Benchmarking of Data Communication Protocol for Integration of Telecontrol Interface with RTU

* Muhammad Aamir, ** Nishat Ahmad Khan and *** B.S. Chowdhry

Abstract — **The outcome of this research work is focused on optimized the design of wireless link for an FPGA based Remote Terminal Unit (RTU). A situation representing multiple RTUs communicating with one Telecontrol Interface (TCI) developed to address optimized implementation of wireless SCADA. It was then further verified by means of benchmarking. The hardware implementation and verification of this particular RTU design has been done using a starter kit based on XILINX Spartan-3 Series FPGA with 500K logic gates and MHX-2400 frequency-hopping 2.4 GHz spread-spectrum communications module which is used as Telecontrol Interface. The FPGA based RTU is flexible in terms of I/Os, CPU and radio related configurations and any expansion in design can be accommodated quickly if needed as FPGA based designs are reconfigurable. However, the integration of MHX-2400 had been examined and found suitable as Telecontrol Interface for this development.**

Index Terms — **Supervisory Control and Data Acquisition (SCADA), Telecontrol Interface (TCI), Remote Terminal Unit (RTU), Received Signal Strength Indicator (RSSI), Packet Error Percentage.**

I. INTRODUCTION

Design of an optimal Remote Terminal Unit (RTU) is a key step in implementation of Wireless SCADA. For development of RTU, a comparative assessment of performance of both methodologies of RTU design is executed, one based on PLCs and other one based on FPGAs which finalized for development of RTU due to its better performance and reliability [1].

The transceiver module MHX-2400 is an embedded wireless data transceiver selected for this particular research work. Its range of operating frequency supports ISM band and it can varied between 2.4000 and 2.4835 GHz. This module uses Frequency Hopping Spread Spectrum (FHSS) technique to provide reliable link to transfer data between all kinds of available equipment that supports an asynchronous serial interface. There are several parameters that must be set in order to establish communication between a pair of MHX-2400 modules. The module may be configured as Master, Slave or Repeater module based on the intended use. Every network must have a Master; however the number of slave nodes may be in any number up to 200 in the desired network [2].

MHX-2400 module uses a command set which is analogous to standard AT style commands, so it can be simply programmed and resembles with those used by conventional telephone line modems. The data transmitted from RTU is being received through MHX-2400 for data integrity and graphical representation for which further benchmarking is done for data communication protocol. A general block diagram of Wireless SCADA components including TCI is shown in Fig. 1 (a) and the MHX-2400 transceiver is shown in Fig. 1 (b).

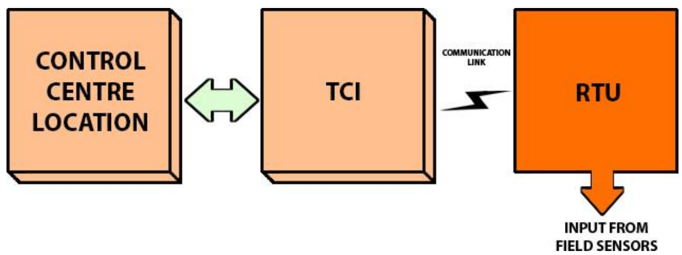

Fig. 1. (a) A general block diagram of Wireless SCADA components including TCI [1].

Fig. 2. (b) Microhard MHX-2400 Transceiver [3].

Basic concept for this project has been taken from the research work containing Performance Analysis of Wide area operation, control and protection using High Scale SCADA

* Department of Electronic Engineering, Sir Syed University of Engineering & Technology, Karachi. muaamir5@yahoo.com
** Advanced Engineering & Research Organization, Karachi. nisahmad@yahoo.com
*** Department of Electronics Engineering, Mehran University of Engineering & Technology, Jamshoro. c.bhawani@ieee.org

System by Muhammad Aamir [17] et al. As an important and necessary part of SCADA, Remote Terminal Units (RTUs) acquire current, voltage and frequency measurements for SCADA system. RTUs are installed at selected locations of different grid stations to acquire complete analog and digital data of the station. These RTUs are getting digital data from field instruments connected with relays to show and operate live status of Circuit breakers or isolators, however for analog data, transducers are connected with CT and PT.

Second encouragement was provided by the successful and low cost implementation of FPGA in real time remote monitoring system that acquires data from any kind of sensor to be transmitted by radio frequency to a computer with an interface module, situated within a 900 m radius designed by Joshua Mendoza-Jasso et al.

II. Integration of Telecontrol Interface

The module can be interfaced with the FPGA module through headers available on training board, serial (RS-232) interface and RS-485 interface [4]. In this practical scenario, MHX-2400 has been interfaced with Spartan 3E using header available on starter kit. The developed RTU contains 16 channels Digital Input, 8 channels Analog Input and 8 channels Relay/Digital Output. This section covers testing at the integration of software – hardware. References to technical manual of MHX-2400, various S Registers affect its operating characteristics ranging from S 101 to S 110 For example S register 101 and 102 are being used for setting operation modes and serial baud rate respectively [5]. Whereas S registers 103 and 104 deals with wireless link rate and network address. We have set fast link rate with forward error correction and maximum allowable serial baud rate which 115200 for which bench marking results will be discussed in next section. The other S registers are intended to set unit address, hopping patterns, encryption key, output power level, hopping interval, data format, packet size and packet size control.

The MHX-2400 has been configured in TDMA mode for communication. The operation of MHX-2400 had been verified in benchmarking described in next section. However, the link between RF module and FPGA has been verified in lab benchmarking using simple steps described below:

The housing of the development board is equipped with LED indicators which are being observed as slave unit in order to check the availability of communication link. As the link is established with good reception then up to three RSSI (received signal strength indicator) LEDs light up (RX/Sync LED) to show good signal strength on the Slave modem. On the other hand, these LED's will remain turned off if the link is open due to configuration or any other fault at either end. However scanning mode is also possible during search for network.

To check transfer of data, one possibility is to input few general characters typed at the master terminal so that the slave's can receive it in simple manner. The same scenario is also valid if slave wishes to initiate communication instead of the master. It was also observed very carefully that the Reception LED (RX) gives signal as packets of data are received at the Master modem. As data is sent from slave to master, the receiver indicator is being blinked on as correct packets of data are received. At this point, the master's LED for RSSI indication has also become active. This scenario has explained the testing of link between RF module and FPGA.

III. Bench Marking of Data Communication Protocol

The post optimization bench marking of data communication protocol has been done considering MHX-2400 frequency-hopping 2.4 GHz spread-spectrum communications module so that it can be finalized as optimal candidate as TCI module upon qualifying the test.

The proposed scenario for bench marking is described in Fig. 2.

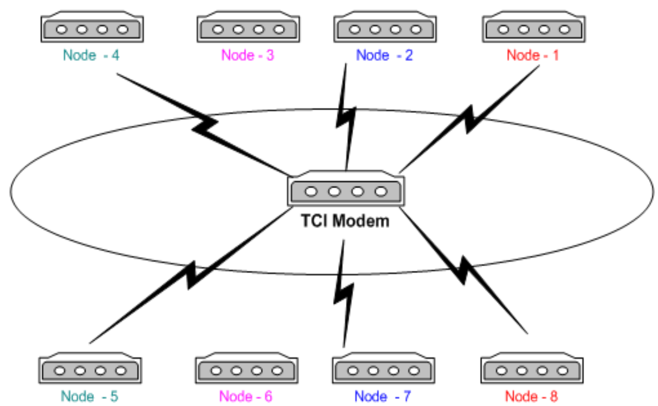

Fig. 2. Scenario used for Bench Marking of Data Communication Protocol.

- In the proposed configuration of TDMA, the Master transmits Data in Broadcast manner i.e. Master can send data to all Nodes at the same time.
- The Master allows data reception with only one Node at a time.
- In the proposed configuration, the Master takes initiative to communicate with the "Node-1" for the predefined hop interval. (Here 12 ms).
- After 12 mS, the Master increments the unit address of the Node and now it communicates with the "Node-2" for next 12 ms.
- Similarly the Master may communicate with "Node-3" for next 12 ms.
- This whole scenario of operation maintains until total number of Node modules is reached, i.e. the Max Address for TDMA.

After communicating the last Node Module in the Network, the "Master" Module will go to "Node-1" again for next TDMA cycle. The Master – Node communication timing diagram is expressed as Fig. 3.

The bench marking process executed to check post optimization functionality of communication link considering parameters like Packet Miss Percentage (PMP), Downlink Packet Miss Rate, Downlink Packet Failure Rate and other relevant parameters [6, 7]. The results of bench marking are shown in next section in graphical format.

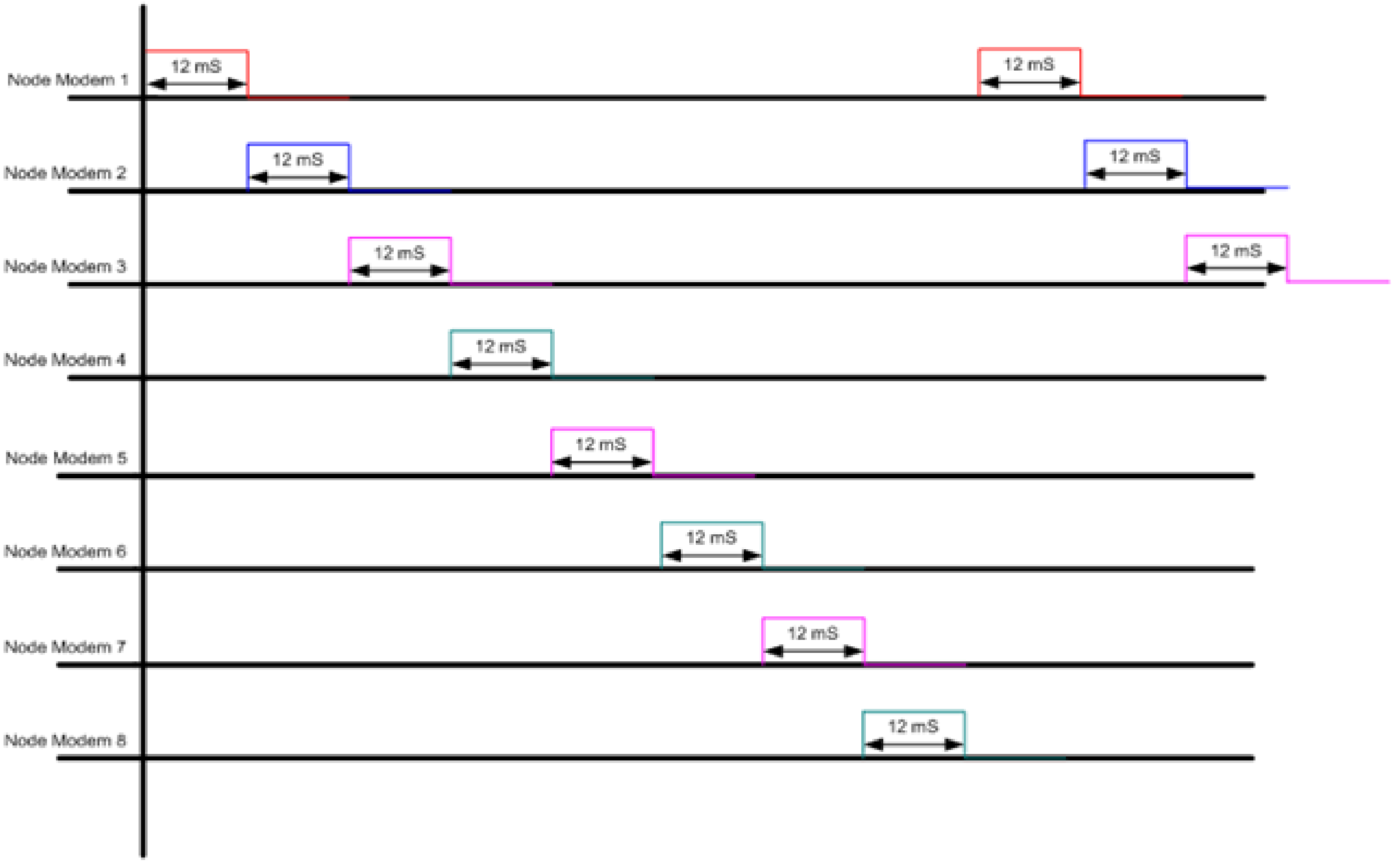

Fig. 3. The Master – Node Communication Timing Diagram.

IV. Results and Discussions

Reference to previous, the proposed scenario for bench marking is described in Fig. 2., which depicts one TCI module (which is MHX-2400 in this case), communicating with 08 nodes. The details about this TDMA operation with sequence had already explained in section 2.

Initially, the "Master" communicated with the "Node-1" for the predefined hop interval of 8 ms for which optimal packet size in 14 bytes which is less than 40 bytes size of our intended packet containing 32 bytes for analog inputs, 2 bytes for 16 digital inputs, 1 byte for digital outputs, 2 bytes for SPI communication and 3 spare bytes. As optimal packet size for 8 ms time slot is only 14 bytes so it is short to accommodate 40 bytes. Thus it has resulted in erroneous situation which is described in Table I and Fig. 4 showing that the downlink Packet Miss Percentage (during the communication) is between 1% and 2.5 % of expected packets. We are showing the state of Data in erroneous situation in Table I, and it is plotted in Fig. 4. This erroneous situation for data transfer can be optimized by increasing hop interval to 12 ms.

TABLE I
BENCH MARKING RESULTS FOR PERCENTAGE PACKET MISS AND PACKET ERROR (ERRONEOUS SITUATION)

Number of nodes	Downlink Packet Miss %	Downlink Packet Error %
1	2.03	0
2	2.21	1.63
4	2.19	0.47
6	2.01	0
7	1.3	0

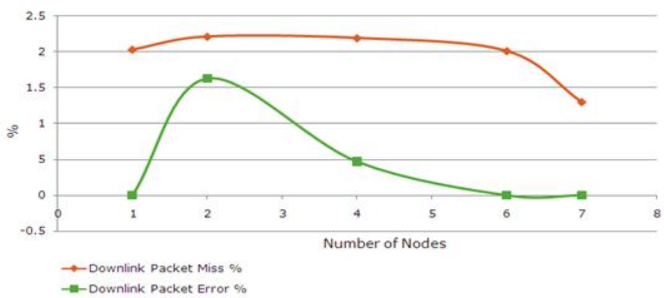

Fig. 4. Bench Marking Graphical Results – Erroneous Situation. (Packet Miss and Packet Error)

The bench marking procedure is further continued to find the best possible performance and maximum packet size at different modes of operation. The experimental setup is based on conditions including a baud rate of 115k with support of maximum packet size of 255 bytes but no retries and no retransmissions.

In actual scenario, the Master transmits Data in Broadcast manner using TDMA mode i.e. Master can send data to all Nodes at the same time. The Master manages data reception with only one Node at a given time. In the proposed configuration, the Master first communicates with Node-1 for the hop interval equivalent to 12 ms for which optimal packet size in 14 bytes which is greater than 40 bytes size of our intended packet. After 12 ms, the "Master" will then increment the unit address of the Node and now it will communicate with the "Node-2" for next 12 ms. Similarly the "Master" will go to communicate with "Node-3" for next 12 ms. This pattern continues until the TDMA Max Address i.e. the total number of Node modules is reached. The results are shown in Table II and Fig.5.

Table II
BENCH MARKING RESULTS FOR DOWNLINK REFRESH RATE (EXPECTED AND ACTUAL)

Number of nodes	Downlink Refresh Rate P/sec	Downlink Expected Refresh Rate P/sec	Downlink Packet Failure Rate P/sec
1	4.89	5	0
2	9.77	10	0.16
4	19.56	20	0.09
6	29.39	30	0
7	34.55	35	0

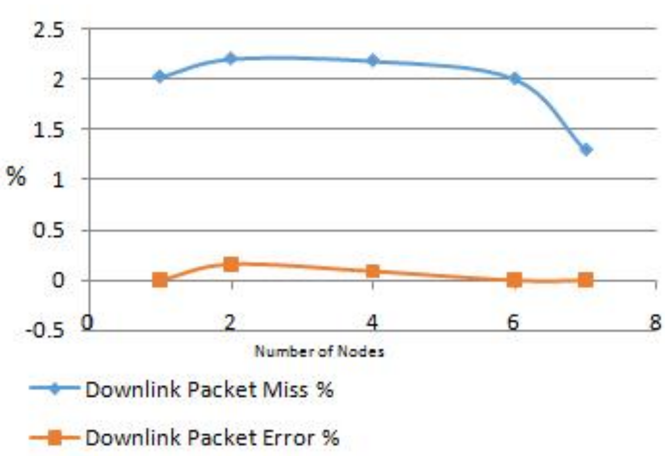

Fig. 5. Bench Marking Graphical Results – Optimized. (Packet Miss and Packet Error)

From Table II and Fig.5, it is revealed that most of the time, packet error percentage (PCER+PLER) is less than 0.5% which shows high performance of selected TCI module and the downlink refresh rate is very close to the expected refresh rate which also endorsed the selection of MHX-2400. Each experiment has been repeated 5 to 10 times to ensure the authenticity of results. However, MHX-2400 module can support 25 nodes for a refresh rate of 5 Hertz (200 ms) for 8 ms which has been decreased to 16 nodes while bench marking had applied by selecting 12 ms hop interval and optimal packet size equivalent to 66 bytes.

V. Conclusion

The data transmitted from RTU is being received through Telecontrol interface for data integrity and graphical representation for which further benchmarking is done for data communication protocol. From bench marking experiment, it was also revealed that most of the time, packet error percentage (PCER+PLER) is less than 0.5% which shows high performance of selected MHX-2400. With available interfaces for telemetry using MHX-2400, the developed RTU has also become a valuable candidate to be incorporated in Wireless based SCADA system.

References

[1] Muhammad Aamir, Javier Poncela, Muhammad Aslam Uqaili, B. S. Chowdhry, and Nishat Ahmad Khan. 2013. Optimal Design of Remote Terminal Unit (RTU) for Wireless SCADA System for Energy Management. Wirel. Pers. Commun. 69, 3 (April 2013), 999-1012. DOI=10.1007/s11277-013-1060-9 http://dx.doi.org/10.1007/s11277-013-1060-9

[2] Gujare, Santosh; Jagtap, Gaurav; Gharpure, Damayanti; Ananthakrishnan, S., "FPGA based data acquisition and analysis system," Physics and Technology of Sensors (ISPTS), 2012 1st International Symposium on , vol., no., pp.177,180, 7-10 March 2012.

[3] "MHX-2400 2.4 GHz Spread Spectrum OEM Transceiver", Operating Manual, Revision 1.56, April 7, 2006, Microhard Systems Inc.

[4] Muralikrishna, B.; Madhumati, G.L.; Khan, Habibulla; Deepika, K.Gnana, "Reconfigurable System-on-Chip design using FPGA," Devices, Circuits and Systems (ICDCS), 2014 2nd International Conference on, vol., no., pp.1,6, 6-8 March 2014.

[5] K. Doerksen, J. F. Levesque, I. Mas, "Design, Modeling and Evaluation of a 2.4GHz FHSS Communications System for NarcisSat," Proceedings of 17th Annual AIAA/USU Conference on Small Satellites, SSC03-VII-3, Aug. 2003.

[6] IEEE Recommended Practice for Data Communications Between Remote Terminal Units and Intelligent Electronic Devices in a Substation, IEEE Std 1379- 2000 (Revision of IEEE Std 1379-1997), 21 September 2000.

[7] Mauricio G.C Resende and Panos M. Pardalos, Handbook of Optimization in Telecommunication, Springer Science Plus Business Media, Inc., 2006