



University of Glasgow | School of  
Computing Science

# Securing and Integrating the IoT with a Smart Home Router

Fergus W. Leahy

School of Computing Science  
Sir Alwyn Williams Building  
University of Glasgow  
G12 8QQ

Masters project proposal

16/12/2013

# Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Statement of Problem</b>	<b>3</b>
<b>3</b>	<b>Background Survey</b>	<b>4</b>
3.1	State-of-the-art IoT Protocols . . . . .	4
3.2	Homework - Smart Home Router . . . . .	4
3.3	Symmetric Security - TinySec, MiniSec, ContikiSec . . . . .	4
3.4	Asymmetric Security - TinyECC . . . . .	4
3.5	Other Works . . . . .	4
3.5.1	MQTT . . . . .	4
3.5.2	IETF Work . . . . .	4
<b>4</b>	<b>Proposed Approach</b>	<b>4</b>
4.1	Security Architecture . . . . .	4
4.1.1	Symmetric Key Cryptography . . . . .	4
4.1.2	Asymmetric Key Cryptography . . . . .	4
4.2	Implementation of IoT Protocol on TinyOS . . . . .	4
4.3	Integration of IoT with Smart Home Router . . . . .	4
<b>5</b>	<b>Work Plan</b>	<b>4</b>

# 1 Introduction

*“The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.”*

– Mark Weiser, *The Computer for the Twenty-First Century*, 1991

The modern home is becoming increasingly filled with a variety of *connected* devices (laptops, tablets, phones, set-top boxes etc.), providing a myriad of different services to users within the home. On top of this, with the advent use of smart phones and introduction of wearable devices, we too are starting to carry around our own personal network of devices everywhere we go, brushing past many others in our daily lives at home, work and on the street. Although all connected to the Internet, these devices are often encapsulated within their own environment and ecosystem, unable to interconnect, creating a fractured and often complex user experience.

Making matters more interesting, the Internet of Things paradigm is once again becoming a field of great interest due to the advent of cheap, low power wireless embedded devices [1]. However, not much consideration has been made for how these Things should be integrated into the existing home network, with many approaches opting to simply bridge the device to the cloud ([2], [3], [7]), with obvious concerns for security, privacy and up-time.

As these devices enter our homes and pockets, bringing with them their own ecosystems, the user is faced with the increasingly difficult burden of managing all of them and the ecosystems [5], [4]. Due to the sheer number and diversity of these devices, many of which will provide overlapping services and functionality, problems arise in how to ensure these devices not only play nicely together but also ensuring the user’s network and information stays secure against new and unanticipated threats.

The Homework home router platform was created to resolve some of these issues. Rather than assume every user is a network administrator, the project investigated the needs and abilities of the average user in order to propose the future of home networking, re-inventing the protocols, models and architectures to truly suit the home environment. This re-invention of the home router allows a user to easily install, manage and use their home network, without the need of a Cisco qualification.

In regards to the Internet of Things development, previous work demonstrated that it was in need a suitable protocol in order to meet the specific needs of a network of Things [6]. Thus, a new protocol was designed and implemented, which could not only run on even the most constrained battery-powered devices (8MHz), but it could also efficiently scale to support hundreds of Things within the same network.

In order for our networks of devices to truly fade away into the fabric of our lives, a platform and relevant protocols need to be engineered to not only support this heterogeneous network securely, but also aid the user in managing both the network and the privacy of their information.

## 2 Statement of Problem

The Internet of Things protocol created in [6] proved to be a successful proof-of-concept; However, in order for it to be considered for deployment and integration into existing homes, several issues need to first be addressed. Intranet of things....

- Security, integration, encryption
- Usability, interoperability
- Privacy, information security - user controls of data

This project seeks to address these issues

## **3 Background Survey**

### **3.1 State-of-the-art IoT Protocols**

### **3.2 Homework - Smart Home Router**

### **3.3 Symmetric Security - TinySec, MiniSec, ContikiSec**

### **3.4 Asymmetric Security - TinyECC**

### **3.5 Other Works**

#### **3.5.1 MQTT**

#### **3.5.2 IETF Work**

## **4 Proposed Approach**

### **4.1 Security Architecture**

#### **4.1.1 Symmetric Key Cryptography**

#### **4.1.2 Asymmetric Key Cryptography**

### **4.2 Implementation of IoT Protocol on TinyOS**

### **4.3 Integration of IoT with Smart Home Router**

## **5 Work Plan**

- Secure IoT Protocol
- Implement Secure IoT Protocol on TinyOS
- Port Secure IoT Protocol to Homework Automata

## References

- [1] 2013: The year of the Internet of Things. <http://www.technologyreview.com/view/509546/2013-the-year-of-the-internet-of-things/>. Accessed: 21/03/2013.
- [2] Smart Things IoT platform. <http://smarththings.com/>. Accessed: 21/03/2013.
- [3] Twine “Internet of Things” Thing. <http://supermechanical.com/>. Accessed: 21/03/2013.
- [4] Anthony Brown, Richard Mortier, and Tom Rodden. Multinet: Reducing interaction overhead in domestic wireless networks. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '13, pages 1569–1578, New York, NY, USA, 2013. ACM.
- [5] Patrick Brundell, Andrew Crabtree, Richard Mortier, Tom Rodden, Paul Tennent, and Peter Tolmie. W-must’11 best papers-the network from above and below. *SIGCOMM-Computer Communication Review*, 41(4):519, 2011.
- [6] F.W. Leahy. A lightweight protocol for constrained devices for use in the Internet of Things paradigm. Technical report, University of Glasgow, 2013. 4th Year Dissertation.
- [7] Z. Shelby. IETF, Constrained RESTful Environments - Resource Discovery, 2012. RFC6690, 1.2.1.