SHARETRACE: PROACTIVE CONTACT TRACING WITH ASYNCHRONOUS MESSAGE PASSING

by

RYAN TATTON

Abstract

Contact tracing is a non-pharmaceutical intervention that aims to control the spread of disease by identifying and quarantining infected individuals and those with whom they came in close contact. Numerous approaches to digital contact tracing have been proposed in the context of the coronavirus disease 2019 pandemic. Decentralized digital contact tracing limits the sharing of personal data, but none of these prior works have utilized non-diagnostic information *and* indirect contacts to effectively estimate infection risk. This work improves on prior efforts of ShareTrace by providing an asynchronous message-passing algorithm that permits a fully decentralized deployment. A reference implementation is provided and evaluated for accuracy, efficiency, and scalability.

Chapter 1

Introduction

Contact tracing is a non-pharmaceutical intervention that aims to halt the spread of infectious disease by identifying and quarantining individuals that have been physically proximal with the infected [19]. To combat the pandemic of coronavirus disease 2019 (COVID-19) [9, 28, 35], numerous approaches to *digital contact tracing* (DCT) have been proposed [5, 11, 21, 26, 32]. While the implementation details vary considerably, all approaches to DCT aim to mitigate the spread of infection by automatically informing individuals of their infection risk.

A popular form of DCT is *proximity tracing*, which uses device-to-device (D2D) communication [12] to approximate in-person interactions. While multiple protocols for proximity detection exist, Bluetooth Low Energy (BLE) is typically used because of its relative accuracy, energy efficiency, and broad support in mobile devices [21, 26]. Proximity tracing entails generating and exchanging pseudonyms (i.e., ephemeral identifiers, contact identifiers) between

nearby mobile devices. What differentiates DCT applications is how these pseudonyms are generated and utilized. *Decentralized DCT* determine an individual's contacts and infection risk locally, thus avoiding the aggregation of sensitive personal data. Afroogh et al. [1], Oyibo et al. [17], and Simko et al. [27] all find that privacy and security are paramount to the adoption of DCT, which is a key determinant of achieving epidemic control [19]. While decentralization is not sufficient for strong privacy and security guarantees, it generally makes attaining such guarantees more feasible.

In the *broadcast model* of decentralized DCT, an infected individual uploads their information to a central service that allows others to determine if they possess any of the pseudonyms belonging to that individual [21]. A major limitation of the broadcast model is that an individual's infection risk does not account for indirect contacts, which can substantially improve the effectiveness of DCT [19]. Moreover, the broadcast model assumes an accurate diagnostic test exists and is broadly accessible and trusted by the public. To address the limitations of the broadcast model, Ayday, Yoo, and Halimi [2] proposed ShareTrace, which uses a message-passing algorithm that incorporates non-diagnostic information and indirect contacts when estimating infection risk. However, the authors assume a centralized deployment, which exposes the entire contact network and personal data to a single entity.

Other approaches to *message-oriented DCT* [6, 22] provide decentralization, but do not account for non-diagnostic information and indirect contacts. Recently, Cherini et al. [5] proposed extending the broadcast model such that mobile devices also share the pseudonyms of their indirect contacts during

D2D interactions, but still depend on diagnostic testing. Gupta et al. [11] incorporate non-diagnostic information to proactively determine an individual's infection risk, but do not account for indirect contacts.

This work proposes an asynchronous formulation of the message-passing algorithm proposed by Ayday, Yoo, and Halimi [2], which permits a decentralized deployment of ShareTrace. In this way, this work addresses the limitations of other message-oriented DCT designs [6, 22] and more recent works [5, 11] that do not incorporate both non-diagnostic information and indirect contacts when estimating infection risk. While message passing has been studied under specific epidemiological models [13, 16], this work does not require such assumptions to infer the transmission of disease.

The remainder of this work is organized as follows. **??** begins with the algorithmic foundations of ShareTrace: the risk propagation message-passing algorithm. Risk propagation is first presented as a synchronous, offline algorithm, which is consistent with prior work [2]. **??** then provides an asynchronous formulation using the actor model. **??** evaluates a reference implementation of the proposed design. Various data distributions and contact network topologies are used to determine the parameter values that optimize asynchronous risk propagation for accuracy and efficiency. The runtime performance of the reference implementation is similarly evaluated. **??** includes prior designs and implementations, including the approach proposed by Tatton et al. [30]. **??** and **??** respectively describe the data structures and pseudocode conventions that are used throughout this work. Chapter 2 concludes with directions for future work.

Chapter 2

Conclusion

This work provided a decentralized design of risk propagation, the message-passing algorithm that powers the ShareTrace contact tracing application. Message reachability was introduced as a means of measuring the dynamics of message passing on temporal networks, such as contact networks. On a practical note, ShareTrace was contextualized as a mobile crowdsensing (MCS) application using the four-layered architecture developed by Capponi et al. [4]. A reference implementation of asynchronous risk propagation was implemented and used to find the values of the send coefficient and tolerance that optimize for accuracy and communication efficiency. Additionally, the scalability of the reference implementation was assessed. To ensure a fair evaluation, several types of contact network topologies and data distributions were utilized.

The following are subject to future work:

- Incorporate differential privacy techniques that are specifically designed for ACT applications, like ShareTrace, which utilize risk scores [23].

- Extend the calculation of risk scores to account for the transmission dynamics of the disease [7, 8].
- Formally define the security and privacy characteristics of ShareTrace, using the framework proposed by Kuhn, Beck, and Strufe [15] to characterize the latter.
- Integrate concepts from related approaches to ACT [5, 6, 11, 22].
- Explore the utility and feasibility of integrating decentralized technologies [3, 14, 25, 31, 33] and SSI [20, 24] into the design of ShareTrace.
- Conduct a simulation-based analysis of asynchronous risk propagation with COVI-AgentSim [10].

In May 2023, the World Health Organization (WHO) declared that COVID-19 is no longer a "global health emergency" [34]. However, as is evident throughout history, the risk posed by emerging pathogens persists [18, 29]. Thus, research on effective approaches, such as contact tracing, to preventing and mitigating future outbreaks remains critically important.

Bibliography

[1] Saleh Afroogh et al. "Tracing app technology: An ethical review in the COVID-19 era and directions for post-COVID-19". In: *Ethics and Information Technology* 24.3 (2022). DOI: 10.1007/s10676-022-09659-6 (cit. on p. 3).

[2] Erman Ayday, Youngjin Yoo, and Anisa Halimi. "ShareTrace: An iterative message passing algorithm for efficient and effective disease risk assessment on an interaction graph". In: *Proceedings of the 12th ACM Conference on Bioinformatics, Computational Biology, and Health Informatics*. 2021. DOI: 10.1145/3459930.3469553 (cit. on pp. 3, 4).

[3] Juan Benet. *IPFS - content addressed, versioned, P2P file system*. 2014. arXiv: 1407.3561 [cs.NI] (cit. on p. 6).

[4] Andrea Capponi et al. "A survey on mobile crowdsensing systems: Challenges, solutions, and opportunities". In: *IEEE Communaction Surveys & Tutorials* 21.3 (2019), pp. 2419–2465. DOI: 10.1109/comst.2019.2914030 (cit. on p. 5).

[5] Renato Cherini et al. “Toward deep digital contact tracing: Opportunities and challenges”. In: *IEEE Pervasive Computing* 22.4 (2023), pp. 15–25. DOI: 10.1109/mprv.2023.3320987 (cit. on pp. 2–4, 6).

[6] Hyunghoon Cho, Daphne Ippolito, and Yun William Yu. *Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs*. 2020. arXiv: 2003.11511 [cs.CR] (cit. on pp. 3, 4, 6).

[7] Luca Ferretti et al. “Digital measurement of SARS-CoV-2 transmission risk from 7 million contacts”. In: *Nature* 626.7997 (2024), pp. 145–150. DOI: 10.1038/s41586-023-06952-2 (cit. on p. 6).

[8] Luca Ferretti et al. “Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing”. In: *Science* 368.6491 (2020), eabb6936. DOI: 10.1126/science.abb6936 (cit. on p. 6).

[9] Alexander E. Gorbalenya et al. “The species severe acute respiratory syndrome-related coronavirus: Classifying 2019-nCoV and naming it SARS-CoV-2”. In: *Nature Microbiology* 5.4 (2020), pp. 536–544. DOI: 10.1038/s41564-020-0695-z (cit. on p. 2).

[10] Prateek Gupta et al. *COVI-AgentSim: An agent-based model for evaluating methods of digital contact tracing*. 2020. arXiv: 2010.16004 [cs.CY] (cit. on p. 6).

[11] Prateek Gupta et al. “Proactive contact tracing”. In: *PLOS Digital Health* 2.3 (2023), pp. 1–19. DOI: 10.1371/journal.pdig.0000199 (cit. on pp. 2, 4, 6).

[12] Michael Haus et al. “Security and privacy in device-to-device (D2D) communication: A review”. In: *IEEE Communications Surveys & Tutorials* 19.2 (2017), pp. 1054–1079. DOI: 10.1109/comst.2017.2649687 (cit. on p. 2).

[13] Brian Karrer and M. E. J. Newman. “Message passing approach for general epidemic models”. In: *Physical Review E* 82.1 (2010). DOI: 10.1103/physreve.82.016101 (cit. on p. 4).

[14] Navin Keizer et al. “A survey on content retrieval on the decentralised web”. In: *ACM Computing Surveys* 56.8 (2024). DOI: 10.1145/3649132 (cit. on p. 6).

[15] Christiane Kuhn, Martin Beck, and Thorsten Strufe. “Covid notions: Towards formal definitions—and documented understanding—of privacy goals and claimed protection in proximity-tracing services”. In: *Online Social Networks and Media* 22 (2021). DOI: 10.1016/j.osnem.2021.100125 (cit. on p. 6).

[16] Bo Li and David Saad. “Impact of presymptomatic transmission on epidemic spreading in contact networks: A dynamic message-passing analysis”. In: *Physical Review E* 103.5 (2021). DOI: 10.1103/physreve.103.052303 (cit. on p. 4).

[17] Kiemute Oyibo et al. “Factors influencing the adoption of contact tracing applications: Systematic review and recommendations”. In: *Frontiers in Digital Health* 4 (2022). DOI: 10.3389/fdgth.2022.862466 (cit. on p. 3).

[18] Jocelyne Piret and Guy Boivin. "Pandemics throughout history". In: *Frontiers in Microbiology* 11 (2021). DOI: 10.3389/fmicb.2020.631736 (cit. on p. 6).

[19] Francisco Pozo-Martin et al. "Comparative effectiveness of contact tracing interventions in the context of the COVID-19 pandemic: A systematic review". In: *European Journal of Epidemiology* 38.3 (2023), pp. 243–266. DOI: 10.1007/s10654-023-00963-z (cit. on pp. 2, 3).

[20] Alex Preukschat and Drummond Reed. *Self-sovereign identity: Decentralized digital identity and verifiable credentials*. Manning, 2021 (cit. on p. 6).

[21] Leonie Reichert, Samuel Brack, and Björn Scheuermann. "A survey of automatic contact tracing approaches using Bluetooth Low Energy". In: *ACM Transactions on Computing for Healthcare* 2.2 (2021). DOI: 10.1145/3444847 (cit. on pp. 2, 3).

[22] Leonie Reichert, Samuel Brack, and Björn Scheuermann. *Ovid: Message-based automatic contact tracing*. Cryptology ePrint Archive, Paper 2020/1462. 2020. URL: https://eprint.iacr.org/2020/1462 (cit. on pp. 3, 4, 6).

[23] Rob Romijnders et al. "Protect your score: Contact-tracing with differential privacy guarantees". In: *Proceedings of the AAAI Conference on Artificial Intelligence* 38.13 (2024), pp. 14829–14837. DOI: 10.1609/aaai.v38i13.29402 (cit. on p. 5).

[24] Frederico Schardong and Ricardo Custódio. “Self-sovereign identity: A systematic review, mapping and taxonomy”. In: *Sensors* 22.15 (2022). DOI: 10.3390/s22155641 (cit. on p. 6).

[25] Ruizhe Shi et al. “A closer look into IPFS: Accessibility, content, and performance”. In: *Proceedings of the ACM on Measurement and Analysis of Computing Systems* 8.2 (2024). DOI: 10.1145/3656015 (cit. on p. 6).

[26] Viktoriia Shubina et al. “Survey of decentralized solutions with mobile devices for user location tracking, proximity detection, and contact tracing in the COVID-19 era”. In: *Data* 5.4 (2020). DOI: 10.3390/data5040087 (cit. on p. 2).

[27] Lucy Simko et al. “COVID-19 contact tracing and privacy: A longitudinal study of public opinion”. In: *Digital Threats* 3.3 (2022). DOI: 10.1145/3480464 (cit. on p. 3).

[28] Sudhvir Singh et al. “How an outbreak became a pandemic: A chronological analysis of crucial junctures and international obligations in the early months of the COVID-19 pandemic”. In: *Lancet* 398.10316 (2021), pp. 2109–2124 (cit. on p. 2).

[29] Syed Amin Tabish and Syed Nabil. “An age of emerging and reemerging pandemic”. In: *Health* 14 (2022), pp. 1021–1037. DOI: 10.4236/health.2022.1410073 (cit. on p. 6).

[30] Ryan Tatton et al. “ShareTrace: Contact tracing with the actor model”. In: *2022 IEEE International Conference on E-health Networking, Ap-*

plication & Services (HealthCom). ©2022 IEEE. 2022, pp. 13–18. DOI: 10.1109/healthcom54947.2022.9982762 (cit. on p. 4).

[31] Dennis Trautwein et al. "Design and evaluation of IPFS: A storage layer for the decentralized web". In: *Proceedings of the ACM SIGCOMM 2022 Conference*. 2022, pp. 739–752. DOI: 10.1145/3544216.3544232 (cit. on p. 6).

[32] Carmela Troncoso et al. "Deploying decentralized, privacy-preserving proximity tracing". In: *Communications of the ACM* 65.9 (2022), pp. 48–57. DOI: 10.1145/3524107 (cit. on p. 2).

[33] Carmela Troncoso et al. "Systematizing decentralization and privacy: Lessons from 15 years of research and deployments". In: *Proceedings on Privacy Enhancing Technologies* 2017.4 (2017), pp. 307–329. DOI: 10.1515/popets-2017-0056 (cit. on p. 6).

[34] Jacqui Wise. "Covid-19: WHO declares end of global health emergency". In: *BMJ* 381 (2023). DOI: 10.1136/bmj.p1041 (cit. on p. 6).

[35] Na Zhu et al. "A novel coronavirus from patients with pneumonia in china, 2019". In: *New England Journal of Medicine* 382.8 (2020), pp. 727–733. DOI: 10.1056/nejmoa2001017 (cit. on p. 2).