ISA100.11a Link Layer Implementation

Group 3: Chenyan Sun, Mingzhe Lai, Jilong Shan

1. Introduction and Motivation

Introduction:

ISA100.11a is an open wireless networking technology standard developed by the International Society of Automation (ISA). It is intend to provide reliable and secure wireless operation for non-critical monitoring, alerting, supervisory control, open loop control, and closed loop control applications. The standard addresses coexistence with other wireless devices anticipated in the industrial workspace, such as cell phones and devices based on IEEE 802.11x, IEEE 802.15x, IEEE 802.16x, and other relevant standards.

The ISA100.11a protocol represents a comprehensive industrial wireless approach that serves a broad, facility-wide wireless network for both process and discrete manufacturing. The technology is designed to meld various specifications such as FOUNDATION Fieldbus, Modbus, Profibus, HART and Common Industrial Protocol (CIP). It supports a wireless platform for diverse operations on the plant or factory floor and enables an open and interoperable application environment, while at the same time providing a robust backhaul to the Process Control Network (PCN). It can emulate legacy application layers for any wired fieldbus, and integrate with existing control systems. You can reuse proven tools and interfaces to reduce development and testing time—resulting in faster and less expensive implementations.

The user-driven ISA100.11a standard handles a much higher volume of process data, and ensures interoperability between wireless field instruments from different vendors.

Motivation

There are two main wireless automation protocols are existed for a future wireless solution for industry: HART Communication Foundation's WirelessHART specification, and the International Society of Automation's ISA100.11a standard. Qualified solution should have good performance in process control, scalability and investment protection.

WirelessHART is an open communication standard for transmission of HART messages over wireless instead of a 4-20 mA or RS484 medium, and uses the same command structure found in 4-20 mA-based HART devices. Nowadays, WirelessHART has been implemented and evaluated.

By contrast, there is still no open source implementation of ISA 100.11a now. So the objective of this project is to use a set of Firefly Nodes to implement some ISA 100.11a data link layer. And do some evaluation of this Standard to build the foundation for future fully implementation of the standard, which can provide industry a chance to compare ISA 100.11a with WirelessHART.

2. ISA100.11a Data Link Layer Overview

The DLs building blocks include timeslots, superframes, links, and graphs.

a. A timeslot is a single, non-repeating period of time. The timeslot durations in this standard are configurable to a fixed value such as 10 ms or 12 ms.
b. Three general operational alternatives are supported by the Data Link Layer
    1) Slotted channel hopping

       Each timeslot uses a different radio channel. > Makes optimal use of available digital bandwidth and supports battery-powered routers.

       It uses 16 channels, channel 11-26 for hopping. (26 is optional)
    2) Slow channel hopping

       A collection of contiguous timeslots is grouped on a single radio channel. Used for join process, network setup, and routers with available energy to run their receiver continuously.

       It uses channel 15, 20, and 25.
    3) Hybrid

       Combination of slotted and slow channel hopping.

       Used for combination of different schedules.
c. Superframe is a cyclic schedule of timeslots. Each superframe is an instance of hopping pattern with designated jobs. A device could contain or participate in more than one superframes. There are 5 hopping patterns defined by the standard, superframe could use any one of them (with offset) to schedule its pattern.

Basically, a superframe defines a certain cyclic scheduled job. For example, we could define a superframe for gateway as RX on every slot and correspond channel.

d. Links are connections between devices. When the system manager defines paths between devices, the devices receive link assignments. A link assignment repeats on a cyclic schedule, through its connection to an underlying superframe. Each link refers to one timeslot or a group of timeslots within a superframe, its type (transmit and/or receive), information about the device's neighbor (the device on the other end of the link), a channel offset from the superframe's underlying hopping pattern, and transmit/receive alternatives.

e. This standard supports graph routing as well as source routing.

A directed graph is a set of directed links that is used for routing DPDUs within a DL subnet. Each directed graph within the DL subnet is identified by a graph ID. During the routing, in the originating DL device (if it is not gateway, it will apply a contract to gateway, and gateway will configure it use a certain graph to destination) will contain a graph in Routing sub-header id to let the slaves know how to forward the DPDU. Each device along the path needs to maintain a graph table containing entries that include the graph ID and neighbor device address.

In source routing, the originating device designates the hop-by-hop route that a DPDU takes through a DL subnet. Graph routing and source routing may be mixed.

f. The DL uses TAI time for its internal operation, and provides a notion of TAI time as a service (through the DMAP) to wireless neighbors compliant with this standard. There are three kinds of nodes in Time keeping.

1). DL clock source: Usually a gateway, or a system manager, such as node of (G,M,S) shown in the figure above.

2). DL clock repeater: it is required to send SYNC signal to other nodes for their updating time, such as node of N1 shown in the figure above.

3). DL clock recipient: it only receives SYNC signal from system manager and does not repeat.

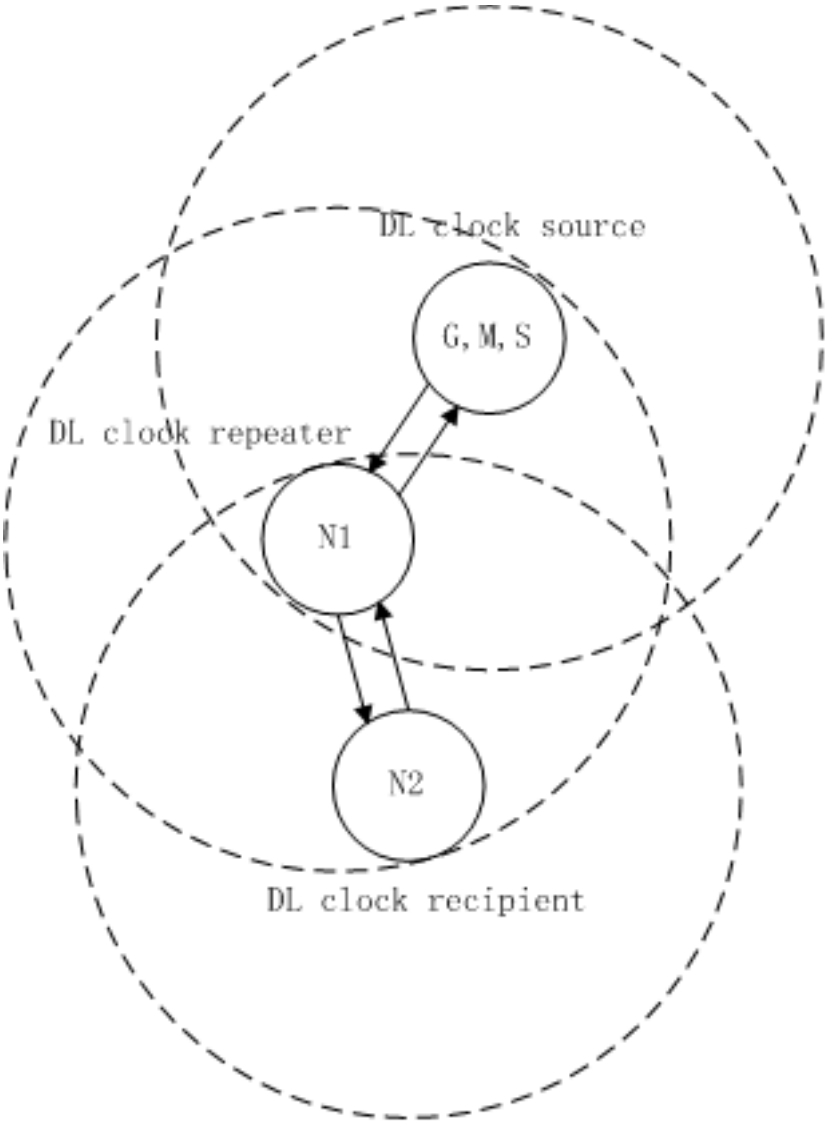


Figure 1. Relation of Clock Source, Clock Repeater, Clock Recipient

Synchronization processing

(1) General

> if a clock update request || normal communication
the device has pairwise time synchronization

> else if *dlmo.ClockExpire == true*
device actively interrogate a DL clock source/clock repeater for a time update
stop sending clock corrections to its clock recipients when receiving a request

>> if *dlmo.DLTimeout == true*
device reset itself and starts searching for new network

> else

>> if *dlmo.ClockStale == true*
clock update from secondary source

>> else

clock update from preferred source

(2) Pairwise Time Synchronization

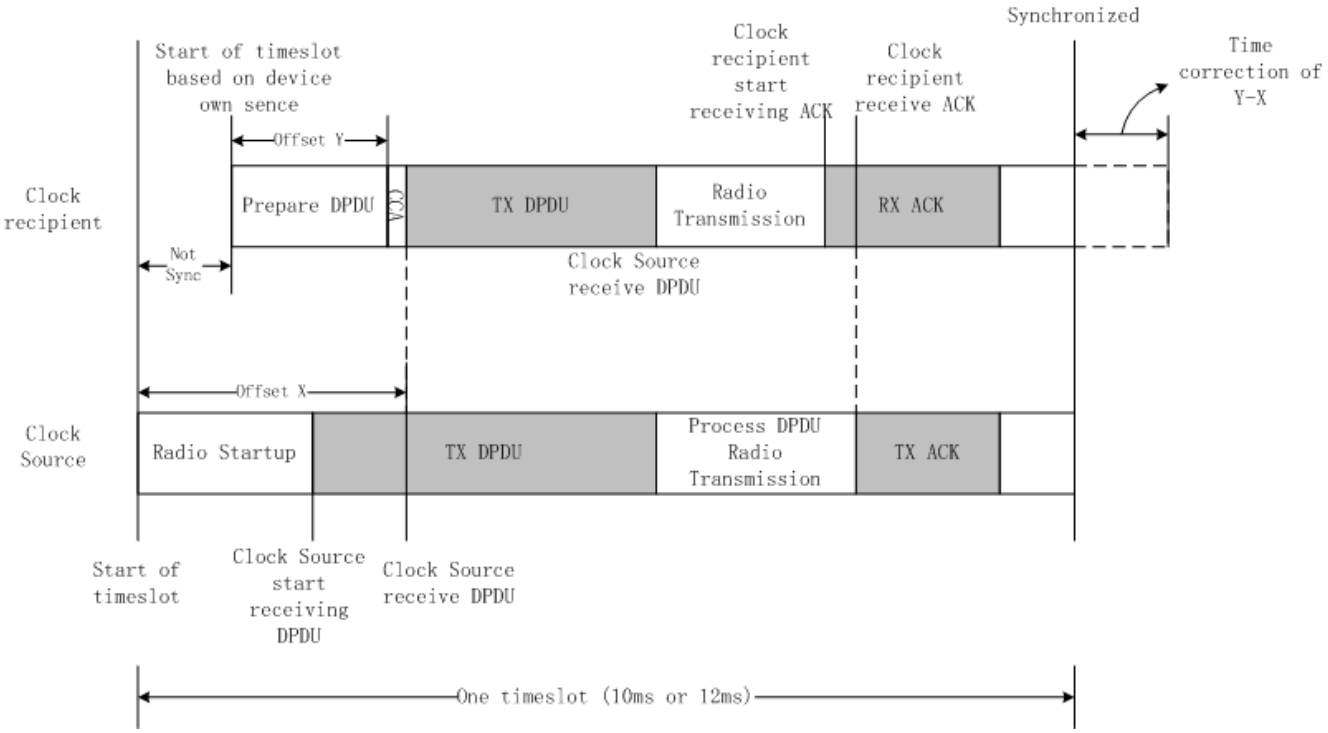


Figure above shows how to synchronize two timeslots using pairwise time synchronization. At the beginning, there is an offset between two slots which means both slots are not synchronized. Therefore clock source would start receiving DPDU in advance. Once clock source receive a packet, it would end up receiving almost at the same time with the recipient who sends the packet. However, clock source would probably consume time on processing DPDU before it sends out ACK and thus the recipient would start receiving ACK in advance. The ACK would include SNYC signal which is actually offset Y and hence recipient would correct its local time based on it. Therefore, both slots end up at the same time, which means they are synchronized.

3. ISA 100.11a Implementation

In the following, we describe our implementation in hardware, architecture, and evaluation three parts.

3.1 Hardware

We used a low-cost low-power hardware platform-FireFly as shown in Figure 2. The board uses an Atmel Atmega32L 8-bit microcontroller and a Chipcon CC2420 IEEE 802.15.4 wireless transceiver. The microcontroller operates at 8Mhz and has 32KB of ROM and 2KB of RAM. The FireFly board includes light, temperature, audio, dualaxis acceleration and passive infrared motion sensors. The FireFly board interfaces with a computer using an external USB dongle.

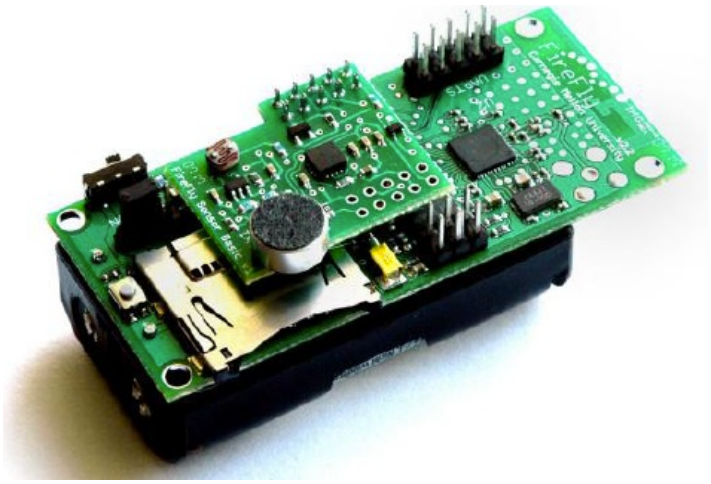


Figure 2. FireFly Sensor Node

3.2 Multi-hop sensor network architecture

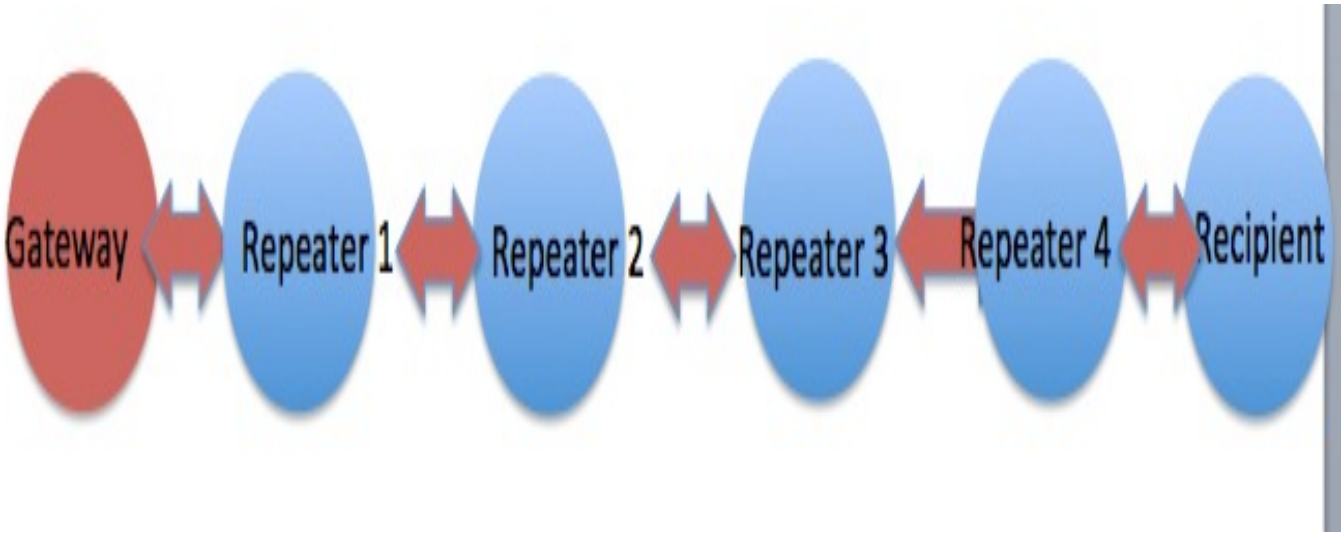
1) Basic Information

Before we start building the network, there is some basic information about our network. One TDMA frame is divided into 25 time slots. Each time slot last 10ms. The network has 6 nodes, so the recipient's messages need 5 hops to reach the destination, which is the gateway.

2) Network design

To test the link layer communication quality, we build a multi-hop sensor network. There are three different nodes in our network: gateway, repeater and recipient. Gateway represents the administrator in the network, which provides the original time source. So

in every TDMA frame, gateway should wake up at least two slots: one is to transmit the clock information and the other is used to receive packets from the nearest repeater. It also requires that every ISA100.11a based network should contain one and at most one gateway node. The network contains four repeaters. Each repeater receives time correction ACK from its previous node. The first repeater receives time correction directly from gateway. Repeater also reserves slots for future nodes to join the network. In our network, we reserve one slot at every repeater for join process. So every repeater should schedule at least three slots: two transmit slot and one receiving slot. The last one is the recipient node. In this network, we have one recipient to send packets and test our network quality. The recipient only needs to transmit in one slot.



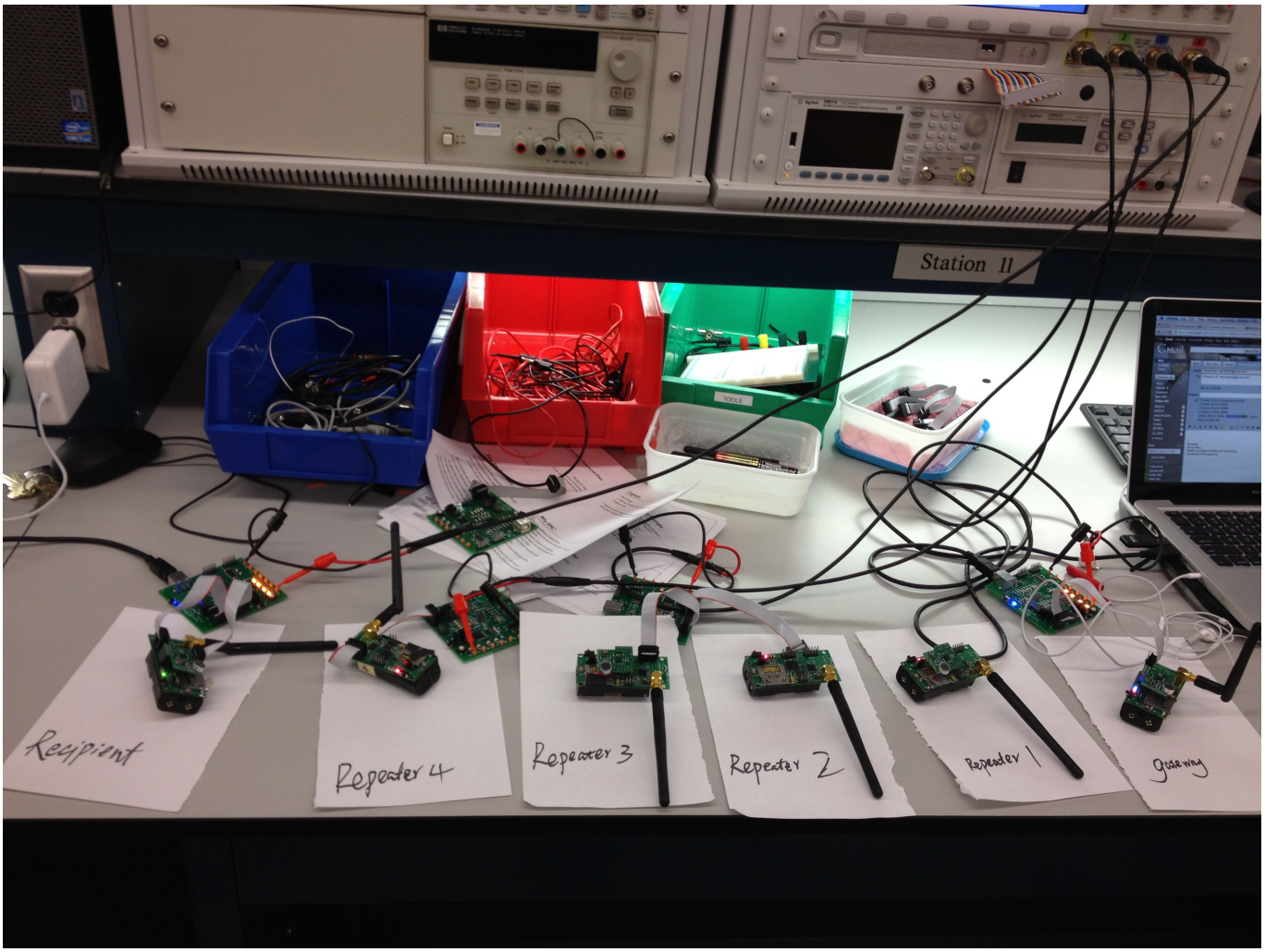
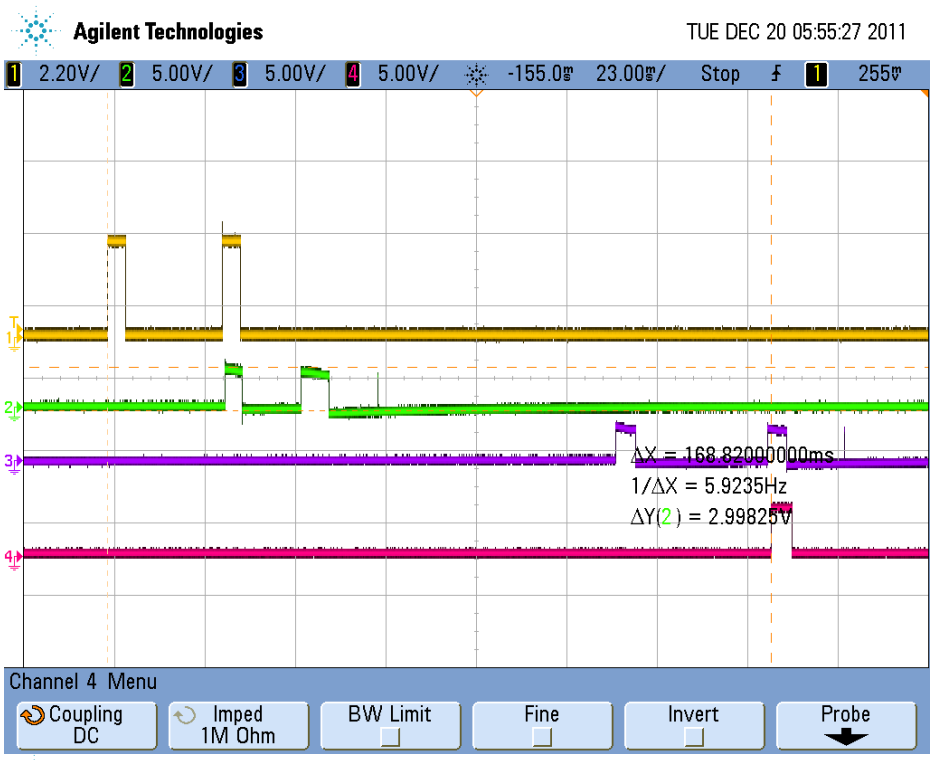


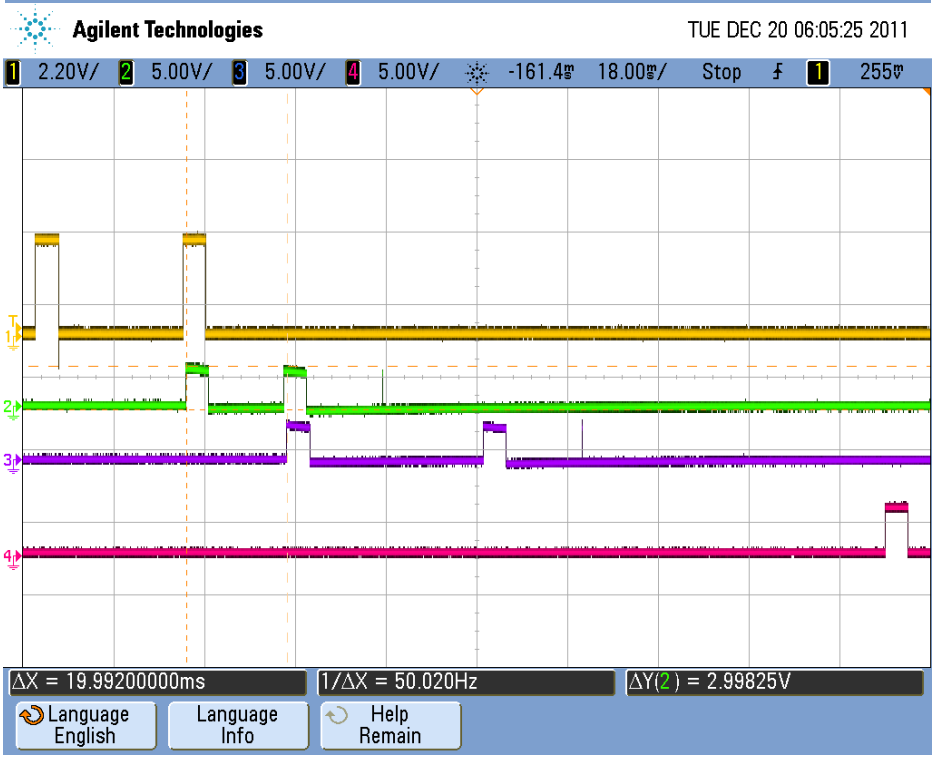
Figure 3. Physical layout of the network

3.3 Network Evaluation

1) Time Drifting

To analyze time drifting in the network, we record the time difference between every one hop nodes and the final time difference between gateway and recipient. The TX and RX slot for each node is shown below.


Agilent Technologies
TUE DEC 20 05:55:27 2011
1 2.20V/ 2 5.00V/ 3 5.00V/ 4 5.00V/ -155.0ms 23.00ms/ Stop 1 255mV
ΔX = 168.82000000ms
1/ΔX = 5.9235Hz
ΔY(2) = 2.99825V
Channel 4 Menu
Coupling DC
Imped 1M Ohm
BW Limit
Fine
Invert
Probe


Agilent Technologies
TUE DEC 20 06:05:25 2011
1 2.20V/ 2 5.00V/ 3 5.00V/ 4 5.00V/ -161.4ms 18.00ms/ Stop 1 255mV
ΔX = 19.99200000ms
1/ΔX = 50.020Hz
ΔY(2) = 2.99825V
Language English
Language Info
Help Remain

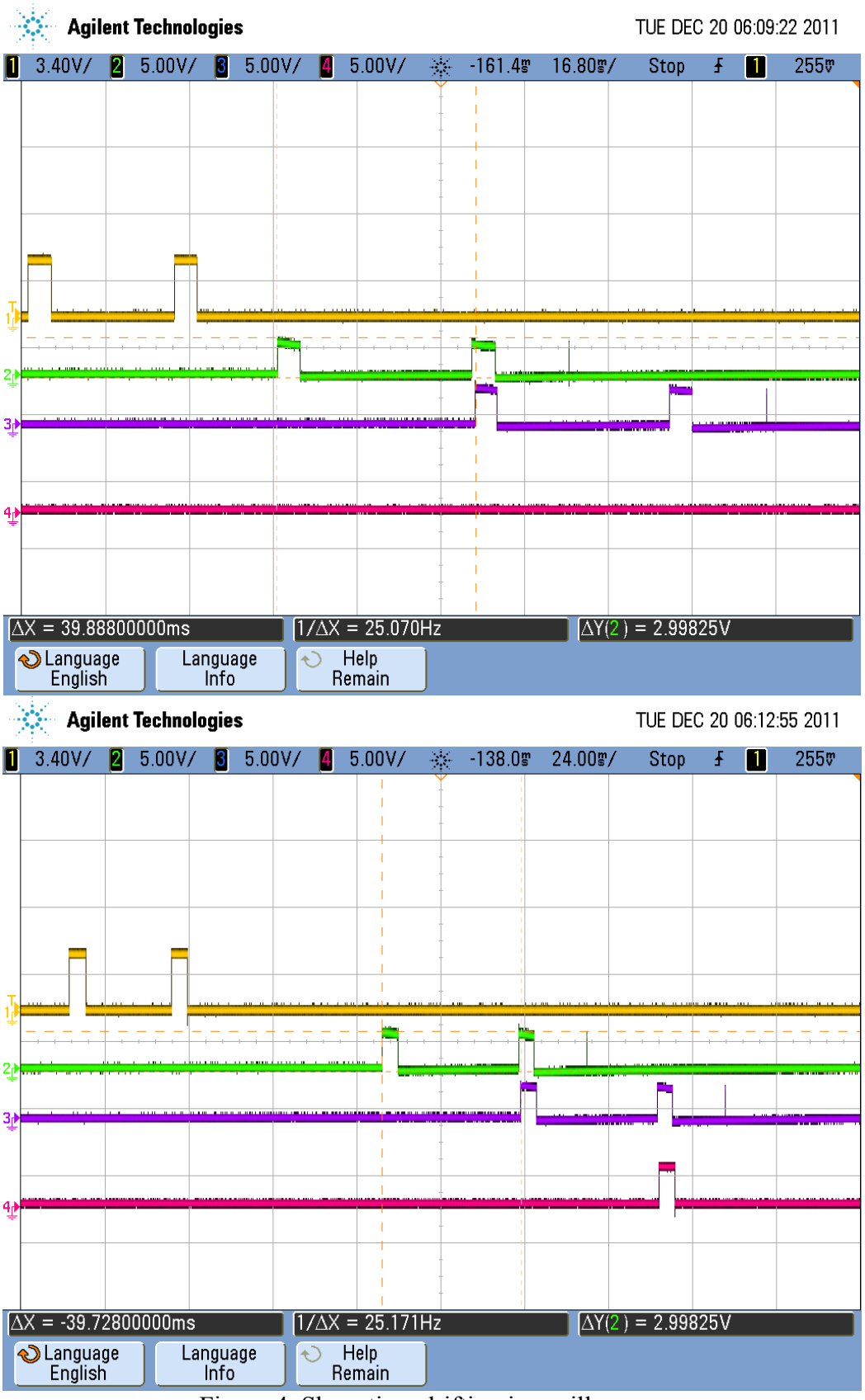


Figure 4. Show time drifting in oscilloscope

The result is below:

	From	To	Time Drift (ms)
1 hop	Gateway	Repeater 1	0.13
1 hop	Repeater 1	Repeater 2	0.01
1 hop	Repeater 2	Repeater 3	0.12
1 hop	Repeater 3	Repeater 4	0.27
1 hop	Repeater 4	Recipient	0.51
5 hops	Recipient	Gateway	0.18

In average, the time drift in one hop is 0.26ms. The length of one slot is 10ms, so time drifting is only 2.6% of the cycle period. As we can see from the result time drift is only depend on its previous node, which is good for network expanding.

2) Packet loss rate

Packet loss rate is another important parameter in network analyzing. In our network, we make the recipient send 200 packets and record on the gateway how many packets have been received. The results are shown below:

Test	Send	Receive
1	200	191
2	200	188
3	200	194
4	200	191
5	200	190
6	2000	1991
7	2000	1989

Packet loss happens at the beginning of the sending process, so that is why when we send more packets the packets lost do not increase. It shows that after the network finished synchronization the stability of the network is very good.

3) Energy Consumption

Every frame has 25 slots, and each node in average 2 slots transmitting and 1 slot listening. The rest slots are sleeping. Since every slot last 10ms, one frame is 250ms. Firefly node would consume 70uA /ms in idle state, 28.8 mA/ms in transmitting state and 27.4 mA/ms in listening state. So the whole energy consumption in one frame is

220 * 70uA + 20*28.8 mA + 10* 27.4mA= 861.8 mA*ms

Conclusion

The ISA100.11a protocol represents a comprehensive industrial wireless approach that serves a broad, facility-wide wireless network for both process and discrete manufacturing. In this project, we implement partly about the ISA100.11a protocol in data link layer. Based on the result, we could see ISA100.11a is a robust and stable protocol in packet transmission. Our next step is to implement channel hopping and dynamic network administration to make it even more robust to industry's harsh environment and more reliable.

Reference:
1. http://www.thewirelessplant.com/isa100-wireless-standards.html
2. http://www.isa.org//MSTemplate.cfm?MicrositeID=1134&CommitteeID=6891
3.http://www.isa.org/Template.cfm?Section=Standards2&template=Ecommerce/FileDisplay.cfm&ProductID=10766&file=ACF5AB9.pdf
4. STANDARD ISA-100.11a-2011, Wireless systems for industrial automation: Process control and related applications
5. Nano-RK Website: http://www.nanork.org/