# A Location Aware Application In WirelessHART

Xiuming Zhu[1], Aloysius K. Mok[1],Song Han[1], Jianping Song[1], Deji Chen[2],Mark Nixon[2]

[1]Department of Computer Sciences, the University of Texas at Austin, Austin TX, USA
[2]Emerson Process Management, 12301 Research Blvd., Bldg. III, Austin TX, USA

## ABSTRACT

WirelessHART is an emerging standard that promises to revolutionize the process control industry through wireless communication. This paper presents the design, implementation and evaluation of a location-aware application built upon WirelessHART™. The application is a software-based solution – no device modifications are required. Thus, it is applicable to any WirelessHART network. The basic idea is the following. Both the mobile device (a handheld device or a badge carried by a worker that needs to be located) and field devices (attached to the plant process) periodically send the health report of their neighbors to the network manager. The network manager analyzes these reports and then chooses the most trustworthy pairs of receive signal levels by comparison and by using deployment information that is already known. The network manager can also estimate the possible location area by extracting negative and positive signal coverage. To the best of our knowledge, this is the first attempt of implementing location-aware application on WirelessHART。

## 1. Introduction

In many large factories (eg, refineries, chemical plants and so on) it is often necessary to identify the location of workers and assets. Often in these large plants workers are faced with many different kinds of hazards. These hazards could be part of the plant, for example a chemical leak, or part of the environment, for example a tornado. In any case, it is very important for the control center to know how many people are exposed to the danger and where they are located in the plant. The solution of such problem becomes easier with the release of WirelessHART[1], the first open wireless communication for process management. Although there is no specification for location awareness in the current release of the WirelessHART standard, we find that it is still feasible for developing such applications.

In this paper, we design and implement a location-aware application on WirelessHART. It is completely software-based and needs no modifications of field devices. Thus, it is applicable for all WirelessHART networks. The key ideas behind locating mobile users includes of the following three techniques: comparison of two-way receive signal strength, extraction of positive signal area and negative signal area[2], and reuse of deployment map. First, both the mobile user through their handheld device or badge and the field devices send neighbor heath report to the network manager. The neighbor health reports contain device ID information and receive signal strength levels. As the worker moves through the plant the handheld and badge with the mobile user will detect the devices around them. Similarly the devices will be able to detect presence of the worker. In many cases there will be more than three devices in close proximity to the worker. As the devices and the worker's handheld or badge transfer information to the network manager. The network manager in turn makes use of this information to filter out the most trustable receive signal strength indication. The easiest way is to compare the health report from a field device with that from the handheld device. If the two matches, both can serve as good indications of distance. If not, the pair will not be considered. Besides, the network manager knows the deployment of all field devices. The actual distance between field devices can also serve as a good reference of receive signal strength indication. And if there are less than three field devices around the worker, the possible area can be still estimated by extracting positive signal coverage and negative signal coverage.

The left of the paper is organized as follows. Section 2 and 3 introduce location awareness in wireless sensor networks and WirelessHART standard. Section 4 describes the challenges and our design in detail. Implementation and experiment design will be shown in Section 5 followed by short conclusion and future work in Section 6.

## 2. Location Awareness in Wireless Sensor Networks

Localization is a hot topic in wireless sensor networks. While GPS is widely used for such purpose, it is costly and does not work in many cases. Normally, in order to localize one object, two kinds of information are necessary. One is the coordination information from anchor nodes. Another is distance indication information.

Presently, there are three kinds of distance indication. RSSI, TDOA and AOA.

RSSI (Received Signal Strength Indicator) makes use of signal strength decaying models to estimate the distance between the sender and receiver. However, when there is noise or obstruction, its accuracy will be affected. Paper [5] serves a good investigation of it.

TDOA (Time Difference of Arrival) makes use of signal propagation speed, which is more robust than the signal attenuation feature used by RSSI. However, since radio signal is too fast for most present crystal time chips, acoustic devices are employed in many localization systems. Also, TDOA needs time synchronization between the sender and receiver, which is very demanding in some cases.

AOA (Angle of Arrival) is a method for determining the direction of propagation of a radio-frequent wave incident on an antenna array. It needs more than one gear and computes the direction based on the time differences between gears.

Our solution is based on RSSI. This is mainly because we do not want to add extra devices onto field devices to maintain its extensibility.

Since the above three techniques are not panaceas for all cases, lots of work have been done for these years. And here, we would like to introduce several related papers.

Paper[3] utilizes two-way sensing to double check the distance indications from both ends, which is very similar to our solution. However, BeepBeep has no central management thus it may be affected by noise on one side. Sextant [2] extracts positive and negative information from anchor nodes and converts it into geographical constraints. This gives us a good idea for our work. Since the deployment of all field devices are already known, we can combine the two kinds of information together to improve accuracy.

## 3. WirelessHART

WirelessHART[1] is the first open wireless standard for the process control industry. Ever since it is released in September 2007, it quickly attracts the intention of many companies and customers. It is expected that products can be seen as early as the end of this year.

In order to make our paper self-contained, we only describe the parts of the WirelessHART specification that are related to this paper in this section.

Figure 1 shows a typical WirelessHART network. There are four kinds of devices in the network. The network manager is the control center for the whole network. It is responsible for managing all the devices in the network. In fact, the network manager is not a physical device but database-like software. The gateway is just like an AP that enables communications between host applications in plant network (including the network manager) and field devices. It is required that the network manager must have secure connection with the gateway. Field devices are sensors attached in all places of the plant. They are both a producer and consumer of messages. They are responsible for collecting the wanted information and transmitting back to plant network. And, they cannot communicate with each other directly but they are capable of routing packets to other devices in the network. The handheld device or a badge is a special device. The handheld is mainly used for configuring and monitoring field devices. The badge is used to provide the user with access to the plant and can be used by the WirelessHART network to identify the worker and their location in the plant. Both handhelds and badges can be carried by the worker.

Each WirelessHART network is identified with a unique network ID. Packets with different network ID cannot be deciphered and thus will be discarded.

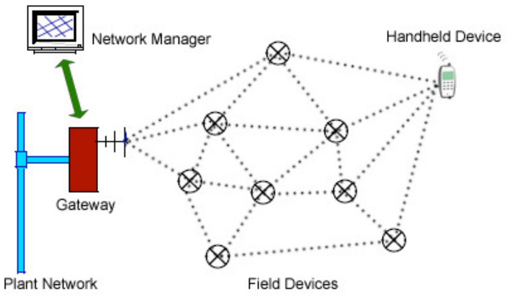
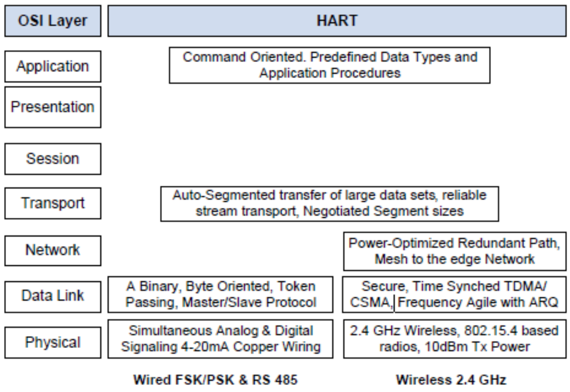


**Figure 1 A typical WirelessHART network**



| OSI Layer | HART | |
|---|---|---|
| Application | Command Oriented. Predefined Data Types and Application Procedures | |
| Presentation | | |
| Session | | |
| Transport | Auto-Segmented transfer of large data sets, reliable stream transport, Negotiated Segment sizes | |
| Network | | Power-Optimized Redundant Path, Mesh to the edge Network |
| Data Link | A Binary, Byte Oriented, Token Passing, Master/Slave Protocol | Secure, Time Synched TDMA/ CSMA, Frequency Agile with ARQ |
| Physical | Simultaneous Analog & Digital Signaling 4-20mA Copper Wiring | 2.4 GHz Wireless, 802.15.4 based radios, 10dBm Tx Power |
| | Wired FSK/PSK & RS 485 | Wireless 2.4 GHz |

**Figure 2 Architecture of HART Communication Protocol**

The architecture of the WirlessHART protocol stack is shown in Figure 2. There are five layers: physical layer, data link layer, network layer, transport layer and application layer. The physical layer utilizes IEEE 802.15.4 compatible DSSS radios. It defines radio characteristics, such as the signaling method, signal strength and device sensitivity. WirelessHART requires that the expected indoor communications distance should be 35 meters with 0 dBm transmitter and 75 meters with 10 dBm transmitter. Also, the transmitting power can be set if requested. Built upon the physical layer, WirelessHART defines a secure and reliable MAC protocol. The network layer supports mesh networking technology. The network manager is responsible for scheduling all communications in the network. On top of all this is the application layer. It is completely command-oriented. Commands provide services to configure the network and send back information to host applications.

Although WirelessHART does not currently specify how to provide location capabilities, it is possible for developing such applications. We will discuss this in the next section.

## 4. Challenges and Solution

As mentioned above, although WirelessHART defines many kinds of services at the application layer, it does not currently specify how to provide location aware support. As such, there is no way to locate the devices or workers by issuing standard commands. It is possible to add device specific hardware and commands to devices, however in this experiment extra gears and acoustic features will not be added. Hence, the only distance indication that we can rely on is the receive signal strength information provided by the physical layer.

In theory, a handheld device or badge can compute its location completely by itself through trilateration. This is mainly because field devices are usually intensively deployed and thus the handheld device can sense many devices around. However, such solution meets several problems in WirelessHART. First, for security issue, each two devices in Wiereless HART cannot talk to each other. That means, even the handheld device knows the distance from a field device by sensing the signal strength (the transmitting signal strength can be set by the network manager and thus it can be the same for all devices), it cannot directly inquire the location of the field device. Of course, it may request the location information from the network manager. However, WirelessHART has not defined any command about location information and as stated early, in this experiment we do not want to modify devices. Second, trilateration only needs three indications but the handheld devices may get more than three. Such redundancy does not help to improve the accuracy and may even cause confusion because the handheld or badge does not know which distance indication is more trustable than others. For the uncertainties of signal strength, it surely needs to filter away "bad" indications. As a workaround for this the handheld will need to select neighbor devices to use in its calculations from a list of possible candidates,

Another problem is dealing with physical obstructions and "blind spots". If there is no line-of-sight connection between two nodes, the distance indication may not reflect the actual information. Also, there may be "blind area" caused by obstacles.

Our solutions for these challenges are as follows:

a. Locating a handheld device or badge is done by the network manager. Since neighbor health report should be sent periodically to the network manager, the network manager can collect enough information for locating the handheld device. Also, redundancy will not confuse the network manager. Because while a field device can report the signal strength from the handheld device, the handheld device can do the same independently. Thus, the network manager can match the two reports. The double check will surely filter out some "bad" indications caused by random noise.

b. If less than three field devices can be sensed by the handheld device, the network manager will estimate the possible area by extracting the negative signal coverage and positive signal coverage. Also, previous location information can be inferred.

c. The network manager will make full use of the deployment information of field devices. It records the relative coordination of each device and also all the obstacles. Even the network manager can flag the "blind area" beforehand. Thus, the inter-node distance can also indicate the accuracy of signal strength. Also, even in the case that the handheld device enters a blind area, based on the previous location information and deployment information, the network manager can estimate the possible area.

## 5. Implementation and Experiment Design

We implement our solution on the network manager. As mentioned before, the network manager is not physical device but just a software application. Our solution services as an extra functionality for the network manager.

WirelessHART defines hundreds of commands in application layer. Here, we want to introduce those related to our work.

Command 780 reports neighbor health list to the network manager. This is the so-called neighbor health report. Command 780 is sent by a device periodically. However, the network manager can also ask a device to resend it. Table 1 and Table 2 show its format.

**Table 1 WirlessHART Command Format**

| 16- Bit command number | Length | Data |
|---|---|---|

**Table 2 Data Format of Command 780**

| Byte | Format | Description |
|---|---|---|
| 0 | Unsigned-8 | Neighbor table index |
| 1 | Unsigned-8 | Number of Neighbor entries read |
| 2 | Unsigned-8 | Total number of neighbors |
| 3-4 | Unsigned-16 | Nickname of neighbor |
| 5 | Bit-8 | Neighbor Flags |
| 6 | Signed-8 | Mean Receive Signal Level |
| 7-8 | Unsigned-16 | Packets transmitted to this neighbor |
| 9-10 | Unsigned-16 | Failed transmits |
| 11-12 | Unsigned-16 | Packets received from this neighbor |
| 13-… | | Number of entries based on response byte 1 |

of mostly four neighbors. If there are more than four neighbors, two packets have to be sent sequentially. Thus, the network manager may have to combine two sequential reports.

Command 787 reports specified neighbor signal levels. It is a solicited response. The network manager should first send command 787 with neighbor index to the field device and then, the field device can send back response telling the receive signal strength of the specified neighbor.

Command 797 enables the network manager to set the transmitting power of any device. It will be sent by the network manager and the receiver should be able to execute it successfully.

All the above commands are required in WirelessHART. Our solution will not add any self-defined command, although it is permitted by the standard. Hence, our implementation will be applicable for all WirelessHART networks.

In our experiment, the network manager is running on a laptop connected to a demo device, which serves as the gateway and is shown in Figure 3.

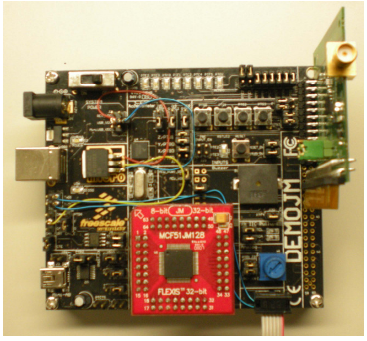


**Figure 3 A demo board of field device**

The demo device has a 48MHz 32-bit CodeFire V1 processor with a programmable 128K flash and 16KB RAM. A full WirelessHART protocol stack will run on it to enable it to perform like a field device.

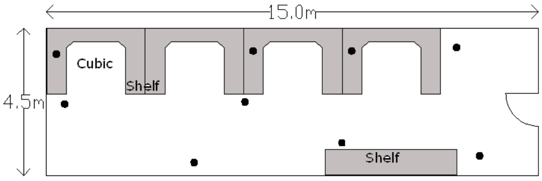


**Figure 4 Indoor Testbed**

Presently, we design three settings for our experiments.

*Case A : Indoor, quiet, no obstacle*. As shown in Figure 4, it is about 10m * 4.5 m. The shelf is made of iron, which can serve as an obstacle between devices. The black points are the possible locations (coordination are carefully measured and computed beforehand) for field devices. In this case, we arrange all the devices in a way that each two has a light-of-sight connection.

*Case B : Indoor , noisy, with obstacle.* In this case, we try to "hide" devices into iron shelves. And also, we try to create noise by a device with different network ID.

*Case C: Outdoor, parking area.* The parking area is surrounded by trees and buildings. It is near to a busy road.

Before each experiment, a thorough survey has to be done. The survey records all field devices' locations and all the obstacles between them. After configuring the network, the network manager will send out command 797 to set the same transmitting power for all devices, which makes it easier for localizing. Then, one person carries a handheld device and walks around. As mentioned above, if the network manager collects more than three distance indications, it will use comparison and prior deployment information to choose most trustable three. Also, the network manager can request the device to send response for command 787 if necessary. After enough information is collected, the network manager can triangulate the mobile device.

## 6. Conclusion and Future Work

In this paper, we implement a location aware application upon WirelessHART. Our implementation is purely software-based and thus can be applicable for all WirelessHART networks. It relies on receive signal strength to estimate the distance. And, the accuracy is improved by carefully use of three techniques: comparison of two-way sensing distance, extraction of negative and positive signal coverage, and full usage of deployment information. We believe that with the widespread of WirelessHART standard, our work will be more and more popular.

Future work will focus on the coding and experiments and enhancements to the WirelessHART standard to improve location-aware abilities

## 7. References

[1] HART Communication. http://www.hartcomm2.org

[2]Saikat Guha, Rohan Narayan Murty and Emin Gun Sirer. Sextant: A Unified Framework for Node and Event Localization in Sensor Networks. In Proc. of MobiHoc 2005, May 2005.

[3] Chunyi Peng, Guobin Shen, Yongguang Zhang, Yanlin Li and Kun Tan, "BeepBeep: A High Accuracy Acoustic Ranging System using COTS Mobile Devices", ACM SenSys, 2007

[4] J. Song, S. Han, A. K. Mok, D. Chen, M. Lucas, M. Nixon, and W. Pratt, WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control. Real-Time Technology and Applications Symposium, 2008.

[5] Eiman Elnahrawy, Xiaoyan Li, Richard Martin, The Limits of Localization Using Signal Strength: A Comparative Study, *IEEE SECON*, October 2004