

Pomona College
Department of Computer Science

Decentralized Group Management in Dissent

Eleanor Cawthon

April 25, 2015

Submitted as part of the senior exercise for the degree of
Bachelor of Arts in Computer Science
Professors Bryan Ford and Tzy-Yi Chen, advisors

Copyright © 2015 Eleanor Cawthon

The author grants Pomona College the nonexclusive right to make this work available for noncommercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the author. To disseminate otherwise or to republish requires written permission from the author.

Abstract

Decentralized approaches to private communication exhibit tradeoffs between decentralization and scalability. We present a protocol for achieving the best of both worlds.

added to make it compile, this abstract is not a draft

Contents

Abstract	i
List of Figures	v
List of Tables	vii
Preface	ix
1 Background and Related Work	1
1.1 Anonymity Designs and Threat Models	1
1.2 Distributed Decision-Making	4
2 Goals and Non-Goals	9
3 Protocol Description	11
4 Security Properties and Correctness	13
5 Evaluation	15
6 Conclusion	17
7 Bibliography	19
Bibliography	21

List of Figures

List of Tables

Preface

Chapter 1

Background and Related Work

Anonymous communication significantly constrains the ability of oppressive regimes and vigilante groups alike to suppress dissent. Newly available information about vulnerabilities and global-scale surveillance in today's centralized internet infrastructure has rendered a swath of anonymity tools obsolete, and poses a significant threat to those that remain.

A trustworthy anonymity tool in the post-Snowden era must be resilient to both surveillance and censorship: It should guarantee its users' anonymity even in the face of a global passive adversary, and it should be unrealistic for such an adversary to simply prevent users from accessing it. A useful anonymity tool must also perform with reasonably low latency - a property which often trades off with security and availability.

This review will first examine the existing anonymity tools The Onion Router (Tor) and Dissent, considering their ability to provide strong anonymity guarantees. Higher performance versions of both Tor and Dissent, however, rely on well-known relay servers which present challenges for availability. Section 1.2 will examine decentralized, peer-to-peer techniques that might be used to improve Dissent's availability.

TODO:
This is just what I turned in last semester; haven't reworked it yet

1.1 Anonymity Designs and Threat Models

Every anonymity tool shares one basic goal: Given a set of assumptions about an adversary's capabilities, an anonymity tool provides a way for a user to broadcast a message without the adversary being able to discover the author of the message. To illustrate the general approach and some

common security assumptions, we first consider The Onion Router (Tor), the most widely used anonymity tool today[For14]

1.1.1 Onion Routing with Tor

Tor aims to provide an anonymity service that, to the end user, behaves like a one-hop proxy: If Alicia wants to send an HTTP request to Badru using Tor, Alicia sends a request through Tor, Tor forwards the request to Badru, Badru replies to Tor, and Tor forwards the response to Alice. Under the surface, when Alicia’s traffic enters the Tor network, it is encrypted and transmitted among several ”onion routers” before reaching an ”exit relay”, which decrypts the request and passes it onto Badru. Each intermediate onion router only knows the next hop in the path from Alicia to Badru - no single node knows its traffic originated at Alicia or is en route to Badru - so no one in the network knows the complete path.

Tor provides anonymity from an adversary who “can observe some fraction of the network traffic; who can generate, modify, delete, or delay traffic; who can operate onion routers of [their] own; and who can compromise some fraction of the onion routers”[DMS04]. If an adversary can observe much more than a small fraction of traffic, or if the adversary controls many colluding nodes, other attacks become possible, and the anonymity guarantees no longer hold. We now know that the U.S. National Security Agency actively uses such attacks, and so a new protocol is necessary in order to remain anonymous from the N.S.A.

1.1.2 New Threat Models

To provide anonymity from an adversary like the N.S.A., a modern anonymity protocol must protect against several forms of attacks. Feigenbaum et. al.[FF13] highlight five specific attacks to which onion routing is vulnerable:

Global traffic analysis: If the adversary can monitor most of the traffic on the internet globally, the adversary can with high probability see the link from Alicia to the Tor network and from the Tor exit relay to Badru. This means the adversary can observe that the messages Alicia sends correspond to messages Badru receives some short amount of time later. Even if the messages themselves are encrypted, the adversary can analyze the lengths and other metadata about the messages to correlate this traffic.

Active attacks: Global traffic analysis attacks only require the adversary to be able to monitor global traffic. If the adversary can also modify or generate traffic, several other attacks are possible. The adversary can launch *man-in-the-middle* (MITM) attacks in which it impersonates Alicia, Badru, or one or more Tor nodes. The adversary can launch *Sybil* attacks, in which many different Tor clients controlled by the same adversary join the network as individual clients. Either of these can be used to create *Denial-of-Service* (DoS) attacks, which might either prevent users from connecting to Tor at all, or force Tor traffic to go through particular, potentially adversary-controlled, Tor nodes — de-anonymizing the users. ‘

Intersection attacks: In general, it is possible to tell when users are using an anonymity service — the anonymity comes from the difficulty of linking any particular user to particular messages produced by the service. Over time, however, the client set of an anonymity service is unlikely to remain fixed. A passive adversary monitoring the outputs of an anonymity service as well as the set of users connected can narrow the set of users who potentially, for example, updated a particular blog with a static pseudonym, by excluding users not online during all updates to the blog.

We now turn to an anonymity service designed to be resilient to these threat models.

1.1.3 Dissent

Dissent is an alternative to Tor that provides provable anonymity even if only one server in the network is honest[CGF10]. In its present form, a Dissent cluster consists of m servers and n connected clients[WCGFJ12]. Provable anonymity is achieved through a modified version of the Dining Cryptographers problem[Cha88]: each client i shares a secret K_{ij} with each server j . Communication proceeds in rounds, within which each client has a designated k -bit slot. Before any messages are sent, a secure shuffle[Nef01] assigns each client to a slot so that the owner of a slot is the only node in the system which knows who owns that slot. In any client s ’s slot, every client and every server generates k bits of random noise seeded with each of its shared secrets K_{ij} , and combines these with an exclusive or (xor) operation to produce that node’s ciphertext. Client s also combines (via xor) a k -bit message with its noise to create its ciphertext. The combination (via xor) of all clients’ and servers’ ciphertext includes the noise stream associated with each shared secret twice, and so all noise cancels out and client s ’ message is revealed. However, since deciphering this requires the participation of all

nodes in the system, it is impossible to tell which client transmitted a message in a given slot. Dissent also incorporates an accountability mechanism, allowing any node that disrupts the protocol to be detected and removed from the cluster [CGWF13].

The original Dissent was fully peer-to-peer [CGF10]. The shift to a client-server model allows for significantly improved performance, but it introduces several new concerns, particularly relating to misbehaving servers, a new class of DoS attacks, and group formation.

1.1.4 The Trouble with Relays

One potential approach to making Dissent widely available would be to have well-known, globally dispersed Dissent servers available for clients to connect to, similar to the current state of Tor. Any such well-known server list, however, is susceptible to blocking by internet service providers. It would therefore be preferable to have servers be short-lived, or at least not well known. Since Dissent takes place over regular TCP connections, detecting that the protocol is being executed without knowledge of the addresses of servers would be difficult to accomplish without a great number of false positives [HBS13], so this may be enough to realistically preclude most attempts to block access to the protocol entirely. Additionally, while the current version of Dissent guarantees that malicious servers cannot deanonymize a client without the cooperation of all servers, and guarantees that disrupting servers can be exposed, it provides no way to remove a disrupting or malicious server from the system.

One way to resolve these problems would be to have clusters of Dissent clients elect temporary servers among themselves, allowing servers to either step down (e.g., by going offline) or be impeached by some portion of the clients. Doing so in a truly decentralized and fair fashion is a non-trivial problem. We consider several other areas of research relevant to solving it.

1.2 Distributed Decision-Making

In a peer-to-peer Dissent protocol that does not specify leaders or servers prior to starting, there must be some way for participants to collectively decide on features of the cluster, such as which nodes will act as servers. In this section, we examine various existing approaches to distributed decision-making problems. We first consider several potential design goals, and then discuss particular approaches to these problems.

1.2.1 Potential Goals

Verifiability: A protocol is verifiable if its output can be inspected to confirm that the protocol was carried out correctly. A simple example of this is signing a message with the private key associated with a well-known public key: Anyone who knows the public key can verify the validity of the signature. Dissent [CGWF13] and the Neff shuffle [Nef01] both use zero-knowledge proofs to achieve verifiability.

Accountability: In the context of Dissent, accountability refers to the ability of a protocol to detect and exclude participants who disrupt the protocol [SCGW⁺14], while proving that the disruptor did indeed disrupt the protocol. Such a mechanism is necessary in peer-to-peer protocols like Dining Cryptographers in which a single disruptor can make the result of a round unusable. In Dissent, accountability checks occur without revealing the link between any message and its sender — moreover, it is not possible to deliberately exclude a participant on the basis of valid messages the participant sends. That is, the Dissent accountability mechanism does not break anonymity.

Forward Progress: A protocol that guarantees forward progress given certain conditions will eventually make progress as long as those conditions are met. More strict bounds on what “eventually” means are possible. In the original Dissent, for example, forward progress can be guaranteed if all clients follow the protocol and remain online, but not otherwise: The accountability mechanism was so arduous that f disrupting clients could prevent any messages from being transmitted for f hours [CGWF13]. Protocols that make use of quorums rather than being fully peer-to-peer are able to provide stronger guarantees of forward progress [Lam98].

Anonymity: A protocol guarantees anonymity in some operation a client can complete if the output of that operation is unlinkable (or, more precisely, cryptographically very difficult to link) to the client who completed it [CGF10]. Dissent makes use of pseudonyms to provide this, separating the protocol correctness and accountability layer from the layer in which messages are revealed. Group membership voting could conceivably take place at either.

1.2.2 Consensus Protocols

Distributed consensus protocols allow groups of nodes to come to an agreement on canonical values. For example, in a distributed database, if an unreliable power supply causes some portion of servers to be offline for each of several transactions, these protocols allow the servers to reconcile their records so that all servers agree on the transaction history. The problem was popularized by [Lam98], which proposed the framing and solution now known as Paxos: A Paxos cluster that consists of $2f + 1$ nodes must have a *quorum* of $f + 1$ participating nodes at any given time. Transactions occur in three phases: First, the single current designated leader (Proposer) proposes the n th change. Next, if no other participants (Acceptors) have received a proposal numbered higher than n , the Acceptors promise to ignore future lower numbered requests. Finally, upon receiving $f + 1$ Promises, the Proposer declares success to all Acceptors. This allows the cluster to maintain a consistent record of transactions as long as a quorum is present.

Paxos and many similar protocols makes the simplifying assumption that all nodes in the system are honest — the only faults considered are those triggered by nodes suddenly going offline. If nodes may be malicious, they may “fail” not just by disappearing, but by forging messages in an effort to influence the consensus value. *Byzantine* consensus protocols allow the honest nodes in a system to arrive at a canonical value, so long as some minimum portion of nodes are honest. The original Paxos can accommodate Byzantine failures if an additional verification stage, in which all Acceptors communicate with all other Acceptors in order to detect equivocation, is added before the final step [CL99]. Additional optimizations to regular and Byzantine Paxos have also been developed [Lam06]. If the adversary can not only send arbitrary messages but also monitor messages exchanged among other nodes, additional attacks are possible. One approach to this divides the nodes into small quorums in an effort to contain malicious nodes [KLST11] while also providing better scalability than solutions that require all-to-all communication to thwart equivocators.

In both its standard and Byzantine formulations, the distributed consensus problem assumes discrepancies in the record will only be due to faults — that is, each assumes all honest participants either agree on what the value should be or agree to accept the value reported by the nodes who do know the value. In the election of rotating leaders or servers, the correct value is not knowable a priori. If our leader election algorithm is modeled on other election protocols, it must be assumed that honest nodes may disagree on which servers they wish to elect.

1.2.3 Electronic Voting

Secure electronic voting systems have arisen largely out of a desire to retain secret ballots (no one should learn how a particular voter voted) while also guaranteeing accurate and fair counting of votes. Unlike distributed consensus protocols, secure electronic voting systems generally achieve their security properties through decentralization of trust rather than computation. They normally depend on a single executor of the vote aggregation protocol, using verifiability to ensure that each voter can be confident their vote was tallied fairly. Voting protocols can be evaluated in their provision of three different kinds of verifiability [KRS10]: *individual* verifiability ensures that a voter can verify their vote was included correctly. *Universal* verifiability requires that anybody can verify the election result correctly represents the collection of ballots cast. Finally, *Eligibility* verifiability allows anybody to verify that only eligible voters voted, and that each voter voted only once.

One solution is presented in [Nef01], and the initial assignment of pseudonyms in Dissent already uses a variation on this protocol. In the Neff shuffle, each voter encrypts their vote in such a way that the aggregator must permute the vote ciphertexts before being able to decrypt them. The result is a permutation which no one knows — a voter can verify that their ciphertext is present in the permutation, but gains no information about the correspondence between other ciphertexts and other voters. It is both individually and universally verifiable.

The individual verifiability of [Nef01] is based on each voter’s retention of their secret key. *Coercion-resistant* electronic voting protocols remain robust even if secret keys are compromised: In [JCJ05], the voter uses their secret key only to establish eligibility, at which point they are assigned a random element of a well known set to use in their actual ballot. The ballots are unlinkable to the secret keys, and there is no way for an outsider to confirm whether a particular random element corresponds with a particular voter. This protocol achieves strong resistance to multiple kinds of coercion by deliberately weakening the eligibility verification property to depend on trust in the “registrar” who validates credentials and assigns the voting keys, preventing “forced-abstention” attacks (in which the adversary demands a voter simply not participate) by making it impossible for outsiders to verify the set of voters.

These protocols provide useful templates for how a distributed voting protocol might accomplish similar security properties.

Chapter 2

Goals and Non-Goals

Chapter 3

Protocol Description

Chapter 4

Security Properties and Correctness

Chapter 5

Evaluation

Chapter 6

Conclusion

Chapter 7

Bibliography

Bibliography

- [CGF10] Henry Corrigan-Gibbs and Bryan Ford. Dissent: Accountable anonymous group messaging. In *Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS '10*, pages 340–350, New York, NY, USA, 2010. ACM.
- [CGWF13] Henry Corrigan-Gibbs, David Isaac Wolinsky, and Bryan Ford. Proactively accountable anonymous messaging in verdict. In *Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13)*, pages 147–162, Washington, D.C., 2013. USENIX.
- [Cha88] David Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, 1(1):65–75, January 1988.
- [CL99] Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance. In *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, New Orleans, USA, February 1999.
- [DMS04] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium*, August 2004.
- [FF13] Joan Feigenbaum and Bryan Ford. Seeking anonymity in an internet panopticon. *arXiv preprint arXiv:1312.5307*, 2013.
- [For14] Bryan Ford. Hiding in a panopticon: Grand challenges in internet anonymity, February 2014.
- [HBS13] A. Houmansadr, C. Brubaker, and V. Shmatikov. The parrot is dead: Observing unobservable network communications. In

- 2013 *IEEE Symposium on Security and Privacy (SP)*, pages 65–79, May 2013.
- [JCJ05] Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-resistant electronic elections. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, WPES '05, pages 61–70, New York, NY, USA, 2005. ACM.
- [KLST11] Valerie King, Steven Lonargan, Jared Saia, and Amitabh Trehan. Load balanced scalable byzantine agreement through quorum building, with full information. In Marcos K. Aguilera, Haifeng Yu, Nitin H. Vaidya, Vikram Srinivasan, and Romit Roy Choudhury, editors, *Distributed Computing and Networking*, number 6522 in Lecture Notes in Computer Science, pages 203–214. Springer Berlin Heidelberg, January 2011.
- [KRS10] Steve Kremer, Mark Ryan, and Ben Smyth. Election verifiability in electronic voting protocols. In Dimitris Gritzalis, Bart Preneel, and Marianthi Theoharidou, editors, *Computer Security ESORICS 2010*, number 6345 in Lecture Notes in Computer Science, pages 389–404. Springer Berlin Heidelberg, January 2010.
- [Lam98] Leslie Lamport. The part-time parliament. *ACM Trans. Comput. Syst.*, 16(2):133–169, May 1998.
- [Lam06] Leslie Lamport. Fast paxos. *Distributed Computing*, 19(2):79–103, October 2006.
- [Nef01] C. Andrew Neff. A verifiable secret shuffle and its application to e-voting. In *Proceedings of the 8th ACM Conference on Computer and Communications Security*, CCS '01, pages 116–125, New York, NY, USA, 2001. ACM.
- [SCGW⁺14] Ewa Syta, Henry Corrigan-Gibbs, Shu-Chun Weng, David Wolinsky, Bryan Ford, and Aaron Johnson. Security analysis of accountable anonymity in dissent. *ACM Transactions on Information and System Security*, 17(1):1–35, August 2014.
- [WCGFJ12] David Isaac Wolinsky, Henry Corrigan-Gibbs, Bryan Ford, and Aaron Johnson. Dissent in numbers: Making strong anonymity scale. In *Presented as part of the 10th USENIX Symposium*

on Operating Systems Design and Implementation (OSDI 12),
pages 179–182, Hollywood, CA, 2012. USENIX.