Wendzel: **Analysis of New Covert Channels in CoAP**, in: Proc. DETONATOR workshop (part of Proc. EICC 2021), ACM, 2021.	New Pattern (Artificial Resets)
	Steffen Wendzel, Luca Caviglione, Wojciech Mazurczyk, Aleksandra Mileva, Jana Dittmann, Christian Krätzer, Kevin Lamshöft, Claus Vielhauer, Laura Hartmann, Jörg Keller, Tom Neubert: **A Revised Taxonomy of Steganography Embedding Patterns**. In: Proc. 16th ARES Conference, 2021.	First Hiding Patterns Taxonomy for Steganography
2022	T. Schmidbauer, S. Wendzel: **SoK: A Survey Of Indirect Network-level Covert Channels**. In: Proc. 17th ACM ASIA CCS, 2022.	First Taxonomy of Hiding Patterns for Indirect Network Covert Channels

Fig. 1: Key Publications on Hiding Patterns

Fig.: Taken from S. Wendzel, L. Caviglione, B. Fechner: Poster: Steganography Hiding Patterns: A Brief Review, in Proc. EICC'22.

Improvements of the Hiding Pattern-based Methodology



2015	Steffen Wendzel, Carolin Palmer: **Creativity in Mind: Evaluating and Maintaining Advances in Network Steganographic Research**, J.UCS Vol. 21(12), 2015.	How to tell whether a hiding technique represents a new pattern or solely uses an already existing pattern.
2016	Steffen Wendzel, Wojciech Mazurczyk, Sebastian Zander: **Unified Description Method for Network Information Hiding Methods**, J.UCS Vol. 22(11), 2016.	How patterns can be used during peer review and making papers on hiding methods replicable and understandable (using patterns).
	Steffen Wendzel, Wojciech Mazurczyk: **An Educational Network Protocol for Covert Channel Analysis Using Patterns (Poster)**, ACM CCS 2016.	How to teach in academia using hiding patterns.
2019	Steffen Wendzel, Florian Link, Daniela Eller, Wojciech Mazurczyk: **Detection of Size Modulation Covert Channels Using Countermeasure Variation**, J.UCS, Vol. 25(11), 2019.	How to transfer a countermeasure that works for one pattern to work with another one.

Fig. 2: Publications on the Research Methodology of Hiding Patterns

Fig.: Taken from S. Wendzel, L. Caviglione, B. Fechner: Poster: Steganography Hiding Patterns: A Brief Review, in Proc. EICC'22.

Towards 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 (2021): *A Revised Taxonomy of Steganography Embedding Patterns*, In: Proc. 16th International Conference on Availability, Reliability and Security (ARES 2021). ACM, 2021. DOI: https://doi.org/10.1145/3465481.3470069

(If not explicitely indicated, figures of the following slides are taken from this paper.)

Limitations of the Network-specific Taxonomy

- **Focus limited to network communications**, neglecting other domains of steganography.
- Level of abstraction does **not allow for inclusion of *non*-network patterns.**
  - E.g., *user-data* from network perspective might be a digital media *payload*.
- Current taxonomy does not differentiate between the **embedding** and the **representation** process, rendering the interpretation of patterns ambiguous.
- If such a differentiation would be applied, some current patterns must be considered as **hybrid** patterns (*temperature* pattern and *value influencing* pattern).
- However, several of the original (=2015) key concepts were kept; some patterns were renamed/made more abstract.

1. Embedding and Representation 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.

2. Improved Pattern Names

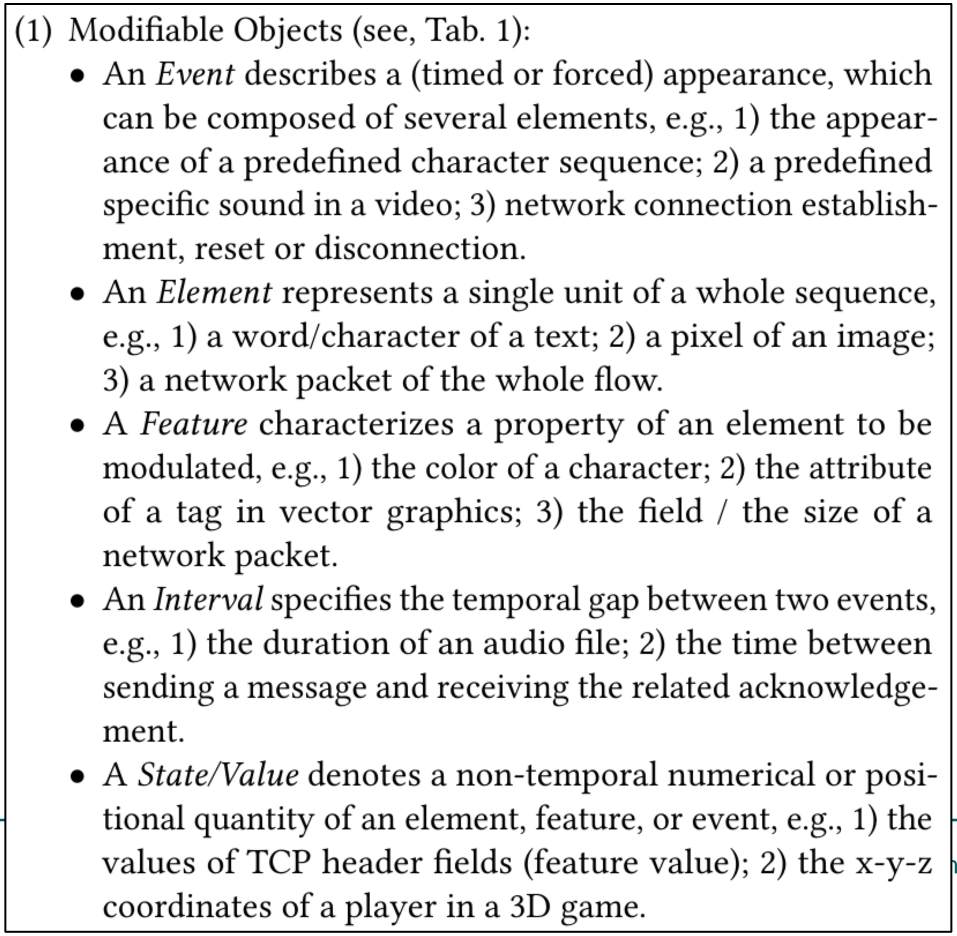
- Several of the original patterns represent suitable concepts but need a naming and description that is not specific to the network context. We renamed several of them.
  - Inter-packet Times → Event/Element Interval Modulation
  - Message Timing → Event Occurrence
  - …
- Some terms in the categorization had to be dropped as well, such as „payload“ and „protocol-awareness“.
- No differentiation between syntax and semantics.
  - Previously, one differentiated between structure-preservation and structure-modification. However, some patterns can modify both (see paper for an example).

2. Improved Pattern Names

- Finally, we came up with a glossary to make things more precise.
- Each pattern name is composed of an **identifier** and a **name**.
- Identifier has the Form **[ER][TN]n{D}**
  - **E**: Embedding Pattern
  - **R**: Representation Pattern
  - **T**: Temporal Pattern
  - **N**: Non-temporal Pattern
  - **n**: number of the pattern (can contain sub-numbers, e.g. **ET1.2.3**.
  - **D**: stego domain (only representation patterns; e.g. n=network, t=text stego, d=digital media, …
  - Example: **RT1t** = Representation Pattern, Temporal, Number 1, Text Steganography.

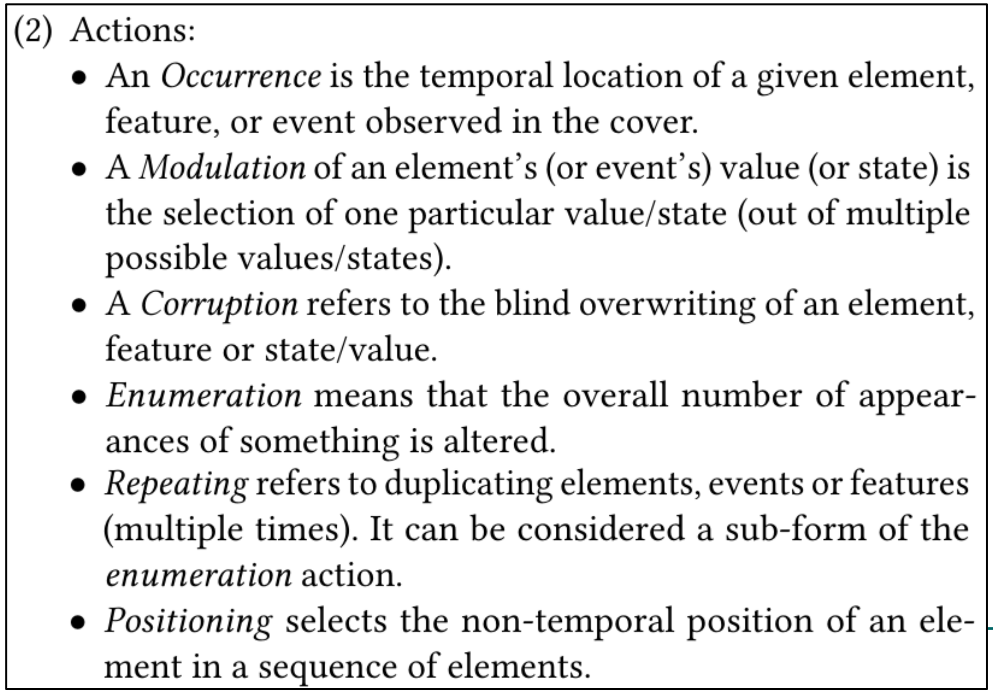
2. Improved Pattern Names

- Name contains the **identifier,** a modifiable **object** (e.g. *event* or *feature*) followed by an **action** (e.g. *modulation* or *occurrence*).
  - Example: **ET2. Event Occurrence**



(1) Modifiable Objects (see, Tab. 1):

- An *Event* describes a (timed or forced) appearance, which can be composed of several elements, e.g., 1) the appearance of a predefined character sequence; 2) a predefined specific sound in a video; 3) network connection establishment, reset or disconnection.
- An *Element* represents a single unit of a whole sequence, e.g., 1) a word/character of a text; 2) a pixel of an image; 3) a network packet of the whole flow.
- A *Feature* characterizes a property of an element to be modulated, e.g., 1) the color of a character; 2) the attribute of a tag in vector graphics; 3) the field / the size of a network packet.
- An *Interval* specifies the temporal gap between two events, e.g., 1) the duration of an audio file; 2) the time between sending a message and receiving the related acknowledgement.
- A *State/Value* denotes a non-temporal numerical or positional quantity of an element, feature, or event, e.g., 1) the values of TCP header fields (feature value); 2) the x-y-z coordinates of a player in a 3D game.



(2) Actions:

- An *Occurrence* is the temporal location of a given element, feature, or event observed in the cover.
- A *Modulation* of an element's (or event's) value (or state) is the selection of one particular value/state (out of multiple possible values/states).
- A *Corruption* refers to the blind overwriting of an element, feature or state/value.
- *Enumeration* means that the overall number of appearances of something is altered.
- *Repeating* refers to duplicating elements, events or features (multiple times). It can be considered a sub-form of the *enumeration* action.
- *Positioning* selects the non-temporal position of an element in a sequence of elements.

2. Improved Pattern Names

- Name contains the **identifier,** a modifiable **object** (e.g. *event* or *feature*) followed by an **action** (e.g. *modulation* or *occurrence*).
  - Example: **ET2. Event Occurrence**

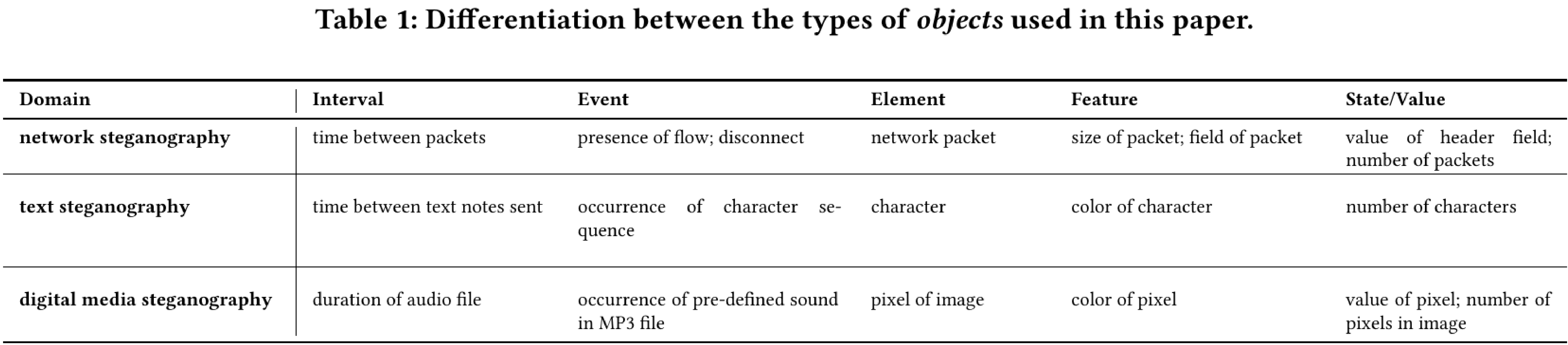
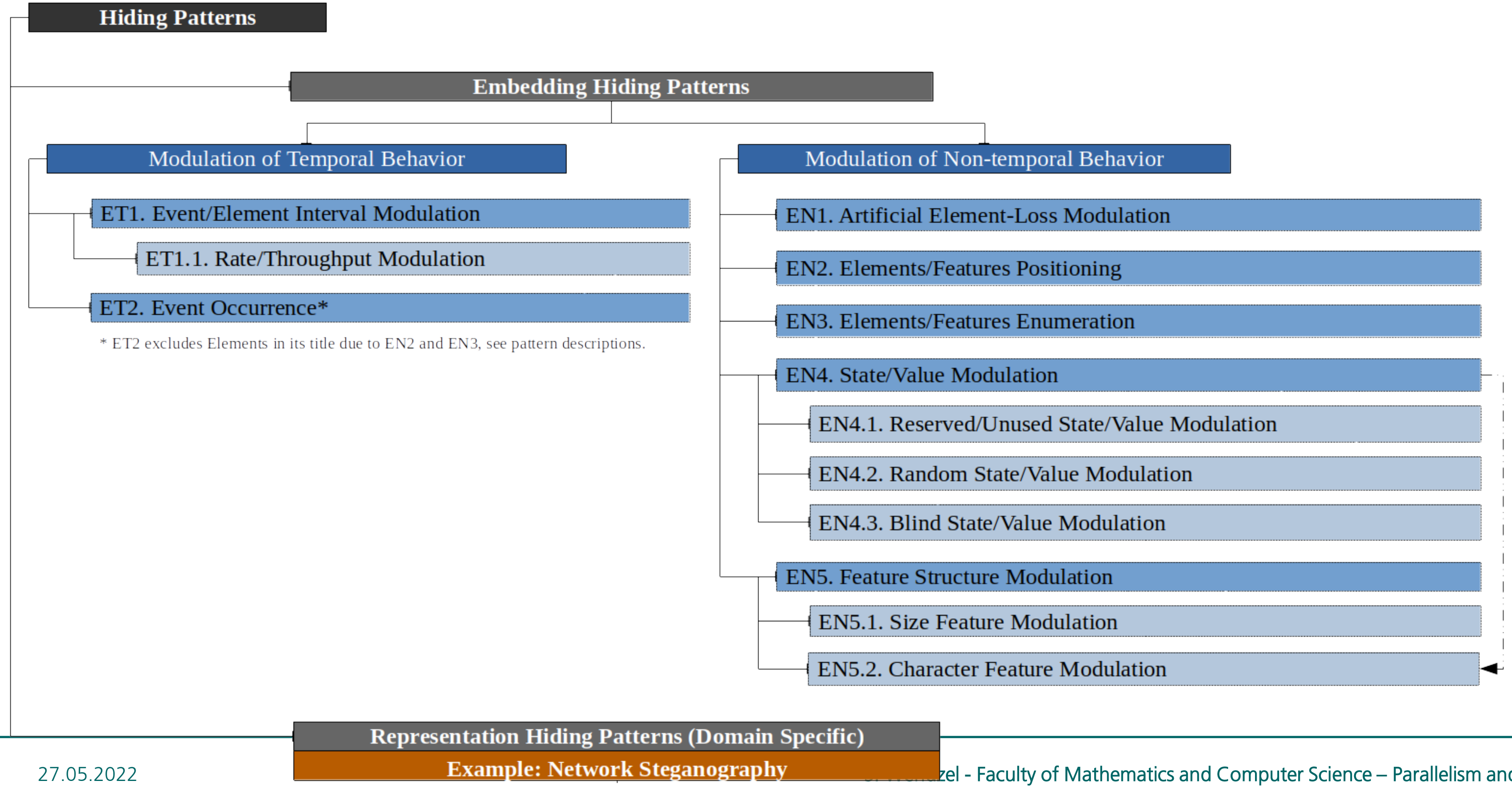


Table 1: Differentiation between the types of *objects* used in this paper.

Domain	Interval	Event	Element	Feature	State/Value
network steganography	time between packets	presence of flow; disconnect	network packet	size of packet; field of packet	value of header field; number of packets
text steganography	time between text notes sent	occurrence of character sequence	character	color of character	number of characters
digital media steganography	duration of audio file	occurrence of pre-defined sound in MP3 file	pixel of image	color of pixel	value of pixel; number of pixels in image

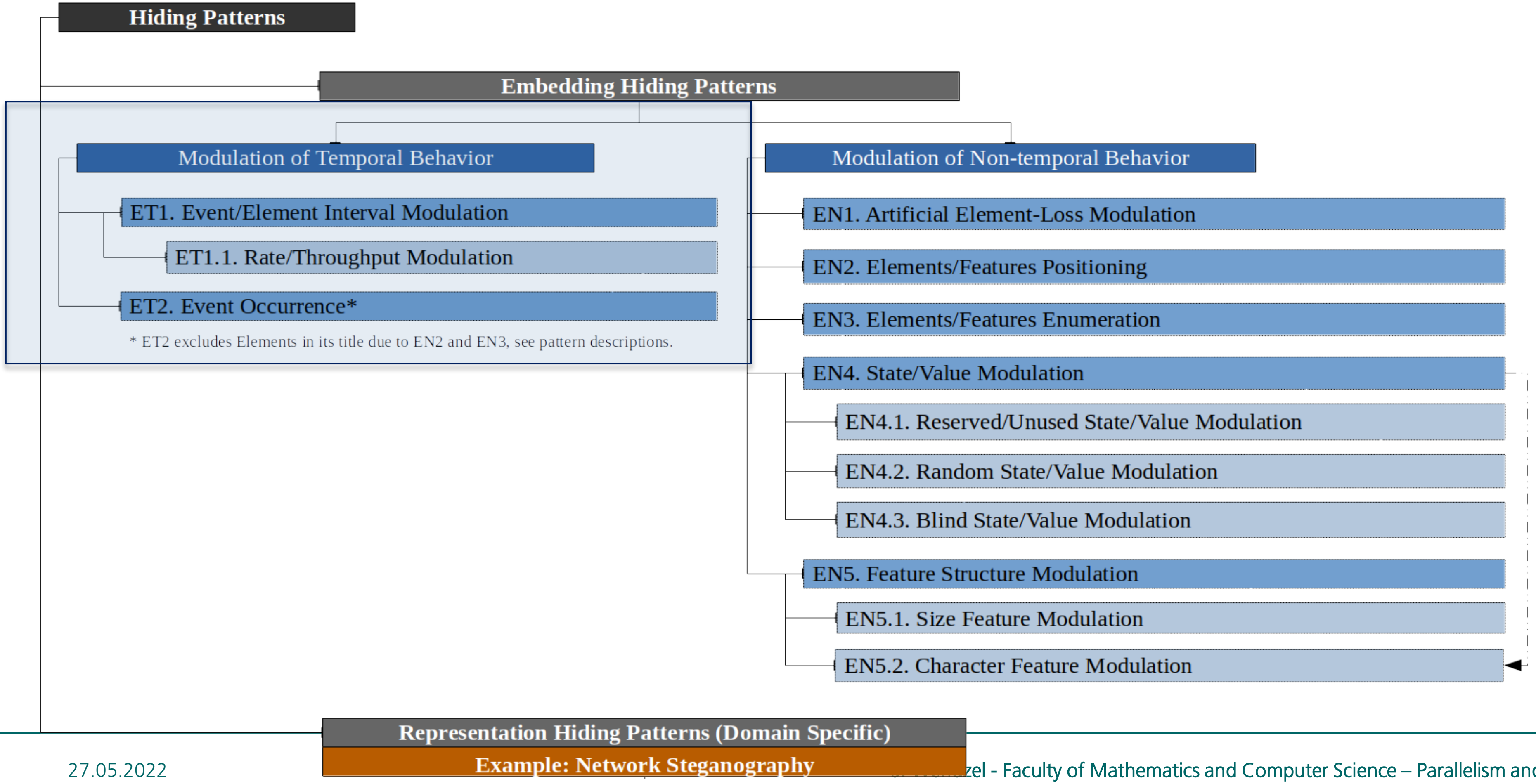
Taxonomy of Embedding Patterns



Hiding Patterns
Embedding Hiding Patterns
Modulation of Temporal Behavior
ET1. Event/Element Interval Modulation
ET1.1. Rate/Throughput Modulation
ET2. Event Occurrence*
Modulation of Non-temporal Behavior
EN1. Artificial Element-Loss Modulation
EN2. Elements/Features Positioning
EN3. Elements/Features Enumeration
EN4. State/Value Modulation
EN4.1. Reserved/Unused State/Value Modulation
EN4.2. Random State/Value Modulation
EN4.3. Blind State/Value Modulation
EN5. Feature Structure Modulation
EN5.1. Size Feature Modulation
EN5.2. Character Feature Modulation
Representation Hiding Patterns (Domain Specific)
Example: Network Steganography

* ET2 excludes Elements in its title due to EN2 and EN3, see pattern descriptions.

Taxonomy of Embedding Patterns



Hiding Patterns

Embedding Hiding Patterns

Modulation of Temporal Behavior

ET1. Event/Element Interval Modulation

ET1.1. Rate/Throughput Modulation

ET2. Event Occurrence*

* ET2 excludes Elements in its title due to EN2 and EN3, see pattern descriptions.

Modulation of Non-temporal Behavior

EN1. Artificial Element-Loss Modulation

EN2. Elements/Features Positioning

EN3. Elements/Features Enumeration

EN4. State/Value Modulation

EN4.1. Reserved/Unused State/Value Modulation

EN4.2. Random State/Value Modulation

EN4.3. Blind State/Value Modulation

EN5. Feature Structure Modulation

EN5.1. Size Feature Modulation

EN5.2. Character Feature Modulation

Representation Hiding Patterns (Domain Specific)

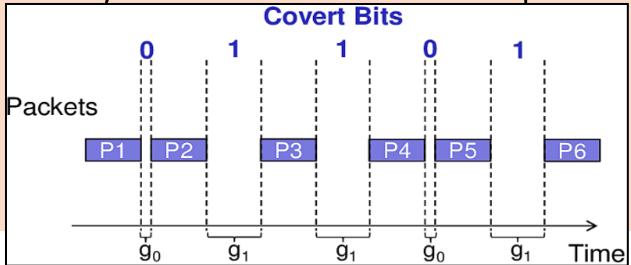
Example: Network Steganography

Temporal Embedding Patterns

ET1. Event/Element Interval Modulation

- The covert message is embedded by modulating the gaps between succeeding events/elements.
- <u>Examples:</u>
  1. modulating the inter-packet gap between succeeding network packets (elements) or between connection establishments (events);
  2. modulating the time-gap between succeeding cyber-physical actions, such as acoustic beeps.

<u>Sub-patterns:</u>
ET1.1 Rate/Throughput Modulation

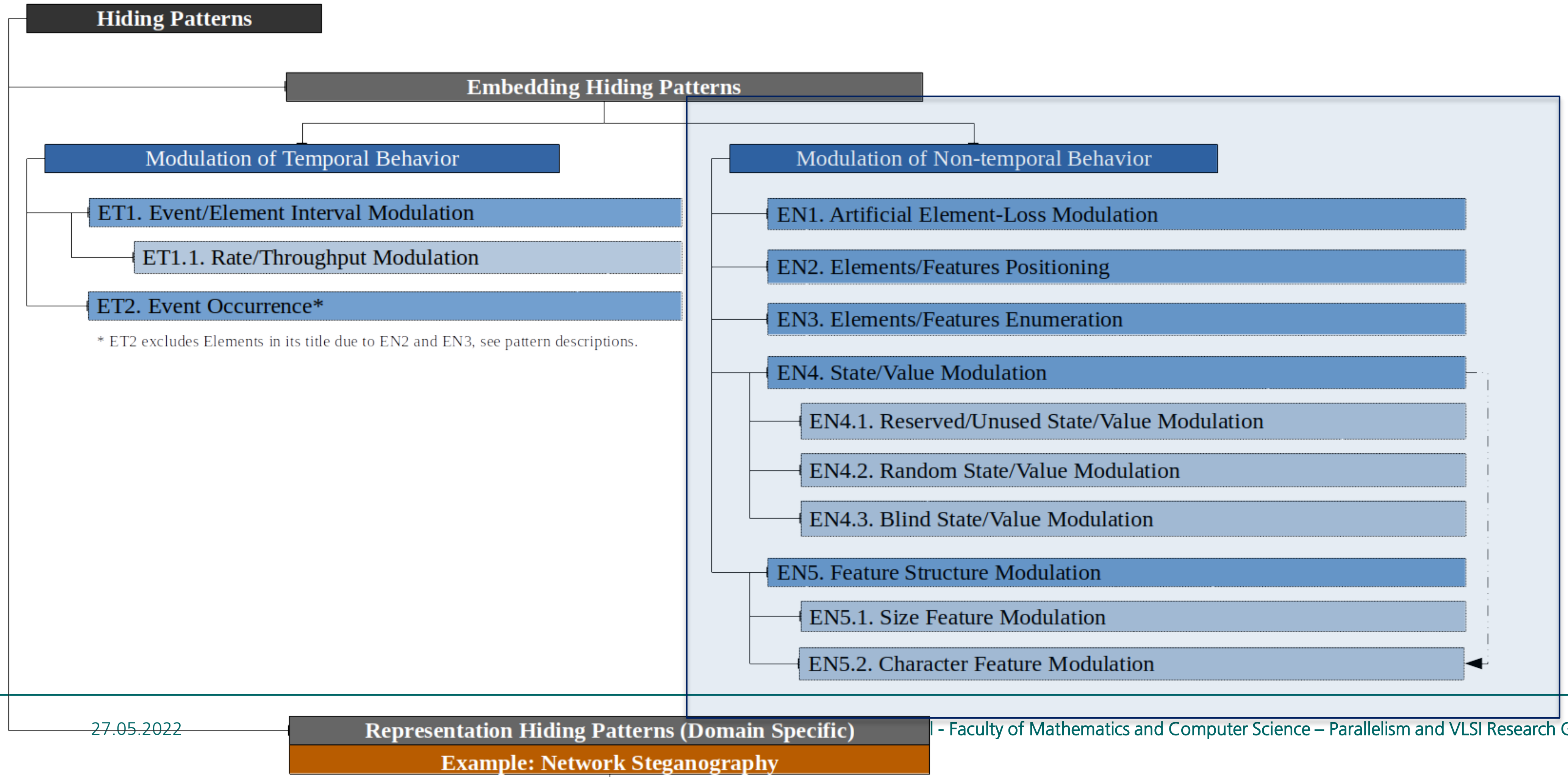


ET2. Event Occurrence

- The covert message is encoded in the temporal location of events (*in comparison to ET1.1, the **rate** of events is not directly modulated but events are triggered at specific moments in time, moreover, ET2 can be a single event while ET1.1 needs a sequence of elements*).
- <u>Examples:</u>
  1. sending a specific network packet at 6pm;
  2. influencing the time at which a drone starts its journey to some destination;
  3. performing a disconnect at a certain time.

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

Non-temporal Embedding Patterns



- Hiding Patterns
  - Embedding Hiding Patterns
    - Modulation of Temporal Behavior
      - ET1. Event/Element Interval Modulation
        - ET1.1. Rate/Throughput Modulation
      - ET2. Event Occurrence*
    - Modulation of Non-temporal Behavior
      - EN1. Artificial Element-Loss Modulation
      - EN2. Elements/Features Positioning
      - EN3. Elements/Features Enumeration
      - EN4. State/Value Modulation
        - EN4.1. Reserved/Unused State/Value Modulation
        - EN4.2. Random State/Value Modulation
        - EN4.3. Blind State/Value Modulation
      - EN5. Feature Structure Modulation
        - EN5.1. Size Feature Modulation
        - EN5.2. Character Feature Modulation
  - Representation Hiding Patterns (Domain Specific)

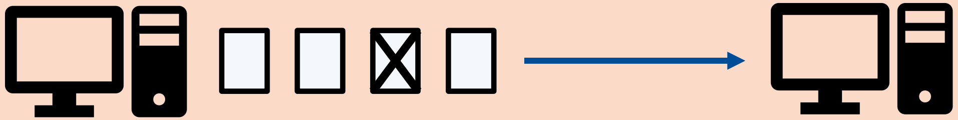
Example: Network Steganography

* ET2 excludes Elements in its title due to EN2 and EN3, see pattern descriptions.

Non-temporal Embedding Patterns

EN1. Artificial Element-Loss Modulation

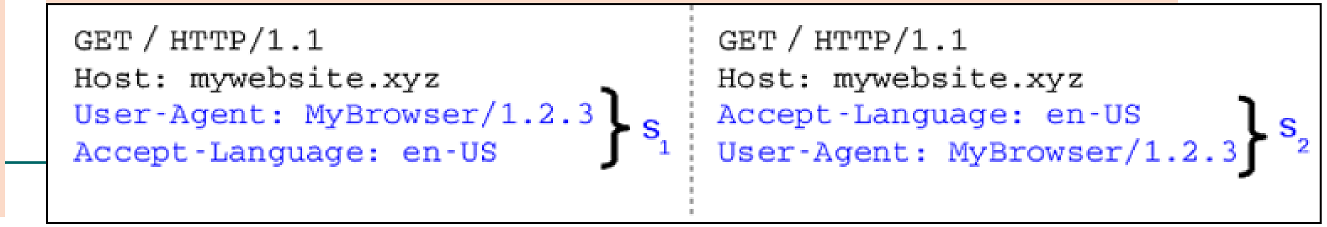
- The covert message is embedded by modulating the artificial loss of elements.
- Examples:
  1. dropping TCP segments with an even sequence number;



  2. removing commas in sentences [1].

EN2. Elements/Features Positioning

- The covert message is embedded by modulating the position of a predefined (set of) element(s)/feature(s) in a sequence of elements/features.
- Examples:
  1. position of a HTTP header line in the list of optional header lines;
  2. placing a specific character in a paragraph.



```
GET / HTTP/1.1
Host: mywebsite.xyz
User-Agent: MyBrowser/1.2.3
Accept-Language: en-US
```

```
GET / HTTP/1.1
Host: mywebsite.xyz
Accept-Language: en-US
User-Agent: MyBrowser/1.2.3
```

[1] Walter Bender, Daniel Gruhl, Norishige Morimoto, and Anthony Lu. 1996. Techniques for data hiding. IBM Systems Journal 35 (Nos3&4) (1996). ||| Figure.: W. Mazurczyk et al.: Information Hiding in Communication Networks, Wiley, 2016.

Non-temporal Embedding Patterns

EN3. Elements/Features Enumeration

- The covert message is embedded by altering the overall number of appearances of elements or features in a sequence.
- Examples:
  1. fragmenting a network packet into either *n* or *m* (*n≠m*) fragments;
  2. modulating the number of people wearing a t-shirt in a specific color in an image file;
  3. repeating an element/feature by duplicating a white space character (or not) in a text [1].

EN4. State/Value Modulation

- The covert message is embedded by modulating the states or values of features.
- Examples:
  1. modulating physical states, such as proximity, visibility, force, height, acceleration, speed, etc. of certain devices
  2. changing values of the network packet header fields (e.g., target IP address of ARP [2], Hop Count value in IPv6 [3] or the LSB in the IPv4 TTL);
  3. modulate the x-y-z coordinates of a player in a 3D multiplayer online game [4].

Pattern has three sub-patterns!

[1] Walter Bender, Daniel Gruhl, Norishige Morimoto, and Anthony Lu. 1996. Techniques for data hiding. IBM Systems Journal 35 (Nos3&4) (1996). ||| [2] Liping Ji, Yu Fan, and Chuan Ma. 2010. Covert channel for local area network. In 2010 IEEE International Conference on Wireless Communications, Networking and Information Security. ||| [3] Norka B Lucena, Grzegorz Lewandowski, and Steve J Chapin. 2005. Covert channels in IPv6. In International Workshop on Privacy Enhancing Technologies. Springer, ||| [4] Sebastian Zander, Grenville Armitage, and Philip Branch. 2008. Covert channels in multiplayer first person shooter online games. In 2008 33rd IEEE Conference on Local Computer Networks (LCN). IEEE.

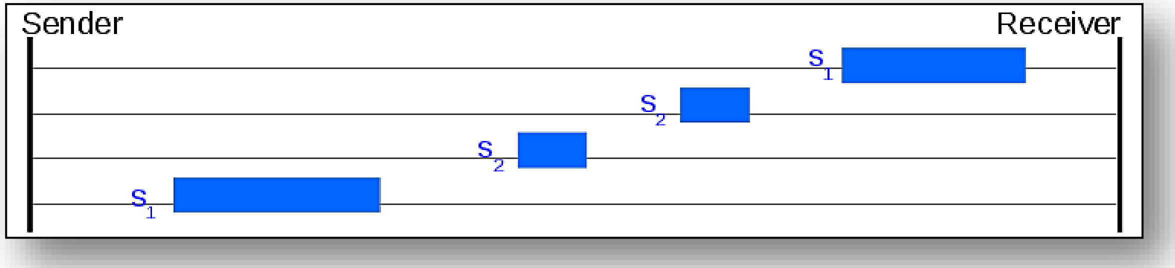
Non-temporal Embedding Patterns

EN5. Feature Structure Modulation

- This hiding pattern comprises all hiding techniques that modulate the structural properties of a feature (but not states/values (EN4), positions (EN2) or number of appearances (EN3)).

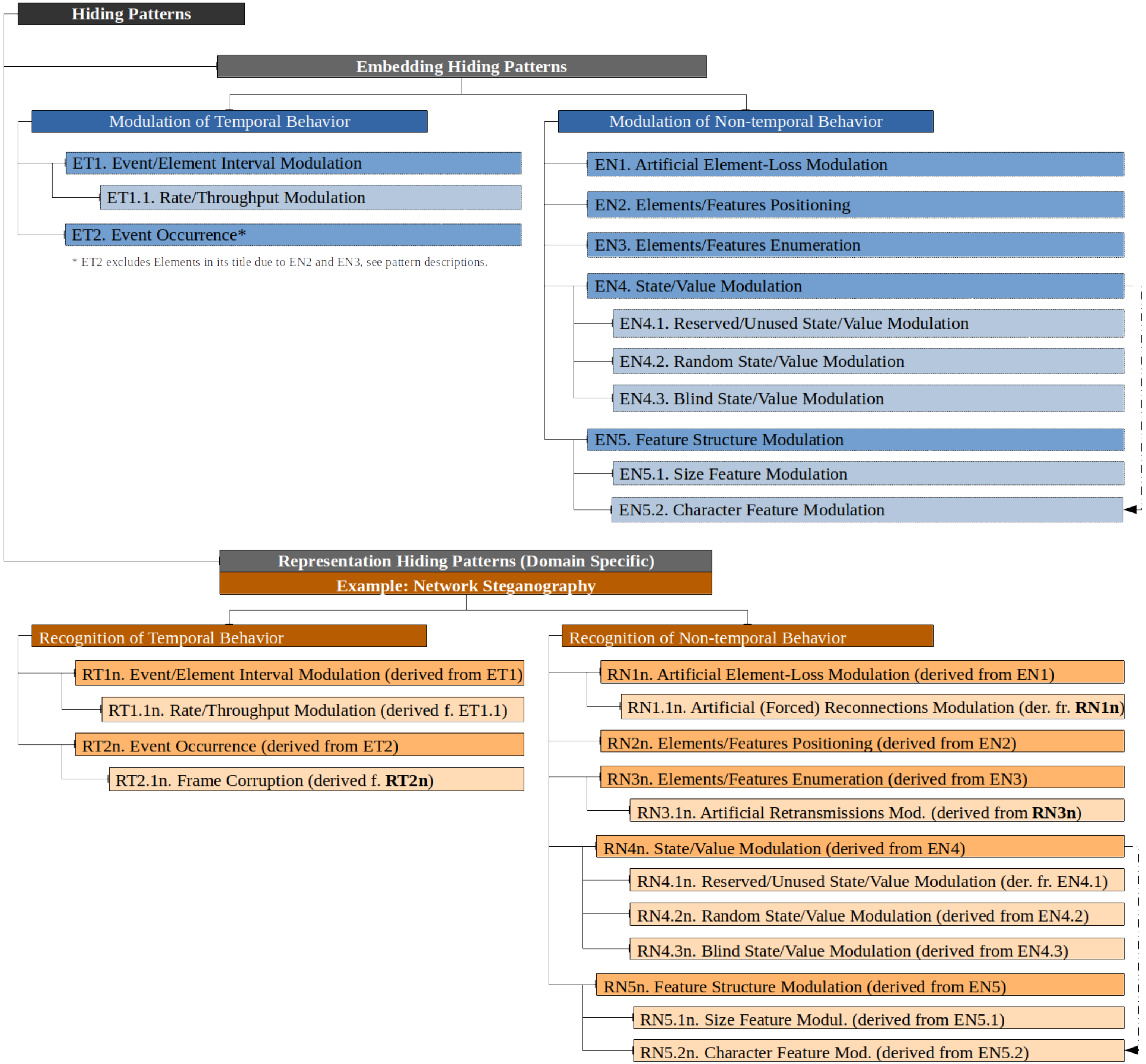
- Examples:
  1. increasing/decreasing the size of succeeding network packets;
  2. changing the color/style of characters in texts.

Pattern has two sub-patterns.



Representation Patterns

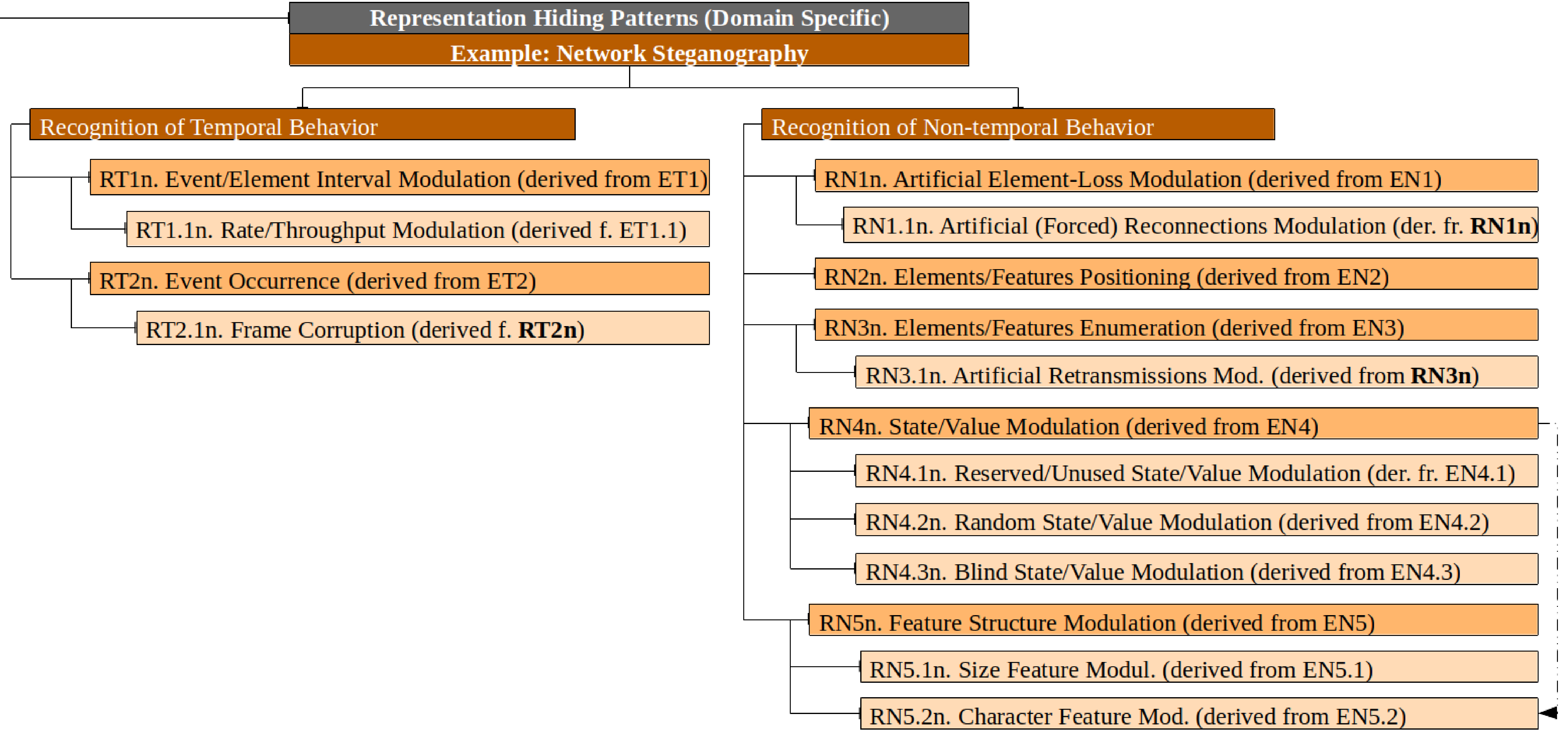
Example: Network Steganography



- Hiding Patterns
  - Embedding Hiding Patterns
    - Modulation of Temporal Behavior
      - ET1. Event/Element Interval Modulation
        - ET1.1. Rate/Throughput Modulation
      - ET2. Event Occurrence*
    - Modulation of Non-temporal Behavior
      - EN1. Artificial Element-Loss Modulation
      - EN2. Elements/Features Positioning
      - EN3. Elements/Features Enumeration
      - EN4. State/Value Modulation
        - EN4.1. Reserved/Unused State/Value Modulation
        - EN4.2. Random State/Value Modulation
        - EN4.3. Blind State/Value Modulation
      - EN5. Feature Structure Modulation
        - EN5.1. Size Feature Modulation
        - EN5.2. Character Feature Modulation
  - Representation Hiding Patterns (Domain Specific)
    Example: Network Steganography
    - Recognition of Temporal Behavior
      - RT1n. Event/Element Interval Modulation (derived from ET1)
        - RT1.1n. Rate/Throughput Modulation (derived f. ET1.1)
      - RT2n. Event Occurrence (derived from ET2)
        - RT2.1n. Frame Corruption (derived f. **RT2n**)
    - Recognition of Non-temporal Behavior
      - RN1n. Artificial Element-Loss Modulation (derived from EN1)
        - RN1.1n. Artificial (Forced) Reconnections Modulation (der. fr. **RN1n**)
      - RN2n. Elements/Features Positioning (derived from EN2)
      - RN3n. Elements/Features Enumeration (derived from EN3)
        - RN3.1n. Artificial Retransmissions Mod. (derived from **RN3n**)
      - RN4n. State/Value Modulation (derived from EN4)
        - RN4.1n. Reserved/Unused State/Value Modulation (der. fr. EN4.1)
        - RN4.2n. Random State/Value Modulation (derived from EN4.2)
        - RN4.3n. Blind State/Value Modulation (derived from EN4.3)
      - RN5n. Feature Structure Modulation (derived from EN5)
        - RN5.1n. Size Feature Modul. (derived from EN5.1)
        - RN5.2n. Character Feature Mod. (derived from EN5.2)

* ET2 excludes Elements in its title due to EN2 and EN3, see pattern descriptions.

Let us have a look at the differences:



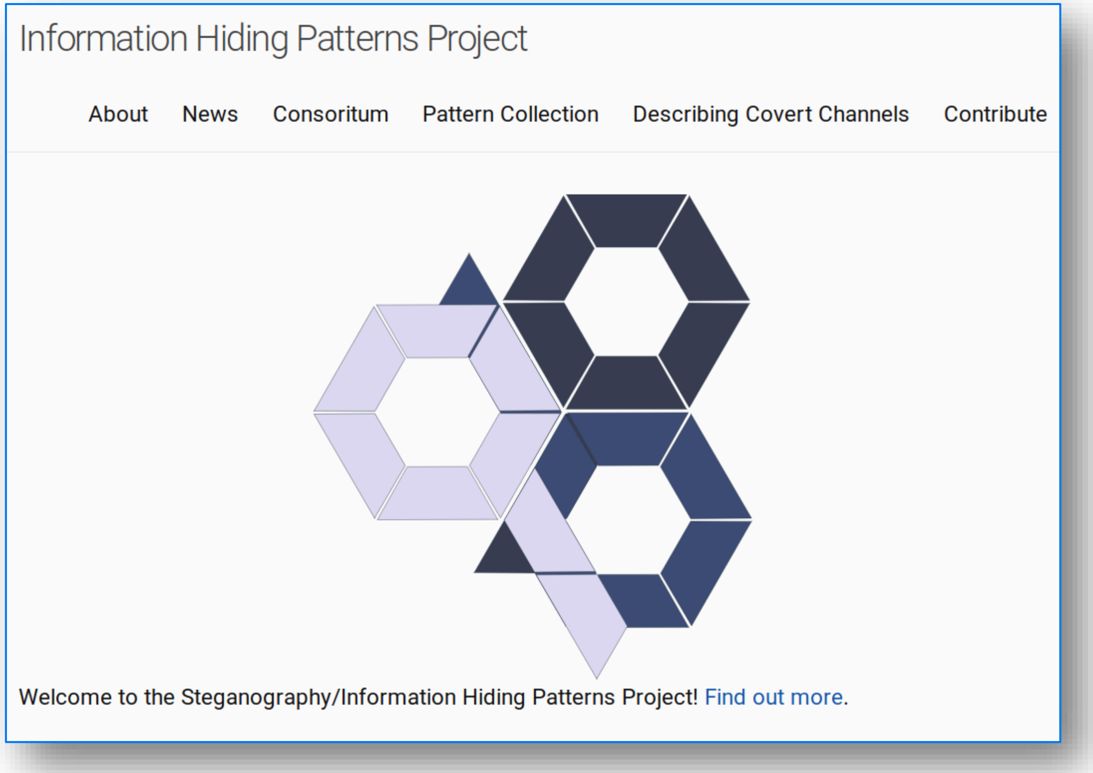
Representation Hiding Patterns (Domain Specific)

Example: Network Steganography

- Recognition of Temporal Behavior
  - RT1n. Event/Element Interval Modulation (derived from ET1)
    - RT1.1n. Rate/Throughput Modulation (derived f. ET1.1)
  - RT2n. Event Occurrence (derived from ET2)
    - RT2.1n. Frame Corruption (derived f. **RT2n**)
- Recognition of Non-temporal Behavior
  - RN1n. Artificial Element-Loss Modulation (derived from EN1)
    - RN1.1n. Artificial (Forced) Reconnections Modulation (der. fr. **RN1n**)
  - RN2n. Elements/Features Positioning (derived from EN2)
  - RN3n. Elements/Features Enumeration (derived from EN3)
    - RN3.1n. Artificial Retransmissions Mod. (derived from **RN3n**)
  - RN4n. State/Value Modulation (derived from EN4)
    - RN4.1n. Reserved/Unused State/Value Modulation (der. fr. EN4.1)
    - RN4.2n. Random State/Value Modulation (derived from EN4.2)
    - RN4.3n. Blind State/Value Modulation (derived from EN4.3)
  - RN5n. Feature Structure Modulation (derived from EN5)
    - RN5.1n. Size Feature Modul. (derived from EN5.1)
    - RN5.2n. Character Feature Mod. (derived from EN5.2)

More Information …

https://patterns.ztt.hs-worms.de



Information Hiding Patterns Project

Welcome to the Steganography/Information Hiding Patterns Project! Find out more.

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 Chapter 9, which also describes the process of finding new patterns (and ensuring the pattern is new).

Final Remarks

There are currently two hiding pattern taxonomies: One specific to **network** steganography (with discussed limitations) and a revised taxonomy for **all** steganography domains.

The revised taxonomy addressed several limitations of the network-specific taxonomy (lessons learned):

- Improved **terminology** and **systematic of pattern enumeration**.
- Made the **taxonomy more general** so that it **can be applied by all steganography domains**, instead of solely network steganography.
- **Kept the good concepts** + pattern-ideas **of the existing taxonomy** whenever feasible.
  - **The network-specific taxonomy is still fine, but** one should use the network hiding patterns while differentiating between the **embedding and receiving process**.

Current research work of the scientific community: Add representation patterns for **digital media, text, filesystem and CPS steganography** (first discussions on digital media and text stego can be found in the cited conference paper from 2021).