Pervasive and Mobile Computing 5 (2009) 133–134

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

journal homepage: www.elsevier.com/locate/pmc

Editorial

Introduction to the special issue on homeland and global security

Larry Holder [a,*], Mohan Kumar [b], Raffaele Bruno [c]

[a] *Washington State University, USA*
[b] *University of Texas at Arlington, USA*
[c] *Institute for Informatics & Telematics, Italy*

ARTICLE INFO

Article history:
Available online 3 December 2008

The development, deployment and coordination of pervasive and mobile computing has been studied for a number of years, and much of this research is beginning to transition into real solutions for a variety of domains. One domain that is ripe for research and development in this area is homeland and global security. Much of the security mission involves the monitoring of various environments (e.g., ports, borders, mass transit hubs, financial centers, power grids, the Internet) and the prediction and detection of threats to these environments. Pervasive and mobile computing represents a general solution to maintaining security in these environments. Components of such solutions include novel sensor and sensor systems for the detection of various threats, efficient and effective deployment of mobile devices and sensors in such environments, heterogeneous systems for surveillance and threat detection, secure and fault tolerant coordination and communication of sensors in homeland and global security environments, information fusion for prediction and detection of threats, integration and registration of data from multiple sources, and effective decision-making in dynamic environments. Since the nature of the challenge restricts in situ testing of the various approaches, high-fidelity simulation and modeling of such systems is necessary, including the mobile devices and sensors, their communication, the data produced, the characteristics of potential threats, and the temporal interaction in response to the sequence of events leading up to the threat.

The advent of pervasive and mobile computing on one hand and the rapid progress in sensor systems and RFID tags on the other have paved the way for the application of three important problems related to global and homeland security: (i) surveillance systems; (ii) military command and control systems; and (iii) crisis prevention, management, and recovery. Static and mobile video cameras, RFIDs, and sensor networks, that provide different media streams (video, audio, signal, textual data and images), together with such techniques as context awareness, information fusion and others are being employed to enhance the view and scope of video surveillance systems [1]. Hostile environments, including crisis management and military situations require adaptive deployment of application services proactively and autonomously. In many such scenarios direct human involvement may pose health and safety problems to the individuals involved. Increasingly, individual robots (including mobile) are deployed to perform such tasks. In modern highly dynamic tactical scenarios, warfighters will not only execute orders from the command center but also make real-time, highly critical collaborative decisions that require timely access to high quality tactical information from diverse sources such as sensors, robots, satellites, and other warfighters in the field [2]. Traditional information systems lead to additional communication and thus incur high energy cost critical to dynamic resource-constrained environments. Given the technological advances, it is imperative to employ advanced techniques to maintain up-to-date consistent information in a distributed fashion on readily accessible and available devices. The users in a military environment typically use heterogeneous mobile devices to access secure information and issue commands anywhere at any time. Sensor systems and associated software tools can be effectively employed to monitor the physical environments, and pervasive and mobile computing devices can be used to deploy appropriate services and manage the situation. Since conventional communication infrastructures can be

* Corresponding address: Washington State University, School of EECS, Box 642752, 9164 Pullman, WA, USA.
E-mail address: holder@wsu.edu (L. Holder).

1574-1192/$ – see front matter
doi:10.1016/j.pmcj.2008.12.001

totally unavailable, or seriously damaged (such as in the aftermath of a disaster or large-scale crisis), self-organizing and autonomic systems appear as the only viable approach for supporting dependable communications services in such military and emergency scenarios [3].

In this special issue we present state-of-the-art research on pervasive and mobile computing applied to the challenges of homeland and global security. Most such solutions to security challenges involve the deployment of sensor networks and the efficient collection of data from these sensors. However, these networks may be subject to deliberate attempts to disrupt the network and the flow of data. Mpitziopoulos et al. address these challenges in their article "JAID: An Algorithm for Data Fusion and Jamming Avoidance on Distributed Sensor Networks", where they describe an approach by which mobile agents traverse the sensor network in an efficient manner while avoiding portions of the network subjected to jamming and maximizing the significant information collected by the sensors. Results from simulated attacks show the superiority of their approach over alternative solutions.

Target localization and tracking is a fundamental functionality for many security applications. However, target localization presents inherent challenges including tracking accuracy, target classification, scalability and energy consumption. In their paper entitled "Self-Organization of Unattended Wireless Acoustic Sensor Networks for Ground Target Tracking" Zhang et al. describe a system of acoustic sensors for an accurate and power-aware localization of acoustic sources. Instead of using pre-assembled microphone arrays, which would be infeasible for large-scale and unplanned network deployments, they propose to organize the sensor nodes into localization sensor groups that can work as virtual acoustic sensor arrays. Then, a bearing-only triangulation method is used for source localization. The aim of the proposed self-organization algorithm is to achieve a trade-off between tracking performance and energy efficiency. Results from a simulated system show that their solution outperforms alternative schemes, such as the closest node approach, in terms of tracking error, while preserving energy resources.

To improve tracking performance, in their article "Target Localization in Camera Wireless Networks", Terzis et al. describe a multi-modal sensor network consisting of networked cameras with pan, tilt and zoom capabilities and tiny sensor nodes equipped with magnetometers. They propose a multi-stage system, where cameras are first used to self-localize the non-imaging sensors. Once localized, ground sensors can accurately detect the presence and position of moving targets, and pilot the cameras to capture images of those targets. In addition, they design a self-calibration procedure, which allows sensors to discover their orientation and to simplify the localization problem. Their results from both an experimental deployment and a simulated system demonstrate the scalability and accuracy of their proposed approach.

In their article "Integration of Sensing and Computing in an Intelligent Decision Support System for Homeland Security Defense" Wu et al. describe a more comprehensive approach for applying pervasive and mobile computing to security problems. They address many of the components along the chain of processing from sensor data collection to high-level decision making: sensor deployment, data routing, network mapping, and data fusion. For sensor deployment they use a genetic algorithm to achieve maximum converge given cost constraints. Their data routing scheme maximizes signal strength and minimizes path loss while maintaining high energy efficiency and effective fault tolerance. They use network mapping to assign computing resources to network nodes in order to maximize distributed computational resources. Finally they optimize the thresholds on binary decision rules to maximize hit rates while minimizing false alarm rates. Their results show that the integration of these components improves decision-making performance.

Dependable and broadband communication is extremely important during disaster recovery and emergency response operations to permit the reliable circulation of critical data. In situations where infrastructure-based communication is not available or has been disrupted, mesh network technology may represent the only technology to dynamically deploy temporary networks that provide communication services for efficient crisis management. In their paper "SafeMesh: A Wireless Mesh Network Routing Protocol for Incident Area Communications" Pirzada et al. advocate the use of hybrid mesh networks, which allow both mobile clients and dedicated infrastructure nodes to form the network and provide routing and forwarding functionality. Then, they propose a novel routing algorithm, called SafeMesh, to exploit the high degree of heterogeneity in hybrid mesh networks, as well as the dynamicity of the network environment. Both simulation and experimental results show that the SafeMesh protocol achieves superior performance over versions of AODV that implement recently proposed routing metrics for wireless mesh networks, including multi-radio mesh networks.

The security of our national and global infrastructures have never been more important in order to ensure the safety and sustainability of our society. The use of pervasive and mobile computing for homeland and global security challenges holds significant potential for improving our ability to automatically detect, pre-empt, and respond to security risks. The research described in this special issue indicates that significant progress has been made in this area, but that there are many important challenges still to be addressed. We hope that this special issue will provide some insight into this field and prompt continued research and progress toward using pervasive and mobile computing to improve the safety and security of our homeland and global communities.

References

[1] R. Cucchiara, Multimedia surveillance systems, in: Proceedings of the Third ACM International Workshop on Video Surveillance & Sensor networks (VSSN'05), International Multimedia Conference, Singapore, Nov. 11, 2005, pp. 3–10.
[2] P. Marshall, Tactical networking: It's more than just command and control, DARPATech, Anaheim, California, 2007.
[3] R. Bruno, M. Conti, A. Passarella, Opportunistic networking overlays for ICT services in crisis management. International Conference on Information Systems for Crisis Response and Management. Washington, DC, USA, May 4–7, 2008.