The road towards private proximity services

Haus, Michael; Ding, Aaron Yi; Ott, Jorg

DOI
10.1109/WoWMoM.2019.8793013

Publication date
2019

Document Version
Accepted author manuscript

Published in
20th IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks, WoWMoM 2019

Citation (APA)
Haus, M., Ding, A. Y., & Ott, J. (2019). The road towards private proximity services. In *20th IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks, WoWMoM 2019* Article 8793013 (20th IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks, WoWMoM 2019). IEEE. https://doi.org/10.1109/WoWMoM.2019.8793013

Accepted Author Manuscript. Link to published article (IEEE): https://doi.org/10.1109/WoWMoM.2019.8793013

The Road Towards Private Proximity Services

Michael Haus
Technical University of Munich
haus@in.tum.de

Aaron Yi Ding
Delft University of Technology
aaron.ding@tudelft.nl

Jörg Ott
Technical University of Munich
ott@in.tum.de

***Abstract*—Towards private proximity services, we realized a set of proximity services at different spatial resolutions. For small-scale ($\sim$0.5 m) securing remote access to smart homes and for mid-scale (10–20 m) to manage nearby Internet of Things (IoT) devices and offer fine-grained service discovery in indoor environments. Regarding large-scale services (100 m), we implemented a device grouping via similarity of light patterns, ambient sound, Wi-Fi signals, and ultrasound communication which is naturally restricted by spatial barriers. To improve user's privacy from a system point of view, we analyzed different security mechanisms in the domain of device-to-device (D2D) communication such as access control, location privacy. Based on visible light communication (VLC), we are implemented and tested a system for private indoor service discovery and distance-bounding authorization. Furthermore, we examined the feasibility of homomorphic encryption for time-series data like visible light patterns.**

I. Problem Domain

The problem domain of the PhD thesis is divided into two parts, proximity of users and their privacy. We introduce position-aware systems including the well-known Location-based Services (LBS) and Proximity-based Services (PBS) as subclass of LBS. The LBS are based upon the absolute position of an user to answer the question: "where are we?" In contrast, PBS are based upon context information to find co-location with other points of interest to answer the question "who are we with?" The goal of LBS and PBS is to improve the users' daily lives by providing a personalized service to enable sharing of location information and location-aware information retrieval. LBS focus on a centralized architecture, where the location server acts as Trusted Party (TP) that receives coordinates from the users to provide location-specific information, e.g., nearby friends. In comparison to LBS with a global positioning, PBS use a relative positioning between entities in a smaller local reference frame. We define the term proximity as "the state of being near to somebody or something". The popularity of PBS is largely driven by social networking applications, in which the direct communication between nearby mobile devices is particularly interesting. PBS are trying to solve the issues of LBS by focusing on an infrastructure-less environment without a TP. We can identify two essential phases of PBS: 1) the user must be able to detect other users in the vicinity and 2) users intuitively want to share information and services among devices in proximity. The second part of the PhD thesis focuses on privacy mechanisms. The location or sensor data used by LBS and PBS is sensitive and must be protected against privacy attacks. For example, adversaries can reconstruct movements across space and time.

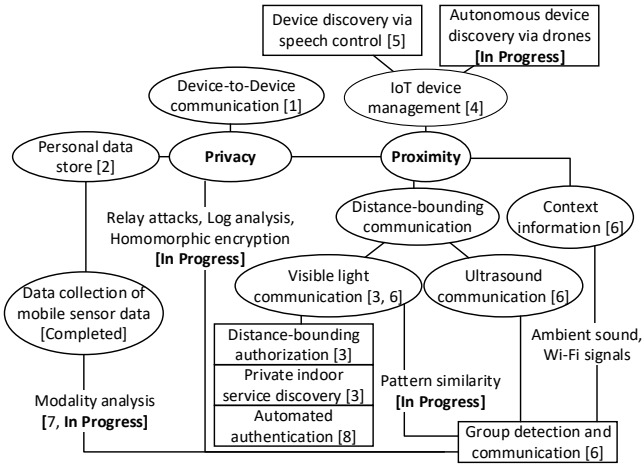

Fig. 1: Overview of approaches for private proximity services

We address the following research questions in terms of private proximity services:

- How to determine spatial proximity of multiple users efficiently, quickly and precisely?
- How to create a decentralized proximity solution that does not require the disclosure of the user locations?

II. Approaches

We provide an overview in Fig. 1 of our approaches with technologies and use cases to highlight how we tackled the aforementioned research questions. In the following, we describe these approaches in more detail.

A. Improving User's Privacy

Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. We analyzed privacy form a network point of view in device-to-device (D2D) communication: *Security and Privacy in Device-to-Device (D2D) Communication: A Review (**Completed**)* [1]. D2D communication presents a new paradigm in mobile networking to facilitate data exchange between physically proximate devices. The development of D2D is driven by mobile operators to harvest short range communications for improving network performance and supporting proximity-based services. We investigated two fundamental and interrelated aspects of D2D communication, security and privacy, which are essential for the adoption and deployment of D2D. We

presented an extensive review of the state-of-the-art solutions for enhancing security and privacy in D2D communication. By summarizing the challenges, requirements, and features of different proposals, we identify lessons to be learned from existing studies and derive a set of "best practices". The primary goal of our work is to equip researchers and developers with a better understanding of the underlying problems and the potential solutions for D2D security and privacy. To inspire follow-up research, we identified open problems and highlight future directions with regard to system and communication design.

Besides that, we improved users privacy from a system point of view with a private personal data hub [2], private indoor service discovery, and a countermeasure against relay attacks. Moreover, we realized a distance-bounding authorization based on visible light communication (VLC) [3] and analyzed the feasibility to apply homomorphic encryption for time-series data like ambient light. Mobile and wearable devices like smartphones or tablets are data hubs of our digital life and contain a large amount of sensitive data, which makes them a potential target for attackers. The aim of our *P^2Hub as Private Personal Data Hub for Mobile Devices (**Completed**)* [2] is to consider the privacy-by-architecture principle directly during the system design phase. We enhanced the isolation of sensitive private information through a privacy-preserving module supported by novel, lightweight virtualization techniques. Thus, we inherently improve the system's security and privacy.

We use our custom light bulb [3] to enable semi-decentralized device-to-device grouping. We detect nearby devices by their similarity of ambient light patterns and associate them together for data sharing. In this scenario, the most crucial attack is a relay attack, at which a user within the VLC range colludes with an adversary outside of the VLC range. The light patterns received from the light bulb are relayed to the attacker which is able to "prove" to be within the semantic space of other users and access sensitive data. Therefore, we designed and implemented a countermeasure against relay attacks via response times. On the other hand, we explored secure multi-party computation (SMC) for private proximity testing (PPT) based on cryptographic primitives to enable a pair of devices to test if they are nearby within a specific distance threshold. The PPT problem is often reduced to private equality testing (PET) or private set intersection (PSI) where each party holds a set of inputs and needs to jointly calculate intersection of the input sets without revealing further information. The two main techniques to solve the SMC problem are: 1) garbled circuits where one party prepares encrypted circuit and 2) homomorphic encryption where we perform computations directly on ciphertexts.

B. Realizing Proximity Services

We realized of set of proximity services at different spatial resolutions. For small-scale (~ 0.5 m) securing remote access to smart homes via two-factor authentication [3] and for mid-scale (10–20 m) to manage nearby IoT devices [4], [5] and offer fine-grained indoor service discovery [3]. With respect to large-scale services (100 m), we implemented a device grouping via similarity of light patterns, ambient sound, Wi-Fi signals, and ultrasound communication [6] which is restricted by spatial barriers.

Managing IoT devices in urban areas is becoming crucial because the majority of people living in cities and the number of deployed IoT devices are steadily increasing. We presented iConfig in *Managing IoT at the Edge: The Case for BLE Beacons (**Completed**)* [4], an edge-driven platform dedicated to manage IoT devices in smart cities. The goal is to address three major issues in current IoT management: registration, configuration, and maintenance. The core of iConfig is its programmable edge module, which can be deployed across smartphones, wearables, and smart boards to configure and interact with physically proximate IoT devices. Through testbed experiments and usability studies, we reveal the hardship and hidden pitfalls in managing IoT devices, especially for low budget devices like Bluetooth Low Energy (BLE) beacons. Our system evaluation showed that iConfig can effectively address the aforementioned IoT management challenges by harnessing the mobile and edge cooperation. In our demo *iConfig - What I See is What I Configure (**Completed**)* [5] we take advantage of speech recognition to enable hands free device configuration on smartphones and smart glasses. Furthermore, we implemented a custom camera control via speech recognition to capture an image of IoT devices for easier device localization.

Previously, iConfig focused on mobile user-dependent end-devices as we tested it on Android smartphone and smart glass (MAD Gaze X5) [5]. Thereby, we have optimized the system interaction via voice commands to be more natural and fluent among users, their smart gadgets and surrounding IoT devices [5]. Currently, we extend iConfig to support drones as end-devices (**In Progress**) to be independent of users and able to create a detailed map of surrounding wireless devices including locations. We are exploring the feasibility to use small COTS drones such as DJI Mavir Air to create indoor maps showing encountered Wi-Fi and Bluetooth devices. This comprehensive device map serves as the basis for add-on services like device localization and monitoring to enhance network security. With iConfig-enabled drones, we achieve a fully autonomous device detection.

We applied VLC and ultrasound communication for small- and mid-scale proximity services. Our work *Enhancing Indoor IoT Communication with Visible Light and Ultrasound (**Completed**)* [6] deals with the steadily increasing number of deployed IoT devices to manage and interact with community assets of smart cities, such as transportation systems and power plants. This may lead to degraded network performance due to the growing amount of network traffic and connections generated by various IoT devices. To tackle these issues, one promising direction is to leverage the physical proximity of communicating devices and inter-device communication to achieve low latency, bandwidth efficiency, and resilient services. We aim at enhancing the performance of indoor

IoT communication (e.g., smart homes, SOHO) by taking advantage of emerging technologies such as visible light and ultrasound. This approach increases the network capacity, robustness of network connections across IoT devices, and provides efficient means to enable distance-bounding services. We have developed communication modules using off-the-shelf components for visible light and ultrasound and evaluate their network performance and energy consumption. In addition, we showed the efficacy of our communication modules by applying them in a practical indoor IoT scenario to realize secure IoT group communication. To enrich our group detection and infer device proximity (**In Progress**) like in [7], we gathered mobile sensor data from 126 devices including accelerometer, barometer, Bluetooth encounters, GSM, locations (GPS, network), magnetometer, and Wi-Fi. Based on the findings from our data analysis we extend the prototype from [6] to achieve an enhanced performance and cover more environments with changing conditions.

Regarding distance-bounding wireless communication, we realized *LocalVLC: Augmenting Smart IoT Services with Practical Visible Light Communication (**Completed**)* [3]. Current VLC designs commonly require dedicated LEDs to emit modulated light beams which entail high energy overhead and unpleasant visual experiences due to the perceptible light blinking effects for end users. This greatly limits the deployment and applicable scenarios of VLC. We designed and developed LocalVLC, a practical and low-cost VLC system that can be used as a standard light source to augment smart IoT services. LocalVLC introduces a novel Morse code-inspired modulation scheme that can operate on off-the-shelf LEDs with low energy overhead. It can effectively overcome the light flickering by encoding data into high frequency light pulses without requiring extra processing hardware such as FPGA or micro-controller. We have implemented and evaluated a full-fledged system prototype based on LocalVLC design. Under practical settings, our LocalVLC prototype can support up to 10 meters of range, and attain reasonable throughput (up to 1.4 Kbps) with low error rate and energy consumption. Compared to the widely adopted Manchester encoding, LocalVLC yields 8x improvement on both throughput and energy consumption. In addition, we demonstrate the practicality of LocalVLC for indoor service discovery and smart home key management. As further use case, our demo *Touchless Wireless Authentication via LocalVLC (**Completed**)* [8] aims to automate indoor wireless (Wi-Fi) authentication. We use VLC for machine-to-machine communication to ease the setup of Wi-Fi networks. LocalVLC streamlines the credential management and achieves a "touchless" authentication experience in a distance-bounding manner, avoiding manual distribution and tedious input of passwords for login. In comparison, other mechanisms to exchange credentials such as WPS or QR codes still require human interaction. LocalVLC covers many target devices including common Wi-Fi equipped devices (e.g., smartphone, tablet, laptop) as well as IoT devices like sensor boards. For the wireless network, LocalVLC broadcasts the security credential data including SSID and password. Via an add-on device equipped with a photodiode, the user's smartphone is able to retrieve the VLC transmitted login data. The smartphone continually scans for nearby wireless networks and in case of spotting a matching SSID, it can perform automated wireless authentication without any manual interaction.

We take further advantage of our custom light [3] which serves as decentralized communication hub for device grouping based on ambient light patterns (**In Progress**). We use multiple distance metrics, correlations methods, and machine learning models to automatically group proximate devices based on the similarity of time-series signals like ambient light. Thereby, we apply automated feature selection via hypothesis tests to reveal the most important features and simulate different number of users in static and dynamic environments. To be specific, we use light signals with random on and off phases to distinguish different areas and we extend the VLC receiver to be able to detect the light pattern without prior knowledge. To allow a more-fine grained device grouping, we analyze the device grouping log to classify the devices into distinct groups such as personal, family and stranger's devices. On this basis, we can automatically restrict the data sharing among different device classes sharing the same geographic group.

III. Conclusion

The overall goal is to create a proximity-based service which is able to strike a balance between user privacy, service quality, and quality of experience. These attributes are contradicting. A strong privacy mechanism such as private proximity testing protects most of the sensitive user information, which negatively affects the service quality of the proximity-based application.

References

[1] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma, and J. Ott, "Security and Privacy in Device-to-Device (D2D) Communication: A Review," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1054–1079, 2017.

[2] M. Haus, V. Cozzolino, A. Y. Ding, and J. Ott, "P2Hub: Private Personal Data Hub for Mobile Devices," in *Proceedings of the 17th International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2016.

[3] M. Haus, A. Y. Ding, and J. Ott, "LocalVLC: Augmenting Smart IoT Services with Practical Visible Light Communication," in *Proceedings of the 20th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2019.

[4] ——, "Managing IoT at the Edge: The Case for BLE Beacons," in *Proceedings of the 3rd Workshop on Experiences with the Design and Implementation of Smart Objects*, 2017, pp. 41–46.

[5] M. Haus, A. Y. Ding, P. Hui, and J. Ott, "Demo: iConfig - What I See is What I Configure," in *Proceedings of the 12th ACM Workshop on Challenged Networks (CHANTS)*, 2017, pp. 1–2.

[6] M. Haus, A. Y. Ding, Q. Wang, J. Toivonen, L. Tonetto, S. Tarkoma, and J. Ott, "Enhancing Indoor IoT Communication with Visible Light and Ultrasound," in *Proceedings of the IEEE International Conference on Communications (ICC)*, 2019.

[7] P. Sapiezynski, A. Stopczynski, D. Kofoed Wind, J. Leskovec, and S. Lehmann, "Inferring Person-to-person Proximity Using WiFi Signals," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 1, no. 2, pp. 1–20, 2017.

[8] M. Haus, A. Y. Ding, C. Xu, and J. Ott, "Demo: Touchless Wireless Authentication via LocalVLC," in *Proceedings of the 16th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2018, p. 531.