The AI Technologies of the Philadelphia Area Urban Wireless Network Testbed

Gustave Anderson and **Andrew Burnheimer** and **Vincent Cicirello*** and **David Dorsey** and **Chris Dugan** and **Iris Howley** and **Moshe Kam** and **Joseph Kopena** and **Rob Lass** and **Kris Malfettone** and **Andy Mroczkowski** and **Gaurav Naik** and **Max Peysakhov** and **Brian Pyles** and **William Regli** and **Evan Sultanik** and **James Thiel** and **Kyle Usbeck** and **Dan Venutolo** and **Marc Winners**
Department of Computer Science and Department of Electrical and Computer Engineering
Drexel University, 3141 Chestnut Street, Philadelphia, PA 19104

Introduction

Drexel University's College of Engineering has been working with local law enforcement and transportation officials to develop a Philadelphia Area Urban Wireless Network Testbed (PA-UWNT) (Cicirello *et al.* 2004). The PA-UWNT is a mobile ad hoc network (MANET) consisting of PDAs (HP iPAQs), Tablet PCs, and laptops. The PA-UWNT integrates: 1) the industrial-strength mobile agent platform of Lockheed's Advanced Technology Laboratories known as the Extendable Mobile Agent Architecture (EMAA) (Lentini *et al.* 1998); 2) an 802.11b wireless network with ad hoc routing; and 3) lightweight computing platforms such as PDAs and Tablets. MANETs, such as the PA-UWNT, can allow for a "bring your own network" solution to communications and management of rescue workers at the location of a natural disaster, where traditional networking infrastructure is not likely to exist or at best is likely to be inoperable. One of the goals of the PA-UWNT is to enable researchers at Drexel University to study research problems of importance to the enabling of police, fire, security, and other emergency personnel to communicate and collaborate effectively over MANETs.

Drexel University—in coordination with local public protector and transportation agencies such as the Philadelphia Police Department, Amtrak, Septa, University City Police, and Drexel Security—have been establishing areas of interest within the city of Philadelphia that present challenges to the eventual deployment of such a system. Some of these are shown in Figure 1 and include: subterranean platforms and corridors/tunnels, consisting of many metal columns and dense interior architecture; large and small buildings that provide communication signal problems due to multi-path, reflections, and interference; and combination of buildings and trees over an extended area creating special radio frequency and modulation needs.

During the Intelligent Systems Demonstration program, we propose to demonstrate some of the AI technologies that are under development as part of the PA-UWNT. These include network-aware agents (see Section), disruption tolerant vote collection (see Section), and localization (see Section), among others.

*Contact author: cicirello@cs.drexel.edu

Figure 1: Examples of Urban Testing Areas in Philadelphia

Supporting Infrastructure

The PA-UWNT builds upon the technology and infrastructure developed as part of the Secure Wireless Agent Testbed (SWAT) project. SWAT is a unique facility developed at Drexel University to study integration, networking and information assurance for next-generation wireless mobile agent systems (Sultanik *et al.* 2003).

SWAT provides agents with secure multi-layer, agent-to-agent group communication on resource-constrained devices. The security framework uses a combination of symmetric and public-key cryptography to support encrypted communication at both the network and the agent application layers, including support for secure group communication. The cryptographic tools integrated in the current implementation of SWAT include: CLIQUES, the Tree Group Diffe-Hellman (TGDH) algorithm, Spread, Secure Spread, a SEcurity Mediator (SEM), and IPSec.

Each host in the SWAT is an integration of the agent system, the network, and security infrastructure. The agent framework contains mobile agents, and static agents (services). The security components include group key management, and group membership revocation, enforced by a security mediator. The agent framework is connected to the security components, enabling an agent (or the whole agent system) to join or leave a group, with the permission to join controlled by the security mediator. The network compo-

nents enable secure point-to-point communication for the agent framework, as well as reliable group communication for the security components. Point-to-point communication is implemented using TCP/IP and is secured using IPSec.

The SWAT infrastructure consists of PDAs, tablet PCs, and laptops on an 802.11b wireless network with ad hoc routing. SWAT is developed on the Familiar Linux distribution, using the Intel Strong Arm architecture found within the HP iPAQ h3800 series PDAs. A similarly configured Linux environment exists for the x86 architecture, to incorporate other portable devices to the testbed such as laptop and tablet PCs. SWAT makes use of Cisco Systems' Aironet 350 series PCMCIA cards across all platforms. The Aironet cards were selected based on empirical studies, demonstrating that the Aironet cards have the best performance in ad hoc mode compared to other network cards.

Network-Aware Agents

The dynamic and uncertain nature of the state of a MANET (Wu & Stojmenovic 2004) has the potential to result in inefficiencies as well as complete failures if it is ignored. Agents at the agent system layer may need to reason about the dynamics of the MANET layer (Peysakhov *et al.* 2004; Artz, Peysakhov, & Regli 2003). A mobile agent may need to migrate to several hosts sequentially to complete a given task. Consider as an example an agent that is tasked with monitoring the battery levels of the hosts on the network. Such an agent might need to traverse the network, collect the data, and return to its source – perhaps a network management tool. For any given MANET topology, there may exist one or more itineraries that are more efficient than others. An agent that considers the topology of the MANET as well as other data such as signal strengths of the links in selecting its itinerary is likely to require less time to complete its data collection task. The problem is further complicated by the fact that in a MANET, the topology and other network characteristics are dynamic. An itinerary planned ahead of time can become obsolete quickly as the network's link-state changes. An agent that considers such dynamics and reasons about the uncertainty of the MANET – perhaps predicting future topological change – using a dynamic itinerary can further enhance its data collection performance. In either of these cases, an agent reasoning about the current state of the MANET or reasoning about the dynamic state of the MANET, the data collection agent is more likely to return timely results. The timeliness of this task can be integral to preventing a costly failure.

Disruption Tolerant Vote Collection

For wired networks, the time cost to collect votes from a set of agents and the accuracy of the vote count are largely deterministic parameters that depend on the size of the agent population. This is due to the fact that one can assume that inter-agent communications is stable and reliable, resulting in perfect information in reasonable time and with negligible network cost. In stark contrast, MANETs create a dynamic and unstable environment in which communication is under constant disruption. Decision making procedures for agents operating on MANET-like environments must adapt to the communications environment in order to make accurate decisions without vast increases in cost. The approach taken by the PA-UWNT to distributed decision-making when communications is unreliable and networks are disruption-filled exploits the ant-based quorum-sensing behavior of social insects to control mobile vote collection agents. This allows us to mitigate the increased communications costs with only a slight decrease in decision quality. The approach uses the properties of emergent stability, decentralized control, and resilience to possible disturbances much like a real ant colony. Experiments confirm the utility of our technique in simulated MANET environments.

Localization

In many environments, especially urban environments, Global Positioning Systems (GPS) often perform poorly. Buildings, trees, and vehicles can obscure the view of satellites from the GPS receiver. Even in a relatively flat locale, clouds and smoke can temporarily obscure satellites, rendering GPS receivers unable to determine location. In the PA-UWNT, nodes that have lost GPS signals, do have some information available to them that can be useful in producing an estimate of their location. Network-aware agents are used to efficiently publish the GPS locations of nodes across the MANET of the PA-UWNT. Thus, "lost" nodes have the location of the nodes directly connected to them, and location of nodes indirectly connected to them via multi-hop MANET routes. The range of all the network cards is also known, and therefore the area over which the lost node could or could not be. This information is used with a Kalman Filter to compute an estimate of the node's location. Additionally, we have shown that signal strength (a network parameter passively accessible) can be a good indicator of distance. Using this, among other network parameters, the PA-UWNT hosts learns functions mapping signal strength to distance to neighboring hosts. These distance functions can then be used to further refine our location estimates.

References

Artz, D.; Peysakhov, M.; and Regli, W. C. 2003. Network meta-reasoning for information assurance in mobile agent systems. In *18th IJCAI*, 1455–1457.

Cicirello, V. A.; Peysakhov, M.; Anderson, G.; Naik, G.; Tsang, K.; Regli, W. C.; and Kam, M. 2004. Designing dependable agent systems for mobile wireless networks. *IEEE Intelligent Sys.* 19(5):39–45.

Lentini, R.; Rao, G. P.; Thies, J. N.; and Kay, J. 1998. Emaa: An extendable mobile agent architecture. In *AAAI Workshop on Software Tools for Developing Agents*.

Peysakhov, M.; Artz, D.; Sultanik, E.; and Regli, W. C. 2004. Network awareness for mobile agents on ad hoc networks. In *Proc of AAMAS-2004*.

Sultanik, E.; et al. 2003. Secure mobile agents on ad hoc wireless networks. In *Proc of IAAI-03*, 129–136.

Wu, J., and Stojmenovic, I. 2004. Special issue on ad hoc networks. *IEEE Computer* 37(2).