DATA MANAGEMENT AND SECURITY IN WIRELESS SENSOR NETWORK

Hee Jin (hjin@smith.edu)
Department of Computer science, Smith College, Northampton, MA, 01063

Abstract

Data management and security is an important subject in wireless sensor network. Many researches have proposed various designs of storing data such as having the SD card embedded in the sensor node, or having a separate storage node that passively stores data that were streamed between other nodes. The security of these data in the local nodes can be enhanced by implementing an encryption and decryption algorithm that involves keys and hash functions. In this project, a prototype is made to present a way to store and transmit data. The data is collected through the GPS and is stored in the SD card. With these data, the prototype performs two scenarios. First, it constantly streams out parsed data with the data also being stored in the SD card. Second, the data stored in the SD card is transmitted which enable access to large amounts of data from the past. This prototype could further be used in GPS tracking systems or health monitoring which requires accurate and secure wireless data transmission.

Introduction

Wireless sensor network refers to any type of computer network that is not physically connected with cables and collects data such as temperature, sound, pressure and etc from distributed sensor nodes. Today, it is widely used in cell phones, computers, health monitoring and so on.

For wireless sensor network, it is important that it not only senses detailed physical or environmental conditions, but also how the data collected is stored and accessed. Therefore, it is important to have a memory card that stores the data that were collected from the sensor nodes. It is possible to constantly transmit the collected data simultaneously without storing, but the quality and accuracy of the data could be tampered due to weather or other obstacles. Also, being able to wirelessly access the data stored in the memory card would decrease physical limitations of accessing the data especially researches in harsh areas where human access could sometimes be restricted.

Data storage without additional security measurements can be manipulated easily. The node itself on the field lacks physical protection which is due to unattended deployment environment and absence of tamper resistance. This allows the attackers to invade the deployment field, capture the nodes and steal the information stored in the nodes (Subramanian 2007).Therefore, data should be encrypted before being sent out to avoid these possible attacks.

In this project, Arduinos and Xbees are used to demonstrate how to store data and wirelessly transmit it to another device. Also, an LCD (Liquid Crystal Display) is used for data demonstration.

References

"SD memory card architecture." *lchu.net*. Web. 17 Dec 2013

Subramanian, Nalin, Chanjun Yang, and Wensheng Zhang. "Securing Distributed Data Storage and Retrieval in Sensor Networks." Iowa State University. 2007. Web. 14 Dec 2013.

Methods

In the prototype for this project, Arudiono GPS shield, Xbee and the LCD was used. The GPS shield also has a SD card slot on it for data storage. The program that is downloaded on the Arduino consists of two parts and is dependent on the "inRange" variable. When the variable is true, the GPS receives the raw data string from the satellite and transmits it to the Arduino. The Arduino then parses through the string to produce a more human readable output. The parsed data is then stored in the SD card. While it is storing data on the SD card, the data also shows on the LCD screen to be more user-friendly and also on the serial port. When the "inRange" variable is true in the program, the Arduino prints the data stored in the SD card to the Serial Port. The data that is printed on the Serial Port is sent to the other Xbee and is shown up on its serial port. The software used to program the Arduino is the Arduino software that the Arduino website distributes which is based on C language.

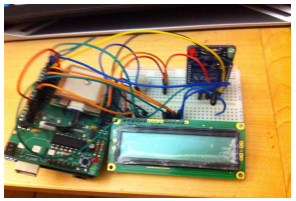

Figure 1. Finished Prototype (GPS shield, LCD, Xbee)

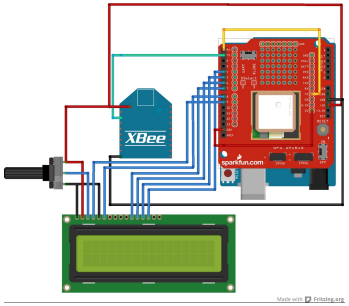

Figure 2. Diagram of the finished prototype

Results

The GPS successfully communicated with the satellite and retrieved correct GPS coordinates. The Arduino program also parsed through the raw data string and printed out correct North, East coordinates along with the time. This was verified by plugging the coordinates in Google Maps which showed the correct pathway the GPS went through. The result was shown successfully on the LCD screen, the SD card and on the Serial Port. The data that were printed on the Serial port also successfully showed on the other Xbee's serial port which suggests successful wireless communication and successful wireless transmission of the data. In the other scenario, where the "inRange" variable is true, the data stored in the SD card was successfully transmitted to the other Xbee and was presented in the correct format on the serial port. This indicates successful transmission of stored data as well.

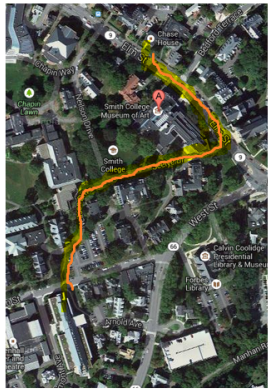

Figure 3. Google Map of the positions of the GPS data received

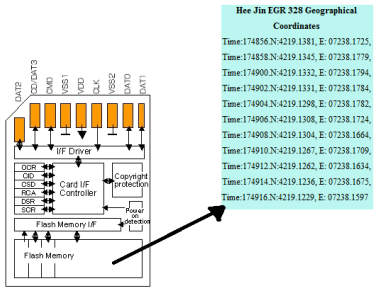

Figure 4. The collected data format that were stored in the SD card

Discussion / Evaluation

My initial idea was to create a prototype that communicates both ways through the two Xbees. The "inRange" variable was to determine if the GPS device was in range with the other Xbee and if it is, then start transmitting the data from the SD card. However, in order to do that, the other Xbee had to be connected to the Arduino which needs further programming to be able to correctly read the data transmitted from the other Xbee. Due to shortage of time, this part was not implemented and the "inRange" variable was changed manually. Also, an encryption is needed for the data to be securely stored and transferred.

The prototype, on a larger scale, could be used as a GPS or other sensors that uses SD card to store data and wirelessly transmits the data if the device is in the range of the wireless network. Environmental research in harsh environments could use this device to easily retrieve data stored in a certain period of time from the SD card without physically retrieving the memory card or having to simultaneously receive data from the sensors which could be tampered with due to weather or other obstacles. In everyday life, people could use this to access stored data more easily without cables or physically moving the memory card from one device to the other. This could enable electronic devices to be made without the sensors embedded in them which results in higher power efficiency. Since the data transmission is from the already stored data, the data have a better integrity and is more error prone which could be caused by weak signals.

Since the prototype includes sensors such as GPS, there are privacy issues that need to be considered. The privacy laws have been updated during the past years, but have yet to catch up with the fast growing technology. There are still difficult questions when it comes to devices sensing other people's activities since they are already around us. However, according to United States vs Jones case, it was ruled that the GPS sensors should not be tracking a person without their consent. And other sensors, if tracking activities of a large pool, should track each person anonymously and only acquire general data. And tampering with the data being collected or acquiring data from the network as an unknown third party is hacking and is a violation of privacy.

Conclusion

As wireless sensor networks are being widely used in everyday lives, managing the data is also important. Storing the data and being able to freely access to those data is an important element that should implemented in wireless sensor networks. In addition, protecting the stored data is also important. The data should be encrypted and then sent out to the network.

In this project, a prototype was built to demonstrate one way of managing data. The data is collected and stored in a memory card and then sent out wirelessly to another device.

With more security measurements and two way communication between the Xbees, this prototype can be further applied in health monitoring or in environmental researches.