Ancile: Pervasively Shared Situational Awareness

Ancile is a distributed architecture for information sharing that satisfies the needs of tracking personnel and notifies them of events of interest in their vicinity. It was demonstrated to be effective in notifying soldiers to mortar rounds that were already in the air; the soldiers who would have been hit by the rounds had sufficient time to leave the impact area before impact. This article describes extensions to the Ancile architecture that make it significantly more flexible and allow it, for instance, to support notifications to emergency response personnel in times of crisis.

Fernando Maymí, Manuel Rodríguez-Martínez, and Yi Qian
University of Puerto Rico at Mayagüez

Paul C. Manz
US Army, Armament Research, Development, and Engineering Center

Improvised explosive devices pose a major threat not only to military personnel in combat zones, but also to first responders during terrorist attacks. In this article, we discuss Ancile, a prototypical military information system that warns dismounted personnel — those who aren't inside a vehicle or fixed facility, such as soldiers on patrol — about imminent threats while simultaneously reporting their locations to existing command and control systems. The main component of this system is a pager-like device that each person — whether a soldier or first responder — wears. Each device periodically transmits its location and listens for threat warnings. When the device receives a threat warning, it sounds an alarm that increases in frequency as the threat approaches. In our experiments using live mortar shells, we had from a few seconds to well over a minute to improve our protective posture before the rounds detonated.[1]

Architectural Overview

The Ancile network, shown in Figure 1a, is centered on several top-level information stores wherein data is organized, validated, managed, and distributed to all other nodes. These stores provide services that require centralization, such as maintaining global information and interfacing with external command and control centers. The Command Stations and Information Stores comprise the top layer of our ar-

1089-7801/08/$25.00 © 2008 IEEE

chitecture, which we call operational because its information systems are used by leaders to command and control field operations.

Although these information stores and operational command systems can communicate directly with the devices, they typically do so with intermediate nodes instead. These nodes can be bridges that span a wide-area network to the Ancile wireless network. Some nodes offer a more traditional interface into the system by presenting a display screen along with an input mechanism. These intermediate nodes are typically installed on vehicles that support dismounted personnel in an area of operations.

Besides these nodes, the bottom or tactical layer is comprised of small, inexpensive, and unobtrusive devices, similar to pagers. These devices store whatever situational awareness (SA) is relevant to the user's mission and constantly check their location against the local SA database to determine whether the user has entered an area with an active information item (such as an unstable structure or a gas leak). The data is organized in such a way to facilitate the frequent location checks that must be performed to generate alerts or user messages.

Typically, events — which are made up of a description, a geographical region, and a timeline — enter the system at one of the top-tier nodes and then propagate throughout the network. When another node receives the event's message, it reacts in one of three ways: first, it can generate a user alert if time and location triggers are met; second, it can store it for future reference if storage permits and the event concerns the broader area of interest to the node; third, it can pass the message to another node for validation, notification, or relay.

Events can also enter at the lower tier nodes. For instance, an injured rescuer can press a button on the device that sends out a call for help; neighboring personnel would receive the distress message and the directions to their fallen comrade even as the message propagates up the system so that the relevant leaders are also aware of the problem.

Given that users are able to feed events into the system, the information store managers must be able to corroborate, refute, or leave unchanged any information item that arrives from the portable units. When an item is corroborated, its integrity level increases to the level of trusted data.[2] In the future, as other devices receive the message, they will note that it has been validated and thus will afford it a higher confidence level. If the item is refuted, a message is generated that instructs all portable units to ignore and delete the information item. Although messages are normally validated by trusted users at the operational layer, in the future, we'll explore automated mechanisms by which the nodes can independently calculate trustworthiness based on parameters such as message source and related messages from other sources.

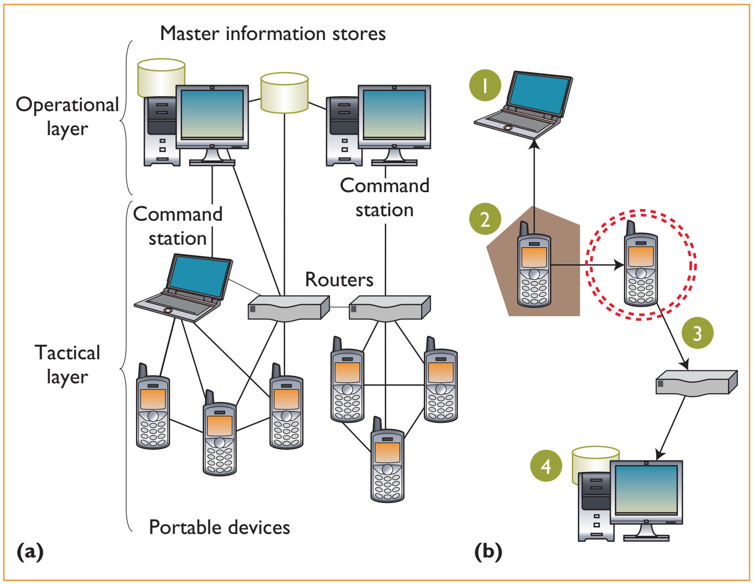

Figure 1. Ancile system architecture. (a) Ancile system architecture showing a top level of data stores that manage user locations and events of interest to them. (b) Sample message flow with device 2 generating an event warning that is relayed through a neighboring device and its bridge to a top level data store for validation.

Basic Information Exchange

When portable units come within range of each other, an information exchange occurs that lets each unit determine what, if any, information should be shared. Figure 1b illustrates this data exchange. At the heart of this process is the identification of specific information items that are of local (both temporally and geographically) interest to a device. Although the locality is easy to quantify using factors such as position, time of day, direction, and speed of travel, it's significantly more challenging to describe what, exactly, is of interest.

Our proposed architecture initially addresses the descriptions of this information through the use of hierarchical data descriptor tags. These tags, defined using the extensible markup language (XML), let us develop fairly simple dataset hierarchies while providing the ability to extend these as needed to support diverse user populations. The information needs of, say, firefighters in New York City could then be satisfied with the same base system as those of soldiers in Iraq; the key parameter that would differ is the schema for describing the data that these two populations need.

To address operational security concerns and control the amount of traffic on the networks,[3] each device can be configured to be more or less "chatty." This means that nodes higher up on the hierarchy, which would thus be assumed to have better feeds from external information systems, will tend to broadcast more information than the devices worn by the soldiers. The devices however, would be able to sense when a neighbor is unable to communicate with a higher node and could then decide whether to share information.

Ancile works very well at warning dismounted soldiers about incoming mortar fires; we think it will work equally well for crisis management. The system described in this article provides an adjustable architecture that enables geotemporal information to be proactively provided to the right users at the right time. This architecture can be modified to meet a specific user's needs in view of the spatial, temporal, and network constraints that affect system-wide information exchanges. The number of potential Ancile-related applications in both the public and private sectors continues to expand at a rapid pace. The continued focus on foundation imperatives (including flexibility, small size, lightweight, long life, low unit cost, simplistic operation, and minimal user intervention) will enable its widespread employment across these large, diverse communities and achieve economies of scale. In the near term, Ancile provides a force protection and life-saving solution path for deployed troops, emergency response personnel, and public safety professionals.

References

1. F. Maymí and P. Manz, "Ancile: Dismounted Soldier Tracking and Strike Warning," *Proc. 25th Army Science Conf.*, US Army, 2006.
2. K.J. Biba, *Integrity Considerations for Secure Computer Systems*, tech. report MTR-3153, MITRE, Apr. 1977.
3. R. Campbell et al., "Towards Security and Privacy for Pervasive Computing," LNCS 2609, Springer-Verlag, 2003, pp. 77–82.

Fernando Maymí is a lieutenant colonel in the US Army currently pursuing a PhD in computing and information sciences and engineering at the University of Puerto Rico at Mayaguez. His research interests include network security, distributed systems, wireless networks, network science, and bioinformatics. Maymí has an MS in computer science from the Naval Postgraduate School. He is a senior member of the IEEE. Contact him at maymi@ece.uprm.edu.

Manuel Rodríguez-Martínez is an associate professor at the University of Puerto Rico at Mayaguez's Department of Electrical and Computer Engineering. His research interests include systems, wide-area middleware technology, adaptive interoperability, extensible database systems, query optimization, wireless databases, the Web and databases, computer networks, and Java technology. Rodríguez-Martínez has a PhD in computer science from the University of Maryland at College Park. Contact him at manuel@ece.uprm.edu.

Yi Qian is with National Institute of Standards and Technology. His research interests include network security, network design, network modeling, simulation, and performance analysis for next generation wireless networks, wireless sensor networks, broadband satellite networks, optical networks, high-speed networks, and the Internet. Qian has a PhD in electrical engineering from Clemson University. Contact him at yqian@ieee.org.

Paul C. Manz serves as the deputy director for enterprise management in the Armament Research Development and Engineering Center (ARDEC) overseeing the Army's Lethality Center of Excellence portfolio. He has both an MPA and BSSE. Manz is a senior member of the IEEE and a multiple-certified senior member of the Army Acquisition Corps. Contact him at paul.manz@us.army.mil.