Sean Grant

Kolby Lacy

October 17, 2017

In certain buildings, the HVAC systems are implemented in a way that they 'work' but are not optimized in a way that would allow for more efficient usage or energy consumption. Mostly because they often times rely on the input from a single source, which implements the same settings for various rooms across the building. What we want is to take an existing system such as this and be able to automate individual temperature readings for each room. With the creation of a sensor network, we can achieve this by having sensors in a room automated to record and report temperature readings to a central location that will process the data and take steps to adjust the temperature. Wireless sensor networks are on the cutting edge of communication technology and many useful applications have been discovered in the military, health, and environmental science fields. What is useful about wireless sensor networks is that they can record much more information than a single source and can obtain valuable information that can be provided by a variety of sensors. Even more, this process can be automated, increasing its efficiency. Another convenience is that because this data is usually sent to a server, it can also be accessed remotely and interpreted by an expert if need be. There are numerous patents and research papers related to the implementation and security of these wireless sensor networks. Our project will implement a design for a sensor network exclusively for increasing HVAC operation.

Section 1

The wireless temperature sensor network project is centered around the current status of the data communications field. At the base of the project is the ability to transmit and receive signals at specific radio frequencies. The transmission of data wirelessly is related to the way in which the analog measurements taken from the temperature sensors will be transferred to the backend database that will monitor the system. The receiving of said signals will be the main task allocated to the backend server because once the signals are received it will be up to the backend CPU to process said data. However, having all of the processing power tied to the backend server is just one implementation idea that is being analyzed. Another idea that is being looked into is having a portion of the processing of the analog signals taken from the temperature sensors done on the actual sensor nodes themselves. This would be done with the purpose of reducing the bandwidth needed to transmit the data to the backend server. If the unprocessed data would consume less bandwidth than the output (processed) data then it would make sense to just

transmit the unprocessed data to the backend CPU. However, if completing some level of processing on the CPU of the temperature sensor itself and then transmitting the data saves bandwidth, then this is the route that our project will take.

Currently, wireless data communications are done using radio frequencies. Any discussion of wireless communications and the use and security of wireless data transfer begins with analysis of the electromagnetic radio frequency spectrum. Wireless communications between devices can be thought of as a transfer of data through the air from one device to another, however, there are more elements at work throughout this process. Electromagnetic radio waves at specific radio frequencies, or channels, on the RF spectrum are used to transmit signals through the air where an electromagnetic signal receiver then receives the signal. Conceptually, the data being transferred is "attached" to an electromagnetic radio wave, as previously described, and then instead of sending the data to the receiver, the radio signal carrying the data is sent. Once the signal reaches the correct receiver (which is determined through identification addressing of the transmitter and receiver) the data is then extracted from the radio wave and analyzed accordingly. The electromagnetic radio frequency spectrum ranges from about 3kHz to 300GHz and each frequency (or channel) holds the capacity to transmit an individual signal. However, not every frequency, channel, or band (a range of channels) is available for use by the public. The Federal Communications Commission (FCC) assigns certain radio frequency bands to licensed entities (primary users) such as cellular phone carriers and government agencies. Any users who are not licensed to operate on a specific frequency band or have not paid to operate on the frequency band are considered secondary users. Secondary users can be any individual with a need to utilize a specific radio frequency channel or band, from wanting to set up their own WiFi network to wanting to establish their own data transfer protocol. The driving factor that separates primary users from secondary users is that primary users usually occupy a certain frequency band for commercial purposes, while secondary users may occupy a specific frequency band for more personal uses.

Section 2

Wireless sensor networks incorporate the operation of many nodes that collect similar data to be sent to a base node/server to be processed. Currently, there are many papers that are researching applications for wireless sensor networks. Some of theses applications include: military surveillance, which would acquire valuable information such as enemy position and capabilities, smart home projects, where the networks can be used to optimize energy consumption for everyday living or be adapted as an alert system for assisted living residents, and environmental research, to collect climate, pollution, or other useful data.

The military architecture VigilNet supports military surveillance with the use of its several subsystems. The sensing subsystem processes magnetic readings, acoustics, and infrared data. This data is interpreted along with the Context-Awareness Subsystem to make the sensed

data useful. The remaining subsystems: the Tracking and Classification, Networking, GUI and Control System, power management, reconfiguration, and,debugging subsystems are used to finalize and record the data so that they may be analysed by military personnel.

AlarmNet is a healthcare application of wireless sensor networks. AlarmNet was developed with the idea that the automation of certain medical devices would allow for not only efficiency, but would also increase the quality of healthcare by allowing devices to continually record and monitor information. This would allow healthcare professionals to remotely monitor and diagnose patients. AlarmNet is an assisted-living and residential monitoring network for adaptive healthcare in assisted living communities.

An environmental science application of wireless sensor networks is Luster. Luster measures the effects of sunlight on under shrub growth on barrier islands. Shrub growth is something that has been increasing across the globe in a number of different climates. It has been shown that this growth is linked to climate change, although it is not certain exactly what is causing it. Currently, scientists are measuring light at single points for extended periods of time in order to try and find answers. However there is a need to carefully measure the effects of the intense direct light on the plant and the rapid photosynthetic actions of the plant so that there is more valuable data to analyze. This is where the Luster architecture comes in. Its task is to measure light at fine spatial and temporal granularity.

Section 3

Our projects primary goal is to create a sensor network that we can use to automate the measurement of temperature readings in a building and use the information for dynamic temperature control. We will uses small computer boards with equipped sensors as nodes in a room that will record temperature readings and report them to a base station where the data can be processed. The processing of the data will create the information needed to adjust the temperature accordingly. The long term or "big picture" of this project is that we will eventually take our sensor network and apply methods to test hardware security and maintenance. We will take a "data anomaly" approach as we analyze the data for appropriate readings and raise flags when a node appears to be compromised. This could mean that either the device has become faulty or the device has been tampered with. In any case it is in our best interest that we create a system that would alert us to any distinct changes in the behavior of a node.

The current status of this project reflects the ever growing appeal of sensor networks. Patents that have been applied on the topic of sensor networks apply to security of the network or a specific technique that is used in the communication between nodes and a server or a data sink. Several existing projects cover a number of fields but not as many individual topics. Our design, other than being a sensor network, has no similarity to other current projects. As it stands, there isn't a need to modify or change the design requirements as there is no infringement on our side.