IoT/Smart Home Router Integration

Student: Fergus Leahy

Supervisor: Joe Sventek

# Background

The digital world is an increasingly unremarkable feature of our lives. Our homes are increasingly populated with a heterogeneous collection of devices often connected to the Internet via a home network. These domestic devices support a host of activities: they deliver media into our homes, allow access to online services and support communication between extended family members. We increasingly carry a range of mobile devices and brush up against a host of devices in our vehicles and at work, all connected to an ever-expanding Internet. Although these devices often share a common infrastructure, the experience of using these devices is disjoint and complex.

The sheer diversity of devices and approaches presents the core of the challenge. Devices are entering the home in a piecemeal fashion, often with no regard to existing infrastructures and services. The net result is that users are faced with distinct families of devices, each of which provide similar functionality, but all of which have distinct infrastructures. For example, network capability in our cars typically does not smoothly interface with our home networks; the proposed Smart Grid infrastructure intends to deploy its own network; and the continuing movement toward Internet of Things (IoT) deployment has not considered the relationship between the IoT and existing home network deployments.

The heterogeneity of devices and the plethora of various stakeholders have resulted in a fragmented approach to the delivery of an intelligent infrastructure in our homes. This presents many problems, key among which are:

* Security: lack of thoughtful integration means unintended interactions between the different networked systems, giving rise to unanticipated attack vectors. Different security models and paradigms compound this problem, particularly as they often need to be resolved by users.
* Usability: the multitude of different systems, providing different features, in different ways, managed through different interaction techniques, means that users face an ever-increasing burden in trying to deploy, configure and manage these different systems, none of which were designed from the start with usability by non-technical individuals in mind.
* Privacy: as these systems become more deeply embedded in our lives, they gather and, due to the two problems described above, make available personal data in ways that we cannot understand/manage.

The current generation of systems places a significant technical burden on the user to build and maintain their own intelligent information infrastructure by “knitting together” different digital devices and managing them as a whole. As the digital world continues to proliferate and the range of devices with which we come into contact diversifies even further, the burden on the users is likely to increase to the point where it becomes unmanageable. As we enter the era of the Internet of Things (with its presumption of a raft of sensors capturing activities in the home, domestic appliances accessing online services, resource-monitoring systems recording our water and energy consumption and a raft of healthcare devices monitoring our physiology) we cannot presume users have either the technical skills or motivation to make these devices work together. Indeed our existing work in this area highlights that users find maintenance of their home network massively problematic even with the small range of currently-connected devices [3][4].

We wish to develop the models and mechanism required to enable users to manage their relationship to a future domestic intelligent information infrastructure. Rather than focus purely on the technical challenges of the Internet of Things, we wish to explore how a user might establish and manage a domestic Intelligent Intranet of Things.

# Goals of the Project

This project provides the first step in creating such an Intranet of Things within the home – the integration of state-of-the-art IoT protocols (and, therefore, devices) with a state-of-the-art smart router. The hypotheses for the project are the following:

1. It is possible to secure IoT protocols and Smart Router protocols sufficiently to prevent eavesdropping of the transported data and injection of events by perpetrators masquerading as sanctioned participants in the home network
2. It is possible to implement the controller roles defined in state-of-the-art IoT protocols as automata supported by the smart router

The project will build on the IoT protocols implementation described in [5] and the Smart Router implementation described in [1][2].

# Key research outputs

* Analysis of security threats faced within the Intranet of Things, and appropriate protocol modifications to address those threats.
* An extended home information platform, building on the Homework smart router platform, able to capture multiple network and data types, including IoT devices, and the data they generate.
* Use of automata in the smart router to implement closed loop control of Things.

# References

1. J Sventek, A Koliousis, O Sharma, N Dulay, D Pediaditakis, M Sloman, T Rodden, T Lodge, B Bedwell, K Glover, R Mortier, “An information plane architecture supporting home network management”, Proc. IFIP/IEEE International Symposium on Integrated Network Management (IM), May 2011.
2. J Sventek, A Koliousis, “Unification of publish/subscribe systems and stream databases: the impact on complex event processing”, Proc. International Middleware Conference, December 2012.
3. P Brundell, A Crabtree, R Mortier, T Rodden, P Tennent, P Tolmie, “W-MUST’11 Best Papers – The Network From Above and Below”, ACM Computer Communication Review (CCR), 41(4):519, August 2011.
4. A Brown, R Mortier, T Rodden, “MultiNet: Reducing Interaction Overhead in Domestic Wireless Networks”, Proc. ACM SIGCHI, April 2013.
5. F Leahy, “IoT Protocols”, final year project report, University of Glasgow, March 2013.