Anonymous Routing

Almir Aljic
KTH Royal Institute of Technology
aljica@kth.se

Hovig Manjikian
KTH Royal Institute of Technology
hoffek@kth.se

Simon J. Binyamin
KTH Royal Institute of Technology
binyamin@kth.se

Telo Johar
KTH Royal Institute of Technology
telo@kth.se

Abstract

Originally, the Internet was not designed for anonymity, but for accountability. Despite that, a multitude of anonymous routing networks, have been developed over the years, whose main purpose is to facilitate anonymous communication online. The most famous anonymous routing network, the Tor network, uses a protocol known as onion routing, which was developed by the United States Naval Research Laboratory in the mid-1990s, and is today widely used by a wide variety of individuals, including political dissidents in oppressive regimes, journalists, whistleblowers, military personnel and privacy-conscious Internet users.

Since then, many other kinds of anonymous routing protocols and systems were developed and implemented, some with different paradigms and principles, such as the I2P network, which is a peer-to-peer mix network that uses garlic routing. The ultimate aim of each such anonymous routing network is to offer anonymity to its clients, but each of them has its own way of achieving this functionality. By analysing the paradigms, the systems and their implementations, one can make intrinsic comparisons and evaluations to determine which ones are more or less suitable for different scenarios. Ultimately, each AR network's viability is dependent on the particular use case in question. AR also requires great sacrifices in terms of latency in the network. Given the current architectures, there is no way to achieve meaningful privacy without introducing significant delays in the network.

Keywords anonymous routing, onion routing, garlic routing, clearnet, dark-net, peer-to-peer networks

1 Introduction

1.1 Background

A lot of information can be collected from users of the Internet, even though the data that is being sent is encrypted [19]. Preserving privacy entails not only concealing the content of messages but also concealing who is conversing with whom. Packets in a packet-switched network feature a header that exposes the source and destination of the packet, as well as a payload that contains the data. The header, which exposes the source and destination of the packet, must be accessible to the network and hence to network observers. Akin to a physical envelope, the use of cryptography within a packet-switched network hides the contents of messages being delivered but can disclose who is talking to whom and how frequently [14]. Not using any techniques to obscure the routing means that many entities will be able to know the communications relations of the user, such as ISPs, governments and many other entities.

There can be many reasons for wanting to be anonymous on the Internet. Ordinary Internet users may use it to access services and websites prohibited by ISPs or to participate in chat rooms for victims of various forms of abuse. For Internet users in oppressive regimes, it can be used to communicate with other freedom seekers, spread information, and avoid censorship [3]. Privacy from entities that wish to monitor online activity is also important for intelligence services, who have developed techniques in order to protect online communications [21].

1.2 Defensive Measures

Since the invention of the World Wide Web, Internet users have prioritised security and privacy from those who seek to monitor their online activities [21]. Thus, different techniques have been developed in order to defend Internet users.

One way of achieving privacy is the use of a proxy at the application layer, or at the communication layer. However, by using a single proxy, the provider of the proxy will learn about all the communications relations of the user. Even if all communication to the proxy is encrypted, an eavesdropper will still be able to use traffic analysis to be able to deduce who is communicating with whom [15].

This issue may be solved by changing the proxy after a certain amount of time, which is frequently accomplished through the use of open proxies. An open proxy is one that anyone without any access control can use. Such proxies are typically the consequence of proxy operators' setup errors. However, the intended use of such proxies is usually not to provide anonymity [15]. Not being careful with the selection may lead to the exposure of identifying information, such as the IP address via the X-Forwarded-For HTTP header element [15].

1.3 Anonymous Routing

One solution which does not have the previously mentioned weaknesses is anonymous routing (AR), which will be examined further in this report. It focuses on the hiding of the identities of various components or parts of a network communication [22]. AR conceals the true identity of the traffic by separating identification from routing and prevents traffic analysis [19]. It can therefore be defined as a technique that makes the identities and location information of parties in communications anonymous [23]. However, an eavesdropper may still observe if a user has sent or received a message. What AR provides is a strong degree of unlinkability [23].

2 Explaining Anonymous Routing

2.1 Goal

The focus of AR is to prevent attackers from linking communication partners or linking numerous communications to or from a single user [13]. This is done by creating an infrastructure that:

complicates traffic analysis, separates identification from routing, and supports many different applications [19].

2.2 Application

AR hides the sender and/or receiver's identity by concentrating on the routing paths. The user's identity is hidden even from the system itself by using different random routing pathways [1].

Chaum's Mix-Net design [4] is the foundation of modern AR techniques. By encapsulating messages in layers of public-key cryptography and relaying them over a route made up of "mixes", Chaum suggested that it will conceal the correspondence between sender and recipient. Before transmitting messages further, each mix decrypts, delays, and reorders them [13].

This report will examine two of the modern techniques, the Tor Project that utilises onion routing (OR), and I2P (Invisible Internet Project) that utilises garlic routing. Following Chaum, relay-based anonymity ideas have diverged into two different foci. One category focuses on increased anonymity at the expense of comparably large and variable latencies. These high-latency networks are resistant to strong global adversaries as a result, but introduce too much lag for interactive tasks such as web surfing, Internet chat, or SSH connections [13]. The other category, to which Tor and I2P belong, focuses is on low-latency networks and therefore focuses on anonymising interactive web traffic.

3 Implementation Comparison: Tor vs. I2P

3.1 The Method

Anonymous routing can be achieved by different methods. Tor uses onion routing which is a bidirectional anonymous socket connection [20] that can be used for both connection-based and connectionless traffic. In this approach, a user establishes the socket via an onion routing proxy where a data structure called onion is created and sent via the Tor network. The onion object has multiple RSA-encrypted layers where each layer reveals a single hop in the network and can be decrypted by a single router. Thus, an onion router can only identify the previous and next routers which will make it very difficult for an adversary to learn the source and the ultimate destination.

Tor aims to protect the user from deanonymisation even when compromised relays co-operate. As long as there is at least one honest onion router, anonymisation is preserved. That is an anonymous connection is as strong as its strongest link [20].

I2P on the other hand builds a new layer on top of the existing network and transport layers. The communication in this network is unidirectional, i.e. there are two separate paths one for the outbound-traffic and one for the inbound-traffic [7]. A data structure called a garlic is sent via the network. Each clove in the garlic implements layers of encryption similar to the Tor approach, thus each node will only know the node before and the node after. However, unlike the onion in Tor, an I2P garlic can contain multiple cloves which represent different messages [6].

The essential parts of both methods are the cryptographic techniques and algorithms. Different cryptographic techniques are used for different types of packets and data structures. The techniques include 2048bit ElGamal encryption, 256bit AES in CBC mode with PKCS5 padding, 1024bit DSA signatures, SHA256 hashes, 2048bit Diffie-Hellman negotiated connections with station to station authentication, and ElGamal / AES+SessionTag. [7, 12]

3.2 The Architecture

Tor uses the conventional server-client architecture with proxies in between that manages the entry and exit to the Tor network [20]. In the Tor network, a node can be either a user or a relay. Relays need to fulfil many technical requirements, such as having a high-speed connection and a large bandwidth. Each onion relay will be connected to multiple onion relays using keyed longstanding connections. When a user wants to establish an anonymous connection a subset of these onion relays will be chosen. The chosen relays will then make a sequence of relays which will be called a circuit. A circuit will be defined at the beginning of the connection setup, after that the path will remain the same as long as the user does not actively choose to change it. During this step, the public keys of the onion routers involved in the connection will be acquired and used in making the onion data-structure objects.

I2P uses a distributed peer to peer architecture. Each node will establish multiple unidirectional paths in the network. These paths are called *tunnels* which will be continuously changed over time [2]. Since the tunnels are unidirectional there will be two types of tunnels, outbound tunnels and inbound tunnels[7, 9]. This means that a response message takes a different path than the request message. To send a message the sender needs to know the router to target with outbound tunnel and the receiver's inbound tunnel. The information about the inbound tunnel of a node needs to be distributed so that the node will be reachable by others. Since the tunnels are temporary and will change periodically this information set is called a *LeaseSet*. These leases will be found in a distributed network database called *netDb*.

One major difference between Tor and I2P architecture is that Tor was designed originally as a proxy to access regular websites and internet services anonymously. With regular websites and services, we mean all kinds of services that can be accessed on the clear-net (the publicly accessible internet). I2P on the other hand was designed as a hidden network, a dark-net, where hidden services reside. This means that I2P cannot be used directly to access clear-net services. Nevertheless, Tor does support hidden services (onion services) that reside within the tor network [12].

3.3 The data at transit

In Tor, the onion data-structure objects that arrive at an onion router will be placed in different queues. However, the queues will not be FIFO queues so that traffic analysis becomes more difficult [20]. The order of a queue will be an arbitrary one where fairness is guaranteed. It is also guaranteed that the order of onion objects within a single anonymous connection is preserved.

On the other hand, a node in the I2P network will place the garlic data structure on a different tunnel each a new garlic arrives. This is possible since each node will have multiple inbound- and outbound-tunnels which keep changing over time. Additionally, since each node in the network is a sender, receiver and router many packets arrive and leave the node making it very difficult for an adversary to know which packets the node is sending, receiving or forwarding [2].

3.4 The implementation

Both Tor and I2P are open-source projects. The Tor project is distributed under a BSD 3-clause license and Mozilla public license. The project is developed by a nonprofit organisation based in Seattle, USA [10]. I2P is also distributed under different licenses for different parts. The licenses are Public domain, BSD, GPL, and MIT. Tor is developed by a nonprofit organisation based in Seattle. The funding of the organisation is mainly by the US government but the Swedish government also contributes via Sida (Swedish International Development Cooperation Agency) [11]. Unlike the Tor project, I2P has no single organisation behind it. I2P is a community project where multiple developers voluntarily contribute to the project. Most of the developers are only known under pseudonyms [5].

3.5 The trade-offs

Both Tor and I2P suffer from performance issues in terms of latency. This is mostly due to the introduced multiple hops between physically far-apart nodes. The encryption and decryption of the different layers of the onion/garlic object plus the algorithms used for key-exchange will also introduce some latency to the connection. Furthermore, the overhead required for establishing/tearing-down paths on the network is another burden that also contributes to decreasing the performance.

Traffic congestion is another issue that both the implementations suffer from. The main reason for this is usually a node on the path with a low-speed connection that reduces the throughput of the entire path. The padding introduced to the packets for protecting against traffic analysis is another factor that contributes to more traffic in the network and thus a higher risk for congestion.

Both Tor and I2P do not consider large scale attacks that require a huge amount of resources. This creates the trade-off of unprotected privacy against major actors. For example, both Tor and I2P will not manage a large scale attack like brute force attacks where an adversary monitors all the connections between nodes and then sends a large 5GB file to a destination. This adversary can then eliminate all the nodes that did not receive 5GB of data and thus will discover the tunnels and circuits in the network. [8]

There are also implementation specific trade-offs that might not be common for anonymous routing in general. As mentioned earlier the Tor project is developed by a non-profit organisation that is funded by different organisations. There is a risk that sponsors might pressure the organisation to implement or not implement certain codes which might lead to the deanonymisation of some or all users. In the I2P case, even though there are no sponsors and the developers are inaccessible the project is still not trustable. Since the developers are anonymous it is very difficult to know what are their real intentions are. It might be that some of the developers are malicious and will plant some backdoor in the system which will ultimately lead to the deanonymisation of the user. Of course, good code reviewing might minimise this problem but it will defiantly not eliminate it. In short, since both approaches are difficult to implement locally and needs a third party that implements and manages the network, a major trade-off will be that our privacy will rely on these third-party developers.

4 Assumptions About Anonymous Routing (TOR/I2P), Its Users and Potential Adversaries

4.1 The System

The Internet is one large, overarching network of sub-networks, which in unison cover a vast geographical area across the world. This system of integrated sub-networks was never designed with anonymity in mind, but accountability [17].

As a result, over the years, networking systems were built on top of existing Internet protocols to enable anonymous communication. This inevitably creates separation and to varying degrees inaccessibility between the anonymised network (such as TOR and I2P), which is often referred to as a darknet, and the clearnet, which can be considered to be "the rest of the Internet". In practice, this entails having specific exit nodes within the anonymised network, whose task it is to act as a proxy for forwarding anonymised requests originating from within the darknet.

Any system of anonymised communication is dependent on having a large, partially homogenous but also fairly heterogeneous (as to facilitate the introduction of new anonymous users) anonymous set of users, also known as the *anonymity set* [18]. That said, the larger the user base of an anonymising network, the more likely preservation of anonymity is. In mathematical terms, this may be formulated as that the anonymity delta approaches zero.

It is also of importance to ensure that the route which traffic takes is not always consistent - the reasons for this have and will be discussed in other parts of this report, but it does require an additional mention here: if a certain set of users within an anonymity set always use the same route when communicating within the anonymous routing network, then that anonymity set is actually reduced to that certain set of users, i.e. the possible users that could be operating within that connection are reduced, which ultimately makes them easier to identify.

4.2 Users

Users of anonymous routing networks can vary from political dissidents or journalists operating in oppressive regimes, to military personnel, to normal Internet users desiring to protect their personal information from mass-scale data collection systems and advertisers and from hackers operating maliciously, in an attempt to gather sensitive information on the network's users.[17].

Oppressive regimes can have massive firewalls that cover the entire nation - a national firewall. This ultimately disables an individual connecting to the Internet from that nation to connect to the outside world. Internet Service Providers (ISPs) in these countries essentially prevent users from accessing services with IP addresses belonging to external countries, much like a blacklist. For example, one may have journalists stationed in such countries, who must publish their work, which requires direct communication with their colleagues and servers where they work.

Political dissidents and whistleblowers require strict anonymous communication. As a political dissident, one risks political and legal persecution and prosecution if one's identity is revealed - and similarly, being a whistleblower is not exactly legal either. One great example of this is Edward Snowden, whose work has largely been considered a significant threat to national security despite his meticulous and careful methodology in unveiling information about mass-scale, government surveillance systems that infringe upon U.S. citizens' privacy rights [16].

To reveal the information that he did, Snowden contacted American journalists that had published PGP keys, which enable end-to-end, fully secure encrypted communication. However, this was not enough. He also needed a way to send this information anonymously, and this is where he used the TOR network (in particular, he used an operating system known as Tails - an OS that only boots in the RAM of the computer via an external USB stick, which prevents cold boot attacks and other memory-related attacks, and also routes all traffic through the TOR network). Had Snowden not cared for his privacy and anonymity, it is likely that he would never have had enough time to leave U.S. soil before being apprehended and put on trial for treason.

Additionally, there are ordinary Internet users that are interested in preserving their privacy and anonymity online, who may wish to use AR networks. There can be a myriad of reasons many, but one common reason is that advertisers collect a lot of information about the users. By not signing up to mainstream services, and by not using mainstream browsers and direct connections, one can minimise one's digital footprint, which ultimately serves to preserve one's online identity and online habits. This can be beneficial for many reasons, and especially for individuals who have a certain level of social exposure, such as politicians.

Distributing an individual politician's Google search history could have a lot of monetary gains. If that politician wishes to minimise the risk and potential impact of being a victim of a privacy-related attack aimed at disrupting his or her political credibility, using an AR network and securing one's online communications and online habits may be an efficient way of fully utilising the wonders of the Internet, while simultaneously not worrying about potential future implications that may come from honestly and uninhibitedly searching the Internet.

4.3 Adversaries

Adversaries with global capabilities can monitor traffic entering the anonymous network and traffic leaving it, and correlate them. This is known as traffic analysis and is a significant threat to the anonymity of users of darknets [17]. These sorts of adversaries have highly technically robust systems and expertise at their disposal, which enables them to perform large-scale attacks against anonymising networks, given enough time and resources. Such attacks are most commonly directed at high-value targets that may be using darknets for their communications, such as terrorists and other national or international criminal leagues, who may facilitate the sale of illicit substances in the form of drugs, inappropriate and illegal sexual content and so on.

Nevertheless, traffic analysis is a task that requires a lot of resources and continuous monitoring, which can be costly in the long run. Besides, analysing *all* traffic entering and leaving the darknet is undoubtedly an excessive amount of information gathered for capturing the few communications that may occur by the aforementioned targets. As a result, police operations targeting major marketplaces that facilitate the sale and consumption of illicit substances and hidden services that distribute sexually inappropriate content have instead been directly targeted. The way this has been done is by locating the servers where the hidden services are hosted. This is not always an easy task, but there are ways of doing it.

One way of doing it is through infiltration, i.e. exploiting the human factor. In practice, law enforcement agents act as knowledgeable individuals and gain the trust of others on forum boards related to these illegal hidden services, and are eventually promoted to administrators. This was part of how the first Silk Road, a major drug marketplace on the TOR network, was taken down. After becoming administrators, retrieving technical information related to the hidden service, such as where it is hosted etc, could perhaps eventually be had. Another way of doing it is by conducting penetration tests against the hidden service to locate vulnerabilities. If, for instance, the hidden service is using a CMS plugin of any kind, then finding vulnerabilities related to that plugin and exploiting them could be one way of uncovering additional information about the hidden service. These are just two examples among many other ways of exploiting the inevitable security weaknesses inherent to all computer systems.

The goal, most of the time, is to somehow make the hidden service establish a direct connection (outside of the darknet) to an external server owned by the adversary attempting to exploit the hidden service. These goals are however not static. For instance, another equally reasonable goal could be to insert a static page element or plugin that causes users' browsers to automatically (and unknowingly) make a direct connection to the external server owned by the adversary, which would ultimately unveil their identities.

4.4 Final Words

With that said, there are different motivations and reasons why and how an adversary might wish to attack an anonymous routing network. Some adversaries may wish to uncover the identities of individual users for the sake of blackmail. This can be done in many ways but hacking personal computers by deploying malware to hidden services, which infect the computer upon being visited, is one example. There are countless more, but the related strategies share commonality with the methods described previously.

Ultimately, there is no one way of doing things here. Anyone can have a reason to use an anonymous routing network, at any time - it is just so that certain individuals are more likely to do so (such as journalists, political dissidents, military personnel, privacy-oriented private individuals and so on). There is always a trade-off between usability and security and privacy, so depending on what one wishes to do, using an anonymous routing network can be both appropriate and inappropriate. It depends on the circumstances.

Large-scale adversaries can have a huge impact on the anonymity of individual users, but the trade-offs are questionable: is it worth all that time and resources to gather all the information and data that enters and leaves an AR network, and on top of that, is it worth analysing it at all? Once again, it depends. If the goal is to subdue a terrorist plot, then it might be worth it. If the goal is to apprehend individuals engaged in the distribution of illicit substances, then other means may be more appropriate, such as penetration testing and other exploits.

5 Conclusion

Anonymous routing is a great tool for achieving a good level of anonymity and thus protect the user privacy. However anonymous routing is not a perfect tool and the question whether the degree of anonymity provided by implementations like Tor or I2P is good enough is difficult. Apart from that, AR will also require great sacrifices in terms of latency in the network. Given the current architectures there is no way to achieve meaningful privacy without introducing significant delays in the network. More specialised hardware for encryption and decryption might cut down some latency and improve the network performance, but problems like hops between physically far routers and path setup overhead are more difficult problems to overcome.

Although Anonymous routing has been around for many years now, there are still many problems and weaknesses in the available technologies which needs to be addressed. Large scale attacks, development attacks, and cryptographic attacks are among other problems that threat the anonymity and privacy of a user.

Nevertheless, there are many benefits that anonymous routing is offering in its current format. Whistle-blowers who just simply want to inform a newspaper or a journalist about a problem can with a good degree of safety use Tor or I2P. It is also an important tool for citizens in an oppressive regime. Privacy conscious users will also enjoy the benefits of anonymous routing with relatively very little risk.

References

[1] Afzaal Ali, Maria Khan, Muhammad Saddique, Umar Pirzada, Muhammad Zohaib, Imran Ahmad, and Narayan Debnath. 2016. TOR vs I2P: A comparative study. In *2016 IEEE International Conference on Industrial Technology (ICIT)*. IEEE, 1748–1751.

[2] Felipe Astolfi, Jelger Kroese, and Jeroen Van Oorschot. 2015. I2p-the invisible internet project. *Leiden University Web Technology Report* (2015).

[3] Abdelberi Chaabane, Pere Manils, and Mohamed Ali Kaafar. 2010. Digging into anonymous traffic: A deep analysis of the tor anonymizing network. In *2010 fourth international conference on network and system security*. IEEE, 167–174.

[4] David L Chaum. 1981. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM* 24, 2 (1981), 84–90.

[5] I2P developers. 2021. *Contact*. https://geti2p.net/en/docs/api/i2ptunnel Accessed: 2021-10-13.

[6] I2P developers. 2021. *Garlic Routing*. https://geti2p.net/en/docs/how/garlic-routing Accessed: 2021-10-13.

[7] I2P developers. 2021. A Gentle Introduction to How I2P Works. https://geti2p.net/en/docs/how/intro Accessed: 2021-10-13.

[8] I2P developers. 2021. *I2P's Threat Model*. https://geti2p.net/en/docs/how/threat-model Accessed: 2021-10-13.

[9] I2P developers. 2021. *I2PTunnel*. https://geti2p.net/en/contact Accessed: 2021-10-13.

[10] Tor developers. 2021. *History*. https://www.torproject.org/about/history/ Accessed: 2021-10-13.

[11] Tor developers. 2021. *How do onion services work?* https://community.torproject.org/onion-services/overview/ Accessed: 2021-10-13.

[12] Tor developers. 2021. *Sponsors*. https://www.torproject.org/about/sponsors/ Accessed: 2021-10-13.

[13] Roger Dingledine, Nick Mathewson, and Paul Syverson. 2004. *Tor: The second-generation onion router*. Technical Report. Naval Research Lab Washington DC.

[14] David Goldschlag, Michael Reed, and Paul Syverson. 1999. Onion routing. *Commun. ACM* 42, 2 (1999), 39–41.

[15] Stefan Köpsell. 2011. *Anonymous Web Browsing and Publishing*. Springer US, Boston, MA, 40–42.

[16] M. Lee. 2015. *Edward Snowden Explains How To Reclaim Your Privacy*. https://theintercept.com/2015/11/12/edward-snowden-explains-how-to-reclaim-your-privacy/ Accessed: 2021-10-11.

[17] P. Golle N. Borisov. 2007. *Privacy Enhancing Technologies*. Springer-Verlag Berlin Heidelberg, 2–5, 63–64, 184.

[18] A. Pfitzmann and M. Hansen. 2010. A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. *ResearchGate* (2010).

[19] Michael G Reed, Paul F Syverson, and David M Goldschlag. 1996. Proxies for anonymous routing. In *Proceedings 12th Annual Computer Security Applications Conference*. IEEE, 95–104.

[20] Michael G. Reed, Paul F. Syverson, and David M. Goldschlag. 1998. Anonymous connections and onion routing. *IEEE Journal on Selected Areas in Communications* (1998), 482–494.

[21] Kyle Swan. 2016. Onion Routing and Tor. *GEO. L. TECH. REV.* 1 (2016), 110–110.

[22] Denh Sy, Rex Chen, and Lichun Bao. 2006. Odar: On-demand anonymous routing in ad hoc networks. In *2006 IEEE International Conference on Mobile Ad Hoc and Sensor Systems*. IEEE, 267–276.

[23] Yi Yang and Sencun Zhu. 2011. *Anonymous Routing*. Springer US, Boston, MA, 39–40.

A Appendix

A.1 Summery of discussion from the seminar

Question 1: Anonymity for everyone - is the tradeoff worth it (criminals can abuse the anonymity, whereas others need it for their freedom of speech)?

Most of the students agreed that the tradeoffs were worth it. The arguments were:

- Anonymous routing is not the cause of criminality. Even if anonymous routing was prohibited, criminals will find other ways to do their criminal activities.
- It's a safe path for whistleblowers and journalists to take so that they don't get into trouble. Even if for example whistleblowers are a very small proportion of society, their impact on society is tremendous.
- It also depends on the use case - a private individual with "nothing to hide" but who cares somewhat about their online privacy might at first use an AR tool like the TOR browser, but then realise that it is slow (or depending on what they wish to do online, e.g. stream movies or just surf websites that serve basic images and text) and switch to using their regular connection ("the clearnet" connection) for the sake of convenience. In this way, there is always the choice between privacy and convenience.

Question 2: In what situations might it be reasonable to sacrifice latency/network speed/performance in order to achieve anonymous communication?

Multiple situations were discussed:

- The sacrifice in terms of latency and performance were insignificant in the cases where a whistleblower will report something. (provided that the whistleblower does not need to upload large data-sets or files)
- In the situation where a car wants to communicate with other cars anonymously this approach was not suitable. The group argued that in such cases latency becomes critically important.
- Lots of people agreed that the sacrifice is definitely worth it when using unencrypted and untrusted local networks to access the Internet. AR networks, much like regular VPNs, do a good job of hiding one's traffic from the local network.
- Another example was connecting to an AR network when located in a country where there are regional or national firewalls that prevent free access to the Internet, or where internet access is highly specific to an individual (e.g. you may have to identify yourself with a passport or social security number in order to buy a SIM card to access the Internet) and the government of that state is known to track and monitor its citizens internet traffic.

Question 3: What are the limitations of anonymous routing?

Multiple limitations were discussed:

- When there is an exit node the system will still be vulnerable to traffic analysis attacks. The anonymous routing will make traffic analysis more difficult but it will not eliminate the risk completely in this case.
- A potential limitation is the fact that there's a relatively low user base for AR networks. This means that simply connecting to an entry node in an AR network ultimately

exposes you as being a user of AR, which could make you a target for government surveillance, for instance. This may be considered to be a limitation and risk factor of such networks.

- If using onion routing, peer-to-peer connections are not possible, you have to use garlic routing (and setup I2P on your computer, which can be a complicated process). There is no one AR network that is flexible enough to have implemented multiple internet protocols, while simultaneously having a large enough user base to allow for anonymous communication.

Optional question 4: What are the consequences of being anonymous on society and people's behavior?

We had some extra time to discuss this question as well. A student brought up an interesting issue that happened in Australia. Apparently the authorities were discussing a new proposed legislation that will Deanonymise the internet all over Australia so that authorities will know the identity of every internet user within Australia. The reason behind this proposal was that many fake accounts are being used on the social network for malicious uses like bullying, spreading fake news or spreading radical ideas. The students discussed this issue and pointed out that even if the authorities implement such a control over the internet, how could they make sure that a malicious activity was done by the user and not a malware that got into the users system.