Statement of Research Plans

As we are entering the era of mobile computing, the wide proliferation of sensor-equipped smartphone is increasingly influencing our daily life. Since smartphone equipped sensors (e.g. microphone, camera, accelerometer, gyroscope, compass) collect an increasing amount of sensitive information, security issues has inevitably critical impact in mobile computing. My current research focuses on exploring the novel ideas and techniques to tackle critical security issues and practical problems for the smartphone sensing systems. In particular, I study smartphone security from the physical layer, leveraging various related characteristics to enable inherently secure and dependable wireless communications. Moreover, I am also experienced in smartphone-enabled crowdsourcing approaches that can build large-scale information infrastructures conveniently at a very low cost. My research approach is in general characterized by the innovative integration of interdisciplinary ideas and synergy through extensive collaborations. First, I find it intriguing to innovate ideas from multiple domains and creatively apply them to solve complex problems. For instance, my previous research integrated ideas from mobile sensing, cloud computing and signal processing to address challenges of securing short-range wireless communication with acoustic wave. Second, my research draws on advanced mathematical models, which allows the system designs to have a solid theoretical foundation. It helps pave the way to achieve robust result, even from inherently incomplete, opportunistic, and noisy crowdsourced data. Third, I am passionate in hands-on research, and believe that intensive experiment implementations on real cloud platforms are indispensable to ensure that my system design is practical and deployable. Finally, my research is invigorated by collaborations with others from diverse backgrounds: professors, industrial research scientist, engineers, and fellow students. Engaging other researchers' expertise not only offers alternative perspectives to approach research objectives, but also diversifies my knowledge and skills as a researcher. The following summarizes my research experience, related projects that demonstrate my research strategy, and my vision of future research directions.

Previous and Current Research

Securing Short-Range Wireless Communications - As an emerging advanced short-range communication technology, near field communication (NFC) is undergoing a fast rate of expansion with many promising benefits including low power, small size, and peer-to-peer communication, without incurring complex network configuration overhead. However, current NFC technologies suffer from one practical limitation: almost all NFC enabled applications require built-in NFC chipsets. Such low levels of penetration of special NFC hardware has stymied its applications on most mobile devices in the market. In addition, from the security perspective the confidentiality of the transmitted data has not been satisfactorily addressed by current NFC technologies, which do not incorporate any security at the physical or MAC layers by assuming that the extremely short range of communication itself has offered a degree of protection physically.

My research in this direction focuses on alternative NFC technologies, with an emphasis on line-of-sight based NFC and acoustic based NFC, which are compatible with legacy devices and

existing infrastructure, and can provide a high level of security guarantee. For secure line-of-sight-based NFC, I have formalized the security analysis based on geometric models, and proposed physical security enhancement mechanisms for barcode communication by manipulating screen view angles and leveraging user-induced motions. For secure acoustics-based NFC, I have adopted the emerging friendly jamming technique from radio communication to achieve data confidentiality, leading to software-based solution to secure smartphone communication without the traditional key agreement phase. Based on the theoretical results, I further design and implement a cloud-assisted mobile system named AcousAuth. AcousAuth is designed for personal authentication. It features a seamless, faster, easier and safer user authentication process without the demand for special infrastructure. Potentially, any mobile devices or computers with microphone and speaker can use AcousAuth, regardless of the underlying hardware and operating systems. The cloud-assisted mobile sensing system provides a purely software-based solution to secure smartphone short-range communication without key agreement phase, and it is potentially well suited for legacy mobile devices. Both alternative NFC techniques have potential to provide NFC-like functionalities to the commercial smartphone applications, and enable much stronger security guarantees, yet with much less strict hardware support. These preliminary results are reported in the IEEE Internet of Things Journal [3]. The system prototype – AcousAuth is in the top 10 finalist from the ACM Mobicom App Competition [1]

Crowdsourcing Systems - Crowdsourcing is a technology with the potential to revolutionize large-scale data gathering in an extremely cost-effective manner. It provides an unprecedented means of collecting data from the physical world, particularly through the use of modern smartphones, which are equipped with high-resolution cameras and various micro-electrical sensors. My research in this area currently addresses the critical yet demanding task of reconstructing the indoor floor map and interior view of a building from crowdsourced data. A typical indoor floor map succinctly illustrates spatial correlations of rooms, hallways and other features of the architecture from a top-down view over a floor. It plays an essential role in many indoor mobile applications, such as localization and navigation. However, unlike outdoor environment, acquiring digital indoor floor plan information is very challenging. The state-of-the-art Google Indoor Maps only have 10,000 locations available on-line, which is not in a position to compete with the total number of indoor environments around the world. The complexity of the indoor environment is the major obstacle to achieve ubiquitous coverage. Existing centralized collection and on-site calibration techniques demand professional devices and multi-party coordination, which are time consuming, inconvenient and costly.

In light of these challenges, I propose and demonstrate CrowdMap, a crowdsourcing system utilizing sensor-rich video data from mobile users for indoor floor plan reconstruction with low-cost. The key idea is to first jointly leverage crowdsourced sensory and video data to track user movements, and then use the inferred user motion traces and context of the image to produce an accurate floor plan. In particular, I exploit the sequential relationship between each consecutive frame abstracted from the video to improve system performance. The experiments in three college buildings demonstrate that our techniques achieve a significant improvement of accuracy compared with other crowdsourcing floor plan reconstruction systems. Going beyond 2D, I further propose, design, and prototype IndoorCrowd2D, a smartphone-empowered crowdsourcing system for indoor scene reconstruction. In particular, I formulate the problem via trackable models and employ a divide and conquer approach to address the inherently incomplete, opportunistic, and noisy crowdsourced data. By utilizing the image information and sensory data in a coordinated way, my system performs high result accuracy, as well as allows a gradual build-up procedure of the

[1] http://www.sigmobile.org/mobicom/2013/app_finalists.html

hallway skeleton. This is corroborated by my evaluations on reconstructing college buildings from 1,151 datasets uploaded by 25 users. It also shows that my image and sensor hybrid method is more robust to overcome errors and outliers compare to image-only method. Once fully hardened, I believe that this system is able to extend existing digital map services to indoor environment on a world scale. Moreover, IndoorCrowd2D can also serve an important stepping stone towards the ultimate goal of economically-viable massive indoor 3D model reconstruction. These preliminary results are reported at IEEE ICDCS [1] and ACM SenSys [2], a highly selective research venue on systems issues of broadly-defined sensors and sensor-enabled smart systems.

Other Collaborative Research - I have also explored research frontier of mobile social networks security, with representative works centering around the proliferation of smart mobile devices. The problem tackled relates to location-based social networks (LBSNs), which features friend discovery by location proximity, and has attracted hundreds of millions of users world-wide. While leading LBSN providers claim the well-protection of their users? location privacy, for the first time my work shows through real world attacks that these claims do not hold. In the identified attacks, a malicious individual with the capability of no more than a regular LBSN user can easily break most LBSNs by manipulating location information fed to LBSN client apps and running them as location oracles. My developed automated user location tracking system could geo-locate any target with high accuracy and readily recover his/her top 5 locations, according to a 3-week real-world experiment on 30 volunteers over leading LBSNs, like Wechat, Skout, and Momo. Besides the attack, I also help develop a framework that explores a grid reference system and location classifications to mitigate the attacks. The result serves as a critical security reminder of the current LBSNs pertaining to a vast number of users. This work was reported in ACM Mobihoc [4].

Future Research

- **Sensor-assisted Mobile Authentication Systems:** I am looking forward to studying practical solutions for securing biometric-based mobile authentication. A lot of interesting yet challenging problems remain to be fully explored, including designing secure mechanism to defend against biometric-based impersonation attacks (e.g. voice impersonation attacks) on smartphones. Given the fact that there is a natural demand for users to control their mobile device in a convenient and non-intrusive way, many biometric-based mobile authentication applications have been developed. However, the human biometrics, e.g. human voice and human face, are often exposed to the public in many different scenarios. Traditional security mechanisms for these biometric authentication systems focus on data encryption and other post-processing techniques, but the biometric themselves often remain vulnerable to attacks in the physical/analog domain. If an adversary captures and manipulates a physical/analog signal prior to digitization, no amount of digital security mechanisms after the fact can help. Fortunately, nature imposes fundamental constraints on how these analog signals can behave. As for my future research, I will study the sensor-assisted mobile physical challenge-response authentication scheme to protect mobile authentication systems against impersonation attacks occurring in the physical/analog domain.

- **Mobile Crowdsourcing Systems:** As we are entering the era of mobile computing, the wide proliferation of sensor-equipped smart phones is increasingly influencing our daily life. Yet challenges remain on system efficiency, functionality, and security. I will continue the line of important research topics discussed earlier and explore the following three directions: First, I will further improve the cloud-assisted mobile systems to build a large-scale information processing cyber-infrastructure with low cost. Second, I will explore the possibility

of utilizing unmanned aerial vehicles for advanced automated crowdsourcing system design with potentially improved accuracy and efficiency. Finally, I am interested in extending existing ubiquitous cloud-based crowdsourcing systems and focus on further processing of the crowd-sourced visual information to extract more context information from the indoor environment, such as object detection and object recognition. By combining technologies from different research domains, e.g., mobile sensing, computer vision, and machine learning, I plan to construct systems that are able to better digitalize our daily life by solving more practical problems.

Selected Publications

[1] Si Chen, Muyuan Li, Kui Ren, Chunming Qiao, "CrowdMap: Accurate Reconstruction of Indoor Floor Plan from Crowdsourced Sensor-Rich Videos". *in Proceedings of the 35th IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2015.

[2] Si Chen, Muyuan Li, Kui Ren, Xinwen Fu, Chunming Qiao, "Rise of the Indoor Crowd: Reconstruction of Building Interior View via Mobile Crowdsourcing", *in Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems (SenSys)*, 2015.

[3] Bingsheng Zhang, Qin Zhan, Si Chen, Muyuan Li, Kui Ren, Cong Wang, Di Ma, "PriWhisper: Enabling Keyless Secure Acoustic Communication for Smartphones", *in IEEE Internet of Things Journal*, 2014.

[4] Muyuan Li, Haojin Zhu, Zhaoyu Gao, Si Chen, Le Yu, Shangqian Hu, Kui Ren, "All your location are belong to us: Breaking mobile social networks for automated user location tracking", *in Proceedings of the 15th ACM international symposium on Mobile ad hoc networking and computing (Mobihoc)*, 2014.