# Privacy-Preserving Use of Social Information in Opportunistic Networks

DISS. ETH NO. 22772
DISS. TIK NO. 155

# Privacy-Preserving Use of Social Information in Opportunistic Networks

A thesis submitted to attain the degree of

DOCTOR OF SCIENCES of ETH Zurich

(Dr. sc. ETH Zurich)

presented by

BERNHARD DISTL

Master of Science, ETH
born March 20, 1980
citizen of Austria

accepted on the recommendation of
Prof. Dr. Bernhard Plattner, examiner
Prof. Dr. Gunnar Karlsson, co-examiner
Dr. Franck Legendre, co-examiner

2015

# Abstract

The popularity of smartphones and other mobile devices has lead to a significant increase in the use of cellular mobile data. As this demand is predicted to continue to grow exponentially in the future, providing sufficient and ubiquitous cellular coverage becomes increasingly challenging and sometimes even unfeasible. In addition to the generally increasing demand, unpredictable crowds are even more challenging to accommodate with existing infrastructure. Even worse, natural or man-made disasters may break infrastructure, thus disrupting connectivity. Also, a lack of economic incentives prevents remote and rural regions from receiving sufficient connectivity.

*Opportunistic networks* are envisioned to mitigate many of those issues. Mobile devices can leverage wireless capabilities (e.g. Bluetooth, WiFi adhoc, WiFi direct) to communicate directly with each other, whenever two devices are in mutual transmission range (in *contact*). State of the art opportunistic networks extract a stable structure (a *contact graph*) from all available contacts. The contact graph can then be used to enable multi-hop communication to maintain connectivity and provide services in an opportunistic manner.

Within the context of opportunistic networks, there is a close relationship between a device and its user. Thus, all communication of one device can be attributed to its user. This highly personal relationship creates severe privacy issues. What content the user consumes, which other users he or she meets and where the user is located can all be easily determined by an interested party. While some privacy aspects (e.g. location) are well investigated, the privacy of social information (e.g. friendships, social structure) has not received much attention. With the first two of the three contributions of this thesis, we investigate the use of social information in the two fundamental building blocks of opportunistic networking: routing and neighbor detection. We find that state of the art solutions do not protect privacy relevant infor-

mation. Therefore, we provide contributions in the area of privacy preserving use of social information within opportunistic networking.

In the *first* contribution, we present an algorithm to protect the privacy sensitive information associated with the social structure encoded by a contact graph as it is used by state of the art routing algorithms for opportunistic networks. A first straightforward approach to hide the social structure by randomly modifying the contact graph quickly leads to wrong routing decisions and thus diminishes opportunistic networking performance. By changing edges in the graph more selectively, we can maintain essential features of the graph that are required for routing (e.g. centrality ranking) while still effectively hiding the social structure encoded in the edges of the graph. We design a step-wise optimal greedy algorithm and a heuristic variant that can be calculated faster and for larger graphs. Eventually, we evaluate routing performance by using privacy protected graphs in existing state-of-the-art opportunistic routing algorithms.

In an anonymous opportunistic network, even friends no longer can recognize each other. Thus, they no longer can rely on existing (real world) social links (e.g. friendships) for security and trust mechanisms. In the *second* contribution, we present a protocol to detect once established social links in a privacy protected manner while maintaining the anonymity provided by a perfectly anonymous opportunistic network. Our hash based protocol can recognize pre-established social links among nodes *without* revealing private information, hence protecting users identity and social information. We implement our algorithm in a smartphone application and evaluate its performance.

Complementary to protecting the privacy of social information in the two fundamental building blocks of opportunistic networks (routing and neighbor detection), our *third* contribution investigates how current generation smart phones impact the physical contact events and thus contact modeling. The radio properties of smartphones (e.g. transmission range, directionality) are an important factor that shape contact events between two devices. However, in contrast to user mobility, which is well investigated, the impact of radio properties of smartphones on wireless contacts has to our knowledge not been investigated so far. We hence investigate the WiFi radio performance of smartphones for opportunistic networking. We start by revisiting the classical link budget, later adding the impact of the phone's carrier. We then perform extensive measurements to fully characterize all components of the link budget between two smartphones. Our measurements also give a clear indication of which of the existing propagation models is suited best for smartphones in

a pedestrian outdoor setting. Finally, to assess the capacity of opportunistic networking, we evaluate a simple scenario of two pedestrians crossing on a path.

# Kurzfassung

Durch die steigende Verbreitung und Populartiät von Smartphones hat sich die Internetnutzung stark verändert. Dank der Mobilfunknetzte konsumieren Menschen Internetinhalte nicht mehr nur zu Hause oder am Arbeitsplatz sondern praktisch überall. Der stetige Ausbau der Mobilfunknetze hat auch dazu geführt, das die Internetabdeckung heute bisher ungekannte Ausmasse erreicht hat. Das Internet der Dinge wird den Druck die Mobilfunknetze auszubauen noch verstärken. Allerdings werden durch diese Ausdehnung die Grenzen der Internetverfügbarkeit unschärfer und die Belastung durch steigende Datenvolumen immer größer.

Opportunistische Netzwerke nutzen direkte, drahtlose Kommunikation von Gerät zu Gerät um Informationen zwischen den Benutzern auszutauschen. Dank drahtloser Kommunikationstechnologien wie WLAN oder Bluetooth können von Smartphones direkt miteinander kommunizieren ohne auf Infrastruktur angewiesen zu sein. Wenn die herkömmlichen Mobilfunknetze überlastet oder nicht verfügbar sind, eröffnet opportunistische Kommunikation neue Möglichkeiten für Anwender. Informationen werden immer dann ausgetauscht, wenn zwei Benutzer gegenseitig in Funkreichweite kommen. Zusätzlich tragen Benutzer die Daten auch physikalisch mit sich herum wenn sich in ihrem Alltag bewegen. Obwohl theoretisch genug Potential besteht, haben sich opportunistische Netzwerke wegen fehlender Geschäftsmodelle bis jetzt noch nicht durchgesetzt. Wir untersuchen drei Themen von denen wir glauben, daß sie die praktische Akzeptanz von opportunistischen Netzwerkern erleichtern werden. Als erstes behandeln wir den Schutz der sozialen Informationen die für Routing genutzt werden, als zweites machen wir soziale Kontakte in einem anonymen Umfeld nutzbar und als drittes evaluieren wir Smarphone WLAN Eigenschaften um besser zu verstehen wie Kontakte durch die eingesetzte Technolgie beeinflusst werden.

Zuerst behandeln wir soziale Informationen, die ein wichtiges Werkzeug sind um opportunistische Netzwerke zu verbessern. Unter anderem kann man mit einem Kontaktgraphen, der soziale Strukturen erfasst, die Erfolgsrate bei Routing maximieren. Dabei untersuchen wir das Verhältnis von Schutz der Privatsphäre und Routingerfolg im Kontaktgraphen. Durch kontrolliertes hinzufügen und entfernen von Kanten können wir den Schutz der echten sozialen Verbindungen verbessern. Anhand von künstlichen und realen Kontaktgraphen zeigen wir erst, dass zufällige Änderungen am Graphen das Ranking von Betweenness centrality (einer typischen Routingmetrik) schnell zerstört wird und zu falschen Routingentscheiden führt. Unser Ansatz immer die Kante mit dem kleinsten Einfluss auf das Ranking zu ersetzen führt dazu, dass die Nutzbarkeit erhalten bleibt während gleichzeitig ein hohes Schutzniveau erreicht wird. Die Skalierbarkeit unserer Lösung wird durch eine Heuristik basierend auf der Ähnlichkeit von Knoten erreicht. Sie modelliert den Basisalgorithmus und ist für grosse Graphen gut einsetzbar. Daß Routing auch mit den geschützten Graphen funktioniert können wir zeigen, in dem geschützte Graphen für routing mit einem bekannten Algorithmus eingesetzt werden.

Im zweiten Teil bewegen wir uns im Spannungsfeld zwischen Anonymität und der Nutzbarkeit von sozialen Informationen. Einerseits müssen soziale Informationen geschützt werden, andererseits können Sie genutzt werden um die Leitung und Sicherheit in opportunistischen Netzwerken zu steigern. Vollständig anonyme opportunistische Netze verhindern jedoch das Wiedererkennen von bestehenden sozialen Verbindungen (z.B. Freundschaften). Wir entwerfen ein Protokoll, dass einen Ausweg aus diesem Dilemma darstellt. Es ermöglicht, einmal erstellte soziale Verbindungen zwischen Benutzern wiederzuerkennen, *ohne* daß private Informationen einsehbar werden, wodurch es möglich wird, Anonymität *und* Leistung und Sicherheit zu unterstützen. Unser Protokoll nutzt mit Bloomfiltern eine Hash-basierte Konstruktion die gleichzeitig dem Schutz der sozialen Informationen und einer zuverlässigen und schnellen Erkennung bestehender sozialer Verbindungen in einem anonymen Umfeld dient. Zusätzlich implementieren und evaluieren wir das Protokoll auf Android Smartphones.

Zuletzt wenden wir uns der Tatsache zu, dass (Funk)Kontakte bisher vor allem vom Standpunkt der Benutzermobilität aus untersucht wurden. Allerdings hängen die Eigenschaften der Kontake zu einem großen Teil auch von den involvierten Geräten (meistens Smartphones) ab. Unseres Wissens nach hat sich bisher noch keine Studie mit dem Einfluss der Funkeigenschaften moderner Smartphones auf opportunistische Kontake befasst. Darum unter-

suchen wir in diesem Teil der Arbeit die Auswirkungen der WLAN Charakteristik von Smartphones auf opportunistische Kommunikation. Wir beginnen mit dem klassischen Linkbudget und erweitern diese Betrachtung um den Einfluss des Menschen der das Gerät trägt. Des Weiteren führen wir Messungen durch, die es uns erlauben alle Komponenten des Linkbudgets zwischen zwei Smartphones zu charakterisieren. Das zwei Strahlen Ausbreitungsmodell stellt sich als das beste Modell für Smartphones heraus. Zuletzt betrachten wir ein Szenario in dem sich zwei Fussgänger begegnen und berechnen die Datenübertragungskapazität der daraus resultierenden opportunistischen Kontakts.