Poster: RI-MAC Enhancements for Interference Resilience

Alex King
School of Computing and Communications
Lancaster University, United Kingdom
a.king4@lancaster.ac.uk

Utz Roedig
School of Computing and Communications
Lancaster University, United Kingdom
u.roedig@lancaster.ac.uk

Abstract

In many Wireless Sensor Network (WSN) deployments, the communication medium is shared with other interference sources, such as WiFi, Bluetooth, and Microwave ovens. The performance of WSN Medium Access Control (MAC) protocols is known to be reduced under these conditions, including diminished packet delivery as collisions increase.

The design of current MAC protocols, which cater for low energy and reliable packet delivery, perform poorly in interference conditions. This is due in part firstly, to the fragility of the sender/receiver rendezvous, and secondly, to the channel arbitration and collision recovery approaches being agnostic to the cause of packet loss.

We analyse the operation of one particular MAC protocol, RI-MAC, and consider its behaviour under interference. Following this, three mechanisms are proposed to bolster interference resilience: Resilient Probes, Resilient Channel Arbitration and Resilient Data transmission. These mechanisms are designed around RI-MAC, however are broad enough to be applicable to most other WSN MAC protocols.

1 Introduction

Wireless Sensor Network (WSN) MAC protocols must enable reliable communication between nodes while minimising use of the radio, in order to conserve energy. In asynchronous MAC protocols, node wakeup times are not synchronized, decreasing the running energy costs at the expense of individual packet transmissions. In sender-initiated MAC protocols, such as ContikiMAC [2], the burden is on the sender to establish syncrhonization; conversely, receiver-initiated MAC protocols, such as RI-MAC [4], rely on the receiver to establish packet transmission.

WSN hardware based on the IEEE 802.15.4 PHY layer share the 2.4Ghz frequency range with other interference sources, including WiFi (IEEE 802.11), Bluetooth (IEEE 802.15.2). These protocols implement different channel access policies. In [3] these, combined with dissimilar PHY characteristics, were found to render ineffective WSN MAC protocol collision mechanisms and disadvantage the WSN. Our work builds on the observations in [1], by bolstering the rendezvous mechanisms resilience to interference.

Collisions may be due to transmitted packets colliding with interference, preventing the receiver from being able to receive the packet. Collisions may also occur through the MAC protocols use of Clear Channel Assessments (CCA) - a true/false indicator of channel energy. CCA are used during packet transmission - to ensure the channel is clear, and during packet reception - to decide whether the radio should be kept powered on to receive incoming data or return to a power efficient sleep state.

In either case, sending nodes must respond to a collision by entering the Collision Recovery Mechanism (CRM), in order to resolve the collision and deliver the packet. In current MAC protocols, the sending state machine cannot discern the type of interferer, and so must assume collisions with another WSN device as the worst-case scenario. The subsequent response, such as a random back-off before retrying later, is in most cases not the optimal policy in interference conditions.

2 RI-MAC

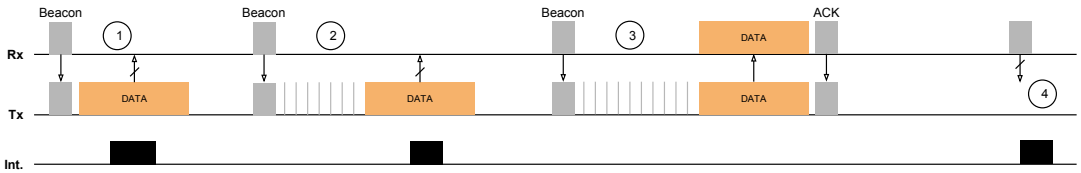
RI-MAC is a receier initiated WSN MAC protocol, where alignment of sender and receiver wakeup intervals are initiated by the latter. Each wakeup interval, nodes broadcast a beacon indicating they are ready to receive traffic. To send a packet, nodes wait to receive a beacon from the destination node, then delay a random backoff before transmitting. Unlike sender-initiated MAC protocols, collisions can be detected by receivers using CCA, meaning that receivers can throttle retransmissions by transmitting another beacon. To arbitrate channel access, receivers increase the backoff window duration advertised in the beacon. The operation of RI-MAC is shown in figure 1a.

In interference conditions, we identify three components of this RI-MAC that can impair performance:

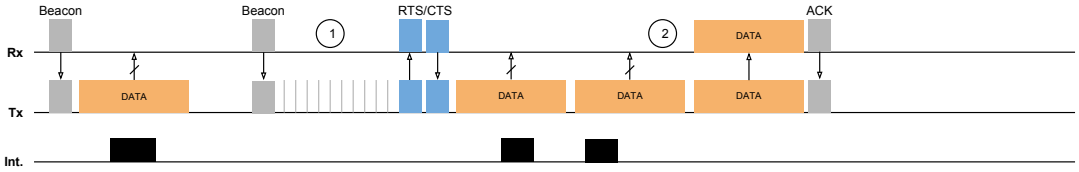
1. Beacon loss - caused by collision with other interference.
2. CCA collision - detecting other interference.
3. Packet corruption - caused by collision with other inter-

International Conference on Embedded Wireless Systems and Networks (EWSN) 2016
15–17 February, Graz, Austria

ISBN: 978-0-9949886-0-7



(a) Standard RI-MAC: 1) Collision prevents data packet from being received 2) Receiver detects collision, and transmits another beacon specifying a backoff window. 3) Further collisions cause the receiver to increment the size of the backoff window, until the packet is received. 4) Probe packet being destroyed by interference halts the sender/receiver rendezvous mechanism.



(b) RI-MAC with Resilient Channel Arbitration: 1) Channel arbitration is handled by RTS/CTS mechanism, following random back-off. 2) Once nodes have received a CTS, exclusive access to the channel is assured, and retransmissions are scheduled immediately.

Figure 1: RI-MAC

ference.

(1) has the greatest impact on communication latency, since transmitters must wait an entire duty cycle to hear another beacon before being able to transmit again.

(2) and (3) both induce the CRM in RI-MAC: transmitting a new beacon specifying an increased backoff window size. In contending for channel access with devices such as WiFi and Bluetooth, which have finer timescales and different channel access mechanisms, this only delays packet reception, and does not improve packet reception rate.

3 Interference Resilience

Based on these observations of RI-MAC, the following solutions are proposed.

3.1 Resilient Channel Arbitration

The current CRM in most MAC protocols combines channel arbitration, and packet delivery: initiating a random back-off for each subsequent retransmission. Resilient Channel Arbitration instead separates the two, first handling channel arbitration where nodes compete for channel access. Then, once one sender is granted exclusive use of the channel, packets can be transmitted without regard for other WSN transmitters. This is achieved using Request-To-Send (RTS)/Clear-To-Send (CTS) packets: senders transmit a RTS packet, and receivers respond with a CTS packet. Upon receiving an CTS packet, senders have exclusive access to the channel, and can transmit packets back-to-back until an ACK is received.

As retransmissions have less time to waste, this achieves better latency, and is based on the assumption that the best response following a collision is immediate retransmission, as is the case with parallel WiFi/Bluetooth deployments. The operation of Resilient Channel Arbitration in RI-MAC is shown in figure 1b.

3.2 Resilient Probes

Beacon transmissions are made more resilient to interference and packet loss, mitigating the affects of beacon loss. This is achieved by embedding multiple beacon packets, including separate preamble, header, and footer. Interference has a lower probability of destroying all packets within a beacon, hence receivers have a greater chance of receiving at least one.

3.3 Resilient Data

Data packets can be made more resilient to corruption by implementing Forward Error Correction (FEC): embedding additional payload within transmitted packets which can be used to correct errors caused by collisions. This increases the energy cost of transmitting packets. Resilient Data strikes a balance between minimum FEC needed to recover the packet, and minimising energy use, by incrementing the degree of FEC transmitted with each packet retransmission, until an ACK is received.

4 Conclusion

In this poster, RI-MAC is used as an example case for current MAC protocol implementations that perform poorly in the presence of interference. This is due to design assumptions that are suitable in quiet environments, such as most packet loss caused by channel contention, that impair performance in busy environments. Three improvements are described to RI-MAC to affect better interference resilience, including more reliable reception of RI-MAC beacons and data packets, and a separated channel contention/packet delivery policy. In future work, we intend to implement and evaluate these features on RI-MAC.

5 References

[1] Carlo Alberto Boano, Thiemo Voigt, Nicolas Tsiftes, Luca Mottola, Kay Römer, and Marco Antonio Zúñiga. Making sensornet mac protocols robust against interference. In *Wireless Sensor Networks*, pages 272–288. Springer, 2010.

[2] Adam Dunkels. The contikimac radio duty cycling protocol. 2011.

[3] Chieh-Jan Mike Liang, Nissanka Bodhi Priyantha, Jie Liu, and Andreas Terzis. Surviving wi-fi interference in low power zigbee networks. In *Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems*, pages 309–322. ACM, 2010.

[4] Yanjun Sun, Omer Gurewitz, and David B Johnson. Ri-mac: a receiver-initiated asynchronous duty cycle mac protocol for dynamic traffic loads in wireless sensor networks. In *Proceedings of the 6th ACM conference on Embedded network sensor systems*, pages 1–14. ACM, 2008.