The Virtual Node Infrastructure Approach to Programming Cyber-Physical Systems

Nancy Lynch, Calvin Newport
MIT Computer Science and Artificial Intelligence Lab
Cambridge, MA 02139, USA

1 Challenges

Many proposed applications for Cyber-Physical Systems will be implemented on a network of computing devices, communicating wirelessly using local broadcast. The network may be *ad hoc*, in that the participating nodes are not known a priori and must self-configure into a coherent network, and *dynamic*, in that the participating nodes can change over time as nodes enter and leave the area of interest, fail, and recover.

Currently, it is difficult for programmers to write, debug, and verify applications that will run robustly under such conditions. These practioners would benefit significantly from clean, well-defined *abstraction layers* that can mask some of the failures, uncertainty, and change inherent to this setting. It is up to the research community to produce these abstraction layers. In fact, we believe that the development of good abstraction layers for dynamic ad hoc networks should be a major goal of any Cyber-Physical Systems research initiative.

The mobile network research community is currently producing *communication abstractions* such as IP-style point-to-point routing for mobile ad hoc networks, and reliable broadcast dissemination. Communication abstractions alone, however, are not enough for systems that need to interact meaningfully with a real-world environment. Consider, for example, a first responder network that needs to monitor temperature changes over time within a burning building, or a campus-based PDA network that needs to maintain "virtual graffiti walls" at several well-trafficked locations. In both scenarios, reliable communication alone does not greatly simplify the task.

To facilitate the development of Cyber-Physical Systems we need abstractions that encapsulate *data-management functions*, such as data collection and dissemination, data storage, and query processing. We also need abstractions that encapsulate *planning and control*, and an *overall architecture* to fit these abstractions together into a coherent whole.

2 An Approach: Virtual Node Layers

For the past four years, our group has been working on the theoretical aspects of one type of abstraction layer for mobile ad hoc networks: *Virtual Node Layers (VNLayers)*. A Virtual Node Layer consists of: a collection of virtual, active state machines that we call *Virtual Nodes (VNs)*; *Client Nodes (CNs)*, which mirror the behavior of physical nodes; and a communication service that connects the VNs with the CNs.[1]

We have defined several different types of VNs: Some are stationary, found at known locations such as the intersection points of a regular grid. Others are mobile, moving according to pre-planned paths or autonomously re-calculating their heading in real time. Within these general classifications, however, our VNs differ in more subtle, yet fundamentally important ways with respect to their assumptions about timing and failures. For example, some of the VNs have approximately-precise control over the timing of their outputs—which will be particularly important for applications that involve controlling some aspects of the real world environment. A typical failure mode for a VN is a crash failure, followed by graceful recovery in its initial state, though we have also studied self-stabilizing VNs that can recover quickly from arbitrary state corruption.

We have developed algorithms to implement our VNLayers over lower-level mobile ad hoc network layers. These algorithms all follow the basic strategy of employing physical nodes in the vicinity of the VN's location to reliably emulate its operation. We have also developed a wide range of higher-level services and applications to run on top of these layers. These include: global atomic memory, "geocast" geographical communication, location services, point-to-point communication, robot motion coordination, and virtual traffic lights. In addition, we have recently begun developing simple air-traffic-control algorithms.

Our theoretical work on VNLayers and related algorithms is being carried out formally within the *Hybrid I/O Automata (HIOA)* and *Timed I/O Automata (TIOA)* modeling frameworks. Precise specifications of the layers and algorithms, including descriptions of timing and resilience, are crucial if these layers are to provide reliable platforms for application programmers. Hybrid and timed interacting-state-machine frameworks such as HIOA and TIOA are needed to model these layers and algorithms, as the models must be capable of describing the motion of the mobile nodes and other continuous aspects of the physical environment.

Although most of our work on this project has been theoretical, we have also completed a preliminary implementation of a basic VNLayer (featuring non-timed, stationary VNs), using the Python programming language, which can run on a variety of mobile devices, including Linux PDAs and laptops. To support the rapid development and debugging of applications for this platform we implemented a packet-level simulator that can run the same VNLayer and application code with (almost) no modifications. To date, we have used this system to implement and deploy a simple Virtual Traffic Light application as well as a geocast communication service.

---

[1] The bibliography at the end of this position paper lists the relevant papers; more information, including and annotated bibliography, can also be found at the project's website: `http://theory.csail.mit.edu/tds/vi-project/`

To fully leverage our theoretical work into the practical arena, however, numerous challenges must still be conquered. Most importantly, the theoretical work is based on strong assumptions about the reliability of the underlying network communication service. Additional work is needed to extend the existing VNLayer implementations to accommodate a greater range of unreliable behavior at these lower levels. Preliminary steps toward this goal include our recent study of the use of (potentially weak) receiver-side collision detection to help overcome an unreliable communication medium [9, 2]. To achieve reasonable performance, it may turn out to be necessary to reflect more unreliability upward into the VNLayer definitions. Finally, in case all else fails, the systems should be designed in a *self-stabilizing* manner, so that, even if the systems get arbitrarily corrupted, they can recover rapidly and gracefully.

These extensions must be made carefully, as they involve many subtleties typical of fault-tolerant timing-based distributed algorithms, as well as issues of interactions with the real-world environment. New theoretical work will be needed to support these extensions. Thus, we expect that any project to identify and develop usable VNLayers will need to include a strong foundational component.

3 Biographical Information

Nancy Lynch is the NEC Professor of Software Science and Engineering at the Computer Science and Artificial Intelligence Laboratory (CSAIL) at MIT, where she heads a research group on Theory of Distributed Systems. She is an ACM Fellow, member of the National Academy of Engineering, co-winner of the 2006 van Wijngaarden Prize, and winner of the 2001 Dijkstra Prize. She has worked on many aspects of distributed system design and analysis, lower bounds, and semantics and proofs for concurrent systems. She is perhaps best known for her result on "Impossibility of Consensus with one Faulty Process," and her textbook on Distributed Algorithms. Most relevant to the topic of this workshop is her work on hybrid system modeling and analysis, and her recent work on algorithms and abstractions for mobile ad hoc networks.

Calvin Newport is a PhD candidate in the Department of Electrical Engineering and Computer Science at MIT. He received a MS in Computer Science from MIT in 2006, and a BA in Computer Science from Dartmouth College in 2004. His current research interests include the study of distributed algorithms and lower bounds for unreliable wireless ad hoc networks.

References

[1] The Virtual Infrastructure Project Homepage. `http://theory.csail.mit.edu/tds/vi-project/`

[2] Calvin Newport, “Consensus and Collision Detectors in Wireless Ad Hoc Networks,” Masters Thesis, MIT, 2006.

[3] Shlomi Dolev, Seth Gilbert, Limor Lahiani, Nancy A. Lynch, and Tina Nolte, “Timed Virtual Stationary Automata for Mobile Networks,” 9th International Conference on Principles of Distributed Systems (OPODIS), December, 2005.

[4] Shlomi Dolev, Seth Gilbert, Nancy A. Lynch, Alex A. Shvartsman, and Jennifer Welch, “GeoQuorums: Implementing Atomic Memory in Mobile Ad Hoc Networks,” Distributed Computing, 125—155, November, 2005.

[5] Shlomi Dolev, Limor Lahiani, Nancy Lynch, and Tina Nolte, “Self-stabilizing Mobile Node Location Management and Message Routing,” Proceedings of the 7th International Symposium on Self-Stabilizing Systems, October, 2005.

[6] Gregory Chockler, Murat Demirbas, Seth Gilbert, and Calvin Newport, “A Middleware Framework for Robust Applications in Wireless Ad Hoc Networks,” Proceeding of the 43rd Allerton Conference on Communication, Control, and Computing, September, 2005.

[7] Shlomi Dolev, Seth Gilbert, Elad Schiller, Alex A. Shvartsman, and Jennifer L. Welch, “Autonomous Virtual Mobile Nodes,” Proceeding of the 3rd Workshop on Foundations of Mobile Computing (DIAL-M-POMC), September, 2005.

[8] Shlomi Dolev, Seth Gilbert, Limor Lahiani, Nancy A. Lynch, and Tina Nolte, “Timed Virtual Stationary Automata for Mobile Networks,” Proceeding of the 43rd Allerton Conference on Communication, Control, and Computing, September, 2005.

[9] Gregory Chockler, Murat Demirbas, Seth Gilbert, Calvin Newport, and Tina Nolte, “Consensus and Collision Detectors in Wireless Ad Hoc Networks,” 24th Annual Symposium on the Principles of Distributed Computing (PODC), July, 2005.

[10] Gregory Chockler, Murat Demirbas, Seth Gilbert, Nancy A. Lynch, Calvin Newport, and Tina Nolte, “Reconciling the Theory and Practice of (Un)Reliable Wireless Broadcast,” International Workshop on Assurance in Distributed Systems and Networks (ADSN), June, 2005.

[11] Nancy A. Lynch, Sayan Mitra, and Tina Nolte, “Motion Coordination using Virtual Nodes,” Proceedings of the 44th IEEE Conference on Decision and Control, 2005.

[12] Shlomi Dolev, Seth Gilbert, Nancy A. Lynch, Elad Schiller, Alex A. Shvartsman, and Jennifer L. Welch, “Virtual Mobile Nodes for Mobile Adhoc Networks,” Proceeding of the 18th International Conference on Distributed Computing (DISC), October, 2004.

[13] Shlomi Dolev, Seth Gilbert, Nancy A. Lynch, Elad Schiller, Alex A. Shvartsman, and Jennifer L. Welch, “Brief Announcement: Virtual Mobile Nodes for Mobile Adhoc Networks,” Proceeding of the 23rd Symposium on Principles of Distributed Computing (PODC), July, 2004.

[14] Shlomi Dolev, Seth Gilbert, Nancy A. Lynch, Alex A. Shvartsman, and Jennifer Welch, “GeoQuorums: Implementing Atomic Memory in Mobile Ad Hoc Networks,” Proceeding of the 17th International Conference on Distributed Computing (DISC), October, 2003.