# Towards Practical Attacker Classification for Risk Analysis in Anonymous Communication

Andriy Panchenko and Lexi Pimenidis*

RWTH Aachen University,
Computer Science Department - Informatik IV,
Ahornstr. 55, D-52074 Aachen, Germany
{panchenko,lexi}@i4.informatik.rwth-aachen.de

**Abstract.** There are a number of attacker models in the area of anonymous communication. Most of them are either very simplified or pretty abstract - therefore difficult to generalize or even identify in real networks. While some papers distinct different attacker types, the usual approach is to present an anonymization technique and then to develop an attacker model for it in order to identify properties of the technique. Often such a model is abstract, unsystematic and it is not trivial to identify the exact threats for the end-user of the implemented system. This work follows another approach: we propose a classification of attacker types for the risk analysis and attacker modelling in anonymous communication independently of the concrete technique. The classes are designed in the way, that their meaning can be easily communicated to the end-users and management level. We claim that the use of this classification can lead to a more solid understanding of security provided by anonymizing networks, and therewith improve their development.
Finally, we will classify some well known techniques and security issues according to the proposal and thus show the practical relevance and applicability of the proposed classification.

**Keywords:** anonymous communication, attacker model, risk analysis.

## 1 Introduction

The primary goal in anonymity networks is to achieve sender anonymity, recipient anonymity, or both. The term *anonymity* is often defined as “the state of not being identifiable within a set of subjects, the anonymity set” [23]. This definition implicitly assumes a system state where there is either no attacker or the attacker is not successful. The task to estimate whether an attacker will be successful in breaking a real system or not is done as a part of the security evaluation or risk analysis. The most critical part of this is to properly define a realistic attacker model. If the chosen attacker model is too powerful - most of the protection techniques will necessarily fail, if the attacker model is too weak

* The authors are funded by the European Commission’s 6th Framework Program.

- the system will inevitably provide false and undesired means about protection level of its users.

Especially in the field of anonymous communication there exist a large number of attacker models. Most of these are describing the actual capabilities of the attacker, not considering the power needed in real life to achieve the proposed capabilities. A common example is the passive global observer. We agree that this model is needed and interesting for mathematical analysis, however end-users should be aware that theoretical results based on this analysis are not representative in real scenarios: an attacker having the capabilities to intercept traffic at the global scale can typically also easily alter and manipulate the traffic and, therewith invalidate the results of the analysis and protection vision of the end-user. From another perspective, it is not realistic for an average end-user to defend against an adversary that is capable of observing the whole worldwide network, because such a powerful adversary can make use of more efficient means in order to obtain the same information.

Only few systems for anonymous communication can be proven to be secure against very powerful attackers, given that the implementation is not faulty. A good example is a DC-network[4] which is known for its high security level. On the other hand, there are systems that provide security against weak attackers but fail against the strong ones. We call the resulting state *practical anonymity* (with regard to the thwarted attackers).

Most of the existing attacker models arised in the way, that at first an anonymization technique was presented and then the model was suggested in order to identify properties of the system. This often resulted in an unsystematic and abstract outcome of the attacker representation. We thus propose a new method for attacker characterization that is less abstract and more practical, therefore can be easily communicated to the end-users. The classification shall also provide a proposal for a simplistic measure of *quality of protection* in anonymous networks. In this specific work we will develop an attacker classification for anonymous communication systems and show an example of its application. At this point we want to clearly state, that the proposed classification is not strict: it is possible to classify in a different way. The same applies to the number of categories and the attacker classes they describe. Herewith we want to give an incentive to the community in the area of anonymous communications to think about realistic attacker models and link them to existing attacker descriptions rather than to replace existing classifications. This work is thus an *overview* on attacker models, their *classification* and *applicability* to current implementations.

### 1.1 Contribution

While it is theoretically feasible to defend against a nearly arbitrarily powerful attacker, it seems to us that such a system would be so slow and prone to denial of service attacks that the amount of users willing to use it would be very small. On the other hand, anonymizing networks are strongly in need for a large number of users to increase the size of anonymity set. Thus, it is not a good choice to defend against arbitrary powerful attackers. Therefore our work's aim is to allow the users to identify the attacker types they want to protect themselves from (*practical anonymity*). Having identified them, it is possible to look for techniques that would provide the desired degree of protection.

Our contribution to this topic is twofold:

1. We propose a classification for categorizing attacker types.
2. We show the applicability of the model with a short analysis of the strength of anonymizing techniques as well as some widely known attacks on them.

## 2 Related Works

To the best of our knowledge there is no paper dedicated explicitly to the attacker classification for anonymous communication, although all major papers in this domain define one or more attacker models. In this section we will give an overview of existing attacker models. Please note also that the majority of these papers primarily proposed a technique for anonymization and developed attacker models in order to distinguish their work from previous results (i.e. in order to identify properties of the new system). Thus these models are quite unspecific with regards to real systems.

In general it is assumed in literature on traffic analysis and anonymous communication that the attacker knows the infrastructure and strategies that are deployed[1]. This assumption is similar to those made in cryptology, where it's commonly assumed that an adversary knows the algorithms that are used.

Some attacker models in literature are quite simple. While this can be correct from a theoretical point of view, it arises difficulties in case of the risk estimation in the real world settings. In [29] the adversary is described as a participant that collects data from its interactions with other participants in the protocol and may share its data with other adversaries. [26] describes an attacker as some entity that does passive traffic analysis and receives the data by any mean that is available. These kinds of attacker models might be interesting in certain special cases but are difficult to generalize and identify in a real system: depending on the influences these attackers might have - they can be completely different entities. So, for example, they can be a secret service or standalone hacker, each being a different threat to the end-user. And the means that should be taken in order to provide the protection depend on the concrete threat entity.

A more general attacker categorization is given e.g. in [16]. Authors introduce three classes of attackers with increasing amount of power and capabilities, namely the *global external passive attacker*, the *passive attacker with sending capabilities* and the *active internal attacker*. While this distinction makes sense in the context of the paper [16] because it helps to show a difference between Mixmaster and Stop-and-Go-Mixes, the difference is marginal to virtually non-existing in real systems. We agree that a purely passive attacker is different from

[1] Since this is a commonly used assumption we intentionally omit a long list of references. See for example `http://www.freehaven.net/anonbib/`

an attacker that also participates in the network and is possibly detectable. On the other hand, it's quite unlikely that an attacker that has global access to network lines does *not* also have the possibility to inject messages. So, the first two attacker types wouldn't differ in their capabilities in real systems but rather in the decision whether to make use of all their features.

The same applies to [25], where the authors propose to split a *global active attacker* into the one that can only insert messages, and the one who can delay messages. If an attacker is able to deterministically delay messages in a real system, he will also be able to insert messages. On the other hand, if an attacker is able to insert messages in a system and observe their effect, he is most probably present on some of the system's lines and thus able to delay messages.

A more detailed list of adversaries can be found in [13], where four attacker types are listed: the *eavesdropper*, the *global eavesdropper*, a *passive adversary* and an *active adversary.* Again there will be little difference between e.g. the global eavesdropper and an global adversary in practice.

The most systematic listing of attacker types for theoretic modelling is found in [24], where Raymond introduces three dimensions of attackers:

**internal-external** Attackers can be distinguished on whether they are participants in the network or not.

**passive-active** Attackers can actively change the status of the network or remain passive.

**static-adaptive** Attackers can't change their resources once the attack has started or they can continue to build up their capabilities.

An additional dimension is given by Pfitzmann in [22]: active attackers can either limit their actions, follow the protocol and thus reduce the chance of being detected, or trade-off their stealth in favor to more powerful attacks by committing actions that are not part of a network's protocol.

The most realistic attacker model can be found in [28] where not only the method of attack is provided (ranging from an observer to a hostile user or a compromised network node) but also the extend of the attacker's influence on the network (i.e. whether it's a single node or some large parts of the network).

There is a large body of survey and classification material associated with risk analysis e.g. in [14, 1]. However, most of them define a set of skills, resources, etc. of an attacker, without binding these to real entities and not focusing on the practical representation.

## 3 Attacker Classification

The central idea of the proposed classification is to give an overview of possible common attackers in *real networks* and classify their strengths, weaknesses and capabilities. It is designated to help management level and end users to do their own personal risk analysis. A reason for this is that it is in general not an adequate choice to defend against the most powerful attacker that is possible. This is especially the issue in the area of anonymous communication where every added piece of protection reduces usability. Our classification can be used for end-users and in business applications to properly communicate the threat of certain known attacks. We will evaluate this estimation and show an example of its application in Section 4.

To achieve a better understanding of the adversary faced with, we propose to classify the formerly abstract attacker types (e.g. passive/active attackers) in a new grid. We still assume that an attacker has the knowledge about the infrastructure of the network and its algorithms. This is reasonable because all major contemporary implementations of anonymizing networks are either open source, well documented or can be downloaded and reverse-engineered. We also assume that an attacker knows about all major attacks that have been discussed and published in the literature.

Every attacker is typically also able to conduct passive as well as active attacks. However, we can neither estimate nor model a potential attacker's skills that go beyond the current state of published attacks[2]. But we might consider attacker class conditioned bounds in order to estimate the amount of required resources for a successful attack depending on the information theoretical calculations ([18]).

The attributes that distinct most real life attackers are the *amount of computational power* and the *amount of influence that the attacker has on the network*. The latter correlates most often with the number of nodes and links that the attacker controls or which are within his reach. Furthermore, computational capabilities are not as relevant in today's scenarios because cryptography is usually too strong to be broken by NGOs[3] and computational breaking of other primitives is only seldom preliminary to attack an anonymizing system.

### 3.1 Proposed Classification

We hereby propose the following classification of attacker types. These are not chosen by the network's infrastructure or topology, but rather as entities and social stereotypes participating in, affected by or being interested in a transaction between two parties using an anonymizing network. However this should not be regarded as a restriction, since it is unlikely that these entities and social stereotypes will be replaced or become irrelevant in the future, even if the underlying networks change.

It is assumed as an unconditional requirement that the user's terminal is under his own control and cannot be compromised by any other party. Otherwise it is trivial breaking the user's privacy and anonymity.

**0. External Party** The least powerful attacker has no control of any computer between the two communicating parties. While this kind of attackers are hardly worth being called so, there should be still taken measures to prevent them from gaining information.

[2] But we will consider it in the future work to keep the classification up-to-date.

[3] Non Governmental Organizations

Note that external parties can be very powerful, e.g. competitors in international trade, but unless further actions are taken to increase their influence on anonymizing networks, their influence is limited.

1. **Service Provider** This class of attacker stands for the user's communication partner. In some scenarios it is desirable to omit the disclosure of the sender's true identity. This attacker is technically bound to the receiving end of the communication and its close neighborhood.
2. **Local administration** This class of attackers can manipulate and read everything in the close network environment of the user[4]. These capabilities can be very powerful if the user blindly trusts all the transmitted and received data or does not care about protection. On the other hand, this attacker can be easily circumvented once the user is able to establish a secure connection to an outside trusted relay.
3. **ISP** The next powerful attacker has access to the significant larger area of computers in the vicinity of the user. The amount maybe so large that it can even be a non-negligible part of the whole global network. It is thus possible that a major number of relays on the way to the communication partner is within the reach of this class of attacker.
4. **Government** This adversary has the power to access not only a significant portion of all networks but also has large resources to fake services, break simpler encryption schemes[5] or prohibit access to specific services. This adversary might also take measures that violate existing laws to a certain extent and has the power to draw significant advantages from doing so.
5. **Secret Services** are forming the highest class of an adversary. They can be assumed to either have access to most parts of the global networks or they can get the access if they think it's necessary for their operation. This class of attacker is also not bounded by any kind of laws. It should be mentioned that the latter two types of attackers will probably not refrain from using non-technical methods to get information - this includes but is not limited to the physical capture of nodes. It is noteworthy that some countries deploy their Secret Services for industrial espionage.

We deliberately don't specify the classes of attackers in more detail, but rather leave them as categories that are intuitively understood by researchers as well as by the end-users. Note that these classes must not be strict: seamless transition is allowed.

For example, traditional law enforcement can be seen as an attacker split up on classes 4 to 5. Furthermore, Figure 1 gives some techniques for anonymous communication and specifies the highest class of attacker they protect against.

[4] Think of sniffing data, manipulated DNS-responses, man-in-the-middle attacks on TLS-secured connections, denial of access to anonymizing networks to force plain communication, and much more.

[5] The German Federal Office for Information Security factored the RSA-640 number in September 2005 and single-DES is known to be weak for decades: `http://www.rsasecurity.com/rsalabs/node.asp?id=2092`

[6] The Mixmaster network is too distributed for attackers of these classes.

| Technique | Defends against |
|---|---|
| Encrypted Communication | class 0 = External Party |
| Open Proxy Relay | class 1 = Service Provider |
| Encrypted Proxy Relay | class 2 = Local administration |
| JAP, Tor | depending on the configuration: class 2 to 3 |
| Mixmaster[6] | class 3 to class 4 |

**Fig. 1.** Example: Techniques and the attacker types they defend against

From our point of view, the minimum requirement for an anonymizing network should be to defeat from attackers of class 0 upwards to the class 2 or 3. While it seems currently to be infeasible and to some people not desirable to protect all end-users from attackers of class 4 and higher ones, we list these for completeness reasons and because there are users that want to defend themselves from this kind of adversaries.

## 4 Application Example

In this section we will at first briefly discuss common approaches for attacks (further called *security issues*) providing for each of them the attacker class at least needed in order to efficiently execute the attack. Afterwards, we will give an overview on the strengths and weaknesses of existing or widely analyzed anonymizing networks. Furthermore, the maximum class of attacker that can be defeated by the corresponding technique will be provided according to the new attacker classification.

We clearly state that the following classification is done on the basis of our experience with anonymizing networks in theory as well as in practice. It is not to space out other possibilities to do the categorization in a completely different way. It is also well possible that extreme user behavior, future attacks or methods will change the level of protection. Thus, we expect a need to update the following lists in the future since they are done from today's perspective.

Furthermore, we distinguish three types of users depending on their behavior: *cautious*, *average*, and *unwary*. However, we intentionally do not describe these behaviors precise. Average behavior is achieved as it is understood in the common sense, e.g. through the usual web surfing. Under cautious users we understand those, that decide whether to use a specified service under concrete circumstances and send only a very limited number of messages. Unwary users do not care much about what are they doing. Further in this paper we will only consider *average* users. In general we expect cautious users to be able to protected themselves at least against attackers of one class ahead, while unwary users can be identified with much less effort.

Due to place restrictions we will not be able to explain all issues and techniques in detail. We thus rely on the reader to be familiar with the handled techniques and attacks, or follow up the referenced documents.

### 4.1 Security Issues

This section will provide a short overview on well known and analyzed security issues for anonymous communication systems. We gill give a short introduction and specify the class of attacker that is likely to draw significant advantage from the corresponding security issue. Note that most issues can be exploited in theory by an attacker with less power than given. But this typically relies upon fractional probabilities or pathological network structures.

We will use the following notation to describe the severeness of a single issue: after its main description we will add a number in brackets. The number denotes the class of attacker that is at least needed in order to *efficiently* mount this attack. By this we refer to the situation where an attacker of the concrete class succeeds in breaking the system (in order to de-anonymize a single average user) with some non-negligible probability.

It is an inherent property of the classification that several different attacks can be mounted by a single class of attacker. This is due to the fact that our work focuses on practical attacker representation, instead of fine-grained theoretical models that are needed to distinguish system properties of different techniques.

**Denial of Service (0)** A network should be as resistant as possible against (distributed) denial of service attacks and selfish nodes. The difficulty of this attack depends on the implementation characteristics of the service but can be as simple as attacking a couple of directory servers. If the anonymizing network is dis-functional due to a DoS-attack, some users switch to unprotected communication and thus give away the information they wanted to protect.

**Hacking into a Node (0)** This security issue deals with an active intrusion into the targeted node, possibly by means of security lacks in some services offered by the host. Having gained the access, the invader can overtake the control over the node (e.g. install spy software, etc.). This issue is of the great importance especially in anonymous communication systems because in most cases the majority of nodes is using the same software. Such a single vulnerability in this software can give an attacker the control over large parts of the network.

**Analyze Application Layer Data (1)** This attack analyzes any data that is transmitted from the client to the service provider without being changed, i.e. in the network layer above the anonymization layer. In most cases this refers to the data that is provided by the user through e.g. filling out a web form but can also include an analysis of HTTP- or email-headers that are transfered without modification. A good overview is given in [5].

**Packet Counting and Delay Attacks (2)** Packet Counting attacks work quite well on a small scale e.g. when the user is surfing the web [12]. However there are no studies that provide this analysis for current anonymity systems and it seems to be infeasible to apply this attack on other type of anonymizing networks like e.g. remailers. Additionally, packet counting can be thwarted by the use of dummy traffic.

On the other hand, delay attacks can be used to minimize the effect of dummy traffic and ease packet counting. In general, every attacker that is able to count the packets also has the possibility to delay them. However, this is not always true (e.g. in case of the shared medium). While delaying rises the chance for success, the attacker runs into the risk of being detectable.

**End-to-End Traffic Analysis (3)** Attackers that control a non-trivial part of the global network have a non-neglible probability of either controlling or observing a user's first node in the route and the exit point. Thus they are able to do end-to-end analysis.

$n - 1$ **Attacks (4)** are also sometimes called Sybil attacks [8]. Depending on the system, it is not always necessary to deploy $n - 1$ decoy nodes, it is rather sometimes sufficient to operate two nodes and wait until they happen to be introductory node, respectively exit point at the same time. In the Tor-network [7], this would suffice to break the system – of course, deploying more nodes raises the probability of the success. Thus, if an attacker of class 4 would like to do so, he would have the resources to run such an attack. Unfortunately, these attacks can only be thwarted by authentication schemes that are currently not solvable or deployable in practical systems.

**Break Mixing (4)** The same amount of influence on the network (i.e. observing the majority of nodes) is also needed to successfully mount a traffic analysis like described in [6, 17][7].

**Replay Attacks (5)** In general, replay attacks are next to impossible to carry out against current implementations like e.g. ANON [3], Tor [7], and Mixmaster [19]. Thus, we grade the difficulty to the level where at least some cryptographic mechanisms have to be broken in order to replay messages. Since there are typically more efficient ways to learn the same information, we doubt that these kind of attacks can be seen in real systems.

### 4.2 Anonymizing Techniques

In this section we will consider the anonymity provided by several deployed anonymization techniques. We will specify the level of protection that is provided for an *average user* against known attacks. As one input we used the previous section 4.1 and weighted the classification according to the probability of success for each security issue with respect to a certain technique. But we also had to take implementation specific details into account as well as general weaknesses of the techniques.

In the following we will use a single number as notation to describe the maximum class of attackers that can be defeated by a certain technique.

**Ants (2)** The anonymizing networks Ants [2] and Mute [21] use ant-routing [11] to achieve anonymity. By their own judgement it can be broken under circumstances if the user is connected only to the nodes of the attacker. Additionally, there is no proof that the algorithms can't be degraded with an

[7] See also section 4.2.

attack similar to the one in [20]. The provided anonymity is at the level 2, whether it is also provided on the 3rd one it is not proven and therefore not known yet.

**NDM, Onion Routing (3)** NDM [9] and Onion Routing [7] can be defeated by end-to-end analysis, sybil attacks, packet counting attacks, and timing attacks [20]. While the risk of the first two can be thwarted and handled to a certain extend in the client's software or by cautious behavior, the latter two problems are more serious. On the other hand, it is still to be shown that the packet counting attacks can be successful in real networks with a high probability, and even if they are, they could be avoided with a software update (e.g. producing dummy traffic). Thus, we rate the protection of the average user to 3.

**Mixing (3-4)** Mixing can be added to Onion-routing in different flavors: fixed size batches, timed mixing, combinations of both [25], or stop-and-go mixes [15]. While the security gain by mixing is possibly questionable [6, 17], it can still provide strong anonymity in open environments if users refrain from sending too much information in a single time interval [18].

We give no security level for Hash-Routing [27, 10] and DC-nets [4] because there are no implementations that have a relevant user-base. Missing this, it is impossible to give a rating of their practical level of security.

## 5 Conclusion

There are currently no widely known implementation of anonymization network that would provide protection against arbitrary strong attackers. Thus, existing and commonly used attacker models, like e.g. global passive observer, are too strong in order to facilitate fine-grained analysis of todays practical systems. Such model is definitely needed for design and property evaluation of networks with strong anonymity properties. Researchers and end users, however, are also in need of a classification that allows differentiation for the methods that are used in today's implementations.

The proposed classification itself does not ease the risk analysis per se as it gives only the categories of attacker classes. The categorization of the difficulty of attacks or the protection provided by each single technique and its implementations is still subject to "manual" analysis. Hereby we mean, that it can only be used as a reference model to determine from which type of attacker the protection can be achieved. Even here it is possible that opinions differ and different people would classify in a different manner than we did.

We are aware that the classification has no analytical background, however it would be cumbersome and difficult to model real world entities. Additionally it seems currently computational infeasible to analytically proof the security provided by any implementation of theoretical techniques. Thus we had to rely on practical experience and not analytical arguments in favor of our criteria.

In this paper we proposed a classification of attacker types with regard to the attacker's influence on the network, the computational power and physical capabilities. It should not be seen as restriction since it is unlikely that the proposed entities and social stereotypes will be replaced or become irrelevant in the future, even if the underlying networks change. Furthermore, the provided classification can be easily communicated to the end-users and management level.

We hope that this document gives incentive to the community of researchers in the area of anonymous communication to think also about linking their theoretical models to realistic attackers and thus contributes to the discussion about measuring the quality of protection.

We'd also like to contribute with this work in future versions to classifications of attackers not only in anonymous communication systems but in the general field of IT-security.

## References

1. Attacker Classification to Aid Targeting Critical Systems for Threat Modelling and Security Review. http://www.rockyh.net/papers/AttackerClassification.pdf, 2005. visited July 2006.
2. ANTS File Sharing. http://antsp2p.sourceforge.net/, 2005. visited Oct 2005.
3. O. Berthold, H. Federrath, and S. Köpsell. Web MIXes: A system for anonymous and unobservable Internet access. In H. Federrath, editor, *Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability*, pages 115–129. Springer-Verlag, LNCS 2009, July 2000.
4. D. L. Chaum. The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. *Journal of Cryptology*, (1):65 – 75, 1988.
5. R. Clayton, G. Danezis, and M. G. Kuhn. Real world patterns of failure in anonymity systems. In I. S. Moskowitz, editor, *Proceedings of Information Hiding Workshop (IH 2001)*, pages 230–244. Springer-Verlag, LNCS 2137, April 2001.
6. G. Danezis. Statistical disclosure attacks: Traffic confirmation in open environments. In Gritzalis, Vimercati, Samarati, and Katsikas, editors, *Proceedings of Security and Privacy in the Age of Uncertainty, (SEC2003)*, pages 421–426, Athens, May 2003. IFIP TC11, Kluwer.
7. R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium*, 2004.
8. J. Douceur. The Sybil Attack. In *Proceedings of the 1st International Peer To Peer Systems Workshop (IPTPS 2002)*, March 2002.
9. A. Fasbender, D. Kesdogan, and O. Kubitz. Analysis of security and privacy in mobile ip. In *Mobile IP, 4th International Conference on Telecommunication Systems Modeling and Analysis*. Nashville, March 1996.
10. S. Goel, M. Robson, M. Polte, and E. G. Sirer. Herbivore: A Scalable and Efficient Protocol for Anonymous Communication. Technical Report 2003-1890, Cornell University, Ithaca, NY, February 2003.
11. M. Günes and O. Spaniol. Ant-routing-algorithm for mobile multi-hop ad-hoc networks. In *Network control and engineering for Qos, security and mobility II, ISBN:1-4020-7616-9*, pages 120 – 138. Kluwer Academic Publishers, Norwell, MA, USA, 2003.
12. A. Hintz. Fingerprinting websites using traffic analysis. In R. Dingledine and P. Syverson, editors, *Proceedings of Privacy Enhancing Technologies workshop (PET 2002)*. Springer-Verlag, LNCS 2482, April 2002.

13. A. Hirt, M. J. Jacobson, and C. Williamson. Survey and analysis of anonymous communication schemes. Submitted to ACM Computing Surveys, Department of Computer Science, University of Calgary, December 2003.
14. J. D. Howard. *An Analysis Of Security Incidents On The Internet 1989-1995*. PhD thesis, Carnegie Mellon University, 1997.
15. D. Kesdogan, J. Egner, and R. Büschkes. Stop-and-Go-Mixes Providing Anonymity in an Open System. In D. Aucsmith, editor, *Information Hiding 98 - Second International Workshop*, pages 83 – 98. Springer Verlag, 1998.
16. D. Kesdogan and C. Palmer. The past present and future of network anonymity. Network Security, Special Issue of Computer Communications Journal, Elsevier, 2003.
17. D. Kesdogan and L. Pimenidis. The Hitting Set Attack on Anonymity Protocols. In *Proceedings of Information Hiding, 7th International Workshop*. Springer Verlag, 2004.
18. D. Kesdogan and L. Pimenidis. The Lower Bound of Attacks on Anonymity Systems – A Unicity Distance Approach. In *Proceedings of 1st Workshop on Quality of Protection, Colocated at ESORICS*, Milan, Italy, September 2005. LNCS.
19. U. Möller, L. Cottrell, P. Palfrader, and L. Sassaman. Mixmaster Protocol — Version 2. Draft, July 2003.
20. S. J. Murdoch and G. Danezis. Low-cost Traffic Analysis of Tor. Oakland, California, USA, May 2005. IEEE Symposium on Security and Privacy.
21. MUTE File Sharing. http://mute-net.sourceforge.net/, 2005. visited Oct 2005.
22. A. Pfitzmann. Security in IT Networks: Multilateral Security in Distributed and by Distributed Systems, October 2004. Script for the lectures "Security and Cryptography I+II".
23. A. Pfitzmann and M. Köhntopp. Anonymity, unobservability, and pseudonymity: A proposal for terminology. Draft, version 0.23, August 2005.
24. J.-F. Raymond. Traffic analysis: Protocols, attacks, design issues and open problems. In H. Federrath, editor, *Designing Privacy Enhancing Technologies: Proceedings of International Workshop on Design Issues in Anonymity and Unobservability*, volume 2009 of *LNCS*, pages 10–29. Springer-Verlag, 2001.
25. A. Serjantov, R. Dingledine, and P. Syverson. From a trickle to a flood: Active attacks on several mix types. In F. Petitcolas, editor, *Proceedings of Information Hiding Workshop (IH 2002)*. Springer-Verlag, LNCS 2578, October 2002.
26. A. Serjantov and P. Sewell. Passive attack analysis for connection-based anonymity systems. In *Proceedings of ESORICS 2003: European Symposium on Research in Computer Security (Gjøvik), LNCS 2808*, pages 116–131, Oct. 2003.
27. R. Sherwood, B. Bhattacharjee, and A. Srinivasan. P5: A protocol for scalable anonymous communication. In *Proceedings of the 2002 IEEE Symposium on Security and Privacy*, May 2002.
28. P. Syverson, G. Tsudik, M. Reed, and C. Landwehr. Towards an Analysis of Onion Routing Security. In H. Federrath, editor, *Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability*, pages 96–114. Springer-Verlag, LNCS 2009, July 2000.
29. M. Wright, M. Adler, B. N. Levine, and C. Shields. An analysis of the degradation of anonymous protocols. In *Proceedings of the Network and Distributed Security Symposium - NDSS '02*. IEEE, February 2002.