Dependable opportunistic communication in a multi-tier sensor network architecture

Atul Prakash, Beng Heng, and Billy Lau, Department of EECS

Vineet Kamat, Department of Civil Engineering

University of Michigan, Ann Arbor, MI 48109

Contact: aprakash@eecs.umich.edu

(Workshop on Research Directions in Situational Self-managed Proactive Comuting in Wireless Ad-hoc networks, St. Louis, March 1-3, 2009.)

Abstract

Research in ad-hoc networks has usually focused on the problem of a group of nodes forming a reconfigurable network, as may be the case in military settings or disaster-response scenarios when networks quickly need to be set up with available computing nodes. In this paper, we examine the needs for a different scenario where you have a multi-tier communication architecture consisting of (1) a combination of low-power and resource-constrained sensor nodes that monitor and collect data on objects of interest; (2) mobile data collection nodes that are assumed to be onboard vehicles with few resource constraints but potentially poor connectivity to the Internet; and (3) backend infrastructure, with full Internet connectivity and reliability. We discuss some of the research challenges in designing this multi-tier architecture for dependable data collection in poor-connectivity scenarios.

Introduction

We are exploring the design of a multi-tier communication architecture system in a new sensor network project on monitoring the health of physical infrastructure systems, such as highways and bridges. Collapse of physical infrastructures occurs more frequently than most people realize. For example, between 1989 and 2000, more than 130 bridges collapsed in the United States. The challenge is that traditional monitoring solutions, which rely on physical inspections, are very expensive to scale up. We believe that appropriately designed multi-tier ad hoc networks, consisting of sensor networks, mobile data collection nodes, and back-end infrastructure may be a way forward. Other applications of such an architecture could include data collection from remote sensors in countries with poor network connectivity.

Because physical infrastructure systems may be in remote locations, we assume that the sensor nodes are of limited range and may need to be power-efficient. The mobile data collection nodes are assumed to be relatively unconstrained, but may not be connected to the backend infrastructure while they are collecting data at remote locations. The mobile data collection nodes serve to "route" data asynchronously between the infrastructure and the sensor nodes.

In this paper, we first outline some of the requirements of this multi-tier architecture from the perspective of communication requirements. Then, we point out some of the research challenges in utilizing these networks effectively.

Requirements

- **Opportunistic communication and data collection:** The sensor network must be self-configuring, form a network with passing mobile nodes opportunistically to get any locally logged data out.

- **Cooperative data transfer:** The nodes in the sensor network may have to cooperate to transfer the logged data to a mobile node that is moving at high speed relative to the range of the network between the sensor nodes and the mobile node. For example, multiple sensors under a bridge may be involved in transferring the data reliably to a data collection van that is moving at 55 miles per hour on the bridge. Failures of some sensors or communication must be handled.
- **End-to-end dependability:** The sensor nodes should attempt to keep the logged data on a best-effort basis till it is acknowledged by the backend infrastructure. Acknowledgements from the mobile data collection unit may not be sufficient since it is possible that it may fail to get the data to the backend infrastructure.

We assume that sensors themselves may be low-power devices and must make efficient use of their memory and CPU. The mobile data collection nodes, on the other hand, may have sufficient power (e.g., provided by a vehicle). But, they may not have connectivity with the backend infrastructure.

Research Challenges

Domain experts tell us that in the case of physical infrastructures, high nodal densities of sensor nodes may be necessary for reliable damage detection. This will require significant amounts of data from infrastructure elements to be transmitted to the locally deployed or back-end data servers. In some deployments, using powered sensor nodes that also have wide-area connectivity (e.g., CDMA, Edge, or 3G) may be an option. In that case, some of the sensor nodes may be gateway nodes that aggregate data from the various low-powered sensors and then periodically transmit it over a wired or wide-area (*e.g.* CDMA, Edge, or 3G) network. Option 1 in Figure 1 shows such a situation.

However, in other cases, the monitored infrastructure (a bridge in our example) may be at a remote location; providing network connectivity for such a bridge requires the laying of expensive network cables, a task economically unfeasible. To provide a solution that can be cheaply deployed anywhere, even in the absence of networking infrastructure, we envisage a mobile data collection and distribution method as an alternative communication channel (Option 2 in Figure 1). In this scheme, data will be collected from the sensors on a bridge by a data vehicle, as it drives over the bridge and stored on medium such as USB flash drives. The data will then be uploaded from the storage medium to the central servers either directly from the vehicle, when the vehicle has good connectivity, or from a satellite office with network connectivity.

Mobile multi-tier data collection is already used in some settings. Many homes in the United States now have water and electricity meters that are monitored over a short-range wireless network by the utility company from outside the home. In the case of utilities, a very small amount of data per home, the meter reading, needs to be captured, visual confirmation of a successful capture is possible, and the data is usually collected at short range and slow speeds.

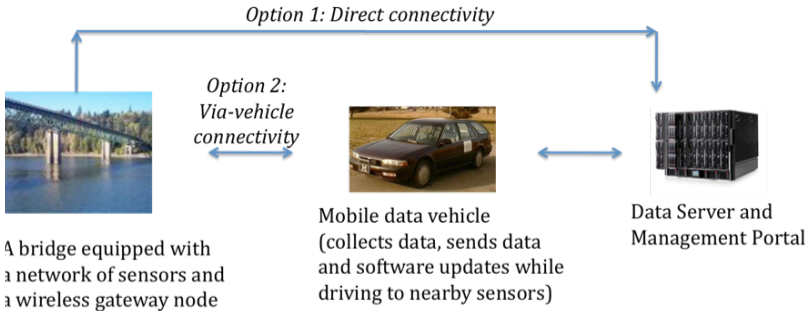

Figure 1: Connectivity between sensor networks and servers

We envisage that a number of research issues need to be solved in extending this architecture to monitoring larger multi-sensor systems. One challenge in the case of bridges is to extend this idea to reliably handle much larger volumes of sensor data that is likely to be buffered in the sensor network. Furthermore, ideally, we would like the data collection vehicle to be able to drive over the bridge at normal speeds. Possibly, if security issues can be addressed, ordinary citizens can help collect data on their smart phones. Opportunistically, prioritizing, aggregating, and compressing sensor data will be important in case all the data cannot be delivered to the vehicle at the desired driving speed. The driver also needs to know that the data is being successfully collected or if corrective driving action is required. Finally, one needs to address any security vulnerabilities in the data collection process. For example, it should not be possible for a hostile mobile data collection unit to cause the data from the sensors to be deleted without the data reaching the backend infrastructure.

Our proposed topology of sensor networks is as follows. On a site of interest (say a bridge or tunnel), we expect there to be *multiple aggregators* who communicate with the outer network. For fault-tolerance, these may be spread out over the monitored infrastructure. These nodes are called aggregators because they are responsible to collect and store (hence aggregate) data that is collected by sensors and communicated over a local ad-hoc, low power sensor network. Other sensors do not communicate with the outer network.

Data that is stored on the aggregators will have to be removed eventually. The question raised here is of the timing and manner of such deletion. There may be two ways of handling this: (1) ***Asynchronous acknowledgements:*** For this to work, the aggregator would need to be able to respond to an acknowledgement from the backend infrastructure (via a mobile data collection node), which will identify the previously collected data that can be deleted. Secure protocols of transmitting and receiving such signal need to be defined in order to prevent malicious parties from transmitting such a signal at will to erase valuable logged data. (2) ***Passive deletion***. This method provides an automatic way of erasing data, with a pre-determined clean-up period. However, this method allows for little flexibility in case of changes in the data collection schedule. Some sort of acknowledgement scheme is still likely to be needed so that aggregators can determine the portion of data to be transmitted to a mobile data collection node.

If a vehicle with a data collection node is moving at high speed relative to the range of the aggregators, the aggregators may have to cooperate to get the logged data out in an environment with intermittent connectivity to the vehicle. We envisage transmittable data to be partitioned among n aggregators with some redundancy so that the mobile node can determine the subset of data that it is has received reliably. Designing algorithms for such cooperative data transmission to mobile nodes is a future research issue.

Acknowledgements

This work is partially supported by a NIST Technology Innovation Program 2008 R&D Award (Advanced Sensing Technologies for the Infrastructure). We acknowledge the input from our colleagues on the project.