Journal of Universal Computer Science, vol. 22, no. 11 (2016), 1456-1486
submitted: 8/6/16, accepted: 28/10/16, appeared: 1/11/16 © J.UCS

Unified Description for Network Information Hiding Methods

Steffen Wendzel
(Worms University of Applied Sciences, Worms, Germany /
Fraunhofer FKIE, Bonn, Germany
wendzel@hs-worms.de)

Wojciech Mazurczyk
(Warsaw University of Technology, Warsaw, Poland /
University of Hagen, Hagen, Germany
wmazurcz@elka.pw.edu.pl)

Sebastian Zander
(Murdoch University, Perth, Australia
s.zander@murdoch.edu.au)

Abstract: Until now hiding methods in network steganography have been described in arbitrary ways, making them difficult to compare. For instance, some publications describe classical channel characteristics, such as robustness and bandwidth, while others describe the embedding of hidden information. We introduce the first unified description of hiding methods in network steganography. Our description method is based on a comprehensive analysis of the existing publications in the domain. When our description method is applied by the research community, future publications will be easier to categorize, compare and extend. Our method can also serve as a basis to evaluate the novelty of hiding methods proposed in the future.
Key Words: Information Hiding, Steganography, Covert Channels, Design Patterns, Scientific Methodology, Scientific Pratice, Network Security
Category: D.2.11, D.4.6, K.6.5, K.7.m

1 Introduction

Steganography research determines, describes and evaluates methods of hiding information within a medium; *steganalysis* research develops, describes and evaluates methods for the detection and prevention of such methods [Petitcolas et al., 1999; Katzenbeisser and Petitcolas, 2000]. Steganography has been applied in ancient Greece, in several wars, including World War I and II, and to digital media (digital images, audio files, and digital videos) [Petitcolas et al., 1999; Fridrich, 2009]. *Network steganography* or *network information hiding*, the most recent sub-discipline of steganography, deals with the hiding of information in network traffic [Mazurczyk et al., 2016].

Well over 100 methods for hiding in network transmissions were published since Girling introduced the first methods in 1987 [Girling, 1987]. Wendzel et al.

[2015] clustered these hiding methods in so-called *hiding patterns* and organized these patterns in form of a taxonomy. Hiding patterns are abstract descriptions of hiding methods.

Using eleven patterns, 109 hiding methods could be described showing how redundant similar ideas were in past research. The introduction of patterns moreover allowed to handle different hiding methods under a common umbrella (i.e. a particular pattern) instead of utilizing several separate terms introduced by previous research to describe very similar ideas. Mazurczyk et al. [2016] refined parts of the pattern descriptions.

On the basis of hiding patterns, a new academic workflow was defined by Wendzel and Palmer for the creativity evaluation of network information hiding methods [2015]. The key concept of this workflow is that if a new hiding method cannot be represented by an existing pattern, it comprises higher novelty than a hiding method that was already described by a pattern and is thus not novel. The evaluation process of hiding methods in conjunction with hiding patterns can be integrated into the traditional peer-review process but requires an author to explain why a hiding method is (or is not) represented by an existing hiding pattern. The approach of [Wendzel and Palmer, 2015] fosters the reduction of terminology inconsistencies as new publications will be aligned to existing pattern terminology and the improved peer review process eases spotting any inconsistencies.

The aforementioned publications emphasize on the categorization of hiding methods, the reduction of inconsistent terminology and redundant ideas, and the evaluation of the novelty of hiding methods.

Contributions. The contributions of our work are twofold: we performed an in-depth analysis of hiding method descriptions and discovered several inconsistencies in these descriptions. We also provide a way to describe hiding methods that helps to prevent such inconsistencies by ensuring a unified, comparable description of the hiding methods.

Contribution A: Literature Analysis: We analyzed 131 hiding method descriptions from 74 publications published between 1987 and 2015. The analysis brang to light relevant inconsistencies in the *description* of hiding methods. In particular, we noticed large differences in the evaluations and technical descriptions between the publications. While for some hiding methods, the channel capacity is described, other publications focus solely on the embedding process, the application scenario of a hiding method or other aspects. In addition, the way in which hiding methods are described changed over time. Moreover, the descriptions of hiding methods even vary *within* some of the papers. We also found that some papers *combine* the evaluation and description for several hiding methods. For example, some publications discuss the overall throughput of multiple hiding methods instead of discussing the different channels separately. These

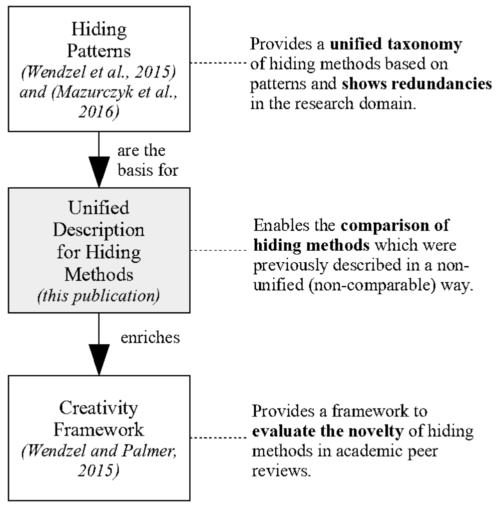

Figure 1: Contribution of this work: While hiding patterns serve as a basis for this new publication, it provides its own contribution by enabling the structured comparison of research work on hiding methods and it can be also used in conjunction with the creativity framework.

non-unified descriptions make it difficult to compare publications that propose new hiding methods and to evaluate each described hiding method separately.

Contribution B: Presentation of a Unified Description Method: We introduce a method for a unified description of hiding methods in network steganography. Figure 1 visualizes our contribution in the context of previous work. The existing hiding patterns describe how hidden information is signaled, and the creativity framework provides a way to reduce redundant research outcomes and to evaluate whether a proposed hiding method is actually new, or not.

This paper fills a missing gap in the previous work by introducing a multi-facetted and detail-rich description for hiding methods. In comparison to existing hiding method descriptions that we analyzed in *Contribution A*, our unified description has several advantages. When applied by the scientific community, our unified description method will enable the easy comparison, categorization, and evaluation of hiding methods. In addition, a unified description also eases the identification of research gaps as these can be easily spotted (for instance, with the unified description method, a reader can easily see whether a channel capacity estimation is still lacking for a hiding method or whether a detection method is not given and must be subject to research first). Last, but not least, our description method can also serve as a basis for the creativity framework and will enrich the evaluation process of the same.

Outline. Section 2 introduces fundamentals and related work. Section 3 provides an overview of the unified description method for hiding methods. The description method is split into three main categories, which are covered in sections 4–6. We discuss results of our literature analysis in section 7 and provide two exemplary descriptions in section 8. Section 9 explains how the unified description can be used in combination with a creativity framework to evaluate the novelty of newly proposed hiding methods. We provide a conclusion in section 10.

2 Fundamentals

By definition, *design patterns* represent a design (or solution) to a recurring problem in a given context, which can have several attributes, such as a pattern name, a pattern identifier or an illustration [Freeman et al., 2004]. Patterns are collected in pattern catalogs.

In network steganography, so-called *hiding patterns* describe how to use a method (solution) to hide data (problem) in network traffic (context) [Wendzel et al., 2015]. In other words, a hiding pattern describes a hiding method in an abstract way. For instance, a pattern could describe how to hide secret data in the least significant bits (LSB) of network protocol header fields but it does not cover details on how this will be achieved for a particular network protocol.

Patterns can also contain a description of their relation to other patterns, forming not only a classification for hiding methods but a taxonomy of hiding methods. Hiding patterns are described in a structured way with a so-called *pattern language* [Wendzel et al., 2015] that specifies all the necessary attributes of such a pattern [Fincher, 2003] and that eases categorization and taxonomy-creation. A hiding pattern's mandatory attributes are its name, a brief illustration of how data is hidden, a context (e.g. that it is a storage channel that modifies a header field) and a proof of existing work about the hiding method of a pattern with references to academic publications. Further, optional attributes can enrich the description of a pattern, such as a code snippet or a graphical illustration of its functioning.

While taxonomy and categorization can be applied at a large scale, such as for the categorization of the Animal Kingdom, it can be also applied to smaller areas, e.g. sub-domains of computer science, such as in Human Computer Interaction [Borchers, 2001] or network information hiding methods. Our work allows to build fine-grained taxonomies of hiding methods based on their attributes.

However, the central contribution of our paper is not a survey of techniques, application areas or countermeasure nor a categorization for network covert channels (such already exist, cf. Meadows and Moskowitz [1996]; Shen et al. [2005]; Llamas et al. [2005]; Zander et al. [2007]; Zhiyong and Yong [2009]; Mileva and Panajotov [2014]; Wendzel et al. [2015]; Carrara and Adams [2016b]).

Instead, our work significantly extends the general description of hiding methods. The presented unified description method additionally improves the workflow presented in [Wendzel and Palmer, 2015] due to its provision of higher description detail.

3 Unified Description Method

We analyzed the literature describing 131 hiding methods published since 1987. The analysis revealed that the descriptions of hiding methods in the related publications differ significantly regarding their provided information. To improve this situation, we designed a unified description method.

3.1 Applicability to Scientific Work

The unified description method can be directly applied to structure new scientific papers. This way, authors which present hiding methods make it easy for other researchers and reviewers to compare the new hiding method with existing hiding methods. Our unified description can be also combined with the 'creativity framework' [Wendzel and Palmer, 2015] to evaluate the *novelty* of a proposed hiding method by applying concepts of creativity research during the academic peer review process. By combining the creativity metric with our unified description method, both, the presentation of a hiding method and the underlying research novelty can be compared in a process that is unified, reasonable and re-constructable.

3.2 Overview of the Description Method

Our description of hiding methods is split into three categories, namely *general information about the hiding method*, *description of the hiding process*, and *potential or tested countermeasures*. The first two categories comprise sub-categories and each (sub-)category can be mandatory or optional. Figure 2 provides an overview.

The category 'hiding method general information' consists of a link to an existing hiding pattern and a detailed description of the hiding method. It also includes a discussion of the application scenario and requirements of the carrier. The category 'hiding method process' is split into four parts: the sender-side and the receiver-side description of the hiding method, the details of the covert communication channel, and the description of an associated covert channel control protocol (if applicable). The third category discusses both potential and evaluated countermeasure, including those that detect, limit or prevent the particular hiding method's use. The following three sections will explain all categories.

Unified Description Method

- **Hiding Method General Information [mandatory]**
  - Hiding Pattern [mandatory]
  - Application Scenario [mandatory]
  - Required Properties of the Carrier [mandatory]
- **Hiding Method Process [mandatory]**
  - Sender-side Process [mandatory]
  - Receiver-side Process [mandatory]
  - Covert Channel Properties [mandatory]
  - Covert Channel Control Protocol [optional]
- **Potential or Tested Countermeasures [mandatory]**

Figure 2: Overview of the description method's structure.

4 Hiding Method General Information

This section describes the general attributes of the steganographic method. These attributes include the hiding pattern that the method belongs to, the considered and potential application scenarios, and general requirements for the carrier.

4.1 Hiding Pattern [mandatory]

In [Wendzel and Palmer, 2015], we proposed that when a new hiding method is to be published, it should be assigned to a particular pattern or provide evidence why it does not match any of the existing patterns. In case the proposed hiding method does not match any existing pattern, a new pattern can be created [Wendzel and Palmer, 2015]. As the existing patterns are based on many hiding methods invented since 1987, it is likely that a new hiding method can be represented by an existing pattern. In the less likely case that no existing pattern fits, the authors of the new method must provide a detailed explanation of a new pattern that underpins the novelty of the hiding method they propose. The consequence of a new pattern is an extension of the existing pattern catalog.

If the authors decide a hiding method can be represented by an existing pattern, the pattern should be stated including the whole hierarchical path of the pattern in the pattern hierarchy (including sub-patterns). The hiding pattern hierarchy is described in detail in [Wendzel et al., 2015] and an on-line version is available under *https://ih-patterns.blogspot.com*.

A pattern name including the path within the hierarchy is the complete path from the root node of the hierarchy to the leaf that represents the pattern. For instance, a hiding method that modifies the least significant bit (LSB) of a header element would be represented by the "LSB" pattern and the full path of the hierarchy would be:

```
Network Covert Storage Channels
`-- Modification of Non-Payload
    `-- Structure Preserving
        `-- Modification of an Attribute
            `-- Value Modulation
                `-- Least Significant Bit (LSB)
```

For each element of the hierarchy, it should be explained briefly why the described hiding method belongs to the element, e.g. why the new method is a covert storage channel (and not a timing channel), why it preserves instead of modifies the structure of a PDU, why it is an attribute modification, value modulation, and LSB-based method. Using the hierarchy-based explanation, every reader who has knowledge of the pattern hierarchy can easily follow and verify the argumentation of an author.

4.2 Application Scenario(s) [mandatory]

This category describes the application scenario for which a hiding method was developed. It helps to identify novel application scenarios and makes it easier to compare different methods as some hiding methods may have application-specific limitations. Such methods may not be usable in other scenarios. For example, hiding methods developed for breaking anonymization [Zander and Murdoch, 2008] may provide only small throughput making them unusable for general-purpose communication.

Many hiding methods were developed for general-purpose communication, i.e. the passing of secret messages between two or more parties. Typically this application is motivated by the existence of an adversarial relationship between different groups, such as government agencies versus criminal or terrorist organizations or dissenting citizens versus their governments. Other existing hiding methods are tailored to the case of hackers or corporate spies whose aim is to covertly control compromised systems or exfiltrate data from compromised systems. Similarly, malware, such as computer viruses or worms, can use hiding methods to spread undetected, to exfiltrate data, or for covertly exchanging information (e.g. execute brute-force attacks on cryptosystems [White, 1989]). Indeed, this rising trend has been recently confirmed by many real-life examples of information hiding-capable malware [Mazurczyk and Caviglione, 2015].

On the other hand, there are hiding methods that were developed for very specific contexts. Some hiding methods were developed for breaking anonymization, for example Murdoch *et al.* developed methods to reveal servers hidden inside anonymization networks [Murdoch and Danezis, 2005],[Zander and Murdoch, 2008]. Other hiding methods were developed for transmitting authentication data, for example to allow authorized users to access open firewall ports while presenting these ports as closed to all other users ("port knocking") [deGraaf et al., 2005]. Another type of hiding methods were designed for packet/flow traceback or watermarking – techniques used for linking different observable instances of network packets or flows in scenarios where packet contents cannot be used for linking [Houmansadr et al., 2009]. Another specific application are hiding methods developed for cheating in on-line games [Murdoch and Zielinski, 2004].

In case a hiding method is for general-purpose communication, no comprehensive description is needed. However, for methods that were developed for a specific application in a specific context, the application scenario should be described in detail. Also, new application scenarios should be described in more detail than well-known scenarios.

4.3 Required Properties of the Carrier [mandatory]

This category is used to specify the properties of the carrier that the hiding method requires. It should describe whether the hiding method is limited to a certain protocol (or a service) as carrier or whether it can be used with several or even many different carrier protocols/services.

If the hiding method is tied to a single carrier protocol, the description must specify the protocol and describe the specific protocol features that are used by the hiding method. If a hiding method works with a set of carrier protocols, the description must specify the protocols and the protocol features the hiding method relies on. If a hiding method depends on certain protocol features that are common to a large number of protocols, the description must list the features and describe them. For truly generic hiding methods that work with all kinds of carrier traffic the description may be short; however, in our experience such generic hiding methods are rare.

For hiding methods that are not only tied to certain protocols or protocol features, but also require certain operational conditions, these conditions must also be described. For example, a method that hides information by intentionally introducing packet losses assumes that packets of the carrier can be discarded. It can only blend in with the normal traffic if there is natural packet loss [Krätzer et al., 2006]; hence, the possibility and occurrence of natural packet loss is an operational condition for this hiding method.

5 Hiding Method Process

This section covers the categories which describe the actual process of the hiding method, including the embedding and the extraction of hidden data, as well as the channel properties and a potentially present control protocol.

5.1 Sender-side Process [mandatory]

This category describes the embedding process performed by the covert sender to hide secret data. It must be explained whether the sender is a centralized host/process or distributed. In the classical scenario, one sender transfers secret data to one receiver (the sender-to-receiver relationship is '1:1'). However, other scenarios are also possible and they depend on the specific context in which a covert transmission is performed or it can be a characteristic feature of the carrier utilized for hidden data exchange. In case of covert channel overlay networks, it is imaginable that one sender broadcasts the covert data to multiple receivers ('1:m'). In case of a distributed sending system, there may be n hosts forming one logical sender that transfers data to one or multiple receivers ('n:1' and 'n:m' relations). For instance, if the source address of a receiver indicates a hidden bit, two senders can be used to transfer a message of zero and one bits to a receiver.

The location of the covert data can be also centralized or distributed depending on whether the hidden data is 'inserted' into a single carrier (or a subcarrier) or it is distributed across several carriers (subcarriers). This means that the covert data can be embedded into one particular part of a packet or into multiple areas of a packet, but it can be also distributed among different flows [Mazurczyk et al., 2016].

This category should also contain information that describe how the sender synchronizes *where* and *when* secret data is encoded. It is worth mentioning that synchronization capabilities can be necessary at two levels of a covert communication, the bit level and the packet/frame level. In case when multiple carriers or subcarriers can be selected for embedding secret data, a synchronization mechanism should be described, at least if it is necessary for the well-functioning of the covert channel. Such a mechanism should describe how the sender selects the carrier or subcarrier in a way recognizable by the receiver. If a timing channel is given, the category should accordingly explain how a synchronization of timing events is done.

It must be also specified whether the steganographic method generates its own cover traffic or whether data is hidden in third-party cover traffic. In case the hiding method is responsible for the cover traffic generation then a description of this process must be included here.

5.2 Receiver-side Process [mandatory]

This category describes the recognition and extraction process of the covert data at the receiver-side. Similar to the sender-side process description, the secret receiver can be also centralized or distributed and the same considerations apply here (see section 5.1). If the receiver is a distributed system, it should be explained how the covert data is extracted from the hidden data carrier and how it is finally merged. If a synchronization mechanism was implemented by the sender, this category should describe how the receiver-side synchronization is performed.

5.3 Covert Channel Properties [mandatory]

In this category the considered hidden communication scenario(s) for the particular steganographic method should be described and it should be indicated whether the created covert channel is direct or indirect. Moreover, four characteristic features of the information hiding technique should be analyzed. This will allow to describe properties of the created covert channel.

For network steganography, two main possible communication scenarios may be considered, as illustrated in Fig. 3. The first scenario, i.e. end-to-end scenario, is the most common: the secret sender and the secret receiver perform overt communication while simultaneously exchanging covert data. In this case the overt communication path is equal to the covert path. In the second scenario, i.e. Man-in-the-Middle (MitM) scenario, only a part of the end-to-end overt communication path is used for the hidden communication, as a result of actions undertaken by intermediate covert nodes. Therefore, the overt sender and overt receiver are, in principle, unaware of the steganographic data exchange. Obviously hybrid scenarios are also possible where the overt sender/receiver serves as secret sender/receiver but the other covert party is located in some intermediate node.

Next, it should be indicated whether the covert channel is *direct* or *indirect*, i.e. whether the overt traffic flows directly from the secret sender to the secret receiver or via one or multiple intermediaries. In case of a direct channel the overt traffic that contains the covert data flows directly from the secret sender to the secret receiver (who both can act as middlemen). A covert channel is indirect when the secret sender does not send covert data directly to the secret receiver (or a destination downstream of the secret receiver). Instead, the secret sender transmits the covert data to an intermediate host which then unknowingly forwards (due to the functions of the overt traffic protocol) the covert data to the secret receiver. This means that there are two flows of the overt traffic conveying the covert data, i.e. the first flow is between the secret sender and an unwitting intermediary and the second flow is between the intermediary and the

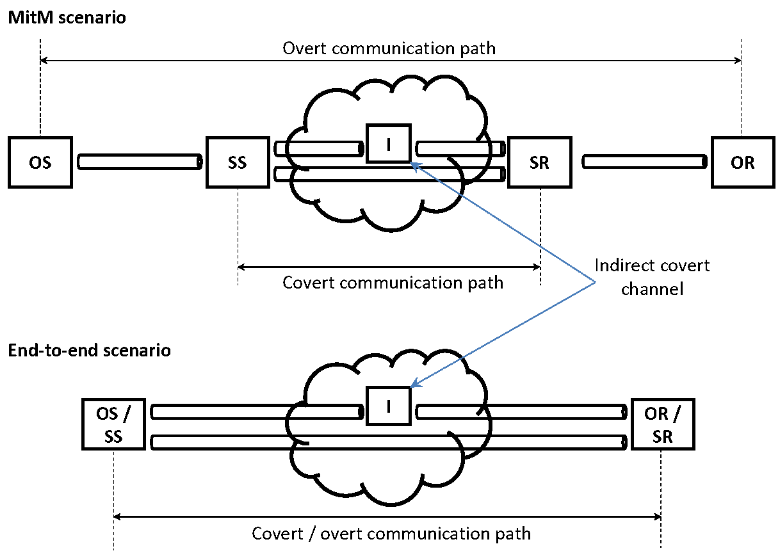

Figure 3: Hidden communication scenarios (OS – overt sender, OR – overt receiver, SS – secret sender, SR – secret receiver, I - intermediate node)

secret receiver. Indirect covert channels provide an increased stealthiness as a warden does not observe a direct flow of information between the covert sender and receiver. On the other hand they are typically harder to implement and have a smaller capacity than direct channels. In case of an indirect channel the requirements on the intermediate need to be described.

For example, Rowland [1997] proposed an indirect channel that exploits the TCP three-way-handshake. Instead of sending a TCP SYN segment with an ISN containing covert data directly, the secret sender sends the TCP SYN segment to the intermediary (a bounce host) with a spoofed IP source address set to the intended destination. The intermediary then sends a SYN/ACK or SYN/RST to the secret receiver with the acknowledged sequence number equal to the ISN+1. The secret receiver decodes the hidden information from the ACK number (ACK−1).

The classic characteristics of any information hiding method as mentioned by Fridrich in [Fridrich, 2009] are: *steganographic bandwidth* (or *channel capacity*), *undetectability* and *robustness.*

Steganographic bandwidth/capacity is the number of secret bits that can be sent per time unit when using a particular method or under a given condition, e.g. being undetectable with a specific detection technique, that is $B_s = b_s/t$. While the absolute bandwidth is most important, another relevant metric is the average ratio of the number of secret bits to the number of carrier bits $r_s = \sum(b_s)/\sum(b_c)$.

Undetectability is the inability to notice a steganogram within a certain carrier, under certain conditions, or the inability to notice the presence of a steganographic communication, at all. A more formal description can be based on [Liu et al., 2010]. Assume there is a sequence of N feature values used to encode covert data, such as N message delays or lengths, and define F and $\tilde{F}$ to be feature distributions for the covert channel and legitimate traffic respectively. Then, a covert timing channel is called polynomially undetectable with respect to a security parameter σ if it holds for any distinguisher D with a runtime polynomial in σ and for any N that is polynomial in σ that $D(F, \tilde{F})$ is negligible in σ.

Robustness is the amount of network and adversary noise a covert channel can withstand so that the covert receiver can still decode the data.[1] What constitutes noise depends on the type of channel, e.g. it could be delay, packet loss or packet modifications. Robustness can be measured as the capability to achieve a decoding bit error rate (BER) smaller than a given robustness threshold ϵ. Since the BER is inversely proportional to the Signal-to-Noise Ratio (SNR), robustness can also be defined in terms of the SNR. A channel is called γ-gain robust if the SNR after performing the encoding and modulation is γ times greater than the original SNR [Liu et al., 2010].

As proposed in [Mazurczyk et al., 2014], another attribute is the steganographic cost, which describes the degradation or distortion of the carrier caused by the application of the steganographic method.

All these attributes should be described, if feasible. Especially for novel methods and for the description of third party tools, a comprehensive description of all four characteristics is hardly feasible. The author of a paper may have no access to implementations of these countermeasures, to testbeds in which countermeasures could be evaluated, or may have no knowledge of all existing countermeasures. Since the detectability issues are also discussed in the category 'Potential and Tested Countermeasures' only a brief description or reference to that category is required here.

5.4 Covert Channel Control Protocol [optional]

Several hiding methods utilize so-called covert channel control protocols. Covert channel control protocols embed small protocol headers providing several features including reliable data transfer (by introducing sequence numbers and ACKs), peer discovery and dynamic overlay routing (between steganographic

[1] Some previous work further distinguishes between *robustness*, robustness against normal network noise, and *active robustness*, robustness against noise created by an adversary, cf. Mazurczyk et al. [2016].

peers), session management for covert transactions, adaptiveness and several features of application layer protocols (e.g. file transfer features) [Wendzel and Keller, 2014; Mazurczyk et al., 2016]. If utilized by a hiding method, both the design, implementation and features of a covert channel control protocol must be described in this category. Otherwise, the category can be left empty.

6 Potential or Tested Countermeasures

This category comprises no sub-categories. It should describe potential as well as tested countermeasures available against the hiding technique. There are three types of countermeasures that can be applied against the covert channel created by a hiding method: elimination, limitation, and detection [Zander et al., 2007]. Not all of these three types may be applicable for a particular hiding method, for example some covert channels cannot be eliminated. The description must contain a discussion which countermeasures are applicable and which are not applicable including a justification. For instance, a reasonable justification for applying a countermeasure would be that it does not significantly influence the legitimate communication in a network. A more formal approach to explain the justification of applying a countermeasure would be to discuss its *Minimal Requisite Fidelity* (MRF), which is a *measure of the degree of signal fidelity that is both acceptable to end users and destructive to covert communications* and that was proposed by Fisk et al. [2003]. Applicable countermeasures should then be described in detail.

Elimination means the covert channel created by a hiding method can be eliminated completely. For example, a method that hides data in unused header fields or padding bytes can be eliminated completely by a traffic normalizer that sets the unused header fields or padding bytes to a default value (e.g. zero). Some hiding methods cannot be eliminated, for example covert channels in online game protocols [Zander et al., 2008]. If a covert channel can be eliminated, the description should include a discussion on how the elimination works and any possible limitations. The description should also include side-effects of the elimination process. For example, if a covert channel in a header extension can be eliminated by removing the header extension from the packets, then the description should include a discussion of the impact on the protocol functionality.

Limitation means the covert channels can be perturbed, for example by introducing noise, so that its capacity is greatly reduced and the channel effectively becomes useless. Limitation usually has side-effects on the carrier, so there is a trade-off between reducing a covert channel's capacity to a small value and not significantly impacting the carrier protocol. The description should include a discussion on whether a channel's capacity can be limited and the impact on the carrier should be characterized. If a channel can be eliminated then a description of a limitation method is optional.

Elimination or capacity-limitation are active countermeasures that require a warden to manipulate the network traffic (active warden) [Fisk et al., 2003]. However, having an active warden may not be possible in every scenario.

The warden can audit the use of any covert channels it can detect. Usually detection mechanisms are based on some characteristics that can be observed, and the characteristics for traffic with covert channels are different from the characteristics of regular traffic (traffic without covert channels). While detection itself is passive, it can be coupled with active measures such as targeted blocking, elimination or limitation where the warden can manipulate suspicious traffic with more impunity. The description should include whether the channel can be detected and outline the detection method. If the channel is impossible to detect, the description should provide a justification why it is undetectable. If a detection method is introduced, the proposed characteristics for identifying the covert channel must be defined.

If an evaluation of the proposed elimination, limitation or detection method(s) has been conducted, the description should summarize the evaluation scenario(s) and results. Ideally, an evaluation is done under realistic conditions, e.g. in real networks using realistic traffic, but in practice this is not always feasible. The description of the evaluation should point out any such limitations.

Another type of countermeasure is to change the specification of a network protocol to prevent its use as carrier in the future. For example, a network protocol prone to covert channels could be revised and updated with a newer version less prone to covert channels. In many cases this may not be realistic, as widely deployed protocols cannot be changed easily. However, in cases where an updated protocol could be realistically deployed, this should be described.

The description should also discuss whether the warden can be a single entity (centralized warden) or has to be multiple distributed instances (distributed warden), and whether the warden has to keep flow state (stateful warden) or can operate without flow state (stateless warden).

7 Literature Analysis

In this section, we provide an analysis of existing publications that describe hiding methods. The goal of our analysis is to determine how well the attributes of our unified description method are described within these existing papers.

To identify relevant publications, we selected those papers that appeared in a Google Scholar search using the search terms 'network AND covert channel(s)' and 'network steganography' as well as the papers that were cited in [Wendzel et al., 2015]. For each publication that we found, we made sure that it described at least one network information hiding method. We limited our search range to the years 1987-2015 as the first academic work on network information hiding was published in 1987. As a result, we analyzed 74 publications that presented new hiding methods. We made the list of all analyzed papers available under the URL `http://www.wendzel.de/J.UCS/db_publications.pdf`.

Figure 4 shows the analyzed publications per year. In early years, only few papers on network covert channels were published. The number of papers grew over time due to the increasing popularity of the topic. As some papers describe more than one hiding technique, the number of analyzed hiding techniques (131 in sum) is sometimes larger than the number of publications, which is also shown in Fig. 4. The number of found publications in the year 2015 is comparable low due to the delayed indexing of academic publications.

As can also be seen in Figure 4, there is a peak of hiding techniques published in the year 2006. This peak is a result of the publication [Lucena et al., 2006] which presented 22 hiding techniques for IPv6, AH and ESP in a single document.

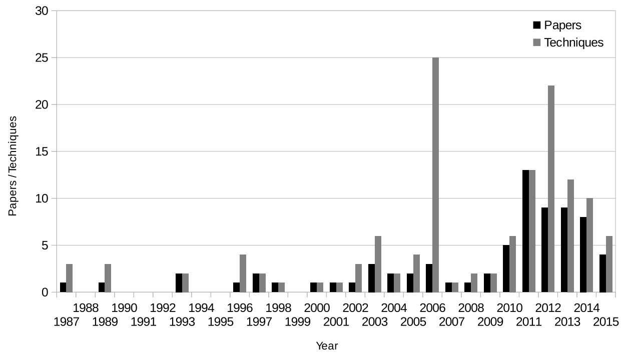

Figure 4: Analyzed publications that present hiding methods (per year).

Finding 1: Several papers lack fundamental attributes

As already stated in the introduction, our analysis shows that publications on hiding methods present varying subsets of attributes. Figure 5 provides an overview of the present attributes for all described hiding methods of the analyzed papers. When an attribute's description is classified as 'partial', the authors provided some aspects but lack other fundamental aspects of the particular attribute. The comprehensive description of an attribute was marked with 'yes' (fully present).

Out of the 131 described hiding methods, the application scenario was provided for 78% of them (74 fully, 30 partially). The required properties for the

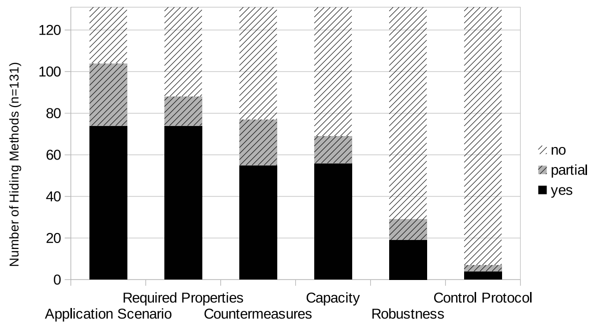

Figure 5: Presence (fully or partially) of selected attributes in the publications.

hiding method were fully described for 74 and partially for 14 hiding methods (combined 67%). For some of the techniques, the authors provided countermeasures: 55 contained a full description with evaluation of at least one countermeasure and for another 13 techniques, possible countermeasures were at least briefly discussed (combined 58%).

The channel capacity was evaluated for 52% of the hiding methods (56 fully, 13 partially; both values also including throughput and bitrate measurements). The robustness of the proposed hiding methods was discussed for only 22% of the hiding methods (19 fully, 10 partially). Control protocols are not part of most hiding methods and for this reason only described for 5% of the hiding methods (4 fully, 3 partially).

Finding 2: Attribute coverage changed over time

The attributes covered by publications changed over time. Figure 6 provides an overview of selected attributes over time. We omitted the sender-side and receiver-side processes that were described in most publications but in very varying detail.

Over time, the covert channel capacity was increasingly discussed, especially in publications from the last six years (2010–2015). Channel robustness was constantly discussed for only 20% of the hiding methods. Both, channel capacity and robustness are part of the 'Covert Channel Properties' in our description method. The discussion of countermeasures varied over time and is similar in the range 2010–2015 as it was in 1987–1999 (approx. 68%). The required properties of the carrier were discussed by fewer publications in recent years (2010–2015) compared to the years 2000–2009.

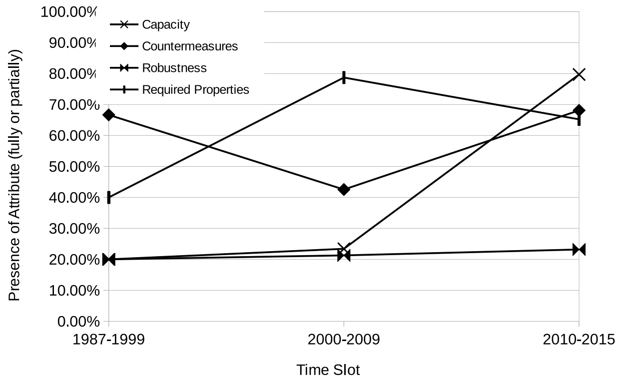

Figure 6: Coverage of selected attributes for hiding methods over time.

Finding 3: Domination of few hiding patterns

Hiding patterns were proposed only recently. For this reason, none of the analyzed publications covered any hiding patterns. We analyzed all hiding methods by verifying whether they were already assigned a pattern in Wendzel et al. [2015] and for several methods which had not been analyzed in that publication, we determined their hiding patterns. We were able to assign 130 of the 131 analyzed hiding methods to their respective patterns. One publication discussed a steganographic key exchange that applies to many hiding methods and thus cannot be assigned to a hiding pattern. Figure 7 shows the distribution of hiding patterns. As shown, most of the hiding methods we found were categorized as 'Value Modulation', followed by the 'Inter-arrival Time' pattern. For the patterns 'PDU Order', 'Re-Transmission' and 'Rate', less than five hiding methods were found. These findings can support the development of countermeasures as an efficient countermeasure may target one of the predominant hiding methods instead of a hiding pattern that is barely implemented.

Finding 4: Varying countermeasure descriptions

We found that the coverage of countermeasures for proposed hiding methods varies greatly among the analyzed papers. While several papers highlight their countermeasures briefly (sometimes only within a single sentence) other publications discuss them in more detail.

We analyzed whether papers covered one of the three types of countermeasures: detection & auditing, limitation, or prevention. Of those papers which provide a more-detailled discussion of potential or evaluated countermeasures, most cover a detection or prevention approach while very few discuss auditing or

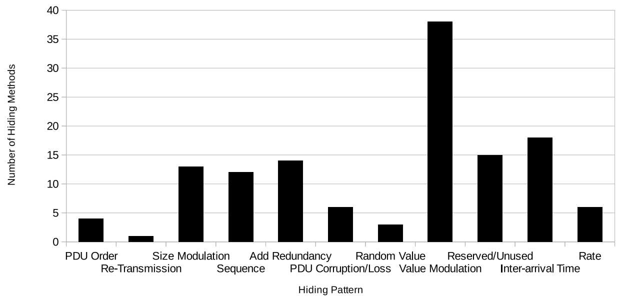

Figure 7: Occurrences of hiding patterns for the analyzed hiding methods.

limitation approaches – examples of the latter are Girling [1987] (auditing and limitation) and Sadeghi et al. [2012] (limitation and prevention). Some works do also cover several countermeasures of the same type, e.g. Cabuk et al. in [2004] propose three methods for the detection the Inter-packet timing method (Section 8.1).

Overall, we found that the vast majority of publications do not discuss all types of countermeasures or even two of them in detail, i.e. featuring an actual evaluation of these. We believe that this is the most significant drawback of current research. However, it must be empasized that researchers are expected to publish several papers during their carrer while facing time pressure. For this reason, countermeasures are sometimes discussed in one or multiple follow-up papers. This approach, however, makes it more difficult to track the progress on research for a particular hiding method.

Finding 5: Inconsistent method descriptions within papers

Some of the publications describe several hiding methods while applying an inconsistent description for these within the same work. We use [Tuptuk and Hailes, 2015] as an example for this scenario. The authors present two covert channels for pervasive computing environments. The first signals hidden information by modulating the Link Quality Indication (LQI) of 802.15.4 wireless networks while the second modulates the values of a temperature sensor to signal hidden information. Table 1 indicates which of the selected attributes of the description are present, partially present, or not present. The table reveals that different attributes are described for each channel. The lack of a unified description makes it harder to compare different channels.

However, the abovementioned paper is not the only paper containing an inconsistent method description as several other papers contain similar descriptions. We assume that inconsistent descriptions of hiding methods are also linked

Table 1: Presence of attributes in descriptions (●= present, ◐= partly present, ○= missing, ⧄= combined description). Exemplified using Tuptuk and Hailes [2015] (**A**) and Tsiatsikas et al. [2015] (**B**)

Hiding Method	Application Scenario	Required Properties	Counter-measures	Sender-Receiver Relation	Direct/ Indirect	Robust-ness	Capacity
Link quality (A)	●,⧄	◐	●	○	○	●	●
Sensor data (A)	●,⧄	◐	◐	●	◐	●	◐
SDP o-tag (B)	●,⧄	◐,⧄	○	○	○	◐,⧄	◐,⧄
SDP a-tag (B)	●,⧄	◐,⧄	○	○	○	◐,⧄	◐,⧄

to the necessity to shorten papers to match certain page limits of workshops and conferences. Such page limits can be matched easier when descriptions are combined for multiple hiding methods.

Finding 6: Combined evaluation of multiple hiding methods

We also found that sometimes multiple hiding methods are treated in a combined way throughout a paper. Tab. 1 summarizes the combined and the non-combined attributes of [Tsiatsikas et al., 2015]. The authors describe two hiding methods for SIP useful for the stealthy command-and-control communication in a botnet. The first channel uses the mandatory ‘$<$ o $>$’ tag to carry hidden information while the second uses the optional ‘$<$ a $>$’ tag and its parameter to do the same. Both channels are combined for the evaluation process as both channels are necessary to transfer the required secret message. This combined evaluation does not allow the reader to understand the performance of each channel separately and it also makes the comparison against other methods difficult.

Finding 7: Varying scenario descriptions

The standard scenario used in information hiding is Simmon's *Prisoner's Problem* [Simmons, 1984]: Two prisoners, Alice and Bob, establish a subliminal communication channel to plan escaping jail while being only allowed to indirectly communicate via the warden Walter. A variation of this scenario is the case where the communication channel is not mediated by the warden [Carrara and Adams, 2016a].

The Prisoner's Problem is used by several publications, especially early ones such as Handel et al. [1996]. However, even early publications provide a variety of scenarios. For instance, Kang and Moskowitz discusses network covert channels in the context of multi-level security (MLS) [Kang and Moskowitz, 1993], i.e. the focus is on a policy-breaking communication and not on a stealthy communication. The scenario by Rowland is the communication of a trojan horse [Rowland, 1997] and in [Wolf, 1989], the author provides the scenario of bypassing filters.

Ahsan and Kundur describe a version of the Prisoner's Problem in a network scenario [Ahsan and Kundur, 2002]. Alice and Bob are connected to a LAN with their workstations. Both wish to establish a stealthy communication but a security-aware warden (network administrator) is present. Similarly, Wendzel et al. [2012] discuss the scenario of a cyber-physical-system (CPS), in particular a smart building. Using the smart building, two parties wish to establish a stealthy communication or use a (relatively insecure) smart building to exfiltrate data out of a cooperative network [Wendzel et al., 2014]. Alice and Bob therefore embed hidden information in a communicaton protocol used to transfer building automation-related data. Tuptuk and Hailes [2015] discuss the scenario of pervasive computing in which a covert communication is performed. The use of a covert channel in their view is either to leak potentially sensitive information or to influence a CPS' operation.

Malware communication is another scenario domain. Tsiatsikas et al. [2015] use the scenario of a stealthy command & control communication for botnets. Calhoun et al. mention two different scenarios: The first is a covert authentication while the second is a wifi-version of the already mentioned botnet that uses a covert channel for its command & control communication [Calhoun Jr et al., 2012].

Although Craver's work [1998] is not specific to network communications, it discusses a public-private key-based approach for steganographic communication, e.g. in audio or video clips. Key exchange can be seen as a fundamental aspect for the communication scenarios as it must be performed a priori in order to allow any stealthy communication between Alice and Bob.

8 Exemplary Descriptions

We now present two exemplary descriptions. The first description is for a covert timing channel, while the second description is for a covert storage channel.

8.1 Example 1: Inter-packet Timing Method

In this example we describe a specific steganographic method for hiding information in inter-packet timings. This method or channel is also referred to as model-based inter-packet gap channel and was proposed by Gianvecchio et al. [2008].

8.1.1 Hiding Pattern

As the covert signaling utilizes the timing of network packets, the method belongs to the 'Network Covert Timing Channel' pattern. In particular, the method falls under 'Inter-arrival Time'. The full path in the pattern hierarchy is:

```
Network Covert Timing Channels
'-- Inter-arrival Time Pattern
```

8.1.2 Application Scenario

The method can be used for general-purpose covert communication between a covert sender and a covert receiver or between a group of covert parties depending on whether the carrier is unicast or multicast.

8.1.3 Properties of the Carrier

The method only requires that the carrier consists of packetized data, such as network-layer packets, whose timing can be manipulated. The method assumes that there is sufficient noise in the timing of packets by senders and along the path, so that manipulations of timings are not immediately suspicious. While the method was proposed and evaluated for HTTP in [Gianvecchio et al., 2008], it is not limited only to this protocol. However, some carrier protocols are more suitable than others. Since the encoding destroys any dependence between the inter-packet times of successive packets, it is best used with carriers that already have independent inter-packet times [Zander et al., 2011].

8.1.4 Sender-side Process

The embedding process involves fitting a model to the inter-packet time distribution of regular traffic and then using the model to generate covert channels with identical distribution (for details see [Gianvecchio et al., 2008]). There is usually a single sender process that embeds the covert channel in a single carrier. Note that a single carrier can be multiple traffic flows.

Since the carrier is HTTP/TCP, the reliability of TCP (handshake, teardown, sequence numbers, ACKs) provides basic bit synchronization and reliable in-order delivery of bits for a single carrier flow. A fully reliable channel, supporting multiple carrier flows, would also require the framing of messages and frame synchronization. While [Gianvecchio et al., 2008] did not discuss this, existing techniques could be used.

In the original work the covert sender generated the overt traffic [Gianvecchio et al., 2008]. However, the method can be also applied to embed the covert channel into existing network traffic at the cost of increasing the latency of the overt traffic [Zander et al., 2011].

8.1.5 Receiver-side Process

The extracting process running on the single receiver decodes the covert bits from the observed inter-packet times of the single carrier as described in [Gianvecchio et al., 2008].

The receiver can leverage TCP's reliability, so there are no lost or reordered bits for a single TCP carrier flow. Additional higher-layer mechanisms may be needed for full reliability as discussed in Section 8.1.4.

8.1.6 Covert Channel Properties

The method can be used in the end-to-end scenario, where covert sender and receiver are also the overt sender and receiver, and in a MitM scenario, where covert sender and receiver are placed between the actual sender and receiver (as well as in hybrid scenarios). The method creates a direct channel between covert sender and receiver(s). The steganographic bandwidth depends on the channel noise and the packet rate of the carrier traffic. Gianvecchio *et al.* measured capacities of 5–20 bits per second in their experiments. Note that in practice the goodput is likely smaller as part of the capacity will be used by a control protocol to provide reliable transport. The channel is hard to detect only if the regular traffic has uncorrelated inter-packet times which is largely the case when HTTP is used as a carrier (as in [Gianvecchio et al., 2008]). Otherwise the channel can be detected with metrics that can measure the dependency of inter-packet times [Zander et al., 2011]. The channel is robust against typical network packet timing noise. If an active warden can manipulate packet timings without impunity, the capacity of the channel would be severely reduced up to a degree where the channel would be practically eliminated. Measurements regarding the steganographic cost were not provided by the authors as the concept of steganographic cost had not been introduced at that time. The steganographic cost depends on the abovementioned channel characteristics and the carrier traffic. In general, the more severely delays are perturbed in overt traffic, the higher the steganographic cost.

8.1.7 Control Protocol

Gianvecchio et al. [2008] only describe the "physical layer" of the covert channel (encoding/decoding of bits) and do not mention a control protocol.

8.1.8 Countermeasures

The covert channel can be limited or even practically eliminated by introducing timing noise, either at the sender or in the network [Fisk et al., 2003]. Depending on the carrier this may introduce unwanted side-effects though, for example, it may add additional latency to the carrier application's traffic.

The covert channel mimics the distribution of inter-packet times of the normal traffic. This makes the channel hard to detect if the normal traffic has uncorrelated inter-packet times [Gianvecchio et al., 2008]. However, for applications that have correlated inter-packet times, the channel can be detected with metrics that can measure the dependency of inter-packet times [Zander et al., 2011].

8.2 Example 2: DHCP Number of Options Storage Method

We now discuss the description of a covert storage channel. Rios *et al.* presented several DHCP-based covert channels, of which one hides information by changing the number of DHCP options in a DHCP packet [Rios et al., 2012].

8.2.1 Hiding Pattern

As the modification of DHCP options represents the modification of a storage attribute, the method falls under 'Network Covert Storage Channels'. The DHCP options are part of the DHCP header and thus, a 'Modification of Non-Payload'. They are also 'Structure Modifying' as the header structure is extended when DHCP options are embedded. The signaling of the hidden information is performed in a way that a sequence of objects (DHCP options) is utilized ('Sequence Pattern') and, in particular, the number of options represents the hidden information itself ('Number of Elements Pattern'). The full path in the pattern hierarchy is:

```
Network Covert Storage Channels
‘-- Modification of Non-Payload
    ‘-- Structure Modifying
        ‘-- Sequence Pattern
            ‘-- Number of Elements Pattern
```

8.2.2 Application Scenario

Rios *et al.* discuss a potential application in a data exfiltration scenario [Rios et al., 2012]: Alice, having privileged access to an embassy network, needs to receive information from Bob, but the direct communication between Alice and Bob is forbidden and the Internet-based communication between them would be suspicious. Bob visits the embassy and transfers network messages to Alice. He embeds hidden information within the non-blocked DHCP protocol using the local network. The application scenario foresees only an uni-directional communication, i.e. no backwards channel from Alice to Bob, but in general the channel could be bi-directional.

8.2.3 Properties of the Carrier

The DHCP protocol must be allowed, i.e. not administratively prohibited by a network security policy (e.g. blocked by a switch or layer-2 firewall). As the intended transfer of hidden information is uni-directional, i.e. only from Bob to Alice, Alice is not required to be able to send over the carrier herself. In addition, sender and receiver must be located within the same network.

The hiding method is protocol-specific and can only be applied to the DHCP protocol. To apply the technique, the network must not block particular DHCP options and the encoding of hidden information must be performed in a way that for all encodable symbols, the resulting DHCP packet is still transferable over the carrier.

8.2.4 Sender-side Process

The secret sender generates its own overt traffic. The sender-side process embeds a hidden symbol by adding the number of DHCP options the symbol requires for its encoding to the DHCP packet. At least two options must be embedded due to the DHCP standard, for example, if the symbols are 'A'–'Z', the symbol 'A' requires two options already [Rios et al., 2012]. The symbol 'Z' would require 27 options, which is likely to raise suspicion [Rios et al., 2012] and may be blocked by firewalls. Each symbol to be transmitted must be encoded in a separate packet.

Reliability is not implemented directly – instead the *recovery mechanisms provided by DHCP against packet loss* are exploited [Rios et al., 2012].

8.2.5 Receiver-side Process

The receiver observes DHCP messages sent by the covert sender and counts the number of embedded DHCP options. The number of DHCP options represents the hidden symbol. The decoding is performed separately for each DHCP packet and the received symbols are combined to reassemble the transmitted message.

8.2.6 Covert Channel Properties

The method works in an end-to-end communication scenario. It cannot be used in a MitM scenario due to the properties of DHCP (broadcast messages that are limited to one subnet). The channel is a direct channel. The bandwidth of the channel depends on the number of DHCP packets sent per second. In general, the channel can transfer as many symbols as packets per second. The detectability of the channel increases with the number of symbols encoded per second and with the size of the encoded symbol. The detectability of a message transfer could be improved by encoding the most frequently used symbols with shorter messages (i.e. apply Huffman coding). Robustness of the covert communication is provided by the use of DHCP's recovery mechanisms. Measurements regarding the steganographic cost were not provided by the authors as the concept of steganographic cost had not been introduced at that time. In general, the distortion of the used carrier (e.g. the Ethernet environment) is minimal as long as the number of DHCP packets does not influence the network's performance in a recognizable manner.

8.2.7 Control Protocol

No control protocol was described in [Rios et al., 2012]. As stated in [Rios et al., 2012], a bi-directional communication over the covert channel is feasible, so bi-directional control protocols could be integrated.

8.2.8 Countermeasures

The easiest way to eliminate the method is to prevent the use of the DHCP protocol or DHCP packets with more than two options. However, this solution may not be practically applicable as the DHCP protocol is essential in most networking environments. A traffic normalizer that deletes uncommon or redundant DHCP options would be a better solution but it may eliminate actually required protocol functionality.

Another potential countermeasure would be to limit the number of DHCP packets per second. This approach reduces the channel's performance as each symbol must be encoded in a separate packet. As the number of DHCP packets per second is unlikely to be high during regular transmissions, a statistical analysis will probably allow an accurate detection of the steganographic method.

Rios *et al.* state that large DHCP packets, i.e. those with many options, may raise suspicion [Rios et al., 2012]. DHCP packets with an unusual large number of embedded options can likely be detected with simple intrusion detection rules.

9 Linking Description Method and Creativity Framework

In the creativity framework [Wendzel and Palmer, 2015], the major focus is on the evaluation of creativity, especially originality, of a proposed hiding method. We will briefly describe the creativity framework and afterwards explain how the new unified description method can be used to improve it.

Steps of the Creativity Framework: The creativity framework consists of five steps which are aligned with the traditional peer review process. In step one, a pattern database is generated by the research community. Due to the availability of an existing pattern catalog, step one is already accomplished.

In the second step, the authors create the idea of a new hiding method, e.g. to embedd hidden bits into a new network protocol. The authors describe their new hiding method in form of a scientific paper in step three. They justify the novelty of their method using the *creativity metric*, which is based on the originality of the method (hiding method pattern) as well as the context (application scenario and carrier network protocol).

The authors submit their paper to a peer review. The reviewers evaluate the novelty of the work using the creativity metric and decide whether the proposed work is a "Big-C" or a "small-c" contribution, i.e. whether the work consists a high level of creativity. Big-C and small-c are standard terms from creativity research. Only in the Big-C case, the work is accepted to represent a new pattern and its pattern description is optimized in step four, otherwise step four is skipped.

The work is published in step five. In case of "Big-C" the publication has to state that the work represents a new pattern – this automatically extends the pattern database. In case of "small-c", the hiding method is published but the authors cannot claim that they have discovered a new pattern; instead they provide new results for an existing hiding pattern.

Benefits of Combining Both Approaches: The creativity metric does not enforce a detailed description structure. Our unified description method can replace the descriptive aspects of the creativity metric since it provides a more fine-grained description and allows for the distinction and comparison of various aspects of a hiding method. Several attributes, such as whether a hiding method can operate in a MitM setup or a distinction between the sender-side and receiver-side processes, were not covered in [Wendzel and Palmer, 2015]. On the other hand, our unified description method can benefit from the creativity framework. There is no reason to create a new approach for integrating the unified description method into the peer review process. Also, the creativity framework evaluates the novelty of a hiding method by applying research from creativity psychology, which can serve as an add-on to the technical evaluation of the unified description method. In summary, the combination of both approaches can be considered beneficial.

10 Discussion and Conclusion

We developed an approach to unify and structure the description of network steganographic methods. To this end, we performed a comprehensive literature analysis in the domain to identify requirements for the description method. Currently, no such description exists, making it difficult to compare the published work on hiding methods. Unified descriptions of hiding methods are desirable as they ease the comparison of research results. They also improve the accessibility of hiding methods and foster the reproduction of experimental results. As a key aspect of our description method is the association of hiding methods with a hiding pattern, the approach automatically enforces a categorization of the research results into the known pattern taxonomy. Last but not least, scientists can easily spot research gaps as they see what aspects of the method were already documented (e.g. channel capacity or detection methods) and which aspects are left for future work.

However, it could be difficult to win recognition for a unified hiding method description as, in the end, it is up to every author to decide how to describe his or her hiding method. For this reason, we designed our description so that it will be applicable and attractive for hopefully many authors. Our description structure does not specify every single detail of all attributes. It leaves several decisions to the authors, such as whether or not to discuss details of certain attributes (e.g. covert channel capacity), the form of descriptions (e.g. text or figures), and the extent of the descriptions. This flexibility allows to apply the unified description method also in short papers which are, for many conferences, limited to four to six pages. As one attribute is specified as ‘optional’, it can be also left out.

We identified a benefit when combining the new unified description method with the existing ‘creativity framework’. The framework’s process is kept but the ‘creativity metric’ of the framework is replaced with our unified description method.

Acknowledgements

The authors would like to thank the anonymous reviewers for their valuable comments.

References

[Ahsan and Kundur, 2002] Ahsan, K., Kundur, D.: “Practical data hiding in TCP/IP”; Proc. Workshop on Multimedia Security at ACM Multimedia; volume 2; 2002.

[Borchers, 2001] Borchers, J.: A Pattern Approach to Interaction Design; Wiley, 2001.

[Cabuk et al., 2004] Cabuk, S., Brodley, C. E., Shields, C.: “IP covert timing channels: Design and detection”; Proc. 11th ACM conference on Computer and Communications Security (CCS’04); 178–187; ACM, 2004.

[Calhoun Jr et al., 2012] Calhoun Jr, T. E., Cao, X., Li, Y., Beyah, R.: “An 802.11 MAC layer covert channel”; Wireless Communication Mobile Computing; 12 (2012), 393–405.

[Carrara and Adams, 2016a] Carrara, B., Adams, C.: "Out-of-band covert channels – a survey"; ACM Computing Surveys; 49 (2016a), 2, 23:1–36.

[Carrara and Adams, 2016b] Carrara, B., Adams, C.: "A survey and taxonomy aimed at the detection and measurement of covert channels"; Proc. 4rd ACM Workshop on Information Hiding and Multimedia Security (IHMMSec'16); 115–126; ACM, 2016b.

[Craver, 1998] Craver, S.: "On public-key steganography in the presence of an active warden"; Proc. Information Hiding; volume 1525 of LNCS; 355–368; Springer, 1998.

[deGraaf et al., 2005] deGraaf, R., Aycock, J., Jr., M. J.: "Improved Port Knocking with Strong Authentication"; Proceedings of 21st Annual Computer Security Applications Conference; 2005.

[Fincher, 2003] Fincher, S.: "CHI 2003 workshop report 'perspectives on HCI patterns: Concepts and tools (introducing PLML)"'; (2003).

[Fisk et al., 2003] Fisk, G., Fisk, M., Papadopoulos, C., Neil, J.: "Eliminating steganography in internet traffic with active wardens"; Proc. Information Hiding; volume 2578 of Lecture Notes in Computer Science; 18–35; Springer, 2003.

[Freeman et al., 2004] Freeman, E., Robson, E., Bates, B., Sierra, K.: Head First Design Patterns; O'Reilly Media, Inc., 2004.

[Fridrich, 2009] Fridrich, J.: Steganography in Digital Media – Principles, Algorithms, and Applications; Cambridge University Press, New York, NY, 2009.

[Gianvecchio et al., 2008] Gianvecchio, S., Wang, H., Wijesekera, D., Jajodia, S.: "Model-Based Covert Timing Channels: Automated Modeling and Evasion"; Proceedings of Recent Advances in Intrusion Detection (RAID) Symposium; 2008.

[Girling, 1987] Girling, C. G.: "Covert channels in LAN's"; IEEE Transactions on Software Engineering; 13 (1987), 292–296.

[Handel and Sandford, 1996] Handel, T. G., Sandford, M. T.: "Hiding data in the OSI network model"; Proc. First International Workshop on Information Hiding; 23–38; Springer, 1996.

[Houmansadr et al., 2009] Houmansadr, A., Kiyavash, N., Borisov, N.: "RAINBOW: A Robust And Invisible Non-Blind Watermark for Network Flows"; Proceedings of 16th Annual Network & Distributed System Security Symposium (NDSS); 2009.

[Kang and Moskowitz 1993] Kang, M. H., Moskowitz, I.: "A pump for rapid, reliable, secure communication"; Proc. 1st ACM Conference on Computer and Communication Security; 119–129; ACM, 1993.

[Katzenbeisser and Petitcolas, 2000] Katzenbeisser, S., Petitcolas, F. A., eds.: Information Hiding Techniques for Steganography and Digital Watermarking; Artech House, Inc., Norwood, MA, USA, 2000; 1st edition.

[Krätzer et al., 2006] Krätzer, C., Dittmann, J., Lang, A., Kühne, T.: "WLAN

Steganography: a First Practical Review"; Proceedings of 8th ACM Multimedia and Security Workshop; 2006.

[Liu et al., 2010] Liu, Y., Ghosal, D., Armknecht, F., Sadeghi, A.-R., Schulz, S., Katzenbeisser, S.: "Robust and undetectable steganographic timing channels for iid traffic"; International Workshop on Information Hiding; 193–207; Springer, 2010.

[Llamas et al., 2005] Llamas, D., Allison, C., Miller, A.: "Covert channels in Internet protocols: A survey"; Proc. 6th Annual Postgraduate Symp. Convergence of Telecommunications, Networking and Broadcasting (PGNET 2005); 2005.

[Lucena et al., 2006] Lucena, N. B., Lewandowski, G., Chapin, S. J.: "Covert channels in ipv6"; Proc. 5th PET Workshop 2006; volume 3856 of LNCS; 147–166; Springer, 2006.

[Mazurczyk and Caviglione, 2015] Mazurczyk, W., Caviglione, L.: "Information hiding as a challenge for malware detection"; Security Privacy, IEEE; 13 (2015), 2, 89–93.

[Mazurczyk et al., 2014] Mazurczyk, W., Wendzel, S., Villares, I. A., Szczypiorski, K.: "On importance of steganographic cost for network steganography"; Security and Communication Networks (SCN); (2014).

[Mazurczyk et al., 2016] Mazurczyk, W., Wendzel, S., Zander, S., Houmansadr, A., Szczypiorski, K.: Information Hiding in Communication Networks: Fundamentals, Mechanisms, and Applications; IEEE Series on Information and Communication Networks Security; Wiley-IEEE Press, Hoboken, New Jersey, 2016; 1 edition.

[Meadows and Moskowitz, 1996] Meadows, C., Moskowitz, I. S.: "Covert channels–a context-based view"; Proc. Information Hiding Workshop; volume 1174 of LNCS; Springer Berlin Heidelberg, 1996.

[Mileva and Panajotov, 2014] Mileva, A., Panajotov, B.: "Covert channels in TCP/IP protocol stack – extended version"; Central European Journal of Computer Science; 4 (2014), 2, 45–66.

[Murdoch and Danezis, 2005] Murdoch, S. J., Danezis, G.: "Low-cost traffic analysis of Tor"; Proceedings of IEEE Symposium on Security and Privacy; 183–195; 2005.

[Murdoch and Zielinski, 2004] Murdoch, S. J., Zielinski, P.: "Covert Channels for Collusion in Online Computer Games"; Proc. 6th Information Hiding Workshop; Springer, Berlin Heidelberg, 2004.

[Petitcolas et al., 1999] Petitcolas, F. A., Anderson, R. J., Kuhn, M. G.: "Information hiding—a survey"; Proc. of the IEEE; 87 (1999), 7, 1062–1078.

[Rios et al., 2012] Rios, R., Onieva, J., Lopez, J.: "HIDE_DHCP: Covert communications through network configuration messages"; D. Gritzalis, S. Furnell, M. Theoharidou, eds., Information Security and Privacy Research; volume 376 of IFIP Advances in Information and Communication Technology; 162–173; Springer, Berlin Heidelberg, 2012.

[Rowland, 1997] Rowland, C. H.: "Covert channels in the TCP/IP protocol suite"; First Monday; (1997).

[Sadeghi et al., 2012] Sadeghi, A.-R., Schulz, S., Varadharajan, V.: "The silence of the LANs: Efficient leakage resilience for IPsec VPNs"; Proc. ESORICS 2012; volume 7459 of LNCS; 253–270; 2012.

[Shen et al., 2005] Shen, J., Qing, S., Shen, Q., Li, L.: "Optimization of covert channel identification"; Proc. 3rd IEEE Int. Security in Storage Workshop (SISW'05); 95–108; IEEE, 2005.

[Simmons, 1984] Simmons, G. J.: Advances in Cryptology: Proceedings of Crypto 83; chapter The Prisoners' Problem and the Subliminal Channel, 51–67; Springer, US, Boston, MA, 1984.

[Tsiatsikas et al., 2015] Tsiatsikas, Z., Anagnostopoulos, M., Kambourakis, G., Lambrou, S., Geneiatakis, D.: "Hidden in plain sight. SDP-based covert channel for botnet communication"; S. Fischer-Hübner, C. Lambrinoudakis, J. López, eds., Trust, Privacy and Security in Digital Business; volume 9264 of LNCS; 48–59; Springer International Publishing, 2015.

[Tuptuk and Hailes, 2015] Tuptuk, N., Hailes, S.: "Covert channel attacks in pervasive computing"; 2015 IEEE International Conference on Pervasive Computing and Communications (PerCom); 236–242; 2015.

[Wendzel et al., 2012] Wendzel, S., Kahler, B., Rist, T.: "Covert channels and their prevention in building automation protocols: A prototype exemplified using BACnet"; Proc. IEEE GreenCom/iThings/CPSCom; 731–736; IEEE Computer Society, 2012.

[Wendzel and Keller, 2014] Wendzel, S., Keller, J.: "Hidden and under control: A survey and outlook on covert channel-internal control protocols"; Annals of Telecommunications (ANTE); 69 (2014), 7, 417–430.

[Wendzel and Palmer, 2015] Wendzel, S., Palmer, C.: "Creativity in mind: Evaluating and maintaining advances in network steganographic research"; Journal of Universal Computer Science (J.UCS); 21 (2015), 12, 1684–1705.

[Wendzel et al., 2014] Wendzel, S., Zwanger, V., Meier, M., Szlósarczyk, S.: "Envisioning smart building botnets."; Proc. Sicherheit 2014; volume 228 of LNI; 319–329; 2014.

[Wendzel et al., 2015] Wendzel, S., Zander, S., Fechner, B., Herdin, C.: "Pattern-based survey and categorization of network covert channel techniques"; ACM Computing Surveys; 47 (2015), 3, 50:1–50:26.

[White, 1989] White, S. R.: "Covert Distributed Processing with Computer Viruses"; Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology; 616–619; 1989.

[Wolf, 1989] Wolf, M.: "Covert channels in LAN protocols"; Proc. Local Area Network Security; volume 396 of LNCS; 89–101; Springer, 1989.

[Zander et al., 2007] Zander, S., Armitage, G., Branch, P. A.: "A Survey of Covert Channels and Countermeasures in Computer Network Protocols"; IEEE Communications Surveys and Tutorials; 9 (2007), 3, 44–57.

[Zander et al., 2008] Zander, S., Armitage, G., Branch, P. A.: "Covert Channels in Multiplayer First Person Shooter Online Games"; Proceedings of 33rd Annual IEEE Conference on Local Computer Networks (LCN); 2008.

[Zander et al., 2011] Zander, S., Armitage, G., Branch, P. A.: "Stealthier Inter-packet Timing Covert Channels"; IFIP Networking; 458–470; Springer, Berlin Heidelberg, 2011.

[Zander and Murdoch, 2008] Zander, S., Murdoch, S. J.: "An Improved Clock-skew Measurement Technique for Revealing Hidden Services"; Proceedings of Usenix Security; 2008.

[Zhiyong and Yong, 2009] Zhiyong, C., Yong, Z.: "Entropy based taxonomy of network convert channels"; Proc. 2nd Int. Conf. on Power Electronics and Intelligent Transportation System (PEITS); 451–455; 2009.