ISSN 2278-7763

Handshaking Problem Associated with Addressing Scheme for the Nodes of a Wireless Sensor Network

Monjur Ahmed

Department of CIS
Daffodil Institute of Information Technology, Dhaka, Bangladesh.
a.monjur@gmail.com

Abstract

This paper discusses a practical problem that arises when assigning ID to wireless sensor network (WSN) nodes. A WSN is consisted of a number of wireless nodes that collects information from environment by means of different sensors. A gateway server computer acts as a bridge between the WSN and the outside world. The gateway server can essentially have the capability to control any specific node. In any given context, it might be necessary to access any specific node from the gateway server. One of the ways to accomplish this is handshaking. In this paper, a problem with accessing any WSN node is discussed with a possible solution. A critical analysis of the approach is also carried out in conjunction with the suitability of different ways to adopt an addressing scheme for wireless sensor network nodes.

Keywords — wireless sensor network, handshake, networking, communication, access control, wireless node, addressing scheme.

I. INTRODUCTION

A wireless sensor network is a special kind of network of wireless nodes. It occupies a large number of wireless nodes equipped with sensors, embedded processors and radios [1], [2]. All the nodes work in a collaborative manner towards the accomplishment of a common task which is generally tracking or monitoring [3]. The nodes in a wireless sensor network are normally deployed on an ad-hoc basis with proper and careful planning [1] – [3]. The nodes must recognise themselves in a collaborative environment of the wireless sensor network for efficient and seamless performance and routing of information [4], [9], [13]. The wireless sensor network is interfaced with the outside world by a gateway server or controlling server. At times, it might be necessary to access information sensed by any specific node for which a communication algorithm must be in place [1] – [3], [6], [9], [11]. One way to access any specific node is by means of handshaking [14]. Without proper and efficient access method, the gateway server might fail to access the desired node of interest and thus the total purpose of the wireless sensor network might appear as a failure [6] – [8], [11], [15].

II. BASIC WSN ARCHITECTURE

In a wireless sensor network, all the nodes communicate with each other by means of wireless. Any given node collects information from environment by means of a sensor and forwards it to another node which in turn forwards the information to another node so that the information can reach at the gateway node. It is the gateway node which interfaces between the nodes and the server where all the collected information from all the nodes are stored and further processed [1] – [3]. Thus the nodes in a wireless sensor network work in a co-operative manner to carry out their own tasks as well as routing [1], [3] – [5], [9], [10], [15]. The gateway node is the interface to the server for the total WSN and vice versa. The server acts as the bridge between the WSN and the outside world. The server can essentially have the communication capability with all or any of the nodes in an automatic or on-demand fashion [11], [16].

A typical architecture of any wireless sensor network looks like the following:

ISSN 2278-7763

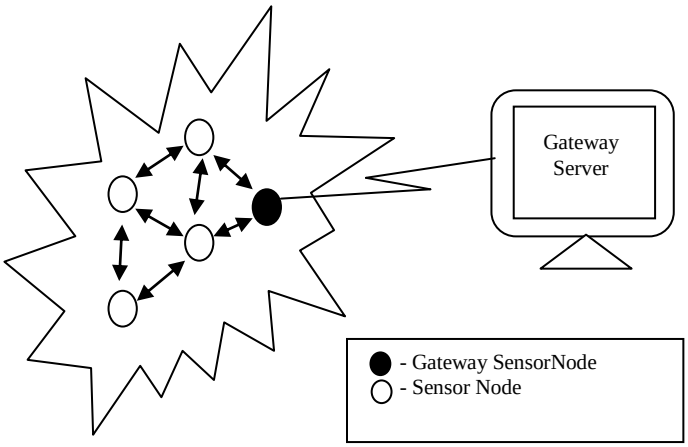

Figure 1: Wireless Sensor Network architecture

III. HANDSHAKING

A wireless sensor network can be configured in such a way so that the gateway server can control and access any specific wireless node. Like any network, the wireless nodes need to have unique ID for efficient and proper communication. When the ID of a node is broadcast, the respective node needs to have the capability to recognize the transmission as destined to it, either for passing information or for establishing communication for follow-up transmission of data [6], [9], [14]. As the node ID is a broadcast, all the nodes within the range will essentially 'hear' the broadcast ID. At the same time, the other nodes must be able to recognise the broadcast ID as not destined to them so that they can ignore the request. In this way, a handshaking will take place between the gateway server and the node of interest, before any communication takes place.

IV. THE DEVELOPED WSN

Three wireless sensor nodes were developed along with the gateway sensor node. All three nodes were able to connect wirelessly to the gateway sensor node. The nodes were assigned the IDs A, B and C respectively. The gateway sensor node was connected to the gateway server using the serial RS-232 port. The following figure depicts the developed WSN:

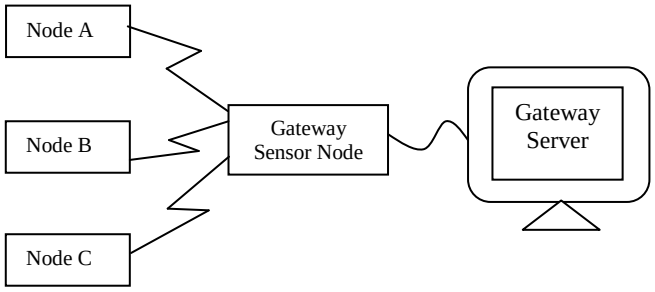

Figure 2: Developed WSN

Table I lists the major components used to develop the sensor network:

TABLE I
COMPONENTS FOR DEVELOPED WSN

Category	Tools/Models
Wireless Module	ER400TRS
Microcontroller	PIC16F876
Compiler	PIC C
Language	CCS C
IDE	MPLAB
Debugger	ICD-2

The wireless nodes were accessed from the gateway server by means of HyperTerminal from windows operating systems. The connection between the gateway server and the gateway sensor node was through RS-232 serial port. The parameters to configure the HyperTerminal were determined carefully as without proper synchronization, communication between the gateway server and the wireless nodes would simply be impossible even after having a full functioning sensor network.

The configuration parameter for the HyperTerminal is depicted in table II below:

ISSN 2278-7763

TABLE II
SETTINGS FOR HYPERTERMINAL PARAMETERS

Parameter	Value
Bit per second	19200
Data bits	8
Parity	None
Stop bits	1
Flow control	None

The developed wireless sensor network was configured in such a way that any wireless node would transmit sensed data when they were requested. The nodes were sensing data by means of sensors and when the ID of any node is broadcast from the gateway server, the respective node was transmitting its then sensed value. For example, upon transmitting the value 'A', the node A was transmitting its sensed value. The sent data from the wireless nodes would then be saved in the gateway server for further processing.

V. THE HANDSHAKING PROBLEM

It was observed that the assigning of the node ID was very crucial when developing any wireless sensor node. It was also observed that situation might arise where the broadcast ID could be erroneously interpreted by other nodes than the one of interest, resulting in more than one node to be communicating with the gateway server. It would simply lead the wireless sensor network to malfunction and the wireless sensor network would become a failure in terms of its collective goal.

The firmware for the nodes was developed in such a way that upon the first request from the gateway server, the respective node would announce its own identity and some introductory information along with its sensed value. For any subsequent request from the server, the node would simply transmit the value with its identity. For example, when node A is requested to transmit its sensed value for the first time, the resulted screen on the HyperTerminal is shown in figure 3 below.

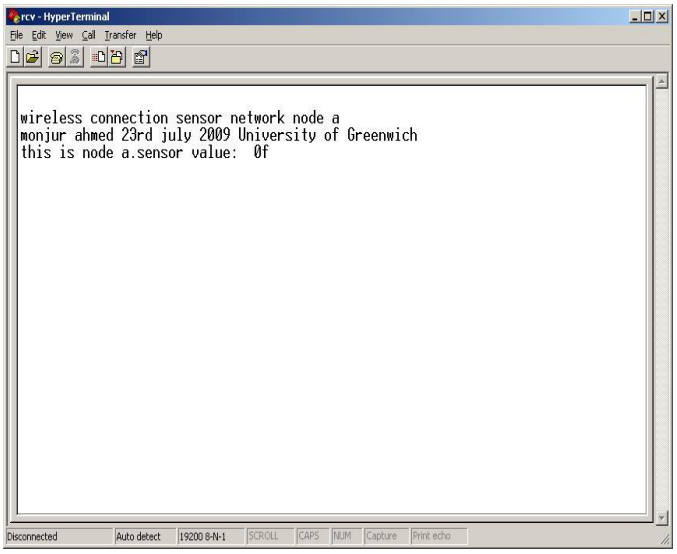

Figure 3: Initial transmission from node A

On subsequent requests, the node A would transmit just the sensed value with its identity. This is shown in figure 4 below.

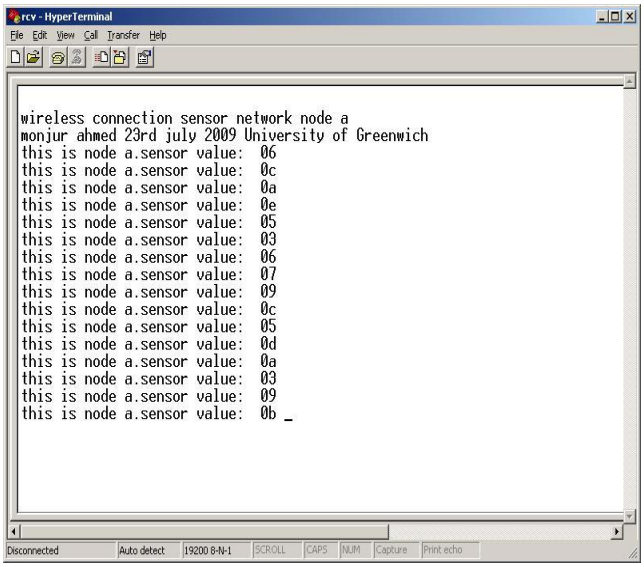

Figure 4: Subsequent transmission from node A

At the time of initial testing, a problem was observed with the handshaking between the gateway server and the wireless nodes. The nodes were given ID as capital A, capital B and capital C so that they can be distinguished from their lowercase counterpart. The initial transmission of

any node was simple sentences made up of words, and one of the words was containing the letter capital 'A' (the family name of the author). As a result, whenever any node other than node A was requested transmission by the server, node A was transmitting at the same time which was simply not desired. It was because of the broadcast nature of the wireless technology. Any message thrown out the wireless interface either from the gateway sensor node or any other node could essentially be 'heard' by all of the nodes. So whenever the initial transmission occurred from any node, node A interpreted it as a request for itself as the initial transmission from any node contained the letter 'A'. The consequence was transmission from node A regardless of whether it had been requested to send data or not.

The solution to this problem was to ensure that the node ID remains unique within the extent of transmission. So it was ensured that no capital A or B or C was transmitted during the transmission as they were the ID for the three nodes respectively. Though this approach looks pretty simple and straightforward, in a complex network the addressing scheme chosen on this soft approach raises a question of credibility. In a complex network, it might not be possible to avoid the problem discussed earlier by adopting the addressing scheme used for the developed sensor network. Any sophisticated addressing scheme that is done in the soft way, might minimize the mentioned problem being occurred but cannot eliminate the possibility of arising the above handshaking problem. In wireless sensor networks, power efficiency is a critical factor and minimizing transmission without compromising the total amount of data needs to be transferred is always of supreme interest [4] – [6], [10], [12], [13], [15]. This is due to limited power capability of the wireless nodes which are normally powered by batteries as they cannot always be solar powered blindly due to the constraints in various environments where the sensor nodes are deployed [3], [16]. To address the handshaking problem, a sophisticated soft approach might reduce the chance of the stated problem being occurred; but it also reduced the energy efficiency due to transmission overheads and processing required for each wireless sensor node [17]. On the other hand, using a hard approach for any addressing scheme for a wireless sensor network would eliminate the problem in terms of error free and unambiguous transmission while reducing data transmission and processing overheads by subsequently keeping the network energy efficient. A number of addressing scheme for wireless sensor networks has been proposed based on MAC address. For wireless sensor networks, hardware based addressing scheme ensures unique and unambiguous identity for the wireless nodes, but it cannot guarantee the elimination of processing and transmission overheads which depends on the efficient design of the addressing scheme [8] – [11].

VI. CONCLUSION

The addressing scheme for the nodes of any wireless sensor network is very crucial for the successful operation of the network. The addressing scheme can be applied in two ways – software based and hardware based. The study indicated that software based addressing scheme might lead a wireless sensor network to malfunction. While the problem can hardly be minimized in software based addressing scheme, it makes the sensor network energy-inefficient. On the other hand, the hardware based approach for addressing scheme can ensure the avoidance of the problem discussed in this paper though transmission and processing overheads still remain as a problem which depends on the efficient design of the addressing scheme.

ACKNOWLEDGMENT

The author is thankful to his project supervisor Dr R C Seals, who helped the author to understand the critical aspects of a wireless sensor network. The contribution of Mr. Irfan Cesur Dilek and Mr. Asha Jagdis is also appreciated.

REFERENCES

[1] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, *Wireless Sensor Network Survey*, Computer Networks, 52 (2008)

[2] I. F. Akyldiz, W. Su, Y. Sankarasubramanian, E. Cayirci, *Wireless Sensor Networks: A Survey*, Computer Netwroks, 38 (2002)

[3] Deepak Ganesan, Alberto Cerpa, Wei Ye, YanYu, Jerry Zhao, and Deborah Estrin, *Networking Issues in Wireless Sensor Networks*, Journal of parallel and distributed computing; 64(2004)

[4] Parick Vincent, Murali Tummala, John McEachen, *A New Method for Distributing Power Usage Across a Sensor Network*, Ad Hoc Networks, 6 (2008)

[5] Kan Baoqiang, Cai Li, Zhu Hongsong & Xu Yongjun, *Accurate Energy Model for WSN Node and Its Optimal Design;* Journal of Systems Engineering and Electronics, 19(2008)

[6] Zheng Yao, Falko Dressler, *Dynamic Address Allocation for Management and Control in Wireless Sensor Networks*, 40th Hawaii International Conference on System Sciences (2007)

[7] D. Syam Sundar, Ch. G. V. N. Prasad, O. Srinivasa Rao, *An Addresing Scheme for a Network of Wireless Sensors and Mobile Clients for Cluster-9*, Georgian Electronic Scientific Journal: Computer Science and Telecommunications, 16 (2008)

[8] Jung Hun Kang, Myong-Soon Park, *Structure-based ID Assignment for Sensor Networks*, International Journal of Computer Science and Network Security, 6 (2006)

[9] Soojung Hur, Jaehyen Kim, Jeonghee Vhoi, Yongwan Park, *An Efficient Addressing Scheme and Its Routing Algorithm for a Large-Scale Wireless Sensor Network*, EURASIP Journal on Wireless Communications and Networking, 2008

[10] Joseph Polastre, Jason Hill, David Culler, *Versatile Low Power Media Access for Wireless Sensor Networks*, SenSys, 2004

[11] Wei Ye, John Heidemann, *Medium Access Control in Wireless Sensor Networks*, USC/ISI Technical Report ISI-TR-580, 2003

[12] Luiz H.A. Correia, Daniel F. Macedo, Aldri L. dos Santos, Antonio A.F. Loureiro, Jose´ Marcos S. Nogueira, *Transmission Power Control Techniques for Wireless Sensor Networks;* Computer Networks; 51 (2007)

[13] KAN Baoqiang, CAI Li , XU Yongjun, *Reliable and Energy Efficient Protocol for Wireless Sensor Network*, Tsinghua Science and Technology, 12 (2007)

[14] Peng Xie, Jun-Hong Cui, *Exploring Random Accessand Handshaking Techniques in Large-Scale Underwater Wireless Acoustic Sensor Networks*, Computer Science and Engineering Department, University of Connecticut, USA

[15] Jian ZHU, Hai ZHAO, Jiuqiang XU, *An Energy Balanced Routing Metric in WSNs;* Wireless Sensor Networks; 1 (2009)

[16] Muneeb Ali, Zartash Afzal Uzmi, *An Energy-Efficient Node Address Naming Scheme for Wireless Sensor Networks*, IEEE, 2004

[17] Jonathan W. Hui, David E. Culler, *IP is Dead, Long Live IP for Wireless Sensor Networks*, SenSys, 2008

