

A U.S. Army Reserve information technology specialist installs a satellite receiver in an exercise in Kaiserslautern, Germany. Urban areas, which may be battlegrounds in future conflicts, often are rife with various municipal and industrial sensors that could provide vital data to Army networks under the ARL's Internet of Battlefield Things (IoBT) research work.

Army Lab Seeds Revolutionary Networking Technologies

March 1, 2018

By Robert K. Ackerman

A rose may be more than a rose for battlefield communicators if U.S. scientists succeed.

Native plant life could join traffic cameras, motion detectors and enemy sensor systems as future sources of battlefield information if the U.S. Army Research Laboratory has its way. The laboratory is applying the Internet of Things approach to theater command, control, communications, computers and intelligence as it plans to equip soldiers and their leaders with vital knowledge from nontraditional information sources, and it is leaving no stone—or crop—unturned in its efforts.

These nontraditional sources can stretch the limits of the imagination. Three years ago, Swedish researchers were able to turn a living rose into an electronic circuit. And they accomplished this without killing the flower. Army scientists say the next step in this research is to turn the organic circuit into a sensor that could be networked on the battlefield.

Other unconventional sources are more mundane. Smart cities, which might find themselves hosting urban warfare, could provide the ultimate situational awareness through their public cameras, traffic sensors and acoustic devices. Both government and industry have street surveillance video sensors that can be tapped for data to input into a battlefield network. These sources could supply crucial information in noncombat missions such as disaster relief.

Exploiting these data sources is part of the Army Research Laboratory's (ARL's) work in the Internet of Battlefield Things (IoBT) Collaborative Research Alliance. This effort explores connected elements

Then, the network must compose the rose and other assets into a networked web that it can use. And it must adapt this dynamic information network to suit rapidly changing battlefield operations. "A single rose is a single rose, but a forest is very different," Russell offers.

A second IoBT research area involves autonomic actuation to enable intelligent services. Where the first research area centers on discovering and adapting the network, the second area aims to empower self-aware actuation. This diverse ad hoc network should be able to know what action to take on behalf of the Army. Research includes focusing on potential capabilities as well as establishing priorities to provide effective C2 across all sensors—friendly, adversarial and neutral.

The third research area addresses distributed asynchronous processing and analytics, which Russell describes as having a feedback loop that confirms the network is operating within parameters and has not been compromised. This area focuses on the data generated by the IoBT. In related work, researchers are attempting to push mission information to the edge of the network, where components would analyze local data and report only essential information to the commander.

All three research areas are interwoven, Russell says. They must interact in a secure and resilient way to meet mission objectives. The concept of C2 exists around all these areas and helps frame the mission and objectives of these devices, he warrants.

Suri points out that traditional C2 networks may consist of hundreds of sensors, but the IoBT could comprise millions of them. Its interconnected nature and complexity as well as the dependencies among systems increase the importance of autonomic aspects. No soldier or commander could manage this system individually, he says.

"Artificial intelligence and machine learning are critical," Russell echoes.

Also, researchers want to avoid building networks in which a single sensor triggers unanticipated cascading effects—the butterfly effect—detrimental to Army forces on the battlefield, Suri continues. Scientists also want to avoid automation surprise, in which systems take unexpected turns that stress commanders.

He notes that the IoBT brings its own communication capabilities, which could benefit U.S. troops in theater. For example, the open source long-range wide-area network radio modulation standard known as LoRaWAN aims to establish a set of publicly accessible gateways. Any sensor could use an available LoRaWAN gateway to send encrypted data reports to a cloud infrastructure, where they could be accessed and decrypted by an authorized user. The IoBT program is examining how the Army could leverage these communication methodologies, Suri allows.

Generating vast new types of data risks information overload, and ARL research aims to overcome that peril. Russell notes that reducing the need to move large amounts of data is part of the laboratory's IoBT effort. This might entail encoding or compressing data as well as enabling more processing at the edge. The key may be using bandwidth more effectively, he says.

Russell points out that the laboratory is taking a joint approach to its IoBT research. Examining C2 and mission command systems will help determine how the science of IoBT can be integrated and advanced in ways that deliver immediate capabilities before the long-term results are achieved. Applied research beyond the basic IoBT thrust would shorten the curve, he states.

The IoBT research effort could achieve more than just a new type of sensor system. Russell elaborates that a successful outcome "will significantly advance our understanding of how self-aware systems operate, how highly complex systems provide insight into what they're doing.

"The kinds of innovations that come out of this program will advance our understanding to a level where a soldier's ability to control a fully autonomous environment can happen in a way that is consistent with military doctrine and approaches," he adds.



U.S. soldiers with the 2nd Theater Signal Brigade camouflage a satellite transportable terminal and its generator. The ARL's IoBT research seeks to make better use of available bandwidth as it adds diverse data to the network.



A soldier with the 1st Infantry Division provides security during exercise Allied Spirit VII in Hohenfels, Germany. In the future, the trees surrounding the soldier may be used as networked sensors if work underway at the Army Research Laboratory (ARL) bears fruit.

such as sensors, small actuators and network devices that can be integrated on the battlefield. Stephen Russell, chief of the ARL's Battlefield Information Processing Branch, describes IoBT research as a convergence of cyber, sensing, mechanical and network technologies. The ARL is striving to bring interdisciplinary research in IoBT technologies to fruition, Russell states.

The laboratory's research on the IoBT falls into two categories. One tends to focus on near-term advances that could see their way to the battlefield in a few years. These would build on largely known technologies and capabilities. The other research prepares for the longer term and may produce truly groundbreaking advances.

Russell explains that many of these nontraditional data sources are becoming both smaller and more ubiquitous in diverse locales ranging from urban areas to austere environments. In military settings, sensor systems belonging to U.S. forces, allies, adversaries and noncombatants alike can contribute to the wealth of IoBT data. Add local flora, and the result is a truly organic network.

"The fear that the trees are listening, which comes out of storybooks as old as a hundred years, is the reality now," Russell states. He adds that recent research turned a living plant into a battery. So even the support elements that empower electronic devices can have a broad presence in these nontraditional sources. "The trees are not only listening, but they also are powering themselves," he offers.

Russell continues that adding artificial intelligence and machine learning can create a convergence, leading to smart trees with self-awareness, their own internal power sources and the ability to listen. "This really changes the battlespace—the way that the Army operates," he warrants. "It really changes command and control in a really big way."

Niranjan Suri, the ARL's Information Sciences Division associate for research, describes how the IoBT raises several issues in command and control (C2). Because information comes from assets the Army does not own, the service must take a different approach compared with data generated by its own sensors. The Army does not control the nontraditional sensors or their communication pathways. This brings up the question of whether data from someone else's source can be trusted, he points out, especially if it can be manipulated by an adversary.

Russell adds that the Army must learn to defend against this new information posing a threat of its own. Similarly, the service must prevent an enemy from employing the same tactics against its own sensor systems. Basic research must include understanding the consequences of these advances, especially how they affect joint and coalition partners. "Understanding the underlying science, in terms of how to do this in complex systems and control system dynamics, is particularly critical and an emergent research area," he states.

Suri explains that when the Collaborative Research Alliance was created two years ago, the ARL began by examining how the IoT would change the commercial environment. Rather than just allow the IoT to affect the Army, the laboratory opted to leverage it in a proactive sense. Suri relates that the ARL looked at applications such as logistics and sensing, paying particular attention to burgeoning municipal capabilities such as transit, weather and traffic monitoring. Databases also can come into play. Knowing the inventories of local hospitals can be life-saving both in combat and disaster relief, Suri notes.

One key research area is device information discovery, composition and adaptation. Russell indicates that in the IoBT, networks will be highly dynamic. For example, if a rose becomes an antenna that is powered by other roses, then the network must discover that capability and ascertain its utility.