

# Portable High-Speed Mobile Networks

## Army Collaboration Increases Response Capabilities - Case Study

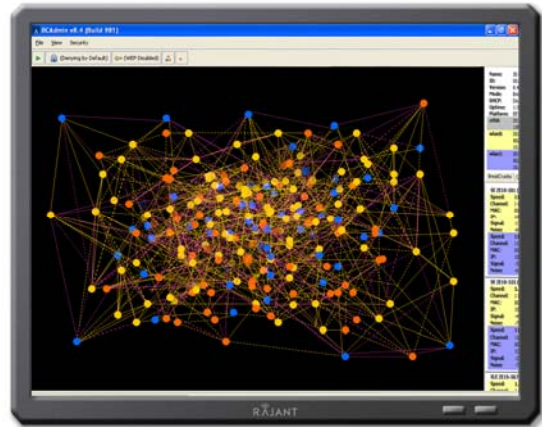


### Portable High-Speed Mobile Networks

Every minute, every day, in the rugged mining environment at the Kennecott Copper mine, over 200 vehicles go about their various missions, each connected and communicating vital information, automatically and with little administration. Location data, fuel information, vehicle routing, video, GPS coordinates, engine temperature, oil pressure, pump controls, load reporting, email, and other applications all reach their intended destinations because of the Rajant BreadCrumb®. These BreadCrumbs form portable high-speed mobile networks through wireless mesh technology and were developed under the guidance of US Army Communications Electronics Research, Development, and Engineering Center (CERDEC).

### Wi-Fi Battlefields and Mines

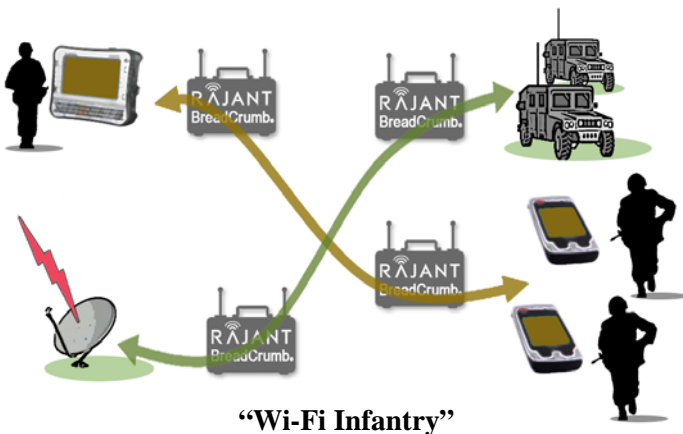
Similarly to battlefield operations, mining operations consist of many vehicles and personnel in a rugged terrain that require constant high bandwidth connections while they are all on the move. As in many military scenarios, there is no existing cellular, 3G or Wi-Fi infrastructure available to assist with the network for the ‘boots-on-the-ground’ foot soldiers. The Rajant BreadCrumbs alleviate this requirement by building a resilient wireless mesh capable of any-node to any-node communications. If a wide area link is required, the BreadCrumb network can easily transmit and receive data through a satellite, point-to-point wireless or wired link.



*Figure 1. Kennecott Copper Mine with Over two hundred Mobile Nodes (four hundred Access Points) in Constant Motion and Connection*

In the Fall of 2007, the BreadCrumb wireless mesh system was selected by Rio Tinto as its primary communications platform for operations within the Bingham Canyon copper mine. This mine is the world’s largest open-pit copper mine and is operated by Kennecott Utah Copper Corporation (KUCC).

Kennecott has successfully implemented over two hundred of the mobile BreadCrumb systems in an interconnected network that allows loader trucks,



## Portable High-Speed Mobile Networks

shovels, pumps, laptops and other production equipment to communicate with each other in real-time. This wireless deployment consists of over four hundred Access Points since each mobile BreadCrumb system consists of two separate access points. These commercially secure BreadCrumbs can scale to much higher node densities as the network grows and bandwidth availability actually increases. They interact with the data command center across a meshed, self-healing network for fleet dispatch, health monitoring and other critical mining applications. The nodes rapidly adapt to any changes in the network topology,



**Figure 4.**  
*Rajant BreadCrumb ME*

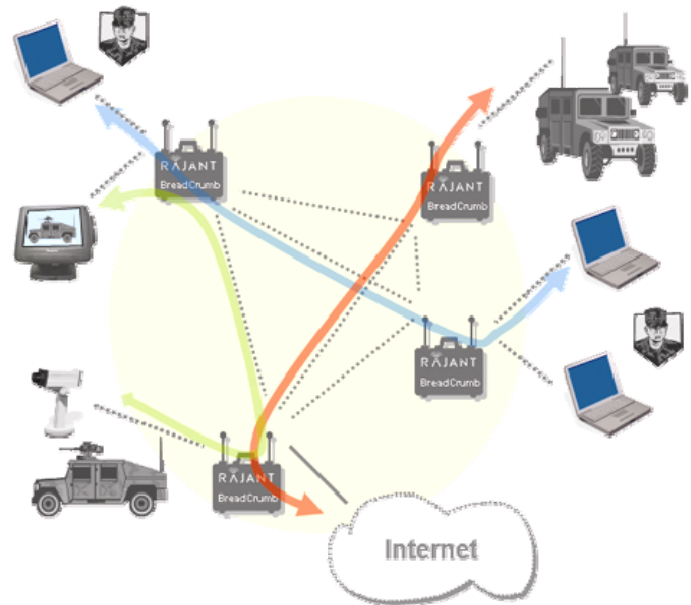
assuring that IP traffic uptime and bandwidth are maximized. The four hundred access points in this large (1x1x2 miles) open pit copper mine provide data transport for much of the operational data that is transmitted to vehicles and critical assets non-stop twenty four hours a day, seven days a week.

### IP Standards

These mobile networks provide first responder, military, homeland security and industrial personnel with voice and data communications across an ad-hoc self-healing network that can communicate with IP based client devices such as laptops, PDAs, video cameras, satellite terminals, networked radios and sensors. Through use of easily deployable wireless nodes such as Rajant Corporation's BreadCrumbs, rapid setup and reliable connectivity of the network is achieved.

The Rajant BreadCrumb line of products consists of small portable, mobile, self-configuring, battery powered, self-meshing, self-healing, wireless bridge and access points. BreadCrumbs are based on IEEE 802.11a/b/g WLAN technology and allow stand-alone networks to quickly organize in places where there is no standing infrastructure and require no network administration with single-button activation. The first responder, soldier on the battlefield or worker in a mine simply flips the 'on' switch and immediately has a self-integrating communications network.

### Rajant BreadCrumb Wireless Network (BCWN)



### Development

The BreadCrumb was developed as a result of the events of 9/11, when parts of the wireless communication infrastructure and emergency response networks were disabled as the result of terrorist attacks. As a result, Congress mandated an initiative that would give first responders a quickly-deployable wireless communications network which could provide instant IP communications including voice, data, and video for both civil and military applications.

BreadCrumb wireless mesh networking technology is an example of how government and industry participation can result in a complex and high-performance product within a short two year

## Portable High-Speed Mobile Networks

timeframe. Rajant Corporation developed this technology in conjunction with the CERDEC, Ft. Monmouth, NJ under a Research & Development contract. The resulting products from this continuing effort have been deployed to the various military units, first responders and commercial users in the US, Canada, UK, Thailand, Singapore and Australia.



### US Army CERDEC Collaboration

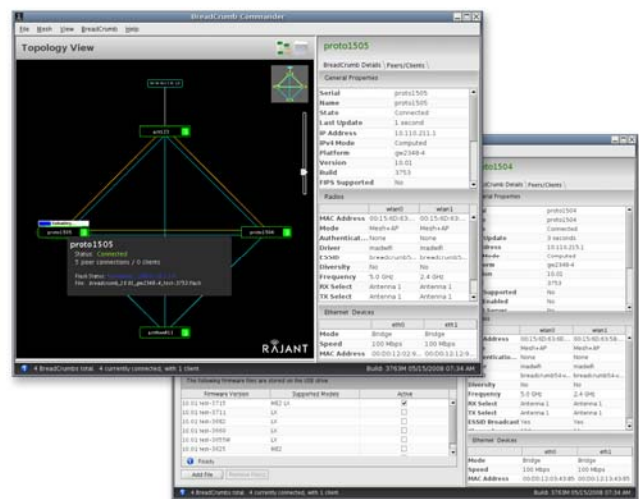
CERDEC and Rajant Corporation collaborated in the Monmouth County, NJ Homeland Security Exercise in 2003 that simulated an attack of a weapon of mass destruction. Participants included first aid squads, paramedics, fire departments, police and county, state and federal emergency coordinators.

The drill was designed to test the skills and preparedness of emergency responders and coordinators in the event of a large scale tragedy in conjunction with five local area hospitals. A Roaming Emergency Communications Network (RECON) consisting of Rajant BreadCrumb Wireless Networks (BCWNs) set up at the scene created an umbrella for surveillance and communication using cameras, cellular telephones, and handheld and laptop computers.

Another collaboration of CERDEC and Rajant was the Joint Warrior Interoperability Demonstration (JWID) 2004 hosted by U.S. Northern Command (NORTHCOM) and the Defense Information Systems Agency (DISA).



JWID was an annual Chairman of the Joint Chiefs of Staff event with the objective of finding technology solutions that will enhance the capabilities of combatant commanders, military services and agencies that support the U.S. Defense Department in its effort to provide Homeland Defense and Security. The focus was on connecting first responders at the local, state and federal levels with operational watch centers. BreadCrumbs were used with laptops, PDAs, wireless cameras, IP phones and sensors to connect a remote site to a command center through the Internet. A recently developed software management tool from Rajant, called "BC Commander", will help CERDEC manage, monitor and configure the BreadCrumbs remotely in real-time.



*Figure 2. Rajant BC Commander Management Tool*

The Rajant BreadCrumb XL was developed under Pathfinder ACTD, sponsored by the Special Operations Command and Urban Technology Office at the U.S. Army Soldier Systems Center in Natick, MA, serving as technical manager. This was an effort to integrate unmanned ground vehicles, unmanned aerial vehicles and unattended smart sensors into a mobile, self-forming and self-healing network. The network enhanced situational awareness, command and control capabilities and communications for commanders and assault forces operating in urban areas. In this exercise, the BreadCrumb network nodes



## Portable High-Speed Mobile Networks

transmitted line-of-sight (LOS) video and data up to three miles.

### Convoy, Search and Rescue

CERDEC and Rajant also collaborated on the man-wearable BreadCrumb for dismounted operations. The man-wearable BreadCrumb and the BreadCrumb XL were demonstrated in Convoy, Search and Rescue and Forward Operations Base (FOB) to transmit voice, video and data in environmentally challenging conditions. CERDEC provided technical engineering support, network design, architecture and contract management support, EMI/EMC, environmental, safety and AES encryption vulnerability testing. Rajant Corporation provided training and over thirty BreadCrumb wireless nodes including twelve man-wearable BreadCrumbs were used in the demonstration.



### Communications Interoperability Exercise

Interoperability of the Rajant BCWN with Department of Defense (DoD) systems was the focus in the DoD Interoperability Communications Exercise (DICE) at Fort Huachuca, AZ held twice in 2006. The primary purpose of the DICE exercises was to conduct interoperability certifications and assessments of communication systems and equipment to be fielded to DoD organizations. Testing was conducted in a simulated Joint Task Force network that mimicked networks currently deployed in support of various ongoing US operations throughout the world.



*Figure 3. Rajant BreadCrumb XL*

Test configurations for the DICE exercise included the use of remote thermal-imaging and ordinary IP cameras for video surveillance and integration of IP phones and portable handheld Personal Digital Assistants (PDAs) into the Breadcrumb network for Voice over IP (VoIP) communications between Breadcrumbs over the NIPRNET. Assessment was conducted on the BreadCrumb XL series product line that was configured to support SecNet11<sup>®</sup>. Harris Corporation's SecNet11<sup>®</sup> is a Type 1 encryption technology that is approved by the U.S. National Security Agency (NSA).

Following the bombings in the London Underground in 2005, Rajant Corporation participated in a trial of an underground wireless network in the subway tunnels. Having heard about the London Underground trial, the U.S. Mine Safety and Health Administration (MSHA) contacted Rajant to explore the possibility of using the company's solution in mines.

MSHA had formed a committee to evaluate communication and tracking system technology that could be adapted for use in underground mines. This effort was in response to the recent Sago and Alma mine accidents which indicated that functioning communication and tracking systems would benefit search and rescue efforts. MSHA solicited input from the public through its website for technology that could be applied in the underground mine environment to improve communications or provide personnel tracking ability.

MSHA field testing was conducted to determine:

- How well signals propagate in Line-of-Sight and Non-Line-of-Sight (LoS/NLoS) and what is the maximum distance between nodes

## Portable High-Speed Mobile Networks

- How much overburden systems can penetrate if capable of through-the-earth communication
- Mine coverage area
- Accuracy of tracking features
- Possibility of RF interference

The BreadCrumb SE was approved by the West Virginia Office of Miner's Health, Safety and Training (WV OMHS&T) as a wireless backbone communication device and is now listed on its website as fulfilling the state's safety requirements for underground mining.

### Rajant BreadCrumb ME2



- Rugged Wireless Mesh Node
- FIPS 140-2 in Process
- IEEE 802.11b/g Radio
- 11Mbps & 54 Mbps Bandwidth
- 100Mbps Ethernet Port
- Portable (weighs 2 lbs.)

The BreadCrumb ME2 has successfully been demonstrated by the US Army for tunnel communication operations. The Army is working to take advantage of the BreadCrumb networking communications ability to fulfill their need for rapidly deployed subterranean tunnel communications to respond to and eliminate Chemical, Biological, Radiological, and Nuclear and high-yield Explosives (CBRNE) hazards worldwide to support Joint and Army force commanders and warfighting operations, but also in support of homeland defense.

### Summary

Through its development efforts, Rajant has "application-proofed" the Rajant BreadCrumb wireless networks by providing powerful functions such as Address Resolution Protocol (ARP) filtering, Broadcast Filtering, Loop Control, and Load Balancing. In

addition, the network can provide Rajant's Automatic Protocol Tunneling (APT) to automatically leverage multiple points of connection to wired networks, 802.11i Security, Virtual LANs (VLANs), and Quality of Service capability (QoS), all while avoiding the single points of failure that other wireless providers cause using root nodes or LAN Controllers. Portable high-speed mobile networks are a valuable resource for first responders, military and mining operations. They create quick, standards-based wireless networks that are portable and rugged.

Since they do not require typical cellular or Wi-Fi infrastructure they are useful today in the battlefield. Through extensive testing and many collaboration exercises, the Rajant BreadCrumb has proven to be highly mobile, reliable, rugged and high performing in many scenarios- Homeland Security, Joint Warrior Interoperability, London Underground, Mining, DoD Interoperability Communications, CBRNE activities and more.



Rajant wishes to thank all the men and women in the Armed Forces including the US Army Communications Electronics Research, Development, and Engineering Center for its ongoing support.

► [www.rajant.com](http://www.rajant.com)

**Rajant Data Sheets**  
WEB QUICK LINK



Rajant Corporation • 400 East King Street • Malvern, PA • 19355 • tel 484.595.0233 • fax 484.595.0244