2-1-2016

Dual protocol performance using WiFi and ZigBee for industrial WLAN

Ghada Afifi

The American University in Cairo

School of Sciences and Engineering

DUAL PROTOCOL PERFORMANCE USING WIFI AND ZIGBEE FOR INDUSTRIAL WLAN

A Thesis Submitted to

Electronics and Communication Engineering Department

in partial fulfillment of the requirements for
the degree of Master of Science

by Ghada Sameh Afifi

under the supervision of Prof. Hassanein H. Amer and Dr. Ramez Daoud
July 2016

To my Family and Friends

Abstract

The purpose of this thesis is to study the performance of a WNCS based on utilizing IEEE 802.15.4 and IEEE 802.11 in meeting industrial requirements as well as the extent of improvement on the network level in terms of latency and interference tolerance when using the two different protocols, namely WiFi and ZigBee, in parallel. The study evaluates the optimum performance of WNCS that utilizes only IEEE 802.15.4 protocol (which ZigBee is based on) without modifications as an alternative that is low cost and low power compared to other wireless technologies. The study also evaluates the optimum performance of WNCS that utilizes only the IEEE 802.11 protocol (WiFi) without modifications as a high bit network. OMNeT++ simulations are used to measure the end-to-end delay and packet loss from the sensors to the controller and from the controller to the actuators. It is demonstrated that the measured delay of the proposed WNCS including all types of transmission, encapsulation, de-capsulation, queuing and propagation, meet real-time control network requirements while guaranteeing correct packet reception with no packet loss. Moreover, it is shown that the demonstrated performance of the proposed WNCS operating redundantly on both networks in parallel is significantly superior to a WNCS operating on either a totally wireless ZigBee or WiFi network individually in terms of measured delay and interference tolerance. This proposed WNCS demonstrates the combined advantages of both the IEEE 802.15.4 protocol (which ZigBee is based on) without modifications being low cost and low power compared to other wireless technologies as well the advantages of the IEEE 802.11 protocol (WiFi) being increased bit rate and higher immunity to interference. All results presented in this study were based on a 95% confidence analysis.

ACKNOWLEDGMENTS

I would like to acknowledge both my supervisors: Prof. Hassanein Amer and Dr. Ramez Daoud for their great support throughout my thesis.

I would like to acknowledge Hassan Halawa for his help during my thesis.

I would like to thank Dr. Hany Elsayed for his constructive feedback to produce this dissertation.

I would like to acknowledge the graduate program directors: Dr. Ayman El Ezabi and Dr Karim Seddik.

TABLE OF CONTENTS

List of Tables

List of Figures

List of Abbreviations

Networked Control Systems (NCSs)

Wireless NCS (WNCS)

Wireless Interface for Sensors and Actuators (WISA)

ASEA Brown Boveri (ABB)

Media Access Control (MAC)

User Datagram Protocol (UDP)

Wireless Sensor Actuator Network (WSAN)

Transmission Control Protocol (TCP)

Wireless local area network (WLAN)

Frequency Division Multiple Access (FDMA)

Code Division Multiple Access (CDMA)

Time Division Multiple Access (TDMA)

Electromagnetic interference (EMI)

Low-rate wireless personal area networks (LR-WPANs)

Command-line user interface for simulation execution (Cmdenv)

Graphical User Interface (GUI)

Access Point (AP)

Sensor Actuator (SA)

Network Description language (NED)

Internet Protocol (IP)

Institute of Electrical and Electronics Engineers (IEEE)

Chapter 1

Introduction

1.1 Contribution of this Thesis

This thesis is an attempt to study the performance of WNCS utilizing two different communication networks, namely IEEE 802.11 and IEEE 802.15.4, in meeting benchmarks requirements set by the industry. This study assesses the feasibility of implementing a totally wireless system in the existence of external interference utilizing the standard IEEE 802.15.4 protocol (which ZigBee is based on) without modifications while achieving benchmarks similar to those present in the literature [8, 10]. It is important to note that ZigBee builds on the physical and Media Access Control (MAC) layers defined in the IEEE 802.15.4 standard. Thus, the results of this feasibility study are also applicable for ZigBee-based industrial WNCSs. The feasibility of implementing a totally wireless system utilizing IEEE 802.11a and IEEE 802.11b (WiFi) is also assessed. This thesis attempts to study the extent of improvement of performance when using both networks IEEE 802.15.4 and IEEE 802.11a in parallel. This proposed WNCS would demonstrate the combined advantages of both WiFi and ZigBee. The main advantages of the IEEE 802.15.4 protocol are its low power consumption and cost effectiveness which makes it appealing for many applications. The main advantages of the IEEE 802.ll are it's higher bit rate providing lower latencies and higher interference tolerance. It is important to note that the IEEE 802.15.4 operates in the 2.4 GHz range and the IEEE 802.11 was chosen to operate in the 5.8 GHz range to ensure that there exists no interference between the two networks being utilized in parallel. The proposed WNCS is expected to demonstrate improved performance as well as interference tolerance in case one or both of the networks are subjected to external interference.

1.2 Thesis Organization

Chapter 2 provides a literature review of benchmark industrial WNCS being utilized currently as well as previous relevant studies of implementation of an industrial WNCS utilizing alternative communication technologies.

Chapter 3 first discusses the performance of the proposed WNCS in case of operating a single protocol, namely ZigBee in both an interference free environment as well as when it is subjected to interference. Then network performance is optimized in case of implementing a totally wireless single protocol utilizing unmodified WiFi without the Ethernet backbone in [9]. The results of each case are discussed and compared versus benchmark requirements in terms of latency and packets dropped.

In Chapter 4, the network performance is analyzed when the network is utilizing both WiFi and ZigBee redundantly in parallel. The network performance is compared to benchmark performance demonstrated by [8]. The deadline for our study was fixed at 36ms versus 40ms demonstrated by [8] leaving a 10% guard band. It is important to note that OMNET measured delays include all types of processing, encapsulation, de-capsulation and propagation delays, while the Wireless Interface for Sensors and Actuators published results are only the air interface delays [8]. Moreover, for the proposed WNCS, zero control packet loss must be guaranteed due to the critical nature of the control application.

Chapter 5 concludes the dissertation.

Chapter 2
Literature Review

This chapter provides a comprehensive literature review of benchmark industrial WNCS being utilized currently as well as previous relevant studies of implementation of an industrial WNCS utilizing alternative communication technologies. Followed by that, a brief coverage of different IEEE 802.11 and 802.15 wireless protocols to be used throughout the study.

2.1 General Background

- **Networked Control System (NCS):** Communication system composed of sensors, actuators and controllers to control a certain process – (In Loop, S2A). Control and feedback signals exchanged in the form of data packets.
- **ZigBee:** A wireless technology developed as an open global standard to address the unique needs of low-cost, low-power wireless M2M networks. The ZigBee standard operates on the IEEE 802.15.4 physical radio specification and operates in unlicensed bands including 2.4 GHz, 900 MHz and 868 MHz.
- ***WiFi:*** A wireless local area network (WLAN) based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards and operates mainly in the 2.4 GHz and 5 GHz frequency ranges.
- ***User Datagram Protocol: (UDP):*** A transport layer protocol that is a part of the Internet Protocol (IP), but is less reliable than Transmission Control Protocol (TCP), which is another transport layer protocol. UDP is fast, connectionless and requires less bandwidth than TCP at the expense of no error correction, no reordering of datagrams and no guarantee of packet delivery.
- ***Payload:*** The actual data or message sent by the user during communication, not taking into account overhead data, such as addressing information, sequencing information or error detection information.
- ***Packet End-to-End Delay:*** The time (in seconds) it takes a packet to travel across the network from the source to the destination application layer

Networked Control Systems (NCSs) are typically composed of a large number of sensors, actuators and controllers designed to carry small packets, with a high data rate [1, 2]. NCS is utilized in the implementation of real-time applications requiring minimal packet losses and an extremely high level of reliability [3]. Depending on the application, the choice of the network protocol to use will differ [4]. To satisfy such requirements, control networks applications traditionally used deterministic network communication protocols (such as CAN, PROFIBUS, etc…) to guarantee high-speed performance with maximum reliability [1, 5, 6, 7]. However, cables fail frequently due to the harsh production line environment, not to mention the cost ineffectiveness of hardwiring a large number of nodes. Hence, the need for a wireless solution arose. Wireless NCS (WNCS) solutions provide lower cost, reduced failures that may arise due to cable breakage in moving parts and easier troubleshooting and maintenance. Fig. 0 provides a block diagram for NCS feedback loop.

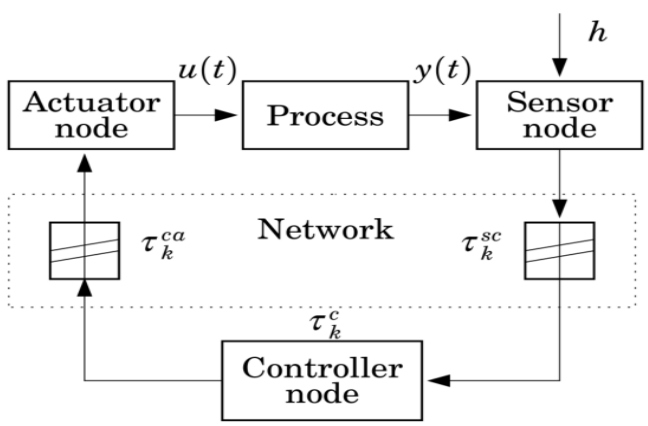

Fig. 0 Networked Control System Block Diagram

Fault-Tolerance can be implemented at multiple levels in a WNCS such as at the sensor, controller, actuator or network fabric level [11-17]. In all cases, redundancy is typically employed in order to be able to tolerate the failure of any single component.

Wireless Interface for Sensors and Actuators (WISA) is a WNCS solution devised by ABB based on modified Bluetooth, which accommodates both communication and wireless powering of the system [8]. In [9], a Wi-Fi implementation of a WNCS was proposed based on unmodified IEEE 802.11b. The proposed WNCS was composed of 30 sensor actuator pairs communicating over two IEEE 802.11b Access Points.

The network's controller node was connected to the Access Points through a wired Switched Ethernet backbone. It was shown that the proposed WNCS system was able to meet the required control deadline with no lost or over-delayed packets.

2.2 ABB's WISA (Wireless Interface for Sensors and Actuators)

The wireless technology used is based on IEEE 802.15.1 (physical layer) and is called WISA - Wireless Interface to Sensors and Actuators[8]. WISA basically consists of two main parts:

- Communication (WISA-COM)
- Power supply (WISA-POWER)

WISA-COM

Network Topology: The WISA wireless communication links the sensors and actuators to a "basestation" that satisfies the rigorous demands of an industrial environment including high reliability, fast response time, serving a large number of sensors and actuators located in a range of several meters radius, and guarantying high data transmission integrity, even where radio propagation may be affected by obstacles and interference. The sophisticated basestation module designed by ABB ensures that the complexity resides in the input module rather than in the SA. One such module can handle up to 120 devices. Although similar to a WLAN access point in many respects, the ABB design has several features that clearly set it apart:

- Simultaneous transmission and reception of radio signals; i.e. full-duplex operation.
- Simultaneous reception of strong and weak signals. The difference in power between a strong signal and a weak one may be as much as a million to one.
- Interference suppression. Reception of a very weak sensor signal is possible even though a large interfering signal may exist at some adjacent frequency.
- Transmit and receive antennas at the input module are swapped every 2 ms to provide a diversity of radio propagation paths against fading and shadowing effects.
- Deterministic frequency hopping to combat broad band interferers.

- Efficient frequency use: Only changes are transmitted combined with discrete presence/status monitoring of the devices (at ~ 500ms intervals).
- Five simultaneous communication channels for free access and immediate acknowledgement.

The devices communication hardware is based on an IEEE802.15.1 (Bluetooth). The integrated radio antenna radiation characteristic in the devices is nearly omni-directional in order to achieve uniform transmission performance irrespective of the devices orientation. The communication protocol provides sensors with collision-free air access by allocating each sensor a specific time slot and frequency for its transmission. The content of the WISA protocol is chosen to meet the requirements of large numbers of sensors, it ensures a short response time and makes full use of the available radio bandwidth. A frequency hopping scheme, combined with error detection and automatic message retransmission in case of transmission errors, ensures that the messages from the sensors are reliably delivered, even in the presence of interfering systems such as Bluetooth, WLANs, microwave ovens and electronic tagging systems. To reduce the power consumption, the sensors communication module hibernates until a change in the sensor state occurs. When an event takes place at the sensor, the sensor quickly establishes the radio link by means of a pilot signal from the input module, before transmitting the message. Typically this air interface handling takes 5 ms, with worst-case scenarios of up to 20 ms if the message must be re-transmitted several times[8].

Physical Layer and Medium Access Control (MAC): WISA is based on IEEE 802.15.1 (physical layer). In a system that needs to achieve the delivery of messages with a very high probability of success and high number of devices, the medium access – the sharing of the communication medium - is important. The techniques widely applied are Frequency Division Multiple Access (FDMA), Code Division Multiple Access (CDMA) and Time Division Multiple Access (TDMA). The TDMA technique is most suitable for low-cost and low-power communication with critical timing. In combination with Frequency Hopping (FH) this can provide reliable communication with the possibility of low-cost and low-power implementation. The medium access in WISA is therefore time division multiple access with frequency division duplex and frequency hopping (TDMA/FDD/FH). The WISA frequency hopping scheme guarantees that the frequencies used in successive frames are widely spread, providing robust communication in the presence of wideband interference or faded channels. The downlink transmission (from the base station) is always active, for the purpose of establishing frame and slo t synchronization for the devices, but also to send acknowledgements and data. It enables the device to quickly find its own time slot, where it is allowed to transmit its uplink message. In order to save power, uplink transmissions from a sensor only occur when it has data to send. In both directions user data bits are exchanged (data or control) dependent on the profile used. [8]

Communication Model: A simple transmission control protocol is applied where telegrams received by the base station are acknowledged. In case of a missing acknowledgement, the device will re-transmit the telegram (automatic repeat request ARQ). The short frames allow for several re-transmissions within the permissible delay window, and provide a sufficiently high reliability also with heavy disturbance. With frame-by-frame frequency hopping and antenna switching at the input module (base station), the radio channel used for re-transmission will largely be independent of the previous transmission, thus noticeably increasing the probability of successful transmission. As any re-transmission occurs on the uplink slot and frequency allocated to the particular SA, it will not affect the transmissions of any other SA. A special requirement for an energy-autonomous system, e.g. a sensor, is the extreme low-power requirement for communication. This is a challenge when combined with the real-time requirement. The use of the sensors and actuators radio needs to be minimized by exploiting the possibility of a more complex base station design. A minimized radio use also minimizes interference to other users. The system has a continuous downlink, offering synchronization information to sensors. When a device (e.g. sensor) wakes up, it can immediately find synchronization, which means less use of the receiver.[8]

Interference Immunity in WISA: WISA like WiFi, Bluetooth and ZigBee operate in the 2.4GHz frequency range [8,10,25,26,27]. A typical factory floor environment contains many sources of interference such as mechanical vibrations, welding equipment, interference from the 2.4GHz and GSM frequency range [28]. After significant amounts of testing, it was found that the interference produced by welding equipment, one of the main sources of electromagnetic interference (EMI), fades out above 1GHz as shown in Fig. 1. Such interference produces frequencies up to 1800MHz, far from the 2.4GHz operating band. The effect of such interference was studied on GSM 900/1800 and WISA. The study proved the immunity of 2.4GHz band, including WISA, to interference from sources other than the 2.4GHz band [28].

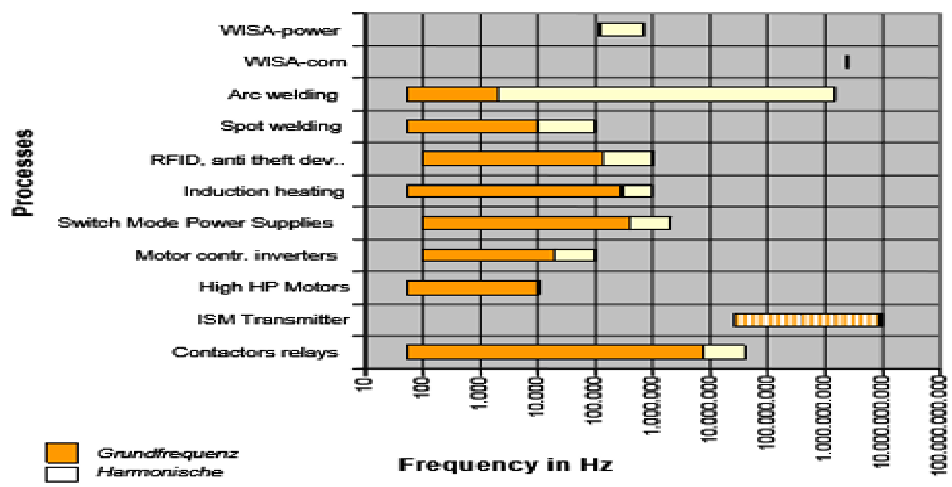

Fig. 1 Frequency areas of different processes or devices in industry

Lately, the wireless communication technologies employed in WISA have been undergoing standardization as the Wireless Sensor Actuator Network (WSAN) standard [18]. However, ABB's wireless powering implementation WISA-POWER still remains an ABB proprietary technology [18]. Recent studies in the area of WSANs have focused on several key areas for industrial control applications such as energy efficiency, fault-tolerance, scalability and meeting hard real-time deadlines. In [19], an approach was presented in order to achieve an optimal WSAN configuration. The focus was on optimizing power consumption and control system delays in order to fulfill the required control performance criteria. While in [20], the focus was on energy efficiency for large-scale WSANs. A hybrid TDMA scheduling scheme was proposed in order to optimize energy consumption. The proposed scheme was analyzed not only in terms of energy savings but also in terms of packet drops and throughput.

2.3 WiFi Implementation of Wireless Networked Control Systems

A Wireless Networked Control System is introduced which uses the IEEE 802.11b protocol without modifications for node communication with minimal cabling and off-the-shelf equipment by Refaat ET. Al. The proposed model, designed to represent a simple machine workcell using 802.11b is shown in Fig.2. In a cell-size of $9m^2$ (3×3m), the sensors communicate through an access point (AP), with the controller, which commands the actuators through the same AP. The control load is divided over 2 of the 3 available non-interfering WiFi channels [9]. The model under study consists of 15 SA pairs on WiFi Channel 1 using AP No. 1, 15 pairs on Channel 6 using AP No. 2 and 1 controller, hard-wired to both APs via a switch.

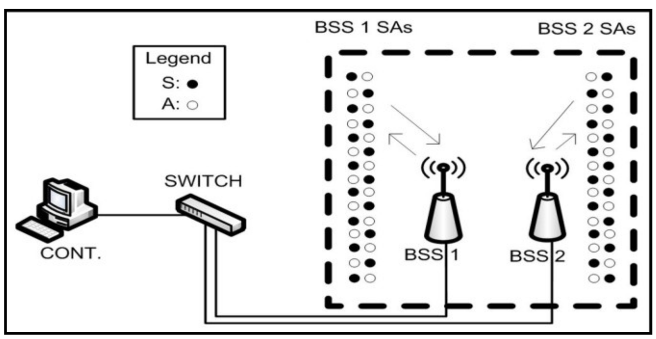

Fig. 2. 3×3m workcell showing sensor/actuator distribution

A UDP protocol is used with a control payload of 10 bytes and a sampling period of 40ms. The distribution of the SAs is arbitrarily chosen as shown in Fig. 2. The controller and the switch are positioned outside the workcell [9]. The performance of the proposed model was analyzed in both interference-free as well as interference model.

The proposed WNCS was studied in case of interference free operation as well as interference operation. For the interference-free scenario, several OPNET simulations were run where control traffic is modeled on top of a video conferencing application. Fig. 3 shows the packets sent by a sensor and total received packets by the controller. The packets sent by one sensor are 25 packets/sec. The controller sends 750 packets/sec which are split accordingly into 25 packets/sec to each actuator.

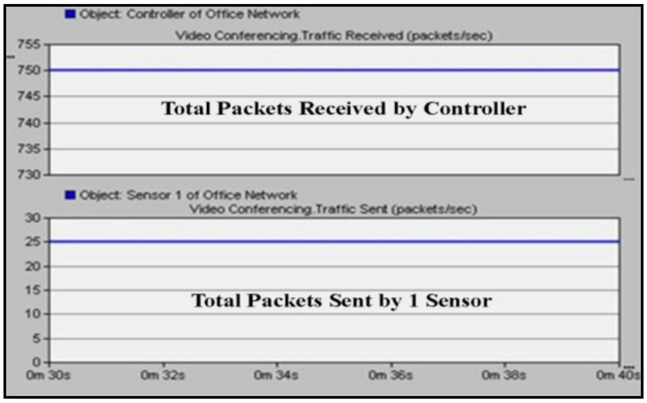

Fig. 3. Packets received by controller and sent by a sensor

The maximum measured delay from any sensor to the controller and from controller to any actuator was found to be 1.65ms and 2.9ms respectively with zero packet loss. These figures are for interference free simulation runs. Note that OPNET results include all types of processing, encapsulation, de-capsulation and propagation delays, while the WISA published results are only the air interface delays [8,9,18].

The proposed WNCS was then subjected to an interference study. It is important to note that the only form of interference worth considering was the 2.4GHz band. An alien node (in this case a laptop) was added to the scenario to subject the model to interference. This laptop communicated with the controller, in the form of an FTP application via the AP(s) using the same WiFi channel as the corresponding AP(s). The laptop position, relative to the cell, would determine the extent of the effect of interference on the system. This alien communication would increase end-to-end delay and/or cause packet loss due to channel interference and bandwidth sharing. A comprehensive search for a worst-case position was conducted. Simulations were run at all possible positions for the laptop along the perimeter of the cell at a distance of 0.75m from the cell boundaries in order to locate the position(s) at which the interference results in a maximum increase of end-to-end delay.

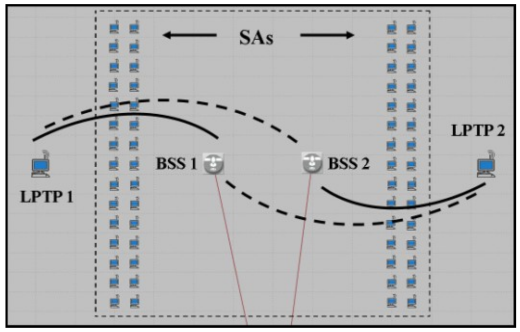

Fig. 4. Possible worst-case positions for laptop

Fig. 4 shows the positions which resulted in the greatest increase in end-to-end delay. From these positions, 6 scenarios were formulated to extensively study the effect of interference on the system. 4 of these scenarios model 1 interferer and 2 scenarios model 2 interferers, including all combinations/permutations of communication.

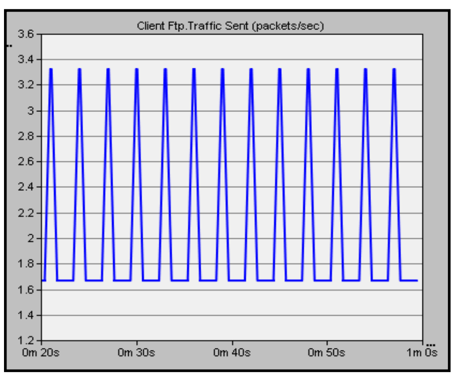

Fig. 5. FTP application between laptop and controller

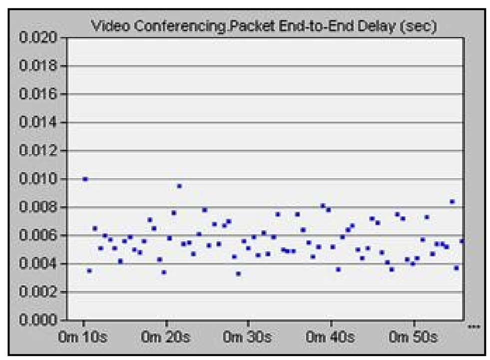

Fig. 6. End-to-end delay at an actuator after introduction of interference

Fig. 5 shows a basic view of the FTP application between the laptop and the controller, simulating a file exchange between a service engineer and the controller, displaying packets sent per second versus the simulation time.

Fig. 6 shows an example of the delay measured in seconds over the period of a simulation at an actuator after being subjected to interference. The results of the study showed that the maximum total end-to-end delay occurred in the scenarios modeling 2 interferers. The maximum total end-to-end delay is 2.05ms from sensor to controller (S→C) and 14.80ms from controller to actuator (C→A). As apparent from the results, the FTP application causes the C→A communication to be delayed.

2.4 Wireless LAN Protocols

2.4.1 IEEE 802.11

The 802.11 family consists of a series of over-the-air modulation techniques that use the same basic protocol. 802.11 technology has its origins in a 1985 ruling by the U.S. Federal Communications Commission that released the ISM band for unlicensed use. In 1999, the Wi-Fi Alliance was formed as a trade association to hold the Wi-Fi trademark under which most products are sold. The base version of the standard IEEE 802.11-2007 has had subsequent amendments. These standards provide the basis for wireless network products using the Wi-Fi brand [25]. The following table summarizes the variations between the different Wi-Fi Standards and shows their evolution:

TABLE I. IEEE 802.11 STANDARDS

Standard	**Data Rate**	**Modulation Scheme**	**Pros/Cons & More Info**
IEEE 802.11 (Wi-Fi)	Up to 2Mbps in the 2.4GHz band	FHSS or DSSS	This specification has been extended into 802.11b.
IEEE 802.11a	Up to 54Mbps in the 5GHz band	OFDM	-Products that adhere to this standard are considered "Wi-Fi Certified." -Eight available channels and less potential for RF interference than 802.11b and 802.11g. -Better than 802.11b at supporting multimedia voice, video, and large-image applications in densely populated user environments. -Relatively shorter range than 802.11b. -Not interoperable with 802.11b. [6]

IEEE 802.11b also referred to as 802.11 High Rate or Wi-Fi	Up to 11Mbps in the 2.4GHz band	DSSS with CCK	-Products that adhere to this standard are considered "Wi-Fi Certified." -Not interoperable with 802.11a. -Requires fewer access points than 802.11a for coverage of large areas. -Offers high-speed access to data at up to 300 feet from base station. -14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels.[6]
IEEE 802.11g	Up to 54Mbps in the 2.4GHz band	OFDM above 20Mbps, DSSS with CCK below 20Mbps	-Products that adhere to this standard are considered "Wi-Fi Certified." - Compatible with 802.11b. -Improved security enhancements over 802.11. -14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels.[6]
IEEE 802.11e			-A wireless draft standard that defines the Quality of Service (QoS) support for LANs. -An enhancement to the 802.11a and 802.11b wireless LAN specifications. -802.11e adds QoS features and multimedia support to the existing IEEE 802.11b and IEEE 802.11a wireless standards, while maintaining full backward compatibility with these standards [7]
IEEE 802.11p also known as DSRC	Operates in the 5.9 GHz frequency range (less interference from outside users since most people use 2.4 GHz range)	OFDM to overcome interference	-The 802.11p allows for data exchange between high speed vehicles, multi-channel solution. -Supports multiple applications and messages can be prioritized (However, throughput may decrease and latency may increase). -Low availability (only a certain number of hardware is available). -Increased cost of hardware components.

			-Operates in a dedicated spectrum (needs a license). [6]
IEEE 802.11n	The real speed would be 100 Mbit/s (even 250 Mbit/s in PHY level)	MIMO	-802.11n builds upon previous 802.11 standards by adding multiple-input multiple-output (MIMO) feature. -The additional transmitter and receiver antennas allow for increased data throughput through spatial multiplexing and increased range by exploiting the spatial diversity through coding schemes like Alamouti coding. -4-5 times faster than 802.11g. [7]

2.4.2 IEEE 802.15.4

IEEE 802.15.4 is a standard which specifies the physical layer and media access control for low-rate wireless personal area networks (LR-WPANs) intended to be low-cost and low-power communication. It is maintained by the IEEE 802.15 working group, the first edition of the 802.15.4 standard was released in May 2003. It is the basis for the ZigBee, WirelessHART, MiWi, and ISA100.11a specifications, each of which further extends the standard by developing the upper layers which are not defined in IEEE 802.15.4.

The physical layer:

Physical layer manages the physical RF transceiver and performs channel selection and energy and signal management functions. It operates on one of three possible unlicensed frequency bands:

- 868.0–868.6 MHz: Europe, allows one communication channel
- 902–928 MHz: North America, up to thirty channels
- 2400–2483.5 MHz: Worldwide, up to sixteen channels

The MAC layer:

The medium access control (MAC) enables the transmission of MAC frames through the use of the physical channel. Besides the data service, it offers a management interface and itself manages access to the physical channel and network beaconing. It also controls frame validation, guarantees time slots and handles node associations. Finally, it offers hook points for secure services.[26,27]

Table II shows different revisions and amendments to the IEEE 802.15.4.

TABLE II. IEEE 802.15.4 STANDARDS

Amendments	Revision Type	Additional Information
IEEE 802.15.4a	WPAN Low Rate Alternative PHY	- Formally called IEEE 802.15.4a-2007 - Providing higher precision ranging, location capability, aggregate throughput, adding scalability to data rates, longer range, and lower power consumption and cost. - Two optional PHYs consisting of a UWB Pulse Radio and a Chirp Spread Spectrum. The Pulsed UWB

		Radio is based on Continuous Pulsed UWB technology operating in 2.4 GHz.
IEEE 802.15.4b	Revision and Enhancement	- Approved in June 2006 and was published in September 2006 as IEEE 802.15.4-2006. - Chartered to create a project for specific enhancements and clarifications to the IEEE 802.15.4-2003 standard, such as resolving ambiguities, reducing unnecessary complexity, increasing flexibility in security key usage, considerations for newly available frequency allocations, and others.
IEEE 802.15.4c	PHY Amendment for China	- Approved in 2008 and was published in January 2009. - Defines a PHY amendment adding new RF spectrum specifications to address the Chinese regulatory changes which have opened the 314-316 MHz, 430-434 MHz, and 779-787 MHz bands for Wireless PAN use within China.
IEEE 802.15.4d	PHY and MAC Amendment for Japan	- Chartered to define an amendment to the 802.15.4-2006 standard. The amendment defines a new PHY dictating changes to the MAC to support a new frequency allocation (950 MHz -956 MHz) in Japan while coexisting with passive tag systems in the band.
IEEE 802.15.4e	MAC Amendment for Industrial Applications	- Approved in 2011 to enhance and add functionality to the 802.15.4-2006 MAC providing better support for industrial markets and permit compatibility with modifications being proposed within the Chinese WPAN. - Specific enhancements were made to add channel hopping and a variable time slot option compatible with ISA100.11a.
IEEE 802.15.4f	PHY and MAC Amendment for Active RFID	- Chartered to define new wireless Physical (PHY) layer(s) and enhancements to the 802.15.4-2006 standard MAC layer which are required to support new PHY(s) for active RFID system bi-directional and location determination applications
IEEE 802.15.4g	PHY Amendment for Smart Utility Network	- Chartered to create a PHY amendment to 802.15.4 to facilitate very large scale process control applications such as the utility smart grid network capable of supporting large, geographically diverse networks with minimal infrastructure, with potentially millions of fixed endpoints.

WiFi vs. ZigBee

Fig. 7 shows the normalized power consumption for the different available technologies.

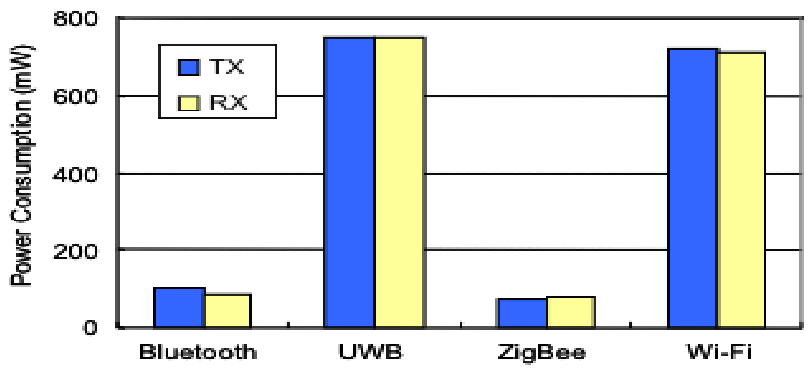

Fig. 7. Normalized power consumption

As highlighted in [23], the basic principle of interference mitigation in coexisting ZigBee and WiFi networks is to avoid the frequency collision by three kinds of diversity techniques (frequency, time and space). It is important to note that the IEEE 802.15.4 operates in the 2.4 GHz range and the IEEE 802.11 can be chosen to operate in the 2.4 GHz range or in 5.8 GHz range to ensure that there exists no interference between the two networks in case they are being utilized in parallel.

Chapter 3

Single Protocol Analysis and Performance

3.1 OMNET Parameter Definition

OMNeT++ is an extensible, modular, component-based C++ simulation library and framework, primarily for building network simulators. "Network" is meant in a broader sense that includes wired and wireless communication networks, on-chip networks, queueing networks, and so on. Domain-specific functionality such as support for sensor networks, wireless ad-hoc networks, Internet protocols, performance modeling, photonic networks, etc., is provided by model frameworks, developed as independent projects. OMNeT++ offers an Eclipse-based IDE, a graphical runtime environment, and a host of other tools. There are extensions for real-time simulation, network emulation, database integration, SystemC integration, and several other functions.

Although OMNeT++ is not a network simulator itself, it is currently gaining widespread popularity as a network simulation platform in the scientific community as well as in industrial settings, and building up a large user community.

OMNeT++ provides a component architecture for models. Components *(modules)* are programmed in C++, then assembled into larger components and models using a high-level Network Description *(NED)* language. Reusability of models comes for free. OMNeT++ has extensive GUI support, and due to its modular architecture, the simulation kernel (and models) can be embedded easily into your applications.

Components

- simulation kernel library

- NED topology description language
- OMNeT++ IDE based on the Eclipse platform
- GUI for simulation execution, links into simulation executable (Tkenv)
- command-line user interface for simulation execution (Cmdenv)
- utilities (makefile creation tool, etc.)
- documentation, sample simulations, etc.

3.2 Model Description

The purpose of this section is to study and compare the performance of the network in terms of latency and interference tolerance when utilizing different protocols, namely WiFi and ZigBee. The model under study is composed of a 9sqm (3m×3m) workspace representing a simple work-cell. The model consists of 30 Sensor/Actuator (SA) pairs communicating with a single multi-channel controller as shown in Fig. 8. The setup of the model is chosen to be similar to the model that was studied by Refaat in [9] as well as WISA model implementation. Every 2 SA pairs shared a communication channel with the controller.

Initially, the network performance is analyzed in case of operating a single protocol, namely ZigBee. The main advantage that this implementation would have vs. the implementation that was presented by Refaat is that this WNCS utilizing ZigBee as the governing communication protocol would have lower cost and lower power compared to the WiFi implementation in [9].

Then network performance is optimized in case of implementing a totally wireless single protocol utilizing unmodified WiFi without the Ethernet backbone in [9] which through which the APs were hardwired to the controller providing mobility if needed.

Finally, the network performance is analyzed when the network is utilizing both WiFi and ZigBee redundantly in parallel. The network performance is compared to benchmark performance demonstrated by [8]. The deadline for our study was fixed at 36ms versus 40ms demonstrated by [8] leaving a 10% guard band. The two measures that are used to analyze the system performance were reliability in the sense of guaranteeing Zero packet loss as well as meeting specified deadline target based on a 95% confidence analysis. It is important to note that OMNET measured delays include all types of processing, encapsulation, de-capsulation and propagation delays, while the Wireless Interface for Sensors and Actuators (WISA) published results are only the air interface delays [8]. Moreover, for the proposed WNCS, zero control packet loss must be guaranteed due to the critical nature of the control application.

3.3 ZigBee Performance

Similar to the WNCS in [9], the User Datagram Protocol (UDP) was used with a sampling period of 40ms. The distribution of the SAs over the workcell was also chosen similar to [9]. A control payload of 1 byte was utilized to allow for a 1-bit signaling scheme. The controller was positioned outside the work cell 1.5m away as shown in Fig.8. The control load was divided over 15 of the available 16 non-interfering IEEE 802.15.4 channels as shown in Fig.9. Each SA pair communicated over a separate communication channel with the controller [22].

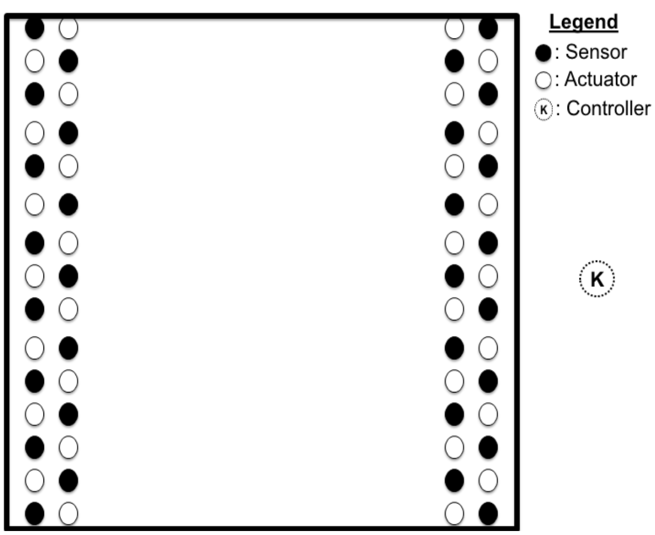

Fig 8. 3×3m work-cell with 30 SA Pairs

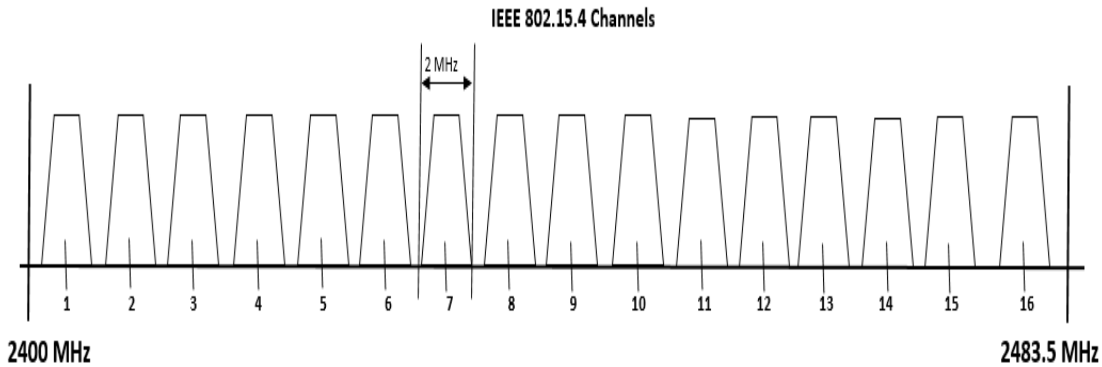

Fig 9. Sixteen Non-Interfering ZigBee Channels

3.3.1 Interference Free Model

The packets sent by one sensor are 25packets/sec. Since there are 30 sensors, the packets received by the controller are 750packets/sec. The controller sends 750packets/sec, which are split accordingly into 25packets/sec to each actuator. A statistical analysis is performed next in order to obtain more accurate results.

Let

X: random variable representing the number of complete burst losses during a trajectory.

μ: Average of random variable X

σ^2: Variance of random variable X

X_i: Number of complete burst losses during i[th] OMNET simulation

n: Number of OMNET simulations

x: Sample mean

s^2: Sample variance

$$x = \frac{1}{n}\sum_{i=1}^{n} X_i$$

$$s^2 = \frac{1}{n-1}\sum_{i=1}^{n}(X_i - x)^2$$

Let n OMNET simulations be performed with different seeds. Random seeds are generated in OMNET to run multiple simulation scenarios with each simulation producing X_i. The average of the X_i's is x and their variance is s^2. x on its own can be considered as a random variable with its own distribution. The Central Limit Theorem indicates that, regardless of the original distribution of the random variable X, the distribution of x approaches the normal distribution. This approximation is better when n is large. Furthermore, the theorem states that the mean of x is μ (mean of X) and its variance is σ_x is equal to $\frac{\sigma^2}{n}$ (σ^2 is the variance of X) [8, 15].

Since x is normally distributed with mean μ and variance $\frac{\sigma^2}{n}$, it is possible to calculate the probability that x is within a certain distance of μ. This probability is the confidence level. Let

$$z = \frac{x - \mu}{\sigma_x}$$

z will be a standardized normal random variable with mean=0 and variance =1. Let:

$$P(-z_\alpha < z < z_\alpha) = \alpha$$
$$P\left[\frac{|x - \mu|}{\sigma_x} < z_\alpha\right] = \alpha$$

Finally, it is important to note that $\sigma_x = \frac{\sigma}{\sqrt{n}}$ is difficult to obtain since σ is unknown. However, if n>30, the sample standard deviation s can be used instead of σ. If the number of simulations were less than 30, the Student T distribution would have to be used instead of the normal distribution [15].

For this statistical study, the number of simulation runs (n) is 33. Hence, the Normal distribution will be used and not the Student T distribution. z_α is calculated for α=95.

Following a 95% confidence analysis, the upper bound of the maximum delay from any sensor to the controller and from the controller to any actuator was found to be 18.63ms and 17.27ms respectively. Therefore, the total delay demonstrated by the system was found to be 35.94ms with zero packet loss. Fig. 10 shows the observed delays at the controller and an actuator for the proposed model in an interference-free environment. Note that the presented results include all types of encapsulation, de-capsulation, transmission, queuing and propagation delays.

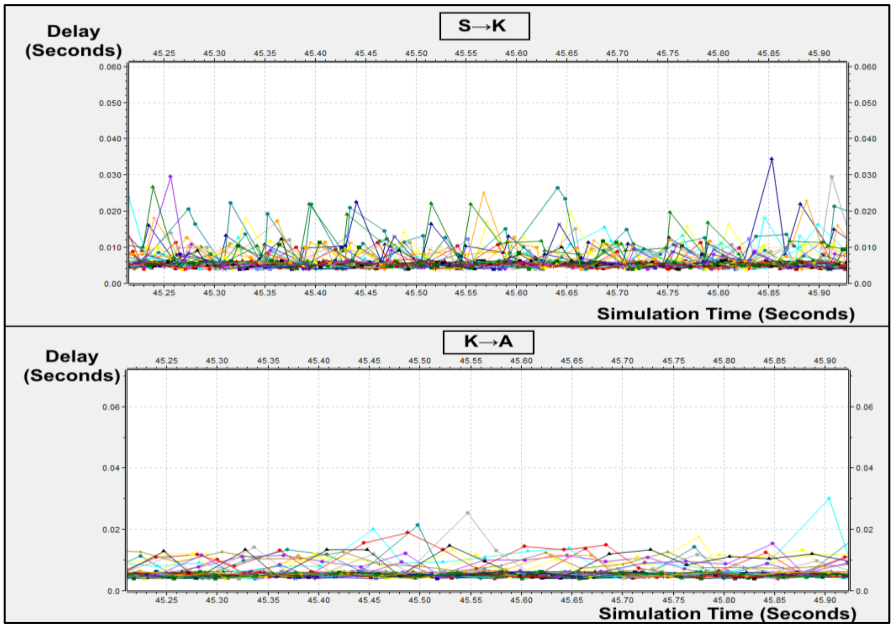

Fig 10. Sensor to Controller and Controller to Actuator Delays (30 SA Pairs - Interference-Free Scenario)

Although these results are within the acceptable 36ms benchmark deadline requirement, this proposed WNCS would not be immune to external ISM band interference. The slightest added interference would yield a delay higher than the 36ms benchmark. Fig. 11. shows that the observed end-to-end delays are higher than the control system deadline when external interference is applied to the system (in the form of two alien nodes exchanging 10 bytes/sec UDP application positioned horizontally at 0.75 m from the cell)

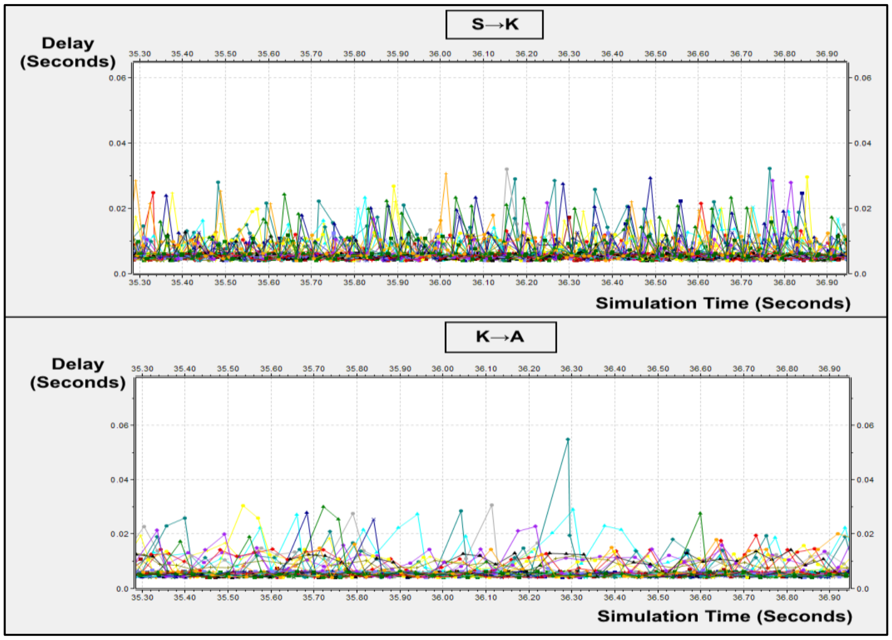

Fig 11. Sensor to Controller and Controller to Actuator Delays (30 SA Pairs– Under Interference)

3.3.2Adjusted Model

The model was adjusted to include 15 SA pairs communicating with a single multi-channel controller as shown in Fig. 12. The controller was also placed outside of the work cell at 1.5 m from the cell boundary. The same control payload of 1 byte was used to allow for the 1-bit signaling scheme. The control load was divided over 15 of the available 16 non-interfering IEEE 802.15.4 channels. Each SA pair communicated over a separate communication channel with the controller. The results of this implementation would again be benchmarked vs. WISA performance in terms of guaranteeing Zero packet loss and meeting deadline requirements as well as benchmarking vs. the WiFi implementation study proposed by Refaat in [9].

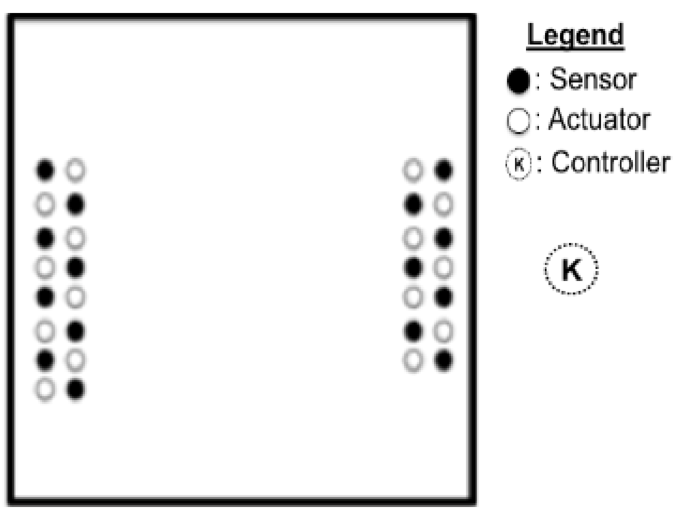

Fig 12. 3×3m work-cell with 15 SA Pair

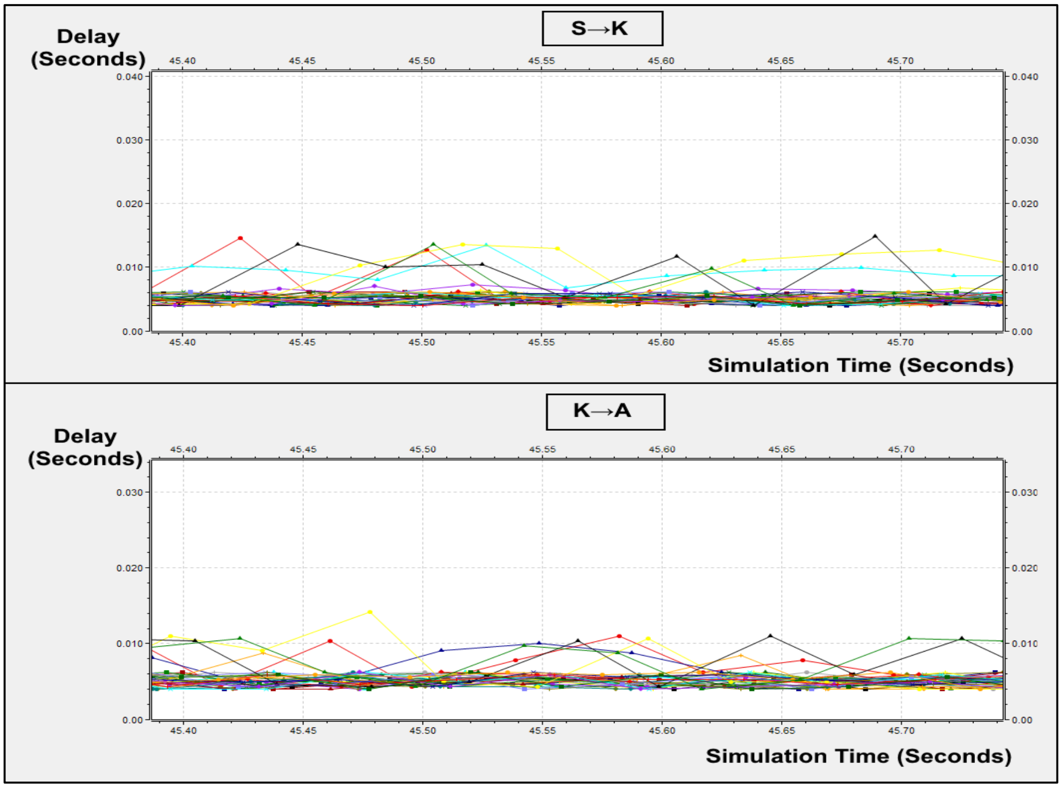

Fig 13. Sensor to Controller and Controller to Actuator Delays (15 SA Pairs – Interference-Free Scenario)

Following a 95% confidence analysis, the upper bound of the maximum delay from any sensor to the controller and from the controller to any actuator was found to be 14.78ms and 15.63ms respectively. Therefore, the total delay demonstrated by the system was found to be 30.41ms with zero packet loss thus meeting the required system deadline.

These results are in line with the expectation that the adjusted model with fewer number of SA nodes would demonstrate lower delay given reduced traffic load on the communication network. Fig. 13 shows the observed delays at the controller and an actuator node for the adjusted model (without external interference). It is important to note that the observed end-to-end delays are less than the system deadline.

3.3.3 *Effect of External Interference*

The model was then subjected to different interference scenarios. Four different placement scenarios were studied where 30 alien nodes (15 pairs) were introduced to subject the model to external ISM band interference. Every pair of nodes (in this case general purpose nodes communicating on the ISM band) communicate together on a separate channel corresponding to the channel distribution of sensors, controllers and actuators. That is, two nodes are exchanging data on the same channel as the corresponding SA nodes utilizing a UDP protocol sending a constant bit rate for the duration of the simulation.

The interfering nodes were placed at several positions horizontally, vertically and diagonally to determine the worst-case interference scenario delays. Similar to [10], the placement is at 0.75m from the cell boundary with nodes of each communicating pair across from each other as shown in Fig. 14.

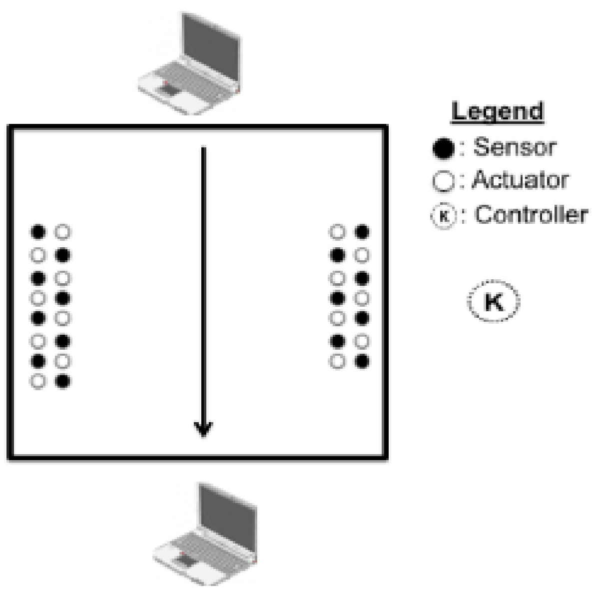

Fig 14. 3×3m work-cell with 15 SA pairs and vertical external interfering nodes

The packet size being exchanged would determine the extent of interference on the system. The alien nodes' communication would increase the control system’s end-to-end delay and/or cause packet loss. For a worst case analysis as in [10], the interfering nodes transmit power was set to 5mW compared to 1mW for the SA nodes.

The packet size being exchanged by the alien nodes was gradually increased and the proposed WNCS's performance was evaluated to determine the maximum interference the network can endure while ensuring that the deadline requirements are met with no packet loss. The maximum interfering load that the network could handle while guaranteeing the required system benchmarks was found to be 97Bytes/sec with a measured end-to-end delay of 35.43ms for the control packets communicating in the system. Interfering loads higher than 97Bytes/sec would result in the system not meeting benchmark deadline requirements implying the possibility of packet drop.

Fig. 15 shows the observed delays at the controller node and at an actuator node under the maximum interfering packet size for the vertical scenario. It is important to note that that the observed delays are less than the system deadline.

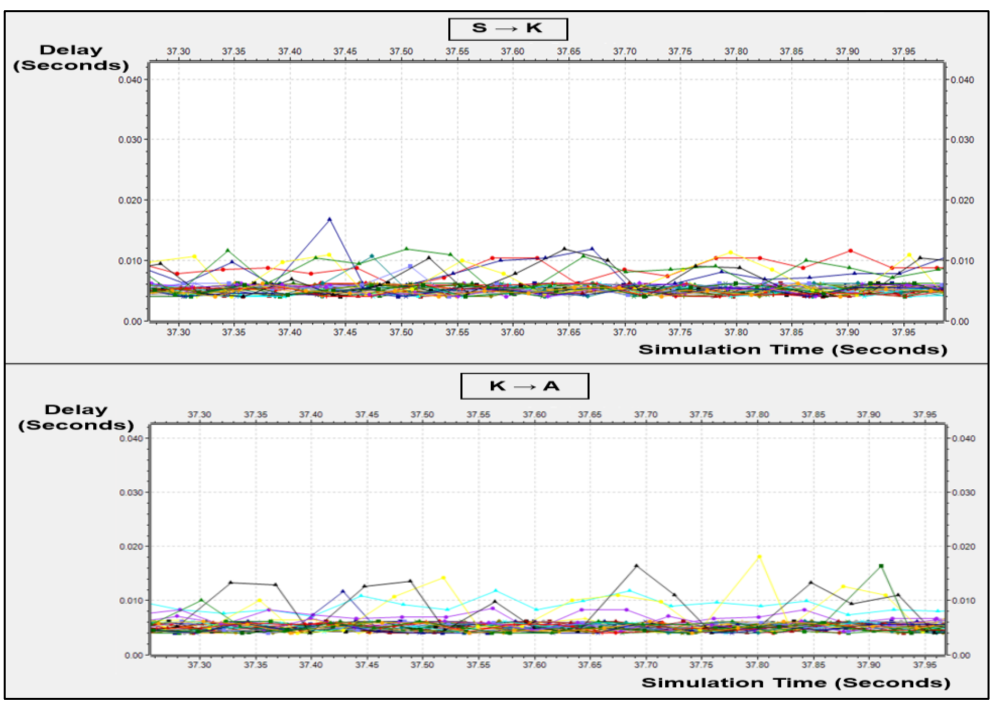

Fig 15. Sensor to Controller and Controller to Actuator delays under maximum interference packet size (15 SA Pairs - Vertical Interference Scenario)

Table III shows the corresponding control packets delays resulting for different interference data rates being exchanged by the alien nodes at different locations.

TABLE III. SUMMARY OF ZIGBEE DELAY RESULTS FOR DIFFERENT INTERFERENCE SCENARIOS (15 SA PAIRS)

Scenario		**Delay**		
		S→K *(ms)*	***K→A*** *(ms)*	***Total*** *(ms)*
Interference Free	0Bytes/sec	[8.66; 14.78]	[8.67; 15.63]	[17.34; 30.42]
Vertical	97Bytes/sec	[10.07; 17.36]	[11.14; 18.07]	[21.70; 35.43]
Vertical	100Bytes/sec	[10.86; 17.03]	[10.98; 19.16]	[21.69; 36.19]
Horizontal	97Bytes/sec	[10.07; 17.36]	[11.14; 18.07]	[21.70; 35.43]
Diagonal *Left to Right*	97Bytes/sec	[10.07; 17.36]	[11.14; 18.07]	[21.70; 35.43]
Diagonal *Right to Left*	97Bytes/sec	[10.07; 17.36]	[11.14; 18.07]	[21.70; 35.43]

It is important to note that all results were based on a 95% confidence analysis. Moreover, zero packet loss was guaranteed in all the above simulations. Looking at the results, it is evident that the delay is increased with increasing the packet size. This is expected given that the larger the packet size, the higher the bandwidth consumption and probability of collision with other packets sent from the sensors or the controller. To find the maximum tolerable interference that the system can handle, the packet size being exchanged by the alien nodes was gradually increased in size till the threshold is determined to meet deadline requirements. It is worth noting that the position of the two alien nodes whether horizontal, vertical or diagonal had minimum impact on the delay results of the system given the small area of the work cell.

3.4 WiFi Performance

The model is composed of the 15 S and A pairs communicating through 3 Access Points (Aps) with a single multichannel controller utilizing the IEEE 802.11 protocol with a data rate of 54 Mbit/sec as shown in Fig 16. The control load was divided over 3 non-interfering WiFi channels.

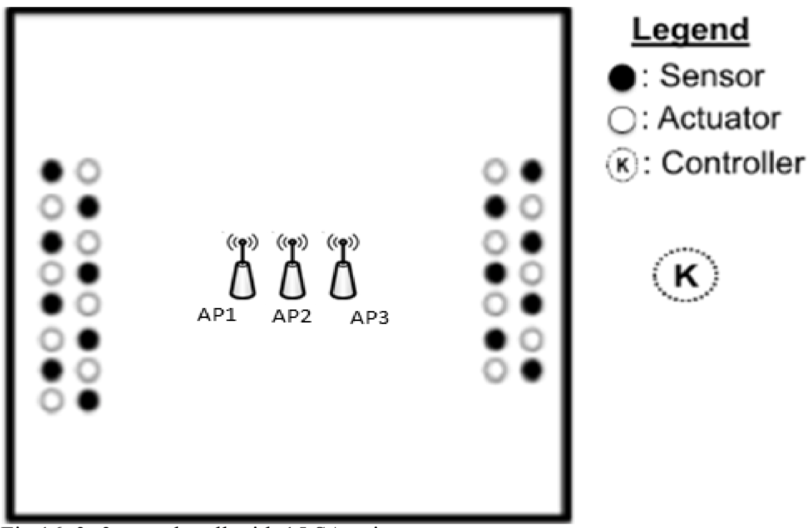

Fig 16. 3×3m work-cell with 15 SA pairs

3.4.1 Utilizing IEEE 802.11a

i. Interference Free Model

The same payload as in the ZigBee model was used in the WiFi model. Consequently, User Datagram Protocol (UDP) was used with a sampling period of 40ms. The packets sent by one sensor are also 25packets/sec. Since there are 30 sensors, the packets received by the controller are 750packets/sec. The controller sends 750packets/sec, which are split accordingly into 25packets/sec to each actuator.

Following a 95% confidence analysis, the upper bound of the maximum delay from any sensor to the controller and from the controller to any actuator was found to be 8.56ms and 7.27ms respectively. Therefore, the total delay demonstrated by the system was found to be 15.83ms with zero packet loss thus meeting the required system deadline. Fig. 17 shows the observed delays at the controller and an actuator node for the adjusted model (without external interference). The results shown are for 33 runs; each color is for a given run with a given seed.

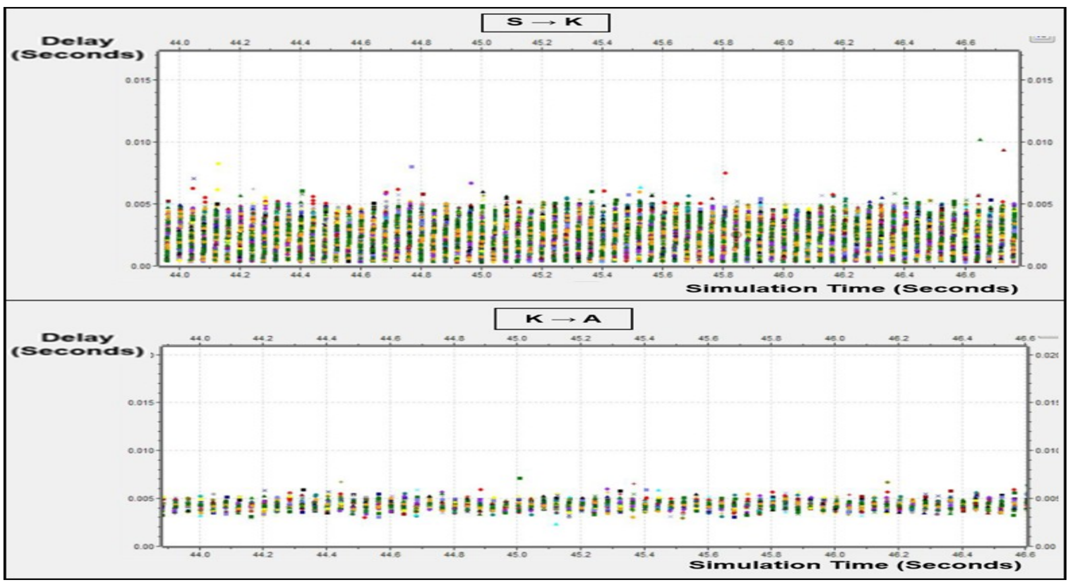

Fig 17. Sensor to Controller and Controller to Actuator delays – Interference free scenario

Looking at the results, it is evident that the delay of the WNCS utilizing IEEE 802.11a is significantly lower compared to a WNCS utilizing IEEE 802.15.4. This is expected given the higher bit rate of WiFi compared to Zigbee.

ii. Effect of External Interference

The model was then subjected to different interference scenarios. Four placement scenarios similar to the scenarios studied in the ZigBee model were studied where 6 alien nodes were introduced to subject the model to external ISM band interference. Every pair of nodes (in this case general purpose nodes communicating on the ISM band) communicate together on a separate channel corresponding to the channel distribution of sensors, controllers and actuators. That is, two nodes are exchanging data on the same channel as the corresponding SA nodes utilizing a UDP protocol sending a constant bit rate for the duration of the simulation as shown in Fig. 18.

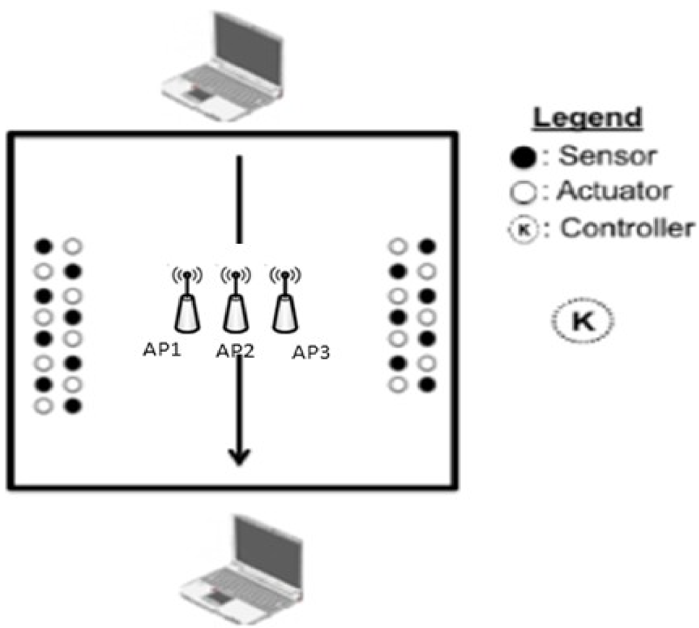

Fig 18. 3×3m work-cell with 15 SA pairs and vertical external interfering nodes

The size of the packet being exchanged by the alien nodes communication would increase the control system's end-to-end delay and/or cause packet loss. For a worst case analysis as in [10], the interfering nodes transmit power is set to 5mW compared to 1mW for the SA nodes.

The packet size being exchanged by the alien nodes was gradually increased and the proposed WNCS's performance is evaluated to determine the maximum interference the network can endure while ensuring that the deadline requirements are met with no packet loss.

The maximum interfering packet size that the network could handle while guaranteeing the required system benchmark of 36ms latency requirement was found to be 19600Bytes/sec with a measured end-to-end delay of 35.49ms for the control packets communicating in the system.

Fig. 19 to Fig. 22 show the observed delays at the controller node and at an actuator node under different interfering packet sizes for the vertical scenario. It is important to note that that the observed delays are less than the system deadline.

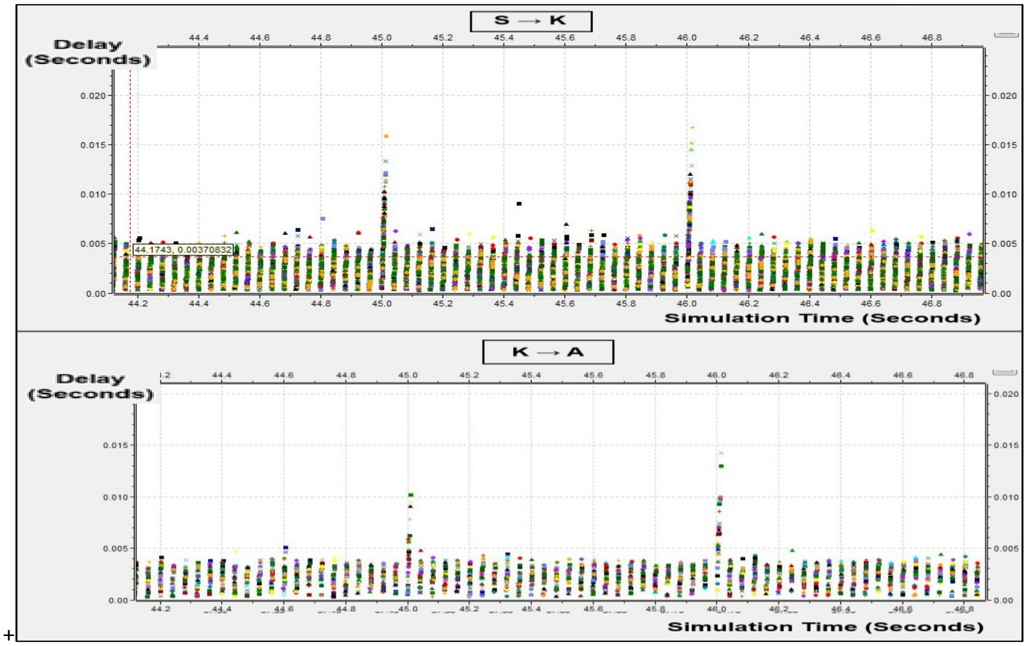

Fig 19. Sensor to Controller and Controller to Actuator delays under interference packet size 18000 bytes per second (15 SA Pairs – Vertical alien node placement)

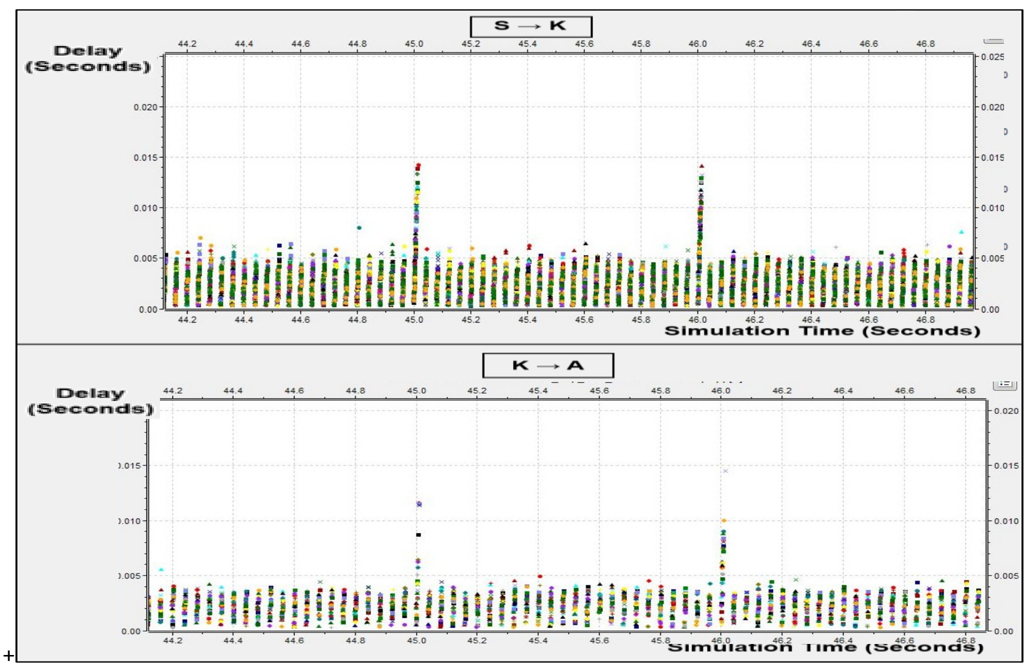

Fig 20. Sensor to Controller and Controller to Actuator delays under interference packet size 19000 bytes per second (15 SA Pairs – Vertical alien node placement)

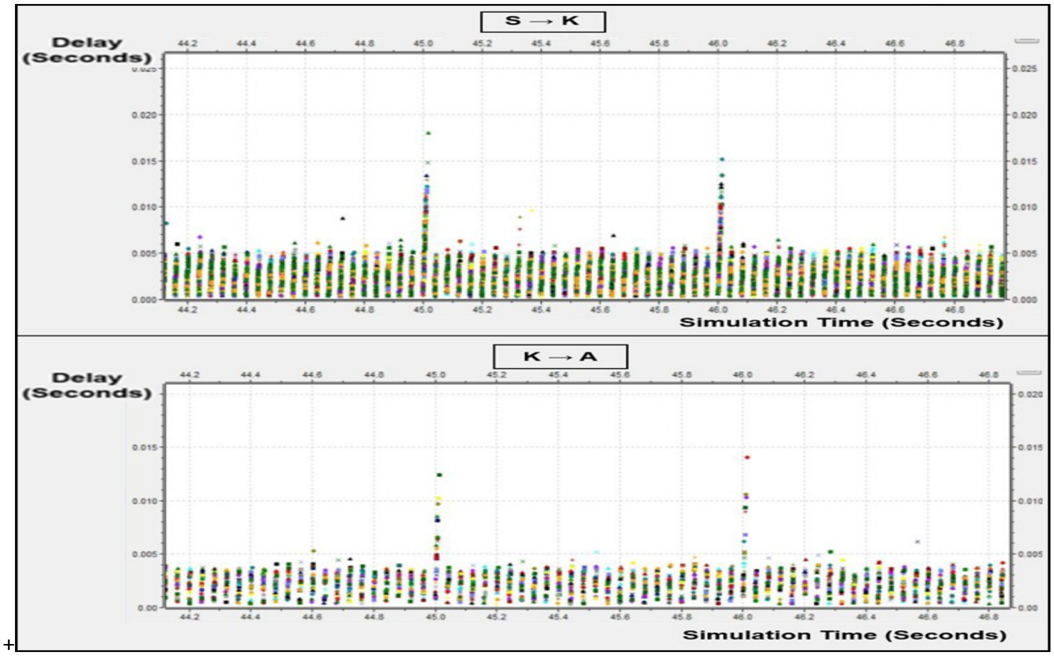

Fig 21. Sensor to Controller and Controller to Actuator delays under maximum interference packet size 19600 bytes per second (15 SA Pairs – Vertical alien node placement)

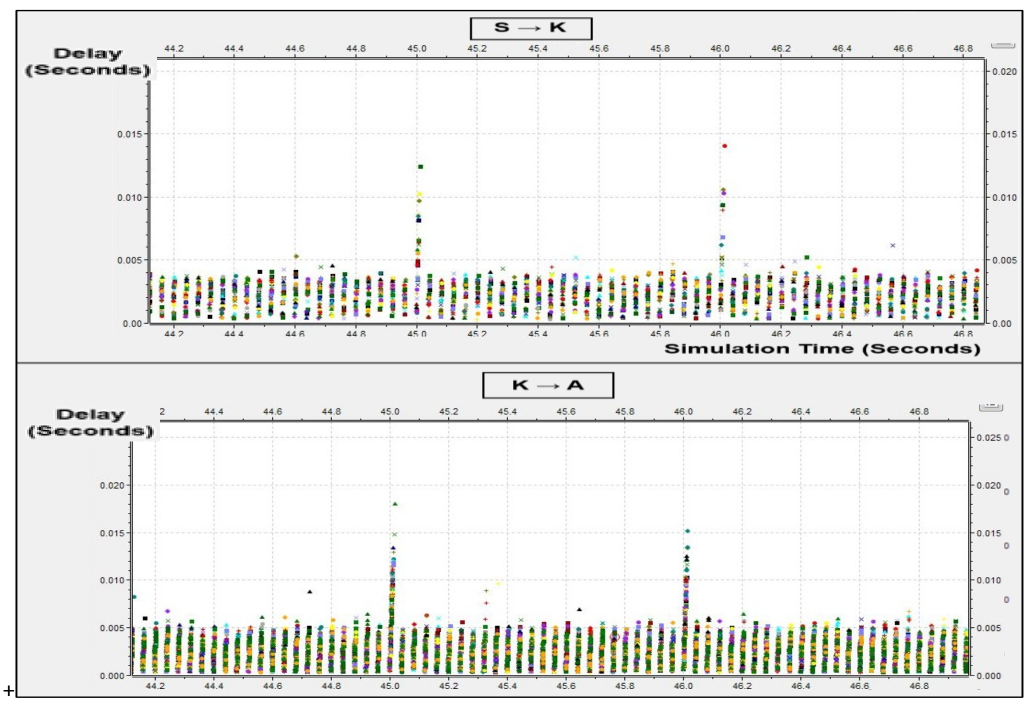

Fig 22. Sensor to Controller and Controller to Actuator delays under maximum interference packet size 19600 bytes per second (15 SA Pairs – Horizontal alien node placement)

Table II shows the corresponding control packets delays resulting for different interference data rates being exchanged by the alien nodes at different locations.

TABLE IV. SUMMARY OF 802.11A DELAY RESULTS FOR DIFFERENT INTERFERENCE SCENARIOS (15 SA PAIRS)

Scenario		**Delay**		
		***S→K** (ms)*	***K→A** (ms)*	***Total*** *(ms)*
Interference Free	0 Bytes/sec	[7.74; 8.56]	[6.74; 7.26]	[14.48; 15.83]
Vertical	18000 Bytes/sec	[16.02; 16.81]	[15.94; 16.63]	[31.96; 33.44]
Vertical	19000 Bytes/sec	[16.56; 17.48]	[16.24; 16.94]	[32.80; 34.42]
Vertical	19600 Bytes/sec	[16.87; 17.93]	[16.48; 17.56]	[33.35; 35.49]
Vertical	20000 Bytes/sec	[17.13; 18.60]	[16.79; 17.50]	[33.93; 36.11]
Horizontal	19600 Bytes/sec	[16.87; 17.93]	[16.87; 17.55]	[33.59; 35.49]
Diagonal *Left to Right*	19600 Bytes/sec	[16.66; 17.50]	[16.54; 17.52]	[33.20; 35.02]
Diagonal *Right to Left*	19600 Bytes/sec	[16.66; 17.50]	[16.54; 17.53]	[33.20; 35.03]

Looking at the results, it is clear that the higher the size of the packet, the larger the upper bound of the delay of the system. This is expected given that the higher size of the packet implies larger bandwidth sharing. It is also important to note that the placement of the two alien nodes either horizontal, vertical or diagonal had minimum impact on the delay results of the system given that the communication within the work cell is within a short range.

3.4.2 Utilizing IEEE 802.11b

i. Interference Free Model

The performance of the system was also evaluated using unmodified IEEE 802.11b in both the interference free scenario and also in case of applying external interference. The control load was divided over 3 non-interfering WiFi channels as shown in Fig. 23.

User Datagram Protocol (UDP) was used with a sampling period of 40ms. The packets sent by one sensor are also 25packets/sec. Since there are 30 sensors, the packets received by the controller are 750packets/sec. The controller sends 750packets/sec, which are split accordingly into 25packets/sec to each actuator.

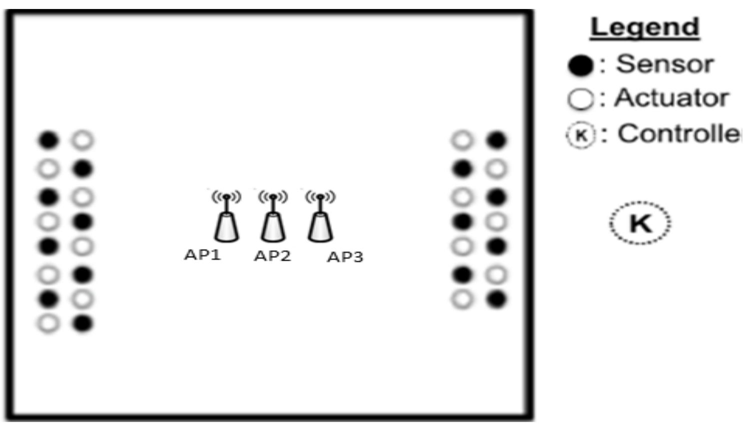

Fig 23. 3×3m work-cell with 15 SA pairs

Following a 95% confidence analysis, the upper bound of the maximum delay from any sensor to the controller and from the controller to any actuator was found to be 13.67ms and 12.5ms respectively. Therefore, the total delay demonstrated by the system was found to be 26.18ms with zero packet loss thus meeting the required system deadline. Looking at the delay results, this is expected as it is less than that of a system utilizing IEEE 802.11a given the higher bit rate of IEEE 802.11a compared to IEEE 802.11b. Also, the performance of this WNCS utilizing IEEE 802.11b in terms of delay is improved vs. the measured delay results of the WNCS utilizing IEEE 802.15.4 given the low bit rate of IEEE 802.15.4.

ii. Effect of External Interference

The model was then subjected to different interference scenarios. Four placement scenarios similar to the scenarios studied in the ZigBee and IEEE 802.11a models were studied where 6 alien nodes were introduced to subject the model to external ISM band interference. Every pair of nodes (in this case general purpose nodes communicating on the ISM band) communicate together on a separate channel corresponding to the channel distribution of sensors, controllers and actuators. That is, two nodes are exchanging data on the same channel as the corresponding SA nodes utilizing a UDP protocol sending a constant bit rate for the duration of the simulation as shown in Fig. 24.

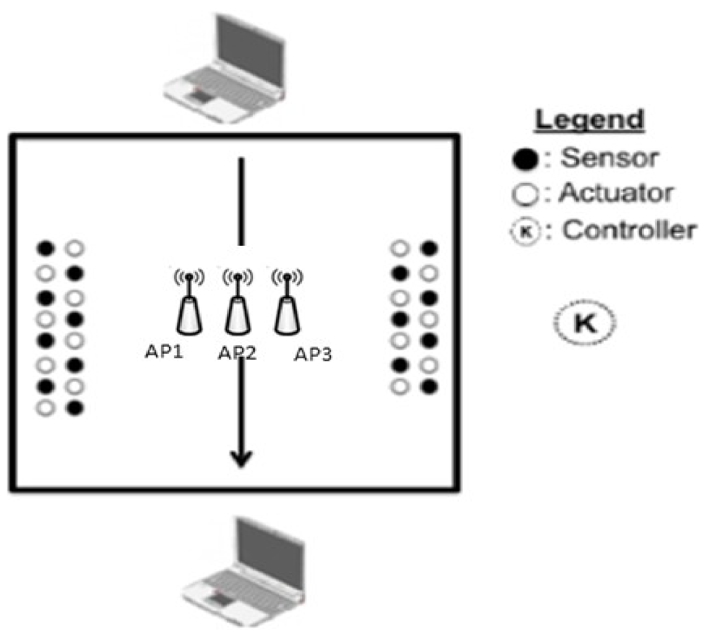

Fig 24. 3×3m work-cell with 15 SA pairs and vertical external interfering nodes

The size of the packet being exchanged by the alien nodes communication would increase the control system's end-to-end delay and/or cause packet loss. For a worst case analysis as in [10], the interfering nodes transmit power is set to 5mW compared to 1mW for the SA nodes. The packet size being exchanged by the alien nodes was gradually increased and the proposed WNCS's performance is evaluated to determine the maximum interference the network can endure while ensuring that the deadline requirements are met with no packet loss.

Following a 95% confidence analysis, the maximum interfering packet size that the network could handle while guaranteeing the required system benchmark of 36ms latency requirement was found to be 6500 Bytes/sec with a measured end-to-end delay of 34.8ms for the control packets communicating in the system as shown in Fig. 25.

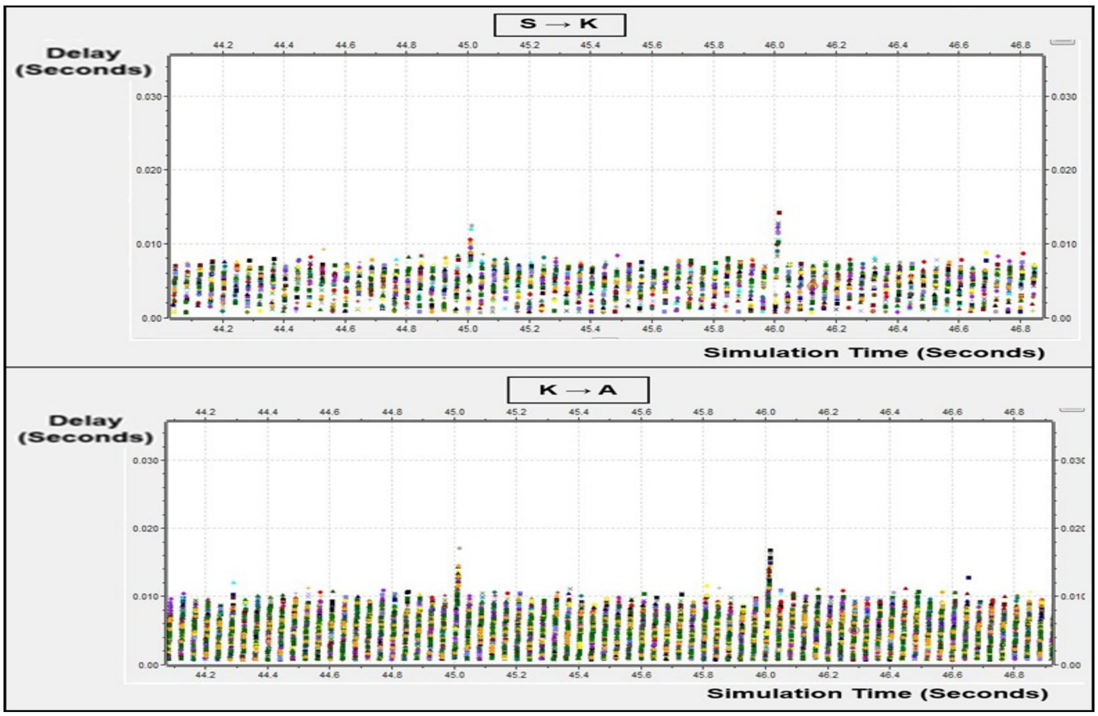

Fig 25. Sensor to Controller and Controller to Actuator delays under maximum interference packet size (15 SA Pairs – Vertical)

Table III shows the corresponding control packets delays resulting for different interference data rates being exchanged by the alien nodes at different locations.

TABLE V. SUMMARY OF 802.11B DELAY RESULTS FOR DIFFERENT INTERFERENCE SCENARIOS (15 SA PAIRS)

Scenario		**Delay**		
		S→K *(ms)*	***K→A*** *(ms)*	***Total*** *(ms)*
Interference Free	0 Bytes/sec	[12.78; 13.67]	[11.97;12.5]	[24.76;26.18]
Horizontal	97 Bytes/sec	[13.1;13.77]	[12.25;12.76]	[25.35;26.53]
Horizontal	200 Bytes/sec	[12.86;13.86]	[12.11;12.61]	[24.97;26.48]
Horizontal	400 Bytes/sec	[13.19;14.16]	[12.11;12.61]	[25.31;26.78]
Horizontal	1000 Bytes/sec	[13.04;13.88]	[12.32;12.76]	[25.36;26.63]
Horizontal	6000 Bytes/sec	[16.31;16.82]	[16.62;17.28]	[32.94;34.10]
Vertical	6500 Bytes/sec	[16.79;17.47]	[16.81;17.33]	[33.61;34.80]
Diagonal *Left to Right*	10000 Bytes/sec	[19.34; 20.30]	[19.42;19.93]	[38.77;40.24]
Diagonal *Right to Left*	10000 Bytes/sec	[19.34; 20.31]	[19.42;19.93]	[38.77;40.24]

The delay results in Table V show an increase with increasing the size of the packet being exchanged by the two alien nodes as expected. This is due to having the larger packet consume higher channel bandwidth. The position of two alien nodes with respect to the work cell either horizontally, vertically or diagonally had minimum impact on the delay results of the system given the relatively small size of the work cell.

Also, it is worth noting that the maximum tolerable interference that WNCS utilizing IEEE 802.11b can handle is lower than that of the WNCS utilizing IEEE 802.11a given the lower data rate of IEEE 802.11b up to 11 Mbps vs. 54 Mbps for IEEE 802.11a.

Chapter 4

Dual Protocol Performance

4.1 Model Description

The performance of the model is then evaluated when both networks IEEE 802.15.4 and 802.11a were operating simultaneously and independently. Each sensor and controller node transmits on both the WiFi and ZiGbee networks simultaneously. The two communication networks transmit in parallel, the first packet arriving on either of the two corresponding networks at the controller/actuator is used in the control process. So basically, the communication network is duplicated through applying the concept of fault tolerance on the communication network level. The motive for the Dual protocol is the implementation of a totally wireless WNCS that demonstrates the combined advantages of both the IEEE 802.15.4 protocol (which ZigBee is based on) without modifications being low cost and low power compared to other wireless technologies as well as the advantages of WiFi being increased bit rate and higher immunity to noise. It is important to note that there is no interference from one network on the other given both networks operation in different frequency bands theoretically. Four different interference scenarios are studied. In the first scenario, the performance of the WNCS is evaluated in an interference free model. In the second and third scenarios, the model was subjected to maximum tolerable interference packet size on the ZigBee network and WiFi network respectively as measured in the previous section. For the fourth scenario, the model is subjected to the maximum tolerable interference packet size on both networks simultaneously [24].

4.2 Analysis and Results

Table IV shows the corresponding packet delays resulting for subjecting different interference data rates being exchanged by the alien nodes on the two networks.

As evident from the results, the measured delay of the proposed redundant WNCS is closer to the delay demonstrated by the WNCS utilizing WiFi alone in case of interference free model or when the ZigBee network is subjected to interference. The measured delay of the proposed redundant WNCS is significantly lower compared to the measured delays of the WNCS utilizing either network individually in case the WiFi network is subjected to interference or when both networks are subjected to interference simultaneously.

TABLE VI. SUMMARY OF DELAY RESULTS FOR DIFFERENT INTERFERENCE SCENARIOS (15 SA PAIRS)

Scenario		**Delay**		
		S→K *(ms)*	***K→A*** *(ms)*	***Total*** *(ms)*
Interference Free	0Bytes/sec	[5.79; 6.40]	[5.92; 6.11]	[11.72; 12.51]
ZigBee Interference	97Bytes/sec	[5.76; 6.15]	[6.08; 6.15]	[11.83; 12.56]
WiFi Interference	20000Bytes/sec	[6.58; 7.89]	[7.26; 8.90]	[13.85; 16.79]
ZigBee Interference and WiFi Interference	97Bytes/sec and 20000Bytes/sec	[6.70; 8.18]	[7.38; 9.25]	[14.08; 17.43]

Figures 26 to 29 compare the upper bound delays of dual protocol WNCS compared to single protocol WNCS under different interference scenarios. As evident from the results, the proposed dual technique has better performance since it gets the minimum delay at each instance since the fastest corresponding packet to arrive on either the WiFi or ZigBee network is used in the control process. Dual protocol performance approaches the performance of WiFi in case of interference free Zigbee interference scenarios. This is expected given the higher bit rate of WiFi vs. Zigbee. Dual protocol performance is improved as well in case of WiFi or both Zigbee and WiFi networks are subjected to interference.

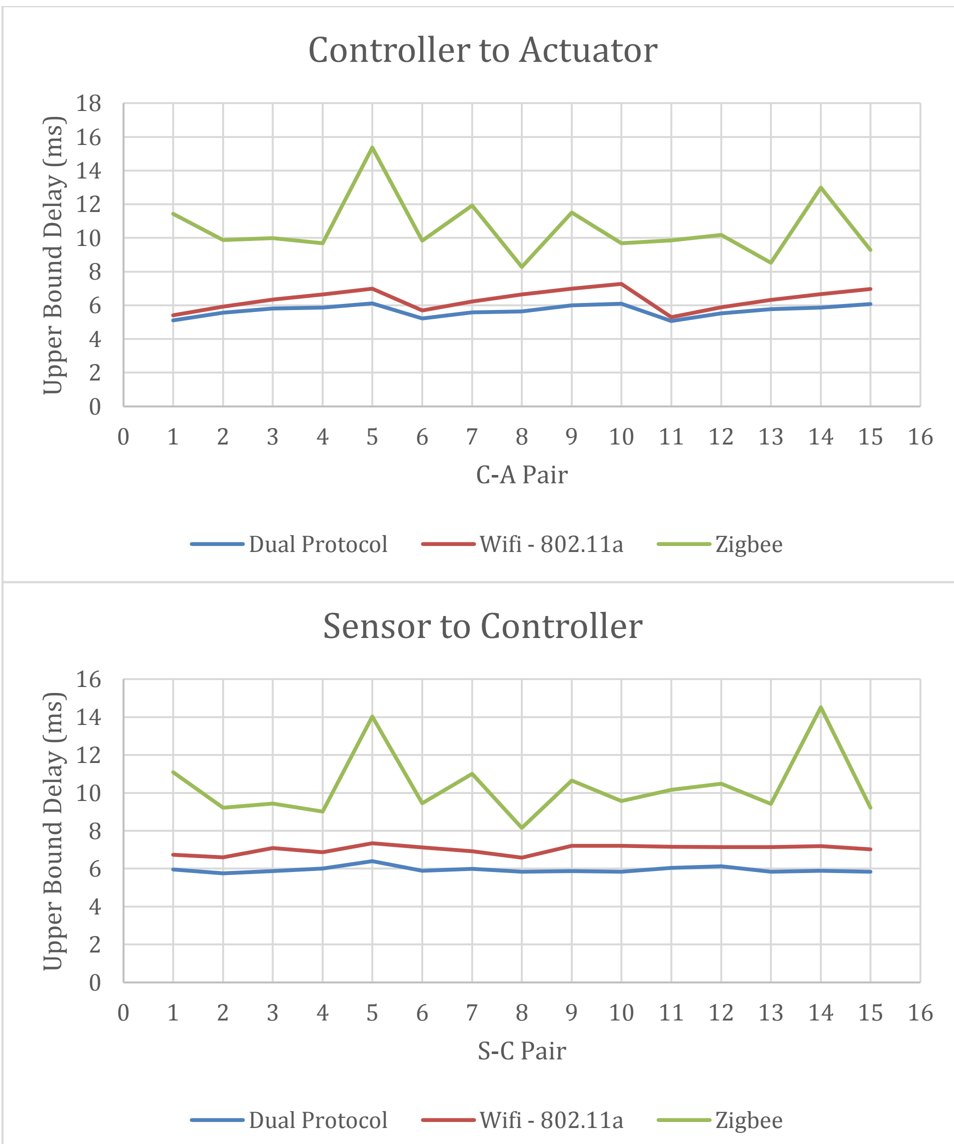

Fig 26. Dual Protocol Performance interference free environment

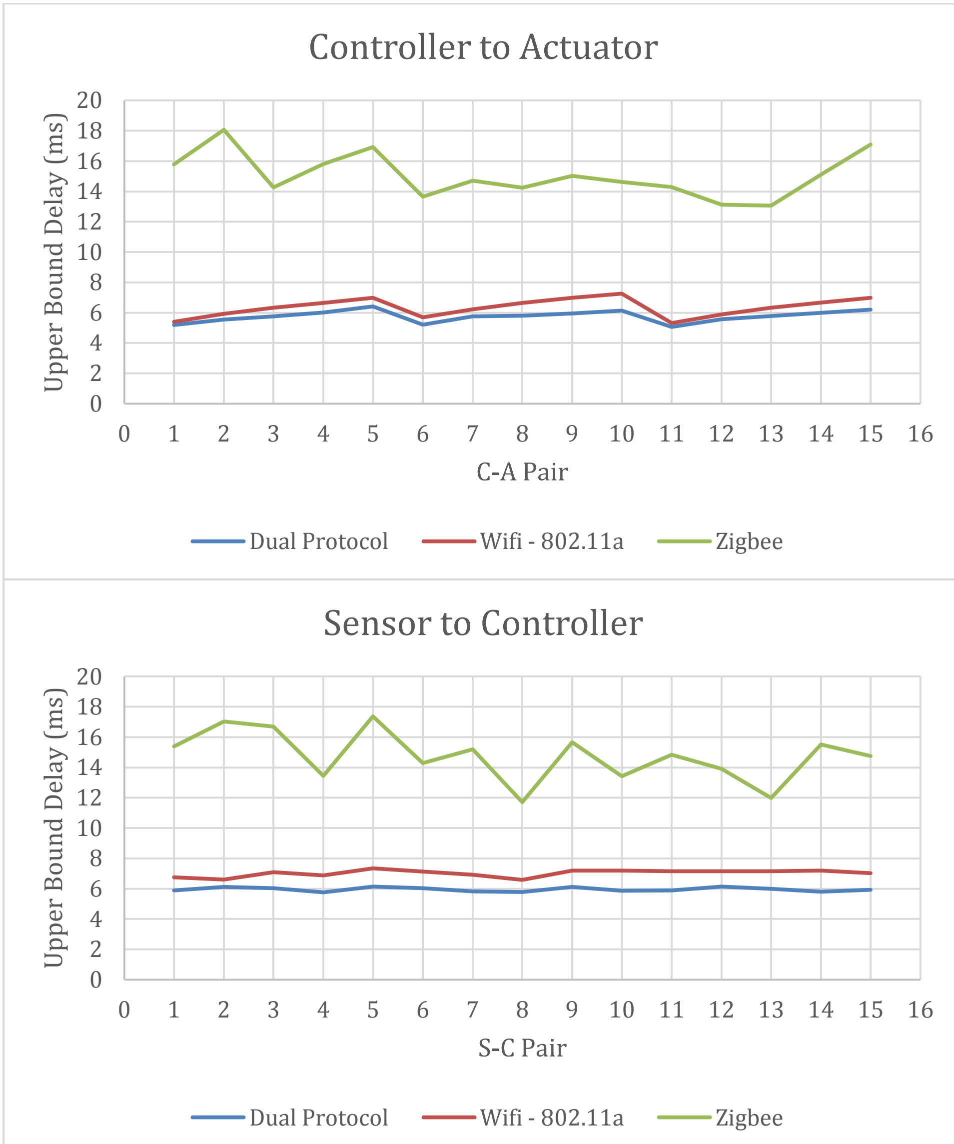

Fig 27. Dual Protocol Performance when ZigBee network only is subjected to max interference

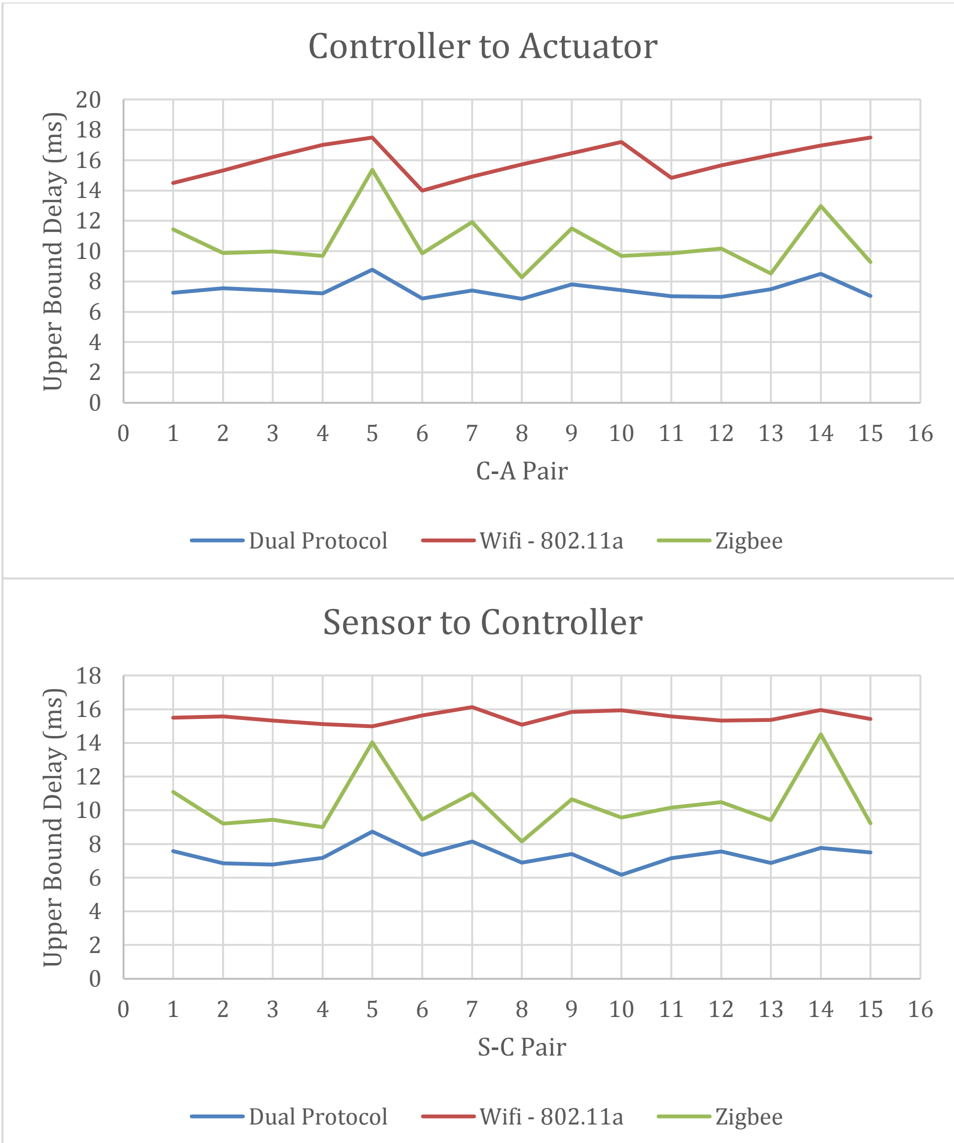

Fig 28. Dual Protocol Performance when WiFi network only is subjected to max interference

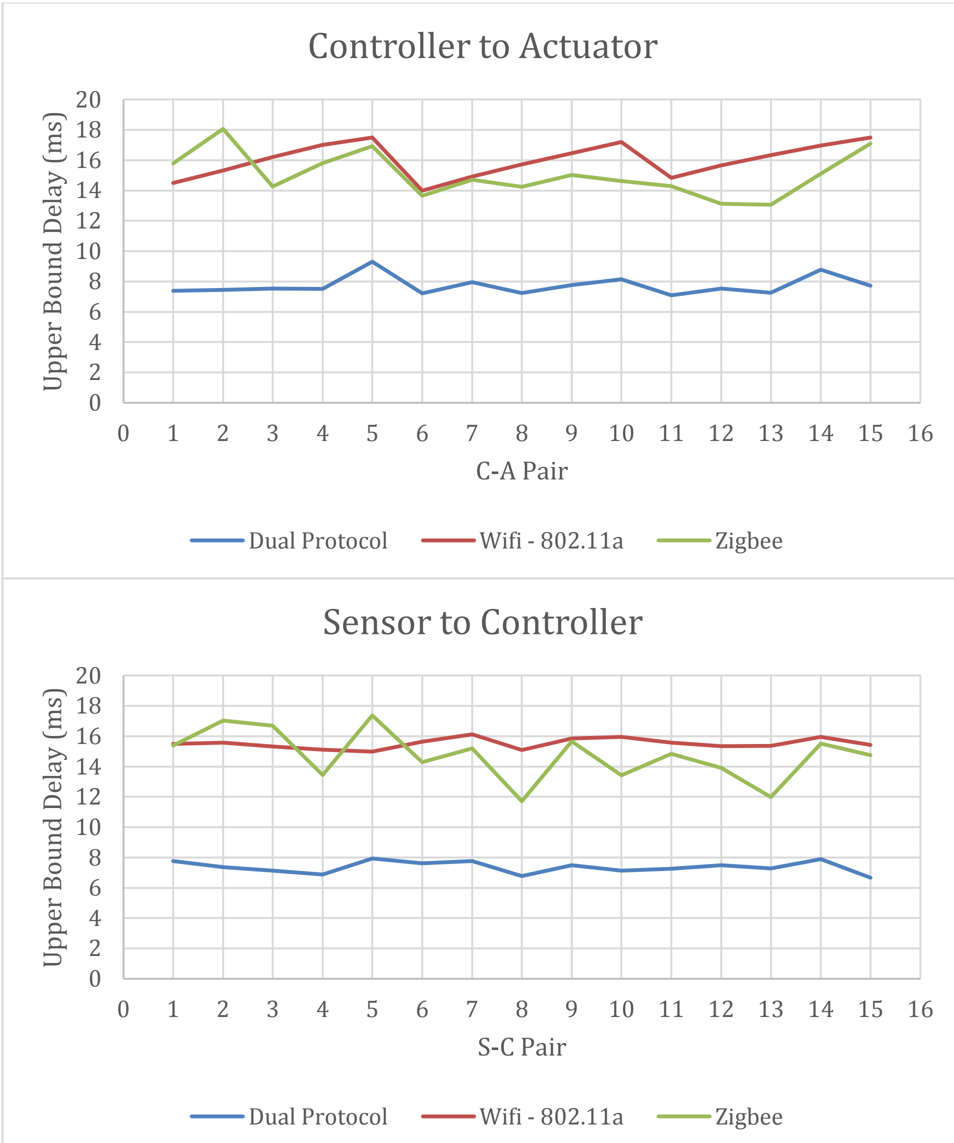

Fig 29. Dual Protocol Performance when both ZigBee and WiFi networks are subjected to max interference

As shown in Fig. 26, Dual Protocol performance approaches the performance of WiFi with slight improvement in an interference free environment. This is expected given the higher bit rate of WiFi compared to ZigBee. This also applies to the scenario where interference is affecting the 2.4 GHz range hitting the ZigBee network, the Dual Protocol performance approaches the performance of WiFi with slight improvement as shown in Fig. 27. However, in case we have interference affecting the 5.8 GHz range only hitting the WiFi network, the Dual Protocol demonstrates roughly 45% improved delay results vs. the single protocol performance as shown in Fig. 28, the reason for this improvement in performance is due to the Dual protocol system taking the minimum delay at each time instant given that first packet arriving on either of the two corresponding networks at the controller/actuator is used in the control process. In case we have interference affecting both the 2.4 and 5.8 GHz range, the performance of the Dual protocol system is significantly superior demonstrating roughly roughly 48% improved delay results vs. the single protocol system performance as shown in Fig. 29. Again, this is attributed to the Dual protocol system taking the minimum delay at each time instant given that first packet arriving on either of the two corresponding WiFi or ZigBee networks at the controller/actuator is used in the control process.

Chapter 5
Conclusions

Wireless NCSs (WNCSs) are becoming more popular due to less cabling which simplifies installation, maintenance and allows for node mobility. However, wireless networks being non-deterministic in nature and prone to external interference dictating strict reliability and deadline requirements to ensure industrial feasibility of WNCS. Networks utilizing parallel redundancy of two different protocols for communication operating on different frequency bands demonstrate improved performance compared to networks utilizing a single protocol.

In this study, a simulation model was developed using OMNET to study the extent of improvement in performance of WNCS utilizing the IEEE 802.15.4 protocol (which the ZigBee protocol is based on) and IEEE 802.11 protocol (WiFi). The performance of the WNCS model was studied when operating on ZigBee and WiFi alone in an interference free environment and it was shown that the total end-to-end delay from any sensor to the controller then from the controller to any actuator is 30.41ms for ZigBee 15.83ms for WiFi. Thus the model satisfied the overall 36ms benchmark end-to-end deadline including all types of transmission, encapsulation, de-capsulation, queuing and propagation delays with zero packet loss for both the ZigBee case and the WiFi case. The WNCS operating on either ZigBee or WiFi network was then subjected to an interference study for harsh environment operation in the presence of 30 and 6 alien nodes respectively communicating across the workcell at various positions to determine the worst-case scenario in the presence of external ISM band interference. It was found that the model can withstand interference up to 97Bytes/sec per channel in case of ZigBee while maintaining a maximum total delay of 35.43ms and 19600Bytes/sec per channel in case of WiFi while maintaining a maximum total delay of 33.72ms satisfying all deadline requirements while maintaining zero packet loss. The proposed WNCS utilizing both ZigBee and WiFi in parallel was then studied in case of different interference scenarios on either one or both of the two networks. It was shown that in case of interference free model or in case of maximum interference affecting the 2.4GHz range in which the

ZigBee network operates, the performance of the parallel system approaches the performance of the WiFi case with a slight improvement demonstrating total maximum delays of 12.51ms and 12.56ms respectively with zero packet loss. In case the proposed WNCS was subjected to interference in 5.8GHz range only or in both the 2.4 and 5.8 GHz ranges as well, the parallel system demonstrates roughly 48% improved delay results with total maximum delays of 16.79ms and 17.43ms respectively with zero packet loss. It is important to note that all the results presented in this study are based on 95% confidence analysis.

References

[1] F.L-Lian, J.R. Moyne and D.M. Tilbury, "Networked Control Systems Toolkit: A Simulation Package for Analysis and Design of Control Systems with Network Communication," Tech. Rep., UM-ME-01-04, July 2001. Available: http://www.eecs.umich.edu/~impact

[2] T. Skeie, S. Johannessen and C. Brunner, "Ethernet in Substation Automation," IEEE Control Syst. Vol. 22, no. 3, June 2002, pp. 43-51.

[3] J. Nilsson, Real-Time Control Systems with Delays, PhD thesis, Department of Automatic Control, Lund Institute of Technology, Lund, Sweden, 1998.

[4] J.P. Thomesse. "Fieldbus Technology in Industrial Automation", Proceedings of the IEEE, Vol. 93, No. 6, June 2005, pp. 1073-1101.

[5] J.D. Decotignie. "Ethernet-Based Real-Time and Industrial Communications," Proceedings of the IEEE, vol. 93, No. 6, June 2005, pp. 1102-1117.

[6] Bosch. "CAN Specification Version 2.0" ISO 11898, 1991.

[7] F. L. Lian, J.R. Moyne and D.M. Tilbury, "Performance Evaluation of Control Networks: Ethernet, ControlNet, and DeviceNet," IEEE Control Systems Magazine, Vol. 21, No. 1, pp. 66-83, February 2001.

[8] R. Steigmann and J. Endresen, "Introduction to WISA: WISA – Wireless Interface for Sensors and Actuators," White paper, ABB, July 2006.

[9] T.K. Refaat, R.M. Daoud, H.H. Amer and E.A. Makled, "WiFi implementation of Wireless Networked Control Systems," Proceedings of the 7th IEEE International Conference on Networked Sensing Systems INSS, Kassel-Germany, June 2010, pp. 145-148.

[10] E.E. Abdel Reheem, Y.I. El Faramawy, H.H. Halawa, M.A. Ibrahim, A. Elhamy, T.K. Refaat, R.M. Daoud and H.H. Amer, "On the effect of interference on Wi-Fi-based Wireless Networked Control Systems," Proceedings of IEEE IET 8th International Symposium on Communication Systems, Networks and Digital Signal Processing CSNDSP, Poznan, Poland, July 2012, pp. 1-4.

[11] D. Gessner, J. Proenza, M. Barranco and P. Portugal, "Towards a reliability analysis of the design space for the communication subsystem of FT4FTT," Proceedings of

the IEEE International Conference on Emerging Technologies and Factory Automation ETFA, Barcelona, Spain, September 2014, pp. 1-4.

[12] S. Kehrer, O. Kleineberg and D. Heffernan, "A comparison of faulttolerance concepts for IEEE 802.1 Time Sensitive Networks (TSN)," Proceedings of the IEEE International Conference on Emerging Technologies and Factory Automation ETFA, Barcelona, Spain, September 2014, pp.1-8.

[13] M. Rentschler and P. Laukemann; "Performance Analysis of Parallel Redundant WLAN," Proceedings of the IEEE International Conference on Emerging Technologies and Factory Automation ETFA, Krakow, Poland, September 2012, pp. 1-8.

[14] M. Short, "Simple bounds on deadline failure probabilities in faulttolerant real-time networks," Proceedings of the IEEE International Conference on Emerging Technologies and Factory Automation ETFA, Barcelona, Spain, September 2014, pp. 1-7.

[15] M. Barranco, F. Pozo and J. Proenza, "A model for quantifying the reliability of highly-reliable distributed systems based on fieldbus replicated buses," Proceedings of the IEEE International Conference on Emerging Technologies and Factory Automation ETFA, Barcelona, Spain, September 2014, pp. 1-8.

[16] A. Thekkilakattil, R. Dobrin and S. Punnekkat, "Bounding the effectiveness of temporal redundancy in fault-tolerant real-time scheduling under error bursts," Proceedings of the IEEE International Conference on Emerging Technologies and Factory Automation ETFA, Barcelona, Spain, September 2014, pp. 1-8.

[17] J. Proenza, M. Barranco, G. Rodriguez-Navas, D. Gessner, F. Guardiola and L. Almeida, "The design of the CANbids architecture," Proceedings of the IEEE International Conference on Emerging Technologies and Factory Automation ETFA, Krakow, Poland, September 2012, pp. 1-8.

[18] A.E. Vallestad, "WISA becomes WSAN – from proprietary technology to industry standard," Wireless Summit 2012, OsloNorway, April 2012.

[19] D. Martinez, P. Balbastre, F. Blanes, J. Simo and A. Crespo, "Design procedure to minimize power consumption and delays in WSAN", Proceedings of the IEEE

International Conference on Emerging Technologies and Factory Automation ETFA, Bilbao, Spain, September 2010, pp.1-8.

[20] J. Singh and D. Pesch, “A energy efficient TDMA scheduling scheme for large-scale WSAN”, Proceedings of the International Conference on Computer Engineering and Technology ICCET, Chengdu-China, April 2010.

[21] J.D. Decotignie. “Ethernet-Based Real-Time and Industrial Communications,” Proceedings of the IEEE, vol. 93, No. 6, June 2005.

[22] G. Afifi, H.H. Halawa, R.M. Daoud and H.H. Amer, “A ZigBee based Industrial WLAN”, Proceedings of the 10th IEEE International Conference on Computer Engineering and Systems, Cairo, Egypt, December 2015.

[23] D. Yang, Y. Xu and M. Gidlund, "Coexistence of IEEE802.15.4 based networks: A survey," IECON 2010 - 36th Annual Conference on IEEE Industrial Electronics Society, Glendale, AZ, 2010, pp. 2107-2113.

[24] G. Afifi, H.H. Halawa, R.M. Daoud and H.H. Amer, “Dual Protocol Performance using WiFi and ZigBee for Industrial WLAN”, Proceedings of the 24th Mediterranean Conference on Control and Automation, Athens, Greece, June 2016.

[25] IEEE Std 802.11

[26] IEEE Std 802.15

[27] IEEE Std 802.15.4

[28] D. Dzung, J. Endresen, C. Apneseth and J. E. Frey, “Design and Implementation of a Real-Time Wireless Sensor/Actuator Communication System,” Proceedings of the 10th IEEE International Conference on Emerging Technologies and Factory Automation, ETFA, Catania, Italy, September 2005.