A Systematic Review of Anonymous Communication Systems

Ramzi A. Haraty[1], Maram Assi[1] and Imad Rahal[2]
[1]*Department of Computer Science and Mathematics, Lebanese American University, Beirut, Lebanon*
[2]*Department of Computer Science, College of Saint Benedict & Saint John's University, Collegeville, MN, U.S.A.*

Keywords: Anonymous Systems, Crowds, FreeNet, NetCamo, Mixmaster, Tarzan, TOR.

Abstract: Privacy and anonymity are important concepts in the field of communication. Internet users seek to adopt protective measures to ensure the privacy and security of the data transmitted over the network. Encryption is one technique to secure critical information and protect its confidentiality. Although there exist many encryption algorithms, hiding the identity of the sender can only be achieved through an anonymous network. Different classifications of anonymous networks exist. Latency level and system model architecture are two essential criteria. In this paper, we present a description of a set of anonymous systems including NetCamo, TOR, I2P and many others. We will show how these systems work and contrast the advantages and disadvantages of each one of them.

1 INTRODUCTION

Due to the increasing use of the Internet and the emergence of wireless technologies, the value of security and privacy is becoming more significant. New online activities have arisen during the last decade with the advancement of the electronic communication. People can now shop online, send and receive emails, pay their mobile bills, and make diverse banking operations. These types of electronic activities produced new challenges. Two main goals the sender of information over the network seeks to ensure: the privacy and the security of the communicated information. Confidentiality and protection of the data can be achieved through encryption mechanisms. Encryption in general is capable of hiding the content of the information in the network. Moreover, in some cases, the sender might wish to hide his/her identity. This objective can be achieved through the use of anonymous systems.

Traffic analysis is the art of examining and intercepting messages transmitted over the network to infer information, thus it violates user privacy. Several technologies exist to ensure data integrity and the security of the transmitted information that might be very critical in certain cases. Anonymous communication protects the identities of the sender and the receiver from third parties and keeps the identity of the user hidden from remote parties (Mittal 2012). Hiding the user-server relationship is another crucial goal behind any communication. For example, let us consider a client that wishes to communicate with a web server. This client might prefer to stay anonymous. One of the protective measures that help hiding the identity of users communicating through the internet is anonymous network. These networks allow users to surf the Web without leaving any tracking information.

In (Chaum 1981), Chaum presented almost the first architecture allowing the transmission of untraceable email. The main idea behind the proposed architecture is to allow communicating peers to transmit data through cascade proxies known as Onion Routers. Anonymity is achieved by the use of public key cryptography. Most other proposed anonymous systems nowadays are based on Chaum's scheme. While the main goal behind anonymous system is to protect the identity of the sender or the receiver, several other motivations exist. Some common ones include freedom of speech, censorships and personal privacy in order to prevent data mining and tracking. Anonymous systems can be classified into two main types: high latency and low latency. In the former category of networks, the transmitted message takes several hours or even several days to reach the desired destination. Quick response is not required for such application including email systems for example (Wiangsripanawan, 2007). For interactive and real-time applications like instant messaging, a low

Haraty, R., Assi, M. and Rahal, I.
A Systematic Review of Anonymous Communication Systems.
DOI: 10.5220/0006216802110220
In *Proceedings of the 19th International Conference on Enterprise Information Systems (ICEIS 2017) - Volume 2*, pages 211-220
ISBN: 978-989-758-248-6

latency communication network is required because of the timing constraint. TOR and I2P are two examples of low latency anonymous systems that will be discussed in the next section (Zantout, 2011)(Haraty, 2014). From an architecture point of view, anonymous systems can be divided into two categories client-server communication system and peer-to-peer based anonymous network. In fact, in the client-server model, only few nodes are selected to provide anonymity to the rest of the users. One disadvantage of this architecture is that the number of server nodes is small, and an attacker can easily track the traffic. The P2P architecture overcomes this challenge. The main idea behind this model is that there is no distinction between a server and a user (Zhang, 2011). In these systems, it is hard to distinguish the sender and the receiver nodes. As a matter of fact, all nodes in the network are considered universal receivers and universal senders making it difficult to detect whether a specific node is transmitting or receiving data.

This paper investigates the network anonymous systems that seek to protect the identity of the sender of information transmitted over the Internet and that provide secrecy. Each upcoming section describes how a specific system works to achieve anonymity. A contrast of the advantages and disadvantages of each technology is illustrated later. Finally, the last section summarizes the major ideas discussed in this paper.

2 BACKROUND

Throughout the research that was conducted during the preparation of this paper, a number of observations where noted for the design and implementation of the new methodology. They are as follows:

1. No Real End-to-End Traffic Analysis Prevention Assurance:

Although many of the previously mentioned implementations claimed avoiding traffic analysis, the possibility for this to occur is extremely high and unavoidable in unmanaged Local Area Networks (LAN).

Securing LAN environments could be a costly, and sometimes an overkill (cost wise), for organizations of different sizes. Using any of the implementations in unsecured LAN environments such as computer labs, work environments, or wireless networks is somehow a hassle and rarely found. Therefore man-in-the-middle attacks can occur at any of these locations or even public networks whereby a malicious attacker can sniff packets being transmitted and received by a particular user or a number of users, and then apply traffic analysis techniques. One has to note here that preventing traffic analysis at the end-to-end level is realistically impossible if infrastructure network security measurements are not implemented on the infrastructure level.

2. Trust is in "Cathy"

In any security model example or illustration, authors tend to use Bob and Alice as two entities wishing to receive and send information from/to each other with a trusted entity called Cathy, and a malicious attacker called Eve. The aim of any traffic analysis avoidance algorithm considers Eve as an eavesdropper that will only sniff information. Hence, the algorithm designed by security personnel tries as much as possible to circumvent traffic being passed to Alice and Bob through many and different routes while camouflaging and encrypting data in order not to allow Eve to sniff this information. What is somewhat confusing is that sometimes one only considers Eve to be on one of the routes that information is being sent to and from Alice and Bob, and that Eve is only capable of sniffing abilities and not injecting information or even tampering with the data being sent through a route or different routes.

Moreover, in any security model, the adoption of a trusted entity, Cathy, is a must to verify the identity of senders and receivers and later to validate the data being transmitted and received from parties involved. Cathy happens to be a fixed host that is susceptible to attacks by Eve also, and any compromise done to Cathy renders the whole security model useless sometimes. As a simple example, if Eve is capable of injecting information onto a stream whereby Cathy has been compromised by Eve, the receiving entity will try to validate this information against Eve and not the trusted entity Cathy. Data integrity is a vital part of any security system and having a single point of failure is ultimately a drawback in any security model. In an ever growing world of communication and networks, one has to consider alternatives to basic security models and concepts. Decentralization of trusted entities needs to be seriously considered in anonymous systems hence the reason why I2P was invented.

3. Questionable Host Reliability and Security

Almost every traffic analysis avoidance design and implementation relies on hosts that belong to users for creating different routes and therefore passing

data through different hops on the network or the Internet.

What some of the implementations lack, is catering for the reliability and security of such hosts mainly because of many factors such as:

a. How trustful are these hosts really? If a host decides to join a network for anonymous communication then should that host be trusted immediately and therefore have data sent to it to route to other hosts. Consider Eve to be a distributed form of traffic analysis whereby a number of malicious hosts join an anonymous communication model at strategically selected locations or routes. Data being transmitted on this network would no longer be anonymous because Eve can now collect information from all hosts on the network and perform traffic analysis on a compilation of streams instead of one.

   Some authors (like Tor developers) argue that the more the number of hosts joining an anonymous system and participating in traffic then more anonymity of traffic being sent and received becomes possible.

b. Hosts are usually personal computers and workstations that could be located at users' homes, labs, and work. These hosts usually have limited bandwidth allocated to them due to network lab restrictions or because of asynchronous bandwidth limitations enforced by Internet service providers (DSL).

   Communication with these hosts could suffer from factors like intermittent connections, lack of reliability because of host reboots, signoffs, power shutdowns, security vulnerabilities/checks, or even policies enforced by organizations' firewall implementations, not to mention downtime for hosts because of day/night time making the number of available nodes much less during non-congestion hours. Accordingly, and although many implementations have managed in deploying their design successfully on the Internet (such as Tor), they have introduced dedicated reliable servers worldwide and continue to encourage users to donate and deploy dedicated servers in order to make their network reliable to compensate users' computer usage behaviors. However how wise is this?

4. No Dynamic Hops

Some anonymous systems require a number of host hops or anonymous-router hops for traffic to pass through, before sending the information to its proper destination. The reason for this is obviously adding more anonymity to the transmission of traffic and also hiding the identity of the sender. However this also adds more latency and overhead on the communication stream. The worst case scenario could be taken geographically whereby regional traffic may travel to remote hops and then come back to the receiver that happens to be close to the sender's region. Hence, dynamic, geographically distributed hops need to exist in order to predict sender and receiver locations and therefore select a certain number of hops that is ideal for communication.

3 SYSTEM DESCRIPTION

1. NetCamo which stands for Network Camouflage is a system designed to provide both security and efficiency for real time systems while avoiding traffic analysis (see figure 1). Traffic analysis avoidance is ensured by two different requirements: Traffic padding and traffic rerouting. In the traffic padding, encrypted data is padded with meaningless data. In other words, in order to camouflage the packets sent over the network, additional packets are inserted into the payload. In the traffic rerouting, unlike the default behavior of transferring the data from source to destination through a single path, data is transmitted through different routes (camouflaged traffic pattern) to reach its destination.

According to the authors in (Guan, 2001), the main challenge in NetCamo is to ensure that the traffic analysis prevention is performed in a realistic time (suiting the nature of the interactive applications). This objective becomes hard to achieve when the network becomes full of padded traffic. Actually, the communication over the system passes through three phases: The system configuration phase where the traffic pattern is determined, the admission control phase where new communication streams are accepted or rejected and the runtime phase where the actual camouflaging of data is done (Haraty, 2015).

2. TOR, as predicted in figure 2, is a low-latency anonymous communication system. It is considered an improved version of the traditional Onion Routing that includes new integrated features. There are three main entities participating in the proposed approach: Tor client which is the sender that wishes to establish an anonymous communication, the Tor servers that are the Onion routers responsible for routing streams to next nodes and the recipient. In

summary, Tor is made up of a collection of onion routers where each one sends information in a secure way to the next hop. Any client can become a server acting as a Tor onion router. To ensure camouflaging the type of data being transferred, data is sent in encrypted format with fixed size packets called cells which are relayed without revealing their content or their complete route. This is achieved through cell encapsulation and multilevel encryption.

To start communication, the client contacts a Tor management node which maintains the list of bridge nodes which accept connections for which a specific handshake occurs. When the client determines the participating nodes, it sends a "create" cell to each of them without allowing any of them to know the presence of the other.

One of the disadvantages of Tor resulting from its architecture is that the central directory containing the list of servers is often a target for the attackers. Another problem with Tor is that it serves a large number of users, therefore the use of a limited number of servers to build an anonymous path will which leads to performance issues. In addition, users must keep track of all the available servers, especially when the number of servers becomes large as this may cause a deterioration of performance due to bandwidth contention.

3. I2P, known as Invisible Internet Project is a low latency anonymizing mix network. Its main scope is anonymous file-sharing and web hosting (Timpanaro, 2014). I2P presents some similarities with tor however, a major difference between the two can lies in the fact that tor focuses on hiding the anonymity of the sender, while I2P also hides the identity of the receiver (Erdin, 2015). It operates on the network layer. One main characteristic of this system is that it distinguishes between user online identity and its geographical location. In fact, the user is not identified by its IP address and port number but by another identifier independent of its location. I2P is message based instead of circuit based. It is a fully distributed system for anonymous P2P communications and not browsing which does not rely on centralized directory servers. Previously encrypted onion cells are grouped together with extra padding as well as delay/no-delay instructions to other I2P nodes and then packaged in so called garlic cloves which are passed in encrypted format. The system uses different types of cryptographic algorithms. I2P is portrayed in figure 3.

4. Crowds is a proposed anonymity system for web transactions. It allows users to surf the web anonymously as shown in figure 4. It is named for the notion of "blending into a crowd" where users are grouped into a large and geographically diverse group. Requests are then issued by the group on behalf of its members, thus web servers will not be able to know the exact source of a request as it might have been issued from any of the crowd members. Even members of the same crowd cannot differentiate between the originator of a request and a member that is only forwarding the request. Each participant in the group is simultaneously protected and protects other user as well. Therefore each participant is playing the role of a proxy (Sui, 2003).

5. Based on Chaum's mix approach, **Tarzan** is yet another low-latency anonymous communication system (see figure 5). Its main goal is to offer anonymity for different applications including instant messaging and web applications. It is a decentralized P2P anonymous network that provides IP service which makes it general purpose and transparent to applications. Each node in the Tarzan model can be both the client and the relay. It supports layered encryption and multilevel routing where a client chooses a path of peers in a restricted way that protects communication against adversaries. It also uses a protocol to ensure unbiased selection of peers. Its cover traffic mechanism offers protection against traffic analysis of message volume or content, against message flooding, and against DoS attacks.

Nodes participating in the communication run software that discovers other participating nodes, intercepts packets generated by local applications that should be anonymized, manages tunnels through chains of other nodes to anonymize these packets, forwards packets to implement other nodes' tunnels, and operates a NAT (network address translator) to forward other participants' packets onto the ordinary Internet. Therefore, the receiver is not necessary belongs to the Tarzan network.

6. FreeNet is decentralized P2P network application for storage and retrieval of files in such a way that protects the anonymity of both senders and receivers. The system works as a location-independent distributed file system where many individual computers that cooperate in routing the requests.

Nodes participating in the Freenet network provide their data storage to the network. Each node maintains its own data store that it makes available to the network and a routing table which contains the addresses of other nodes. Requests are passed through a series of proxys where every node locally

decides the next node to receive the request. Hence, each node in the proxy chain is only aware of the node it received the request from and the node it forwards it to which makes infeasible to determine if a particular node is the actual originator of the requests or a forwarder. This is revealed in figure 6. In addition, files are dynamically replicated in locations close to requesters and removed from locations where no requests for them are made.

Some disadvantages of Freenet system related to the performance are that it sometimes poorly locates files and it presents a low speed in downloading found files (Skogh 2006).

7. Mixmaster is the most widely deployed and used remailer system. Remailers are servers whose main goal is to send email without providing any information about the source. Messages are encrypted while keeping their size is kept constant by appending random noise at the end of the message. This noise is generated using a secret shared between the remailer and the sender which makes allows protecting the integrity of the header and content of the message. Besides protecting anonymity, Mixmaster allows sending large emails without the need to use special software. It also protects against traffic analysis. Mixmaster is illustrated in figure 7.

4 ANONYMOUS SYSTEMS COMPARISON

Each of the mentioned anonymous communication systems has its own characteristics and architecture. Some follow the client-server architecture, some other adopt the peer-to-peer design. Different systems are suitable for different type of applications. Real-time application requires low-latency communication systems whereas high-latency systems can fit to other applications. Moreover, these anonymous communication models are susceptible to various attacks (Haraty, 2015). Table 1 presents the advantages and the disadvantages of the discussed approaches and help deciding which model is best proper to each application.

5 CONCLUSIONS

In this paper, we discussed how protecting the information shared by users over the Internet, and the identity of the users themselves are very important. Adopting anonymous systems is one way to achieve secrecy of the user's identity. Each of the mentioned technologies has its own limitations. In fact, some are not applicable for real time applications and some others might not be able to detect malicious attacks. As each system has its challenges, we can explain the conflict in each system between its advantages and its drawbacks. Besides the various implemented systems hiding the identity of the users, studies in the field of anonymous networks continue to grow.

ACKNOWLEDGEMENTS

This work was funded by the Lebanese American University in Beirut, Lebanon.

REFERENCES

A. A. M Direct. Retrieved on February 11, 2017 from http://aamdirect.sourceforge.net/.

Atlassian Documentation. Retrieved on February 11, 2017 from https://confluence.atlassian.com/display/CROWD/Crowd+2.2.2+Release+Notes.

Chaum, D. 1981. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM, pp. 84-90.*

Erdin, E., Zachor, C., and Gunes, M. 2015. How to find hidden users: A survey of attacks on anonymity networks. *IEEE Communications Surveys & Tutorials pp. 2296-2316.*

Guan, Y., Fu, X., Xuan, D., Shenoy, P., Bettati, R., and Zhao, W. (n.d.). 2001. NetCamo: Camouflaging network traffic for QoS-guaranteed mission critical applications. *IEEE Transactions on Systems, Man, and Cybernetics - Part A*, pp. 253-265.

Guide (n.d). Retrieved on February 11, 2017 from https://trac.i2p2.de/attachment/wiki/Content/i2prouting.png.

Haraty, R. and Zantout, B. 2014. The TOR data communication system – a survey. In *Proceedings of the Sixth IEEE International Workshop on Performance Evaluation of Communications in Distributed Systems and Web based Service Architectures (PEDISWESA'2014)*. Madeira, Portugal.

Haraty, R. and Zantout, B. 2014. The TOR data communication system. *Journal of Communications and Networks*, 16 (4) (2014) ISSN 1229-2370.

Haraty, R. and Zantout, B. 2015. A Collaborative-based Approach to Avoiding Traffic Analysis and Assuring Data Integrity in Anonymous Systems. *Computers in Human Behavior Journal. Volume 51, Part B, pp. 780–791.*

Haraty, R. and Zantout, B. 2015. *The NetCamo data communication system. Advanced Science Letters. Volume 21, Number 3, pp. 472-477.*

Mittal, P., and Borisov, N. 2012. Information leaks in structured peer-to-peer anonymous communication systems. *ACM Transactions on Information and System Security, pp. 1-28.*

Skogh, H., Haeggstrom, J., Ghodsi, A., and Ayani, R. 2006. Fast Freenet: Improving Freenet performance by preferential partition routing and file mesh propagation. In *Proceedings of the Sixth IEEE International Symposium on Cluster Computing and the Grid.*

Sui, H., Wang, J., Chen, J., and Chen, S. 2003. An analysis of forwarding mechanism in crowds. In *Proceedings of the IEEE International Conference on Communications.*

Sysmagazine. Anonymous networks and timing attacks: Tarzan and MorphMix. Retrieved on February 11, 2017 from: http://sysmagazine.com/posts/117586/.

Timpanaro, J., Chrisment, I., and Festor, O. 2014. Group-based characterization for the I2P anonymous file-sharing environment. In *Proceedings of the 6th International Conference on New Technologies, Mobility and Security (NTMS).*

Tor - The Onion HTTP Router. Retrieved on February 11, 2017from http://tohr.sourceforge.net/.

Wiangsripanawan, R., Susilo. W., Safavi-Naini, R. (2007) Design principles for low latency anonymous network systems secure against timing attacks. In *Proceedings of the Fifth Australasian Symposium on ACSW Frontiers*, Balart, Australia.

Zantout, B. and Haraty R. 2011. I2P Data Communication System. *In Proceedings of the Tenth International Conference on Networks (ICN 2011)*, pp. 401-409, St. Maarten, The Netherlands Antilles.

Zeinalipour-Yazti, D., Kalogeraki, V., and Gunopulos, D. 2003. Information Retrieval in Peer-to-Peer Systems. University of California at Riverside. Available: http://www.cs.ucr.edu/~csyiazti/papers/cise2003/cise2003.pdf.

Zhang, J., Duan, H., Liu, W., and Wu, J. 2011. Anonymity analysis of P2P anonymous communication systems. *Computer Communications, pp. 358-366.*

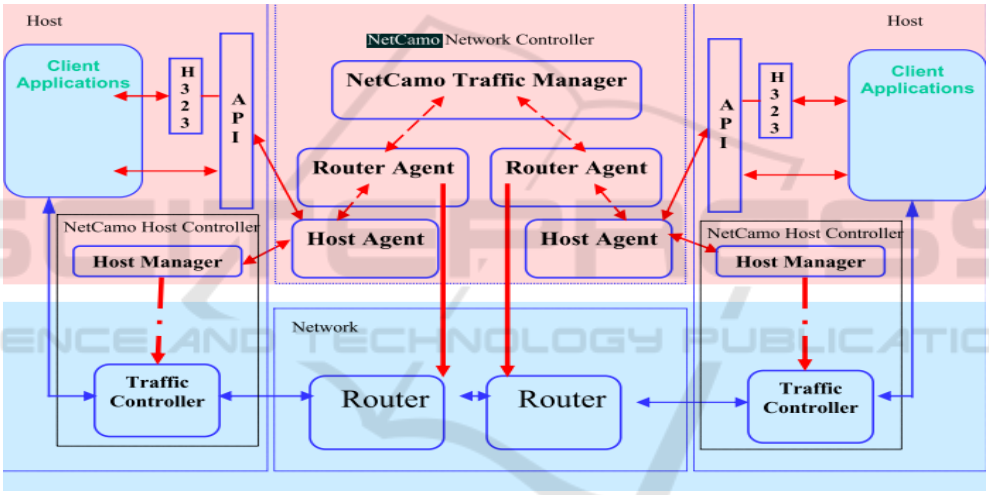

Figure 1: Architecture of NetCamo (Guan, 2001).

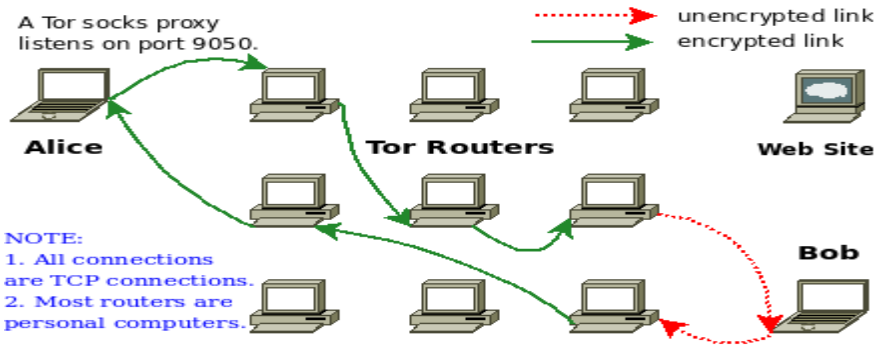

Figure 2: Tor architecture (TOR - The Onion HTTP Router, 2017).

Table 1: Comparison of the different anonymous systems Advantages.

		Disadvantages
BitTorent	• Excellent peer-to-peer communication technique for utilizing peer bandwidth. • In case file transfer is interrupted, only the missing pieces are re-downloaded and hence saving time and bandwidth. • Bandwidth chocking and throttling are efficient to assure bandwidth reliability and availability for both existing and new peers.	• Blocked by most ISPs based on fingerprinting due to the excessive traffic it generates. • To enhance traffic, a P2P caching appliance was created which still constitutes a security risk as many portions of downloaded files are cached for new coming peers, so spoofing techniques may allow any user to stream existing cached information. • Strictly used for file transfer and does not contain any substantial security measures. • Cannot be used for real time communication like secure shell, Telnet, VoIP…
NetCamo	The system is able to distribute traffic through different predetermined paths and routes in order to prevent against traffic analysis.	• It does not consider geographical distribution of hosts and routes. • Dependent on hosts and routers where a single managing component takes control of all routers and hosts to determine acceptance or rejection of a traffic stream which is hard to implement in the real world. • Dependent on routers to set the rate of traffic and control the network flow. • Since the system is centralized, attacks on the main node can render the system useless. • Traffic padding is performed at a rate of $1/\alpha$ where α can be determined if kept constant. • Un-trusted hosts can join. They can drop packets or interfere in malicious ways to make the system unreliable. • End-to-end prevention for data sniffing and traffic analysis is impossible when it comes attacks occurring at the LAN level
TOR	Protects against strong and weak attackers based on Tor design as well as encryption techniques. Protects anonymity of sensitive published content. Tor nodes are not aware of the complete plan of communication, so even if one node is acting maliciously, it can only know little. The addition of more Tor nodes adds more anonymity. Contacting nodes gradually adds more security as building the path is based on a list of bridge nodes.	• Directory information server can be blocked. • Blocking based on fingerprinting Tor`s connection: handshakes are clear to authorities thus any intelligent firewall can detect them and block them. • Centralization of directory servers for managing the Tor network: attackers can fake the identity of the Tor directory by redirecting traffic to a local server, the attacker can maliciously modify a Tor client and then repackage it for users to download. • Single path for a data stream moving inside a circuit: saving the traffic for latter analysis may reveal the identity of sender and receiver. • Malicious attackers and relayers may not be identified. • Slow performance: more load on Tor dedicated nodes which decreases anonymity, security and reliability. • Successes or failures in data integrity checks may render a circuit useless. • Website fingerprinting and backtrack attack due to lack of packet camouflaging.
I2P	Message based instead of circuit based: which leads to the decrease in overhead and odds randomness while allowing hops to control data delivery. Various protocols support: offers a wide range of internal services, anonymous hidden services... New P2P infrastructure over the Internet: P2P activities become anonymous to all participating parties. Different encryption techniques: good set of algorithms (symmetric, asymmetric.. Decentralized System: protected against attacks on its directory serves. Different types of un-directional tunnels which enhances the amount of peers participating in communication and therefore increasing number of hops. End user Node Participating in communication: encourages every node joining I2P to use part of its bandwidth as relay node which adds more hops and thus leads to randomness.	• Vulnerable to partitioning attacks: may disconnect targets in the system and reveal identities of all parties involved. • Possible intersection attacks: attacker may eliminate nodes that have not participated in communication with target until target's paths are narrowed down which makes nodes participating exposed for monitoring. • Lack of node and bandwidth monitoring, participating peers variably change their relay capabilities and random joins and departures may allow wide distributed attacks resource consumption attacks without being detected. • NetDB conflicts and resolution • DOS attacks: 1. Greedy user attack: users willing to download more than upload which decreases traffic replay, less anonymity since the number of hopes is less. 2. Starvation attack: bad and intermittent communication for end users.

Table 1: Comparison of the different anonymous systems Advantages (cont.).

Crowds	It offers the user some degree of deniability for her observed browsing behavior, if it is possible that she was using Crowds. No single failure discontinues all ongoing web transactions Privacy is enhanced by increasing the average number of times a request is forwarded among members before being submitted to the end server with less impact on the performance because of the use public private key operations… Probability of receiver anonymity increases as size of crowd. Sender anonymity against end servers Protection against timing attacking the crowd Good performance due to load balancing	• A user may be incorrectly suspected of originating a request • It cannot protect user`s anonymity if the content of her web transaction reveals her identity to the webserver • It can be undermined by executable web content that, if downloaded into the user`s browser, can open network connections directly from the browser bypassing Crowds and exposing the user to the end server. • No effort to defend against DOS attacks by crowd members • No sender anonymity against local eavesdropper and no receiver anonymity against end servers • Firewalls represent a barrier to wide-scale inter-corporation adoption of Crowds
Tarzan	Reduces effort needed to incorporate anonymity into existing designs without the need to change them. Self-organizing and fully-decentralized. Scales to much larger networks. Better protection against static adversaries than Crowds and Onion Routing Effective and efficient peer-discovery mechanism Its cover traffic mechanism offers protection against traffic analysis of message volume or content, against message flooding, and against DoS attacks of slowing incoming rates. Prevents information leakage at exit points by using integrity checks Fast packet forwarding rate, high throughput, and reasonable tunnel-setup latency.	• No sender protection against malicious routers. • It may be susceptible to some attacks that use additional application-layer information. • No real protection against information that leaks through application-layer interaction. • A new tunnel is unlikely to traverse the same small path thus long-term node observation or time-intensive attacks are less effective.
Freenet	It keeps information available while remaining highly scalable. Sender`s anonymity is preserved beyond suspicion against collaboration of malicious nodes. Key anonymity and stronger sender anonymity are achieved by pre-routing of messages. Protection of data source by the occasional resetting of the data source field.	• Since routing depends on knowledge of the key, key anonymity is not possible in the basic FreeNet scheme. • Against local eavesdropper, there is no protection of messages between user and the first node contacted. • Requested files can be modified by malicious nodes in addition to data being vulnerable to dictionary attacks • Subject to DoS attacks.
Mixmaster	Supports sender anonymity. Allows large emails to be transmitted without the use of special software and messages to be transmitted multiple times using different paths. Protects against email spammers. Protects content by including a hash of the message in the header.	• No analysis on the impact of its anonymity features has ever been performed. • No filtering of content.

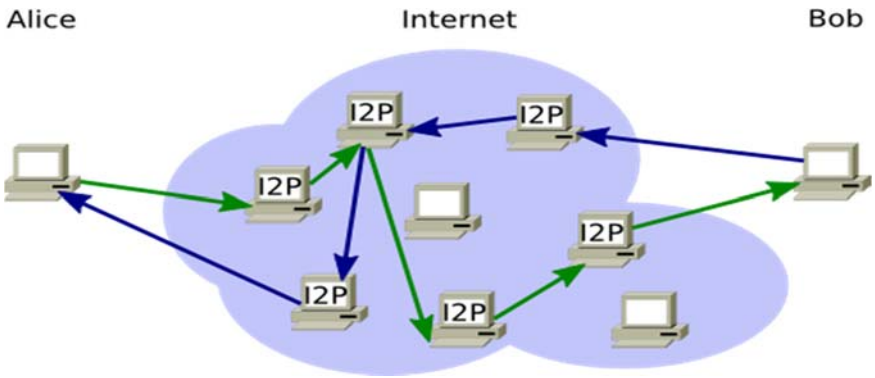

Figure 3: I2P architecture (Guide, 2017).

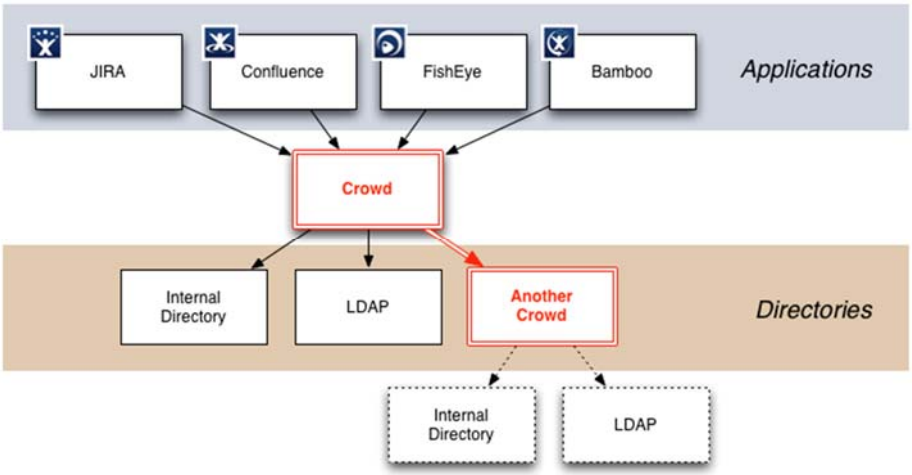

Figure 4: Architecture of Crowds (Altassian, 2017).

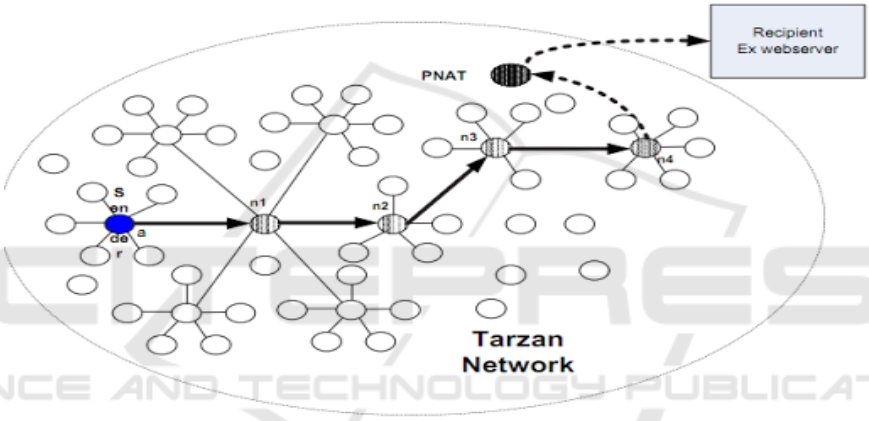

Figure 5: Tarzan Architecture based on simulators (Anonymous networks, 2017).

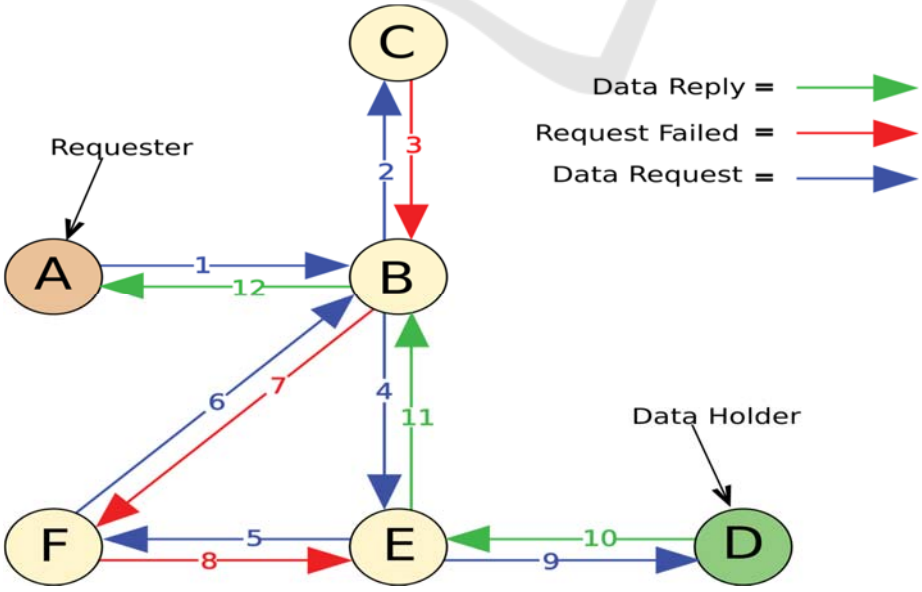

Figure 6: The Freenet architecture (Zeinalipour-Yazti, 2003).

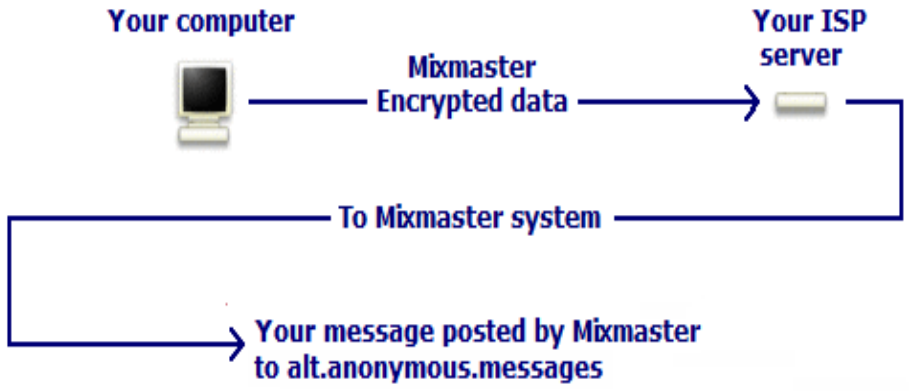

Figure 7: The Mixmaster remailer model (AAM Direct, 2017).