Challenges in Supporting Federation of Sensor Networks

Christos Efstratiou

Computer Laboratory, University of Cambridge
Cambridge, UK
christos.efstratiou@cl.cam.ac.uk

Abstract. Wireless sensor networks are more and more seen as a solution to large-scale tracking and monitoring applications. However, existing networks are designed to serve a single application and deliver information to one authority; typically the owner of the network. This approach is clearly inefficient considering the high cost of deploying a sensor network. Supporting federation of sensor networks can allow the development of new applications that can access recourses offered by multiple existing sensor networks. This paper discusses the challenges in designing a platform for federated sensor networks.

1 Introduction

Wireless sensor networks are more and more seen as a solution to large-scale tracking and monitoring applications. Examples range from environmental (e.g. monitoring pollution in urban areas, monitoring wildlife for research purposes) to industrial (asset tracking, monitoring manufacturing processes) and every day applications (health monitoring and assisted living for elderly people). These networks, however, are usually designed to serve a single application and collected information is commonly available to one authority (that is usually the owner of the sensor network). This often leads to inefficient use of resources and limits the potential for building new applications that could use existing sensing infrastructure.

Considering the high cost and effort involved in the deployment of a sensor network, the current approach of designing networks that serve only a single application and a single user, is highly inefficient. One example that illustrates this problem is the deployment of cameras on the UK roads and motorways. Typically different authorities (police, highway agency, local city authorities) will deploy their own networks of cameras, occasionally covering the same areas.

Many of the shortcomings of existing sensing infrastructures spawn from the fact that we do not yet have the means to deal with a secure multi-purpose federated sensor network, involving tens of thousands of sensor nodes running different applications in parallel and able to reconfigure dynamically to run others. The communication paradigms which have been usually devised for small and single owner sensor networks simply do not have the right scalability, security, reconfigurability characteristics required for this environment. The vision for the future generation of sensor networks is of a world where sensing infrastructure is a shared resource that can be dynamically re-purposed and re-programmed in order to support multiple applications. Furthermore multiple sensor networks (possibly owned by different authorities) can be combined in a federated fashion in order to create a more complete picture of the world. For instance an in-building sensor network charged with the task of controlling room temperature, may need to be re-tasked dynamically to monitoring a fire in the building. Furthermore federating this network with a network of mobile phones of people in the building can allow the activation of an evacuation application diverting people away from the fire.

2 Challenges

In the University of Cambridge, FRESNEL (Federated Secure Sensor Network Laboratory)[1] is a new project that investigates the challenges in designing a framework that supports federation of sensor networks. In this project we consider a city-wide federated network consisting of a large number of nodes with diverse communication and computation capabilities and belonging to different authorities. Nodes are equipped with a variety of sensing devices (temperature, magnetometers, pollution sensors, mini-cameras) that allow them to serve a large spectrum of applications, ranging from environmental monitoring to traffic monitoring, surveillance and hazard detection. In designing such a federated network a number of challenges need to be addressed:

- *Dynamic resource allocation:* Nodes should be able to dynamically reassign their sensing, communication and computation resources to address the needs of multiple applications running in parallel and to negotiate what and how to share. In an environment where multiple sensors may belong to different administrative domains, resource allocation will need to take into account the diverse requirements of the different stakeholders. Dynamic resource allocation will need to comply to different allocation policies as they are specified by network owners while trying to address the demands placed by the applications.
- *Flexible Network partitioning* There must be a flexible and adaptive mechanism to partition the common sensor network platform into *virtual sensor networks*, one per application. An overlay network must be formed to cover the nodes of a particular application whilst ensuring reliable and efficient communication among these nodes. Supporting federation over heterogeneous networks imposes additional challenges. Sensor networks may use different communication technologies (IEEE 802.15.4, GSM/3G, WiFi). Establishing virtual sensor networks over heterogeneous networks will require appropriate bridging mechanisms that may impose constraints on the scalability of the system.
- *Secure and safe sharing of resources* Security constraints must be enforced to guarantee correct behavior in the shared network; applications need to be able to communicate securely (some applications might be transmitting sensitive data) but, at the same time, the resource allocation determined by the managing system needs to be observed (i.e., no application should be allowed to steal resources or to disrupt the behavior of other applications). Furthermore, privacy policies specified by network owners or application users will need to be enforced across the shared network.
- *Support for legacy networks* It should be possible to incorporate existing sensor networks that do not have built in support for federation. Such networks are expected to expose a single interface abstracting over the whole network. In these cases data and meta data exported by the network need to be specified in a well defined format. New applications should be able to access information offered by legacy sensor networks in a secure and managed way.

3 Approach

One of the primary aims of FRESNEL is to deploy a prototype federated sensor network across the University of Cambridge, also partly integrating existing sensor networks. The federated network will span different university departments and colleges and will cover heterogeneous monitoring needs ranging from in-building sensing (temperature, humidity, light, sound), air quality (using pollution monitoring sensors around the city), to traffic and mobile activity monitoring (using mobile phones as sensor nodes).

The main challenge that we are trying to address is the deployment of sensor networks that are able to support multiple applications that run in parallel over the network. The programming paradigm used by existing sensor network operating systems is fundamentally unsuitable for supporting multiple applications. TinyOS for example, is designed for building monolithic applications that have full control over the operation of a sensor node. Virtualization on the sensor node level is a feasible approach that will allow multiple applications to run in isolation within each node. The work in [2] and [3] show successful efforts in supporting virtualization in pervasive computing. Our approach is to create a virtualization environment that not only allows the execution of multiple application on each node, but will also support a standardized set of services that will allow the dynamic partitioning and distributed management of a sensor network. This will offer a platform on which applications can be installed, reconfigured and shared.

Following this approach our primary aim is to establish a testbed environment that supports virtualization on the sensor node level, offering a standardized interface for application allocation and network partitioning. The partition needs to define a virtually isolated network among the nodes running the application. This management needs to have very low overhead given the limitations of the sensor nodes involved. The partition could be compared to a PlanetLab [5] slice although the challenges of maintaining the slice in a sensor network environment are many and include energy and limited bandwidth, processing and sometimes mobility.

Nevertheless, there are some lessons to be learned both in terms of management [6] and in terms of security [7].

This testbed will allow us to experiment with issues of resource allocation and network virtualization in a federated environment. Furthermore the incorporation of existing networks already deployed around the University of Cambridge will allow us to work towards a general purpose API for accessing legacy sensor networks in a federated fashion.

4 Conclusions

Existing approaches in sensor networks consider networks in isolation that are designed to support a single application. Allowing multiple sensor networks to work in a federated manner can offer new opportunities for the development of applications without the high cost of deploying new sensor networks. In order to achieve this level of collaboration, we need to address a number of challenges regarding resource allocation, network management and security. In the context of the FRESNEL project we try to address this issue by supporting virtualization on the sensor node level and allowing the formation of virtual network overlays on top of multiple sensor networks.

References

1. FRESNEL Project, *http://www.cl.cam.ac.uk/research/srg/netos/fresnel/*, Date accessed: 1 March 2010.
2. Philip Levis , David Culler, Maté: a tiny virtual machine for sensor networks, In *Proceedings of the 10th international conference on Architectural support for programming languages and operating systems*, San Jose, California, October 05-09, 2002.
3. S. Kabadayi and C. Julien. A local data abstraction and communication paradigm for pervasive computing. In *Proceedings of the 5^{th} Annual IEEE International Conference on Pervasive Computing and Communications*, pages 57-66, March 2007.
4. J. Shneidman, P. Pietzuch, J. Ledlie, M. Roussopoulos, M. Seltzer, and M. Welsh. Hourglass: An Infrastructure for Connecting Sensor Networks and Applications. Harvard Technical Report TR-21-04, 2004.
5. A. Bavier, M. Bowman, B. Chun, D. Culler, S. Karlin, S. Muir, L. Peterson, T. Roscoe, T. Spalink, and M. Wawrzoniak. Operating System Support for Planetary-Scale Network Services. In *NSDI 04*, May 2004.
6. R. Ricci, D. Oppenheimer, J. Lepreau, and A. Vahdat. Lessons from Resource Allocators for Large-Scale Multiuser Testbeds. In *(OSR 06)*, 2006.
7. Y. Fu, J. Chase, B. Chun, S. Schwab, and A. Vahdat. SHARP: An Architecture for Secure Resource Peering. In *(SOSP 03)*, 2003.

Short CV

Dr. Christos Efstratiou is a Senior Research Associate in the Computer Laboratory, University of Cambridge. He received his Ph.D. in 2004 from Lancaster University, UK. He has been a Research Associate in Lancaster University and a visiting researcher in Sony Electronics Distributed Systems Lab in San Jose. His early work focused on the support for adaptive and context-aware applications in mobile environments. More recently, he has been actively involved in research projects in the areas of wireless sensor networks, and pervasive computing. His is currently working in the area of system support for federated sensor networks. He has authored over twenty published papers, and has been a member of the organizing committee of HotMobile 2009 and 2010, and AmI 2008. His current research interests include networked mobile systems, wireless sensor networks, novel mobile and pervasive applications.

Contact details

Dr. Christos Efstratiou
University of Cambridge
email: christos.efstratiou@cl.cam.ac.uk
phone: +44 (0)1223 763694