Intersection Attacks on Anonymous Microblogging

Minh Tung Tran

May 17, 2021

1 Introduction

When accessing a resource on the Internet, users cannot hide from every other entity that is also in the global network, especially ones at internet service provider-grade can keep logs of all clients' traffic, also identify each one of them by IP addresses. An adversary can even intercept, monitor, and analyze traffic patterns to and from a targeted IP address. This raises concerns about Internet privacy since it suppresses freedom of Internet usage and opinion expression, where the network administrator is being controlled by opposing organizations.
Anonymous communication techniques have been studied since some time ago to fight network surveillance. Anonymous communication usually comes at the cost of latency, cryptographic computation power, and user base size, therefore a dedicated system is designed to make this trade-off applicable to a particular use. The popular Tor network should consist of several thousand relays and multi-layer encryption to protect client anonymity but provides low-latency communication [3], while other mix networks, in contrast, may have higher latency due to long chain of proxy servers, time-consuming shuffling and delaying mechanisms, still require much smaller anonymity sets to break the link between sent and received messages [4]. Tor is suitable for short-time and one-time communications such as web browsing, but clients using Tor for repeated communications are vulnerable to long-term intersection attacks and statistical disclosure attacks, which, for instance, can be performed through measuring uptime and downtime statistics due to the fact that clients do not constantly participate in the network. The disclosure of the connection between sender and receiver accumulates over time as the attacker keeps collecting this data and intersecting groups of suspects until one client stands out from the others.
In this bachelor thesis, we will investigate the efficiency of intersection attacks to break the sender anonymity in an anonymous microblogging scenario. Also, we will evaluate the ability of existing solutions like TASP [1] and Buddies [5] to resist this attack.

2 Background

Typically, one or more proxy servers can be used for private communication between clients instead of "direct" communication. By using a chain of proxy servers known as Mixes these communications can even harder to be traced, which shuffles and reorders incoming messages before sending them to the destination. Messages can usually be encrypted in multiple layers beforehand so that each proxy is able to remove only one of these layers before transmitting messages to the next node, which makes the network resistant even to malicious mix nodes. There are also several well-known basic techniques that counter network traffic analysis.

Cover Traffic: Since messages are all encrypted, content-based linkability is not possible, therefore real messages and cover messages must be packed so that they are indistinguishable from the adversary. The overhead of cover traffic must also be considered in practical systems.

Traffic Delay: Users usually have their own pace of communication, thus it is possible for the adversary to match the rate of messages sending on incoming channels with one of receiving on outgoing channels in order to find the connection between sender and receiver. Accordingly, the transmitted data entering and leaving the system at the same rate provide no useful information to the adversary. This method obviously slows down the communication.

Besides, it is clearly beneficial to group clients with similar communication patterns into anonymity sets with a small expense of effectiveness so that the adversary cannot exclude the unrelated ones out of a set of suspects, for example, who communicate as fast as the targeted one. However, practical systems must cope with the fact that clients do not constantly participate in the network, users can therefore lose anonymity over time.

3 Related Work

In 1981 David Chaum [2] proposed Mixes as the first approach to anonymous communications, which are relaying routers using multi-layer asymmetric cryptography, shuffling, and reordering techniques to break the connection between input and output messages, thus anonymize the communications. The work served as a foundation of many subsequent anonymity designs such as Tor [3] or Mixminion [8].

In the work by Hayes *et al.*, they introduced two methods that preserve the anonymity of clients in groups: When clients submit their first message, they are put into possibilistic anonymity sets whose members also send messages in the same round, which is a defined time length. Clients in an anonymity set are required to send a message in every subsequent round or they are removed from the set. There can be a threshold specified for an anonymity set, like in the work of [5], below which the system will block clients from posting messages to maintain anonymity.

TASP is a protocol run by an ACS, capable of creating anonymity sets based on clients' communication patterns, thereby hiding their identities efficiently from network surveillance. The system operates in two phases, a learning phase and an online phase. The learning phase is the initial phase when clients are required to send either a real message or a cover message in every round so that in the meantime the system tries to learn the communication pattern of each client in order to put them into their appropriate anonymity sets. There comes the dynamic time warping algorithm as a grouping mechanism for calculating the similarity be-

tween two sequences of message send time. After the anonymity sets are formed the system closes its entry for newcomers and moves into the online phase, where cover traffic is no longer needed, however, clients are still required to send messages in each round in order to maintain the pattern of the group, otherwise they are removed permanently from the system. Another work by Wolinsky *et al.* [5] suggested an approach to take the adversary's perspective as a means of avoiding false assumptions of global information which can be used as a mechanism allowing clients to communicate only when it is safe. In addition, clients are masked by multiple pseudonyms when posting so that this virtually creates larger sets of suspects for the adversary, thus hinders the effective surveillance on outgoing traffic.
Danezis *et al.* [7] showed that messages sent by bi-directional ACSs can be linkable and the attack will be efficient as it takes only linear time to correlate a sender with its receivers.

4 Research Problem

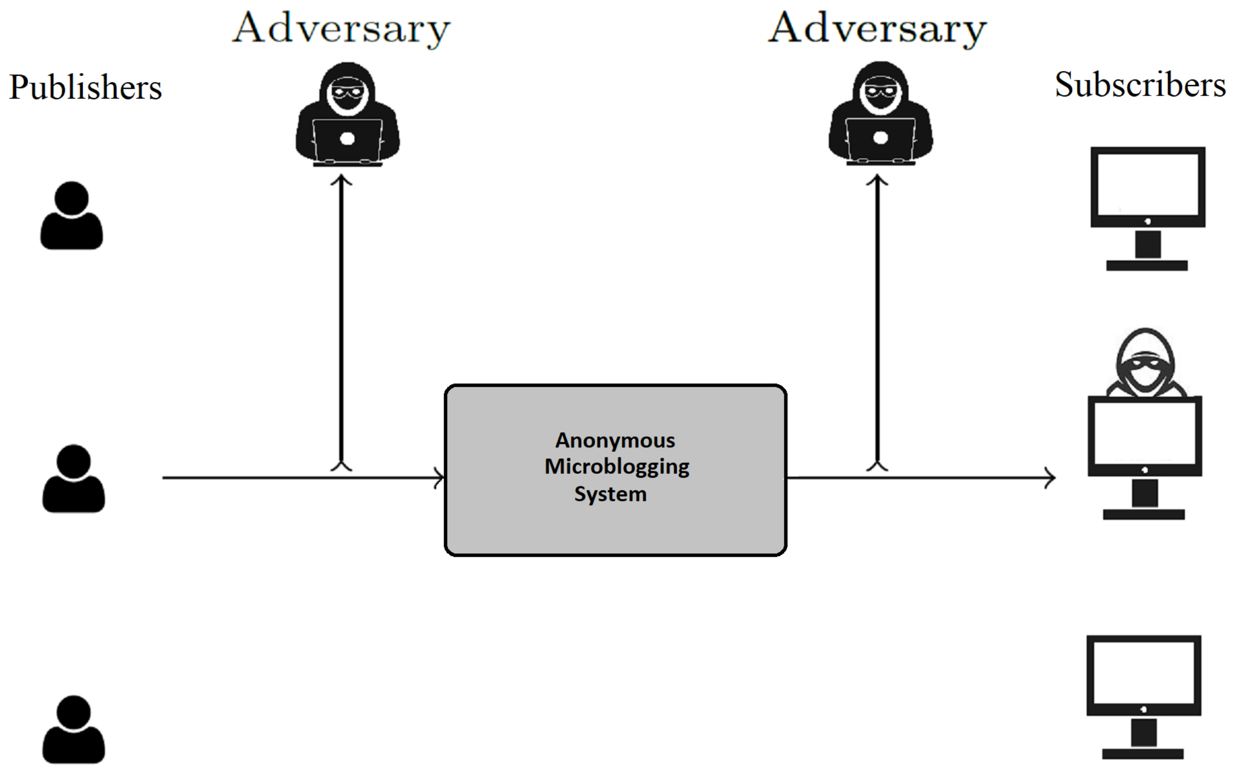

Figure 1: Publishers blog anonymously via an anonymous microblogging system. The attacker eavesdrops on all incoming and outgoing messages and also subscribes to all topics.

We consider an anonymous microblogging system that allows users to publish messages on publicly known topics without revealing their identities. This system is assumed to be a trusted black box. It requires clients to communicate in rounds, by sending either a real message or a cover message, in case they do not have any useful request to post. Each client sends one message per round. Messages are all indistinguishable from a public adversary because of message-content encryption. After receiving messages from all clients, the system encrypts the messages and forwards plain text messages to the subscribers, and ends the round.

We assume a global passive adversary with an ability of network surveillance by monitoring all incoming and outgoing messages on all user and server lines, but unable to intercept the traffic by dropping, altering transmitted data packets or to gain intelligence about the actual content of messages while transmitting due to end-to-end message encryption. Also, the adversary can subscribe to all topics to get all published messages every round. Over time the adversary records for each user every possible topic based on active topics when the user is online and repeatedly intersect sets of suspects to point out the user's interest.

5 Methodology

In this thesis, we are interested in breaking the anonymity of senders who use an anonymous microblogging system to spread their own words in public discussions. We describe an approach that the adversary uses to reveal the interests of the user.

To launch the intersection attack in the mentioned scenario, the adversary records traffic in very small and same-length time intervals as rounds. Let O_i be the set of online users in round i. By intersecting for n rounds the set $S_m = \bigcap_{i=0}^{n} O_i$ of senders who possibly posted the message m, the adversary finds the minimized set of sender suspects who are online when the message m is posted. Besides, the adversary can perform analogous analysis regarding the number of packets, rate of sending, and intersects these sets altogether to deanonymize the sender.

We will measure the effectiveness of long-term intersection attacks in the particular context of microblogging systems as well as the efficiency of state-of-the-art systems as the main objective of this research by answering how long it takes attackers to reveal the interest of a publisher on blogging platforms. We will determine thereby the extent to which the current defense techniques can provide in this specific scenario.

6 Evaluation

For the evaluation, we use a real dataset from Twitter and simulate the attack trying to identify users posting to the social microblogging platform. We measure thereby the required time of the deanonymization against varied solutions, assess by that the efficiency of each solution regarding its resistance against the attacks. To measure the performance of a system, we consider the average delay between message sending and receiving that clients have to tolerate to maintain anonymity, the overhead produced by cover traffic, and also the system's scalability.

Our baselines can be TASP [1] and Buddies [5], which use methods resembling possibilistic anonymity sets formation to sustain the sender anonymity in groups.

7 Timetable

Month	Task	Goal
Start	Research problem determination	Official begin of work
1	Literature research	Understand how the problem could be solved in prior work and be familiar with the present state of the art system
2	Implementation	Implement the system
3-4	Simulation	Simulate system's behaviour and collect results
4-5	Evaluation	Review, analyze, summarize the simulation results, compare them with ones of prior work
5-6	Finalizing the thesis	Submit the thesis

References

[1] Jamie Hayes, Carmela Troncoso, and George Danezis. *TASP: Towards Anonymity Sets that Persist.* WPES '16: Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic SocietyOctober 2016 Pages 177–180.

[2] David Chaum. *Untraceable electronic mail, return addresses, and digital pseudonyms.* Commun. ACM 24(2), 84–88 (1981).

[3] Roger Dingledine, Nick Mathewson and Paul F. Syverson. *Tor: The Second-Generation Onion Router.* June 2004

[4] Oliver Berthold and Heinrich Langos. *Dummy Traffic against Long Term Intersection Attacks.* In: Dingledine R., Syverson P. (eds) Privacy Enhancing Technologies. PET 2002. Lecture Notes in Computer Science, vol 2482. Springer, Berlin, Heidelberg.

[5] David Isaac Wolinsky, Ewa Syta, and Bryan Ford. *Hang With Your Buddies to Resist Intersection Attacks.* ACM CCS'13, Nov 04-08 2013, Berlin, Germany.

[6] David Chaum. *The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability.* J. Cryptology 1(1), 1988, pp. 65-75.

[7] George Danezis, Claudia Diaz, and Carmela Troncoso. *Two-Sided Statistical Disclosure Attack.* N. Borisov and P. Golle (Eds.): PET 2007, LNCS 4776, pp. 30–44, 2007.

[8] George Danezis, Roger Dingledine, Nick Mathewson: *Mixminion: Design of a type iii anonymous remailer protocol.* In: IEEE Symposium on Security and Privacy, pp. 2–15. IEEE Computer Society Press, Los Alamitos (2003) N. Borisov and P. Golle (Eds.): PET 2007, LNCS 4776, pp. 30–44, 2007.

17.05.2021

Date, student's signature

Date, supervisor's signature