WASP
Wireless Arduino Sensor Protocol

Group SW513E15

Christian Lundtofte
Henrik Djernes Thomsen
Jonathan Hastrup
Bjørn Opstad
Morten Mandrup
Mathias Corlin

AALBORG UNIVERSITY
STUDENT REPORT

Department of computer science
Selma Lagerlöfs Vej 300
9220 Aalborg Ø

Title:
WASP - Wireless Arduino Sensor Protocol

Theme:
Embedded Systems

Project period:
02/08/2015
21/12/2015

Project group:
SW513E15

Members:
Christian Lundtofte Sørensen
Henrik Djernes Thomsen
Jonathan Hastrup
Bjørn Opstad
Morten Mandrup Hansen
Mathias Corlin

Supervisor:
Hua Lu

Synopsis:

Synopsis her!

No. printed Copies: ?
No. of Pages: ?
No. of Appendix Pages: ?
Total no. of pages: ?
Completed: 21/12/2015

The contents of this report is freely accessible, however publication (with source references) is only allowed upon agreement with the authors.

Bjørn Opstad

Christian Lundtofte

Morten Mandrup

Henrik Thomsen

Matihas Corlin

Jonathan Hastrup

Contents

1 Project introduction **5**
1.1 Initializing problem statement 5

I Analysis **6**

2 Context **8**

3 Use case **9**
3.1 Interview 9

4 Technologies **10**
4.1 Networks 10
4.2 Wireless communication 10
4.3 Communication protocols 10

5 Problem Statement **13**
5.1 Requirements 13

II Implementation **14**

6 Theory **15**

7 Design **16**

8 Implementation **17**

9 Test **18**

III Conclusion **19**

10 Reflection **20**
10.1 What have we done!? 20

11 Summary **21**
11.1 It ended like this 21

12 Future Work **22**
12.1 To be done 22

IV Appendix **24**

1. Project introduction

This is an introduction.

Here is the initializing problem statement:

1.1 Initializing problem statement

How can a sensor network and a protocol be designed, so that data can be relayed throughout the network, enabling an endpoint device to receive the information without being within range of all sensors in the network?

It is a good question and we will analyze it.

Part I

Analysis

The analysis will discuss and look into the different aspects of the initializing problem formulation and the topics therein. The sections in this chapter blah-blablah..

2. Context

3. Use case

The purpose of this project is to create a protocol that allows multiple Arduinos to share data to a single endpoint, but a use case is needed to test the protocol.

The chosen use case for this report is soil moisture for use on golf courses. A golf course is usually very large, and covering an entire golf course with cords would be a big task. Furthermore this would make the system hard to extend and make hot pluggable.

That makes this project a good use case for golf courses, as soil moisture is important in determining where it is necessary to water the course. Wasting water is not much of a problem in Denmark, but some places in the world water is a sparse resource. Using less water on a large golf course could save money down the line too, and is good for the environment. The use of radiocommunication is well suited for large, open spaces, like a golf course.

3.1 Interview

An informal interview was performed with a greenkeeper at Aalborg Golfcourse, Kim Jensen. Kim provided insights on the requirements of the system, potential problems, and ideas for later iterations of the system. The interview questions and answers can be found in Appendix ##.

Some holes on Aalborg Golfklub is located in a swampy area, which often makes watering them obsolete. This project could help stop some of this water waste. Some holes are in a moor, where watering is often required. When it is required, this project could inform the greenkeepers, who could act on this. Making the product hot pluggable would be useful if there is suddenly more or less water than usually, in which case the product can be added to this location, and the water levels can be measured to determine if there is a problem, and in that case how to solve it. The same applies if an area is more dry than usual.

An important consideration is where to place the devices. The sensors needs access to the soil in order to measure the moistore levels, but they should not be placed above ground as golfers could hit and destroy the devices. The initial idea was to place it in the holes for the sprinklers, but this was bad since sprinklers often leak, and the sensor would therefore get inaccurate readings. This makes it necessary to bury the devices at known locations in the course. The depth the devices are buried at are important, due to the differnet types of grass. The greens use a 2cm. layer of sand at the top, which allows water to quickly go through. This makes it necessary to bury the devices 10-15cm. in the ground. These requirements changes based on the kind of grass and what is beneath.

Regarding future iterations of the project, Kim suggests adding a pH meter to the devices. This would allow the greenkeepers to create specific mixes of fertilizer for different parts of the course, depending on the pH value of the soil.

We shall look at some existing technologies now.

4.1 Networks

4.2 Wireless communication

4.3 Communication protocols

A mesh network can use a wide variety of protocols, to manage the route data is transferred. In networking, a protocol is a special set of rules and standards for how nodes would interacts with each other. A well known protocols could be TCP/IP(Transmission Control Protocol/Internet Protocol), which today are used to communicate between almost anything with a internet connection. The mesh network we are looking at is a radio based network, and therefore some more relevant protocols will be examined. A few excising protocols will be presented in this section.

4.3.1 Time division multiple access

Time division multiple access(TDMA) is protocol that divides a single channel into smaller time slots. Each time slot transmits one byte or a segment of a signal, in a sequential serial data format. Each slot is active of a small amount of time, before the next slot in the queue get time to transmit.

TDMA is as an example used in the T1 telecommunication transmission system. Each T1 channels carry up to 24 voice telephone connections. Where each connection covers 300 Hz to 3000Hz and is digitized at an 8-kHz rate, which is two times the highest frequency component needed to retain all the analog content.

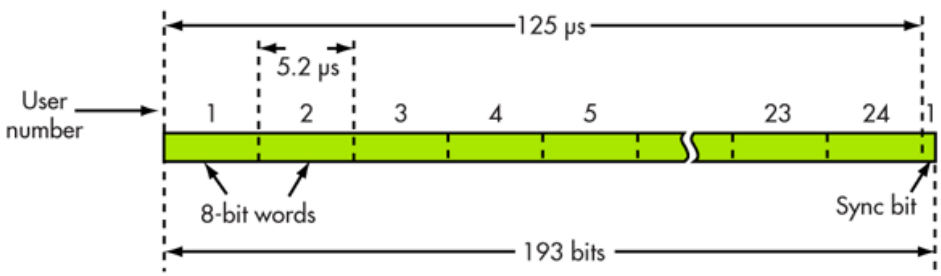

Figure 4.1: Illustration of the TDMA protocol

On Figure 4.1 it is seen how the channel, for T1, is split up into 24 smaller pieces. Each time slot is accountant for a user using a voice channel, to talk to some

other user. Each time slot is of the size 8-bit, the user is unaware of this small data size, and that other are using the same channel, because the shift between each time slot happens so fast. This gives the illusion of each user talking with no interruptions, even though each user only is assigned 1/24 of the total bandwidth. A single bit is used to synchronization. The TDMA system can maximum achieved a data rate of 1.544 Mbit/second.[1]

TDMA can be used for any system that require several device to use the same channel, without interfering with each other.

4.3.2 Ad hoc On-Demand Distance Vector Routing

Ad hoc On Demand Distance Vector(AODV) routing algorithm is a routing protocol designed for ad hoc networks. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes.[2]

AODV is a network where only the local nodes around a newly added node, is affected by the addition. If a link between nodes is broken, and it does not affect an ongoing transmission, no global notification occurs. This leads to a network where new nodes easily can be added and removed without overhead on the entire network. The transmission route in AODV is managed so, that only nodes in the direct route is active, which reduce the need for route maintenance and reduce idle nodes. The protocol can determine multiple routes between a source and a destination, but only a single one is implemented. The route is not necessarily the shortest.

A downside to AODV is that if a single route breaks, due to a defect node, it is not possible to know whether other routes exists. But if a route breaks, the protocol discovers a new route, if possible, as and when necessary.

When a node is ordered to send a packet to a specified destination, it checks its routing table to determine if it has a current route to the destination. If there already exist a node, the packet will be delivered to the next node in the route, repeating until it arrives at the correct location. If there does not exist a route, the node will initiates a route discovery process.

A route discovery process begins with the source creating a Route Request (RREQ) packet. The packet contains the sources node's unique ID and IP, and the destination node's unique ID and IP. The packet is then transmitted out from the source to it's neighbours. The unique ID of each node is then stored in the packet, to ensure the same node is not transmitting more than once. The destination ID is to ensure it knows when the destination node is reached. A simple AODV network can be seen on Figure 4.2, where S and D represent the source and destination. It is visualized how the route discovery is invoked using the RREQ packet.[3]

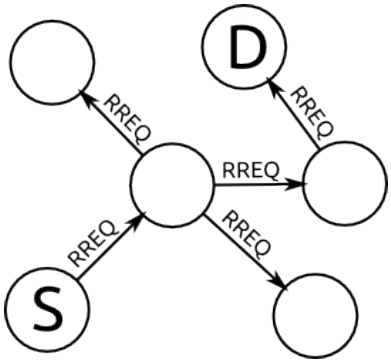

Figure 4.2: Illustration of the AODV route discovery

4.3.3 Radio Link Protocol

Radio Link protocol(RLP) is a automatic repeat request(ARQ)[1] fragmentation protocol used over a wireless air interface. Most air interface protocols have a packet loss of up to 1% which is intolerable when handling sensitive data. RLP detects losses in packets and with a retransmission tries to bring down the losses. The retransmission can bring the loss down to 0.1% to 0.0001%. This loss rate is more tolerable when handling sensitive and precise data.

RPL cannot request a certain payload size from the air interface, the air interface scheduler instead determines the packet size, based on changing channel conditions constantly. Most of the other fragmentation protocols, such as 802.11b[2] and IP, determine a payload of a certain size by the upper layers, and call upon the MAC. These protocols are not as flexible as RLP, and sometime fail transition during small fades in a wireless environment.[4]

RLP is used to make a more fail-safe environment for the transmitted data, and to ensure nothing is lost on the way. The Radio Link Protocol is typically used in cellular transmission.

[1] An error-control method for data transmission that uses acknowledgements and timeouts
[2] An wireless networking specification

5. Problem Statement

Very good problem statement for you, my friend. Special prize.

Make a good sending data network for arduino.

5.1 Requirements

There are some requirements to the system and its software. These are split in two categories: functional and non-functional. This is based on some smart guys work [**keylist**].

5.1.1 Functional requirements

The list of functional requirements:

1. Actually run is an important part to passing the exam

5.1.2 Non-functional requirements

List of non-functional requirements:

1. Looking good is not a bad thing.

Part II

Implementation

6. Theory

7. Design

8. Implementation

Part III

Conclusion

10. Reflection

oh..

10.1 What have we done!?

11. Summary

ok..

11.1 It ended like this

12. Future Work

Here's what's missing..

12.1 To be done

Bibliography

[1] Lou Frenzel. *Fundamentals of Communications Access Technologies: FDMA, TDMA, CDMA, OFDMA, AND SDMA*. URL: http://electronicdesign.com/communications/fundamentals-communications-access-technologies-fdma-tdma-cdma-ofdma-and-sdma.

[2] Samir Das Ian Chakeres Charles Perkins Elizabeth Belding-Royer. *AODV*. URL: http://moment.cs.ucsb.edu/AODV/.

[3] Johns Hopkins Dr. Baruch Awerbuch Dr. Amitabh Mishra. *Ad hoc On Demand Distance Vector (AODV) Routing Protocol*. URL: http://www.cs.jhu.edu/~cs647/aodv.pdf.

[4] Man Young Rhee. *Mobile Communication Systems and Security*. Cram101 Textbook Reviews, 2009. ISBN: 978-0-470-82336-1. URL: https://books.google.dk/books?id=eqY3q9D0NhsC&pg=PT138&lpg=PT138&dq=1%25+packet+loss+is+intolerable+to+all+variants+of+TCP&source=bl&ots=yd6kC7p1GB&sig=OhvtdRJNfxaXvQsmHjPTz5jDfqg&hl=en&sa=X&ved=0CCQQ6AEwAWoVChMIy8-B5vj9xwIVI_ByCh1frgJt#v=onepage&q=1%25%20packet%20loss%20is%20intolerable%20to%20all%20variants%20of%20TCP&f=false.

Part IV

Appendix