Abstract

Today, location and proximity information are key to a number of emerging applications. With the advent of the Internet of Things and autonomous cyber-physical systems, the dependency on location and proximity is likely to increase in the future. Current proximity verification and ranging systems are prone to distance modification attacks that can lead to loss of property (e.g., cars [57]) and even human life (e.g., IMDs [119]). Additionally, GPS which is today the de-facto outdoor localization system is vulnerable to spoofing attacks [76] that forces a receiver to compute a false location. Given the safety and security implications of the applications mentioned above, it is important to ensure the security of the location and proximity estimates used in these systems. Existing solutions based on distance bounding are not suitable for a variety of applications or are not secure against all types of attacks. For example, the design and hardware complexity of current solutions make them unsuitable for contactless access control and authentication systems.

In this thesis, we address these shortcomings and make the following contributions. First, we propose a novel distance bounding system design called Switched Challenge Reflector with Carrier Shifting that enhances existing analog designs to be resilient against strong attackers capable of terrorist fraud. Second, we analyze and enhance a new class of chirp-based ranging solutions that enable the realization of low-power ranging systems. We analyze the security of existing chirp-based ranging systems and demonstrate their vulnerability to distance decreasing relay attacks. We then propose a novel design based on frequency modulated continuous wave (FMCW) and backscatter communication techniques, specifically designed for short-range contactless systems. Finally, in the context of outdoor localization, we present SPREE, the first GPS receiver capable of detecting or mitigating all GPS spoofing attacks described in the literature.