**Title:**

“Countering the Parking Lot Attack – Design for a Detection System Employing Monopulse Radar Methods to Detect and Spatially Attribute RF Targets in the 2.4 GHz ISM Band”

**Abstract:**

Many attacks on information systems occur when an adversary exploits wireless networking technology to remotely gain access to sensitive or confidential data within a targeted facility.   Where such attack vectors exist, even the most stringent physical security safeguards can fail in preventing an attacker from executing a stand-off attack aimed at compromising facility systems.   This class of attack, where the attacker remains positioned outside the physical confines of a facility and instead penetrates a network using a wireless vulnerability, is commonly referred to by security researchers as the “Parking Lot Attack”.  In this work, we present a scheme deploying an integrated network of sensors intended to detect and geo-locate any wireless emitter attempting the Parking Lot Attack.  We first introduce the context for such a system by presenting a threat model describing the facility and data systems targeted for attack.   Specific vulnerabilities in the attack surface of our model, which make the Parking Lot Attack a viable and preferred exploitation vector, are explained.  We describe the motivations and capabilities of the adversary employing this attack, and provide a constrained, but realistic Parking Lot Attack scenario which drives our detection system design.   A novel feature of our system is the use of monopulse radar methods to assign Line-of-Bearing estimates to a detected RF target.  We briefly cover monopulse radar theory, and then present a concept of operation and propose a deployment scheme for facility protection using our system.  We then discuss in detail the design and architecture of a second generation sensor implementation; a device which we constructed to perform real operational experiments.   We provide a quantitative analysis of the prototype hardware performance, which showed promise during controlled field testing.  We conclude with a discussion of simulation models we developed for our system to research deployment and operational strategy.