

A Priority Based Routing Protocol for Wireless Sensor Networks

Christian Andrä, Kae Hsiang Kwong, Craig Michie and Ivan Andonovic
Department of Electronic and Electrical Engineering, University of Strathclyde,
204 George Street, G1 1XW Glasgow, United Kingdom
email: { christian.andrae, kwong, c.michie, i.andonovic } @eee.strath.ac.uk

Abstract—Recently, the demands on wireless sensor networks have switched from low traffic rate and static topology to more challenging requirements in order to meet the rapid expansion of WSN into various domain applications. This paper proposes a seamless cross layer solution that integrates network layer and medium access control to accommodate some of the new challenges. This new solution allows routing paths being generated dynamically to meet the requirement of potential mobile nodes. Higher data throughput and flow control are part of the new demands required to be addressed urgently. The proposed solution integrates a priority based MAC to handle congestion and packet loss problems which commonly happened in WSN when an occurrence of event spread into wide area.

I. INTRODUCTION

A Wireless sensor network (WSN) is a network system that is formed autonomously by a group of sensor nodes which are commonly fabricated by using low cost/specification hardware. The development of wireless sensor networks has evolved from its original initiative and found its way into broader applications. Some of the new applications pose higher demands than conventional WSNs and exceed its original design spaces. For instance, in [1] the design principle has moved from the conventional low data volume to information-rich data applications in which data volume is dramatically distinguished from conventional WSNs. In [2], the WSN technology has been applied into farming industry, where individual animals are mounted with a sensor node that is fabricated into a collar. The location of the sensor node is mobile and it will change whenever the animal moves. Therefore, this new application has broken one of the common assumptions of WSN, where the location of sensor nodes is said to be static.

Cross layer implementation is a common way of efficient protocol implementation, where different layers of the protocol stack exchange information. In the case under consideration, network layer and medium access layer (MAC) are implemented in such a way. MAC and routing layer exchanging information about the nodes status and the message type that is going to be send. This way of implementation looses the strict way of the layered structure of the OSI definition. It makes it easier for the applications to gather information directly from the physical layer (PHY), [3]. As a result, a light-weight protocol referred to as PriBaR is developed. In order to allow this protocol to run and survive in challenging environment

during the development process a few principles are followed rigorously:

- i Small in size. The code size has to be in the region of a few, less than 100 kBytes. That was achieved, the total size of the transfered code image of the proposed protocol was 43.6 kBytes.
- ii Low memory usage. The hardware restriction of the MI-CAZ nodes just allow 512K byte of data, [4]. Therefore, a routing table that records all neighbouring nodes might not be advisable.
- iii Low power consumption. Hand-shaking, neighbour discovery, network congestion and packet retransmission all cost power. All these should be kept to minimum.
- iv Autonomous and independent operation. Data transmission tasks (i.e. packet relay, link establishment, routing) should run independently and should not impact the sensor actuation. Each sensor node should be able to operate autonomously as well as part of a WSN. Protocols should not be over-complex and require frequent hand-shaking to establish new links.

The paper is structured as follows. Section II gives an overview of related work. In section III, the PriBaR cross layer protocol is introduced and the experimental setup is described. Following this, section V presents the results of this work. Finally, section VI summarizes the findings of this paper and gives an outlook to future work.

II. RELATED WORK

A depth survey in [5] has outlined that WSNs can effectively conduct some of the networking tasks that require co-operative action from neighbouring nodes (i.e. resource sharing and autonomously networking). WSNs are still lacking capability to perform an integrate network management such as network resource allocation and data loss recovery in which will adapt to current network condition. For example, in [6], [7], [8] novels resource management and channel access schemes have been studied. Whereas, issues related to congestion avoidance and packet loss recovery have been discussed in [9], [10]. Generally, researchers look into these problems in isolation. With a single layer of routing and networking scheme it might not work well when the environment changes. A WSN is deployed commonly in challenging and complex environments. Such environments might be unmanned, impossible to retrieve for manual reconfiguration or simply hazardous.

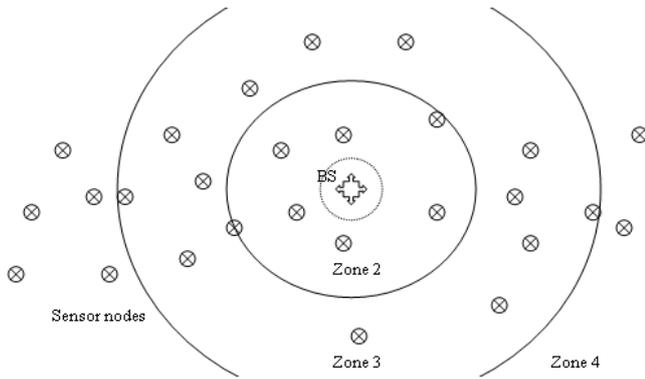


Figure 1. A typical network topology configuration by PriBaR protocol

To the best knowledge of the authors there was no such work, combining the prioritised medium access with a autonomous zone set up. The used AIMRP routing protocol has been studied extensively in [11]. The P-MAC medium access was implemented before at Strathclyde University. The expertise following from this can be used to implement the combination of these both protocols. The expected advantages of a lightweight implementation and prioritised medium access will be explained in more detail in the following section III.

III. PRIORITY BASED ROUTING PROTOCOL, PRIBaR

The proposed PriBaR protocol is the first step to developing a fully integrated protocol that equips WSN with traffic engineering module that allows it to perform dynamic routing and network congestion management. This PriBaR protocol is comprised with two parts:

- i. the dynamic routing module and
- ii. the congestion management module

A unique network topological structure, which dissects the sensor nodes into a number of zones according to their position is required by the PriBaR protocol. The zones are extended, starting from the base station outwards to the farther remote sensor nodes. These zones are organised and identified by using the (hop-)distance between sensor node and base station. This information is recorded by each individual sensor node in a unique field - TIER ID. The base station is set to zone 1. If the sensor node is one hop away from the base station it is said that this particular sensor node is located in zone 2 and for all the sensor nodes that are one hop away from the base station the value for their TIER ID is equal to 2. Whereas, if a node needed to forward a packet to the base station and this packet requires assistance of 3 sensor nodes performing multi-hop relays then this sensor node is said to be in zone 5 (TIER ID=5). The number of zones is limited by the variable type it was assigned to, `uint8_t` which allows 256 values starting from zero.

To establish the network topology configuration, a simple passing through mechanism is used. The base station broadcasts a network configuration packet which contains BS ID = 0 and TIER ID = 1. When this packet is received by a sensor node located in vicinity to BS it will know that it is one hop away from BS and set its TIER ID = 2. All other

nodes that received the message will do the same. The nodes that received the first broadcast will continue the network configuration process by issuing a configuration packet with TIER ID = 2. This message will be received by other nodes which will set their TIER ID to 3 accordingly. This process then continues until all the nodes are reached and assigned with a corresponding TIER ID. As soon as the configuration packet has been successfully passed through the network topology, the PriBaR protocol can start to route packets back to the BS.

The second part of PriBaR protocol is network congestion management module. In TCP/IP network, congestion management is based on:

- i comparison of historical traffic volume [12],
- ii response time [12], and
- iii packet loss [13]

These approaches not only require large amount of memory and computing power but also reside on top of TCP/IP layer, which associate with an overhead that is not possible to apply in WSN. To mitigate the network congestion, the PriBaR protocol relies on the CSMA/CA medium access control with priority packet support. This module works like this:

- i when the channel is too busy random delay kicks in, the nodes have to wait for x amount of time before re-transmission
- ii prioritised packets are associated with important or critical data, therefore they will access the channel with higher priority.

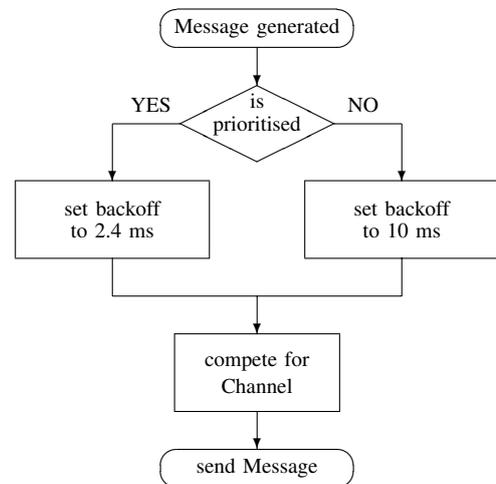


Figure 2. Flow chart; setting initial backoff when competing for the channel

Nodes can distinguish between three types of messages. First message type is TIER message. A node that did not receive a TIER message does not know its position in the network, and therefore is not going to take over any forwarding jobs and does not generate traffic itself. This type of message is recognised by the MAC layer since it has a different message type ID and therefore triggers a different function. The flow chart of the triggered function is displayed in Fig. 3. Second type of message is the data message. Initially white-spaced with zeros, the only information in this message is the origin

node ID and TIER zone ID, the time of departure from the origin node, the buffer utilisation and dropped messages count at the origin node and whether it is a prioritised message or not. Each intermediate node is filling its information about ID, TIER zone ID, buffer utilisation and number of dropped packets at the first white space it finds next to the information from the previous node. A data message usually is acknowledged on reception. Therefore, the MAC acknowledgement (ACK) is turned on and indicates that the sent message is received from the relay node or base station. On reception of an ACK the transmission is finished. It is prompting the buffer pointer to be increased and therefore sending the next message, if there is one. Furthermore, the resend-counter is reset. The reset counter is used to limit the retries before a messages is going to be dropped. The flow chart of PriBaR's medium access is illustrated in Fig. 2.

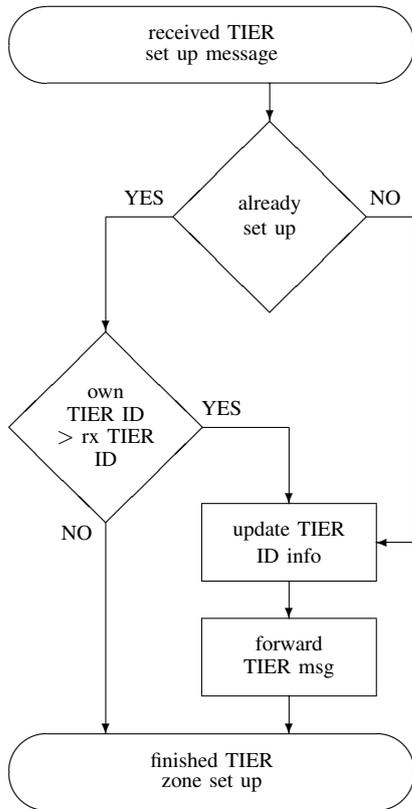


Figure 3. TIER set up flow chart

IV. EXPERIMENT CONFIGURATION

Main goal of the experimental set up was to create 4 zones each hosting 5 nodes. In order to set up a non-overlapped multi-tier environment, it was impossible within the given environment to set up more than 4 zones, where each zone got a LoS (line of sight) to the next upper and lower zone and every node can receive the time base signal. The experiment required a careful configuration so that the nodes in x^{th} -TIER zone could only communicate to nodes in $(x+1)^{\text{th}}$ and $(x-1)^{\text{th}}$ tiers but no others. This was done by separating the nodes in different screened areas within the lab; concrete walls are

utilised to provide necessary partitioning allowing a number of TIERS being setup in a confined area. Fig. 4 illustrates the experiment configuration. With this set up there was no zone x that had a line of sight (LoS) with neither $x-2$ nor $x+2$.

In the experiment, 20 nodes, always 5 node in one of the 4 zones, were used and one base station node, all based on MICAz [xbow] hardware.

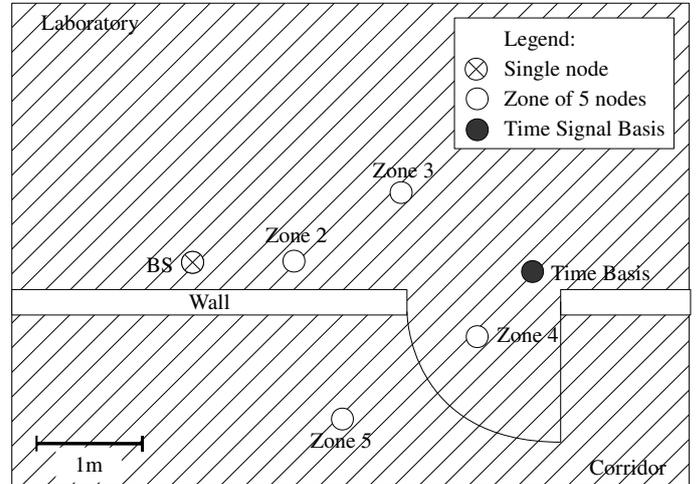


Figure 4. Dimensions of the experimental set up

After the zone configuration was completed, the nodes only performed forwarding task to those nodes that were located in the previous zone, which have a higher TIER ID. This means that, for example, nodes in zone two would not accept a message from nodes in zone four. In the experiment, the sensor nodes did not only act as a relay node, but also as traffic sources. Each node is programmed with an exponential traffic generator, which will generate $\frac{2}{3}$ normal packets per second and 1 priority packet every 60 seconds.

The measurement with this set up will be presented in the following section. The presented figures will all be organised in the same way that they x-axis represents the zone IDs, the y-axis the measured physical quantity, and the different grey scales represent a different node in the corresponding zone. If the value drops to zero in a certain zone and rises above zero in the following zone, this simply means that the physical quantity could not be measured at this specific node.

V. RESULTS

The measurements that were carried out within the experiment include the total delay of both, normal and prioritised messages, the amount of dropped messages at each node, again for both kinds of messages. Furthermore, each node that forwarded a message was stamping its buffer utilisation of normal messages, if the message was a non-prioritised message, or the prioritised buffer utilisation was stamped, if the forwarded message was a prioritised message. Additionally, each node was putting its ID and its TIER zone ID into the message. Based on that information it can be shown that no message that arrived at the base station was taking an unnecessary turn or was looping between zones at all.

VI. CONCLUSION AND FUTURE WORK

In this paper, a cross layer solution has been proposed to fulfil the latest evolution trends of WSN in which data load increases from its conventional low volume to a moderate load. Instead of using static topology, here, the network topology is dynamic which changes frequently. This evolution has offered new challenges in WSN research and development, contradicting current WSN design spaces.

From the values in Tab. I the prioritised message handling was proven. Decreasing the initial back off time and always handling prioritised messages first, increases the likelihood to win the channel for the transmission and hence faster forwarding is achieved. Also the routing scheme of PriBaR is proven, since not a single message that arrived at the base station took an unnecessary hop or looped between zones. This scheme of straight forward routing will be adjusted in the future to guarantee delivery even if there is no next hop directly available. Therefore, the experimental set up needs to be reconfigured and the implementation of further functionality is required.

REFERENCES

- [1] I. F. Akyildiz, T. Melodia, and K. R. Chowdury, "Wireless multimedia sensor networks: A survey," *IEEE Wireless Communications*, 2007.
- [2] M. Radenkovic and B. Wietrzyk, "Wireless mobile ad-hoc sensor network for very large scale cattle monitoring," in *Proc. IEEE Sixth International Conference on Networking (ICE'07)*, 2007.
- [3] H. Karl and A. Willig, *Protocols and Architectures for Wireless Sensor Networks*. The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England: John Wiley & Sons Ltd., 2005.
- [4] C. Technology, *MICAZ Datasheet*. [Online]. Available: http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/MICAZ_Datasheet.pdf
- [5] C. Wang, K. Sohraby, B. Li, M. Daneshmand, and Y. Hu, "A survey of transport protocols for wireless sensor networks," *Networking, IEEE*, vol. 20, no. 3, 2006.
- [6] K. H. Kwong, H. G. Goh, C. Michie, and I. Andonovic, "Priority medium access control for wireless sensor network," *Communication Systems and Networks*, 2008.
- [7] C. Suh and Y.-B. Ko, "A traffic aware, energy efficient mac protocol for wireless sensor networks," *Circuits and Systems, 2005. ISCAS 2005*, vol. 3, 2005.
- [8] L. van Hoessel and P. Havinga, "A lightweight medium access protocol (lmac) for wireless sensor networks," *1st Int. Workshop on Networked Sensing Systems (INSS 2004)*, 2004.
- [9] M. Zawodniok and S. Jagannathan, "Predictive congestion control protocol for wireless sensor networks," *IEEE Wireless Communications*, vol. 6, no. 11, 2007.
- [10] C.-Y. Wan, A. T. Campbell, and L. Krishnamurthy, "Pump-slowly, fetch-quickly (psfq): A reliable transport protocol for sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 4, 2005.
- [11] S. Kulkarni, A. Iyer, and C. Rosenberg, "An address-light, integrated mac and routing protocol for wireless sensor networks," *Networking, IEEE*, vol. 14, no. 4, 2006.
- [12] S. Feit, *TCP/IP Architecture, Protocols, and Implementation with IPv6 and IP Security*. New York: McGraw-Hill, 1996.
- [13] S. Hashim, H. T. Mouftah, and N. D. Georganas, "A new transport layer sensor network protocol," in *Proc. IEEE Canadian Conference on Electrical and Computer Engineering 2006. (CCECE'06)*, 2006.

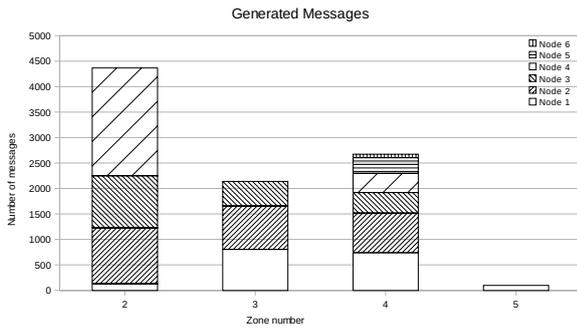


Figure 5. Generated packets at nodes over the network

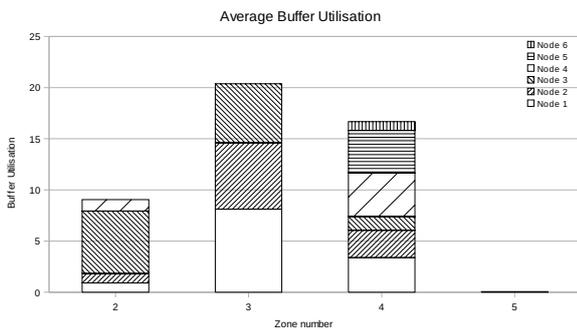


Figure 6. Buffer utilisation over the network

The first graph that is presented in Fig. 5 shows the amount of generated messages at each node that arrived at the base station, which does not mean that every message arrived at the base station. This graph shows that messages from TIER zones further away from the base station suffer from higher likelihood of packet loss and therefore fewer packets arrived from there. In an ideal network, including an ideal channel with zero loss, unlimited bandwidth and unlimited buffer capacity, one would expect a uniform distribution of generated messages. The message counter at each node, which includes also the dropped messages, suggest such a distribution. The reason for this is increased buffer utilisation towards the base station and hence the resulting higher contention for the channel. Fig. 6 shows the corresponding buffer utilisation.

One important issue of the experiment was to show that prioritised messages are travelling through the network faster than others. As it can be seen from Tab. I, prioritised messages travelled faster through the network than not prioritised ones.

Table I
DELAY TIMES

Delay [ms]	zone 2	zone 3	zone 4	zone 5
p messages	1753.2	3627.8	4630.9	6859.9
non-p messages	3475.1	6255.0	8365.1	5493.7