Mutual Aid Among Sensors: An Emergency Function for Sensor Networks

Costas Michaelides* and Foteini-Niovi Pavlidou**

School of Electrical and Computer Engineering, Aristotle University of Thessaloniki, Thessaloniki, 54124, Greece

*Member, IEEE

**Senior Member, IEEE

Abstract—A large number of wireless sensor nodes in a certain area results in high contention. Inevitably, the transmissions of any possible critical data packets may fail due to collisions. In this article, we introduce an aspect of human intelligence in wireless sensor networks, influenced by cooperative networking, which enhances the timely delivery of critical data. Mutual aid among sensors (MAAS), is an emergency out-of-the-box medium access control (MAC) function for IEEE 802.15.4-2020. Specifically, the network coordinator detects critical data packets and sets an emergency flag to its next beacon, to inform the nodes that they may overhear data packets. When a node overhears a critical data packet from a neighboring node it switches to sleep mode and stays idle until the end of the superframe. Thus, interference is mitigated locally and temporarily. Simulation results, using the CC2650 radio parameters in OMNeT++, show that interference is reduced significantly, in favor of the timely delivery of critical data packets.

Index Terms—Access protocols, cooperative networks, interference mitigation, wireless sensor networks.

I. INTRODUCTION

Amy transmits critical data and Jon stays silent instead of interrupting her. This may not be science fiction. Recently, the devastating fires in Australia and the COVID-19 outbreak have shifted our focus towards sensing [1]. On this occasion, we revisit interference mitigation in sensor networks with a new perspective: we argue that mutual aid deserves to be a built-in capability of sensors. Therefore, we propose a medium access control (MAC) function for IEEE 802.15.4-2020 [2], based on the principle that each sensor node is willing to assist its neighbors.

The monitoring of an area is a common application in sensor networks. We place the sensors and expect them to transmit their data packets to the coordinator using random access, without any further configuration. However, interference increases as the number of nodes increases and the delivery of any critical data becomes uncertain. In the tradition of cooperative networking [3], we propose mutual aid among sensors (MAAS). First, the coordinator detects critical data packets and notifies the nodes that there is an emergency. Next, a node may overhear a critical data packet and switch into sleep mode to lower the level of interference. This moderate use of overhearing is feasible thanks to ultra-low power consumption transceivers, such as CC2650 [4].

IEEE 802.15.4-2020 includes a modern MAC with several capabilities for multiple PHY. Apart from star topology, it supports peer to peer formations such as clusters. There is a distinction between full-function devices (FFDs) and reduced-function devices (RFDs). The time is divided in superframes. A coordinator, essentially an FFD, transmits beacons periodically to inform the rest of the nodes about the upcoming superframe. A superframe may contain a contention access period (CAP), which supports slotted carrier-sense multiple

access with collision avoidance (CSMA/CA), and a contention-free period (CFP) with guaranteed time slots (GTS). Additionally, the standard provides a persistent CSMA/CA with priority channel access (PCA), to enhance the delivery of critical data. PCA is a backoff algorithm, where a node performs a persistent random backoff after a failed clear channel assessment (CCA), in order to gain access to the channel as soon as possible. Also, two modes of channel diversity are supported: time slotted channel hopping (TSCH) and deterministic and synchronous multi-channel extension (DSME).

Interference is a well known cause of signal degradation. There are quite a few approaches in the literature regarding interference mitigation. An early attempt to improve the timely delivery of critical data was [5], which added queuing strategies to CSMA/CA. The combination of scheduled and random access is desirable as well, see [6]. As described in [7], a way of mitigating collisions due to hidden nodes is clustering. Also, a collision avoidance algorithm was proposed in [8] which can be useful in mesh networks. Moreover, contention can be reduced using adaptive transmission power, see [9]. TSCH has been exploited in several works to date, such as [10] and [11]. DSME is also an active area, see [12]. Indeed, channel diversity is effective, but has a significant cost of complexity due to scheduling and channel hopping. Our goal is to present a simple out-of-the-box function, compatible with the standard.

The rest of this article is structured as follows. In Section II we present and discuss MAAS. Our system model is presented in Section III. In Section IV, we discuss the results of the simulations. Section V concludes the article.

II. MUTUAL AID AMONG SENSORS

MAAS is an emergency MAC function for IEEE 802.15.4-2020 which reduces contention and enhances the timely delivery of critical data. As a MAC capability, it may be enabled or disabled adaptively in a beacon enabled superframe, as described in [13].

Corresponding author: Costas Michaelides (e-mail: cmich@computer.org).

Fig. 1. Flow diagram of MAAS.

The coordinator transmits beacons periodically to synchronize the nodes and to inform them about the upcoming CAP. Amy, a node that has critical data, receives a beacon and transmits a critical data packet. The coordinator receives the critical data packet from Amy and sets an emergency flag to the following beacon. Jon, a node that does not have critical data, receives the beacon and schedules a timer to switch to sleep mode and another one to enter CAP. Then, Jon starts overhearing. In the meantime, Amy transmits a critical data packet again. Jon detects the critical data packet and cancels its CAP timer. Therefore, it switches to sleep mode and wakes up just on time to receive the next beacon. Jon may not detect any critical data. In this case, it switches to sleep mode for a while and enters CAP as scheduled. This flow of events is depicted in Fig. 1.

MAAS is inspired by the cooperative methods in networking, based on overhearing and forwarding, and offers a simple and intuitive alternative: a node may provide help by sleeping instead of forwarding. This idea suits well many applications in sensor networks, particularly critical systems suffering from high contention. When a node does not have any critical data, it may be more useful to sleep instead of transmitting: it mitigates contention and it saves some energy as well. Each node is rewarded with some sleep time for its help.

The proposed protocol does not require any additional frame transmissions. Instead, we attach one field to the beacon frame and one to the data frame. In the case of the beacon frame it indicates whether there is an emergency or not, while in the case of the data frame it indicates whether the frame contains critical data or not. We can assume with confidence that this overhead is negligible.

The duration of a critical event is assumed to span across multiple superframes. This refers to the cases where the nodes sense and transmit continuously. In case of extremely bursty traffic (e.g. one critical packet), the notification of the nodes at the beginning of the following superframe would be too late, since the critical packet has been already transmitted successfully. However, we expect that MAAS will be beneficial in most cases.

Fig. 2. Lognormal pathloss model.

Fig. 3. Operation of MAAS during a superframe, repeated over time.

III. SYSTEM AND CHANNEL MODEL

Our system model was implemented with Castalia [14], in OMNeT++ [15]. Castalia is a modular and extensible framework which allows us to test MAAS using its infrastructure.

The wireless channel module uses a lognormal model to calculate pathloss as a function of distance: $PL(d)_{dB} = PL(d_0) + 10\eta \log_{10}(d/d_0) + X(\mu, \sigma^2)$, where d is the distance, $PL(d_0) = 55$ dBm is the pathloss at distance $d_0 = 1$ m and $\eta = 2.4$ is the pathloss exponent. X is a normally distributed variable with $\mu = 0$ and $\sigma = 4$ dB. Apart from interference, pathloss is also a cause of signal degradation. A harsh pathloss model (see Fig. 2) helps us draw realistic conclusions about the performance of MAAS. Pathloss affects every signal, so it mitigates interference as well.

The simulated radio module is CC2650, by Texas Instruments. Its power consumption is calculated using the provided values by the data sheet [16]. The level of interference is calculated using the default additive interference model of Castalia. The estimation of bit errors for each received signal takes place after the subtraction of the received power from each other node.

The MAC module with MAAS capability is based on the baseline IEEE 802.15.4-2020 implementation of Castalia. It supports beacon enabled superframes and a CAP with slotted CSMA/CA, in compliance with the standard. MAAS requires the scheduling of two special timers. Upon the reception of a beacon with an emergency flag, Sleeping and CAP timers are scheduled as depicted in Fig. 3. Overhearing is limited to the first quarter of the superframe, Sleeping takes place during the second quarter and CAP during the second half of the superframe. If Jon does not detect any critical data packets from Amy, it follows the predefined schedule: it switches to sleep mode and enters CAP in the second half of the superframe. Else, if Jon detects a critical data packet from Amy, its CAP timer is canceled. Thus, it switches to sleep mode and stays in this state until the end of the superframe.

TABLE 1. Simulation parameters.

	Parameter	Value
Application	Time	5 s
	Area	20 m × 20 m
	Coordinator	1 (placed in the center)
	Nodes in total	5-50
	Nodes that have critical data	1-10
	Node deployment	Uniformly distributed
	Packet rate	10 packets/s
	Data payload	100 bytes
	Application packet overhead	5 bytes
	Network packet overhead	10 bytes
Network	MAC	
	Superframe	16 slots
	Slot duration	0.48 ms
	Access method	Slotted CSMA/CA
	Backoff period	0.16 ms
	Buffer	32 packets
	MAC frame overhead	14 bytes
	PHY	
	Carrier frequency	2.4 GHz
	Modulation	OQPSK
Channel	Bit rate	250 kbps
	Noise bandwidth	194 kHz
	Sensitivity	-100 dBm
	RX power	17.7 mW
	TX power	27.3 mW (5 dBm)
	Sleep power	1.65 mW
	PHY frame overhead	6 bytes
	Pathloss model	Lognormal

Fig. 4. Received packets by the coordinator (one realization).

IV. SIMULATION RESULTS

We evaluate the baseline IEEE 802.15.4-2020 implementation and MAAS, using a variable number of nodes that have critical data and a variable number of total nodes. Our simulation represents a 5 s critical event. See Table 1 for more details. The provided results are the mean values of 1000 realizations.

Fig. 4 depicts the received packets after one realization of the simulation using 20 nodes in total where 1 node has critical data, denoted with red color. The area matches the typical range of a coordinator in low-power networks, about 10 m. Each node transmits data packets to the coordinator. At first glance, MAAS seems effective, since packet reception from the red node is increased.

Fig. 5. Failed packets due to interference, 20 nodes in total.

Fig. 6. Received critical packets, 20 nodes in total.

Next, we evaluate MAAS using 20 nodes in total and a variable number of nodes that have critical data. In Fig. 5, failed packets due to interference are reduced significantly when a few nodes have critical data and increase as the number of nodes increases. Similarly, in Fig. 6, received critical packets are increased when a few nodes have critical data and decrease as the number of nodes increases. Fig. 7 shows that the received data packets with latency below 100 ms are increased only when a few nodes have critical data. Specifically, there is a peak at 3 nodes, indicating that interference from nodes that do not have critical data is minimized. This result depends on the range of each node. Fig. 8 shows that energy consumption is not affected. In fact, it is slightly reduced due to the applied sleep time. The aforementioned results of MAAS converge with the baseline. Essentially, MAAS has identical results to the baseline when every node has critical data, since every node participates in CAP.

Fig. 7. Received packets with latency below 100 ms, 20 nodes in total.

Fig. 8. Total consumed energy, 20 nodes in total.

Fig. 9. Failed packets due to interference, 5 nodes have critical data.

Fig. 10. Received critical packets, 5 nodes have critical data.

Scalability should be investigated as well. Fig. 9 and Fig. 10, show the failed packets due to interference and the received critical packets respectively, when 5 nodes have critical data and the number of total nodes is variable, from 5 to 50. We notice that the performance of the baseline declines rapidly due to contention. In contrast, MAAS maintains a low number of failed packets and high packet reception, even though the error bars indicate an increased level of uncertainty towards 50 nodes in total. Lastly, Fig. 11 shows the received data packets with latency below 100 ms, when 5 nodes have critical data. Note that, in Fig. 7, the performance of MAAS when 5 nodes out of 20 have critical data is low. This is also confirmed in Fig. 11 for a variable number of total nodes. Despite this, the performance of MAAS is consistently better than the baseline.

Our results, using a variable number of nodes that have critical data and a variable number of total nodes, show that the proposed function performs well. One may argue that the nodes that do not have critical data are treated somewhat unfairly. However, this is not the case. In sensor networks, the nodes usually have common goals, and MAAS guarantees that each one can rely on its neighbors' help when needed. Everyone has the opportunity to choose whether to stay silent or not. In the long run, everyone wins.

Fig. 11. Received packets with latency below 100 ms, 5 nodes have critical data.

V. CONCLUSION

In this article we introduced MAAS, an emergency function for interference mitigation in sensor networks, where the nodes may overhear critical data packets and switch temporarily to sleep mode. MAAS is compatible with IEEE 802.15.4-2020, it can be used as an out-of-the-box function and is very effective regarding timely delivery of critical data. It seems that artificial intelligence will be a key feature of future networks. We hope that mutual aid, a noble aspect of human intelligence, will be the first choice.

REFERENCES

- [1] J. J. Gooding and S. M. Liu, "A new year period emphasizing the need for better sensors," *ACS Sensors*, vol. 5, no. 3, pp. 597–598, Mar 2020.
- [2] *IEEE Standard for Low-Rate Wireless Networks*, IEEE Std. 802.15.4, July 2020.
- [3] F. H. Fitzek and M. D. Katz, *Cooperation in wireless networks: principles and applications*. New York: Springer, 2006.
- [4] CC2650. [Online]. Available: <http://www.ti.com/product/CC2650>
- [5] A. Koubaa, M. Alves, B. Nefzi, and Y.-Q. Song, "Improving the ieee 802.15.4 slotted csma/ca mac for time-critical events in wireless sensor networks," Polytechnic Institute of Porto, Tech. Rep. TR-060704, Jul 2006.
- [6] I. Rhee, A. Warrior, M. Aia, J. Min, and M. L. Sichitiu, "Z-mac: A hybrid mac for wireless sensor networks," *IEEE/ACM Trans. Netw.*, vol. 16, no. 3, pp. 511–524, Jun 2008.
- [7] A. Koubaa, R. Severino, M. Alves, and E. Tovar, "Improving quality-of-service in wireless sensor networks by mitigating "hidden-node collisions"," *IEEE Transactions on Industrial Informatics*, vol. 5, no. 3, pp. 299–313, Aug 2009.
- [8] J. I. Choi, M. Jain, M. A. Kazandjieva, and P. Levis, "Granting silence to avoid wireless collisions," in *The 18th IEEE International Conference on Network Protocols*, Oct 2010, pp. 82–91.
- [9] M. Chincoli, C. Bacchiani, A. A. Syed, G. Exarchakos, and A. Liotta, "Interference mitigation through adaptive power control in wireless sensor networks," in *2015 IEEE International Conference on Systems, Man, and Cybernetics*, Kowloon, China, Oct 2015, pp. 1303–1308.
- [10] K. Muraoka, T. Watteyne, N. Accettura, X. Vilajosana, and K. S. J. Pister, "Simple distributed scheduling with collision detection in tsch networks," *IEEE Sensors Journal*, vol. 16, no. 15, pp. 5848–5849, Aug 2016.
- [11] R. Tavakoli, M. Nabi, T. Basten, and K. Goossens, "Dependable interference-aware time-slotted channel hopping for wireless sensor networks," *ACM Trans. Sen. Netw.*, vol. 14, no. 1, pp. 3:1–3:35, Jan 2018.
- [12] F. Kauer, M. Köstler, and V. Turau, *openDSME: Reliable Time-Slotted Multi-Hop Communication for IEEE 802.15.4*. Cham: Springer International Publishing, 2019, pp. 451–467.
- [13] C. Michaelides and F. Pavlidou, "Programmable mac in body area networks, one command at a time," *IEEE Sensors Letters*, vol. 3, no. 7, pp. 1–4, Jul 2019.
- [14] Castalia. [Online]. Available: <https://github.com/boulis/Castalia/>
- [15] OMNeT++. [Online]. Available: <https://www.omnetpp.org/>
- [16] CC2650 SimpleLink™ Multistandard Wireless MCU, Texas Instruments, Jul 2016.