A Suitable MAC Protocol for Transmit-Only Sensor Nodes in a Housing Community Wireless Network

John Maloco and Séamus McLoone

Department of Electronic Engineering, National University of Ireland Maynooth
Maynooth, Co. Kildare, IRELAND
E-mail: john.maloco; seamus.mcloone @ eeng.nuim.ie

Abstract

This paper investigates the development of a suitable Medium Access Control (MAC) protocol for a housing community wireless network that consists of both wireless infrastructural mesh nodes and wireless sensor nodes. In this network, transmit-only sensor nodes are employed in order to obtain a low cost, easy to deploy and low power solution. However, such sensor nodes have no way of verifying successful data transfer and it is, therefore, imperative that the associated MAC protocol provides a high level of confidence for transferring this data. In this paper, we examine methods of packaging and transmitting sensor node data in order to obtain such a MAC protocol for the aforementioned housing community wireless network. Microchip's rfPIC is used as the platform for the sensor node. Some preliminary analysis and results are presented within.

Keywords: Mesh Sensor Networks, Medium Access Control (MAC), Collision Avoidance.

1   Introduction

The area of wireless devices and wireless networking has seen a rapid growth in recent years. This is also very evident in the domestic environment. Automating the living space through wireless control and sensors is on the threshold of becoming commonplace in many homes. Systems such as Zigbee [1], Bluetooth [2] and Z-Wave [3] are being deployed to meet the requirements of wireless home automation.

Recently, wireless applications such as remote meter reading and radio frequency identification (RFID) tags [4] for refuse bins have found their way out of the house and into the wider community. Our research looks at extending the use of wireless devices, in particular sensor networks, to outside the home and into the housing community of a typical housing estate. The system should be both affordable and beneficial to a housing community and to service providers of the estate [5].

Much research is being carried out in the area of sensor networks. These networks are a collection of intelligent nodes equipped with sensors and radios. The nodes work together to accomplish tasks such as asset tracking and environmental monitoring. In Europe, most sensor networks operate at 433Mhz or 2.4Ghz in the licence exempt Industry, Science and Medical (ISM) radio band, or in the pan-European licence-free band at 868Mhz. The main requirements of sensor networks are low power, ease of deployment and reliable data transfer. Sensor networks are often deployed in a mesh configuration. Mesh networks are ones in which nodes transmit data to adjacent nodes [6]. These nodes then forward the data on to its destination, either directly (single-hop) or, via additional routing nodes (multi-hop). In order to

meet all the requirements of a sensor network one of the main challenges is to design a suitable Medium Access Control (MAC) protocol [7].

In typical mesh sensor networks the mesh node incorporates a hardwired sensor. In our system the sensor is connected to a mesh node through a single channel unidirectional wireless link, thus providing greater flexibility in sensor deployment. With this configuration, multiple transmit-only sensor nodes must share a single transmission channel. It is impossible for the nodes to establish whether data has been transferred successfully or not, due to such factors as data corruption or collision. There is also no way of synchronising the nodes for scheduled transmissions such as Time Division Multiplexing (TDM). In TDM each node would be required to receive a synchronisation marker. The best that can be done for transmit-only sensor nodes, is to maximise the probability of a transmission being successful. It is this probabilistic transmit-only link from the sensor to the mesh node, governed by a suitable MAC protocol, which forms the main focus for this paper.

The rest of this paper is structured as follows. In next section an overview of the proposed housing community wireless network is presented. In order to fully understand the operation of the proposed MAC protocol it is necessary to understand the operation and design of the sensor node. Hence the sensor node design is outlined in section 3. A description of the proposed suitable MAC protocol is given in section 4 while section 5 provides an analysis of data collision between the sensor and mesh nodes. Finally, the paper ends with conclusions and some suggestions for future work.

2   System Overview

The proposed housing community network comprises both wireless infrastructural mesh nodes and wireless sensor nodes. Figure 1 depicts the topology of these devices together with a base station.
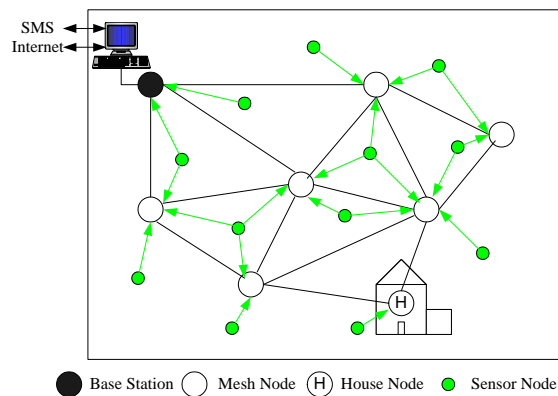

Figure 1 - Housing Community Wireless Network Topology

Mesh nodes are strategically placed to give full zoned coverage of the target area (i.e. the housing estate). They act as wireless routers in the system relaying sensor node data to the base station, where the data is then processed. The mesh node contains two radio interfaces. One is used for inter-mesh communications using the 868Mhz band while the other is a dedicated receiver for the sensor node operating at 433Mhz.

The sensor node is a battery powered single channel wireless device. The main function of this device is to read sensor inputs and transmit the data to any/all mesh nodes within radio range. This device contains a

433Mhz transmit-only radio. The number of sensor nodes in each mesh node zone will tend to be evenly distributed due to the uniform physical layout of housing estates in general. However, some of the sensor nodes within the network will be mobile. These nodes will be free to move between mesh zones and are intended to be used for radiolocation purposes. Additional mesh nodes may be added or removed on an ad-hoc basis. These additional nodes can be used to assist in more accurate radiolocation and for blind-spot coverage.

The proposed system has many possible benefits in a housing estate environment including oil tank monitoring, house alarm notification, locating of assets and people, refuse services, personal aid notification. Further detail on this housing community wireless network can be found in [5].

3   Sensor Node Design

The basic structure of the mesh sensor network was outlined in the previous section. Here, the design of the sensor node is presented in more detail. The main specifications for a wireless sensor node can be summarised as follows:

- Low power (long battery life)
- Transmit small amounts of data
- Reliable data transfer
- Low cost
- Easy to deploy

Research has shown that typical power consumption ratios for a sensor node equipped with a transceiver operating at 433Mhz for *idle listening : receiving : transmission* are typically 1 : 1 : 1.41 [7]. It can be seen from this that the inclusion of a receiver significantly increases power consumption. Hence, this is one of the factors that governed the design of a transmit-only sensor node, resulting in a lower cost solution with less power required.

The proposed operation of the sensor node is to wake from sleep (or switch on), transmit a short burst of data and go back into sleep mode (or switch off). This very basic function fulfils the specifications listed above. Switching on for very short periods of time to transmit and then immediately switching off again will greatly extend battery life. Data transfer is kept to a minimum as no transceiver protocols are needed. Furthermore, a sensor node is deployed by simply switching it on.

The only category above in which this transmit-only device may encounter problems is in relation to the reliable data transfer. A transmit-only sensor node typically adopts a *'transmit and hope'* approach. In other words, it transmits its data but has no way of verifying a successful transmission. Instead, it can only hope that this was indeed the case. Improving the reliability of these transmissions are addressed in detail in section 4 with the development of an appropriate MAC protocol.

The sensor node is designed around Microchips rfPIC12F675F (rfPIC) [8]. This is an ASK/FSK transmitter operating in the ISM band at 433Mhz. The rfPIC has been chosen for several reasons including its small physical size, low power consumption, integrated micro-controller (with A/D capability) and low cost with minimum external components required. It also offers ease of access to free development tools and extensive literature.

The rfPIC is configured to operate in ASK mode. The reason for this is that the transmitter output power amplifier is only switched on when data input to the transmitter is high, thus saving power. The maximum data rate for the rfPIC, using the Manchester encoding (a standard encoding technique used in wireless

communication) is 20Kbps in ASK mode [8]. While this is not particularly fast, this data rate is nevertheless deemed acceptable for our system due to the small amount of data being transferred. The rfPIC transmitter output power can be easily adjusted to one of four levels by a single resistor selection. The maximum output power will allow for a transmission radius of around 100m, giving a transmission zone area of approximately 31,400m^2. This zone area is relatively large. Having the option to vary the output power and, therefore, the effective zone size offers potential benefits in the deployment of the system, particularly where radiolocation is concerned.

There are two configurations for the sensor nodes in the system, namely a mobile and static sensor node.

3.1   Mobile Node

The mobile sensor node, as shown in Figure 2, is effectively an active RFID tag [4] which must transmit an ID periodically. This node also reports low battery and tamper alerts. It is intended to be used as a tracking device. For this reason the node incorporates a movement sensor. This sensor ensures that the node does not transmit unless it has changed position. The embedded software then ensures that there is a minimum 30s interval between transmissions. This event driven transmission scheme greatly aids in extending the battery life of this device.
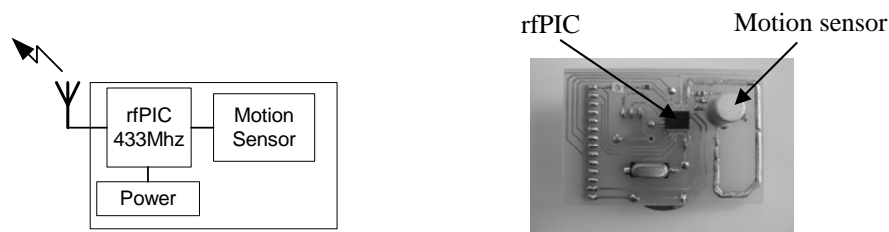

Figure 2 - Mobile Sensor Node

3.2   Static Node

The static sensor node, as shown in Figure 3, replaces the motion sensor in the previous design with an onboard sensor or sensor interface. These static nodes are used to monitor stationary objects such as the oil level in an oil tank, the temperature of a greenhouse or the activation of a house alarm, for example. Transmissions from these devices are initiated in one of two ways, either periodically or event driven. Periodical transmissions are set to occur every 30 minutes. Event driven transmissions only occur after a given event has taken place. This is explained in more detail in the next section.
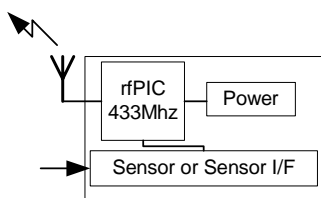

Figure 3 - Static Sensor Node

4   MAC Protocol Between Mesh and Transmit-Only Sensor Nodes

The basic structure of the proposed mesh sensor network and an overview of the transmit-only sensor node design have been outlined in the previous sections. Here, a suitable MAC protocol is proposed to enable sensor nodes to transfer their data successfully to relevant mesh nodes. One of the primary tasks of the MAC protocol is to implement some method to ensure that transmissions from multiple nodes do not interfere with each other, a phenomenon that is known as collision avoidance [9].

Data collision is when two wireless devices transmit at overlapping times on the same channel. With transmit only devices it is impossible to achieve total collision avoidance. Therefore the MAC protocol for this system must be tolerant of collisions, but these collisions must be kept to a low level in order to preserve system performance and to achieve a high level of confidence in successful data transfer.

The following are some areas which have been explored in minimising the effect of data collision for this novel application - data rate; transmission packet length; period between transmissions; and receiver requirement for consecutive packet separation.

The data rate is an obvious factor in avoiding data collision. The faster the data can be sent the less time is required for the transmission, thus reducing the probability of a data collision. As mentioned previously, the maximum data rate for the rfPIC in ASK mode using Manchester encoding is 20Kbps.

The transmission packet length should also be kept to a minimum. The longer the data packet the more time is taken up on the single wireless channel. This then leads to the greater possibility of data collision between two or more packets. The following data packet frame has been designed for our system:

Preamble	ID	CS1	Data	CS2

Figure 4 – Sensor Node Data Packet

The preamble normally consists of ones and zeros. This data is used as padding allowing time for the transmitter to switch on, including time for the transmitter oscillator to build up and for the phase lock loop (PLL) to lock on to the oscillation [8]. In the case of the rfPIC this time has been measured to be approximately 600μs. It is important, both in terms of packet length and power consumption, to keep the preamble as short as possible. The transmitter oscillator will start as soon as the transmitter is enabled. By keeping the data line low for the first 600μs, this guarantees that no carrier is transmitted for this time. Effectively the start up time is removed from the preamble. This therefore allows other nodes to transmit during this start up period. The proposed preamble is shown in Figure 5.
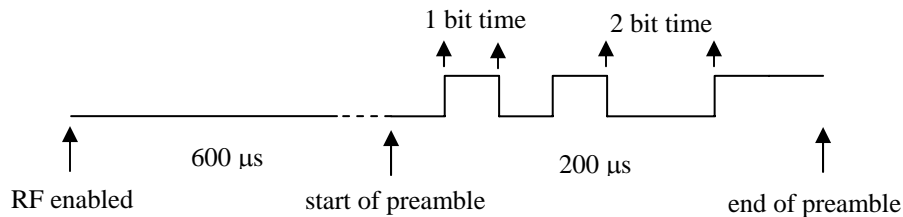

Figure 5 – Sensor Node Transmission Preamble

In this system it is important that the preamble is a unique pattern as it also identifies the start of the data packet. The data pattern in Figure 5 is unique, as this pattern will not appear in the normal Manchester encoding of ones and zeros. The 200μs preamble is equivalent to 8 bits in terms of overall packet size.

The remainder of the data packet shown in Figure 4 comprises the following. The ID is set to 16 bits allowing for over 65,000 unique IDs. CS1 is a 4 bit checksum which verifies the 16 bit ID. This checksum is used to help recover the ID of a partially collided packet. Data is an 8 bit field reserved for sensor node data/status. CS2 is a 4 bit checksum that verifies the entire data packet.

The total number of bits including the preamble is 36 bits. At 20Kbps, this translates into a transmission time for the entire packet of 1.8ms In order to calculate an accurate time for the transmission of data packets from the sensor node, we must also consider the receiver in the mesh node. If a receiver is to accept two consecutive packets there is a certain amount of time required for the receiver to finish receiving/processing one packet before it can receive the next. Preliminary tests have shown this time to be one bit time. This in effect adds 50μs to our 1.8ms packet transmission time. This is relatively a small amount, at just under 3% of the total packet transmission time, giving a maximum total time of 1850μs.

The period between individual sensor node transmissions is a major factor in the performance of the system. Reducing the number of transmissions in any one period is a major contributor to successful data transfer. The following scheme has been adopted. Static sensor nodes transmit at 30 minute intervals if no event has occurred. After each 30 minutes the node transmits 3 data packets in three consecutive 10 second windows. These transmissions occur randomly within each 10 second period, as shown in Figure 6. Event driven transmissions only occur after an event has taken place. Again this data transmission consists of 3 data packets in three consecutive 10 second windows. Mobile sensor nodes adopt the same transmission scheme, treating a movement as an event. Additional movements on the same node will only be processed after the 30s transmission window has elapsed.
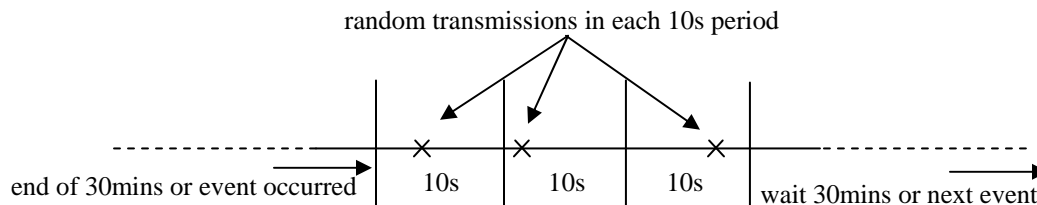

Figure 6 - Sensor Node Transmit Scheme

In general, due to the distributed nature of the system, not all nodes will be competing for the same radio space during any 10s period. This is particularly the case for static nodes. Static nodes have a relatively even distribution over the housing estate. Mobile tags however, can congregate in large numbers in small areas of the estate. For this reason the mobile tags only transmit when they move position.

It should be noted that this transmission interval scheme is application specific. As such, the outlined times between transmissions is deemed acceptable for the proposed system in this paper.

5   Analysis of Data Collision

To analyse the MAC protocol, given in the previous section, with regard to data collision avoidance, we estimate the probability of successful data transfers taking into account the criteria established above. The probability of collision for T nodes transmitting in the same zoned area is given by the equation:

$$P_{\text{collision}} = 1 - P_{\text{success}} = 1 - \left(\frac{S-1}{S}\right)^{T-1} \qquad (1)\ [10]$$

where S is the number of time slots in one transmission window.

This formula shows the basic relationship between node density and data packet collisions. However this formula is more suited to single point events or slotted transmissions where data is sent from the start of a time slot or not at all. The scheme presented in this paper does not fall into either of these categories. In our case, data is transmitted randomly and can collide anywhere during a transmission, as illustrated in Figure 7(a) below. However, the formula above can still be used if we assume the size of the time slot to be twice that of the data packet. This idea is represented in Figure 7(b).
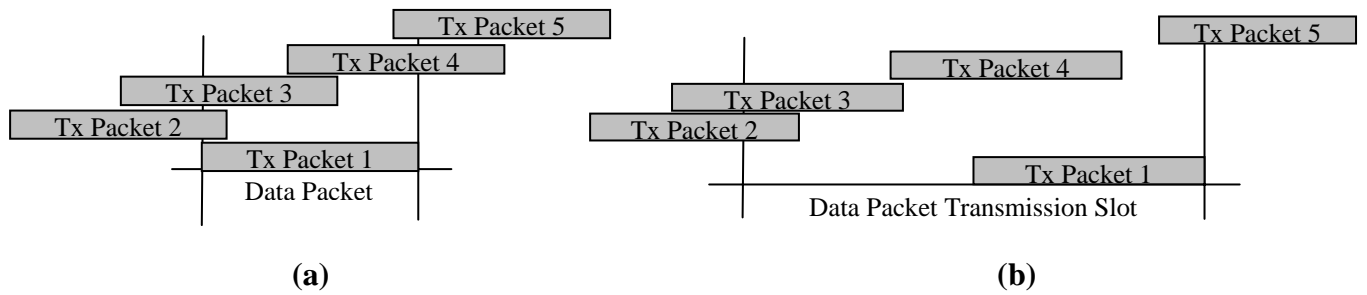

(a)   **(b)**

Figure 7 – Illustrating Possible Collisions

It can now be stated that only packets starting within this allotted time will collide. In this case, it is now possible to calculate the probability of data collision for the system as follows. Given 200 transmitting nodes in one zoned area (for example), then:

Packet duration = 1850µs

S = Number of Slots in 10s period = 10,000,000 / (1850 x 2) = 2,702

Hence, $P_{\text{collision}} = 1 - \left(\dfrac{2701}{2702}\right)^{199} = 0.07$ or $P_{\text{success}} = 0.93$.

Figure 8 shows the correlation between the probability of successful transmissions and node density in any zoned area.
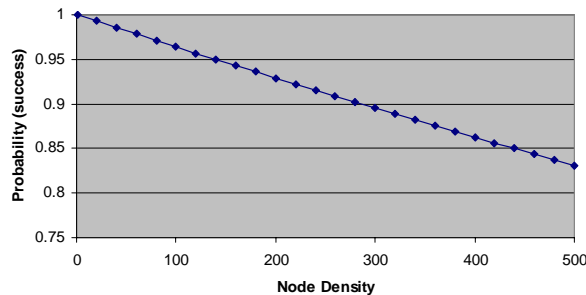

Figure 8 - Correlation between Probability of Successful transmissions and Node Density

This figure shows that a data packet sent by a sensor node is likely to avoid data collision. However, it should be noted that this analysis allows for the worst case scenario. The system, in practice, should perform much better than this analysis suggests. The correlation between the probability of successful data transfer and node density above assumes that every sensor node is attempting to transmit data during a single 10s window. This is not the case as explained previously. It is more likely that only a small percentage of the nodes will ever be competing for any one 10s transmission window. This low contention rate greatly increase the probability of success. Furthermore, the probability is increased by repeating each transmission three times in three consecutive 10s periods. Also, as sensor nodes will transmit to all mesh nodes in range, there can be multiple paths for the sensor node to transfer its data. Therefore a transmission colliding at one mesh node may be received successfully by another mesh node within range.

Yet another factor, which was briefly mention earlier, that further improves the probability of a successful transmission is the possibility for data recovery from partially corrupted packets. If any of the last 12 bits of the data packet are corrupted then the data from the preamble to, and including, the first checksum (CS1) can still be used to acquire the ID of the transmitted packet. Taking this into account, the data packet *Tx Packet 1* in Figure 7 would survive a collision with *Tx Packet 5,* thus providing some useful data.

Hence, these results confirm that the MAC protocol outlined in section 4 would result in a highly probable successful transmission of data from the transmit-only sensor nodes to the mesh nodes.

6   Conclusions and Future Work

In this paper, we designed a MAC protocol that facilitates the use of transmit-only sensor nodes in a proposed housing community mesh sensor network. Analysis of data collision avoidance using the MAC protocol revealed that, for the application in question, the probability for data collision between sensor and mesh nodes is very low.

The main focus of future work will be the ongoing research into developing and implementing the housing community wireless network described in this paper. Immediate focus will involve further modelling and testing of the MAC protocol between the sensor and mesh nodes.

References

[1]   Cross, P. (2005). Zeroing in on Zigbee (part 2), *Circuit Cellar Digital Library*, Issue 176.
[2]   http://www.bluetooth.com. Last accessed May 2007.
[3]   http://www.z-wavealliance.org. Last accessed May 2007.
[4]   http://www.rfid.ie. Last accessed May 2007.
[5]   Maloco, J., McLoone, S., Delaney, D.T. (2006). Using Rugby MSF Broadcast for Time Division Multiplexing Synchronisation in a Housing Community Sensor Network. *ISSC Proceeding,DIT, Dublin.*
[6]   Culter, T. (2005). Implementing Zigbee wireless mesh networking, *Industrial Automation*, http://www.rfdesign.com.
[7]   Ye, W. and Heidemann, J. (2003). Medium Access Control in Wireless Sensor Networks. *USC/ISI Technical Report ISI-TR-580.*
[8]   Microchip Corporation, rfPIC12Fxx datasheet. http://www.microchip.com.
[9]   Stathopoulos, T., Kapur, R., Estrin, D., Heidemann, J., Zhang, L. (2004) Application-Based Collision Avoidance in Wireless Sensor Networks. *Proceedings of the 29th IEEE International Conference on Local Computer Networks* (LCN'04).
[10]   Cerpa, A. and Estrin, D. (2002). ASCENT: Adaptive Self-Configuring sEnsor Networks Topologies. *INFOCOM, IEEE Vol. 2.* Issue 2002: 1278-1287.
[11]   Zhen, B., Kobayashi, M., Shimizu, M. (2005). The Reading of Transmission-Only Active RFID Tags. *International Journal of Computers and Applications*. Vol. 27 No. 1.