2009 15th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications

A Location-determination Application in WirelessHART

Xiuming Zhu,Wei Dong,Aloysius K. Mok,
Song Han, Jianping Song
Department of Computer Sciences, the University of
Texas at Austin, Austin Texas, USA
e-mail:{xmzhu,wdong86,mok,shan,sjp}@cs.utexas.edu

Deji Chen,Mark Nixon
Emerson Process Management, 12301 Research Blvd.,
Bldg. III, Austin Texas, USA
e-mail: {Deji.Chen, Mark.Nixon}@emerson.com

***Abstract*—WirelessHART is an emerging wireless communication standard that is targeted at the real-time process control industry.An example application of wireless communication in an industrial process control plant is the location of field engineers. The capability to locate personnel is a safety critical issue in process control plants because of high risks posed by toxic chemicals and other hazards. This paper presents the design, implementation and evaluation of a location-aware application built upon WirelessHART. The aim of this application is to locate a mobile device (and thus the person carrying the device) via the deployed WirelessHART network. The application is a software-based – no device modifications are required. Consequently, it is applicable to any WirelessHART network. In this application, both the mobile device (a handheld device or a badge carried by a worker) and field devices (attached to the plant process) periodically send health reports of their neighbors to the network manager. The network manager analyzes these reports and discards the untrustworthy pairs through comparison. Next, the network manager feeds the average received signal indications to a well-trained radio propagation model to derive the location. To evaluation our solution, several preliminary experiments are carried out and the results are very promising, with a median error less than 4 meters, which is good enough for the industrial requirement. To the best of our knowledge, this is the first attempt to develop location-aware application in WirelessHART networks.**

Keywords-WirelessHART,Location Awareness,Received Signal Strength indication

I. INTRODUCATION

In many large factories (e.g. refineries, chemical plants) it is usually valuable to be able to track the location of workers and assets because of the hazardous conditions in industrial environment, for example, a chemical leak, 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 problems becomes easier with the release of WirelessHART[1], the first open wireless communication for process management.

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 to all WirelessHART networks. The key ideas behind locating mobile users are based on the following two techniques: the comparison of two-way received signal strengths and choosing best parameters of radio propagation model that uses training data collected beforehand. In this approach, the first step is to select a radio propagation model and then collect enough training data to train the model. Then, during the localization procedure, both the mobile user through their handheld device or badge and the field devices send “neighbor heath report” to the network manager. These neighbor health reports contain both device ID information and receive signal strength levels. As the worker moves around the plant, the mobile device will detect field devices around them. Similarly the field devices will be able to detect the presence of the worker. Frequently, there are 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 untrustworthy received signal strength indications. The easiest way to do this is to compare the health report from a field device with that from the handheld device. If the two match, both can serve as good measures of distance. If the difference is bigger than a certain threshold, the pair will not be considered. Since the network manager knows the deployment of all the field devices, it is easy for the network manager to locate the node accurately by using well-trained localization model.

The rest of the paper is organized as follows. Section 2 reviews existing well-known localization technologies in wireless sensor networks. Section 3 gives a brief description of the WirelessHART standard. Section 4 describes the challenges and discusses our design details. Our implementation will be introduced in Section 5 and extensive experiment results are shown in Section 6. We conclude the paper in Section 7 and discuss the future work.

II. RELATED WORK

Localization is a hot topic in wireless sensor network research. While GPS is widely used for such purpose, GPS is costly and does not work in some cases (e.g. indoor environment). Normally, in order to locate one object, two kinds of information are necessary. The first is the coordination information from the anchor nodes and the second is distance indication information.

Currently there are three types of distance indication information: RSSI, TDOA and AOA.

1533-2306/09 $25.00 © 2009 IEEE
DOI 10.1109/RTCSA.2009.36

RSSI (Received Signal Strength Indicator) makes use of signal strength decay models to estimate the distance between the sender and the receiver. However, its accuracy is affected by noise and by obstruction. Eiman [5] provides a good investigation of this issue.

Different from RSSI, TDOA (Time Difference of Arrival) makes use of the signal propagation speed which is more robust than the signal attenuation feature used by RSSI. However, since radio signal processing is too fast for most current crystal timer chips, acoustic devices are instead employed in many localization systems. Also, TDOA requires 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-frequency wave incident on an antenna array. This approach requires more than one antenna and computes the direction based on the time differences between antennas.

Since the above three techniques are not a panacea for all cases, lots of work has been pursued in the past on the localization problem.

In [5], Eiman points out that the accuracy of RSSI is expected to be about 10 ft under indoor environment. Because of the instabilities of signal strength indication, recent works focus on improving the accuracy by the use of technical tricks and probabilistic models. Shu[7] utilizes environmental features (e.g. temperature, humidity, noise) , and signal strength to recognize the location. Saikat[2] proposes an attractive algorithm to combine negative constraints (outside of sensing range) and positive constraints (inside sensing range) to determine the location even without enough anchor nodes. Jessica[8] derives a statistical model specially for measurement error and tries to minimize the error by a gradient-based algorithm. Juan[9] introduces a novel iterative method to reduce the least-square errors of localization. Since there is usually no analytical solution for these localization problems, iterative algorithms are widely adopted. However, because of its high computational complexity, it may not be suitable for sensors with low computational capability. Lei[10] utilizes prior location knowledge of sensor groups to estimate the node location based on a statistical model. Before sensors are deployed, the location of the sensor group has been pre-determined and coordinates have been stored in sensor's memories. However, during deployment, sensors may not be placed the right locations. Hence, a sensor should contact its neighbors to get the stored location information and then estimate its own coordination.

Our solution proposed for location determination applications is based on RSSI. We choose this approach because we do not want to add extra devices to the field devices in consideration of extensibility. We adopts a method similar to BeepBeep[3],which utilizes two-way sensing to double check the distance indications from both ends. With the help of the centralized management in WirelessHART, we can detect the error introduced by transient noise. Our approach makes use of *Floor Attenuation Factor* propagation model [6].We further tune this model by collecting and feeding training data to our model. This dramatically improves the accuracy of our location estimation.

III. WIRELESSHART

WirelessHART[1] is the first open wireless standard for the process control industry. Ever since it is released in September 2007, it has quickly drawn the attention of the industry. WirelessHART products have started emerging since the end of 2008.

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

Figure 1 shows a typical WirelessHART network. There are four types of devices in the network. The network manager is the control center for the whole network. It is responsible for managing all the resources and scheduling communications for all the devices in the network. Note that the network manager is not a physical device but a piece of database-like software. The gateway is just like an Access Point that enables communications between host applications in the plant network (including the network manager) and the field devices. The network manager must have secure connection with the gateway. The field devices are sensors installed all over the plant. They are both a producer and consumer of messages and are responsible for collecting the needed information and transmitting it back to the plant network. They cannot communicate with each other directly but they are capable of routing packets for other devices in the network. The handheld device or a badge (we call them handheld or mobile devices here) 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 it can be used by the WirelessHART network to identify the workers and their location in the plant. Both handhelds and badges can be carried by workers.

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

Figure 2 describes the architecture of the WirelessHART protocol stack according to the OSI 7-layer communication. 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 the radio characteristics such as the signaling method, signal strength and device sensitivity. WirelessHART requires that the minimum indoor communication distance should be 35 meters with a 0 dBm transmitter and 75 meters with a 10 dBm transmitter. Also, the transmitting power can be adjusted if necessary.

Built on top of the physical layer, WirelessHART defines a secure and reliable MAC protocol. Some notable features of the MAC layer include strict 10ms time slot, network wide time synchronization, channel hopping, channel blacklisting, and industry-standard AES-128 ciphers and keys. The network layer and transport layer on top of MAC layer support various network topologies, such as the star and mesh. The network layer uses source routing and graph routing to provide reliable end-to-end communication with the presence of interferences and obstacles. Also, the network layer utilizes session keys (allocated by the network manager) to encipher and decipher packages. Thus, one device cannot decipher packages from another device if it does not have the corresponding session key. The application layer is the topmost layer in the stack. It is completely command-oriented and hundreds of commands have already been defined in WirelessHART. It is also possible for customers to define their own commands for specific use. Host applications can issue commands to configure the network and collect information from the field network.

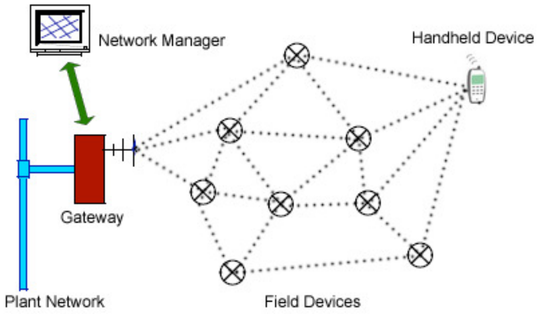
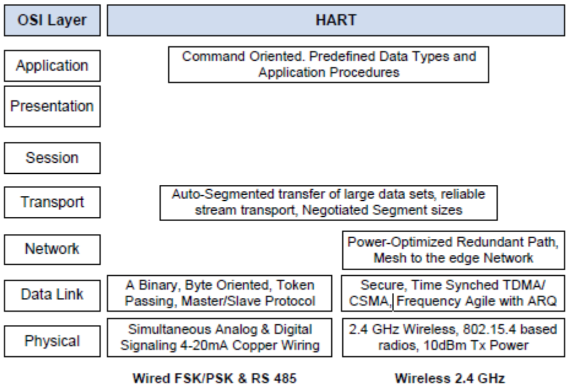


Figure 1. A Typical WirelessHART Network



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

Although WirelessHART currently does not explicitly support localization, it is possible to develop such applications as we shall demonstrate in the next section.

IV. METHODOLOGY

As mentioned in Section 3, although WirelessHART defines many kinds of services at the application layer, it does not specify how to provide location awareness support. As such, there is no way to locate the devices or workers by issuing the standard commands defined by WirelessHART.

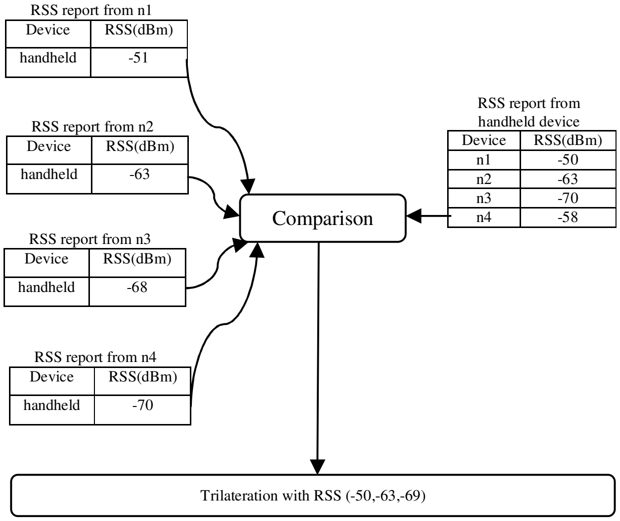
While it is possible to add device-specific hardware and commands to the devices, we choose not to add extra gears and acoustic features in our implementation. The only distance indication that we shall rely on is the received signal strength information provided by the physical layer.

In theory, a handheld device or badge can compute its location completely by itself through trilateration,as field devices are usually extensively deployed and the handheld device can sense many devices around it. However, such solution has several problems in WirelessHART. Firstly, for security concerns, no two devices in WirelessHART are permitted to talk directly to each other. So, even if the handheld device knows the distance from a field device by sensing the signal strength, it cannot directly inquire about the location of the field device. Of course, the handheld device may request the location information from the network manager. However, WirelessHART has not defined any command for location information and as stated earlier, we do not want to modify the devices in our solution. Secondly, the handheld device may receive more than enough distance indications. However, such redundancy may not help to improve the accuracy and may even cause confusion because the handheld or badge does not know which distance indication is untrustworthy. The uncertainty in signal strength surely must filter out the “bad” indications. The handheld will need to select the neighbor devices to use in its calculations from a list of possible candidates.

Our solutions meet these challenges as follows:

- In order to improve the precision of localization, we need to derive accurate parameters for radio propagation model. In our approach, a survey is taken to collect enough training data in the first step. Then, with the training data, we calculate the best parameters by use the least-square method.
- WirelesHART requires every device (including the handheld device) to send out Keep-alive messages to its neighbors every constant period (normally 30 seconds; however, it can be set by the network manager) and the receivers should send acknowledgements back. Through such bidirectional communications, each device can get the signal strength of the other end.
- Locating a handheld device or badge is done by the network manager. Since neighbor health reports are sent periodically (15 minutes by default, also, it can be set by the network manger) to the network manager, the network manager can collect enough information for locating the handheld device. In fact, the network manager can request the neighbor

health report actively. As stated before, redundancy will not confuse the network manager. This is 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. If the difference between two signal strength values is bigger than a certain threshold(*c*), the pair of reports will be discarded. Otherwise, the network manager will average the two and put it into trained propagation model. In this way, we can filter out some "bad" indications caused by random noise. Figure 3 shows an example of the procedure. Here, suppose the threshold is 5. The network manager first collects four signal strength reports about handheld from field devices *n1*, *n2, n3, n4,* respectively and one correspondent report from the handheld device. After comparison, it will discards the RSS reported related to *n4* because the difference is big than the threshold. Then, the average values of the left three pairs of signal strength will be put into trilateration model.


RSS report from n1

Device	RSS(dBm)
handheld	-51

RSS report from n2

Device	RSS(dBm)
handheld	-63

RSS report from n3

Device	RSS(dBm)
handheld	-68

RSS report from n4

Device	RSS(dBm)
handheld	-70

RSS report from handheld device

Device	RSS(dBm)
n1	-50
n2	-63
n3	-70
n4	-58

Figure 3. Filtering Untrustworthy RSS Reports

V. SYSTEM IMPLEMENTATION

We implement our approach on the network manager. Our solution services as an extra functionality for the network manager.

A. *Hardware platform*

We implement our solution on JM128[11] demo board. However, as stated above, our designed is platform-independent and can be applicable to other hardware platforms.

Figure 4 is the picture of JM128 demo board. It can server both a gateway and a device (either a field device or a handheld device). The features are listed as follows:

- Up to 50.33 MHz ColdFire [12] V1 core.
- Up to 128 KB of flash memory and up to 16K RAM with security circuit.
- Supports four low-power modes.
- On-board Logic Analyzer and Virtual Serial Port.
- USB device mode and host mode support with Mini-AB USB connector.
- 8 User LEDs and 5 Push Buttons.

Since JM128 demo board uses the same MCU as the EVBQE128 [13] toolkit and has larger memories, our hardware platform is powerful enough to meet the stringent timing requirements defined in the WirelessHART specification

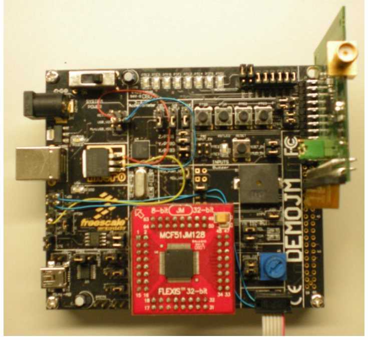


Figure 4. A JM128 Demo Board

B. *Related WirelessHART Commands*

In WirelessHART, all communications between the network manager and devices are represented as commands/responses (Figure 5 shows the command format) and WirelessHART has defined hundreds of commands. Here, we only introduce those commands 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 send it. It should be mentioned that due to the maximum length limit of a packet,one packet can only contain information at most four neighbors. If there are more than four neighbors, two packets have to be sent sequentially. Thus, the network manager should be able to combine two sequential reports. Table 1 shows the format of response to Command 780.

16- Bit command number	Length	Data

Figure 5. WirelessHART Command Format

Table 1. Format of Command 780 (Response)

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 tranmits
11-12	Unsigned-16	Packets received from this neighbor
13-…		Number of entries based on response byte 1

- Command 787 reports specified neighbor signal levels. It is a solicited response. That is, the network manager should first sends Command 787 request with neighbor index to the field device and then, the field device can send back response. Compared to command 780, the command response is much shorter because it only reports the signal levels of the specified neighbors. To save power, the network manager sends out this command instead of Command 780 to devices in our experiments.
- Command 797 enables the network manager to set the transmitting power of any device. The receiver should be able to execute this command successfully.
- Command 795 sets the timer interval of a specified device. Through this command, the network manager can set the frequencies of Keep-alive packages and neighbor health reports. Because of power issue, the interval should not be too short.

Normally, more than one Keep-alive message will be received between two consecutive neighbor health reports because the interval of two health reports is usually longer than that of Keep-alive messages. WirelessHART adopts an IIR filter[14] to calculate the average receive signal level as follows:

N_RSL= C_RSL- (RSL/RSLDamp)+(MeasuredRSL/RSLDamp)

Where the *C_RSL, N_RSL* is the current RSL and new RSL value respectively, *MeasuredRSL* is the RSL of the incoming packet; RSLDamp is the damping factor, which must be a power of 2 and defaults to 64.

Note that a device should set the *RSL* to zero after sending out a health report as history data is of no interest in this approach and may even cause counter-effects.

C. *Localization Model*

In this section, we will describe how to compute the coordination from raw RSS data. We first discuss the propagation model and then introduce trilateration model.

1) Radio Propagation Model

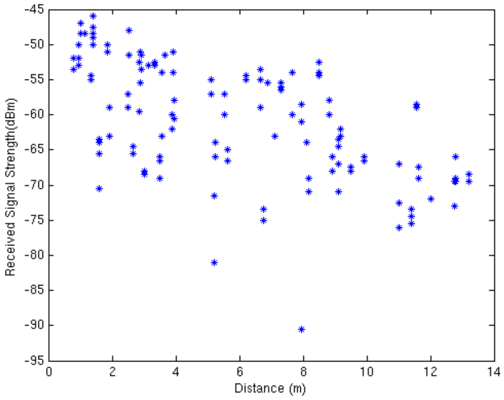


Figure 6. Actual Distances and Received Signal Strength

Figure 6 shows some raw data collected in one of the indoor experiments under noisy test scenario. It demonstrates the correlations between actual distances and received signal strength. From the figure, we can see even with the same distance, the received signal strength varies largely. This effect is mainly because there are different types and numbers of obstacles between transmitters and receivers.

In our solution, we follows the suggestion in RADAR[6] and chooses *Floor Attenuation Factor* propagation model for its simplicity and flexibility. The model is expressed as follows:

$$P(d)[dBm] = P(d_0)[dBm] - 10nlog\frac{d}{d_0} - nw * WAF \quad (1)$$

where n is the rate at which the path loss increases with distance, $P(d_0)$ is the signal power at certain reference distance d_0 and d is the distance, nw is number of obstructions and WAF is obstruction attenuation factor. Based on this formulate, it is not difficult to derive the formula for d:

$$d = 10\hat{}\left(\frac{P(d_0)[dBm]-P(d)[dBm]-nw*WAF}{10n}\right) \quad (2)$$

Except $P(d_0)$, every other parameter can be derived empirically. This provides more flexibility as we can change them for different environments. However, it is not realistic to get one value for all cases even within the same test scenario. This is because there are different numbers of obstacles between transmitters and receivers and also, obstacles are made of different materials.

In RADAR[6], these parameters are set empirically. However, we formulate it as an optimization problem. Before the localization, we can collect enough data about received signal strength and distance. These data can be used to train the model.

Thus, all we want now is to get a parameter tuple *(n,nw,WAF)* which makes $\sum_i (d_i - d'_i)^2$ smallest, where d_i, d'_i are the actual distance and estimated distance respectively. Since there is no analytical solution for the above problem, an iterative optimization method will be applied. We will detail this method in Section 6.

2) Trilateration

Trilateration is the method used to calculate a subject's location (in two dimensional space) using known locations of three reference points (field devices, in our case) and measured distance between the subject and each reference point. Theoretically, the coordinate could be computed by calculating the intersection point of three circles (shown in Figure 7). Unfortunately, due to the inaccurate RSI, the intersection among the three circles is usually not a point but an area and sometimes no intersection at all.

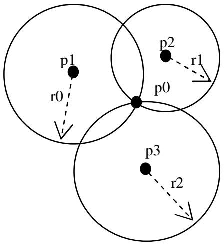


Figure 7. An Example of Trilateration

For this reason, instead of computing the intersection point directly, we calculate the point p_0 that minimizes $\sum_i^n (|p_0 - p_i| - r_i)^2$, where *n*, p_i, r_i are the number of anchor nodes, coordination of anchor node *i* and estimated distance between p_i and p_0, respectively. Same as above; there is no analytical solution for this problem and we shall apply the similar iterative optimization method.

D. Choosing Threshold(C)

As mentioned in Section 4, while the network manager tries to collect as many pairs of received signal strength as possible, it also has to discard the untrustworthy pairs according to a certain threshold (*C*). The threshold (*C*) also varies with the different environments. After the optimal parameters are derived in the training stage, we define the threshold as follows:

$$C = 10n\log(\Delta d) + nw * WAF$$

In all our experiments, Δd is 1.5m. That is, if the difference of two signal strength values will cause a distance error more than 1.5 meters, the pair will be discarded.

VI. EXPERIMENTS EVALUATION

We evaluate our location application under the following three environments.

- *Case A: Indoor, noisy, with obstacle*. As shown in Figure 4, it is an office with 15 m * 4.5 m area and several people working around. The shelf (shade area) is made of iron and wood and full of office utilities (computers, books, cups and so on), which can serve as obstacles between devices. The black points are the possible locations (coordinates are carefully measured and computed beforehand) for the field devices. The indoor temperature is constant at 26°C.

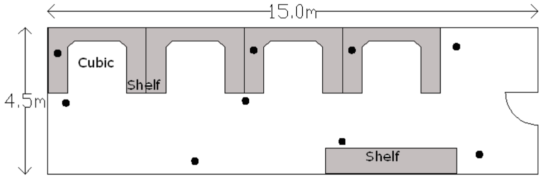


Figure 8. Indoor Testbed

- *Case B: Indoor, quiet, no obstacle.* In this case, we choose a public discussion area (about 4 m * 6 m, shown in Figure 9). In this experiment, we guarantee there is light-of-sight connection between any pair of devices.

Figure 9. A Picture of the Discussion Area

- *Case C: Outdoor, parking area.* The parking area (shown in Figure 10) is about 10m * 25m and is surrounded by trees and buildings. It is beside a busy road.

Figure 10. A Picture of the Parking Area

Before every evaluation starts, there is a training phase beforehand. For the former two cases, we do the training and testing nearly at the same time. However, for the outdoor case, we collect training data in the afternoon and then test our solution at night.

A. *Indoor Environment,noisy with obstacle*

As mentioned earlier, we first gather training data to derive the parameters in the model. Based on our measurements, for all scenarios, *P(d0)* is -50*dBM* where d_0 is one meter. For other parameters, we use the MatLab function *fminsearch* to compute them.

Table 2. Values for (*n,nw,WAF*) in Noisy Environment

n	*nw*	*WAF*
2.91	0	0

Table 2 shows the derived parameters in this scenario. It is a little surprising to see both *nw* and *WAF* are zero, although there are obstacles existing between transmitters and receivers. A possible explanation is that the *fminsearch* method balances the effect of obstacle attenuation (*WAF*) with optimized attenuation factor (*n*) .

Figure 11 illuminates the CDF of distance error and Table 3 gives out the maximum, minimum, average and median value of the distance errors.

Table 3. Max, Min, Average and Median Values (noisy)

	Max	Min	Average	Median
Error: (m)	11.72	0.39	4.56	3.96

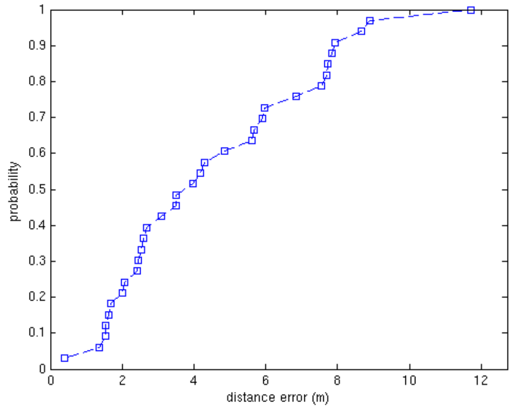


Figure 11. Distance Error CDF(noisy)

The result so far is very promising. In Figure 11, we can see the distance error is below 8 meters with more than 75% confidence. And in Table 3, the average distance error is less than 5 meters and the median error are less than 4 meters.

B. *Indoor Environment,quiet without obstacle*

As above, we display the optimal model values for this scenario in Table 4. CDF and statistical results are shown in Figure 12 and Table 5, respectively.

Table 4. Values for (*n,nw,WAF*) in Quiet Environment

n	*nw*	*WAF*
4.12	0	0

Similar as the first experiment, the *nw* and *WAF* are zero. This is consistent with real scenario because there are no obstacles.

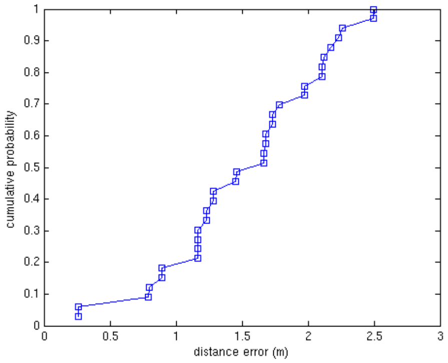


Figure 12. Distance Error CDF (quiet)

Table 5. Max, Min, Average and Median Values (quiet)

	Max	Min	Average	Median
Error: (m)	2.49	0.26	1.52	1.67

Compared to the noisy case, it is much better. The maximum distance error is less than 2.5 meters and the median value are less than 2 meters, which is very accurate.

The high accuracy in this experiment can be attributed to the fact the training data and the test data are under the same uniform environment. Compared with the noisy case, there are no obstacles between two devices and no noise around. Hence, the received signal strength can reflect the distance more accurately than the noisy environment.

C. *Outdoor,parking area*

In order to make our solution more general, we carry out experiments in an outdoor environment. Compared to indoor experiments, it is more difficult to collect information outside because of the power issue. At this point, there is no independent power source for our devices and we have to connect our devices with notebooks, which cannot last long just with batteries, either. So, we can only do a limited survey before localization procedure, which also is much shorter than indoor experiments

The optimal parameters are shown in Table 6.

Table 6. Values for (*n,nw,WAF*) in Outdoor Environment

n	*nw*	*WAF*
3.58	0	0

The CDF of distance error and statistical data are shown in Figure 13 and Table 7 respectively.

Compared to the quiet case, the distance errors are larger, which is a little counter-intuitive. The reason, we think, is that the training and testing for this experiment were done in different environments. We collected the training data in the afternoon and then came back to charge our notebooks. The testing phase was done at night. Humidity may vary with the temperature and thus affect the propagation of signal. However, the result is still exciting. The median is below 4 meters, which is quite accurate for industrial use.

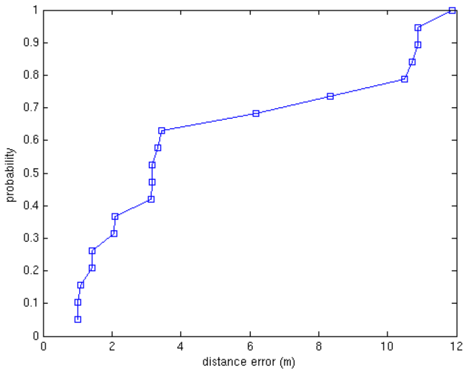


Figure 13. Distance Error CDF(outdoor)

Table 7. Max, Min, Average and Median Values (outdoor)

	Max	Min	Average	Median
Error: (m)	11.87	1.00	5.03	3.16

VII. DISCUSSION AND FUTURE WORK

In this paper, we have designed, implemented and evaluated a location deterministic method on WirelessHART. Our implementation is software-based and thus is applicable to all WirelessHART networks. It relies on the received signal strength to estimate distance. Accuracy is improved by the careful use of two techniques: comparison of two-way sensing distance and training parameters before localization.

Our solution is evaluated in various test scenarios and results are very promising. All median distance errors are below 4 meters, which is good enough for industrial use. With the widespread adoption of the WirelessHART standard, our work will be increasingly relevant and important in practice.

However, our solution is still limited and there is also lots of room for improvement. Firstly, our design is based on the fact that there are at least three field devices around, which is not always the case in real life. In such a case, there are several other solutions for estimating the location. Sextant [2] is one of them. Furthermore, since the handheld device is supposedly carried by a worker, historical record can be used for predication. Secondly, our localization algorithm is still preliminary. We just use MatLab *fminsearch* function (which uses the simplex searching method) to find the best coordination pair based on least-squares. Since our application can run on a powerful desktop computer, computational complexity is not a concern and we can employ more fanciful iterative algorithms. Moreover, since it involves training and testing, machine learning can be applied to it. Thirdly, we can find a better radio propagation model. As we can see in the experiments, the optimal values for *nw* and *WAF* are zero for all cases, which is a little counter-intuitive. Also, the results are not optimal. In another approach, we can make use of environmental features. Since all field devices are installed, we can make good use of the deployment map and filter out untrustworthy received signal indications (e.g. devices close to a noisy obstacle). Lastly, since WirelessHART is specially designed for industrial process control, the timing requirement is very stringent. Thus, it is possible to create a real-time location aware application based on our implementation, which would be very useful in motion tracking. And also, compared to industrial environment, our experimental settings are still preliminary and real field data are highly helpful to improve the applicability of our solution.

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.

[6] BAHL, P., AND PADMANABHAN, V. RADAR: An In- Building RF-based User Location and Tracking System. In Proc. IEEE INFOCOM (Tel-Aviv, Israel, Mar. 2000].

[7] Shu Chen, Yingying Chen, Wade Trappe, "Exploiting Environmental Properties for Wireless Localization," the Thirteenth Annual International Conference on Mobile Computing and Networking (MobiCom 2007), Montreal, Canada, September 2007.

[8] Jessica Feng, Lewis Girod, Miodrag Potkonjak, Location Discovery using Data-Driven Statistical Error Modeling, IEEE INFOCOM, April 2006)

[9] Juan Liu, Ying Zhang, Feng Zhao, Robust distributed node localization with error management, Proceedings of the seventh ACM international symposium on Mobile ad hoc networking and computing (MobiHOC, May 2006).

[10] Lei Fang; Wenliang Du; Peng Ning, A beacon-less location discovery scheme for wireless sensor networks, IEEE Infocm, March 2005.

[11] "DEMOJM Board", http://www.pemicro.com/fixed-links/demoqetoolkit.cfm.

[12] "Freescale Codefilre", www.freescale.com/codefire.