Fleet Tracker
(Technical Report)

Ethics in the Self-Powered Internet of Things
(STS Topic)

A Thesis Prospectus in STS 4500
Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia
In Partial Fulfillment of the Requirements of the Degree
Bachelor of Science in Engineering

Author

Nojan Sheybani
October 30, 2019

Technical Project Team Members

Jesse Dugan
Nayiri Krzysztofowicz
Vivian Lin
Malcolm Miller

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature _____ Date _____

Approved _____ Date _____
Rider Foley, Department of Engineering and Society

Introduction

The Internet of Things (IoT) has been described as the next technological revolution (Feki, 2013). The IoT is defined as a collection of wireless sensor nodes that interact with each other in order to achieve a common goal or monitor a certain environment. This networked technology can be applied in myriad contexts, from turning on a light with your Alexa to monitoring the amount of lux in all the rooms of your house. Some of the other fields in which IoT is applicable include social networking, healthcare, industrial plants, and many more widespread domains (Atzori, 2010). IoT is a groundbreaking movement in the technological field and by 2025, assuming current trends continue, there will be 75 billion IoT devices in the world (Bera, 2019). While this is an exciting statistic, there is a very good chance that this milestone will not be achieved due to a common component of most IoT systems: batteries. Soon, around 50 billion devices, we will plateau in our production of IoT systems due to their reliance on batteries (Calhoun, 2019). This problem is currently being addressed through research, development, and commercialization, from local companies such as Everactive, of self-powered and internet-connected devices.

A more appropriate name for self-powered systems would be environment-powered systems as self-powered systems are defined as technological devices, such as an IoT device, that is powered by ambient energy that is harnessed from the environment of the system (Glynne-Jones, 2001). There are many sources of energy from the environment that can be utilized in a self-powered system, such as vibrations, solar, and heat. While there are many harvesting modalities that a self-powered system can use, none of these modalities provide the constant power to a system that a battery would. Self-powered systems do not rely on batteries, but their harvested power fluctuates due to the randomness of the environment (Wang, 2010). Motivated

by the challenge of building a system powered by the unpredictable environment, my group will be building a self-powered system that utilizes solar energy to power an IoT Global Positioning System (GPS) module. As with any new technology, there are ethical implications that must be considered when analyzing the shift towards self-powered systems. This paper will discuss the reason for the shift towards self-powered systems and the ethical concerns that face this shift.

Technical Topic

The task of tracking assets, whether these are cars, buses, trains, or other vehicles, requires reliable and continuous data transport from global positioning systems (GPS). While batteries may be able to provide power to GPS tracking systems, all batteries eventually run out of energy and need to be replaced. As the IoT grows, battery replacement can pose an inconvenience when a user has thousands of widely dispersed nodes that need replacement. This capstone project aims to solve communication and power-limiting problems that are faced by current GPS trackers that primarily require batteries. This technical project will result in a product that is able to provide continuous data transmission to a home node and is solar-powered, allowing users to put it on all the assets that need to be tracked without the frequent maintenance.

The Fleet Tracker is an IoT application that tracks vehicles in real time through a reliable and secure network of wireless devices. A series of devices, called roaming nodes, are attached magnetically to moving vehicles. They send location information to a stationary home node, which visualizes this data in a user interface. The interaction between the roaming nodes and the home node is demonstrated in Figure 1. The roaming nodes are self-powered by solar energy, which solves the problem of high maintenance required by single-use batteries. In order to

ensure reliability even in unstable environmental conditions, these nodes use techniques to store excess energy for later use and to reduce power consumption. The Fleet Tracker also accounts for simple security breaches by encrypting location data transmitted wirelessly between nodes.

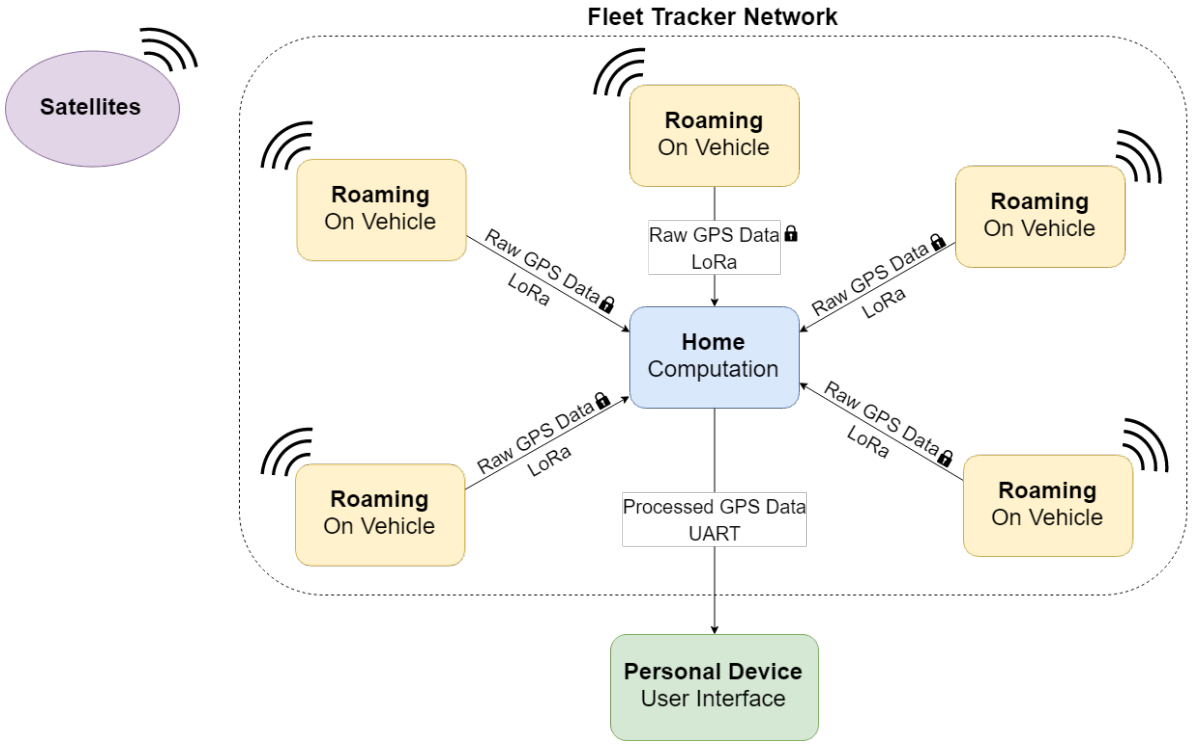

Figure 1. Diagram showing the interaction between home and roaming nodes in the fleet tracker network (Created by Sheybani, 2016)

In order to ensure that a self-powered system has a long lifetime, we have to utilize several low-power methods. The roaming nodes are made up of an MSP430, a microcontroller that is used for low-power applications, and printed circuit boards (PCB) that manage our power storage and communication to the home node. The home node is simply an MSP430 that is connected to and powered by a laptop via USB. In order to limit the amount of power usage by the roaming nodes, the amount of computation done by the node will need be kept to a minimum. Rather than

doing any processing of the GPS data on the roaming node, the raw data will be sent straight to the home node for analysis. The home node, not having the same power constraints, will do all the heavy computation that is involved with processing the data and sending it to the user interface. One computation that will be done on our roaming node is a low-power, non-intensive form of encryption to ensure the privacy of the data being transmitted.

Another way we are minimizing power on the roaming nodes is by utilizing a technique called duty cycling. Duty cycling is the process of putting the system to sleep when there are no ongoing operations. In our system, the roaming node will read and send data every 15 seconds and put the system to sleep in between these intervals. This will make the system much more energy efficient. With self-powered systems, the power budget is the biggest constraint, so we are using many different power-efficient techniques to stay within that budget. Financially, we are given roughly $500 to develop several prototypes and our final product. This technical project addresses one of the reasons that the shift towards self-powered systems is occurring, which is the reliance regular systems have on batteries. Also, the proposed system is constantly tracking and transmitting location data without the reliable power that batteries provide, which raises questions of the security and privacy of a user's data. The ethical implications that face our technical project are similar to concerns that will face many self-powered systems that are handling sensitive data.

Ethics in the self-powered IoT

The IoT is often discussed in a technical sense, but due to the ethical implications that surround the implementation of IoT, this technology must be viewed through a sociotechnical lens (Ghaffari, 2019). A sociotechnical system consists of four interactive

elements: technology, structure, tasks, and actors. The development of IoT consists of all of these elements and the interactions between them. Technology is the physical artifacts, such as hardware, software, and network and security. Structure consists of the formal regulations, rules, and standards for IoT development, as well as the informal norms, expectations and behaviors. Tasks in this sociotechnical system are defined as the actions that need to be taken in order to make progress in the development of the IoT. A very important task for IoT is research and development, which is where the feasibility and prototyping of IoT systems are presented. Finally, actors are any entities that influence or are influenced by the IoT. Four of the most prominent actors in the IoT are the government, industries, consumers, and entrepreneurs. One of the key aspects of the elements of a sociotechnical system is the interaction of the elements with each other. For instance, the actor-structure interaction is crucial to the development of IoT. Governments create rules and regulations for the development of IoT that industries and entrepreneurs must adhere to when proposing new advancements for the IoT. Customers also have a strong relationship with structure, as structure allows standards and regulations to be declared pertaining to a customer's data privacy and security (Ghaffari, 2019). This framework, which focuses on the four elements of a sociotechnical system and their interactions, will be used to analyze self-powered IoT systems.

The self-powered IoT will be evaluated using a normative framework, *responsible innovation*. Responsible innovation is formally defined as "taking care of the future through collective stewardship of science and innovation in the present" (Stilgoe, 2013, p.1570). The self-powered IoT will be evaluated to ensure that the presented technology will affect positive change in the environment. Responsible innovation consists of four dimensions: anticipation, reflexivity, inclusion, and responsiveness. Anticipation consists of asking "what if?" questions

about new innovations. Foresight and technology assessment must be utilized in in order to avoid unforeseen detrimental implications of growing technological systems. The reflexivity dimension forces innovators to consider the "socio-ethical context of their work". Reflexivity simply wants scientists to enforce morality into their innovation process. For example, codes of conduct can be set in the laboratory setting to ensure that morals and external values are connected to the practice of innovation. The inclusion dimension is concerned with getting the wider public and stakeholders involved in the discussion and practice of innovation. The use of conferences, focus groups, and citizen panels/juries are a few examples of practicing inclusion in responsible innovation. Finally, the responsiveness dimension considers the ability of an innovation to pivot in response to stakeholder opinions or changing circumstances. Responsiveness can be approached in many different ways, such as regulation and standards, to ensure that an innovation will be able to change directions when needed. In order for responsiveness to be correctly analyzed and responsibly governed, it is important that the product and purpose are considered (Stilgoe, 2013). These four dimensions of responsible innovation will be used to evaluate the analysis of self-powered systems as sociotechnical systems, with a focus on the ethical implications of security and privacy in self-powered systems.

Security and privacy are the most challenging ethical implications to address in the IoT (Dutton, 2014). Analyzing security and privacy in self-powered IoT systems is especially difficult, as self-powered systems add a strict power budget to regular IoT systems. This is due to the fact that these systems harvest power from the environment, so the harvested power is always fluctuating as the environment changes. This strict power budget brings security into question as most security techniques, such as encryption, require a lot of computation, so a self-powered system, which can also be referred to as an "energy-starved" system, may not be able to provide

the same level of security as a battery-powered system (Schaumont, 2017). For self-powered systems, the issue of security has been a very prevalent one that has few solutions. Currently, one of the main techniques for security is energy-optimized cryptography, but this is not as reliable as standard cryptography techniques (Schaumont, 2017). When analyzing the self-powered IoT as a sociotechnical system, all of the sociotechnical elements are affected by security and privacy. There must be tasks that are clearly defined to drive IoT development in a direction that emphasizes security and privacy. The correct technological approach must be taken in order to provide actors with products that ensure that a customer's privacy and security is safe. Structure must be provided in the form of rules and regulations that affect the interaction of actors with the self-powered IoT. For instance, rules and regulations (structure) pertaining to security and privacy that are set by the government (actor) influence the products that entrepreneurs and industries (actor) build, which become a part of consumers' (actor) everyday lives. This is a good example of an actor-structure interaction within a sociotechnical system. Security and privacy issues must be taken into consideration in the analysis of the self-powered IoT as a sociotechnical system and in the evaluation of self-powered systems as responsible innovation.

Research Question and Methods

I will address the following question: What is causing the shift towards self-powered IoT systems and what are the ethical concerns with this shift? The shift towards self-powered IoT systems is seen in the rising amount of work done by industries and entrepreneurs to build companies around self-powered systems, such as Phoenix-based Fortune 500 company ON Semiconductor and Charlottesville-based startup Everactive (Aspencore Network, 2019). Although the systems presented by these companies are cutting-edge, consideration of ethical

implications such as security and privacy in the development process are not clearly relayed. This research question is important to answer because self-powered IoT systems are slowly being introduced to our environment, so the justification and ethical considerations of its development must be presented. The self-powered IoT will be analyzed as a sociotechnical system and evaluated with the framework for responsible innovation. Alongside this, my research will utilize interviews of entrepreneurs working on self-powered systems and field experts. There are a few key questions that I would like to ask these experts. What is driving the IoT industry towards self-powered systems? How are you accounting for the ethical implications that come with self-powered systems? What are the most concerning consequences of implementing self-powered systems? The outcomes of these interviews will be used to inform case studies that will provide further information on the topics that the interviewees provide.

There are many aspects of self-powered systems that I would like to question experts on in my interviews. Self-powered systems have much more overhead than IoT systems, as the development process must take into account many components for the "self-powered" portion of the system (Adila, 2018). Battery-powered systems do not have this overhead, so I would like to consult experts about why this shift towards the self-powered IoT is occurring even though it requires so much overhead. I would also like to ask how the products they make and research are taking security and privacy into account, as I have not been able to find many resources that address this. Building off of this, the IoT is more susceptible to attacks as more IoT nodes are added to the system, so I would like to know what practices of "safe scaling" are employed in this field to gain insight on how self-powered systems will properly scale without risking security and privacy (Roman, 2013). I would like to interview professors at the University of Virginia and the University of Michigan that lead prominent lab groups focusing on the

development and research of self-powered systems. Alongside this, I would like to interview engineers at Everactive, a Charlottesville-based startup that is commercializing self-powered systems, to learn more about the design considerations for self-powered systems. The information gathered from these interviews will be used to inform case studies to further answer my research question.

The case studies will be used to provide evidence for the information that is collected during the interview process. As an example of a case study that can be used, (Shin, 2014) presents a case study offering insights that were gathered through observing the development and implementation of IoT in Korea with human-centered contexts. This case study explains the sociotechnical problems that were faced in the implementation of the IoT and how they were addressed throughout the development process. Cases like this are not conclusive enough to act as the sole evidence of ethical implications and solutions, but they represent attempts to integrate IoT into certain societies, which I believe will provide very valuable information. As I learn more about the self-powered IoT from the interviews, I will find more specific case studies that focus on the areas that are heavily emphasized by my interviewees. After analyzing the case studies, I will schedule follow up interviewers to tie up any loose ends with my research and ask questions about works presented in the case studies that were not mentioned in the first interview.

Conclusion

Figure 2 shows a timeline that will be followed in order to successfully complete the STS research. The biggest time commitment is conducting the initial interviews, as I would like to make sure that I am very thorough and get as much information as possible from this process.

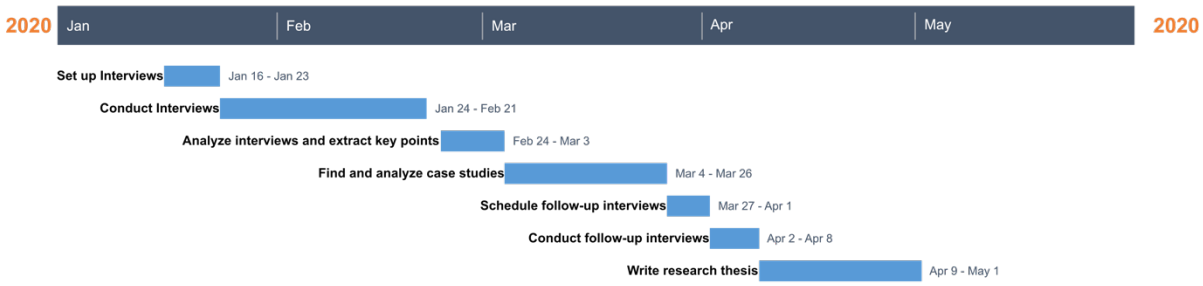

Figure 2. Gannt chart highlighting major tasks for STS 4600 (Created by Sheybani, 2019)

The output for my technical project will be a working solar-powered IoT GPS tracker, alongside an IEEE formatted conference paper. With this research, we will show the feasibility of a system that can use LoRa modulation and be self-powered, so that data can be continuously transmitted from anywhere. The outcome of studying “Ethics in the self-powered IoT” will be a clear answer to my research question backed by evidence from case studies and interviews.

References

Adila, A. S., Husam, A., & Husi, G. (2018). Towards the self-powered Internet of Things (IoT) by energy harvesting: Trends and technologies for green IoT. *2018 2nd International Symposium on Small-Scale Intelligent Manufacturing Systems (SIMS)*, 1–5. https://doi.org/10.1109/SIMS.2018.8355305

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

Aspencore Network (2019, May 2). Battery-less IoT could soon be a reality with Bluetooth multi-sensor platform – IoT Times. Retrieved October 30, 2019, from https://iot.eetimes.com/battery-less-iot-could-soon-be-a-reality-with-bluetooth-multi-sensor-platform/

Bera, A. (2019, February 25). 80 IoT Statistics for 2019 (Infographic). Retrieved September 22, 2019, from SafeAtLast.co website: https://safeatlast.co/blog/iot-statistics/

Calhoun, B (2019). ECE 6501: Self-Powered Systems, Virginia, VA

Dutton, W. H. (2014). Putting things to work: Social and policy challenges for the Internet of Things. Info, *16*(3), 1-21. https://doi.org/10.1108/info-09-2013-0047

Feki, M. A., Kawsar, F., Boussard, M., & Trappeniers, L. (2013). The Internet of Things: The Next Technological Revolution. *Computer*, *46*(2), 24–25. https://doi.org/10.1109/MC.2013.63

Ghaffari, K., Lagzian, M., Kazemi, M., & Malekzadeh, G. (2019). A socio-technical analysis of IoT development: An interplay of technologies, tasks, structures and actors. *Foresight*, 21(6), 640-653. https://doi.org/10.1108/FS-05-2019-0037

Glynne-Jones, P., & White, N. M. (2001). Self-powered systems: A review of energy sources. *Sensor Review, 21*(2), 91-97 https://doi.org/10.1108/02602280110388252

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed IoT. *Computer Networks*, *57*(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018

Schaumont, P. (2017). Security in the Internet of Things: A challenge of scale. *Design, Automation Test in Europe Conference Exhibition vol*, 674–679. https://doi.org/10.23919/DATE.2017.7927075

Shin, D. (2014). A socio-technical framework for Internet-of-Things design: A human-centered design for the IoT. *Telematics and Informatics*, *31*(4), 519–531. https://doi.org/10.1016/j.tele.2014.02.003

Stilgoe, J., Owen, R., & Macnaghten, P. (2013). Developing a framework for responsible innovation. *Research Policy, 42*(9), 1568–1580. https://doi.org/10.1016/j.respol.2013.05.008

Wang, Z. L. (2010). Toward self-powered sensor networks. *Nano Today, 5(6),* 512-514. https://doi.org/10.1016/j.nantod.2010.09.001