Sandia develops secure wireless technology

June 22 2005

Project considered milestone for next generation of secure wireless networks

Sandia National Laboratories in cooperation with Time Domain Corporation and KoolSpan Inc. has developed a secure wireless Ultra Wideband (UWB) data communication network that can be used to help sensors monitor U.S. Air Force bases and DOE nuclear facilities and wirelessly control remotely operated weapon systems.

The new wireless technology also promises to be a gateway for a new generation of advanced sensors created by fusing UWB communication with UWB radar and used to detect intrusion of adversaries or insurgents for the protection of tactical forces and forward bases such as those deployed in the Middle East or Iraq. This is of particular value to the U.S. Air Force Electronic Systems Center (ESC) whose mission is to provide the latest in command, control, and information systems for the Air Force and who sponsored the work.

This secure form of wireless communication developed for practical use leverages UWB with the unyielding encryption protection of the 256-bit Advanced Encryption Standard (AES) to form UWB/AES. In an age of electromagnetic warfare and increasing threat from malevolent radio frequency (RF) attacks from high-tech adversaries, UWB is of strategic value providing stealth for covert operation by hiding within the noise floor to prevent detection and where other forms of RF communication find it virtually impossible to operate. UWB's probability of survival increases in a toxic RF battlefield when compared to many other forms

of RF.

UWB, also known as "impulse radio," is different because it does not use a carrier as do other forms of RF for wireless networking or communication technologies. Instead UWB transmits a flood of ultra-short microwave pulses of energy on the order of 100 pico-seconds (one pico-second is one-millionth of one-millionth or 10-12 second) in duration that extend over an extremely wide band of energy covering several Gigahertz of frequency.

"With the spreading of impulse energy over such wide frequency spectrum, the signal power falls near or within the noise floor making these signals extremely difficult to detect, intercept or jam and, when combined with AES, virtually impossible to crack," says H. Timothy Cooley, senior scientific engineer at Sandia. "Utilizing the immense available spectrum of UWB also improves wireless performance to accommodate the increased data rate needed by advanced sensors."

Among the key wireless features of the UWB/AES are its IP network compatibility and its "per-packet" rotating 256-bit encryption keys for even greater crypto-protection. The UWB/AES network architecture requires no computing infrastructure, provides real-time (hardware) encryption, and requires zero maintenance for complete self-recovery if interrupted or when a sensor goes down.

Based on tests conducted at the KoolSpan Encryption Laboratory in Santa Clara, Calif. this spring, Sandia with KoolSpan demonstrated a wireless UWB network bridge with real-time 256-bit AES encryption for live-streaming video images generated from a surveillance camera or thermal imager. The tests used only microwatts of transmitted power approximately 1000 times less power than typically used by conventional wireless IEEE 802.11b or Wi-Fi.

Source: DOE/Sandia National Laboratories