Exploiting Modbus Protocol in Wired and Wireless Multilevel Communication Architecture

Giuliano B. M. Guarese, Felipe G. Sieben, Thais Webber, Marcos R. Dillenburg*, César Marcon

PPGCC – Programa de Pós-Graduação em Ciência da Computação
PUCRS - Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, Brazil
**Novus Produtos Eletrônicos Ltda., Porto Alegre, RS, Brazil*

{felipe.sieben, giuliano.guarese, thais.webber}@acad.pucrs.br, dillen@novus.com.br, cesar.marcon@pucrs.br

***Abstract*—This paper proposes an architectural improvement for the Modbus RTU protocol to integrate equipments in industrial automation networks, employing hybrid communication with wired Modbus RTU and wireless IEEE 802.15.4. These environments have different electromagnetic interferences, requiring protocols with noise immunity to varied equipments such as motors and generators. Modbus RTU is a simple and robust master-slave protocol that accepts the integration of a master with up to 247 slaves into a bus topology. In addition, the IEEE 802.15.4 protocol emerged recently as a wireless solution to industrial environments since it allows electromagnetic spectrum evaluation, and the choice of avoiding communications in noise frequencies and decreasing the error rate between packets. The proposed hybrid communication protocol increases control and topological limits imposed by Modbus RTU by enabling a wired/wireless tree-bus topology and master multiplexing. Moreover, the academy-industry cooperation resulted in features implemented in a gateway, whose efficiency is evaluated with practical experiments in different topologies.**

Keywords - Modbus RTU; IEEE 802.15.4; Wired/Wireless hybrid network; Modbus master multiplexing.

I. INTRODUCTION

Especially in industrial manufacturing automation, the Modbus RTU (Remote Terminal Unit) protocol has a large field of application. Furthermore, Modbus is adopted for its simplicity, open specification and wide range of products by multiple manufacturers [1]. Modbus RTU is a robust data communication protocol designed for use in industrial environments, although fairly simple. It is based on master-slave architecture allowing a master to control up to 247 slaves in a network [2].

The current trend of adopting wireless communication solutions has originated a new competition to the definition of communication standards, for example: ZigBee, Wireless HART and ISA100.11a. Regardless of the standards that will prevail, IEEE 802.15.4 protocol stands as a robust protocol that defines the physical and data link layers. Moreover, IEEE 802.15.4 based protocols allow many types of communication in wireless networks with operating frequency (2.4 GHz) divided into 16 channels. The protocol provides assessment of the electromagnetic spectrum of channels, and allows selecting the best frequency, in the moment of channel choice, with less interference. In order to reduce energy consumption, the protocol may reduce the network traffic by sleeping devices that are not communicating. This procedure improves the operating time of battery-powered equipments. Given that the wireless medium has limitations with respect to safety, this standard protocol provides an encryption system for communication between network nodes. In addition, IEEE 802.15.4 provides two basic network topologies (peer-to-peer and star), low maintenance, and high flexibility and scalability [3][4].

Efficient operation on distributed control plants or services may require the use of heterogeneous networks composed by wired and wireless communication systems. Several works are dedicated to evaluate and/or propose these heterogeneity with a diversity of communication protocols [5][6][7]. Similarly, this paper describes a hybrid wired/wireless network, where RS485 wired segments with Modbus RTU protocol are connected through IEEE 802.15.4 wireless links. Using the bus topology of wired architecture, with star topology of wireless architecture, the architecture proposed in this paper may perform a scalable tree-bus network topology. Innovative resources to the Modbus protocol such as master multiplexing are also addressed.

This paper is organized as follows. Section II discusses related work on the chosen protocols, and a comparison between this work and other implementations. Section 0 presents the theoretical background underlying the proposed communication protocol. Section IV discusses the developed gateway, its communication interfaces, main features, the system layered structure, and the functionality provided by the application layer. Section V shows the set of tests executed over the implemented gateway that enables to perform hybrid architecture. Section 0 presents final considerations and conclusions.

II. RELATED WORKS

Leyva et al. [8] addresses the development of a wireless system capable of testing up to 4 remote slave units that use the Modbus RTU protocol to communicate with a master via radio modem. This system comprises a master unit, which permanently runs a graphical software, which requests information from remote slave units. Each slave unit can be up to 4 km away via radio modem, using the wireless physical media on the 900 MHz band to communicate. The function of each slave unit is to

Financial support granted by CNPQ and FAPESP to the INCT SEC (National Institute of Science and Technology Embedded Critical Systems Brazil), processes 573963/2008-8 and 08/57870-9; CAPES-Brazilian Ministry of Education (PNPD project 058792/2010); Novus Produtos Eletrônicos Ltda.

978-0-7695-4929-3/12 $26.00 © 2012 IEEE
DOI 10.1109/SBESC.2012.12

Authorized licensed use limited to: Pontificia Universidade Catolica do Rio Grande do Sul (PUC/RS). Downloaded on November 11,2022 at 20:17:55 UTC from IEEE Xplore. Restrictions apply.

monitor measurements in a three-phase power grid and make them available to the master unit.

Carlsen et al. [9] present a system that uses Modbus RTU protocol and a proprietary protocol based on IEEE 802.15.4 (named DUST Wireless) to monitor temperature data, aiming the prevention of leaks in oil and gas wells. The system consists of a gateway that integrates a Modbus RTU network over RS232 or RS485 to a WSN based in DUST protocol, which operates in a mesh topology. Temperature sensor nodes that communicate with the gateway via DUST wireless protocol were also developed.

Yuhuang [10] describes the MZ (Modbus and ZigBee) communication protocol. The MZ was developed to cope with different communication protocols used by Programmable Logic Controllers (PLCs) in industrial environments. The system consists of a gateway that converts the Point-to-Point protocol (used by PLC Siemens S7-224) and Modbus (used by PLC XC3-24RT-E Xinjie) in a common protocol MZ, which is based on ZigBee. In this system, the integration between a computer and supervisory system in two PLCs is accomplished through three gateways that communicate by MZ protocol.

Table I outlines a relationship between our work and the systems developed in the above mentioned related works. With the exception of [8], all other works based their wireless communication protocols in IEEE 802.15.4.

TABLE I: COMPARISON BETWEEN RELATED WORKS.

Work	Protocols	Network topology	Maximum number of masters	Maximum number of slaves	Wireless range
Our	IEEE 802.15.4, Modbus	Star Tree-bus	2	247	1,2 km
[8]	Modbus, Radio modem 900MHz	Star	1	4	4 km
[9]	IEEE 802.15.4, Modbus	Mesh	Not available	Not available	25 m
[10]	ZigBee, PPI, Modbus	Star	1	Not available	Not available

Among solutions developed in the literature, at the best of the authors' knowledge, only the proposed solution in this paper demonstrates a hybrid communication between two protocols allowing the segmentation and integration of Modbus networks. Other gateways implement specific solutions, where only a slave or purely wireless sensor nodes are integrated into the Modbus network. Since related works exploited Modbus protocol, it is remarkable how strong the acceptance of this protocol in industrial environments is. However, only this paper presents a solution enabling the use of more than one master on the Modbus network, which is a controllability improvement.

III. THEORETICAL REFERENCE

A. IEEE 802.15.4 Protocol

The IEEE 802.15.4 protocol specifies the Physical Layer (PHY) and the Medium Access Control (MAC). This standard aims to construct a Wireless Personal Area Network (WPAN). WPAN are networks that require information transmission over relatively short distances. This standard is maintained by the IEEE 802.15 WPAN ™ Task Group 4 (TG4), aiming to build a network of low transfer rates to implement wireless networks of low energy consumption. This network is called Low Rate WPAN (LR-WPAN). Making a comparison with the seven layers of the Open Systems Interconnection model (OSI), the IEEE 802.15.4 standard operates in the physical and data link layers, respectively, equivalent to PHY and MAC layers of the standard.

The IEEE 802.15.4 standard defines two basic types of device to function on a network: (i) the Full-Function Device (FFD), which contains all the functions defined by the standard as well as aims to start and coordinate a network of sensors; and (ii) the Reduced-Function Device (RFD), which is a limited function device that communicates exclusively with a FFD, and perform sensing with low energy consumption.

Figure 1 shows that depending on the application requirements, two network topologies can be implemented using the IEEE 802.15.4 standard: (i) *star topology*, where a FFD device, called the PAN Coordinator, starts a network centralizing the communication flow. Other devices that can be both FFDs and RFDs are communicating with the central PAN Coordinator; and (ii) *peer-to-peer topology*, where there is no centralized communication flow, thus all FFDs devices can communicate. In addition, based on these two basic network topologies, other topologies can be implemented to create a network layer that manages the information flow.

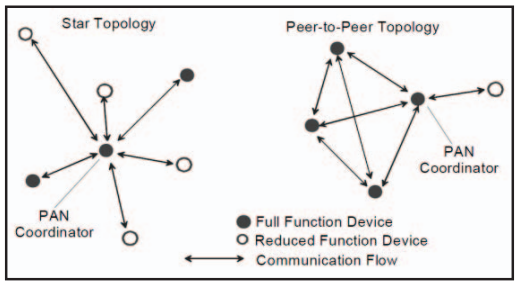

Figure 1. Network topologies supported by IEEE 802.15.4 protocol [11].

B. Modbus Protocol

The Modbus protocol is openly published, and defines a way to exchange data between PLCs. Since 2004 the Modbus protocol is maintained and controlled by the Modbus-IDA, which is a community of users and suppliers of automation equipment. This community seeks to openly maintain and control the Modbus protocol upgrade and standardization, in such a way that it can be used by several products maintaining compatibility regardless of the manufacturer.

Figure 2 shows that Modbus protocol operates at the application layer based on client/server architecture, in which the server only works from a client request. This protocol provides an interface for communication between devices connected on different types of networks.

Authorized licensed use limited to: Pontificia Universidade Catolica do Rio Grande do Sul (PUC/RS). Downloaded on November 11,2022 at 20:17:55 UTC from IEEE Xplore. Restrictions apply.

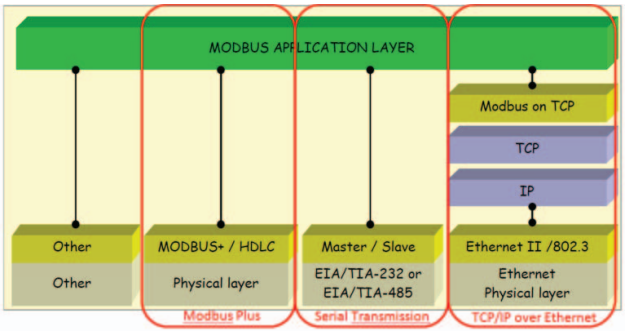

Figure 2. Structure of Modbus protocol layers [2].

Different communication interfaces can be used. However, Modbus protocol is currently implemented using:

- *TCP/IP over Ethernet* - This mode implements data encapsulated in binary format, in frames TCP (Transmission Control Protocol), using the Ethernet protocol (IEEE 802.3). The medium access control used is the Carrier Sense Multiple Access with Collision Detection (CSMA-CD);
- *Serial Transmission* - This mode operates on varied physic mediums (wire, fiber optics and radio). The main protocols that operate in wire physic medium are: EIA/TIA-232-E (known as RS232), EIA-422 (known as RS422) and EIA/TIA-485-A (known as RS485). The serial transmission mode has two variants: (i) Modbus RTU - data is transmitted in 8-bit binary format, where integers from -32768 to 32767 are represented by two bytes; (ii) Modbus ASCII - data are transmitted in 7-bit ASCII format, i.e., readable messages but much larger, causing a higher traffic on the network.
- *Modbus Plus* - This mode implements a network of high-speed transfer with many additional features for routing, diagnosis, data consistency and addressing. Although more robust and efficient, this mode lacks an open specification, since it is domain of Schneider Electric.

IV. DEVELOPED SYSTEM

A. Gateway Interfaces

In academy-industry cooperation (PUCRS and Novus), a gateway was developed to enable the conversion between Modbus RTU over RS485 and IEEE 802.15.4. This conversion is transparently performed to the Modbus network, providing a replacement of long structured cabling stretches for wireless segments. As can be seen in Figure 3, each gateway device has three communication interfaces. An USB interface is provided to facilitate configuration and connection to SCADA (Supervisory Control and Data Acquisition) systems. To communicate with Modbus RTU master and slaves, two connectors are available for a RS485 interface, which have their functionality according to the operation mode the gateway is configured. The IEEE 802.15.4 wireless interface is used for communication between gateways arranged in a star topology, whereas a network gateway coordinator can communicate with up to 247 gateways (Modbus addressing limitation), and those can be connected to Modbus RTU slaves.

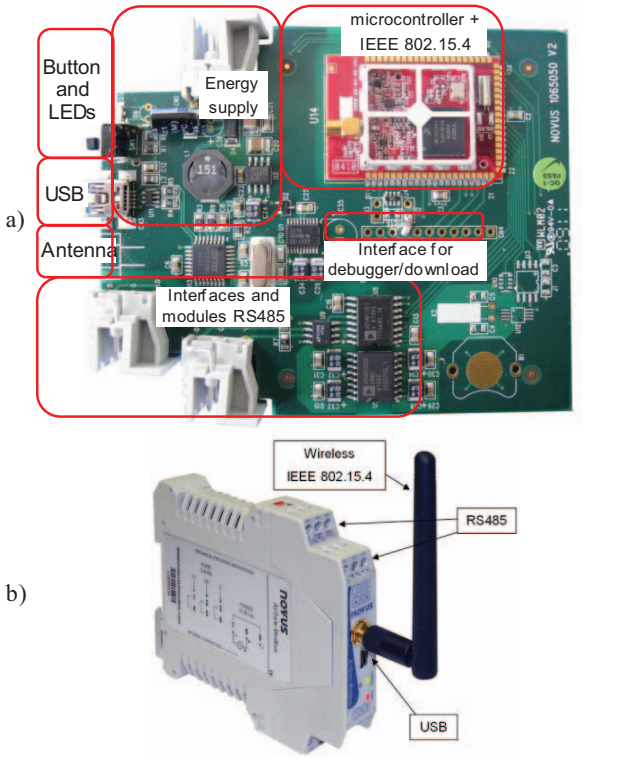

Figure 3. Gateway details with a) board layout, b) Novus™ product design.

Many industrial applications using Modbus RTU networks require more than one master Modbus. Examples of these applications are: (i) a system with SCADA software and a data logger device, or (ii) a system with SCADA software and a human-machine interface. Modbus RTU does not allow more than one master on the same Modbus network. In order to improve this protocol, the gateway implements master multiplexing, allowing two masters to control the same network.

B. Gateway Layers

Figure 4 shows the gateway with three independent protocols in the first layer of OSI model: (i) IEEE 802.15.4 PHY - responsible for providing an interface to access wireless physical medium; (ii) USB PHY - responsible for providing an interface to USB media access; and (iii) RS485 PHY - responsible for providing an interface to access the RS485 physical layer.

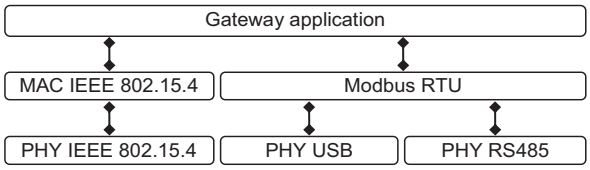

Figure 4. Gateway layers.

Authorized licensed use limited to: Pontificia Universidade Catolica do Rio Grande do Sul (PUC/RS). Downloaded on November 11,2022 at 20:17:55 UTC from IEEE Xplore. Restrictions apply.

At the second level of the OSI model there are two protocols: (i) IEEE 802.15.4 MAC - responsible for providing control functions of association, and network communication in a star topology; and (ii) Modbus RTU - responsible for recognizing received and transmitted packages via RS485 and USB PHY protocols. Finally, equivalent to the third level of OSI model, the gateway application layer is responsible for routing packets received by each one of the three communication interfaces.

IEEE 802.15.4 Layers: PHY and MAC

Along with MAC layer there has been developed a transport sublayer. This sublayer is responsible for providing the transport of a unit data up to 4096 bytes for the application layer. This sublayer is needed because the IEEE 802.15.4 protocol provides a data payload of 112 bytes, for filling in the application layer, and the Modbus RTU protocol that can take a maximum ADU (Application Data Unit) of 256 bytes. The availability of 4096 bytes refers to the fact that some devices do not follow the Modbus protocol rules using an ADU greater than specified. Thus, the transport sublayer allows data packets up to 4096 bytes.

Wireless systems are inherently vulnerable to attacks. Unlike wired systems, the media access is not restricted. In order to prevent this occurrence, a control device association and disassociation sublayer was established by the MAC layer to ensure that only registered equipment can communicate. The control sublayer uses data encryption AES-CBC-128 as specified by IEEE 802.15.4, where a common 16-bytes key is shared by all network devices. Thus, data packets transmitted over the IEEE 802.15.4 wireless interface are recognized only if the receiver has the encryption key configured correctly.

Modbus RTU Layer

This layer creates a link between the application layer and the USB and RS485 interfaces. For each interface is provided a buffer for transmission and reception of 4096 bytes. Thus, even devices with data packets exceeding the maximum size will be recognized, having their messages forwarded to the correct recipient. Following the timing requirements of the Modbus standard, packets received by the USB and RS485 interfaces are buffered and sent to be routed by the application layer. Packets received from the application layer are forwarded and transmitted to the requested interface.

Application Layer

The gateway has a fairly complex application layer responsible for routing messages that can be received by USB, RS485 or IEEE 802.15.4. It is also responsible for multiplexing masters and for the possibility of deploying a network topology of tree-bus, using hybrid architecture with IEEE 802.15.4 and Modbus RTU.

Following, the operation modes created by the application layer are presented, since application layer provides the functionality needed for the deployment of different network topologies and applications.

a) RS485-Slaves Operation Mode

Figure 5 shows gateways operating in mode RS485-Slaves, which are intended to continue the Modbus network. A gateway uses the IEEE 802.15.4 wireless interface to communicate with another gateway, where the master is placed. The RS485 interface is used to communicate with Modbus slaves. The gateway operates as RFD searching for a FFD, and remains paired after network boot.

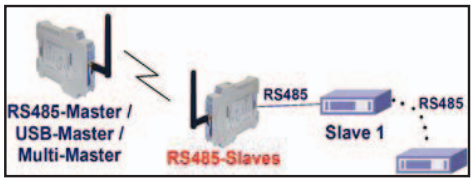

Figure 5. Operation Mode RS485-Slaves.

b) RS485-Master Operation Mode

Figure 6 illustrates the operation of RS485-Master mode, in which the gateway uses the RS485 interface to communicate with a Modbus network. Operating as FFD, the gateway performs the function of coordinator in the IEEE 802.15.4 network, initializing the network on a channel previously selected by the ED (Energy Detection) algorithm [11].

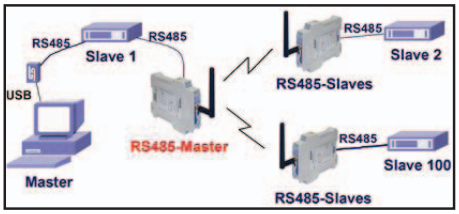

Figure 6. Operation Mode RS485-Master.

The gateway waits for association requests of other gateways operating in mode RS485-Slaves thus extending the wired segments. Subsequently, the gateway waits for Modbus messages, and starts routing them to the network segment in which the message recipient is located. The response messages received from the IEEE 802.15.4 wireless interface are routed directly to the RS485 interface.

c) USB-Master Operation Mode

Similar to the RS485-Master operating mode, in USB-Master mode the gateway also operates as FFD initializing and coordinating the network (Figure 7).

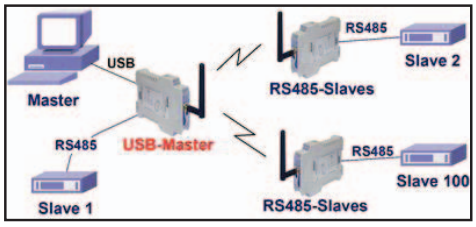

Figure 7. Operation Mode USB-Master.

Authorized licensed use limited to: Pontificia Universidade Catolica do Rio Grande do Sul (PUC/RS). Downloaded on November 11,2022 at 20:17:55 UTC from IEEE Xplore. Restrictions apply.

However, the gateway uses the USB interface to communicate directly with a Modbus master, and the RS485 interface to communicate with a network of Modbus slaves.

d) Multi-Master Operation Mode

Figure 8 shows a gateway operating as FFD, in Multi-Master mode, which uses its RS485 and USB interfaces for multiplexing Modbus masters.

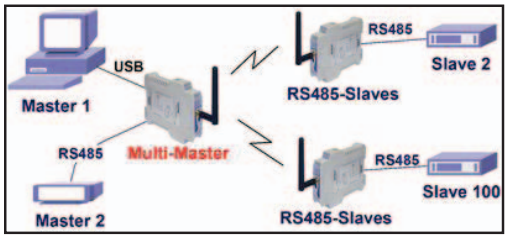

Figure 8. Operation Mode Multi-Master.

The gateway multiplexes requests from Masters (1 and 2), sending them to the respective segment where the slave is addressed. This occurs transparently to the Modbus network, so only the master who requested the information receives the response, and no collision occurs between requests of masters.

V. EXPERIMENTAL ANALYSIS

This section addresses one of the tests used to verify the system's functionality. The goal is to provide an experimental setup in a multi-level architecture that covers all operation modes.

The experimental setup contains a computer (Master 1 and 2), 10 gateways and 13 slaves, performing a tree-bus topology with three levels of hierarchy, each level specified by a given PAN ID.

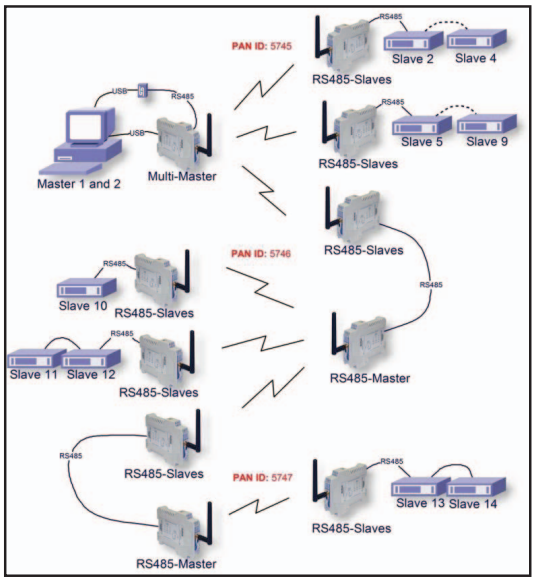

Figure 9. Experimental setup.

As can be seen in Figure 9, the computer is connected to a gateway, which operates in Multi-Master mode, directly via USB interface (Master 1), and indirectly via USB-RS485 converter (Master 2). Each one of the two communication ports of the computer was used by an instance of Master software.

The two masters request the reading of the registers of slaves located on all three levels of depth in the network: (i) at level 1 (PAN ID: 5745) there are three slave segments where: (a) in the first of the three segments there are slaves addressed from 2 to 4; (b) in the second segment are located slaves addressed from 5 to 9; (c) in the third segment there are two gateways used to expand the range of the network, giving rise to a new depth level; (ii) at level 2 (PAN ID: 5746) there are three segments of slaves: (a) in the first segment there is a slave with address 10; (b) in the second segment there are two slaves with addresses 11 and 12; (c) in the third segment, a new pair of gateways is installed to expand the range of the network; (iii) at level 3 (PAN ID: 5747) are located two slaves with addresses 13 and 14. To validate communications with different packet sizes, the masters request a different number of registers for each slave (Table II). In addition, the size of the request packet is 8 bytes for each slave.

TABLE II: SUMMARY OF MASTERS REQUEST.

Slaves	Number of requested registers	Response packet size
2, 3, 4, 10	10	26 bytes
5, 6, 7	80	166 bytes
9, 11, 12, 13, 14	125	256 bytes

Table III and Table IV show a quantitative assessment of data submitted by the master for each slave: (i) slave network address; (ii) depth; (iii) number of transmitted packets; (iv) the amount of register read on every request; (v) size of each received packet; (vi) number of communication errors; and (vii) the percentage rate related to communication errors.

TABLE III: TEST RESULTS FROM MASTER 1 ON USB INTERFACE.

Slave address	Depth	Number of Tx packets	Number of regs	Size Rx packet	Number of errors	Error rate (%)
2	1	27592	10	26	107	0.39
3	1	27592	10	26	118	0.43
4	1	27592	10	26	118	0.43
5	1	27592	80	166	109	0.40
6	1	27592	80	166	58	0.21
7	1	27592	80	166	77	0.28
8	1	27592	125	256	97	0.35
9	1	27593	125	256	72	0.26
10	2	27593	10	26	236	0.86
11	2	27593	125	256	181	0.66
12	2	27593	125	256	80	0.29
13	3	27593	125	256	99	0.36
14	3	27592	125	256	90	0.33
Average error rate (%):		0.40	**Minimum error rate (%):**	0.21	**Maximum error rate (%):**	0.86

Both Table III and Table IV show data obtained by monitoring programs associated to Master 1 and 2, respectively. It is noticeable that slaves with Depth 1 present an error rate from 0.18% to 0.45%, whereas slaves with Depth 2 present error rates from 0.25% to 0.96%, and slaves with Depth 3 present error rates

Authorized licensed use limited to: Pontificia Universidade Catolica do Rio Grande do Sul (PUC/RS). Downloaded on November 11,2022 at 20:17:55 UTC from IEEE Xplore. Restrictions apply.

around 0.27% to 0.39%. The average error rate of the network was around 0.40% for Master 1, and it was approximately 0.39% for Master 2.

TABLE IV: TEST RESULT FROM MASTER 2 ON RS485 INTERFACE.

Slave address	Depth	Number of Tx packets	Number of regs	Size of Rx packet	Number of errors	Error rate (%)
2	1	27640	10	26	108	0.39
3	1	27640	10	26	79	0.29
4	1	27640	10	26	125	0.45
5	1	27640	80	166	85	0.31
6	1	27640	80	166	71	0.26
7	1	27640	80	166	85	0.31
8	1	27640	125	256	98	0.35
9	1	27639	125	256	50	0.18
10	2	27639	10	26	265	0.96
11	2	27639	125	256	171	0.62
12	2	27639	125	256	68	0.25
13	3	27639	125	256	76	0.27
14	3	27639	125	256	107	0.39
Average error rate (%):	0.39	**Minimum error rate (%):**	0.18	**Maximum error rate (%):**	0.96	

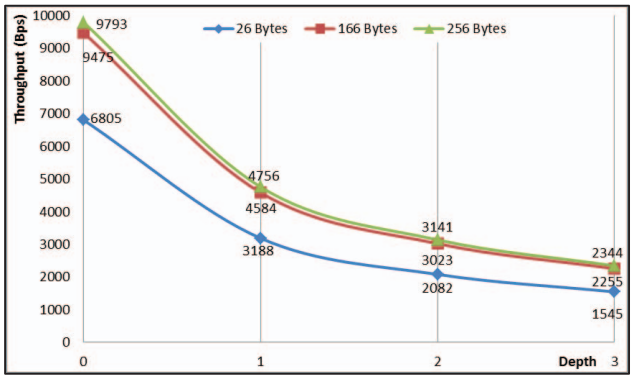

Figure 10. Throughput versus number of wireless steps.

All communication errors are handled by the application layer of the Modbus master to non-responded re-request packets. Thus, low error rates of a maximum of 0.96% are masked by the master. Therefore, the low error level demonstrates that our architecture does not compromise the overall system performance. Results show that there is no relation between the wireless depth and the error rate. On the other hand, Figure 10 shows that the throughput is dependent on the number of wireless steps, where Depth 0 represents the original Modbus protocol and Depths 1 to 3 represent the number of wireless steps. The throughput (in bytes per second) is compared with wireless depth, for different packet sizes: 26 bytes, 166 bytes and 256 bytes.

VI. CONCLUSION

The proposed wired/wireless multi-master architecture increases the spectrum of applications that can use the consolidated Modbus protocol. The multiple communication interfaces and the diversified operation modes enable the designed gateway to couple several applications such as new industrial automation projects as well as the possibility of maintenance of existing networks. The creation of a hybrid communication solution makes the Modbus protocol more attractive, since it allows Modbus networks to enjoy the wireless communication benefits joint with improvements such as masters multiplexing.

Therefore, this research contributes in many ways for innovations in industrial automation network, since several distributed control plants or services may require the use of heterogeneous networks composed by wired and wireless communication systems. Based on tests, the proposed architecture has presented a low communication error rate, indicating that the developed solution can meet the robust requirements of industry communication networks.

REFERENCES

[1] C. Wilson. **Common Industrial Communications Protocols**. *The International Journal of Thermal Technology, digital edition*, 2011.

[2] Modbus-IDA. **Modbus application protocol specification v1.1b**. 51 p. Dec. 2006.

[3] P. Neumann. **Communication in industrial automation—what is going on?.** *Control Engineering Practice*, v. 15, pp. 1332-1347, 2007.

[4] R. Bayindir, Y. Cetinceviz. **A water pumping control system with a programmable logic controller (PLC) and industrial wireless modules for industrial plants-An experimental setup**. *ISA Transactions*. v. 50, pp. 321-328, 2011.

[5] A. Flammini et al. **Wired and wireless sensor networks for industrial applications.** *Microelectronics Journal*. v. 40, pp. 1322-1336, 2009.

[6] H.-Y. Chen, C.-H. Lee**. Analysis of the number of hops in wired-wireless heterogeneous networks**. *IEEE WCNC*, pp. 1806-1810, 2012.

[7] A. Sameh, S. Wagh, Q. Salama. **Dealing with Quality of Service in Hybrid Wired-Wireless Networks**. *NETAPPS*, pp. 105-109, 2010.

[8] F. Leyva et al. **Wireless System for Electrical Networks Testing Based on MODBUS Protocol**. *Int.Conf.on Electronics, Communications and Computers (CONIELECOMP)*, pp. 58-62, 2004.

[9] S. Carlsen et al. **Using Wireless Sensor Networks to Enable Increased Oil Recovery**. *IEEE ETFA*, pp. 1039-1048, 2008.

[10] Y. Zheng. **MZ: An Ubiquitous Communication Protocol in Industrial Environment**. *Int. Conf. EBISS '09*, pp, 1-4, 2009.

[11] IEEE Standard. **802.15.4™ Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs).** *IEEE Computer Society*. 2003.

Authorized licensed use limited to: Pontificia Universidade Catolica do Rio Grande do Sul (PUC/RS). Downloaded on November 11,2022 at 20:17:55 UTC from IEEE Xplore. Restrictions apply.