

Where2Park: An Internet of Things Approach to Managing Travel Congestion
(Technical Topic)

Enhancing Security Infrastructure and Safety Measures for Internet of Things Devices
(STS Topic)

A Thesis Project Prospectus Submitted to the

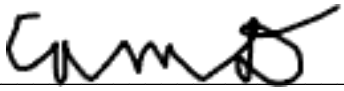
Faculty of the School of Engineering and Applied Science
University of Virginia ~ Charlottesville, Virginia


In Partial Fulfillment of the Requirements of the Degree
Bachelor of Science, School of Engineering

Cameron Davis
Fall 2020

Technical Project Team Members: Gunther Abbot, Sean Reihani, Nawar Wali

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 12/09/2020
Cameron Davis, Computer Engineering Undergraduate

Approved  Date 12/10/2020
Technical Advisor: H. Powell, Department of Electrical and Computer Engineering

Approved _____ Date _____
STS Advisor: S. Travis Elliott, Department of Engineering and Society

Introduction

All engineers need to account for the environmental impact and durability of their projects as the global population continues to grow and change its surroundings. People are moving from rural areas to urban areas at an increasing rate, a phenomenon known as urbanization. The United Nations projects that by 2050 about 68% of the world's population will live in an urban environment (United Nations, 2018). Urbanization has taken tolls on the environment resulting in lower water quality, lower air quality and habitat loss for animals.

Carbon monoxide and smog from vehicles used for transportation are one of the major causes of air pollution associated with urbanization. This directly impacts the health of urban populations, such as in Brazil where links have been found between exposure to traffic-related air pollution and developing asthma (Ponte, Eduardo Vieira, 2018). In order to mitigate these issues, modern urban planning has a focus on creating “smart cities” and “sustainable cities” to minimize these malignant effects. The technical portion of this project, *Where2Park*, aims to help individuals reduce their personal carbon footprint by developing a parking node to track available spots that can be seen on a web based interface. The technology would be used in parking garages or open air parking lots, which would increase parking efficiency and reduce emissions from idling, providing a way for individuals to contribute to reduce their carbon footprint.

The STS portion will examine privacy concerns associated with the development of IoT devices like the technical project. Common IoT devices like the Amazon Alexa and the Apple Watch have created a comfort level between society and this new technology but this increased use inherently raises our exposure to security risks for both private and public parties. Security must be constantly updated during the IoT lifecycle, which creates a unique challenge for both

consumers and manufacturers. As a relatively new field, IoT devices lack a standardization of security protocols which make it difficult to ensure a high level of protection for all devices (Das, 2018). The thesis will try to develop protocols that account for current security measures and risks which will make it easier to approach future risks.

Technical Topic: *Where2Park*: An Internet of Things (IoT) Approach to Travel Congestion

IoT is on track to become a central pillar of urban development, as a 2015 projection expected cities to spend \$41 trillion on IoT across the following two decades (Adler, 2020). Where2Park is an IoT project that consists of a series of battery-powered sensor nodes designed to increase efficiency while parking. The project focuses on sustainability by providing users with information to reduce their individual carbon footprint. Each node will feature a metal detecting sensor, power management hardware and will interface with a microcontroller that will connect with the other nodes using a Zigbee protocol mesh network. The nodes interface with a centralized application that will update the availability of the parking spaces in a lot, the battery status of each node and a running count of free spots. The technical project was broken into four

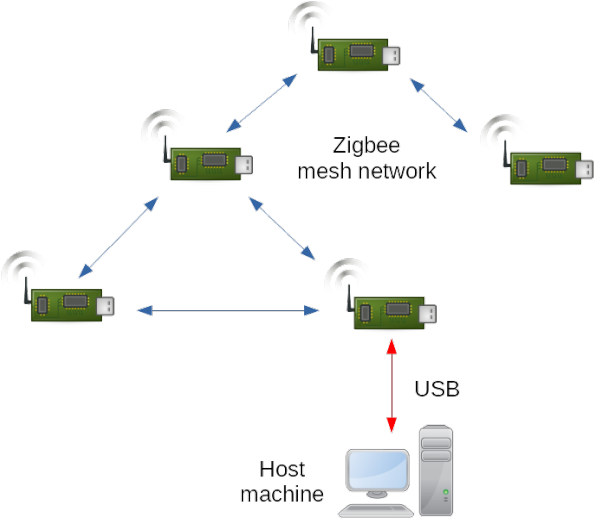


Figure 1: Diagram of Mesh Network

sections: Metal Detector, Networking, Signal Conversion and GUI Interfacing, which allowed the team to work on parallel paths and improved development speed. The purpose of the sensor node is to interpret the vacancy of its parking spot. The metal detector will detect the car in the spot to avoid deviations that can occur using other types of sensors. The inductor would be the metal detecting coil which would oscillate near metals without a power source and a BJT will provide continuous gain to offset this.

The microcontroller used on the sensor node is a TI SimpleLink Cortex-M device with built-in Zigbee functionality and multiple analog to digital converters. This part was chosen due to its integration with Zigbee and low-power architecture which are characteristics well suited for battery-powered wireless sensor nodes. Additionally, Zigbee is a Mesh Network that possesses the capability to self-heal, i.e. if a node on the network fails, other nodes will automatically reroute (Bosch, 2020). Two analog to digital converters will be used on the microcontroller, one for monitoring the voltage of the battery and another for reading from the metal. Each node will be identical from a hardware standpoint, i.e. any node can serve as a router, coordinator, or end-device. This serves two purposes: scalability and reliability. In regards to the former, if new parking spaces are added to a lot, then installing new sensor nodes is a trivial matter. In regards to the latter, if one device fails, then another can take over. This means that if a coordinator/end-device fail, then a sensor node in router configuration can take its place, and if a router fails, traffic can be rerouted through other nodes.

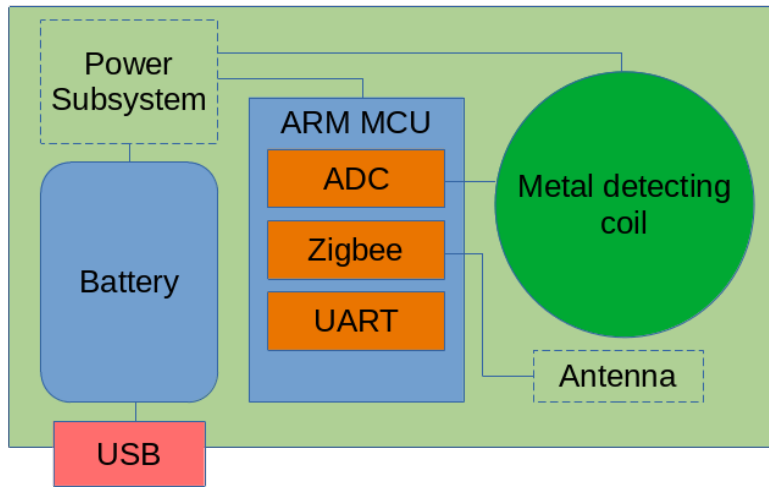


Figure 2: Diagram of the Sensor Node

The desktop application will serve as the interface to visualize the data. The application will connect to a Zigbee node fashioned as a router. The other Zigbee nodes, fashioned as coordinators, will send signals so that the system can manage and interact with the number of available parking spots. The application will be designed to show an image of the structure where the system is implemented and the available parking spots will be displayed. Additionally, the system will keep a running count of available spaces out of the total available spaces. Our mesh network will connect to our computer using a USB and will function on UART communication protocol. The application will be designed using the Nana C++ library, a cross platform library for GUI programming. This platform will allow us to seamlessly integrate with our chosen microcontroller and produce an interface available to the user.

There are a series of problems anticipated in the development of the parking system. First, the Zigbee module will take some trial-and-error to get to a working state. While comparable to Bluetooth or WiFi, Zigbee is still a complex standard with many facets, including coordinators, routers, and end devices. The metal detector will also pose several problems and

after construction might need to be tuned or redesigned, as necessary. For instance, its range or power consumption may be greater or less than initially designed for, and could need adjustment. In addition, the battery consumption and replacement will be considered. For the purposes of the Capstone, a regular alkaline battery will be used but for industrial use, a solar cell could have been used to power the system. If a complete board is designed rather than a Launchpad header, the project would be faced with the challenge of designing an antenna to broadcast and receive Zigbee signals. Another potential issue is the interfacing between the sensor node network and the desktop application. There are other ways to connect the mesh network and the desktop application, however the USB option is the most feasible option.

The expected outcomes of the project include a successful interface between sensor nodes and host machine as well as proper calibration of ADC and successful detection of a vehicle. To build a successful project, PCB software such as KiCad will be needed. To build the desktop application, a suitable GUI framework is needed, such as Juice. Another component which is integral to the project is Github and GitKraken. Both of which allow group members to check on the progress of the project and provide housekeeping details. To successfully test for the project outcomes, a vehicle will be needed for testing purposes.

STS Topic: Developing Safety Measures and IoT Security Infrastructure

Background

The proposed thesis will examine how to approach the security risks and ethical issues associated with IoT solutions. The analysis will be completed using the theory of Social Construction of Technology (SCOT) in order to understand the compromises society makes to adopt these advancements since the increase in population has correlated with an increase in

pollution and IoT devices are the proposed solution. Society has created a need for appropriate security measures but there are no unified technical or government IoT standards for manufacturers or developers, which creates ethical issues when interacting with IoT technologies. “The issues associated with security of IoT are not only the issues related with security of wireless medium, WSN and internet, but also access control, authentication and privacy issues associated with IoT” (Cynthia, 2018).

The major categories that we can look at from a societal perspective are privacy and regulatory standards. These issues “stem from integrating devices into our environments without us consciously using them” (Banafa, 2017). In the technical portion, the user will be interacting with a GUI that provides them location data within a parking lot. Protecting this data presents a major concern associated with our product since remote access to specific parking spots create a risk for interpersonal crimes like stalking or robbery. While these dangers can manifest in other ways, this concern requires added security measures so users can avoid an increased risk compared to the benefit of using the system (Vasilomanolakis, 2015). Other types of technologies within IoT such as wearables carry the significant privacy risk of storing user’s health data (Wei, 2014). The lack of regulation can lead to misuse of this data and leave users vulnerable to parties such as health insurance companies or hospitals who could upcharge customers if they are able to associate with a specific user with unusual health factors.

Methodology: Social Construct of Technology

In order to fully understand SCOT we must “consider the five components of SCOT—relevant social groups, interpretation, closure, technological frame, and the wider social context” (Klein, 2002). The first part of SCOT aims at addressing the different considerations made when

developing a solution. By considering the problem from the viewpoints of “relevant social groups”, engineers can better understand the full scope of a technology’s impact in the community. This pairs with the core concept of “interpretive flexibility”, which takes a neutral approach towards design by considering all arguments made for or against a technology by those relevant social groups. The concept of “design flexibility“ helps determine how to best build the product for each group given their unique social challenges and pairs with “interpretive flexibility”.

The second part of SCOT focuses on addressing the proposed problem through a closure and stabilization. Reducing global pollution lends itself well to this analysis since “a multigroup design process can experience controversies when different interpretations lead to conflicting images of an artifact.” (Klein). The “closure” component focuses on resolving the conflicting views until the artifact can “stabilize” to a form that can be accepted by all the relevant social groups. Two forms of “closure” offered through SCOT are “rhetorical closure and closure by redefinition”. The former concludes with a declaration that no further problems exist and that no additional design is necessary. The latter occurs when unresolved problems are redefined so that they no longer pose problems to social groups. The final part of SCOT discusses the “technological frame” developed between actors and “wider social context” of the relevant groups that make and benefit from the technology and how they fit into or change societal structure.

I plan to use SCOT to examine how to create a set of standards aimed at aligning security amongst IoT solutions to ensure a comprehensive and satisfactory level of cybersecurity for user’s personal data. All of the factors mentioned above play a role in deciding how to secure networks so by consulting a variety of data sources I can determine which social groups are

most relevant, namely engineers, company shareholders, general consumers, and lawmakers will be accounted for. Security changes during the device's lifecycle, so there is a need to better understand how cybersecurity is understood by consumers. Short questionnaires and interviews can be used to gather data to understand the "interpretive flexibility" of this problem by each group with the goal of drawing a consensus and examining it to determine how to incorporate the users into the solution. Example questions would be which kinds of IoT devices they have in their house and how often they update that device. Another data source will come from examining previous accidents involving IoT devices, what security measures failed and what changes could have been made to prevent that failure. Gathering these perspectives will help me look at what innovations have been made to any failed security measures to help figure out what closure method would be most appropriate. After a closure method is chosen, the proposed set of security measures will be considered in their societal context to see what impact it would have on the relevant social groups.

Conclusion

By analyzing the effects of IoT security in society and how those devices can be sustainable, this paper aims to figure out how to better protect society both physically and digitally. As urban development continues to innovate with "smart cities", traditional security methods will not suffice and new measures must be considered to keep up with the rapid innovation in IoT devices (Kawamoto, 2014). I plan to determine what relevant social groups can contribute to the security solution and look to each individual for guidance. One target group would be manufacturers without the adequate training or materials to ensure a minimum level of security. Another target group would be education of citizens and how they can protect

themselves. Finally, I will survey engineers who work on the project to better understand the difficulties when scaling the number of devices.

The desired benefit of the technical project focuses on sustainability by reducing individual carbon emissions while the social topic focuses on the accountability required for the scalability of IoT solutions in “smart cities”. Ideally, this research can help provide a set of protocols to maximize the security in IoT devices at several levels. If a set of standards cannot be developed across industries, I aim to better understand the limitations behind developing such a system and focus on creating standards for different sectors. Under SCOT, both of these results would provide value and better guide society towards making the appropriate considerations for different social groups. I also hope to explain why existing security measures cannot cover the full scope of technologies and why there is a need to focus on developing measures specifically for IoT solutions. In order to consider the impact of the protocols, I will end with considering what role society plays in developing future IoT devices and whether updates to a industry-wide standard or sector-wide standard would be more worthwhile.

REFERENCES

- Adler, L. "The Urban Internet of Things", Data-Smart City Solutions, 2020. [Online]. Page 2. Available:<https://datasmart.ash.harvard.edu/news/article/the-urban-internet-of-things-727>.
- Banafa, A. (2017, March 14). *Three Major Challenges Facing IoT*. IEEE Internet of Things. <https://IoT.ieee.org/newsletter/march-2017/three-major-challenges-facing-IoT.html/>.
- Bosch Devices. "The wireless smart parking sensor for detecting parking space occupancy", Bosch Connected Devices and Solutions, 2020. [Online]. Available: [https://www.bosch-connectivity.com/products/connected-mobility/parking-lot-sensor/#:~:text=The%20Parking%20Lot%20Sensor%20\(PLS,parking%20is%20installed%20in%20minutes](https://www.bosch-connectivity.com/products/connected-mobility/parking-lot-sensor/#:~:text=The%20Parking%20Lot%20Sensor%20(PLS,parking%20is%20installed%20in%20minutes).
- Cynthia, J., Sultana, H. P., Saroja, M. N., & Senthil, J. (2018). Security Protocols for IoT. *Studies in Big Data Ubiquitous Computing and Computing Security of IoT*, 1–28. https://doi.org/10.1007/978-3-030-01566-4_1
- Das, A. K., Zeadally, S., & He, D. (2018, June 28). *Taxonomy and analysis of security protocols for Internet of Things*. <https://www.sciencedirect.com/science/article/pii/S0167739X18308112>.
- Hasan, M. (2022, June 14). *State of IOT 2022: Number of connected IOT devices growing 18% to 14.4 billion globally*. IoT Analytics. <https://iot-analytics.com/number-connected-iot-devices/>
- Kawamoto, Y., Nishiyama, H., Kato, N., Yoshimura, N., & Yamamoto, S. (2015, July 30). *Internet of things (IOT): Present state and future prospects*. Tohoku University. <https://tohoku.pure.elsevier.com/en/publications/internet-of-things-iot-present-state-and-future-prospects>
- Klein, H. K., & Kleinman, D. L. (2002, January 1). The Social Construction of Technology: Structural Considerations. *Science, Technology, & Human Values*, 27(1), 28-52. <https://journals.sagepub.com/doi/10.1177/016224390202700102>
- Ponte, E. V., Cruz, A. A., Athanazio, R., Carvalho-Pinto, R., Fernandes, F. L., Barreto, M. L., & Stelmach, R. (2016). Urbanization is associated with increased asthma morbidity and mortality in Brazil. *The Clinical Respiratory Journal*, 12(2), 410–417. <https://doi.org/10.1111/crj.12530>
- Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., & Kikiras, P. (2016). On the security and privacy of internet of things architectures and systems. *2015 International Workshop on Secure Internet of Things (SIoT)*. <https://doi.org/10.1109/siot.2015.9>

Wei, J. (2014). How wearables intersect with the cloud and the internet of things : Considerations for the developers of wearables. *IEEE Consumer Electronics Magazine*, 3(3), 53–56.
<https://doi.org/10.1109/mce.2014.2317895>