Hindawi
Security and Communication Networks
Volume 2019, Article ID 7010717, 8 pages
https://doi.org/10.1155/2019/7010717

WILEY | Hindawi

Research Article

Enhancing Modbus-RTU Communications for Smart Metering in Building Energy Management Systems

Claudio Urrea and Claudio Morales

Grupo de Automática, Department of Electrical Engineering, Universidad de Santiago de Chile, Santiago, Chile

Correspondence should be addressed to Claudio Urrea; claudio.urrea@usach.cl and Claudio Morales; claudio.morales.d@usach.cl

Received 23 April 2019; Revised 6 September 2019; Accepted 24 October 2019; Published 16 November 2019

Academic Editor: Cristina Alcaraz

In this work, a method for detecting and correcting errors in Modbus-RTU communications is designed, implemented, and assessed in a smart metering application. This is a low-cost solution for improving communication quality in conventional Modbus-RTU architectures with copper fieldbus. It consists of introducing error detection and correction devices in the network segments most susceptible to errors caused by electromagnetic interference. Experimental validations were conducted and demonstrated the effectiveness of this method for isolating noisy segments in the communication bus, maintaining full compatibility with commercial devices and improving the performance of the entire network.

1. Introduction

Over the last years, the efficient use of energy has become a major concern around the world. The challenge of satisfying the increasing energy demand while reducing costs, seeking sustainability, and cutting carbon emissions has boosted research on smart energy management. Special importance has been given to building automation (smart buildings) and to smart energy generation and distribution on both large (smart grid) and small (microgrid and nanogrid) scales [1–3].

These energy management systems require smart metering to operate in a cognitive and adaptive way [4, 5]. Smart metering systems consist in measuring devices interconnected through networks and are able to share their measurements in real-time by means of local and distributed controllers. In these systems, security issues [6] and reliability are mandatory [7].

Communication networks are critical for the operation of energy management systems [3, 4]. Therefore, most efforts have focused on modeling, simulating, and implementing test systems in order to determine the most suitable communication protocols for the transmission of metered data and control signals to different devices from the power system [3–5, 8–13]. Research has explored the application of diverse wire and wireless technologies. In [8], the implementation of a microgrid that integrates smart metering is presented, and the real-time requirements of a network that integrates Modbus, CAN, TCP/IP and Ethernet protocols are studied. In [9], a monitoring system is introduced, which is used for the management of the energy needs of an agricultural production plant by means of a wireless communication network that incorporates Modbus and the IEEE 802.15.4 standard. In addition, Oliveira et al. [10] proposes a building automation system that integrates the existing electricity network and the information and communication architecture into a small-scale network (Home Area Network) by using devices with multiple communication protocols, including proprietary systems, Modbus over EIA-485, and an OPC-based middleware. Studies [11–14] present in-lab test systems for advanced research on smart grid communication, which are aimed at assessing the real-time communication features and vulnerability to cyberattacks in SCADA systems that use Modbus and TCP/IP standards as backbone. Finally, Chen et al. and Colmenar-Santos [15, 16] present the results of a real large-scale implementation for energy management and electrical variable monitoring. All those recent works demonstrate that Modbus-RTU protocol

is still part of power systems. In other words, despite the most recent advances on communications for power systems, Modbus-RTU communications still have applicability in field meters [17].

Typically, building automation systems and smart grids consists of a three-level architecture: (i) a field level where meters, sensors, and actuators are located; (ii) an intermediate layer where measurements are processed, control loops are executed, and alarms are activated; and (iii) a management layer in which data presentation and collection are conducted [5]. Although several alternatives exist for smart meters, which use different communication protocols and standards, it is widely acknowledged that Modbus-RTU over EIA/TIA-485 is the *de facto* communication standard for interconnecting metering devices at the field level [8, 10].

Modbus-RTU is a simple standard that has been extensively used and well tested in the industry since its invention in 1979. However, its simplicity limits the number of devices that can be connected to the bus, as well as some variables such as transmission speed and security. This fact has promoted the development of specific research lines aimed at enhancing Modbus-RTU communication to meet the current standards for building automation and critical infrastructure protection [18, 19]. This work focuses on that research line and proves the feasibility of improving communication quality in conventional Modbus-RTU architectures with copper fieldbuses through the introduction of error detection and correction devices into the network segments susceptible to errors caused by electromagnetic interference.

The paper is structured as follows. Section 2 presents the justification of this research and reviews the literature on the topic. Section 3 shows the conceptual basis for the proposed solution, while Sections 4 and 5 describe the test system used for validation and the results obtained, respectively. Finally, Section 4 presents the conclusions.

2. Justification and Related Studies

The growing concern of companies and institutions for optimizing electrical energy consumption has given rise to the need of implementing energy management systems in all buildings. New buildings deal with this aspect from their design stage, and thus, physical plants are conceived as integrating electrical, data, and safety systems. This need also extends to buildings designed decades ago such as historical or heritage structures whose physical plant was not meant to accommodate electrical, communication, and control systems simultaneously.

When installing smart metering systems in old buildings, technicians usually install equipment and wires using the racks and conduits holding power feeders, which in many occasions, have poor earthing for shielding communication lines. It is widely known that these conditions cause the communication bus to be more vulnerable to electromagnetic interference, and consequently, this increases the transmission error rate [20]. Moreover, the introduction of a great quantity of nonlinear elements (LED lamps, computers, etc.) that produce electromagnetic interference at 2 to 150 kHz frequencies (supraharmonic) increases the probabilities that close communication devices and lines be affected [21, 22].

One of the alternatives found in the market for solving this issue is substituting the copper fieldbus by optical fiber in areas especially prone to electromagnetic interference, but this material and its installation are costly. Another solution is using wireless communication on the 4-GHz band, and recent research has proposed solutions that combine the Modbus-RTU and Modbus/TCP protocols with the wireless communication standards Wi-Fi [20, 21] and IEEE 802.15.4 [23].

In contrast, the solution proposed in this work consists of using Forward Error Correction (FEC) to enhance communication in systems with conventional Modbus-RTU over an EIA/TIA-485 copper fieldbus. This alternative is economical and especially suitable for the implementation of energy management systems in facilities with segments prone to transmission errors caused by electromagnetic interference, for example, old buildings.

The proposed solution extends the scope of a previous study that dealt with error detection and correction systems for the Modbus-RTU protocol by means of systematic codes [24]. This system previously tested data transmission between a manipulator robot and its dedicated controller [25] but has not been validated with commercial equipment yet.

The method introduces additional bytes to the bus in order to detect and correct errors. These additional bytes are not part of the Modbus data frame. Therefore, it was necessary to validate the application of this method with commercial equipment to verify that the additional data did not lead to data collisions or problems to interpret the Modbus frame in devices directly connected to the bus.

In this work, the error detection and correction system is implemented in a typical energy management configuration, using commercial power meters to assess the effectiveness of the solution in ensuring error-free communications in a copper fieldbus channel with noise.

3. Basis of This Proposal

Modbus-RTU is the variant of the communication protocol Modbus, which is widely used for the transmission of industrial data at the field level. Its specifications are available to the public through two documents elaborated by the Modbus Organization: the MODBUS Application Protocol and the MODBUS Serial Line Protocol. The first protocol structures messages for the application layer in a client/server mode [26], while the second specifies a master/slave architecture for the data link layer, for the ASCII (American Standard Code for Information Interchange) transmission protocol and the Remote Terminal Unit (RTU), as well as the requirements for their implementation in EIA/TIA-485 and EIA/TIA-232 lines [27].

Modbus-RTU establishes a single message structure comprising four fields: address, function, data, and Cyclic Redundancy Check (CRC) verification. The first three fields contain the necessary information for the transaction, while the forth corresponds to the 16-bit CRC calculation, which is aimed at detecting errors. The structure of the data frame is shown in Figure 1.

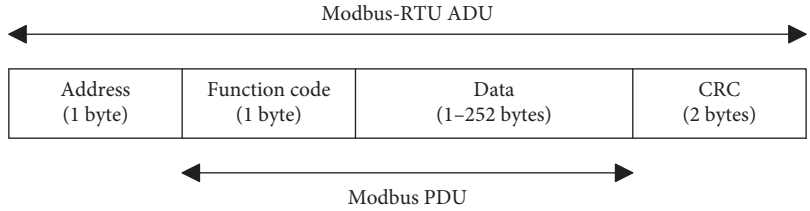

Figure 1: Data frame in Modbus-RTU.

During transmission, the CRC value is calculated from data contained in the address, function, and data fields and then transmitted as part of the message. During reception, the CRC value is calculated again based on the address, function, and data received before and then compared to the received CRC value. If both values coincide, the message is considered valid and processed. Otherwise, the message is regarded as corrupted and discarded without sending any notification [27].

The CRC-based error detection system is simple and very effective to prevent the processing of incorrect messages, yet it presents two disadvantages: (1) since the master does not get any notification in case of transmission errors, the only mechanism for detecting a failed transaction is to wait for the timeout to conduct a retransmission, which hinders network performance; (2) when all slaves receive the same requirement (broadcast), the Modbus protocol orders slaves to execute it without sending any confirmation to the master. As a consequence, if a slave receives a corrupted broadcast message, the master has no way of knowing that the slave discarded the message and therefore the requirement was not executed. Due to the above, the performance of the Modbus-RTU network can be severely impaired by repeated timeouts and retransmissions if there is a high rate of transmission errors, as it may be the case in environments with high electromagnetic interference.

The method proposed in [24] allows the improvement of transmission quality in Modbus-RTU communications in environments with high electromagnetic interference. This is performed using retransmitters able to detect and correct errors on the receptor side by employing systemic codes like Reed–Solomon's, as shown in Figure 2. During transmission, each repeater/error-corrector (R/C) device sends the message sent by the end device again and introduces additional parity characters while keeping compatibility with the protocol. The R/C device on the side of the receptor takes the message and parity characters to recompose the original message in case of transmission errors and then retransmits it to the end device without errors.

To maintain full compatibility with the protocol, parity characters need to be transmitted after a time longer than 3.5 characters—as defined in the Modbus-RTU protocol for the detection of message ends—and before any device sends a reply, in order to avoid data collision. These timeframes exist in any transaction, although their duration varies and depends on the response speed of the devices connected to the network.

Figure 3 shows the use of the bus in different points of the network for a transaction containing transmission errors between the master and slave n. This method enhances transmission quality in Modbus-RTU communications but delays any transaction between master and slave. However, since polling rates in energy management systems are relatively long and requirements for real-time communication are inexistent in general, this method is feasible for improving the quality of service in this type of applications.

4. Test System

To assess the performance of Modbus-RTU communications in the presence of noise in the communication bus, a test system was implemented. The test system consists in interconnecting four metering devices for energy management systems, manufactured by Schneider Electric. The devices used were the following:

(i) PowerLogic ION7400 meter: this is a high-range meter with a RS-485 communication interface and a two-port Ethernet switch, which is used as a Modbus master to communicate with other connected devices. This device also integrates a web server that grants remote access to the information recorded by the network meters.

(ii) PowerLogic VarPlus Logic VL12 power factor controller: this is a device used for compensating power factor which delivers measurements of electrical parameters as well as information about capacitor banks by means of an RS-485 communication interface. The slave 10 address is assigned to this controller.

(iii) PowerLogic PM5110 meter: this is a medium-range meter with an RS-485 communication interface. The slave 20 address is assigned to this meter.

(iv) PowerLogic PM870 meter: this is a medium-range meter with an RS-485 communication interface. The slave 30 address is assigned to this meter.

Figure 4 shows the architecture of the implemented network, which represents a conventional energy management system. This architecture includes (A) Ethernet link, (B) Main meter: Modbus master and web server−, (C) EIA/TIA-485 bus, and (D) Modbus slaves. Following the manufacturer recommendations, the Modbus-RTU network was set at a transmission rate of 19200 bps with 8N1 data format (8 bits of data, no parity, and one stop bit). The physical interconnection between devices is conducted through daisy chain.

Hardware includes twisted pair 24AWG wires, nonshielded, and terminal blocks on all devices. The total length

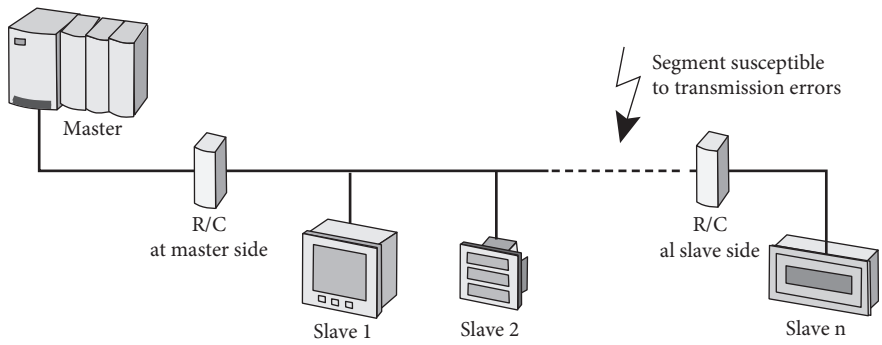

Figure 2: Implementation of error detection and correction method in Modbus-RTU communications by means of systemic codes [24].

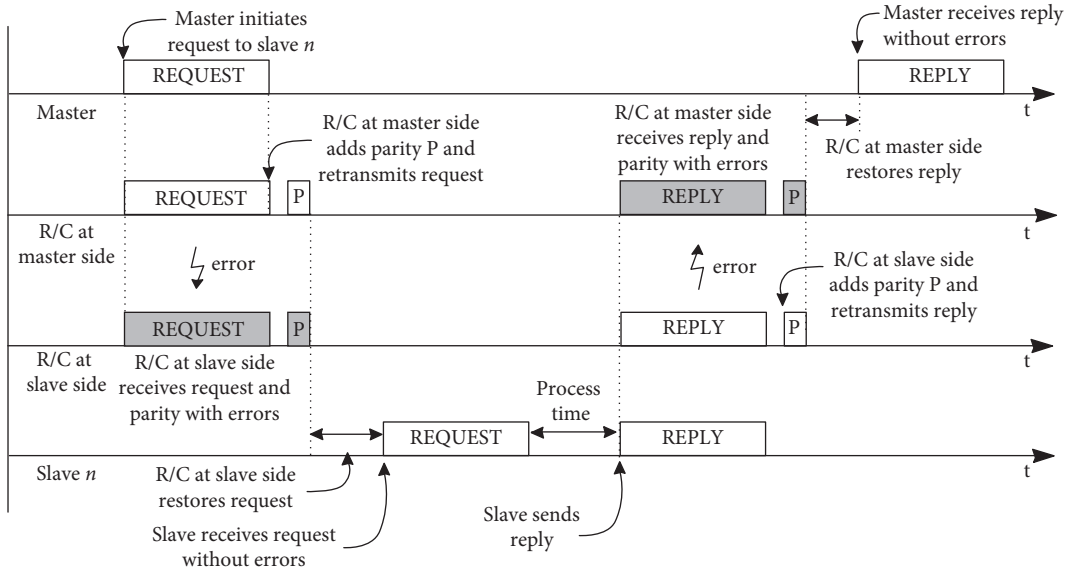

Figure 3: Error detection and correction process for Modbus-RTU communications using systemic codes [24].

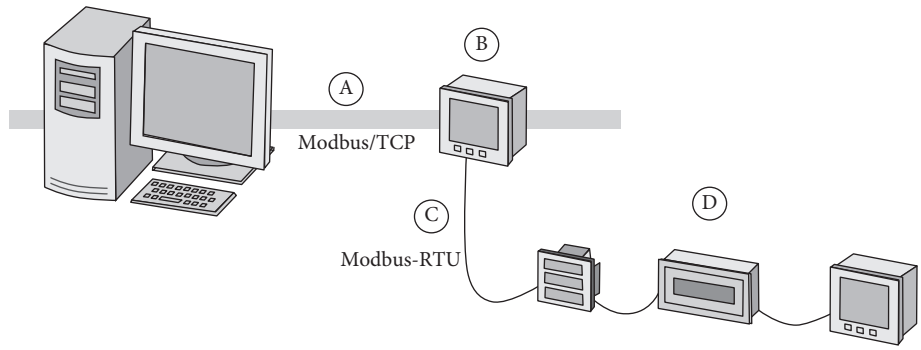

Figure 4: Implemented network architecture: (A) Ethernet link, (B) Main meter: Modbus master and web server, (C) EIA/TIA-485 bus, and (D) Modbus slaves.

of the bus was 50 meters. 120-ohm termination resistors are set on both sides. The test system also comprised a white noise generator and a digital oscilloscope. The former is connected to the communication bus to cause transmission errors, while the latter is used for monitoring the communication bus.

To detect and correct errors, Reed–Solomon RS(255,251) coding and decoding are used. Reed–Solomon RS(255,251) inserts two additional characters to the Modbus frame. These characters allow the detection and correction of random errors that may affect one byte per message. To assess the

performance of the system, algorithms for measuring bit error rate and message error rate are added.

To measure the bit error rate (BER), reference messages are defined to compare received messages. In the test system, these messages are selected from information requests that return fixed values from the meters. The received message is compared to the reference message character by character and bit by bit, and the number or incorrect bits is stored in an accumulator called Nerror_bits. The total number of bits received is stored in other accumulator called Nreceived_bits. The BER value is calculated based on BER = Nerror_bits/Nreceived_bits.

The measurement of the message error rate (MER) is conducted in parallel, using the same reference messages. The total number of messages containing errors, Nerror_msgs, and the total number of received messages, Nreceived_msgs, are counted and then MER = Nerror_msgs/Nreceived_msgs is calculated.

The algorithms for measuring BER and MER, together with algorithms for error detection and correction, are implemented in two 32-bit and 80-MHz ARM Cortex-M4F microcontrollers by means of Texas Instruments Tiva Launchpad TM4C123G development boards. These devices act as error repeaters/correctors (R/C) and log the system performance information. The Tiva Launchpad boards are inserted in the communication bus by means of MAX485 transceivers, and recorded data are collected through a USB connection in a laptop. Figure 5 shows the internal structure of R/C devices.

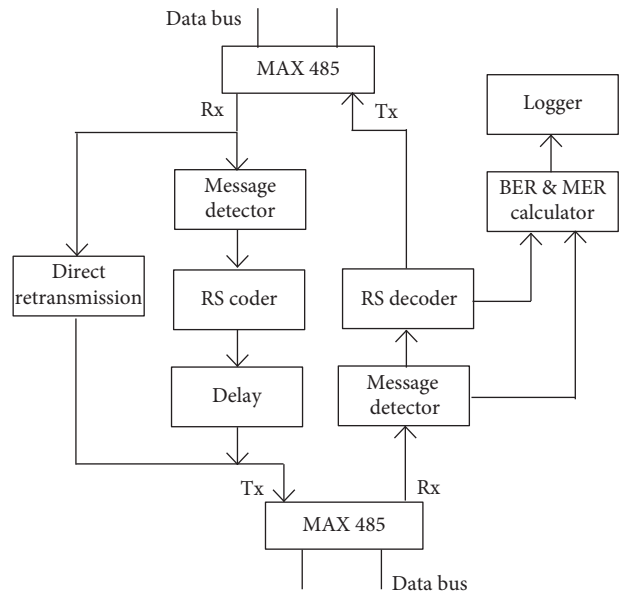

Figure 5: Internal structure of the R/C devices implemented in the test system.

Table 1: Reference messages.

Request	Expected response	Length
10 01 00 00 00 64 3d e1	10 81 02 c1 91	5 bytes
20 03 04 05 00 01 95 3b	20 03 02 41 c7 c9 86	7 bytes
30 03 0f a8 00 03 87 3f	30 03 06 00 00 00 00 00 00 21 75	11 bytes

5. Experimental Results

As a starting point, the system is configured and started following the instructions from the user's manual of each device. During commissioning, the white noise generator is not connected to the communication bus. In addition, the Modbus master is set to refresh data at a polling rate of 1 second, producing 3600 transactions per hour.

Data required for the slaves are selected in order to obtain records with nonvariable values from the meters. By expecting known responses from slaves, it is possible to compare the received responses to the reference messages and thereby calculate BER and MER. The reference messages defined are shown in Table 1.

Once the white noise generator is connected to the communication bus, the level of noise is adjusted until repeated errors appear in the transmission. The resultant signal-to-noise ratio was only 1.46 dB when using a signal level of ±7 volts as defined in the standard. The noise level introduced is kept constant during the test. Figure 6 presents the data recorded before and after noise is introduced, which were obtained from the digital oscilloscope.

The test system used represents a serial data bus that interconnects several measuring devices. These devices have segments susceptible to high electromagnetic interference, for example, the part of the bus that passes next to power supplies or very close to a group of high power nonlinear loads. In such cases, the electromagnetic interference introduced at that single point affects the communications of the entire bus. Considering this case, tests are carried out to study the effect of introducing R/C devices into two different configurations.

The configuration shown in Figure 7 is used for test 1. An R/C device is inserted next to the Modbus master, and other next to slave 3. The noise is inserted in the data bus segment between slaves 2 and 3.

The bit error rate and message error rate for the three slaves connected to the communication bus is measured under these conditions. After 3 hours of system operation, the values recorded are summarized in Table 2.

The implemented configuration makes the noise affect all the communication bus, but the error detection and correction method is only applied to the transactions between the master and slave 3. The transactions between master and slaves 1 and 2 are processed without error detection and correction. The results show a high rate of corrupted messages for slaves 1 and 2, whereas this rate is considerably reduced in transactions between slaves 1 and 3, thanks to the R/C devices.

In test 2, the error detection/correction location is changed according to Figure 8. Noise is inserted again in the data bus segment between slaves 2 and 3.

Under these conditions, the bit error rate and message error rate are measured again in the three slaves connected to the communication bus. After 3 hours of system operation, the recorded values are summarized in Table 3.

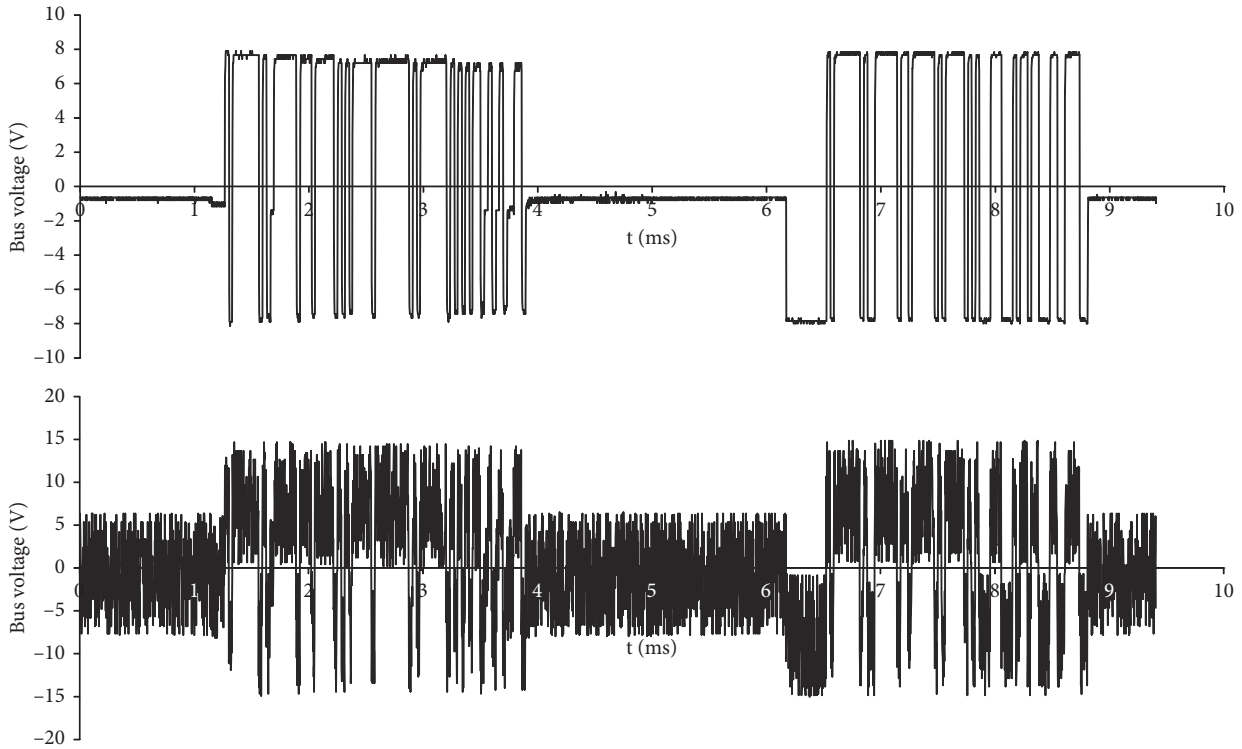

Figure 6: Signal in the communication bus. (a) Without white noise. (b) With white noise added.

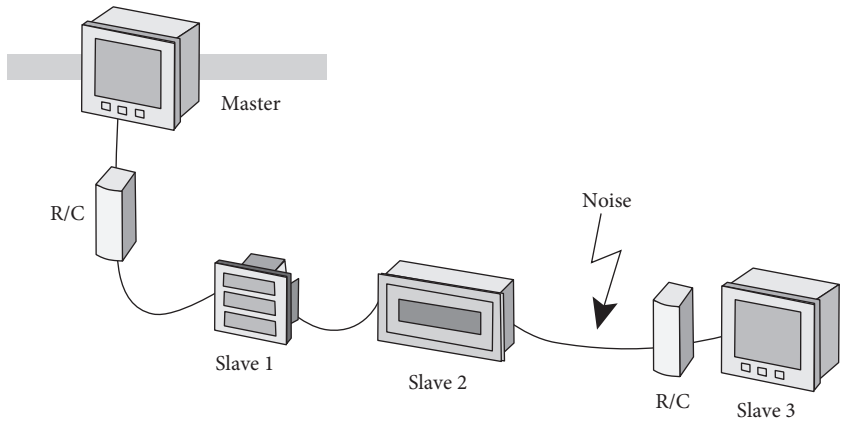

Figure 7: Test 1 configuration.

Table 2: Results for test 1.

Transaction	Messages transmitted	Bits transmitted	Corrupt messages	Error bits	BER	MER
Master: slave 1	10800	691200	529	612	$8.85e{-4}$	$4.90e-2$
Master: slave 2	10800	691200	617	764	$1.11e{-3}$	$5.71e-2$
Master: slave 3	10800	691200	14	37	$2.03e{-5}$	$1.30e-3$

In the second configuration, the noise introduced is isolated in the bus segment between slaves 2 and 3, where transactions are processed by R/C devices, maintaining a low error rate in the whole network. Transactions between master and slaves 1 and 2 are processed again without error detection and correction. However, in this case, the noise is isolated by R/C devices, and therefore, transactions are not affected by it. It must be noted that no transmission errors were detected during the test time. The corrupted messages present in master and slave 3 transactions are those that

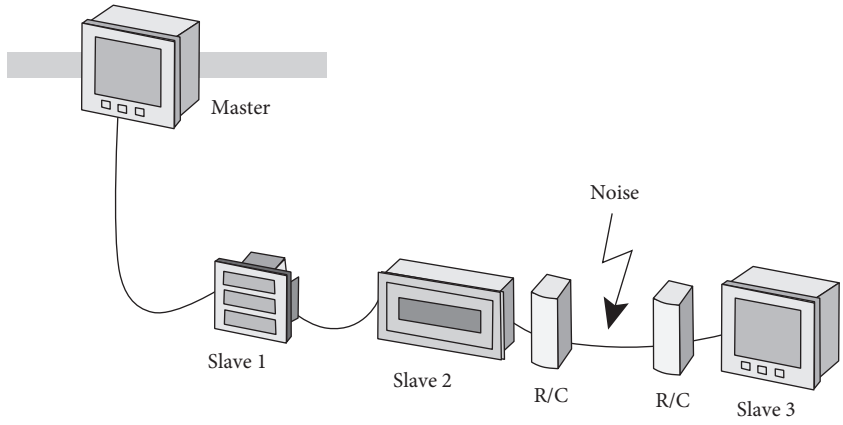

Figure 8: Test 2 configuration.

Table 3: Test 2 results.

Transaction	Messages transmitted	Bits transmitted	Corrupted messages	Incorrect bits	BER	MER
Master: Slave 1	10800	691200	0	0	—	—
Master: Slave 2	10800	691200	0	0	—	—
Master: Slave 3	10800	691200	12	35	$5.06e{-5}$	$1.11e{-3}$

exceed the correction effectiveness of the implemented RS(255,251) code.

6. Conclusions

The results show the feasibility of isolating segments of the communication bus that were more susceptible to electromagnetic interference by introducing error detection and correction devices into them. Through this solution, it was possible to maintain full compatibility with commercial devices and the performance of the entire network was improved.

The tests were carried out using a network interconnecting several commercial devices and proved the feasibility of employing this method in real smart metering networks for energy management. We also concluded that the proposed error detection and correction method for Modbus-RTU communications is able to deal with high levels of noise in segments of the data bus. By adding R/C devices to specific critical points of the communication bus, it would be possible to achieve adequate performance in smart metering networks, even if those points are subjected to high levels of electromagnetic interference.

Furthermore, it was demonstrated that medium-range microcontrollers are enough to implement those R/C devices. Therefore, this solution is much more economical and simpler than optic fiber and wireless communications.

Further work in this line should include modeling electromagnetic interference induced by electrical feeders in order to define the characteristics of transmission errors occurring in a real communication bus and thereby determine the most suitable Reed–Solomon code for the detection and correction of errors in these systems. Finally, the validation of this method will be carried out in a real energy management system.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by Proyecto Fortalecimiento USACH USA1799_UC123012 and Vicerrectoría de Investigación, Desarrollo e Innovación of the Universidad de Santiago de Chile, Chile.

References

[1] M. L. Tuballa and M. L. Abundo, "A review of the development of smart grid technologies," *Renewable and Sustainable Energy Reviews*, vol. 59, pp. 710–725, 2016.

[2] D. Burmester, R. Rayudu, W. Seah, and D. Akinyele, "A review of nanogrid topologies and technologies," *Renewable and Sustainable Energy Reviews*, vol. 67, pp. 760–775, 2017.

[3] M. Yu and N. Ansari, "Smart grid communications: modeling and validation," *Journal of Network and Computer Applications*, vol. 59, pp. 247–249, 2016.

[4] K. Coffey, R. Smith, L. Maglaras, and H. Janicke, "Vulnerability analysis of network scanning on scada systems," *Security and Communication Networks*, vol. 2018, Article ID 3794603, 21 pages, 2018.

[5] P. Domingues, P. Carreira, R. Vieira, and W. Kastner, "Building automation systems: concepts and technology review," *Computer Standards & Interfaces*, vol. 45, pp. 1–12, 2016.

[6] P. S. Woo, B. H. Kim, and D. Hurr, "Towards cyber security risks assessment in electric utility SCADA systems," *Journal of*

Electrical Engineering and Technology, vol. 10, no. 3, pp. 888–894, 2015.

[7] W. F. Ravanales and A. R. Garcia, "Analysis of the regulatory requirements for the smart grid in Chile," *IEEE Latin America Transactions*, vol. 15, no. 1, pp. 13–20, 2017.

[8] D. A. Sbordone, L. Martirano, M. C. Falvo et al., "Reactive power control for an energy storage system: a real implementation in a micro-grid," *Journal of Network and Computer Applications*, vol. 59, pp. 250–263, 2016.

[9] E. Fabrizio, V. Branciforti, A. Costantino et al., "Monitoring and managing of a micro-smart grid for renewable sources exploitation in an agro-industrial site," *Sustainable Cities and Society*, vol. 28, pp. 88–100, 2017.

[10] M. Oliveira, F. Trojan, A. C. Francisco, and A. A. Xavier, "Digital energy management for houses and small industries based on a low-cost hardware," *IEEE Latin America Transactions*, vol. 14, no. 10, pp. 4275–4278, 2016.

[11] W. Ming, S. Yan, J. Yuan, and W. Junlu, "Function-aware anomaly detection based on wavelet neural network for industrial control communication," *Security and Communication Networks*, vol. 2018, Article ID 5103270, 11 pages, 2018.

[12] A. Tesfahun and D. L. Bhaskari, "A SCADA testbed for investigating cyber security vulnerabilities in critical infrastructures," *Automatic Control and Computer Sciences*, vol. 50, no. 1, pp. 54–62, 2016.

[13] R. Kowalik, D. D. Rasolomampionona, and M. Januszewski, "Laboratory testing of process bus equipment and protection functions in accordance with IEC 61850 standard. Part I: electrical arrangement and basic protection functions tests," *International Journal of Electrical Power & Energy Systems*, vol. 90, pp. 54–63, 2017.

[14] J. Jee-Hoon, "Test platform development of vessel's power management system using hardware-in-the-loop simulation technique," *Journal of Electrical Engineering & Technology*, vol. 12, no. 6, pp. 2298–2306, 2017.

[15] C. N. Chen, M. Y. Cho, and C. H. Lee, "Design and implementation of building energy management system," in *Proceedings of the 3rd International Conference on Green Technology and Sustainable Development Design*, pp. 106–111, Kaohsiung, Taiwan, November 2016.

[16] A. Colmenar-Santos, M.-Á. Pérez, D. Borge-Diez, and C. Pérez-Molina, "Reliability and management of isolated smart-grid with dual mode in remote places: application in the scope of great energetic needs," *International Journal of Electrical Power & Energy Systems*, vol. 73, pp. 805–818, 2015.

[17] S. Chih-Che, A. Hahn, and C. Liu, "Cyber security of a power grid: state-of-the-art," *International Journal of Electrical Power & Energy Systems*, vol. 99, pp. 45–56, 2018.

[18] G. W. Adhane and D. S. Kim, "Distributed control system for ship engines using dual fieldbus," *Computer Standards & Interfaces*, vol. 50, pp. 83–91, 2017.

[19] L. Alonso, J. Barbarán, J. Chen, M. Díaz, L. Llopis, and B. Rubio, "Middleware and communication technologies for structural health monitoring of critical infrastructures: a survey," *Computer Standards & Interfaces*, vol. 56, pp. 83–100, 2018.

[20] D. Reynders, S. Mackay, and E. Wright, "Practical industrial data communications: best practice techniques," in *Series. Practical Professional Books from Elsevier*, Elsevier Science, Amsterdam, Netherlands, 2004.

[21] G. F. Bartak and A. Abart, "EMI in the frequency range 2–150 kHz," Report 15P-B, vol. 1, IEICE, Tokyo, Japan, 2014.

[22] S. Rönnberg, *Emission and interaction from domestic installations in the low voltage electricity network, up to 150 kHz*, Ph.D. thesis, Luleå University of Technology, Luleå, Sweden, 2013.

[23] G. B. M. Guarese, F. G. Sieben, T. Webber, M. R. Dillenburg, and C. Marcon, "Exploiting Modbus protocol in wired and wireless multilevel communication architecture," in *Proceedings of the Brazilian Symposium on Computing System Engineering*, pp. 13–18, Florianopolis, Brazil, November 2012.

[24] C. Urrea, C. Morales, and R. Muñoz, "Design and implementation of an error detection and correction method compatible with MODBUS-RTU by means of systematic codes," *Measurement*, vol. 91, pp. 266–275, 2016.

[25] C. Urrea, C. Morales, and J. Kern, "Implementation of error detection and correction in the Modbus-RTU serial protocol," *International Journal of Critical Infrastructure Protection*, vol. 15, pp. 27–37, 2016.

[26] Modbus-IDA, *Modbus Application Protocol Specification V1.1b3*, Modbus-IDA, 2012, http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf.

[27] Modbus-IDA, *Modbus over Serial Lines Specification and Implementation Guide V1.02*, Modbus-IDA, 2006, http://www.modbus.org/docs/Modbus_over_serial_line_V1_02.pdf.