Secure Positioning in Wireless Systems

Mridula Singh
CISPA Helmholtz Center for Information Security
Saarbrücken, Germany
singh@cispa.de

Aanjhan Ranganathan
Khoury College of Computer Sciences
Northeastern University, Boston, USA
aanjhan@northeastern.edu

***Abstract*—With the development and deployment of numerous wireless mobile devices, ranging from smartphones to autonomous drones and self-driving cars, and the exponential growth in the Internet-of-Things field, it has become increasingly important to securely determine and verify location information. the numerous ranging and positioning systems in use today provide limited security and privacy guarantees and have repeatedly shown to be vulnerable to modern day cyber-physical attacks with severe implications: an attacker can gain entry into a restricted area, make fraudulent payments, steal property, deviate vehicles from their intended paths, or cause physical collisions in autonomous vehicles. Proving proximity in wireless systems isn't a trivial task and must satisfy numerous design requirements to be secure and several designs have been proposed in literature. In this tutorial, we will provide an overview of techniques used by wireless positioning systems, expose their vulnerabilities, discuss the current state of standards and the an overview of existing secure ranging system designs. It is expected that the tutorial will shed light on the unique challenges that exist in designing and deploying secure and private positioning systems including open research opportunities. Finally, with the emergence of multiple proximity-based contact tracing systems due to the COVID-19 pandemic, location privacy is also becoming increasingly critical and the tutorial will highlight the fundamental trade-off that exists between designing secure and private positioning networks.**

I. Motivation

With the development and deployment of large numbers of wireless mobile devices ranging from smartphones to autonomous drones and self-driving cars, and the predicted growth in the Internet-of-Things space, the ability of determining one's own location, querying locations of object and of securely verifying location claims of other devices is becoming critical to variety of applications. Prominent applications include civilian and military navigation and transportation systems, people and asset tracking, emergency rescue and support, location-based access control and authentication, and modern communication systems. For example, the use of contactless tokens has been accepted as a means of executing money transactions, unlocking digital devices, providing access to infrastructure, and verifying credentials using electronic passports [1]–[3]. With the advent of autonomous cyber-physical systems such as self-driving cars and unmanned aerial vehicles, the demand for ranging information is only bound to increase e.g., a stringent requirement for these systems is to avoid crashing into buildings, pedestrians, properties, or each other. Keeping autonomous vehicles and drones on their intended paths and preventing their collision can be achieved if they are able to calculate their relative distances accurately and securely. Ranging systems are in more demand than ever due to the COVID-19 pandemic [4]. Contract tracing apps, where distance is measured between co-located mobile devices, facilitate the public, social organizations, and government to prevent and control the pandemic. These apps are a healthy supplement to manual tracing in which human workers interview people who have been diagnosed with COVID-19 and then track down their recent contacts.

The use of ranging information in safety- and security-critical applications make it a target of attackers with different motivations. Distance manipulation attacks have led to car thefts, unauthorized payment execution, and location coordinates manipulation as shown in Figure 1 [5]. It is therefore essential to explore the current distance measurement systems' performance and security guarantees. Use cases like contactless access tokens generally need to establish an upper bound on the measured distance. Upcoming use cases like autonomous vehicles demand measured distance to be exact, i.e., device should establish both upper and lower bound on the measured distance [6], [7]. It is evident that there is a strong need for secure and private ranging and positioning ecosystem. *Therefore, this tutorial aims to educate the audience on the importance of secure positioning, the design challenges and trade-offs, limitations of existing designs, and future research opportunities and directions.*

II. Outline and topics covered

In this tutorial, we will first introduce the importance of location information in the modern world. We will further motivate the need for secure and private positioning and present a few real-world attack scenarios. Then, we will give an overview of various wireless positioning techniques that exist, their advantages, and limitations. We will introduce the concept of ranging using broadcast signals and bi-directional signals, and provide insights into their security guarantees. We will then go into the depths of the security and privacy of popular as well as emerging wireless positioning systems such as GPS, UWB, WiFI NGP, 5G-NR, etc. and present research challenges in enabling secure positioning. Below, we go into the details of the topics covered.

Wireless Positioning Techniques. Numerous ranging and positioning technologies have been developed in the last decade. These techniques differ in communication channels (e.g., radio-frequency, optical), position-related parameters

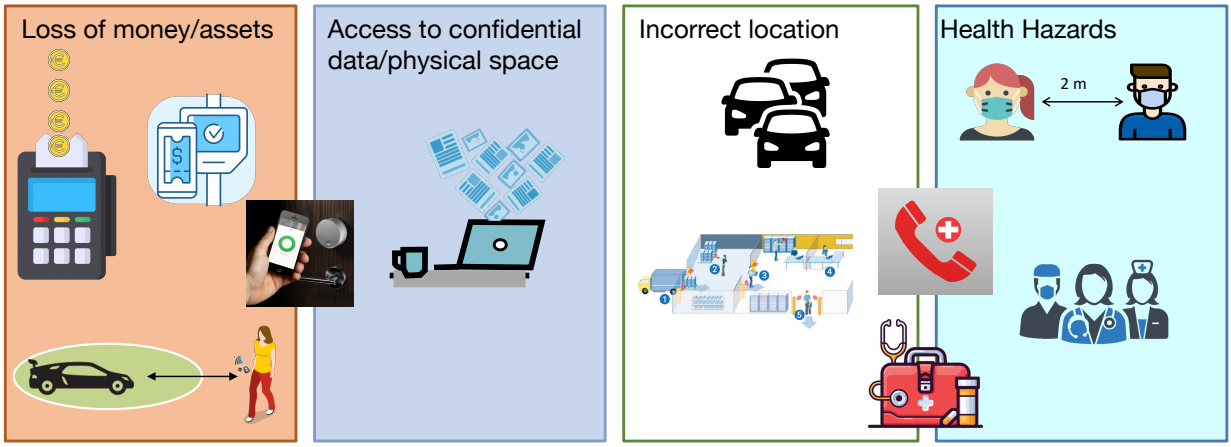

Fig. 1. Incorrect and insecure distance measurement has serious implications. It can lead to the loss of money, assets, and human life.

(e.g., received signal strength (RSS), time-of-arrival (TOA), time-difference-of-arrival (TDOA)), precision and reliability. In this part of the tutorial, we will provide an overview of different ranging techniques and compare them across their operating environment and the precision guarantees we achieve using these techniques. We will also introduce logical and physical layer attacks that are instrumental in manipulating the perceived distance between two devices.

Satellite-based Positioning Systems (e.g., GPS). Global Positioning System (GPS) is the most widely used Global Navigation Satellite System (GNSS) including applications such as positioning, navigation, asset and personnel tracking, communication systems, power grids, emergency rescue and support, and access control. Due to the lack of authentication in civilian navigation messages, GPS is vulnerable to signal spoofing attacks [8]. The reliance on one-way navigation messages allow systems like GPS to scale well and offer wide-area coverage but makes them inherently vulnerable to spoofing by attackers that control the communication channel and are capable of delaying (works even if the messages are cryptographically protected), relaying, or generating navigation messages. Many countermeasures for protecting GPS have been proposed in the recent years. Some proposed cryptographic methods, many relied on detecting physical-layer signal anomalies and spatial characteristics. Some proposed the use of additional sensors, antennas, or receivers. In this part of the tutorial, we aim to cover the basics of how a satellite-based navigation system works, the spoofing problem, countermeasures proposed and their limitations, and finally ongoing research efforts and important challenges that need to be addressed.

UWB, 5G, and WiFi. In order to satisfy the ever-increasing demand for ranging and positioning information, many communication systems, including UWB, WiFi, LTE, and 5G, have incorporated ranging operation as a feature. These systems target different use cases and provide different levels of performance and precision. For example, Apple iPhone and Samsung are using UWB as a *digital key*, and 5G positioning is expected to help in tracking a person requesting emergency services [9]. This part of the tutorial will elaborate on how ranging and positioning are enabled in these communication systems. We will compare them with respect to their performance, precision, and security guarantees. We will also discuss some case studies on how to design a secure ranging system.

Ongoing standardization efforts The motivation of the attacker to perform distance manipulation is increasing with the increase in applications that use ranging information. This has inspired academia and industry alike to develop secure ranging approaches, enabling security at both logical and physical layers. The standard IEEE 802.15.4z for UWB was finalized recently in 2020, and the hardware based on this standard is already available in the market [10]. Standardization efforts are in progress to enable secure ranging between WiFi-enabled devices as part of the Next Generation Positioning (NGP) standard IEEE 802.11az [11]. Similarly, 3GPP has plans to enable secure positioning in 5G, and multiple ranging techniques are being proposed to enable that [12]. In this part of the tutorial, we provide an overview of the approaches proposed in these standards.

Future Research Directions While much advancement has been done in the last decade, providing distance establishment with decimeter level accuracy in certain scenarios, enabling systems that can achieve performant, precise, and secure ranging under different channel conditions is still far from reality. This part of the tutorial will provide an overview of different research directions that someone can take to enable such ranging systems.

III. Tutorial Format & Pre-requisites

The tutorial will be delivered as a lecture and is planned for a duration of 3 hours. At the end of the tutorial, we will provide take-home hands-on exercises (e.g., use open source software GPS receiver to process GNSS signals, Matlab

exercises for understanding the security guarantees of the positioning systems discussed during the tutorial) that the attendees can try at their own convenience. If necessary, we can also provide a virtual machine with all the necessary software installed.

Knowledge Prerequisites: Although there is no stringent pre-requisite for this tutorial, the attendee will derive maximum benefit with a reasonable understanding of wireless communication fundamentals and general security notions. Basic Matlab or Python programming skills will help progress in the take-home hands-on exercises. We are also open to providing some learning materials before the tutorial for the attendees to brush up on some of the above topics.

IV. Biography of tutorial presenters

Mridula Singh is Faculty at CISPA – Helmholtz Center for Information Security in Saarbrucken, Germany. Her research interests are primarily in the areas of Systems Security, Wireless Networks, and Ubiquitous Computing. She is currently exploring various aspects of wireless and security to design secure autonomous systems. She pursued Ph.D. in Computer Science from ETH Zurich, Switzerland. The work she did during her Ph.D. was instrumental in enabling secure passive keyless entry and start systems of various car models. She holds an M.Tech degree with a specialization in Mobile and Ubiquitous Computing from IIIT-Delhi. She co-founded Trishulam while pursuing her master's degree. She worked as a research engineer at Xerox Research Center India, where she was involved in smart transportation and healthcare projects.

Aanjhan Ranganathan is an Assistant Professor in the Khoury College of Computer Sciences at Northeastern University in Boston, USA. He is interested in the security and privacy of wireless networks with a strong focus on autonomous cyber-physical systems and smart ecosystems. He has worked on a wide variety of topics including physical-layer security of wireless systems, secure localization and proximity verification, trusted computing architectures, and side-channels. He is a recipient of several awards including the outstanding dissertation award from ETH Zurich, regional winner of European Space Agency's Satellite Navigation competition and the Cyber Award from Armasuisse (Switzerland's Department of Defense). Prior to joining Northeastern, he was a senior researcher in the System Security group at ETH Zurich and has over 3 years of industry research experience as a senior engineer at Robert Bosch GmbH's Car Multimedia Division "Blaupunkt" where he was involved in the development of embedded modules for top automotive manufacturers including Audi and Volkswagen. He holds an M.Sc with specialization in Electronics and Microelectronics from EPFL, Switzerland and a Ph.D in Computer Science from ETH Zurich, Switzerland.

References

[1] "Contactless Payments: The Future Of Digital Payment Technologies," https://www.csiweb.com/what-to-know/content-hub/blog/contactless-payments-the-future-of-digital-payment-technologies/, [Online; Accessed 01. July 2021].

[2] "A Mac can be unlocked by an Apple Watch," https://support.apple.com/en-gb/guide/security/secc7d85209d/web, [Online; Accessed 01. July 2021].

[3] "How to Use NFC Door Locks," https://www.getkisi.com/academy/lessons/how-to-use-nfc-door-locks, [Online; Accessed 01. July 2021].

[4] L. Ferretti, C. Wymant, M. Kendall, L. Zhao, A. Nurtay, L. Abeler-Dörner, M. Parker, D. Bonsall, and C. Fraser, "Quantifying sars-cov-2 transmission suggests epidemic control with digital contact tracing," *Science (New York, N.Y.)*, vol. 368, no. 6491, May 2020.

[5] A. Ranganathan and S. Capkun, "Are we really close? verifying proximity in wireless systems," *IEEE Security Privacy*, vol. 15, no. 3, pp. 52–58, 2017.

[6] M.-A. Russon, "Drones to the rescue!" http://www.bbc.com/news/business-43906846, May 2018.

[7] "Six Ways Autonomous Driving is Relying on Precise Positioning," https://www.wardsauto.com/industry-voices/six-ways-autonomous-driving-relying-precise-positioning, [Online; Accessed 01. July 2021].

[8] A. Ranganathan, H. Ólafsdóttir, and S. Capkun, "Spree: A spoofing resistant gps receiver," in *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '16. ACM, 2016.

[9] "LRP deployment in automotive." https://www.3db-access.com/article/18, [Online; Accessed 25. March 2021].

[10] "802.15.4z - standard for low-rate wireless networks amendment: Enhanced high rate pulse (hrp) and low rate pulse (lrp) ultra wide-band (uwb) physical layers (phys) and associated ranging techniques," https://standards.ieee.org/develop/project/802.15.4z.html, [Online; Accessed 7. August 2018].

[11] "802.11az," http://www.ieee802.org/11/Reports/tgaz_update.htm, [Online; Accessed 24. September 2019].

[12] "3GPP," https://www.3gpp.org/ftp/Specs/archive/38_series/38.211/, [Online; Accessed 26. November 2019].