Introduction to the Cellular and Wireless Networks Minitrack

Edoardo Biagioni
University of Hawaii at Manoa
esb@hawaii.edu

John McEachen
Naval Postgraduate School
mceachen@nps.edu

Murali Tummala
Naval Postgraduate School
mtummala@nps.edu

1. Cellular and Wireless Networks

As everyone knows, this has been an unusual year. In-person meetings, including this conference, have gone entirely online. This minitrack, which first appeared in 2005, will be entirely online and asynchronous in 2021.

On the plus side for the development of Information and Communication Technologies, remote conferencing has become common, accepted, and even required for many work environments. Had the pandemic struck 20 years earlier, working from home would not have been an option for many of the workers who now daily telecommute instead of physically going to work. This ever greater diffusion of the internet into daily life is supported by a worldwide cellular network that is slowly moving towards the 5G vision of providing ever-higher throughput for our wireless connectivity.

While personal internet usage has skyrocketed, the Internet of Things (IoT) also continues its slow diffusion into both homes and those workplaces that are still active.

This ever widening availability of Internet access makes it easier for attackers to target equipment that may record sensitive information.

The first paper in this minitrack, which has been nominated for a best paper award, considers how an attacker capturing the timing advance signal from a mobile device may be able to locate that device. Depending on the 5G network's selection of specific parameters, the device may be located to a resolution ranging between 5 meters and 80 meters.

This paper was written when there was still hope of the conference being held in person, and the simulation presented in the paper is situated on the grounds of the conference hotel.

The second paper in this minitrack looks at snooping Bluetooth Low Energy (BLE) traffic from a pulse oximeter. While this iss a very specific attack, the technique illustrated in the paper is applicable more generally to devices using BLE to communicate. As in the previous paper, an attacker must be within wireless range to snoop the traffic, but if that constraint can be met, it seems likely that many other more that rely on BLE for communication might have similar weaknesses.

The final paper in this minitrack considers wireless ad-hoc networks, which are wireless networks where any device may forward data for other devices. In these ad-hoc networks, some devices, perhaps due to compromise, may be untrustworthy. By comparing a neighbor's report of being attacked to the device's own experience of being attacked, a device can over time determine the reputation and level of trustworthiness of the neighbor. This is designed to be similar to the way a colony of bees can make decisions in a distributed fashion, with each bee operating on limited information and with very limited compute power. The techniques described in this paper are designed to be scalable to larger networks, and are part of the broader field of Collaborative Intrusion Detection Systems, or CIDS.

We hope you enjoy these papers, and hope to see you in person at the 2022 HICSS!

URI: https://hdl.handle.net/10125/71445
978-0-9981331-4-0