

Privacy-enhanced Opportunistic Networks

Iain Parris
School of Computer Science
University of St Andrews
St Andrews, Fife, KY16 9SX, UK
ip@cs.st-andrews.ac.uk

ABSTRACT

Opportunistic networks have been the study of much research — in particular on making end-to-end routing efficient. Social network information is often exploited in opportunistic network routing, but simple social network routing schemes broadcast social network information, which introduces privacy concerns. These inherent privacy issues have not been the subject of much research. Is it possible to add privacy features to opportunistic networks without degrading the user experience? What privacy concerns do users have? How might we build an opportunistic network that can mitigate users' concerns while efficiently delivering data?

Our early work suggests that it is possible to modify social network routing to add privacy-enhancing features. We are currently planning experiments to determine the privacy concerns of users in different contexts when using opportunistic networks. We will then use our understanding of these concerns to inform design of a privacy-aware social network routing protocol which dynamically adapts to users' privacy requirements in different contexts.

Categories and Subject Descriptors

C.2.2 [Computer-Communication Networks]: Network Protocols—*Routing Protocols*; H.3.4 [Information Storage and Retrieval]: Systems and Software—*Social Networking*; K.4.1 [Computers and Society]: Public Policy Issues—*Privacy*

General Terms

Algorithms, Performance, Design, Human Factors

1. INTRODUCTION

Opportunistic networks [9] are becoming increasingly popular and relevant as more people carry mobile devices. In a disconnected store-and-forward architecture, nodes opportunistically make use of any other nodes that they encounter, as long as these encountered nodes are likely to help the message reach its destination.

The performance of an opportunistic network depends on accurately determining which encountered nodes will be useful in forwarding. Early opportunistic network routing protocols used net-

work or mobility characteristics of nodes. Another approach is social network routing – using social networks to inform routing decisions – which has been used in many schemes, such as SimBet [5].

An open, but oft over-looked, area for research is examining and mitigating privacy issues when using social network routing, or indeed opportunistic networks in general. There exist many privacy concerns when broadcasting social network information. For example, an opportunistic network user may not wish to share with the world that they have an embarrassing friend. Or a user may be happy with their social network information informing routing decisions but not with their whole network being world-viewable: it is one thing for a curious person to be able to infer some of the social network based on forwarded messages, but another to distribute the potentially sensitive information freely.

Research which has considered privacy, such as the HiBop scheme [3], assumes the existence of some key distribution infrastructure. However, key distribution and management is difficult in a mobile ad hoc environment. And requiring key distribution may impede opportunistic networking's most appealing feature — the ability for nodes to forward to *any* node participating in the network.

Stepping back, it is difficult with current methodologies to accurately determine which privacy threats are of concern to real users. There is a disconnect between what people say and what people do with respect to privacy. Moreover, if there is a performance impact due to adding privacy, users may choose to accept an increased risk of privacy violations in exchange for better quality of experience.

My proposed PhD thesis statement is:

It is possible to add the privacy-enhancing features that users desire to opportunistic networks, without an intolerable impact on the users' quality of experience.

To demonstrate this thesis, three research contributions are planned:

1. New schemes for enhancing privacy by obfuscating social network information prior to use in social network routing, including a routing performance evaluation for each scheme.
2. Capturing high-quality data on opportunistic network users' privacy concerns, by performing a novel user study.
3. Design and evaluation of a social network routing protocol, based upon the previous two contributions, which may dynamically adapt to users' privacy requirements in different contexts.

2. CURRENT RESULTS

Inspired by [1], we target the social network routing privacy threats by obfuscating the sender's social network at the time of

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

MobiOpp '10, February 22-23, 2010, Pisa, Italy.

Copyright 2010 ACM 978-1-60558-925-1/10/02 ...\$10.00.

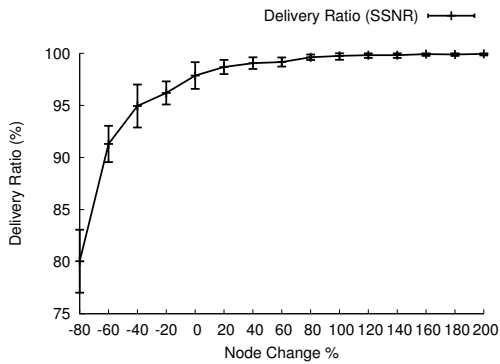


Figure 1: SASSY dataset. Delivery ratio vs target percentage modification of each message sender’s social network. Error bars indicate 95% confidence intervals.

message generation. For each message transmitted, the sender makes changes to the message’s copy of the sender’s true social network — adding or removing nodes. This introduces a degree of deniability: any node seeing the social network sent along with the message now cannot say with certainty whether a particular node is truly part of (or truly absent from) the sender’s social network. Named for a portmanteau of *statistical manipulation*¹, we call this scheme *Statisticulated Social Network Routing (SSNR)*.

We evaluated the performance of the SSNR scheme as compared with unmodified social network routing to see the impact on network performance. We used trace-driven simulation with two different real-world datasets: one collected in a previous experiment [2], which we call the SASSY dataset, and the well-known MIT *Reality Mining* dataset MIT [6]. For brevity, the details are omitted, and we present only the plot for the SASSY delivery ratios (Figure 1).

Figure 1 shows that it is possible to obfuscate a sender’s social network by removing up to 60% of the nodes from the social network while still maintaining a delivery ratio of 90% that of unaltered social network routing. We find the same is true for the *Reality Mining* dataset. For further details, see [8].

Although we note that the two datasets we have used to evaluate the SSNR scheme may not be representative of general opportunistic networking — both involve participants who have opted in to small-scale experiments which may not be representative of universal deployment — these initial results are encouraging. It may well be possible to add privacy-enhancing obfuscation to social network routing while preserving good routing performance.

3. FUTURE WORK

Our initial results in Section 2 suggest that it is possible to add privacy-enhancing features to social network routing in opportunistic networks. Given that adding privacy is possible, we are now interested in understanding what privacy the opportunistic network users actually want. Which privacy threats do they worry about? Do they have different privacy expectations at different times (for example, at work and at home)?

To explore these privacy conceptions, we are planning a user study involving a variant of the *experience sampling method*[4]. Since we do not have access to, or the ability to create, a real-world large-scale opportunistic network, we intend to simulate oppor-

¹Huff coins the term *statisticulation* in [7], where he writes: “Mis-informing people by the use of statistical material might be called statistical manipulation; in a word (though not a very good one), statisticulation.”

tunistic network applications using Facebook²; Facebook is very widely used and provides access to a wealth of real social network data. Participants will carry sensor-equipped smartphones tied to a custom Facebook application. We will use the phone sensors to infer context (for example, proximity to another participant from a Bluetooth encounter), and ask users in real-time what information they would be comfortable publishing via Facebook, and to whom.

We hope to gain understanding of users’ privacy concerns in different contexts, and to use this new understanding to inform opportunistic network design. In particular, we are working towards creating a social network routing protocol which may dynamically adapt to users’ privacy requirements in different contexts. For example, if a user is in a context where high privacy is desirable (perhaps at a particular location), the user’s device could detect this and modify its behaviour — perhaps refusing to forward data for other users, or automatically applying heavy social network obfuscation at message generation time. The device may even infer what type or degree of obfuscation would likely be appropriate for the user’s particular context.

4. ACKNOWLEDGEMENTS

This work is kindly supervised by Tristan Henderson.

5. REFERENCES

- [1] S. K. Belle and M. Waldvogel. Consistent deniable lying: Privacy in mobile social networks. In *Proc. Workshop on Security and Privacy Issues in Mobile Phone Use*, Sydney, Australia, May 2008.
- [2] G. Bigwood, D. Rehunathan, M. Bateman, T. Henderson, and S. Bhatti. Exploiting self-reported social networks for routing in ubiquitous computing environments. In *Proc. 1st Int’l Workshop on Social Aspects of Ubiquitous Computing Environments*, pp 484–489, Avignon, France, Oct. 2008.
- [3] C. Boldrini, M. Conti, and A. Passarella. Exploiting users’ social relations to forward data in opportunistic networks: The HiBOP solution. *Pervasive and Mobile Computing*, 4(5):633–657, Oct. 2008.
- [4] S. Consolvo and M. Walker. Using the experience sampling method to evaluate ubicomp applications. *IEEE Pervasive Computing*, 2(2):24–31, Apr.-June 2003.
- [5] E. M. Daly and M. Haahr. Social network analysis for information flow in disconnected delay-tolerant MANETs. *IEEE Trans. Mob. Comp.*, 8(5):606–621, May 2009.
- [6] N. Eagle, A. S. Pentland, and D. Lazer. Inferring friendship network structure by using mobile phone data. *PNAS*, 106(36):15274–15278, Aug. 2009.
- [7] D. Huff. *How to Lie With Statistics*. W. W. Norton & Company, 1954.
- [8] I. Parris, G. Bigwood, and T. Henderson. Privacy-enhanced social network routing in opportunistic networks. In *Proc. IEEE Int’l Workshop on SECURITY and SOCIAL Networking*, Mannheim, Germany, Apr. 2010. To appear.
- [9] L. Pelusi, A. Passarella, and M. Conti. Opportunistic networking: data forwarding in disconnected mobile ad hoc networks. *IEEE Communications*, 44(11):134–141, Nov. 2006.

²<http://www.facebook.com/>