DOI: 10.48011/asba.v2i1.1172

Towards handover in IWN: a fast data collection technique

Tiago Rodrigo Cruz * **Gustavo Cainelli** * **Max Feldman** * **Ivan Muller** *

* *Universidade Federal do Rio Grande do Sul (UFRGS), Porto Alegre, Rio Grande do Sul, Brasil (e-mail: tiagorcruz1@gmail.com, gustavo.cainelli@gmail.com, max.feldman@ufrgs.br, ivan.muller@ufrgs.br).*

Abstract: The communication protocols used in industrial wireless networks are designed to meet requirements of security and reliability in communications. These requirements are guaranteed by techniques like message enciphering and radio frequency interference avoidance. The *Wireless*HART protocol was the first one developed specifically to meet the needs of industrial applications. *Wireless*HART networks use centralized control where one element, the network manager, is responsible for configuring, creating and maintaining the network. This feature increases reliability as management conflicts will not occur, but the route of communications between network manager and field devices may need several hops on the network due to the mesh topology employed in the protocol. Procedures such as joining new devices require the exchange of a series of commands with the network manager, which takes a large period of time to be executed. This paper presents a technique designed for mobile devices aiming the reduction of time needed for the publishing service. The proposed technique favors the use of mobile devices with strict time constraints under the range covered by the wireless network and precedes the study of an efficient handover process. The results present a time comparison between the standard and proposed data collection.

Keywords: *Wireless*HART protocol; join process; mobile devices; handover

1. INTRODUCTION

The increase in use of wireless communication technologies has enabled the development of Industrial Wireless Networks (IWN). A IWN is composed of various nodes which can sense and actuate in automation systems. These nodes are interconnected through radio communication links and their data may be processed to monitor and control the system Salam and Khan (2016). Industrial applications require robustness and reliability, as critical system decisions may depend on these sensors and actuators, therefore the communication protocol must provide such requirements.

*Wireless*HART (WH) was the first open wireless communication standard for IWN designed specifically for process monitoring and control applications HART Communication Foundation (2008a). It has been developed to meet requirements of reliability and safety of communications in industrial applications. Some other features of the standard are the IEEE 802.15.4 based physical layer where the characteristics of the radio are defined, a time synchronized data link layer that uses Time Division Multiple Access (TDMA) providing collision free and deterministic communications and the reliable end-to-end communication provided by the self-organized and self-healing techniques of the network layer. The application layer is command based forming the basis of the communications in the protocol where the command number determines the content of the message. Each command has a request and response form Chen et al. (2010).

The WH networks also use centralized control where one element, the Network Manager (NM), is responsible for configuring the network, scheduling communications between devices, managing message routes and optimizing the network Ovsthus et al. (2014). Thus, the devices connected to the network do not perform management tasks enabling the development of low price and low power consumption devices. In contrast, the network communications take more time to be executed when compared to a decentralized control, given that the path routed between network devices and the NM may take more than one hop.

The presence of mobility in IWN demands a frequent topology update which is not a characteristic of WH networks. Mobility can be classified in two groups: weak and strong Ali et al. (2005). Weak mobility is defined as regular network topology changes caused by node joins or failures. It occurs in networks with both types of nodes, mobile or static. Strong mobility, on the other hand, is described as the physical movement of the node. These movements can be subdivided in robotic (the node can move by itself) or parasitic (attached to a moving object) Silva et al. (2014).

⋆ This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001 and by the Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq).

In order to maintain connectivity of mobile devices as they move through the network it is necessary to update its communication links to avoid data loss and additional delays. This task is performed by a mechanism called handover, which is responsible to collect neighbor information and decide when it is necessary to change the route of the node Zinonos and Vassiliou (2014). The handover process can be classified in different criteria Ahmed and Alzahrani (2019); Thakur and Ganpati (2019). Some of them are presented below:

1.1 Soft and hard

In hard handovers a new connection is established when the previous attachment point is broken (break-before-make). Soft handovers, conversely, establish a new point of attachment before losing connection to the previous one (make-before-break).

1.2 Horizontal and vertical

In horizontal handovers the new point of attachment belongs to the same type of network, for example Wifi to Wifi or WH to WH. On the other hand, in vertical handovers the new connection is established to a node of a different type of network.

1.3 Downward and upward

In downward handovers the connection is changed from a network of large coverage area to a network of smaller coverage area while in upward handovers the connection is changed from a network of small coverage area to a a network of wider coverage area.

Some process in WH networks, like connection and disconnection of devices, are associated with large periods of time Müller (2012). These processes demand a series of commands exchange between field devices and NM before considering a device connected or disconnected from the network. This feature precludes the use of mobile devices which intermittently participate in the network. The network is not dynamic enough to support this kind of device because they may not have enough time to conclude the process to join the network and then request or publish information in the network.

A study has been done in the process of joining new devices in to a WH network. The objective of this work is to modify the join technique in order to provide a faster way to mobile devices to participate in the network. The results present a comparison of time between standard and modified techniques since the device tries to access the network until publishing its dynamic variable.

2. RELATED WORKS

The industrial wireless communication protocols are designed to overcome challenges in the propagation of radio frequency and guarantee QoS in the industrial environment. However, these protocols have been mainly designed for static nodes. Some techniques as joining and disconnecting devices, network discovering or provisioning devices are not optimized for networks with mobile nodes Montero et al. (2017). In order to handle mobile devices it is necessary to implement a mobility management mechanism to maintain these devices connected to the network or process its information as demanded by the application. In this context, studies propose the reduction of time of slow processes and topology control.

The impact of mobility on the performance of industrial wireless communications was analyzed in Montero et al. (2012). Two scenarios were considered, where mobile devices perform soft and hard handover processes. The performance metric is the channel utilization that can be used by a node to transmit data, which is defined as the ratio of slots assigned for data messages and the size of superframe. In general, the results show a degradation in the data transmission capability, which is a consequence of the inadequate management mechanisms to handle mobility in IWN. The negative effect is observed, in particular, when the space time a mobile device is under network coverage is small.

Two neighbor discovery protocols are presented and evaluated in Montero et al. (2017). The objective of the study is to remain mobile devices connected to the network as they move and reduce the time needed for their detection. The authors propose the utilization of advertise messages in the neighbor discovery process instead of the keep-alive used in WH. Since advertises are more frequently transmitted, the average time necessary to detect neighbors is reduced. It is also proposed an update of this protocol where each device only tries to receive advertises from its one- and two-hop neighbors. This approach aims to maximize the utilization of radio resources and minimize the energy consumption. Some metrics used in the evaluation are: probability that a mobile device remains connected while it moves around under the network coverage, discovery probability, average number of bytes consumed by the discovery process per superframe and energy consumption. The results show that the proposed protocols can detect neighbor devices up to 25 times faster when compared to WH, but with the expanse of a higher energy consumption.

Another approach to remain mobile devices connected in IWN is the handover process. The main steps of this process are link quality monitoring and the decision. In the first phase, the quality of the current connection link is measured through indicators that can sense its degradation. Some examples are: Received Signal Strength Indicator (RSSI), Signal to Noise Ratio (SNR), distance and Bit Error Rate (BER). In the second phase, it is decided wheter a handover process is needed and if so, a new communication link is selected based on the current resource availability and the network load Bhuvaneswari (2011); Zinonos and Vassiliou (2014). The performance evaluation of this technique is based on metrics such as rate of handover and duration of interruption.

In Müller et al. (2013) it is proposed the decentralization of the protocol where a special field device, called FDAP (Field Device - Access Point), with an incorporated coprocessor is developed. This device has local management capabilities to deal with intermittent devices. A session is created between a joining device and the FDAP where the join request is locally manage. The proposal includes changes in the WH stack and the creation of special com-

mands but maintaining the security and reliability of the protocol.

This paper presents an approach where the mobile device will not complete the join sequence, but it will store its dynamic variable at the gateway application in a faster way. This process is repeated every time the new device tries to join the network. Once it is available at the gateway, external application can access this data and process it.

3. METHODS

The approach selected aims to reduce the time new devices take to start the publish service by modifying the join sequence of the WH protocol. This section presents a description of the standard join sequence and the proposed technique. In both cases it is considered a network already formed and ready to receive new devices.

3.1 Standard join sequence

This sequence presents all the communications a new device must exchange with the NM to access and become integrated into the network. The key steps in the joining process include:

- Periodic advertise packets by network members. These packets allow the network to be identified;
- Monitoring by the new device to locate and synchronize with the network;
- Establishing a secure channel between the new device and the NM;
- Verifying the trustworthiness of the new device;
- Provisioning the device and allow it to integrate the network.

A simplified model of the join sequence specified by the WH protocol is presented in the sequence diagram in Fig. 1.

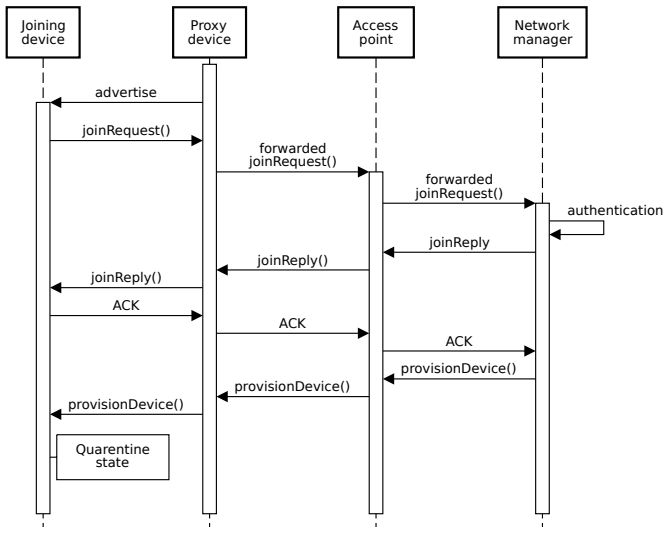

Figure 1. Standard join sequence diagram.

In detail, the main steps of the standard join sequence are described in the following paragraphs.

Initial device provisioning Before attempting to join the network, a new device must be configured with the join key and the network ID. The join key works as a password to allow the device to join the network and the network ID identifies the correct one as there may be more than one WH network in the area. These two configurations are written to the device using a standard HART-enable maintenance tool via the device's maintenance port. After this initial provision the device can be instructed to automatically attempt joining the network with command 771 (Force Join Mode). Another option is to manually place the device into join mode using a HART-enabled maintenance tool after the device is mounted in the process. In the join mode the device starts to listen to the network and gather information from neighbors.

Network advertise The devices that are already part of the network are responsible to periodically send advertisement packets, if previously configured to do so. These packets contain the necessary information for new devices to attempt joining the network. They are transmitted in the first available non-shared transmit link after the time set by the advertise interval timer lapses. In general, advertisements have lower priority than other traffics. The information in the advertise packet includes:

- Absolute Slot Number (ASN): a timestamp that represents the number of slots lapsed since the creation of the network.
- Join control: indicates the acceptance capacity of the advertising device to receive new devices. The lower this value the better.
- Channel map: indicates the available communication channels. The ASN, the channel map and the channel offset are used to select the communication channel of each transmission.
- Join links: lists all of the advertising device join links (transmit or receive) by superframe. The joining device is limited to use these links until it is provisioned by the NM with normal links.

Synchronization The new device listens the physical channels for a period defined by the channel search timer and then switches to the next channel and resume listening. This scanning period ends after elapsing of the active search timer or when a packet with the same network ID is received. The packet received is used to try to synchronize the new device's slot timing with that of the network. Slot timing statistics are evaluated with other packets captured from the network in order to confirm the synchronization. If it is not confirmed, the scanning is resumed.

Join request Once synchronized the new device requests access to the network by answering an advertisement packet. Based on information like signal strength and join priority previously collected from neighbors, the new device chooses the best candidate, which will be called proxy device. This device is used to forward packets between NM and the new device. This proxy route is used until the integration of the new device into the network. The join request is sent to the NM in a join link and contain three commands in response format:

- Command 0 (Read Unique Identifier) - Returns identity information about the field device.

- Command 20 (Read Long Tag) - Returns the name of the device.
- Command 787 (Report Neighbor Signal Levels) - Returns discovered neighbors not linked yet.

After sending the message, a response timer is started as part of the retry join request task. If this timer lapses another join request is generated to the next available advertise and the join retry counter is decremented. The process ends with an error if the retries are exhausted. As join requests are sent in shared slots, more than one device may try to answer it in the same time slot and channel resulting in collisions and retransmissions. Another example of using the retry task is when path failures occur and a device loses connectivity to neighbors.

Join response When the join request reaches the gateway, a join session is requested to the NM. This session allows the NM to receive and validate the join request and construct the join response, which contains the following commands:

- Command 961 (Write Network Key) - Write the network key to the joining device.
- Command 962 (Write Device Nickname Address) - Set a short address to the joining device.
- Command 963 (Write Session) - Establish a NM session to the joining device, so that the NM can manage it.

The join response commands are in request form and the new device must send the response back.

Integration into the network After receiving an acknowledge from the join response, the last step is to fully integrate the device into the network. At this point, its communications are still proxy routed. These final configuration includes: transfering the communication from join links to normal links, configuring time sources and updating communication tables. After that, the device is considered joined into the network and stays in a quarantine state where the device only communicates with the NM. In this state the device operates normally and starts the health report service where field devices periodically report their neighbor health (primarily the RSL value) to the NM. The NM uses this information to adjust the mesh network. The device leaves the quarantine state when a gateway session is created. Then, the device needs to obtain enough bandwidth to provide the publishing service of its process data. This session enables external applications (e.g. an automation controller) to gather information from field devices through the gateway HART Communication Foundation (2008b).

3.2 Proposed technique

Some modifications were made in the standard join sequence to reduce the time a mobile device needs to make its dynamic variables available in the gateway. The new sequence demands the same initial provisioning and period of synchronization. After choosing a proxy device, the join request is sent but with different commands. The join request is transmitted through the wireless network until the access point, then its application forwards it to the gateway which identifies there is a new device trying to communicate and request a join session to the new device. Then, before forwarding the message to the NM, the content is deciphered in the gateway. At this moment the commands are extracted and tested in order to identify whether it is a standard or a modified join request. In the standard case the message is forwarded and the join sequence normally continues, and if it is a modified join request the join sequence is ceased and the dynamic variables which were added in the request are stored in the gateway. An overview of the proposed join sequence is presented in Fig. 2. This cycle is repeated while the device is under network coverage and able to answer advertises. The time between each cycle depends on the value defined by the join retry time in the field device firmware.

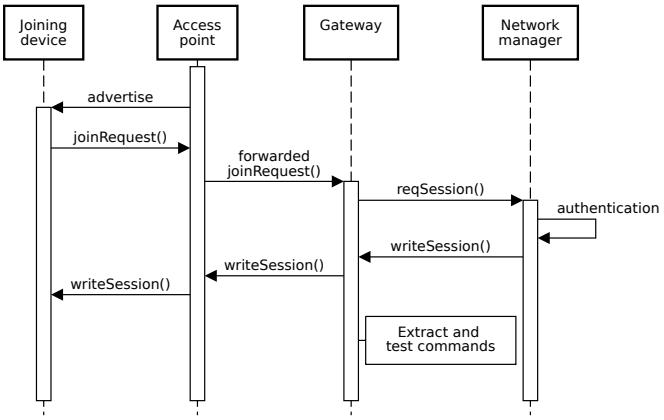

Figure 2. Modified join sequence diagram.

The firmware of the special device generates a different join request. The command 787 (Report Neighbor Signal Levels) was removed because it is important only for the NM but the message will not reach the NM. The device information provided by commands 0 (Read Unique Identifier) and 20 (Read Long Tag) are maintained. The command 1 (Read Primary Variable) was added in the join request to represent the process data the new device wants to publish in the network.

4. MATERIALS

The implementation of the proposal technique was enabled due to the equipment available in the laboratory where the tests were conducted. It consists of a complete setup to create a WH network. Differently from commercial wireless gateways, the system used provides access to the applications of the NM, gateway and access point host. Thus, it is possible to implement modifications in the protocol and create a network to compare the modified join procedure against the standard one. An overview of the system is presented in Fig. 3.

Data from commercial wireless gateways were also used in order to compare the join sequence time in the standard case. A case study, performed in Müller (2012), presents data from two wireless gateways: an Emerson Rosemount 1420 and a Nives Versa Router 810. These data were collected using a wireless sniffer, together with some tools developed for the work.

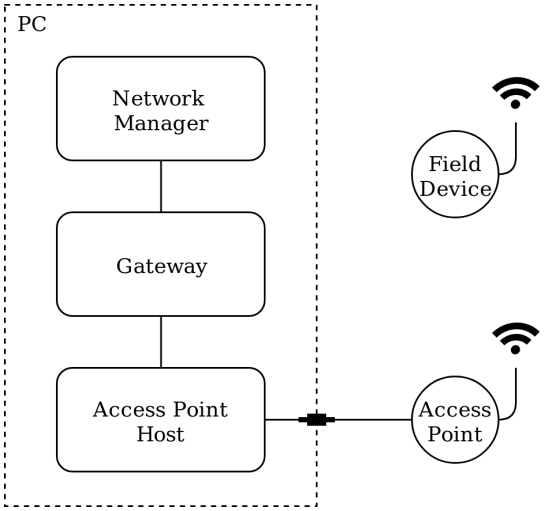

Figure 3. *Wireless*HART network.

5. EXPERIMENT AND RESULTS

In order to evaluate the difference in time between the standard and the modified technique, an experiment was designed. The experimental setup is composed by: three radios Muller et al. (2010), where two are designated as field devices with different firmware (standard and modified) and the other one as the access point; one computer to run the applications of the NM, gateway and access point host; and a USB serial converter to connect the access point to its host application. The measurements were acquired using timestamps with millisecond precision in the gateway application logs. The period measured starts when the radio first answers an advertise, therefore the searching and synchronization period are not considered. These previous steps might affect the join time but this approach focus in the impact of the changes applied. In the standard situation the measurement period ends when a gateway session is created to the joining device. At this point its dynamic variables can be accessed by external applications through the gateway. In the modified case, the measurement ends when the join request is deciphered in the gateway and the commands are extracted to obtain the primary variable (command 0).

In order to conduct a reliable analysis, a prospective study was done to identify the right amount of data (sample size). Using information from a preliminary study and considering a statistical power of 90%, the sample size equals to 20. The experiment was performed in a random run order following the guidelines of the experimental methodology Montgomery (2012).

All the samples were collected in the same day. The field devices were placed next to the access point and no physical interference was considered. The data were analyzed with computer assistance of the statistical and data analysis software Minitab. A One-Way ANOVA (analysis of variance) was performed using a significance level $\alpha = 0.05$ and the results are presented in Table 1.

As ***P*-Value** is lesser than the significance level (α) it is possible to conclude with 95% of confidence that the technique significantly affects the response variable (time). The average results for each technique are shown in Table 2 and as can be seen the proposed technique takes, in average, almost eight seconds less to have its dynamic variables available in the network.

Table 1. Analysis of variance.

Source of Variation	**Degrees of Freedom**	**Sum of Squares**	**Mean Square**	***F*-Value**	***P*-Value**
Technique	1	635.387	635.387	23173.790	0.000
Error	38	1.042	0.027	-	-
Total	39	636.429	-	-	-

Table 2. Results.

Technique	**Average time [s]**	**Standard deviation [s]**
Standard	9.998	0.224
Modified	2.027	0.068

The data of this experiment is also presented in a comparison with commercial wireless gateways in Table 3. The period analyzed in each case represents the time needed to perform the same process, starting from the answer of an advertisement to the joined state.

Table 3. Gateway comparison - Standard join sequence

Wireless gateway	**Average time [s]**
Proprietary	9.998
Emerson Rosemount 1420	15.63
Nives Versa 810	7.02

6. CONCLUSION

A modified join technique for WH networks was proposed in this paper in view of the large time needed for new devices to participate in the network. In consequence of this time, mobile devices with strict time in the range of the network coverage, may not have enough time to conclude the joining procedure. To achieve the results some steps of the join sequence were removed and consequently affecting the security of the communications. The messages containing the dynamic variables that before were enciphered using a secret key, now use the join key which is the initial security level. The results of the experiment show the proposed technique is approximately five times faster than the standard one. The difference could be even higher given that in the standard case the device would need to request communication resources to the NM in order to provide its publish service while in the modified case the join links are used for this purpose. The proposed join technique creates a more suitable way for mobile devices to connect and participate in *WirelessHART* networks.

As future work it is intended to increase the security of the method by characterizing modified devices in the network. Thus, when the automation system identifies a special device it might decide accepting or not the dynamic variables based on its critical influence in the system. The realization of this study starts including mobility support to the WH protocol and will be used as basis for the implementation of a handover process aiming the

possibility to have mobile devices efficiently working in these kind of networks.

REFERENCES

Ahmed, A.A. and Alzahrani, A.A. (2019). A comprehensive survey on handover management for vehicular ad hoc network based on 5g mobile networks technology. *Transactions on Emerging Telecommunications Technologies*, 30(3), e3546.

Ali, M., Suleman, T., and Uzmi, Z.A. (2005). Mmac: A mobility-adaptive, collision-free mac protocol for wireless sensor networks. In *PCCC 2005. 24th IEEE International Performance, Computing, and Communications Conference, 2005.*, 401–407. IEEE.

Bhuvaneswari, A. (2011). Survey on handoff techniques. *Journal of Global Research in Computer Science*, 2(6), 140–144.

Chen, D., Nixon, M., and Mok, A. (2010). *WirelessHART: real-time mesh network for industrial automation*. Springer.

HART Communication Foundation (2008a). Hart protocol specifications.

HART Communication Foundation (2008b). Network management specification.

Montero, S., Gozalvez, J., and Sepulcre, M. (2017). Neighbor discovery for industrial wireless sensor networks with mobile nodes. *Computer Communications*, 111, 41–55.

Montero, S., Gozalvez, J., Sepulcre, M., and Prieto, G. (2012). Impact of mobility on the management and performance of wirelesshart industrial communications. In *Proceedings of 2012 IEEE 17th International Conference on Emerging Technologies & Factory Automation (ETFA 2012)*, 1–4. IEEE.

Montgomery, D.C. (2012). *Design and analysis of experiments*. John wiley & sons.

Müller, I. (2012). *Gerenciamento descentralizado de redes sem fio industriais segundo o padrão WirelessHART*. Ph.D. thesis, UFRGS.

Muller, I., Pereira, C.E., Netto, J.C., Fabris, E.E., and Allgayer, R. (2010). Development of a wirelesshart compatible field device. In *2010 IEEE Instrumentation & Measurement Technology Conference Proceedings*, 1430–1434. IEEE.

Müller, I., Winter, J.M., Pereira, C.E., and Netto, J.C. (2013). Wirelesshart fast collect: a decentralized approach for intermittent field devices. In *2013 11th IEEE International Conference on Industrial Informatics (INDIN)*, 254–259. IEEE.

Ovsthus, K., Kristensen, L.M., et al. (2014). An industrial perspective on wireless sensor networks—a survey of requirements, protocols, and challenges. *IEEE communications surveys & tutorials*, 16(3), 1391–1412.

Salam, H.A. and Khan, B.M. (2016). Iwsn-standards, challenges and future. *IEEE Potentials*, 35(2), 9–16.

Silva, R., Silva, J.S., and Boavida, F. (2014). Mobility in wireless sensor networks–survey and proposal. *Computer Communications*, 52, 1–20.

Thakur, P. and Ganpati, A. (2019). Survey on handover techniques in vanets.

Zinonos, Z. and Vassiliou, V. (2014). Handoff algorithms for industrial mobile wireless sensor networks. In *2014 6th International Conference on New Technologies, Mobility and Security (NTMS)*, 1–6. IEEE.