

Creating Adaptive Wireless Networks for Supporting Next-Generation Highly Mobile, Highly Secure Army Battle Command Systems

Dr. James P. Davis
Capt. Michael C. Haggard

jimdavis@cse.sc.edu
Computing Systems Design Laboratory
Department of Computer Science and Engineering
University of South Carolina
Columbia, SC 29208 USA

Abstract

The advent of higher-bandwidth wireless communications technology promises to facilitate creating a large-scale infrastructure of mobile, always-on, ubiquitous communications channels, thus extending the scope and capabilities of the Army's Battle Command System (ABCS) into a whole new range of applications and services. The extension of capabilities using wireless communications coupled with ubiquitous computing platforms (such as wireless PDA-types of devices or sensor networks that are either carried or are worn by field personnel) promises to radically change the Army's ability to further automate communication-intensive staff processes while also improving timeliness and value of intelligence through making real-time situational awareness and Intel data available through the wireless medium. This comes at a time when the Army has laid out its vision for a next-generation C4ISR architecture. At issue is the type of wireless communications to be adopted, and how such communications can be scaled and managed dynamically and securely in a wide range of quickly changing operational environments with different levels of security threat on the battlefield. In this paper, we discuss our approach to address the Army's concerns--using wireless LAN-based networking architectures as a means to establish a high-throughput, secure and adaptive platform on which to build a number of innovative applications for improving C4ISR in battlefield theatre of operations. Our approach is based on the development of models, architectures, prototypes and platforms for creating adaptive, self-monitoring, self-regulating, distributed systems using the biological model of "swarm" intelligence.

In this paper, we present ASOWN—Adaptive, Self-Organizing Wireless Networks--our approach to addressing this dual-pronged problem of availability and security management in a large-scale, ad-hoc wireless network. This work is to be based on creating self-regulation, environmental awareness, adaptation, and emergence properties in the wireless network. It is our belief that—in order for wireless communications to scale efficiently, while remaining adaptive and secure in a hostile, threat-oriented battlefield environment—the very nature of the wireless network Link Layer infrastructure must be rethought. To wit, we are embarking on research over a 2 to 3-year time frame that addresses this goal of creating a scaleable, manageable, secure wireless infrastructure—so vital to the evolution envisioned for the ABCS--through the creation of a model of WLAN "emergence". This is predicated on a redefined architecture for the 802.11 WLAN MAC Layer that is adaptive to its local conditions and is capable of detecting and responding to certain classes of security and availability threats in its environment. Furthermore, it is based on the premise of creating a VLSI implementation using reconfigurable computing techniques of this new MAC that is capable of realizing adaptive behavior of the individual station—thereby opening up the possibility for emergent properties of the wireless network as a whole to develop. We believe that true adaptability and ability to deal with operational conditions in the environment can be optimized most effectively through mimicking the model successfully employed in nature.

Index Terms: 802.11 LANs, Adaptive systems, Communications Security, Distributed Intelligence, Emergence, Reconfigurable Computing, Self-Organization, VLSI Design, Wireless Communications.