Received: 4 November 2022 | Revised: 27 March 2023 | Accepted: 28 May 2023

IET Communications

DOI: 10.1049/cmu2.12640

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

Design and implementation of a wireless CAN module for marine engines using ZigBee protocol

Akpojoto Siemuri | **Tobias Glocker** | **Mike Mekkanen** | **Kimmo Kauhaniemi** | **Timo Mantere** | **Mohammed Elmusrati**

School of Technology and Innovations, University of Vaasa, Finland

Correspondence
Akpojoto Siemuri, University of Vaasa, Fabriikki F454 (Digital Economy), Wolffintie 34, Vaasa 65200, Finland.
Email: akpo.siemuri@uwasa.fi

Funding information
Regional Council of Ostrobothnia; Smart Energy Systems Research Platform (SESP), School of Technology and Innovations, University of Vaasa; Wärtsilä Oyj Abp

Abstract

This paper describes the design and implementation of a wireless control area network (CAN bus) protocol for communication between the smart NOx (nitrogen oxide) sensor on diesel engines and the engine control unit (ECU). In this research, the approach taken is based on a case study of Wärtsilä's smart NOx sensor on a W4L20 diesel engine with the objective of replacing the wired CAN protocol with a wireless CAN communication node. In the current setup, the smart NOx sensor is connected to the engine control unit (ECU) with a wired CAN bus connection. The XBee module, which uses the ZigBee (IEEE 802.15.4) technology was used in the design and implementation of the wireless CAN prototype. With the emergence of 5G networks and the era of IoT, the topic of wireless industrial automation becomes essential in the modern industry. In addition to the great advantages and opportunities that the use of wireless nodes has in automation systems, there are many real challenges. The practical design challenges have been addressed in this paper.

1 | INTRODUCTION

Modern industries' development has been rapid, and this has been influenced by the continuous growth in the global economy. Therefore, data collection, analysis, and integration have become essential pillars for the new industrial structure. The need to have real-time information in automation systems on all levels is extremely important. In wireless automation, one crucial step is to decide on the required wireless communication protocol for a certain automation system. The decision is made based on automation requirements such as latency, data rate, coverage distance, reliability (outage and packet losses), costs, security etc. Therefore, studying some well-known wireless communication solutions is crucial in achieving reliable and flexible data transfer [1]. This paper investigates the feasibility of implementing a reliable, secure, and fault-tolerant wireless communication between the smart NOx sensor on ship engines and the Speedgoat (real-time rapid prototyping tool) or engine control module (ECM). In the current setup, the smart NOx sensor is connected to the engine control unit (ECU) with a wired control area network (CAN bus) connection. Data is transmitted using the SAE J1939 protocol (Society of Automotive Engineers standard) which is built on top of CAN Networks. SAE J1939 is developed specifically for use in heavy-duty environments, with an emphasis on achieving reliable and fault-tolerant communication. In this research, the approach taken is based on a case study of Wärtsilä's smart NOx sensor on a W4L20 diesel engine with the objective of replacing the wired CAN bus with a wireless CAN node. Therefore, a wireless CAN module has been designed.

The purpose of this research is to investigate the implementation possibility and security implications when using wireless communication in the CAN network. This is to achieve remote monitoring of marine engine performance for a more efficient diagnostics activity and coordination of the operation of the separate subsystems. With the findings from this research, work will be extended to other types of sensors on the ship engine, and managing multiple sensors will be addressed.

The application of wireless CAN networks in maritime vessels is quite a new area of research different from the common applications such as railway applications seen in streetcars, trams, undergrounds, light railways, long-distance trains, and

lifts and escalators which use embedded CAN networks. The introduction of wireless networks in marine engines makes for a more efficient diagnostics activity and coordination of various separate subsystems' operations. To the best of our knowledge, this paper is the first to investigate the application of wireless CAN in maritime technology for monitoring and controlling marine engines using practically oriented research on ZigBee and CAN (except for our own ZigBee-CAN related research work [2]). Therefore, we want to raise awareness and discuss the possibility of integrating ZigBee and CAN technologies for application in the communication, monitoring, and control of marine vessels and technology. The design steps, implementation, and performance analysis are discussed in the next sections.

1.1 | Related works

A study of related works shows the application and implementation of CAN in several domains such as industrial automation and robotics besides automotive (for which is it commonly known). Its latest application has been in precision farming applications [3], where ZigBee is used with CAN bus for real-time monitoring of agricultural variability. The integration of the wired CAN Bus and ZigBee communication was designed to extract the data regarding the geographical coordinate from the global positioning system (GPS) receiver with the help of ZigBee communication and the data is sent to a central computer with the help of the wired CAN bus. The aim is to adapt the ZigBee messages to the CAN bus and therefore, reduce the use of wires. The results show that the system was capable of sending GPS data through ZigBee and the ZigBee message sent via CAN bus. It was also used to collect and merge the CAN messages with the help of a central computer.

In ref. [4], the combination of ZigBee and CAN bus was applied to the coal mine safety monitoring and alert system. The aim is to improve the level of monitoring production safety and reduce accidents in the coal mine. According to this paper, the use of ZigBee technology was to reduce the cost and improve the speed of communication between the base station and sync nodes. The use of ZigBee and CAN bus for non-safety-critical applications of vehicles was investigated in ref. [5]. A gateway was designed to ensure interoperability between the conventional CAN bus and the ZigBee wireless network. Transmission reliability was ensured through repeated transmission, taking into account the vehicle environment where wireless local area network (WLAN) interference exists.

Another application is in home network protocol [6–8]. From ref. [6], the application of CAN was done for direct load control programs for home automation. The purpose of this system was to allow its users to monitor and control the use of individual loads in their homes, thereby helping in the deregulation of the electricity markets by providing flexibility on the demand side. The entire system has three subsystems, with each subsystem having its unique function. The subsystems are namely a sub-system of interaction, a subsystem of measurement, and a subsystem of the drive. The data transmissions were achieved by making use of the CANopen system.

In ref. [7], the research stated that most building automation technologies do not offer sufficient bandwidth applicable for voluminous data required in many home automation needs. Furthermore, such technologies have not yet provided solutions that are robust against harsh environments as addressed by CAN. CAN advantage of being cost-effective, and resilient to extreme heat makes it an attractive solution. It also has high signalling rates suitable for the fast transmission of data from one node to another.

Othman et al. in ref. [8] presented a stand-alone single-chip embedded system that has been equipped with five CAN port used for the monitoring and control of home appliances locally. Each of the five CAN ports is connected to a separate home appliance. The CAN devices are said to be able to send and receive data in contrast to previous works, where devices can only receive messages sent from a master. The proposed system can communicate to the GPRS network using a GPRS modem which allows for the system to communicate with a user through the public wireless mobile network and the home internet.

Equipment in intensive care units, operating rooms, and several other healthcare equipments, including lights, tables, cameras, X-ray machines, and patient beds make use of CAN networks [9].

The CAN protocol is applied for a home automation system to design a WCAN-based home automation system [10]. This proposed system comprises many WCAN nodes located in certain places around the house and these nodes are connected to electrical appliances in the home. The system also has a central controller server. The controller server is used as the command center by sending commands to all the nodes in the network and can receive commands from the user device. In this application, a smart controller is used to communicate with the controller server making use of a Bluetooth connection. When the controller server receives the command, it transmits messages across the network to all the nodes. The message identifier embedded in the token influences what the receiving sensor nodes does with the messages, it will either store the message for further processing or simply transmit the message back into the network. If the message is kept for further processing, this helps in performing tasks or actions with the connected household appliances.

The discussions in ref. [11], present the point that in the automotive industry, embedded control has evolved from stand-alone systems to highly integrated and networked control systems. The networking of electro-mechanical subsystems makes it possible for the modularization of various functionalities and hardware, thereby, facilitating reuse and adding capabilities. The functions of the ECU are the control of the engine, turbo, fan etc. however, it is also used for CAN communication. The combination of networks and mechatronic modules leads to the possibility of the reduction of the need for cabling and the number of connectors, which in turn, facilitates production and increases reliability. The use of CAN is seen in the US Navy boat where the Navy developed a distributed electronics architecture denoted as SeaCAN and had it installed in

all new seaborne targets and has been retrofitted into several older targets. It has a SeaCAN architecture for a 7 m remotely controlled rigid-hull inflatable boat. An autopilot based on a feedback control loop closed over the network is implemented by the system, which comprises the nodes rudder feed-back, GPS receiver, pitch/roll/heading, command/control, and two engine throttle nodes [12].

In ref. [13], intra vehicle wireless sensor network is employed utilizing Bluetooth low energy (BLE) within vehicular ad hoc network to achieve a low-cost and energy-efficient communication between sensor nodes and ECU. In this paper [14], BLE and CAN bus have been investigated based on their use in the communication of raw engine data between ECUs and sensors, and ECU and onboard unit (OBU) with respect to energy efficiency, throughput, latency, and coverage area. The research combined both technologies in using the CAN bus to transmit the time-critical sensor data to the ECU while energy-efficient BLE is used to transmit less critical sensor data to the ECU. This hybrid prototype was proposed to provide improved results in terms of reliability, robustness, and cost-efficiency. It was observed that the proposed BLE-based system showed very high successful packet delivery ratios both in static and moving scenarios of the vehicles with acceptable average received signal strength indicator (RSSI) values of at least −10 dBm.

In this paper, a wireless CAN module has been designed. The introduction of wireless networks in marine engines will make it possible for a more efficient diagnostics activity and the coordination of the operation of the separate subsystems. The application in maritime vessels is quite a new area of research different from the common applications such as railway applications seen in streetcars, trams, undergrounds, light railways, long-distance trains, and lifts and escalators which use embedded CAN networks. As far as we know, there is no other paper that investigates the application of wireless CAN in maritime technology for monitoring and control of engines using practically oriented research on ZigBee and CAN (except for our own ZigBee CAN-related research work [2]). Therefore, we want to raise awareness and a discussion about the possibility of integrating ZigBee and CAN technologies for application in remote monitoring and control in marine technology.

2 | MATERIALS AND METHODS

This section presents the material and methods used in this research.

2.1 | Smart NOx sensor

The smart NOx is a sensor that measures the oxygen (O_2) and nitrogen oxide (NOx) content in the exhaust of combustion engines. Oxygen is measured as a percentage, while the NOx concentration is measured in parts per million (ppm) [15]. Nitrogen Oxides (NOx) is a generic term for a group of poisonous, highly reactive gases of which two occur naturally, namely nitric oxide (NO) and nitrogen dioxide (NO_2). The combustion of fossil fuels is the most common source of NOx emissions. The amount of emission depends on the air-fuel mix ratio as well as the amount of nitrogen in the fuel. At high temperatures and conditions that encourage oxidation NOx formation in combustion is favoured. (NO_2) has adverse effects on human health and at high concentrations, it can lead to the inflammation of the airways. NO_2 is also responsible for the formation of secondary particulate aerosols and ozone (smog (O_3)) in the atmosphere. These are noticeable air pollutants because of their severe impacts on human health [12].

2.2 | Speedgoat and engine control module (ECM)

The Speedgoat applies real-time systems with Simulink real-time from MathWorks to various applications across many industries such as, in laboratories, on the field, in classrooms, or embedded in machinery. Speedgoat solutions and Simulink are seamlessly integrated and allow for a fast test run of Simulink software designs with hardware [14].

The engine control module (ECM), also called engine control unit (ECU), is a kind of electronic control unit that manages the control of a series of actuators on an internal combustion engine to ensure that the engine's performance is optimal. This is done by reading the values from all the sensors within the engine bay and interpreting the data using multidimensional performance maps (referred to as lookup tables) and adjusting the engine actuators accordingly [16]. The diesel engine used in this research is a medium-speed W4L20 diesel engine. The engine produces approximately 1 MW of power and it is paired with an ABB generator [17]. This combustion engine is located in the Vaasa Energy Business Innovation Center (VEBIC) laboratory. VEBIC is a new research and innovation platform hosted by the University of Vaasa. The VEBIC environment has two laboratories namely, the internal combustion engine laboratory and a separate but related fuel development laboratory. It also has a program for energy and sustainable development research projects [18].

The impact of the diesel engine on wireless protocols was tested to see if issues like vibrations of the engine would have negative impacts on communication and data transmission. From the test done, we investigated for packet loss, and signal availability while running the engine to evaluate the wireless CAN module. The choice of using a diesel engine is influenced by common industry standards; where most ship and generator engines use a reciprocating diesel engine. The case study was done on a Wärtsilä W4L20 diesel engine in collaboration with Wärtsilä a company based in Finland and known for its business in marine technology [19].

2.3 | CAN protocol and the wireless module

In this section, the required wireless module is discussed. The selection is based on the automation requirements and available wireless standards.

2.3.1 | Controller area network (CAN)

CAN is a solution for automation industries and the CAN protocol is used in systems that needs to transmit and receive a small amount of data with real-time requirements. CAN bus was originally developed for the car industry to replace point-to-point connections in automotive systems. CAN protocol has been stipulated as an international standard by 150 International Standard Organizations [20]. CAN transmits signals on the CAN network using two wires, CAN-High and CAN-Low. These two wires operate in different modes carrying inverted voltages which decreases noise interference. The standard being used determines the voltage level and other characteristics of the physical layer. The two standards are the ISO11898 (CAN High Speed) standard and the ISO11519 (CAN Low Speed) standard [21].

The challenges of implementing the CAN module by the wireless method was the aspect of integration and interaction of the existing CAN network with the wireless protocol to achieve the wireless CAN. We had to research and test several CAN modules and development boards to find a compatible device and developed the best way to program it to fit the communication protocol existing in the wired CAN. Next is the choice of the wire-less protocol to implement, this was done with certain criteria of security, availability, and signal penetration since the module was to be used in a ship environment. All these factors lead to the testing and choice of the ZigBee XBee module used to implement the wireless CAN.

The requirements when implementing wireless CAN come from the drawbacks associated with wireless networks such as security issues, coverage, and transmission speed (as wireless transmission can be slower than a "wired" network. Also, using a wireless protocol based on a CAN network must satisfy the message delivery time for real-time applications to which CAN is applied to.

2.3.2 | Wireless communication protocols

Wireless applications typically require burst transmission and reduced overhead, and they use a very small amount of data per node, therefore, the bandwidth is not the main requirement. Some applications require coverage of large areas; reliability, availability, bounded latency for real-time behaviour, and energy efficiency as some key performance indicators [22]. Therefore, careful considerations were made when choosing a wireless protocol to be implemented for this industrial application.

The XBee module used during implementation uses the ZigBee (IEEE 802.15.4) technology. ZigBee is a short-range wireless protocol that is a standard for personal-area networks developed by ZigBee Alliance aiming at providing a low cost, low power consumption, reliable and two-way wireless communication standard for short-range applications. It allows the nodes to find new routes throughout the network when one route fails. Thus, ZigBee is a robust wireless solution [23].

The choice of using the ZigBee protocol was made by comparing four wireless solutions based on the analysis of

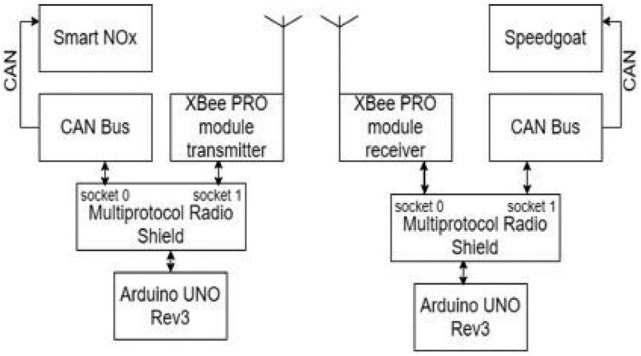

FIGURE 1 Block diagram for the hardware setup of XBee-CAN module.

experiment results. The wireless protocols compared were namely Wi-Fi, LoRa, BLE, and ZigBee. Performance analysis for these four wireless protocols was conducted based on key considerations that should influence the choice of wireless protocols for a specific application. The experiments and measurements were performed in the Technobothnia laboratory. Technobothnia is a wide-ranged advanced and modern laboratory unit that occupies 8000 m^2 and which is within the campus of the University of Vaasa [24].

The importance of RSSI, packet loss, and security to the CAN module are discussed briefly. The RSSI measurement gives us an idea of how well the wireless CAN modules (transceivers) will receive the signals sent between them. RSSI is a useful value in determining if the signal strength is good enough for wireless connection and communication. The CAN applications are used in real-time applications [25] and depending on the application, data loss could be critical, therefore there is a need to investigate the packet loss performance of the designed module.

Wireless communication also introduces a new challenge of security which is less in the case of a wired connection in which a security breach will involve taping the line. This security challenge must be investigated and tested to ensure the benefits of wireless communication are not overturned by the security risk if not properly implemented.

2.3.3 | System architecture

The system consists of a 24 V power supply for the smart NOx sensor, which is connected to the CAN Bus of the wireless-CAN module (transmitter). Furthermore, the wireless-CAN modules (receiver) are connected to the Speedgoat, the Speedgoat device that contains a MATLAB Simulink model to calculate, monitor, and display the (O_2)% and NOx ppm.

The XBee-CAN bridge hardware design of the wireless CAN prototype is a customized module based on the ZigBee standard integrated with the CAN bus based on the CAN protocol. The setup in Figure 1 provides a proof-of-concept that can be further developed from a prototype into a product.

In the wireless CAN module, a multiprotocol radio shield is connected over the Arduino board and the CAN Bus module

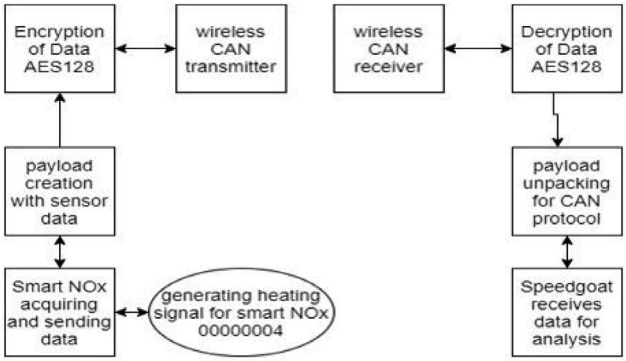

FIGURE 2 XBee-CAN flowchart.

is placed in socket 0 of the multiprotocol radio shield while the XBee module is placed in socket 1. This setup is done for both the transmitter and receiver modules.

At the transmitter side, the CAN Bus module is used to interface the transmitter XBee module with the smart NOx sensor using twisted pair cables (CAN High and CAN Low). While at the receiver side, the CAN Bus module is used to interface the receiver XBee module with the Speedgoat also using twisted pair cables (CAN High and CAN Low).

2.3.4 | Programming the XBee-CAN prototype module

The header file XBee802SendCANDataAES128.h is used in the transmitter to initialize the XBee and CAN bus modules at the transmitter side. It also implements the required C functions to program the features and functions of XBee-CAN module hardware.

The XBee-CAN bridge Software implementation was done using the Arduino IDE environment. At the transmitter side, the smart NOx sensor has a 29-bit CAN ID and the transmitter hardware is programmed to send an initialization heating signal "00000004h" (8 bytes hexadecimal) through the CAN bus to this CAN ID to start heating and collecting the smart NOx data. The CAN bus then receives the data sent from the amart NOx after it starts heating and transfers the data through SPI to the XBee module for wireless transmission. While on the receiver side, the hardware is programmed to receive the smart NOx sensor data and transfers the data through SPI to the CAN bus of the receiver module. The CAN bus is connected to the Speedgoat using two twisted-pair cables (CAN High and CAN Low) for analyzing the received data. The receiver module also performs packet loss and RSSI measurements.

The flowcharts for the programming of the wireless CAN module are illustrated in Figure 2.

The transmitted payload is a 10-byte hexadecimal data comprising of a 1-byte pre-amble, 8-byte smart NOx data, and 1-byte checksum data as illustrated in Figure 3.

The preamble is a set of symbols or bits used in packet-based communications systems to indicate the start of a packet. The preamble is a set of signals preceding genuine data in transmission. It is used to help check data transmission errors. It helps to synchronize data transmission between the transmitter and receiver.

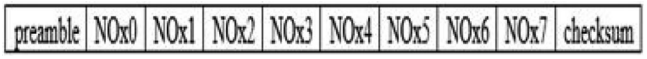

FIGURE 3 Transmitted smart NOx payload.

The checksum is a small-sized block of data. It is the sum of the correct digits from the transmitted digital data, against which later comparisons can be made to detect errors in the data.

Equation (1) is the checksum and it is the hexadecimal summation of only the 8-byte smart NOx hexadecimal data.

$$\mathrm{NOx0} + \mathrm{NOx1} + \mathrm{NOx2} + \mathrm{NOx3} + \mathrm{NOx4} + \mathrm{NOx5} + \mathrm{NOx6} + \mathrm{NOx7} = \mathrm{checksum} \quad (1)$$

The preamble is computed as illustrated in Equation (2). The preamble is computed from the hexadecimal summation of the 8-byte smart NOx data plus the checksum value, that is, smartNOx + checksum = preamble.

$$\mathrm{NOx0} + \mathrm{NOx1} + \mathrm{NOx2} + \mathrm{NOx3} + \mathrm{NOx4} + \mathrm{NOx5} + \mathrm{NOx6} + \mathrm{NOx7} + \mathrm{checksum} = \mathrm{preamble} \quad (2)$$

Both the checksum and preamble are used to verify data integrity, which ensures an error-free data transmission and prevents the alteration of data.

2.3.5 | ZigBee security concerns

ZigBee-enabled systems encounter some security threats like traffic sniffing (eaves-dropping), denial-of-service (DoS) attacks, nonce-reuse attacks, packet decoding, and data manipulation/injection, which an attacker who uses special hardware and software developed especially for attacking purposes can exploit [26].

In our paper, securing wireless communication protocol was done by doubling the process of AES with two different keys at the two levels (AES128 security API libraries level and ZigBee module level) which gives difficulty to the attacker or malware to interrupt the network or system as a result of the strength of the double encryption of AES. This is similar to what was done in ref. [27]. The key is manually pre-install onto each legitimate device of the ZigBee-enabled network (two devices). There is a trade-off between usability and security in this key management scenario with respect to the size of the network if it is large. Therefore, it is possible for the network administrator to go for less secure but more usable options. The key can be updated regularly especially in a case of a missing or tampered device, to prevent unauthorized use of the whole ZigBee-enabled network.

When the message integrity is not verified, having the communicated messages encrypted will not be enough as a DoS

attack can still happen. This is because usually, the ZigBee device wakes up at intervals to send and receive messages as they run on batteries and have a very low duty cycle, that is, the ratio of active broadcast time compared to the silent period. The networks usually have a predefined wake-up interval for saving battery life, however, this can open new access for DoS attacks [26]. In a DoS attack, an attacker repeatedly jams the medium by sending a message to the victim device which decrypts the payload to a random plain text, which has no meaning to the next upper protocol layer. The attacker uses a high-water mark of the frame counter set to the maximum value, therefore, a legitimate frame that arrives after the DoS attack will automatically be denied reception by the victim device, as a result of the frame counter value of the received message being less than the high-water mark used during the DoS attack.

The implementation of security in the wireless CAN module prototype using the AES128 (AES CCM) provides data encryption and authenticity. It utilizes the combination of the counter mode with the CBC-MAC authentication. It makes use of the same encryption key for both modes. ZigBee makes use of a version that is a little modified type of CCM referred to as CCM*, which provides room for more flexibility than the standard CCM. CCM* allows the use of either authentication or encryption, while both are always required in CCM. The operation of ZEDs in a non-beacon mode where the ZED actively polls the network coordinator to check for data availability can curb DoS. The wake-up action can be made to happen at irregular intervals, to make the attacker not be able to guess the exact time when data transfers will take place. This means a predefined wakeup interval should not be used. The nonce-reuse attacks are catered for by ZigBee specification using non-volatile memory (NVM). The ZigBee system can be vulnerable to the same-nonce attack after a power failure which causes a clear in access control list (ACL), therefore, the use of a non-volatile memory (NVM) to recover them after a power failure [26].

The developed security framework for the wireless transfer of CAN data using the XBee module makes use of the XBee module's extra feature of enabling AES128 encryption on the XBee module itself. In addition, an optional feature provided by a customized API library for data encryption is utilized. The AES 128 encryption on the XBee modules is done twice, first, during the configuration of the XBee modules, and second, using AES128 encryption API libraries to provide encryption of the data at the coding level. The security can be further improved by implementation using FPGA which can also improve the battery life of the device.

The implementation of security for the wireless CAN data transfer in the designed prototype also comes from the use of ZigBee technology. The XBee module used makes use of the AES128 (AES-CCM). It utilizes the combination of the counter mode with the CBC-MAC authentication. The operation of ZEDs in a non-beacon mode where the ZED actively polls the network coordinator to check for data availability is also used to curb DoS attacks. Furthermore, wake-up action can be made to happen at irregular intervals, which can mitigate the attacker from being able to guess the exact time when the data transfer will take place. This means a predefined wakeup interval was not used. These findings were applied in our case. The nonce-reuse attacks are catered for by ZigBee specification using "non-volatile memory (NVM)" which helps to recover them after a power failure.

TABLE 1 XBee maximum and minimum RSSI measurement in Technobothnia.

Distance in meters	5	10	15	20	25	30
Minimum RSSI value (dBm)	−45	−47	−52	−56	−60	−66
Maximum RSSI value (dBm)	−40	−43	−46	−51	−53	−57

TABLE 2 XBee maximum and minimum RSSI measurement in VEBIC.

Distance in meters	5	10	15	20	25	30
Minimum RSSI value (dBm)	−53	−54	−60	NA	NA	NA
Maximum RSSI value (dBm)	−42	−47	−52	NA	NA	NA

2.3.6 | ZigBee (XBee module) performance measure

The communication performance analysis done on the XBee module is discussed here. The test performed includes RSSI, bit error rate, latency, and packet loss. The maximum and minimum measured RSSI values measured in Technobothnia and VEBIC are shown in Tables 1 and 2 respectively. At each distance of 5 m apart, 200 RSSI measurements were taken. From the datasheet of the XBee module, it was noted that it has a receiver sensitivity of −100 dBm and a maximum range of 750 m [28].

The RSSI values can be noticed to decrease (greater negative value) as the distance increases as seen in Tables 1 and 2. This is in line with the RSSI theory, however, in an ideal case, the RSSI values should decrease linearly. The distance used in this test is influenced by the nature of the application of this project which does not require a very large distance (the maximum required distance is 15 m), therefore the RSSI of the module above the specified maximum distance was not tested in VEBIC where the actual engine test was conducted.

The bit error check for all the wireless protocols was implemented in the same way. As illustrated in Figure 3, the payload is a 10-byte data payload. At the receiver side, the payload is checked for error using a 1-byte preamble (called ErrorDectNum in the code used to program the device) and 1-byte checksum computed and appended to the original 8-byte smart NOx data before transmission at the transmitter side. The checksum is the computed value mentioned in Equation (1) and the preamble is the value mentioned in Equation (2). At the receiver side, the preamble and checksum are verified and if they are the same as the values from the transmitter, the data is

error-free. Alternatively, if the sum of the 8-bit smart NOx data plus 1-bit checksum (that is, the preamble) at the transmitter equals the preamble value also at the receiver side for the same payload been considered, the data is error-free.

The delay in a network specifies the duration required to transmit a bit of data through the network from one node to another. It is usually measured in multiples or fractions of seconds. The delay otherwise called latency can be slightly different depending on the environment where the specific pair of communicating nodes are located. Packet loss is the measure of the amount of data packet that is lost before it reaches the receiver and it occurs when a data transmission error occurs, usually across wireless networks, or due to network congestion. Packet loss is a percentage of the data lost with respect to data sent.

Based on the fact that no equipment is 100 percent efficient, the energy used by a piece of equipment is more than the energy really needed. This happens as a result of energy lost as heat, vibrations, and/or electromagnetic radiation. Most wireless radio frequency (RF) devices are usually battery-powered. This can introduce a challenge depending on the application and the location of the device may make it difficult and/or expensive to replace the battery. In many real-world scenarios, extending battery life is important and critical.

More details about the results of the ZigBee test in comparison to other wireless protocols (BLE, LoRa, and WiFi) are provided and discussed in Section 3.

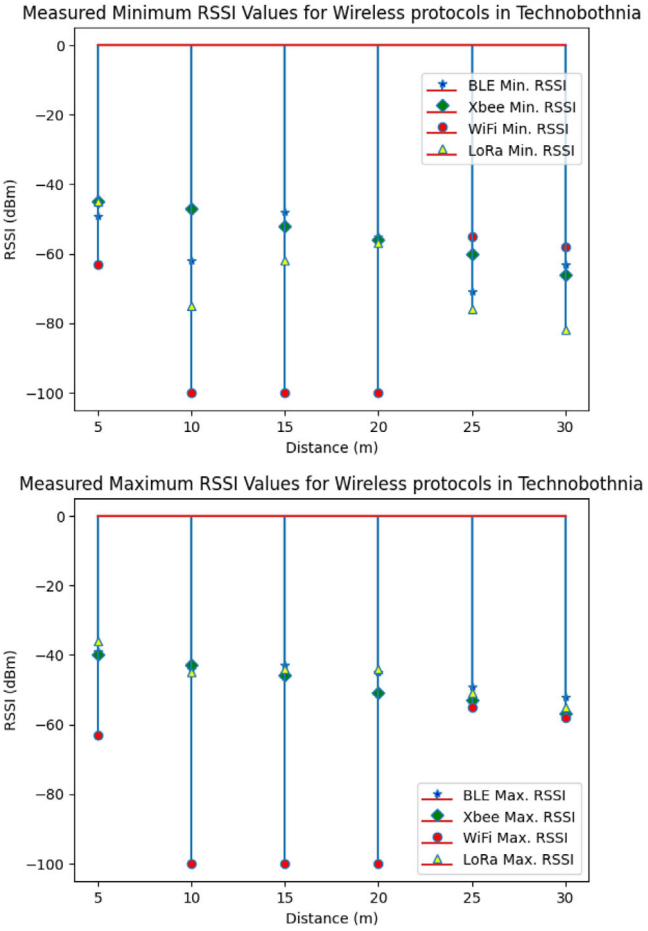

FIGURE 4 RSSI measurements for all the wireless protocols (BLE, XBee, WIFI, and LoRa) for the test done in Technobothnia.

3 | RESULTS

3.1 | Wireless communication test using smart NOx sensor

From the experiments (see Table A1), the XBee had better RSSI values and security features than the other wireless modules used. These features with some other factors like good performance in the packet loss test; ability to enhance battery life; better penetrating capability and range when compared to the BLE lead to the choice of implementing the ZigBee wireless protocol in designing the wireless-CAN protocol called the XBee-CAN module.

In Figures 4 and 5, we present the measured minimum and maximum RSSI values of the wireless protocols during tests done in two different locations. These results show a good signal strength for several distances in meters as seen on the *x*-axis. The RSSI measurement gives us an idea of how well the wireless CAN modules (transceivers) will receive the signals sent between them. The *y*-axis is the RSSI values and the *x*-axis is the distance in meters between the wireless CAN module connected to the sensor on the ship engine and the wireless CAN module connected to the Speedgoat used to read and analyze the received CAN data.

A MATLAB Simulink module was programmed into the Speedgoat to receive CAN frames, calculate $(O_2)\%$ and NOx ppm, and display the results on a monitor connected to the Speedgoat.

Packet loss – For every 100 packets sent, the error is (less than) <0.5% packet loss during the experiment at the maximum test range of 30 m and a minimum of 15 m (actual maximum range for the application). This was done in an engine laboratory having noise from the vibration of the engine and WiFi signals were also present. There were a lot of metal parts and equipment in the room and movements of people, all these were part of the potential sources of interference. They were two nodes, one at the sensor side and the other connected to the Speedgoat to receive the CAN data. The distance between them was a vertical distance with the module connected to the sensor above. By standard design, ZigBee has access to 16 separate, 5 MHz channels in the 2.4 GHz band of which several of them do not overlap with US and European versions of Wi-Fi. Furthermore, an IEEE 802.15.4-defined CSMA-CA protocol that reduces the probability of interfering with other users is incorporated into ZigBee and it utilizes the automatic re-transmission of data to cater to network robustness. As a result of the extremely low-duty cycle of ZigBee products, we have relatively few packet data transmissions, thereby, reducing the likelihood of an unsuccessful transmission. It was noticed that our designed module had an acceptable average latency of 104ms. The maximum and minimum latency measure-

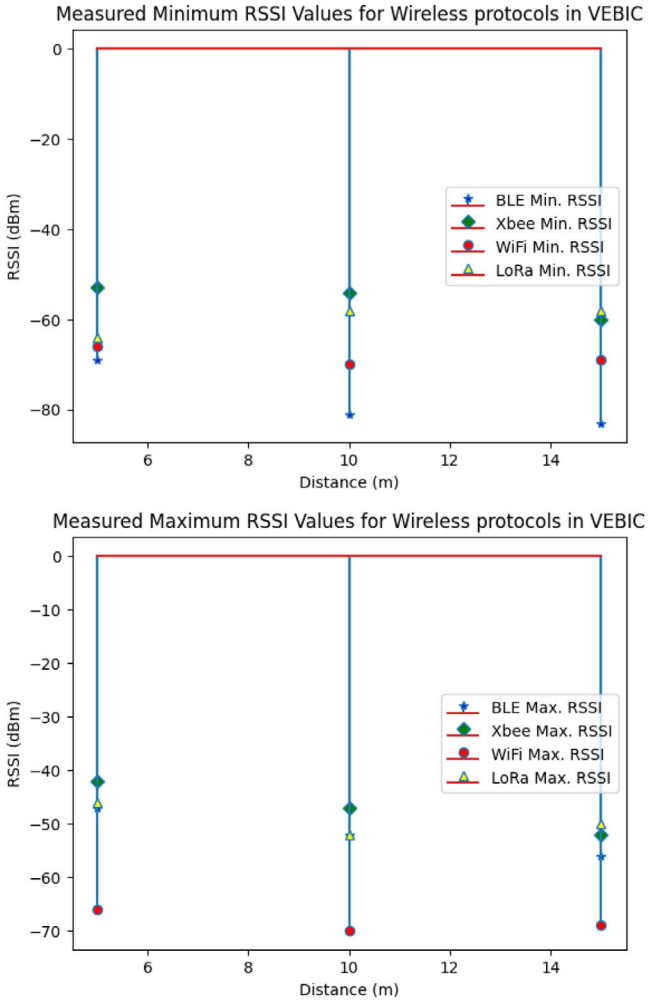

FIGURE 5 RSSI Measurements for all the wireless protocols (BLE, XBee, WIFI, and LoRa) for the test done in the Wärtsila diesel engine test room located in VEBIC.

TABLE 3 XBee module maximum and minimum latency measurements.

Latency	Value in milliseconds
Minimum latency value	102
Maximum latency value	106

ments noticed for the XBee implementation are illustrated in Table 3.

The application sublayer (APS) layer handles retransmission, the Network (NWK) layer, and also the MAC layer. If APS acknowledgment is enabled, the APS layer will attempt several times (configurable, default value 3) before receiving Acknowledgement (ACK). The NWK layer also performs a number of retries (configurable, default value 2) for the next hop message, once the medium access control (MAC) layer retries are exhausted for that message. MAC-level acknowledgments and retries are default and automatic regardless of the service used. MAC layer will retry 3 times (configurable) before

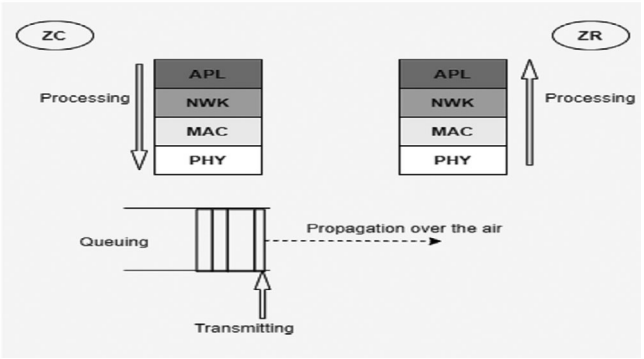

FIGURE 6 Packet transmission process from ZC to ZR/ZED.

returning a failure status to the network layer. The time interval between each attempt depends on the CSMA/CA algorithm [29].

During our test, the APS layer acknowledgment was disabled therefore, the APS layer will not retransmit; the NWK layer performs two attempts for the next-hop message, the interval is unpredictable, depending on the packet length, surroundings, and distance between nodes; the MAC layer will retry three times for each attempt before announcing failure, and delays a random amount of time (from 3 to 10 ms) before each attempt. In the worst case, the sender will transmit at most 8 times and the receiver will attempt eight times to respond as well. The packet transmission process is shown in Figure 6.

Security – The XBee module has the extra feature of enabling AES128 encryption on the XBee module itself. In other modules (BLE, WIFI, and LoRa), data encryption is an optional feature provided by an API library. However, the WIFI module also provides the feature of installing secure sockets layer (SSL), it requires installing the corresponding certificate, created by a CA (Certification Authority). This makes it more complex than the feature of the XBee module. Likewise, the BLE module uses AES-128 link-layer encryption for encrypting the connection to make the connection processes secure. The data, however, is not encrypted.

The AES 128 encryption on the XBee modules is done twice, first, during the configuration of the XBee modules, and second, customized AES128 encryption API libraries were used to provide encryption of the data at the coding level during the programming of the wireless CAN prototypes. Power Consumption – In Table A1, the BLE shows better battery life, next is the XBee and the third is the WIFI module. Wi-Fi is mostly used for data transmission, with a long-range and data throughput of 2–11 Mbps. The power consumption of the XBee module implementation can be optimized by putting the ZigBee devices to sleep and waking them up only during the transfer of data. Also, another option is integrating field programmable gate arrays (FPGAs) into the device.

ZigBee and Bluetooth have similar features as both are types of IEEE 802.15 wireless personal-area networks (WPANs) making use of the 2.4-GHz unlicensed frequency band and using small form factors and low power. However, ZigBee is more suitable for control and automation in exchanging small

TABLE 4 Comparison of ZigBee, BLE, and WiFi wireless standards.

	ZigBee 802.15.4	Bluetooth 802.15.1	Wi-Fi 802.11b
Applications	Monitoring and control	Replacing cables/wires	Web, video, and email
Data capacity	250 Kbps	1 Mbps	11 Mbps
Range (meters)	approx. 75	10 – 100	100
Battery life	Years	Days	Hours
Nodes per network	up to 65,533	8	30
Software size (Kbytes)	4–32	250	>1000

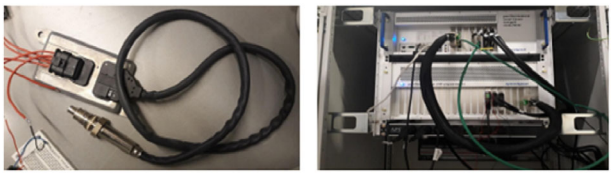

FIGURE 7 (a) Smart NOx sensor and (b) Speedgoat located in VEBIC.

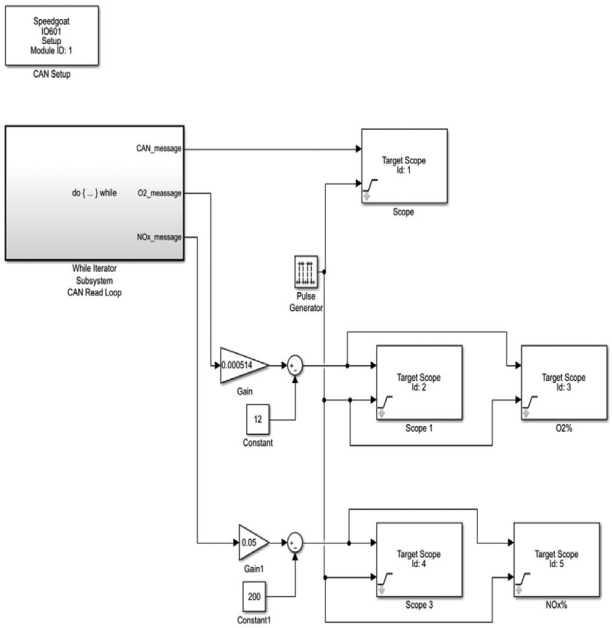

FIGURE 8 Simulink model to receive smart NOx CAN frame.

packets over a large network; while Bluetooth is suitable for connectivity issues between laptops and PDAs, and applicable to more general cable replacement scenarios in which large packets are transmitted over a small network [30]. Table 4 shows a general application comparison of ZigBee, BLE, and WiFi wireless standards.

BLE uses high data rates and a lot of power on large packet devices while ZigBee employs low data rates and little power on small packet devices. This can be seen in their battery life in Table 4. However, from Table A1, we can see that the BLE had better battery life than ZigBee, this is because the same data rates were used for both BLE and ZigBee. Lowering the ZigBee data rate to 1 megabit per second will lead to the results shown in Table 4. Note that, ZigBee has a network speed of up to 1 megabit per second. While the network speed of BLE is up to 250 megabits per second.

The wireless CAN module was initially tested with an external Smart NOx sensor (see Figure 7(a)). Sending the 8 bytes hexadecimal heating signal "04h" to the smart NOx sensor with a Receive ID 0x18FEDF00 makes the smart NOx sensor start heating and then sends back its CAN frames through the CAN Bus to the wireless module for transmission to the receiver module where a Speedgoat CAN Bus interface is used to view the data (see Figure 7(b)). Repeating the 8 bytes hexadecimal heating signal "04h" every 100 ms will maintain the heating of the smart NOx. The module was also tested on a diesel engine utilizing the CAN network in the ECM.

The MATLAB Simulink model in Figure 8 is used to continuously poll the client/receiver CAN module four times per second, extract data bytes, calculate O_2% and NOx ppm and display a continuously updated sliding graph on a monitor connected to the Speedgoat.

3.2 | Performance test of the designed XBee-can module on Wartsila W4120 diesel engine

The wireless CAN was tested with the Wärtsilä W4L20 because the case study was done in collaboration with Wärtsilä, however, the module can also be used for engines that utilize the CAN network in the ECU.

The smart NOx sensor was installed on the Wärtsilä 4L20 Diesel Engine and the O_2% and NOx ppm values were measured and compared with the readings from the SICK MCS100E. The MCS100E HW is an analyzer system used for extractive measurement of up to eight (8) active gas components from an engine [31]. Table 5 illustrates the comparison between the values from MCS100E and the wireless XBee-CAN prototype seen on the Speedgoat device for the W4L20 diesel engine in different operation modes (the engine is idle, running without load, and running with load). It is the percentage error of the XBee-CAN module prototype values when compared to the values from the MCS100E. The measurements from MCS100E and the XBee-CAN module were performed at the same time. The difference between their readings in Table 5 comes from the fact that both had their own separate sensor (installed at a different location on the exhaust of the same engine), therefore, their measurement time could not be properly synchronized. However, it was concluded from observation that the values obtained were close to what was expected from the engine test for the XBee-CAN module and the MCS100E (as a reference).

TABLE 5 Comparing values from SICK|MCS 100e and the XBee-CAN module.

Device name	Engine operation modes					
	Idle		Without load		With load	
	NOx ppm	(O_2)%	NOx ppm	(O_2)%	NOx ppm	(O_2)%
XBee-CAN module % error	0.0	0.0	3.09	7.22	3.83	2.06

4 | DISCUSSION

The benefit of using the wireless CAN module is the ease of access to the state of the engine - in terms of remote monitoring, also it brings flexibility, and cost savings as it saves on installation problems, increased flexibility, and creation of new opportunities and application scenarios, however, the drawbacks come from security issues, coverage and transmission speed (as wireless transmission can be slower than "wired" network. With proper planning and techniques, these challenges can be addressed through well know technologies created to reduce their effect.

The present application (the engine test phase), has a delay in the wireless CAN (XBee-CAN module) when compared to the wired SICK|MCS 100E. However, this delay is within an acceptable range for the present application. The results from Table 5 show an average percentage accuracy of 95.95% in the transmission and reception of the sensor data using the wireless CAN when compared to the wired solution (SICK|MCS 100E). The percentage accuracy of 95.95 was computed using the percentage errors in Table 5. The values 3.09, 7.22, 3.83, and 2.06 in particles per million (ppm) were averaged and then subtracted from 100 to arrive at the value 95.95. This was done irrespective of the gas being measured (NOx or O_2) as both measurements occur simultaneously using the same sensor.

ZigBee can be used to create a network of sensors. This implies that several sensor values can be read and transmitted for monitoring on the speedgoat. The XBee-CAN module network could be made up of several END devices or nodes (sensors) and a CO-ORDINATOR device as the ZigBee protocol supports three nodes types namely ZigBee Coordinator ZC, ZigBee router (ZR), and ZigBee end device (ZED). Additive manufacturing was applied in designing two protective casings, and they were 3D printed. These casings were used to encapsulate the receiver and transmitter XBee-CAN Modules prototypes as illustrated in Figure 9(a,b).

The material used in printing the protective casings is PLA filament. A 3D printer was used to print the prototype casing with settings having a printing temperature of 200°C for the extruder and 60°C for the bed plate and an infill of 20%. The test in this research was done in a test facility (VEBIC) where the test ship engine was located. It was not done on a real ship in a live scenario. However, the design prototype was tested for vibration as the wireless module connected to the smart NOx was placed on a metal platform very close to the vibrating engine and other metal parts. During the test, no effect was noticed that showed any significant delay or loss of data packet compared to when it was tested in Technobothnia which is an office building located in the University of Vaasa.

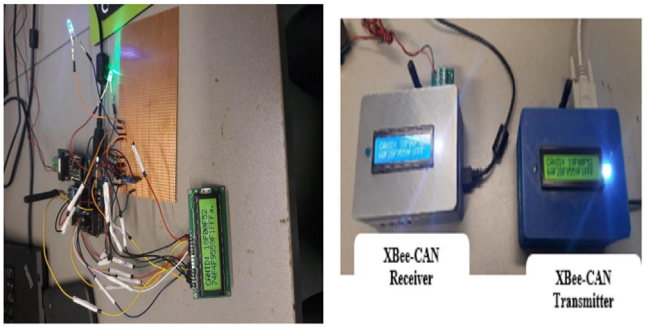

FIGURE 9 (a) XBee-CAN prototype without 3D printed casing and (b) XBee-CAN prototype in 3D printed casing.

5 | CONCLUSION

Research on the feasibility of replacing the existing wired CAN bus connection between the smart NOx sensor and the rapid control prototyping system speedgoat and possibly in the future the engine control unit (ECU) with a wireless communication solution was performed. The hardware setup and implementation were implemented. The devices were programmed to meet the required application in line with the performance expectation for communication in an industrial environment. A communication performance test was performed. The wireless CAN module has been monitored for almost a year and has proven to work fine in monitoring diesel engine NOx emissions. The results of using the wireless CAN showed an average percentage accuracy of 95.95% in the transmission and reception of the sensor data when compared to the wired solution (SICK|MCS 100E). The designed wireless XBee-CAN prototype is currently installed on a W4L20 diesel engine in the Vaasa Energy Business Innovation Center (VEBIC), Vaasa, Finland. A possible future work would be to further develop the system of the prototype by integrating field programmable gate arrays (FPGAs). The main motivation is to optimize the software to improve the battery life of the present prototype by optimizing all parameters associated with data rates, and energy consumption. Another possible work will be to extend to other types of sensors on the ship engine where managing multiple sensors will be addressed.

AUTHOR CONTRIBUTIONS

Akpojoto Siemuri: Conceptualization, investigation, methodology, resources, software, validation, visualization, writing - original draft, writing - review and editing. Tobias Glocker: Conceptualization, methodology, supervision, validation, writing - review and editing. Mike Mekkanen: Funding acquisition, investigation, writing - review and editing. Kimmo Kauhaniemi: Funding acquisition, supervision, writing - review and editing. Timo Mantere: Formal analysis, supervision, writing - review and editing. Mohammed Elmusrat: Conceptualization, methodology, supervision, writing - review and editing.

ACKNOWLEDGMENTS

The authors would like to express thanks to Reino Virrankoski for the opportunity to work on this project and to Rayko Toshev for granting access to the digital manufacturing laboratory in Technobothnia, University of Vaasa to achieve the 3D printing aspect of this project. Regional Council of Ostrobothnia; Smart Energy Systems Research Platform (SESP), School of Technology and Innovations, the University of Vaasa; Wärtsilä Oyj Abp. We also acknowledge Storm Xiaoguo a project researcher at the University of Vaasa for the design of the Simulink model used for receiving the Smart NOx CAN frames.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflict of interest.

DATA AVAILABILITY STATEMENT

No data are available for this publication.

ORCID

Akpojoto Siemuri https://orcid.org/0000-0002-2644-1985
Kimmo Kauhaniemi https://orcid.org/0000-0002-7429-3171

REFERENCES

1. Xiang, G., Huang, D., Chen, Y., Jin, W., Luo, Y.: The design of a distributed control system based on CAN bus. In: Proceedings of 2013 IEEE, International Conference on Mechatronics and Automation, pp. 816–821. IEEE, Piscataway, NJ (2013)
2. Siemuri, A.A., Glocker, T., Mekkanen, M., Kauhaniemi, K.T., Mantere, T., Rösgren, J., Kuusisto, J., Elmusrati, M.S.: Design and implementation of a wireless automation module for diesel engines. In: 2019 27th Telecommunications Forum (TELFOR), pp. 199–278. IEEE, Piscataway, NJ (2019)
3. Unal, I.: Integration of ZigBee based GPS receiver to CAN network for precision farming applications. Peer-to-Peer Networking Appl. 13, 1394–1405 (2020). doi:https://doi.org/10.1007/s12083-020-00897-3
4. Kumar, T.A., Rao, K.S.: Integrated mine safety monitoring and alerting system using ZigBee & can bus. IOSR J. Electr. Electron. Eng. 8(3), 82–87 (2013). doi:http://www.iosrjournals.org/iosr-jeee/Papers/Vol8-issue3/N0838287.pdf?id=7590
5. Wexler, J.: Wireless sensor networking for vehicle environments. Thesis, School of Electrical Engineering and Computer Science College of Engineering Seoul National University (2020)
6. Molina-Garcia, A., Torres, R., Munoz, J.L., Encinas, N.: Application of controller area networks to direct load control in residential areas. In: IEEE Lausanne Power Tech, pp. 1970–1974. IEEE, Piscataway, NJ (2007)
7. Hoo, T.C., Singh, M., Siah, Y.K., Ahmad, A.R.: Building low-cost intelligent building components with controller area network (CAN) bus. In: Proceedings of IEEE Region 10 International Conference on Electrical and Electronic Technology, pp. 466–468. IEEE, Piscataway, NJ (2001)
8. Othman, H.F., Aji, Y.R., Fakhreddin, F.T., Al-Ali, A.R.: Controller area networks: evolution and applications. In: 2nd Information and Communication Technologies, pp. 3088–3093. IEEE, Piscataway, NJ (2006)
9. National Instruments: Controller Area Network (CAN) Overview. National Instruments. https://www.ni.com/fi-fi/innovations/white-papers/06/controller-area-network–can–overview.html (2022). Accessed 11 October 2022.
10. Ng, W.L., Ng, C.K., Noordin, N.K., Rokhani, F.Z., Ali, B.M.: Home appliances controller using wireless controller area network (WCAN) system. In: International Conference on Computer and Communication Engineering (ICCCE 2010), pp. 199–278. IEEE, Piscataway, NJ (2010)
11. Johansson, K.H., Törngren, M., Nielsen, L.: Vehicle Applications of Controller Area Network, pp. 199–278. KTH Royal Institute of Technology, Stockholm (2009)
12. EPA region 1: Nitrogen oxides (NOx) emissions. Environmental Protection Agency. https://www3.epa.gov/region1/airquality/nox.html (2022). Accessed 11 October 2022.
13. Mirza, N., Khan, A.N.: Bluetooth low energy based communication framework for intra vehicle wireless sensor networks. In: International Conference on Frontiers of Information Technology (FIT), pp. 29–34. IEEE, Piscataway, NJ (2017)
14. Speedgoat GmbH: Speedgoat - Applications and Industries Overview. https://www.speedgoat.com/applications-industries (2022). Accessed 10 October 2022.
15. Continental, A.G.: Specification smart NOx sensor – UniNO_x-sensor. Continental Trading GmbH. https://az666937.vo.msecnd.net/32/cc3c940a-86a4-43ed-9945-4a08319f5b4e.pdf (2004). Accessed 10 October 2022.
16. Wikipedia: Electronic Diesel Control. https://en.wikipedia.org/wiki/Electronic_Diesel_Control (2022). Accessed 10 October 2022.
17. Antti, K., Marko, J., Teemu, K., Tero, F.: W4L20 VEBIC Genset dynamics-baseframe design. Jo. Struct. Mech. 50, 292 (2017)
18. VEBIC: VEBIC - Vaasa Energy Business Innovation Centre. University of Vaasa https://www.uwasa.fi/fi/tutkimus/tutkimusalustat/vebic (2022). Accessed 11 October 2022.
19. Wärtsilä, A.B.: Oy: Marine solutions deliver value. (2022). https://www.wartsila.com/marine. Accessed 11 October 2022.
20. Xiao-feng, W., Yi-si, X., Li-xiang, C.: Application and implementation of CAN bus technology in industry real-time data communication. In: International Conference on Industrial Mechatronics and Automation (ICIMA), pp. 29–34. IEEE, Piscataway, NJ (2009)
21. Nilsson, S.: Controller Area Network - CAN Information. https://staffannilsson.eu/developer/frames.htm (1997). Accessed 11 October 2022.
22. Khan, A., Turowski, K.: A survey of current challenges in manufacturing industry and preparation for industry 4.0. In: Proceedings of the First International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'16), pp. 15–26. Springer, Cham (2016)
23. Texas Instruments: ZigBee – Technical documents. Texas Instruments. https://www.ti.com/lit/ug/swru556/swru556.pdf?ts=1626176121784&ref_url=https%253A%252F%252Fwww.google.com%252F (2022). Accessed 11 October 2022.
24. Technobothnia: Technobothnia Laboratory. University of Vaasa (2022). https://www.technobothnia.fi/. Accessed 11 October 2022.
25. Tindell, K.W., Hans, H., Wellings, A.J.: Analysing real-time communications: controller area network (CAN). In: IEEE Proceedings Real-Time Systems Symposium, pp. 259–263. IEEE, Piscataway, NJ (1995)
26. Olayemi, O., Keijo, H., Asikainen, M., Niko, V., Pekka, T.: Three practical attacks against ZigBee security: attack scenario definitions, practical experiments, countermeasures, and lessons learned. In: 14th International Conference on Hybrid Intelligent Systems, HIS, pp. 199–206. IEEE, Piscataway, NJ (2014)

27. Javed, Y., Khan, A., Qahar, A.: Preventing DoS attacks in IoT using AES. J. Telecommun., Electron. Comput. Eng. 9(3–11), 55–60 (2018). doi:https://www.researchgate.net/publication/322243661_Preventing_DoS_Attacks_in_IoT_Using_AES. Accessed 12 October 2022.
28. Digi International Inc.: ZigBee Datasheet. https://www.digi.com/resources/library/data-sheets/ds_xbee_zig (2023). Accessed 12 October 2022.
29. Liu, K.: Performance evaluation of ZigBee network for embedded electricity meters. KTH Electrical Engineering. Stockholm. https://www.diva-portal.org/smash/get/diva2:571735/FULLTEXT01.pdfThanks (2009). Accessed 12 October 2022.
30. Wexler, J.: Bluetooth, and ZigBee: Their similarities and differences. IDG Communications, Inc. https://www.networkworld.com/article/2318704/bluetooth-and-zigbee–their-similarities-and-differences.html (2005). Accessed 12 October 2022.
31. CEMS solutions: CEMS solutions MCS100E HW. https://www.sick.com/fi/en/analyzer-solutions/cems-solutions/mcs100e-hw/c/g285463 (2002). Accessed 12 October 2022.

How to cite this article: Siemuri, A., Glocker, T., Mekkanen, M., Kauhaniemi, K., Mantere, T., Elmusrati, M.: Design and implementation of a wireless CAN module for marine engines using ZigBee protocol. IET Commun. 17, 1541–1552 (2023). https://doi.org/10.1049/cmu2.12640

APPENDIX

Table A1 shows the performance analysis of the selected wireless protocols. These values are derived from the datasheet of the wireless protocol used (BLE, XBee, WiFi, and LoRa) and from the results of the experiment.

TABLE A1 Performance analysis of wireless protocols These values are derived from the datasheet of the wireless protocol used (BLE, XBee, WiFi, and LoRa) and from the results of the experiment.

Analysis	BLE		XBee (802.15.4)		WIFI		LoRa	
	Data sheet	Expt[a]	Data sheet	Expt[a]	Data sheet	Expt[a]	Data sheet	Expt[a]
RSSI in VEBIC	−103 dBm	−83 dBm	−100 dBm	−60 dBm	−94 dBm	−70 dBm	−134 dBm	−64 dBm
RSSI in Technobothnia	−103 dBm	−71 dBm	−100 dBm	−66 dBm	−94 dBm	−100 dBm	−134 dBm	−82 dBm
Packet loss %	N/M[b]	0%	N/M[b]	0%	N/M[b]	0%	N/M[b]	0%
Min. latency	N/M[b]	24ms	N/M[b]	102ms	N/M[b]	1169ms	N/M[b]	2102ms
Max. latency	N/M[b]	60ms	N/M[b]	106ms	N/M[b]	1213ms	N/M[b]	2106ms
Power consumption	Tx	3.7 V	Tx	3.7 V	Tx	3.7V	Tx	3.7V
	36 mA	6600	36 mA	6600	36 mA	6600	36mA	6600
	Rx	mAh	Rx	mAh	Rx	mAh	Rx	mAh
	8 mA	battery	8 mA	battery	8 mA	battery	8mA	battery
Battery life [Hours]	N/M[b]	Tx	N/M[b]	Tx	N/M[b]	Tx	N/M[b]	N/M[b]
		183		31		19		
		Rx		Rx		Rx		
		825		119		51		
Security	AES128	AES128	AES128	AES128	AES128	AES128	AES128	AES128
		at		at	256	at		at
		code		Module	SSL3	code		code
		level		and	TLS1	level		level
				code	HTTPS			
				level	RSA			

Expt[a] = experiment results; N/Mb = not mentioned