Investigation and Analysis of Anonymizing Networks

Ms. Nikita L. Vikhar,
M. E. in Computer Science and Engineering,
Prof. Ram Meghe Institute of Technology and Research, Badnera, Amravati,
n.vikhar@gmail.com,
INDIA.

Abstract— *the networks like Tor (Anonymizing networks) allows users to access Internet services privately by using a series of routers to hide the client's IP address from the server. But this networks success is limited up to users those are employing this anonymity for abusive purposes like defacing popular Web sites. In such cases, the administrator of website depends on solution of periodic IP-address blocking for disabling access to misbehaving users, however blocking IP addresses is not practical if the abuser routes through an anonymizing network. This problem statement is our research area. However in this investigation work, we are presenting the literature and comparative study over the different types of anonymous networks. We will discuss their working procedure, their benefits and limitations for anonymous communication networks. Finally based on existing experimental studies, we will present the comparative analysis each type of anonymous network.*

Index Terms— anonymity, mix networks, peer-to-peer, IP address, latency, flooding attack, timing attack.

1 Introduction

When you open the document, select "Page Layout" from the Internet has become an essential to everyone's standard of living. Folk's access to net to do business, to find job, to contact friends, to pay bills etc. Internet has become another utility like water and electricity, which plays more and more vital role in each day life.

With the impact of net on society, folks became more sensitive concerning privacy issues in the net. They realized that they leave all types of traces and personal data whereas aquatics websites and exchanging emails. In some cases, people do not need others understand what they are talking. So, secret writing like Pretty Good Privacy (PGP) was introduced, eavesdropping on content becoming very difficult. However, protective privacy means that not only the content of messages, but also concealing routing data which implies United Nations agency is speech whom. Unfortunately, the Internet was not designed with namelessness in mind; in truth, one among the original design goals was accountability [1]. Informatics packet which is one among the foremost an important infrastructure protocol in network contains a lot of fingerprint. There many reasons due to which the interest and demand in using anonymous networks has increased. Following are important reasons:

- The material or its distribution is illegitimate. Music and moving-picture show files sharing in peer-to-peer The material or its distribution is illegitimate. Music and moving-picture show files sharing in peer-to-peer network systems, e. g. Bit Torrent, Kazaa.
- The material is real according to laws. However it's problematic for social world. For example, individuals could overtly discuss personal stuff which might be embarrassing to inform many of us regarding, like sexual issues.
- Fear of retribution. (Whistle-blowers, unofficial leaks, and activists who don't believe restrictions on data or knowledge).
- Censorship at the native, structure, or national level. Cisco designed and deployed packet content filtering equipments in each ISP access points in mainland China. The transmission control protocol affiliations are going to be reset if it contains susceptive name, IP address or maybe key words.
- Personal privacy preferences like preventing pursuit or data processing activities. MAC and IP address is used to determine one device. Moreover these persistent addresses are joined to physical persons, seriously compromising their privacy.
- In this investigation studies, we are discussing the technical issues and security issues with Anonymous networks. Following section II present the literature review over the network anonymity. Section III presents the anonymous networks based on centralized methods. Section IV presents anonymous networks based on distributed approaches. In section V we will discuss the comparative study between all types of anonymous networks.

2 Literature Review

Achieving anonymity during a network is incredibly tough. Encoding is used to defend data's confidentiality, whereas anonymity suggests that defend each information and participants during this communication. Sadly, the net wasn't designed with anonymity in mind; indeed, one of design style goals was irresponsibleness. In packet switching network, each IP packet contains a header to explain the packet itself, the header contains Identification contains a number that identifies this datagram. This field is employed to assist piece along datagram fragments.

Time-to-Live maintains a counter that gently decrements right down to zero, at that point the datagram is discarded. This keeps packets from iteration endlessly, source Address specifies the sending node, and Destination Address specifies the receiving node. What additional is, there\'s lots of helpful data among packet for network analyzers to spot communication between 2 parties. This data includes supply port, destination port, sequence variety, window size. Therefore the anonymize communication is to code the information within the packet, modification supply informatics address, modify port variety and Time-to-Live price to cover the fingerprint of instigator. However, these ways don't seem to be enough to counter network traffic analyzers. Additional refined anonymous ways are desired. Following sub sections gives the terminology, taxonomy and models details:

2.1 Terminology

Depending on the previous research papers on in this field, researchers planned a collection of precise terminologies [3]. These definitions may facilitate researchers invents new word with same that means. I\'m about to use these terminologies in latter sections.

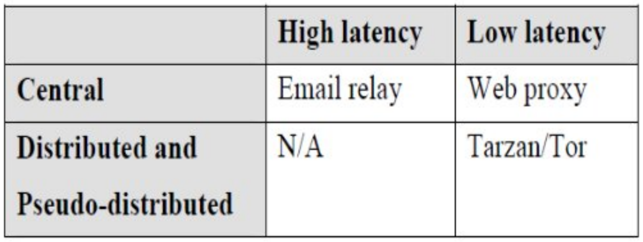
Anonymity: Anonymity of a theme from an attacker's perspective means the attacker cannot sufficiently establish the topic among a collection of subjects, the obscurity set.

Unlinkablity: Unlinkability of 2 or additional things of interest (IOIs, e.g., subjects, messages, actions,) from an attacker's perspective means among the system (comprising these and presumably alternative items), the attacker cannot sufficiently distinguish whether or not these IOIs are connected or not.

Unobservability: Unobservability of an item of interest (IOI) means that undetectability of the IOI against all subjects uninvolved in it and obscurity of the subject(s) concerned within the IOI even against the opposite subject(s) concerned therein IOI.

2.2 Taxonomy

Based on the network architecture and its usability, the anonymity communication divided into 4 parts such as:



	High latency	Low latency
Central	Email relay	Web proxy
Distributed and Pseudo-distributed	N/A	Tarzan/Tor

Figure 1: Types Anonymous Networks

Central/High latency: - there's a central server that has anonymity service to clients, as an example email relay service such as anon.penet.fi.

Central/Low latency: - clients will send requests to the central server, the server modify the packet and resend these requests to destinations. As an example, Anonymizer and Safe net are such kind of service.

High Latency and Distributed/Pseudo-Distributed/High Latency: - Because of distributed networks volatile and interaction like ajax and Flash between user and server is desired these days.

Low Latency/Pseudo-Distributed: - clients need to transfer network structure data from accepted servers to start out anonymity communication. One illustrious example is that the Onion Router.

High latency/Distributed: - there's no central server to store data of anonymous network. Each node among network is adequate others. Tarzan and Morph combine are such style of implementation.

2.3 Security Threats and Limitations

Anonymous networks are vulnerable for various attacks those are listed below:

Message coding attack: - during this attack, messages that don't amendment their cryptography may be derived through the network by pattern matching.

Message length attack: - This attack examines the length of a message because it travels through the network.

Replay attack: - an assailant replays information packets and waits that focus on node processes an equivalent packet repeatedly, so sanctioning the attacker to correlate incoming and outgoing packets.

Collusion attack: - This happens if a particular variety of concerned parties collude to interrupt the anonymity of connections.

Flooding attack: - anonymity is sometimes achieved with reference to a particular cluster. During this attack, an resister floods the system to separate bound messages from the cluster.

Message volume attack: - during this attack, it's tried to observe an end-to-end association by observant the message volume at the endpoints.

Timing attack: - A temporal order attack tries to look at the period of an association by correlating its institution or release at the doable endpoints.

Profiling attack: - A profiling attack tracks users over long-run periods. It's essentially a mixture of the temporal order and message volume attack over a protracted time.

First 2 sorts of attack may be prevented from re-encrypting message once transmittal between nodes. artefact and chunk ways may be applied to form all messages flatten also. Maintain a brief information base to manage processed message may be wont to stop replay attack.

Decentralized network architecture will effectively stop Flooding attack. Message volume, temporal order and identification attack area unit traffic analysis attack from network wide scale. As long as attacker's area unit designated uniformly haphazardly to be an area of active set and sessions may be known across path reformations, the degree of anonymity of any sender can degrade vulnerable.

But to attain network wide scale analysis attack or recorder attack is expensive. It's nearly impractical to pay an outsized quantity of your time to identify the relation between sender and receiver in web scale that contains many hosts and interconnected globally. Supported this assumption, anonymize network is feasible. Plenty of implementation has been developed recently.

3 Anonymizing Networks Based on Centralized Approach

In this section we will investigate the centralized approaches for anonymizing networks.

3.1 Anonymizer and SafeWeb

Anonymizer offers kind of services embrace proxy server, encrypted email so on. Anonymizer can access web on behalf of real user. Some dynamic content like JavaScript, Java applets and Flash are filtered out, since knowledge exchange which can cause info outpouring are required for these dynamic applications.

From security point of view, centralized service is weak moreover. Initial of all, we should always have a doubt however will we tend to trust proxy service? Will your service neutral? However you are able to prove your service isn't compromised once clients are accessing? Second weakness is mortal will determine requestor using the message volume attack. As an example, mortal will analysis proxy's in and out traffic to match messages that consumer has an equivalent packet size. Third, consumer principally browses web content through links at intervals page. Mortal could extracts this info and trace users' pattern exploitation machine learning technology. Fourth, centralized server may be a single purpose of failure. Mortal could launch a denial of service attack to require down proxy. Or receiver will merely block all packets transmitted from proxy. Following figure 2 shows the structure of this kind of networks:

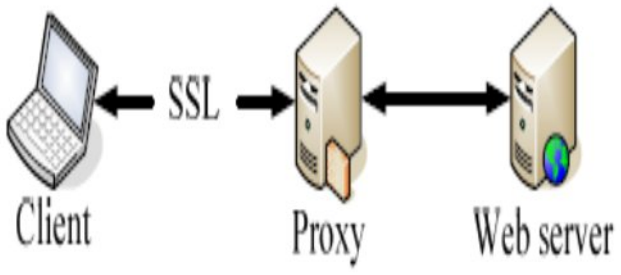


Figure 2: Structure of SafeWeb

3.2 Crowds

Crowd is nothing but the proposed projected anonymity network that provides probable innocence within the face of an outsized range of attackers. Crowd is very important because it introduced the construct of users mixing into a crowd of computers, and lots of the ideas employed in later systems.

The main plan behind Crowds anonymity protocol is to cover every user's communications by re-routing packets indiscriminately inside a bunch of users. User will register himself to a Crowd. All the opposite users area unit notified then. The request message from leader will be sent out from indiscriminately elite node inside Crowds. From outside world, it's tough to inform who the real leader is. For instance as showing in figure 3, node five registers itself and retrieves info from server to affix a bunch. Node five routes request to indiscriminately designated node three. Node three randomly decides relay this message or send. During this case, node 3 decides to relay to node 1.Node one determined to route message to node 2. Finally, node 2 sends out the request on behalf of node 5.

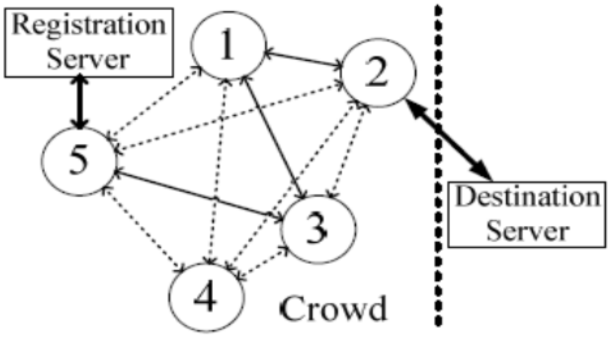


Figure 3: Example of Crow Network

The advantage of Crowd over Anonymizer is although one or a couple of number of nodes is subverted; the system will still give some extent of anonymity. The idea of Crowd is opposer cannot adversary the traffic at intervals cluster. Since, attacker will reckon the time of a specific message undergo every node. The node that has highest rank might be initiator. The registration server may be a single also of failure similarly.

4 Anonymizing Networks Based on distributed Approach

In this section we will investigate the centralized approaches for anonymizing networks

4.1 Chaum's MIX

The main plan is to use a network of proxy servers. First, initiator randomly chooses a path at intervals combine to route message. Based on the chosen proxy nodes on path, initiator encrypts the message using corresponding nodes' RSA public key. Once routing, every proxy will the foremost the foremost out layer of the message. Finally, the message is shipped out to destination server till all layers are patterned out by corresponding nodes. The return message will route back to instigator in reverse manner. In MIX, every node solely has plan concerning its precursor and successor.

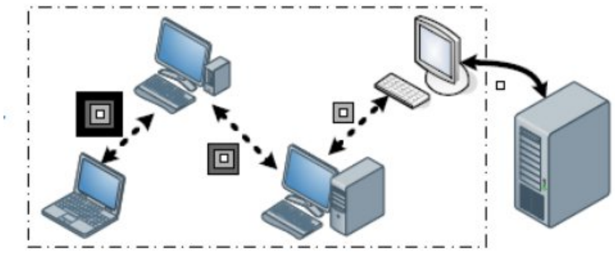


Figure 4: Architecture of distributed networks

Not solely sender obscurity however conjointly receiver obscurity is planned by Chaum. The hidden receiver will wrap his address in RSA public keys we same manner we have a tendency to did. The wrapped packets are often distributed to users who wish to request this hidden service. User can use this wrapped packet as header of his own message to send.

To improve anonymity, junk are often added to message whereas routing to cover its fingerprint and create all messages in same size. To form adversary harder to trace message, every node could delay message, and send messages in batch. Node will send dummy messages randomly to form eavesdropper confuse.

However, there are still many weaknesses are known within the classic combine network. Combine provides low level of protection on unlinkability. The nature property of RSA brings such weakness. Active attacker will inject a duplicated message into combine node to seek out the route that contains 2 same messages [11].

Since combine nodes haven't any plan concerning the payload in every message, they'll not sight active attack. Lots of recent anonymity network systems are supported the concept of combine, like onion routing, Mixminion, Tarzan.

4.2 The Onion Router (Tor)-

Tor is the implementation of second generation onion routing supported classic combine. It had been originally sponsored by United States naval laboratory, and so became a project of Electronic Frontier Foundation. In theory, Tor isn't a completely distributed system. Since there are some central servers take the responsibility to take care of the topology of the anonymous network. Tor works like Napster.

4.2.1 Architecture and Design:-

Tor provides "hidden server". Hidden service might permit Tor users to line up an internet site wherever individuals publish material without concern concerning censorship.

1. Server picks some introduction points and builds circuits to them.

2. Server advertises his hidden service "XYZ.onion" at the db.

3. Alice hears "XYZ.onion" exists, and she or he requests info from db.

4. Alice writes a message with rendezvous purpose to hidden server through introduction purpose.

5. Alice and hidden server validate one-time secret in rendezvous purpose.

6. Tor circuits established between Alice and hidden server.

Following figure 5 shows the Tor network:

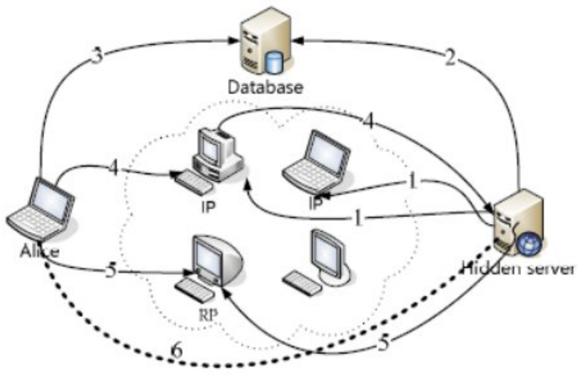


Figure 5: Tor Network

Nobody would be able to verify who was giving the location, and no-one who offered the location would apprehend who is visiting. to produce hidden service, an external server is desired to store some info of the service. Clients will retrieve this info from server to send request.

4.2.2 Analysis of Security

The directory server acts as an hypertext transfer protocol server, clients will fetch current network state and router list. Presently there are three directory servers globally and maintain a homogenous directory list. The node that needs to be an onion router and be more to OR list in directory server should be approved by directory server administrator. The ORs ought to periodically update state info and validate themselves using keys with directory servers. Directory is cached the same as Tapestry mechanism in every Onion Router to avoid the performance bottle neck.

The topology is comparatively static. Adversary will take down key onion routers and directory servers, or snoop on them. Dummy messages ar used to cowl network traffic; however dummy messages bring an excessive amount of over head. Since each node participated node has got to send dummy messages.

Several web applications directly send DNS requests while not invoke Tor's native proxy. This could leak some clues to snooper, thus sometimes Tor is companied with Privoxy. After 0.2.0.1-alpha, Tor has enforced its own DNS service. Peer to look anonymous network ar planned to unravel weaknesses in centralized anonymity network.

4.3 MorphMix and Tarzan

Tarzan is nothing but the peer-to-peer MIX network. It was introduced by researchers from Massachusetts Institute of Technology and New York University in the year 2002. Tarzan provides anonymous service at transport level, thus applications repose on the highest will transparently use anonymous communication. The implementation of MorphMix is similar to the Tarzan.

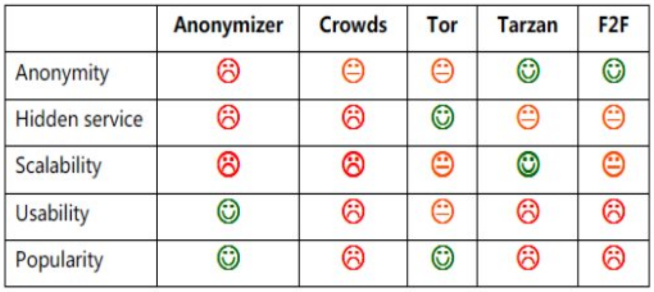
4.3.1 Security Analysis

The initiator could select subverted nodes in mimic in high probability [5]. The subverted node could only transmit information to alternative subverted nodes. Then, adversary will have some plan regarding who is talking to whom. Traffic analysis of a user's links by her ISP might simply show that she is automatically forwarding files. One answer resolution, enforced in WASTE, is to send and receive to add stream of mindless information, in order that traffic analysis cannot find whether or not significant information is being transmitted at any given time [5]. Another chance would be to feature artifact to files.

5 CONLCUSION AND FUTURE WORK

In this investigation study we presented details of anonymizing networks, their types and their security concerns etc. We studied the both centralized as well as distributed approaches for anonymizing networks. As per our study we find the in distributed approach, basic anonymity is preserved better. Tor supports hidden server. Owing to volatile of distributed system, Tarzan and F2F network can't support this perform tolerably. There not doubt centralized approaches can meet performance bottleneck that

have an effect on its quantifiable. For F2F (Friend to Friend) network, it's laborious to use since the network is growing too slow. From usability and recognition purpose of read, the majority like better to use proxy which may be simply found each wherever. Thousands of users are using Tor everyday to visit Wikipedia or expurgated sites. I can't notice any implementation of Tarzan and Crowds networks.



	Anonymizer	Crowds	Tor	Tarzan	F2F
Anonymity	☹	😐	😐	☺	☺
Hidden service	☹	☹	☺	😐	😐
Scalability	☹	☹	😐	☺	😐
Usability	☺	☹	😐	☹	☹
Popularity	☺	☹	☺	☹	☹

With the event of web more and a lot of folks become aware about their non-public info leaked. A way to preserve anonymity is becoming a hot topic. Nowadays, implementations like Tor are protective thousands of folks' lifestyle and supply people opportunities of freed from speech. Anonymous networks are studied over twenty years. It is evolving from centralized to completely distributed, from high latency to low latency. However, supported the analysis of existing systems, there's no good answer nevertheless.

6 REFERENCES AND BIBLIOGRAPHY

[1] D. Clark. Design Philosophy of the DARPA Internet Protocols. In *Proceedings of the ACM Special Interest Group on Data Communications*, pages 106–114, August 1988.

[2] M. Allman and V. Paxson. Issues and Etiquette Concerning Use of Shared Measurement Data. In Proceedings of the ACM SIGCOMM Internet Measurement Conference, page To appear, 2007

[3] Anonymous P2P. (2008, March 23). In Wikipedia, the Free Encyclopedia. Retrieved 08:00, March 25, 2008, from

[4] A. Pfitzmann and M. Hansen, Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology,Retrieved 15:00, May 7, 2008, from

[5] J. Brickell and V. Shmatikov. The Cost of Privacy: Destruction of Data-Mining Utility in Anonymized Data Publishing. In Proceeding of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pages 70–78, 2008.

[6] M. Rennhard, S. Rafaelit, L. Mathyt, B. Plattner and D. Hutchisont, an Architecture for an Anonymity Network. In *Proceedings of the IEEE 10th Intl. Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises.*

[7] George Danezis, Claudia Diaz. A Survey of Anonymous Communication Channels. Microsoft Research Technical Report (MSR-TR-2008-35). January 2008.

[8] M. Wright, M. Adler, B. Levine, and C. Shields. An analysis of the degradation of anonymous protocols. Technical Report 01-??, April 2001. University of Massachusetts, Amherst.

[9] B. Ribeiro, W. Chen, G. Miklau, and D. Towsley. Analyzing Privacy in Enterprise Packet Trace Anonymization. In Proceedings of the 15th Network and Distributed Systems Security Symposium, to appear, 2008.

[10] J. Mirkovic. Privacy-Safe Network Trace Sharing via Secure Queries. In Proceedings of the 1st ACM Workshop on Network Data Anonymization, October 2008.

[11] A. Narayanan and V. Shmatikov. Robust De-anonymization of Large Sparse Datasets. In Proceedings of the 2008 IEEE Symposium on Security and Privacy, pages 111–125, 2008.

.

.