Performance Evaluation of WirelessHART for Factory Automation

Stig Petersen
SINTEF ICT
Trondheim, Norway
stig.petersen@sintef.no

Simon Carlsen
StatoilHydro ASA
Harstad, Norway
scar@statoilhydro.com

Abstract

The WirelessHART specification has given the industry access to their first open standard specifically aimed at wireless instrumentation for factory automation. For WirelessHART to be a viable solution for the process and automation industry, it has to provide a robust and reliable alternative to today's wired networks.

This paper presents the results of a performance evaluation of a WirelessHART network deployed in an industrial environment. It also presents a performance analysis and deployment considerations for IEEE 802.11g coexistence.

The conclusion of the paper is that the WirelessHART network is capable of providing data reliability of 100% when operating in an industrial environment, and when coexisting with three IEEE 802.11g networks.

1. Introduction

Recent advances in wireless communication technologies have enabled the development of low-cost, low-power wireless solutions capable of robust and reliable communication [1]. International standards such as the IEEE 802.11 for Wireless Local Area Networks [2] and the IEEE 802.15.4 for Low-Rate Wireless Personal Area Networks [3] have enabled applications within the fields of wireless computer networks and wireless sensor networks (WSN).

Despite the rapid development and deployment of wireless technology in consumer, office and public space applications, the adoption of wireless solutions in factory and process automation industries is still in its initial phase. IEEE 802.11 wireless access points which enable field workers equipped with PDAs (Personal Digital Assistants) or tablet PCs to wirelessly access plant and enterprise networks, are becoming more commonplace as the industry starts to realize its potential benefits [4][5]. For WSNs on the other hand, the lack of an open, international standard which fulfils industrial requirements has been the major reason for the lack of industrial adoption [6][7]. However, with the release of the HART Field Communication Specification Revision 7.0 in September 2007 [8], the factory and process automation industries have access to the first open standard, referred to as WirelessHART, specifically aimed at wireless instrumentation for the factory automation industry. WirelessHART offers a self-configuring, self-healing multi-hop mesh network with robust and secure communication links, promising interoperable devices capable of delivering sensor data even in the most hostile and remote areas of a process plant.

In this paper, the results from a performance evaluation test of a WirelessHART network are presented. The network, consisting of nine sensors and one gateway, was deployed in a semi-industrial laboratory environment, presenting a challenging RF (Radio-Frequency) environment in the shape of large metal structures, pipes with flowing liquids and electrical machinery. The test network was also subject to interference from IEEE 802.11g networks, as well as denial-of-service attacks from a chirp jammer.

The organization of this paper is as follows: section 2 gives an introduction to the WirelessHART technology, section 3 discusses coexistence issues with WirelessHART and IEEE 802.11, section 4 presents the results from the laboratory experiments, section 5 discusses deployment considerations for WirelessHART and WLAN coexistence, and section 6 concludes the paper.

2. The WirelessHART Specification

This section provides an overview of the WirelessHART specification.

2.1. Physical Layer

The WirelessHART Physical Layer (PHY) is based on the IEEE 802.15.4 PHY. Unlike IEEE 802.15.4, WirelessHART only defines operation in the 2.4 GHz band, employing Direct Sequence Spread Spectrum (DSSS) and Offset-Quadrature Phase Shift Keying (O-QPSK) modulation. This allows for a bit rate of 250 kbit/s. WirelessHART uses only 15 of the 16 channels defined by the IEEE 802.15.4; which is channel

number 11 to 25. Channel 26 is not included in the WirelessHART specification since it, due to national regulations, is not legal to use in some countries. The WirelessHART channels each utilize a bandwidth of 3 MHz and they are uniformly distributed 5 MHz apart throughout the frequency band to ensure non-overlapping communication.

At the physical layer (PHY), the WirelessHART packet format is identical to the PHY Protocol Data Unit (PPDU) of the IEEE 802.15.4. It consists of a preamble (4 bytes), a delimiter (1 byte), the length of the PPDU (1 byte) and a variable length payload. Data structures from the higher protocol layers are encapsulated in the PHY payload.

2.2. Logical Link Control Layer

The logical link control layer defines the format of the Data-Link packet (DLPDU). It consists of 1 byte set to "0x41", a 1 byte address specifier, a 1 byte sequence number, a 2 byte Network ID, a 2 or 8 byte destination and source address, a 1 byte DLPDU specifier, a 1 byte keyed Message Integrity Code (MIC), a 2 byte Cyclic Redundancy Check (CRC) and a variable length DLL Payload. The contents of the DLL Payload are defined by the DLPDU packet type. The structure of the PPDU and DLPDU packets are illustrated in Figure 1.

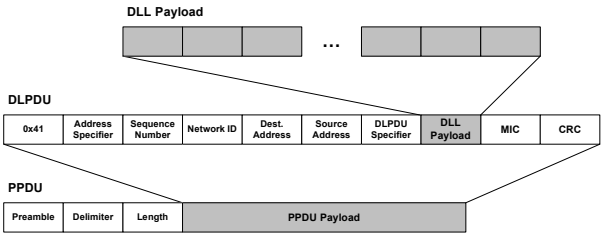

Figure 1. WirelessHART Packet Structures

2.3. Medium Access Control Layer

Time Division Multiple Access (TDMA) is used as the channel access in WirelessHART. TDMA allows for communication between devices to occur in distinct timeslots, where a series of timeslots form a superframe, as illustrated in Figure 2. All WirelessHART devices must support multiple superframes. One superframe is always enabled, while additional superframes can be enabled and disabled throughout the network lifetime. The number of timeslots in a superframe is fixed, and the superframes are repeated continuously throughout the network lifetime. To ensure contention free access to the wireless medium, two devices are assigned to a given timeslot, one as the source and the other as the destination.

WirelessHART also employs channel hopping, alternating which of the 15 available channels are used in the communication between two devices. Creating links on the same timeslot, but with different channel offset, allows for the simultaneous operation of up to 15 communication links in the network.

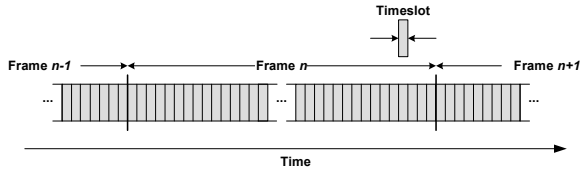

Figure 2. TDMA Timeslots

2.3.1. Slot timing

Within a WirelessHART timeslot, there is room for the transmission of a DLPDU from the source, followed by the transmission of an ACK DLPDU from the destination. The ACK DLPDU will only be transmitted upon the destination's successful reception and validation of the DLPDU. If the source does not successfully receive and validate the ACK DLPDU from the destination, the data transmission is regarded as a failure. If the transmission fails, the DLPDU will be retransmitted by the source in the next available timeslot. If repetitive failures occur on a specific link, alternative routes in the network will be considered, based on the routing tables of the source device.

When the source is transmitting a DLPDU, the destination is listening (RX), and when the destination is transmitting an ACK DLPDU, the source is listening (RX), as illustrated in Figure 3.

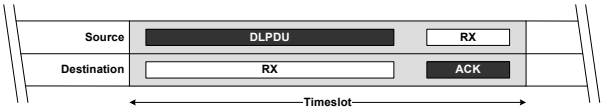

Figure 3. WirelessHART Slot Timing

3. WirelessHART and IEEE 802.11 coexistence

For the adoption of WirelessHART in industrial plants and facilities to become a success, it is imperative that the technology is able to friendly coexist with other wireless devices and systems operating in the same portion of the frequency spectrum. As the 2.4 GHz band is open for license free use, the local RF environment is likely to be crowded with devices transmitting in this band. Wireless Local Area Networks (WLANs) based on the IEEE 802.11 specification, cordless telephones and Bluetooth devices are good examples of 'noise sources' as seen from the perspective of WirelessHART. Additionally, in an industrial setting one must expect broadband RF

noise emitting from machinery, electric and electronic devices in the area.

The widespread deployment of WLANs has fully reached the process plant, and when introducing wireless sensor networks in the plant, one must expect that the environment is under influence from a nearby WLAN. The ISM band spans from 2.400 MHz to 2.485 MHz, with slight variations from country to country. A total of 14 WLAN channels are defined, each with a bandwidth of 22 MHz. However, due to national rules and regulations, channel 14 (at 2.484 MHz) is only available in a select few countries (Japan, Spain), and in addition channels 12 and 13 are prohibited in North America and some Central and South American countries.

The centre frequency of the WLAN channels are spaced only 5 MHz apart, which means that neighboring channels actually overlap in frequency since the channel bandwidth is 22 MHz. In a typical corporate WLAN installation, it is desirable to have a dense access point distribution to ensure maximum utilization of the frequency band, and to prevent possible network congestion due to a user overload on a single access point. However, with the overlapping nature of the WLAN channels, the only channel configuration which allows for non-overlapping communication for three networks is using channels 1, 6 and 11.

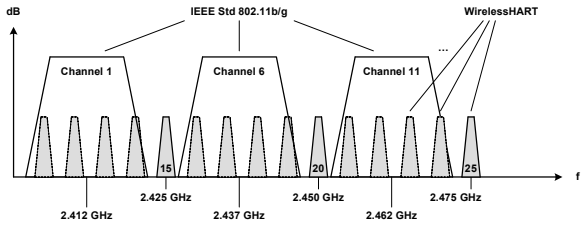

Figure 4. WirelessHART and IEEE 802.11 channels in the 2.4 GHz ISM band

Figure 4 illustrates the distribution of the 15 WirelessHART channels and the three non-overlapping WLAN channels in the 2.4 GHz band. With this configuration, WirelessHART channels 15, 20 and 25 are positioned in between the three WLAN channels, which will limit the WLAN interference on WirelessHART communication in these channels. However, as WirelessHART employs non-adaptive frequency hopping where each link in a network switches randomly between the 15 available channels, 80% of the WirelessHART communication (12 channels out of 15) will suffer from direct interference from the WLAN networks. The coexistence with WLAN should therefore have a degrading effect on the WirelessHART network performance in the shape of increased packet loss [9]. This is further investigated in the laboratory experiments in section 4.2.

4. Laboratory Experiments

The purpose of the laboratory experiments was to evaluate the performance of a WirelessHART network when deployed in an industrial environment. A laboratory was chosen instead of a live production facility in order to have complete control of the environment, both regarding work activities and the operation of other wireless devices utilizing the same frequency band.

The research laboratory contains full-scale replicas of various process equipment and prototype rigs, in addition to large and dense metal structures, flowing liquids and gases, and electrical motors, pumps and valves.

The WirelessHART network consisted of nine temperature and pressure sensors and one gateway. The location of the sensor nodes where chosen based on achieving both good spatial distribution and to provide each sensor with a challenging RF environment in regards close proximity to metal structures and electrical machinery, and limiting line-of-sight to the other sensors and the gateway. The physical location of the devices is presented in Figure 5.

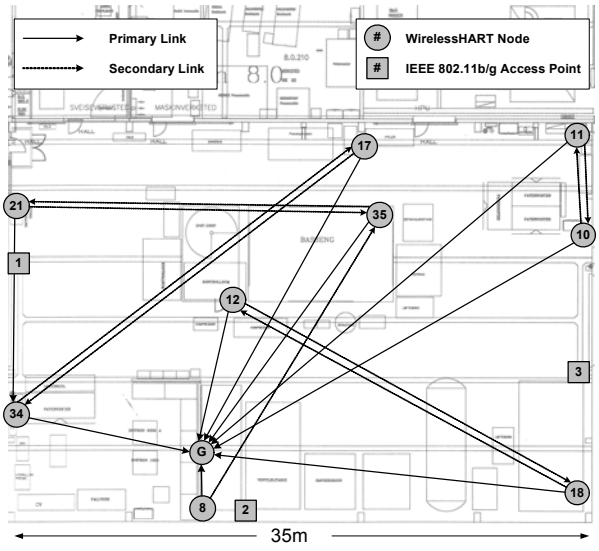

Figure 5. Laboratory installation

The scope of the tests were to examine the network performance under three different ambient conditions; normal operation with no interference, coexistence with IEEE 802.11g networks, and attacks from a 2.4 GHz chirp jamming device. The monitored network parameters were packet loss, reliability and latency. The *packet loss* is the number of data packets in the network which fail to reach their destination, measured on a link to link basis. The *reliability* is the measure on how many packets reach their final destination. In a multi-hop mesh network this can include several hops.

Note that with retransmissions of lost packets and redundant paths to combat broken links, the network reliability can be high even with high packet loss. The *latency* is a measure on how long it takes a packet to reach its destination. This can also include several hops.

The WirelessHART sensor nodes were configured to provide sensor data with a periodic one minute update rate, and the network was configured to operate with one superframe consisting of 150 timeslots, giving a superframe length of 1500 ms.

4.1. Network Performance

The general network performance evaluation was conducted over a period of 120 hours. There were no other wireless devices operating in the same frequency band in the area during the test.

The average network packet loss and average latency of the network is presented in Figure 6 and Figure 7 respectively. The reliability of the network remained at 100 % for the entire test period, and it is therefore not presented in the figures.

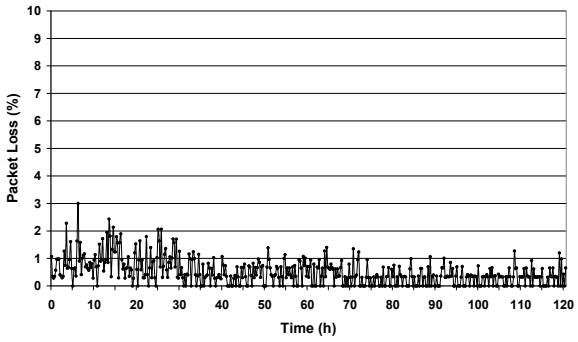

Figure 6. Network Performance – Packet Loss

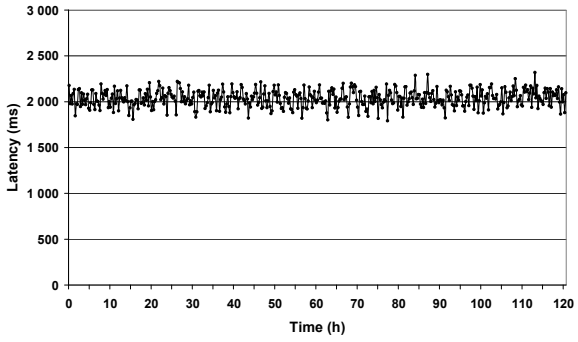

Figure 7. Network Performance - Latency

The average network packet loss was below 1% for most of the test period. The slightly higher packet loss which is experienced in the first 30 hours of the test coincides with periods of work-related activity in the laboratory. Both people and small vehicles were present in the area, creating obstructions and thereby attenuation of the wireless signals – which leads to reduced link quality and increased packet loss. In the last 90 hours of the test period there was no activity in the laboratory. The latency of the network stabilized at around 2000 ms for the entire test period. This relatively high latency is related to the size of the network superframe (150 slots of 10 ms), which means that any given link between two devices in the network can only communicate once every 1500 ms. With retransmissions of lost packets and a multi-hop mesh network topology where some of the sensor nodes use other neighbouring sensor nodes as routers, a latency of this magnitude is to be expected.

4.2. IEEE 802.11g coexistence

The purpose of the IEEE 802.11g coexistence test was to examine how a WirelessHART network is affected when IEEE 802.11g WLAN networks is operating in the same area. Three IEEE 802.11g access points (APs), configured to operate on the three non-overlapping channels 1, 6 and 11 (illustrated in Figure 4), where deployed in the same area as the WirelessHART network. The locations of the APs in relation to the WirelessHART devices are shown in Figure 5.

Every AP in a WLAN infrastructure periodically broadcasts beacon frames. They are used for synchronization of the network, and additionally contain information about capability and regulatory information for the network. A beacon uses *legacy* format, i.e. it must be transmitted using the mandatory CSMA/CA algorithm at the basic bandwidth of 1 Mbps which is compatible with all IEEE 802.11 protocols. The *beacon interval* is defined as the time between two subsequent beacon transmissions.

In an idle network, the transmissions of beacons correspond exactly to the specified beacon interval. In a network with traffic, MAC payload packets are prioritized; the transmission of the next beacon frame will be on hold until the transmission of the current data frame has finished. Thus the real beacon interval may stretch slightly beyond the specified interval. This is illustrated in Figure 8.

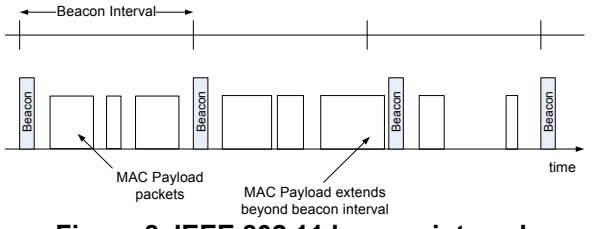

Figure 8. IEEE 802.11 beacon interval

A common beacon interval in a normally populated WLAN is 100 ms, which is a reasonable trade-off between throughput, client joins and roaming response. Decreasing the beacon interval results in a more responsive network, at the cost of increased packet overhead and reduced network throughput.

Transmitting beacons at a rapid rate can be utilized to generate fully deterministic traffic in an otherwise idle WLAN. This is the technique employed in this experiment. The other option for traffic generation would have been to deploy three WLAN clients in the area, one for each of the three APs, and have them set up a high load communication link with the APs. However, in [9], it is identified that IEEE 802.15.4 based traffic, and thus also WirelessHART traffic, will create interference in a WLAN network either in the shape of collisions between IEEE 802.15.4 and WLAN packets, or as channel occupation due to the IEEE 802.15.4 transmissions in the WLAN channel and the use of the CSMA/CA (carrier sense multiple access with collision avoidance) mechanism. This will lead to a non-deterministic behaviour of the WLAN traffic, and it will thus be challenging to give an exact theoretical explanation of the observed behaviour of the WirelessHART network when coexisting with WLAN networks.

The impact on the WirelessHART network was monitored when the beacon interval for the WLAN was decreased from 100 ms to 20 ms. For an idle WLAN channel, the relationship between the beacon interval and the *duty cycle* of the channel is defined as:

$$D = \frac{b}{R} \cdot \frac{1}{BI} \cdot 100\% \qquad (1)$$

where:

D	is the duty cycle
b	is the beacon transmission time
R	is the basic data rate
BI	is the beacon interval

A beacon packet is around 97 bytes long. The length of the beacon may be slightly longer depending on how much vendor specific information is contained in variable length payload. In our calculations, we have used 97 bytes as the length for the beacon, as a few bytes difference only causes a negligible change in the calculated duty cycle. As mentioned above, the basic data rate for an IEEE 802.11 network supporting the *b* and *g* protocols is 1 Mbps [2].

Figure 6 and Figure 7 presents packet loss and latency of a WirelessHART network operating in an environment free from WLAN interference. The average packet loss is in the case below 1 %, and the average network latency is around 2000 ms throughout the 24 hour test period.

The beacon interval in the WLAN was initially set to the default rate 100 ms. The duty cycle of the WLAN networks can be found using equation (1):

$$D_{100ms} = \frac{97 \text{ bytes}}{1 \text{ Mbps}} \cdot \frac{1}{100 \text{ ms}} \cdot 100\% = \underline{\underline{0.8\%}}$$

$$D_{20ms} = \frac{97 \text{ bytes}}{1 \text{ Mbps}} \cdot \frac{1}{20 \text{ ms}} \cdot 100\% = \underline{\underline{3.9\%}}$$

After 2:45 hours of operation, the beacon interval was decreased to 20 ms, which, referring to equation (1) corresponds to a 3.9 % duty cycle for each of the three WLAN channels. After 21:30 hours, the beacon interval was increased to 100 ms. No ordinary WLAN traffic was present during the experiments.

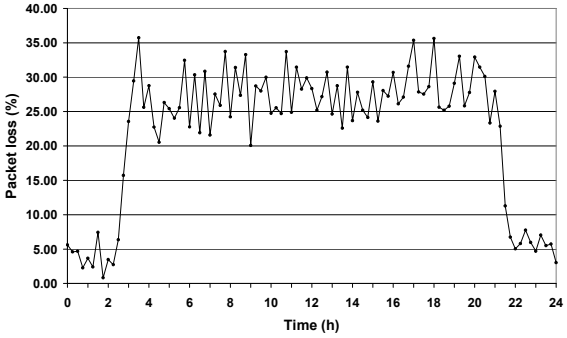

Figure 9. IEEE 802.11g coexistence – Packet Loss

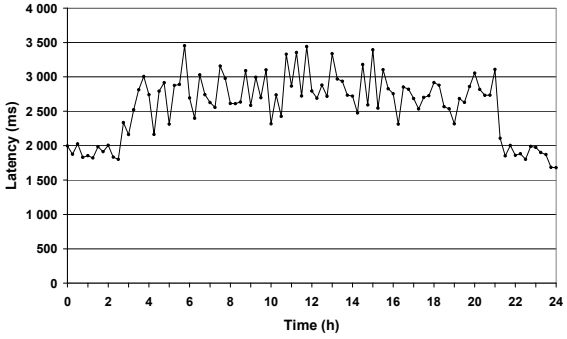

Figure 10. IEEE 802.11g coexistence – Latency

Table 1. IEEE 802.11g coexistence – Mean and Std. Dev.

Beacon interval (ms)	Packet Loss (%)		Latency (ms)	
	Mean	Std.dev.	Mean	Std.dev.
N/A	0.50	0.48	2037	92
100	4.83	1.87	1885	99
20	27.20	4.28	2760	315

Figure 9 and Figure 10 shows the average network packet loss and latency during the 24 hour test period. In addition, Table 1 shows statistical data, i.e. arithmetic mean and standard deviation for the WirelessHART network for the three different levels of

WLAN influence: No WLAN present (referred to as N/A in Table 1, this is are the results from the network performance test in section 4.1), WLAN beacon interval at 100 ms and WLAN beacon interval at 20 ms. There is a noticeable degradation of the WirelessHART performance when coexisting with the WLAN networks. The observed results can be explained theoretically if we examine the timing specifications for the IEEE 802.11 and WirelessHART standards [2][3][8]. Figure 11 illustrates a timing diagram for WirelessHART packets together with WLAN beacon transmissions at a 20 ms beacon interval. The time scaling for the respective packets is correct relative to each other.

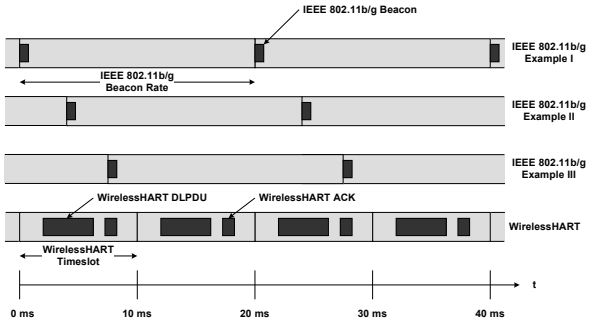

Figure 11. WirelessHART and IEEE 802.11 beacon transmissions

A WLAN beacon consists of 97 bytes, and is transmitted at 1 Mbps. The transmission time t_b for the beacon thus becomes:

$$t_{b,WLAN} = \frac{97\ bytes}{1\ Mbps} = \frac{776\ bits}{10^6\ bits/s} = \underline{\underline{0.776\ ms}}$$

The MAC payload in a WirelessHART packet (DLPDU) contains 133 bytes. The ACK packet is 26 bytes, thus the total data exchange within a WirelessHART timeslot is 159 bytes. With a data rate of 250 kbps, the total transmission time for a WirelessHART packet and the corresponding ACK is:

$$t_{b,WirelessHART} = \frac{159\ bytes}{250\ kbps} = \frac{1272\ bits}{250 \cdot 10^3\ bits/s} = \underline{\underline{5.088\ ms}}$$

Hereafter, the combined WirelessHART DLPDU and ACK is referred to as the WirelessHART frame. A WirelessHART timeslot is 10 ms [8]. In the time domain, this means that the active transmission period for the WirelessHART frame occupies 50% of the available timeslot.

In the following, we assume that a WLAN beacon which collides with any part of the WirelessHART frame (either the DLPDU or ACK parts), destroys the information in the WirelessHART packet. As previously explained, in an idle WLAN beacon transmissions are deterministic, i.e. the time spacing between each beacon corresponds exactly to the beacon interval. A 100 ms beacon interval statistically means that a beacon transmission will occur in every tenth WirelessHART timeslot, and with a 20 ms beacon interval, a beacon transmission will occur in every second WirelessHART timeslot. Since the WirelessHART frame occupies 50% of the available timeslot, the probability for a collision between the beacon and the WirelessHART frame becomes

$$p_c = \frac{T_s}{BI} \cdot 50 \quad [\%] \qquad (2)$$

where:

p_c is the collision probability
T_s is the WirelessHART timeslot length
BI is the WLAN beacon interval

Given that the WirelessHART data exchange only occurs in channels which overlap with the WLAN channels, the probabilities for a collision between the beacon and WirelessHART frame for 20 ms and 100 ms beacon intervals are:

$$p_{c,20ms} = \frac{T_s}{BI} \cdot 50 = \frac{10}{20} \cdot 50 = \underline{\underline{25\ \%}}$$

$$p_{c,100ms} = \frac{T_s}{BI} \cdot 50 = \frac{10}{100} \cdot 50 = \underline{\underline{5\ \%}}$$

However, WirelessHART networks utilize frequency hopping, where all links in the network will for each timeslot randomly select which of the 15 available channels are used for communication. The utilization of the 15 available channels is uniformly distributed, resulting in the probability of a WirelessHART data transmission taking place on a given channel equal to:

$$p_{channel} = \frac{1}{15} = \underline{\underline{6.7\ \%}}$$

As 12 of the 15 WirelessHART channels overlap with the WLAN channels (see Figure 4), the probability for a collision between a WLAN beacon and a WirelessHART frame is:

$$p_{20ms} = p_{c,20ms} \cdot 12 \cdot p_{channel} = 0.25 \cdot (12 \cdot 0.067) = \underline{\underline{20\,\%}}$$
$$p_{100ms} = p_{c,100ms} \cdot 12 \cdot p_{channel} = 0.05 \cdot (12 \cdot 0.067) = \underline{\underline{4\,\%}}$$

To further adhere to the theory, more parameters should be taken into consideration when calculating the probability of a WLAN beacon colliding with a WirelessHART frame.

First of all, the offset between the WLAN beacon and the WirelessHART frame will drift slowly with time, as there are no time synchronization between the WSN and the WLAN. In addition, the WirelessHART frame is subject to drift within the boundaries of the 10 ms timeslot. This means that the probability for a collision between a beacon and a WirelessHART frame will be time variant. Figure 11 provides examples of three different time offsets. The upper diagram (Example I) shows WLAN beacons arriving before the WirelessHART frame, thus no collision will take place. The second and third diagrams from the top (Examples II and III) show WLAN beacons colliding with the WirelessHART DLPDU and ACK packets respectively, which might destroy the WirelessHART data transmission. But, as the time drift is short (µs magnitude) compared to the timeslot length (10 ms), the relative position of a beacon transmission within the WirelessHART timeslot is set when the WLAN APs are powered up, and the position will remain more or less the same throughout the 24 hour test duration.

Furthermore, the WirelessHART specification [8] employs error-correcting code. In the cases, it is likely that the WirelessHART error-correcting code will manage to repair the actual frame, especially where the WLAN beacon only slightly overlaps with one edge of the WirelessHART frame.

However, comparing the experimental data in Table 1 with the theoretical probabilities p_{100ms} and p_{20ms} for a collision between a WLAN beacon and a WirelessHART frame, a close correlation is found. For 100 ms beacon interval, the measured average network packet loss is 4.83% with a std. dev. of 1.87, whereas the theoretical p_{100ms} equals 4%. For 20 ms beacon interval, the measured average network packet loss is 27.20% with a std. dev. of 4.28, while the theoretical p_{20ms} is 20%. The slightly higher packet loss observed in experiments compared to the theoretical calculations can be explained with the time offsets and the WirelessHART error-correcting codes mentioned above. For this experiment, the relative position of the WLAN beacons and the WirelessHART frame was probably so that the beacon transmissions would overlap with the WirelessHART frame when the WirelessHART transmissions occurred in one of the 12 overlapping channels. However, due to the fact that a beacon transmission which coincides with a WirelessHART frame does not necessarily result in packets loss (because of the WirelessHART error-correcting codes which can repair bit errors), the observed network packet loss is lower than the worst case scenario where all WLAN beacon transmissions will destroy a WirelessHART frame:

$$p_{wc,20ms} = \frac{T_s}{BI} \cdot 12 \cdot p_{channel} = \frac{10}{20} \cdot 12 \cdot 0.067 = \underline{\underline{40\%}}$$
$$p_{wc,100ms} = \frac{T_s}{BI} \cdot 12 \cdot p_{channel} = \frac{10}{100} \cdot 12 \cdot 0.067 = \underline{\underline{8\%}}$$

Based on both the observed measurements and the theoretical analysis, it is apparent that deploying one or more WLAN APs in the same area as a WirelessHART network will lead to a degradation of the WirelessHART network, especially considering that the experiments and analysis described here only utilized the WLAN beacons to generate network traffic (having a duty cycle of only 3.9% for 20 ms beacon interval).

The actual increase in WirelessHART packet loss depends on many factors, including the WLAN channel configuration, the distance between the WirelessHART devices and the APs, and, most importantly, the amount of WLAN traffic. To have a successful coexistence of WLAN and WirelessHART in an industrial facility, careful deployment considerations should be made. This is discussed further in section 5.

4.3. Resilience to chirp jamming

In this laboratory experiment, the WirelessHART network was exposed to attacks from a 2.4 GHz linear chirp jamming device, transmitting time-varying noise with a sweep period of 10 microseconds. A chirp is a time-frequency varying function, commonly of swept-sine type. There are different types of chirp signals. In an up-chirp signal the frequency increases with time and in a down-chirp the frequency decreases with time. The frequency sweep could either vary linearly with time (linear chirp) or exponentially with time (exponential chirp).

Direct Sequence Spread Spectrum (DSSS) based networks are in general vulnerable to time-varying spectral noise, as both the spread signal and the jammer interference have large bandwidths. WirelessHART employs DSSS with Offset Quadrature Phase-Shift Keying (O-QPSK) modulation [3][8].

The jammer was placed approximately 1 meter from the WirelessHART gateway (see Figure 5 for device locations). The average packet loss, latency and reliability of the WirelessHART network in the period before, during and after the jammer attack are presented in Figure 12, Figure 13 and Figure 14. The jammer was activated 15 minutes into the test period, and it was active for 45 minutes.

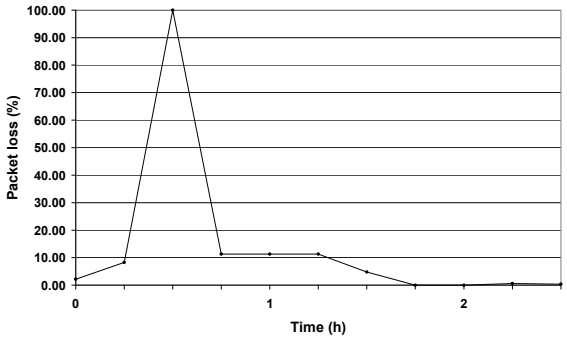

Figure 12. Chirp Jamming – Packet Loss

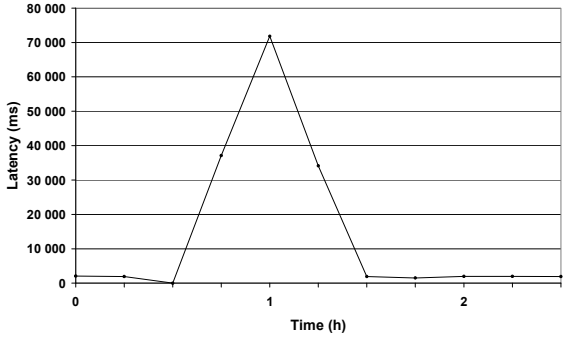

Figure 13. Chirp Jamming – Latency

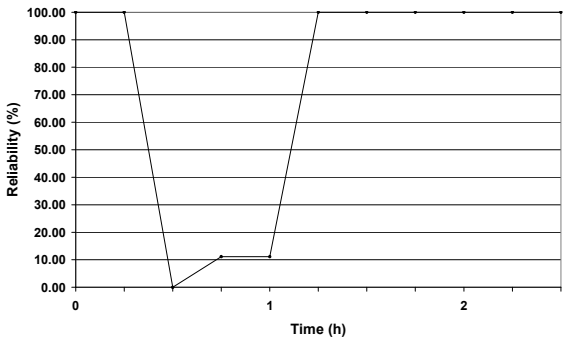

Figure 14. Chirp Jamming - Reliability

It is apparent that the jammer attack significantly degraded the WirelessHART network. In the initial phase of the jammer attack (from 15 min to 30 min), the WirelessHART network broke down completely, with no data reception on the gateway and a resulting reliability of 0%.

5. WirelessHART and WLAN coexistence deployment considerations

Based on the results from the coexistence test in section 4.2, it is clear that having an IEEE 802.11 based WLAN in close proximity of a WirelessHART network affects the WirelessHART network in an unfavourable manner. This knowledge should be taken into consideration and be included as a part of the planning stage before deploying WLANs and WirelessHART networks in the same area.

To avoid potential degradations of a WirelessHART network coexisting with WLANs, it is essential to carry out an overall radio planning for the site, especially when three (or more) WLAN access points are within radio range of the WirelessHART network. Normally, industry best practices for WLAN deployment with respect to interference free operation among the WLAN access points involves configuring the WLAN access point to operate on channels 1, 6 and 11, respectively (this is described in section 3). Unfortunately, this approach limits the performance of a WirelessHART network operating in the same area, since it leaves the WirelessHART network with only 3 of the 15 available channels free from WLAN interference, as illustrated in Figure 4. The actual impact on the WirelessHART network depends on the network load on the neighbouring WLANs, but from the experiments we see that as little traffic as only 2% duty cycle on the WLAN channels significantly increases the WirelessHART packet loss, from about 1% with interference free operation to around 30% when coexisting with WLAN. Further increase in WLAN load will probably result in a WirelessHART packet loss which is so high that it will affect the reliability of the network, leading to loss of sensor data. Even though the reliability remained at 100% in the coexistence test, the significant increase in retransmissions due to the increased packet loss affects both latency and the sensor nodes power consumption and thereby limits battery lifetime.

Radio planning should be carried out as a combination of channel planning and spectrum measurements in the field. As an alternative to expensive specialized spectrum analyzing instruments, several PC tools on the market are good alternatives for such tasks. The important thing from a WirelessHART point of view is to make sure that there are some interference free channels available in the frequency spectrum. The safest approach to avoid any conflicts between WLAN and WirelessHART is to have the WLAN operate in the 5 GHz band instead of the 2.4 GHz band, i.e. using IEEE 802.11a instead of IEEE 802.11b/g. This approach has until recently had some disadvantages, e.g. shorter radio range and limited availability of client equipment. However, with the forthcoming IEEE 802.11n specification, the utilization of the 5 GHz license free band is expected to grow significantly in the near future.

If moving the WLAN to the 5 GHz band is not an alternative, a recommended approach to avoid interference in the 2.4 GHz band is to avoid the presence of more than two WLAN access points within range of the WirelessHART network. For example, two WLAN access points configured for interference free operation (for example channels 1 and 6) would

leave the WirelessHART network with 6 interference free channels.

If site requirements for WLAN coverage demands for three (or more) access points within close proximity of the WirelessHART network, careful channel planning should be carried out. One possible compromise is to sacrifice the interference free operation of the WLAN access points, and configure them to operate on overlapping channels. This will leave parts of the frequency spectrum unoccupied and thus provide interference free channels for the WirelessHART network. An example for the case of three WLAN access points is to have them operate on channels 1, 4 and 7 respectively. WLAN channel 7 has an upper cut-off frequency at 2.453 GHz, allowing interference free operation for WirelessHART channels 21 to 25. It is not recommended to use neighbouring WLAN channels for access points that are within radio range of each other, as this leads to significant cross-channel interference are thereby degraded WLAN performance. On the other hand, as already stated above, the full spectrum of the 2.4 GHz band should not be utilized for WLAN when coexisting with WirelessHART. How much of the frequency spectrum which should be reserved for WirelessHART depends on how many WirelessHART networks which are planned within the area, the size if the WirelessHART network with respect to number of nodes, and finally the criticality of the WirelessHART application(s).

6. Conclusion

The WirelessHART specification offers many possibilities for wireless instrumentation for industrial applications. From the WirelessHART network performance evaluation presented in this paper, the following conclusions can be drawn:

- A WirelessHART network is fully capable of reliable operation in a challenging RF environment.
- When coexisting with IEEE 802.11 based WLAN networks, the interference from the WLAN will cause increased packet loss rates in the WirelessHART network, and careful deployment consideration should be made before having a WirelessHART network coexists with WLAN installations.
- A WirelessHART network is vulnerable to malicious denial-of-service attacks, and if there is a potential risk of such attacks, the networks should be installed in areas with strict access control security procedures.

Suggested future work is to evaluate short-term and long-term reliability and stability performance of a WirelessHART network when deployed in a live production environment.

Based on the results from the coexistence performance evaluation, a suggested enhancement for future versions of the WirelessHART specification is to employ *adaptive* frequency hopping. With adaptive frequency hopping, a WirelessHART network will blacklist and stop using channels which suffers from high packet loss, and thereby be able to avoid the increased packet loss which occurs when coexisting with one or more WLAN networks.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A Survey on Sensor Networks", *IEEE Communications Magazine*, Aug. 2002, pp 102-114.

[2] IEEE Standard for Information Theory – Telecommunications and information exchange between systems – Local and Metropolitan networks – Specific requirements – Part 11: Wireless Local Area Network Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Computer Society, 2007.

[3] IEEE Standard for Information Theory – Telecommunications and information exchange between systems – Local and Metropolitan networks – Specific requirements – Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs), IEEE Computer Society, 2006.

[4] S. Petersen, S. Carlsen and A. Skavhaug, "Layered Software Challenge of Wireless Technology in the Oil & Gas Industry", *Proc. of the Australian Conference on Software Engineering (ASWEC) 2008*, March 2008, pp. 37-46.

[5] S. Petersen et al., "A Survey of Wireless Technology for the Oil and Gas Industry", *SPE Projects, Facilities and Construction* Vol. 3, No. 4, Dec. 2008, pp. 1-8.

[6] A. N. Kim, F. Hekland, S. Petersen and P. Doyle, "When HART Goes Wireless: Understanding and Implementing the WirelessHART Standard", *Proc. of the IEEE International Conference on Emerging Trends and Factory Automation (ETFA) 2008*, Sept. 2008, pp. 899-907.

[7] S. Petersen, P. Doyle, C. S. Aasland, S. Vatland and T. M. Andersen, "Requirements, Drivers and Analysis of Wireless Sensor Network Solutions for the Oil & Gas Industry", *Proc. of the IEEE International Conference on Emerging Trends and Factory Automation (ETFA) 2007*, Sept. 2007, pp. 219-226.

[8] HART Communication Foundation, "HART Field Communication Protocol Specification, Revision 7.0", Sept. 2007.

[9] L. Angrisani, M. Bertocco, D. Fortin and A. Sona, "Experimental Study of Coexistence Issues Between IEEE 802.11b and IEEE 802.15.4 Wireless Networks", *IEEE Trans. on Instrumentation and Measurement*, Vol. 53, No. 8, Aug. 2008, pp. 1514-1523.