

Improvised Explosive Device Detection Based on Unintentional Electromagnetic Emissions

T. Hubing*, D. Beetner, S. Seguin, B. Moss, and M. Schmidt
University of Missouri-Rolla, USA

Improvised explosive devices are often manufactured from common and inexpensive components that contain active electronics. All active electronic devices, especially devices employing microprocessors or radio frequency receivers, radiate electromagnetic energy. The levels of these electromagnetic emissions are generally well above instrument noise levels even at distances far from the source. Previous investigations have shown that electromagnetic emissions from the types of electronic devices usually associated with IEDs have unique signatures that can be used to identify these devices even in noisy environments. Attempts to disguise these emissions or attenuate them with shields or filters are generally ineffective and may actually make these devices easier to detect.

This paper describes work performed at the University of Missouri-Rolla to detect and identify electronic devices that are commonly associated with IEDs at safe distances. The focus of this work has been the development of signal processing algorithms that detect the presence of threatening device signatures even when they are buried in noise generated by other electronic systems and intentional transmitters. A combination of algorithms working in both time and frequency domains is employed to zero in on the unique features of each device being detected. Current algorithms working with readily available receivers and digitizers are capable of detecting devices located tens of meters away in noisy environments. Enhanced algorithms in conjunction with specialized hardware should be capable of detecting devices at much greater distances. The techniques described can also be applied to the detection and location of other devices such as computers, cameras or audio recording devices.