Open Access

Open Journal of Internet of Things (OJIOT)
Volume 1, Issue 1, 2017
http://www.ronpub.com/ojiot
ISSN 2364-7108

Mitigating Radio Interference in Large IoT Networks through Dynamic CCA Adjustment

Tommy Sparber [A], Carlo Alberto Boano [A], Salil S. Kanhere [B], Kay Römer [A]

[A] Institute for Technical Informatics, Graz University of Technology, Inffeldgasse 16/1, 8010 Graz, Austria, tommy@sparber.net, cboano@tugraz.at, roemer@tugraz.at

[B] School of Computer Science and Engineering, The University of New South Wales, Building K17, Gate 14, Barker Street, Kensington NSW 2052, Sydney, Australia, salil.kanhere@unsw.edu.au

Abstract

The performance of low-power wireless sensor networks used to build Internet of Things applications often suffers from radio interference generated by co-located wireless devices or from jammers maliciously placed in their proximity. As IoT devices typically operate in unsupervised large-scale installations, and as radio interference is typically localized and hence affects only a portion of the nodes in the network, it is important to give low-power wireless sensors and actuators the ability to autonomously mitigate the impact of surrounding interference. In this paper we present our approach DynCCA, which dynamically adapts the clear channel assessment threshold of IoT devices to minimize the impact of malicious or unintentional interference on both network reliability and energy efficiency. First, we describe how varying the clear channel assessment threshold at run-time using only information computed locally can help to minimize the impact of unintentional interference from surrounding devices and to escape jamming attacks. We then present the design and implementation of DynCCA on top of ContikiMAC and evaluate its performance on wireless sensor nodes equipped with IEEE 802.15.4 radios. Our experimental investigation shows that the use of DynCCA in dense IoT networks can increase the packet reception rate by up to 50% and reduce the energy consumption by a factor of 4.

Type of Paper and Keywords

Regular research paper: *Clear Channel Assessment, CCA, Contiki, Internet of Things, radio interference, RPL*

1 Introduction

Networks of low-power wireless sensors are an integral part of the Internet of Things (IoT) and enable a large number of applications with high societal relevance and impact. Miniature low-cost wireless sensors and actuators are indeed increasingly being used, among others, to build smart cities and make life in dense urban environments more comfortable, to control and optimize production processes in smart factories, to monitor the vital functions of patients in hospitals, or to maximize the comfort of inhabitants in residential buildings and offices while reducing their monthly energy bill.

This paper is accepted at the *International Workshop on Very Large Internet of Things (VLIoT 2017)* in conjunction with the VLDB 2017 Conference in Munich, Germany. The proceedings of VLIoT@VLDB 2017 are published in the Open Journal of Internet of Things (OJIOT) as special issue.

Several of these IoT applications employ a considerable number of devices and can be deployed on a very large scale (e.g., across several districts of a city [22], or across several wards in hospitals [13]). Despite the scale and the number of nodes, the network is expected to operate reliably and efficiently for extended periods of time. On the one hand, the sensed data or any actuation command needs to be reliably and timely delivered (e.g., alarms due to intrusion detection or deteriorating vital signs of patients). On the other hand, the energy consumption of the network needs to be minimized, as wireless sensors and actuators are typically powered by batteries with limited capacity. A highly energy efficient network implies a longer system lifetime and avoids a frequent battery replacement.

A major threat to the reliability and energy efficiency of low-power wireless networks used in the IoT is *radio interference*. Most of the commercial wireless IoT devices use indeed the increasingly crowded and lightly regulated ISM radio bands, freely-available portions of the radio spectrum reserved worldwide for industrial, scientific and medical purposes. The 2.4 GHz frequency spectrum is a notorious example of a crowded ISM band: Wireless devices specifically marketed for the IoT, such as IEEE 802.15.4, Bluetooth low-energy (BLE) and Wireless-HART, communicate using these frequencies and have not only to co-exist with each other, but also with other wireless devices and home appliances that communicate or emit noise in this frequency range [30]. The latter includes IEEE 802.11 (Wi-Fi) devices and microwave ovens, which are nowadays ubiquitous in households and residential or public buildings.

Figure 1 shows an example of wireless technologies employing the same frequencies for communication. IEEE 802.11, IEEE 802.15.4 and BLE use overlapping channels and their communications may hence experience disturbances from surrounding devices. The presence of neighboring devices transmitting at higher power may lead to unpredictable medium access contention times and high delays as well as to a significant increase in the packet loss rate. In addition, interference from surrounding devices may significantly worsen the energy efficiency of the system, as well as increase network traffic due to packet re-transmissions. As more and more IoT devices are being deployed nowadays, and as their number will grow exponentially in the coming years, it is to be expected that the shared frequency spectrum will become increasingly more crowded and that interference from surrounding devices will represent a major threat for the dependability of IoT applications deployed in large-scale installations.

An orthogonal problem to unintentional interference from surrounding wireless devices are *malicious jamming attacks* to IoT devices. The shared nature of the wireless medium makes indeed it easy for an adversary to launch denial of service attacks on low-power wireless devices, and these attacks can be easily accomplished also by using off-the-shelf equipment [20]. The presence of malicious jammers in the surroundings of a low-power wireless sensor or actuator can easily block the transmission and reception of packets, as well as quickly deplete a battery if no proper mechanisms are in place at the medium access control (MAC) layer [19].

The problem of denial of service attacks is even more significant given that most IoT devices are left unattended during their operation. For this reason, it is important to give low-power wireless sensors and actuators the ability to autonomously mitigate – when possible – the impact of surrounding interference.

In this paper we develop an approach, DynCCA [25], which dynamically adapts the clear channel assessment (CCA) threshold of low-power MAC protocols employed in common IoT applications. DynCCA uses only information computed locally to adjust the clear channel assessment threshold and can be used by all low-power MAC protocols based on carrier sense multiple access with collision avoidance (CSMA/CA). We show experimentally that this mechanism can significantly help in minimizing the impact of malicious or unintentional interference on both network reliability and energy efficiency. In particular, we demonstrate that varying the clear channel assessment threshold at run-time allows to filter the (malicious) noise generated by surrounding nodes, allowing a large-scale dense IoT network to sustain a high packet reception ratio and high energy efficiency even in the presence of interference.

The rest of this paper is organized as follows. The next section describes the body of work that has studied the role of clear channel assessment on the performance of IoT networks. Section 3 describes in detail how the CCA threshold can be used to tune network density and minimize the impact of malicious or unintentional interference on both network reliability and energy efficiency. We present the design of the DynCCA algorithm in Section 4, along with a description of its implementation on top of ContikiMAC. In Section 5 we evaluate experimentally the performance of DynCCA in a network of 30 nodes and show that a large portion of the devices in the network can efficiently escape the interference in their surroundings and sustain a high packet reception ratio. We finally summarize our contributions and conclude the paper in Section 6, along with a discussion of future work.

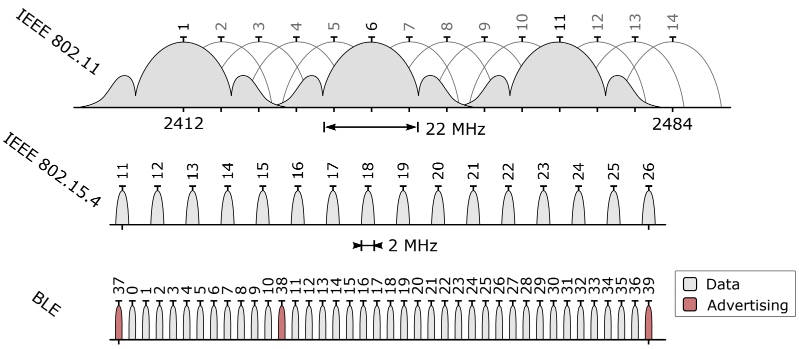


Figure 1: Wireless technologies used to build IoT applications, such as IEEE 802.15.4 and BLE, have to co-exist with each other as well as with co-located Wi-Fi networks [26]

2 Related Work

The influence of clear channel assessment on the performance of low-power wireless networks has attracted a large interest in the research community.

A large body of work has analyzed the impact of different clear channel assessment modes [29] and parameters such as back-off times [2] on the performance of IEEE 802.15.4 networks, providing helpful hints on how to optimize the use of the CCA algorithm. Wong et al. [27] and Kim [16] have analyzed the benefits and drawbacks of multiple clear channel assessments following the detection of a busy channel. Kiryushin et al. [18] have shown that low-power CSMA/CA-based MAC protocols suffer from a high number of collisions when transmitters can hear each other and start their transmissions almost at the same time, and suggested to select a CCA threshold close to the noise floor to reduce the number of such collisions.

Another body of work has proposed the use of algorithms that dynamically change the clear channel assessment threshold to improve network performance. In the remainder of this section, we review these algorithms, highlighting the key differences in comparison to our work.

Adaptive CCA to reduce channel access failures. King et al. [17] have shown that employing a back-off strategy when colliding with traffic generated by non IEEE 802.15.4 devices decreases network throughput and does not contribute to a collision resolution. Their findings confirm the experiments of Bertocco et al. [3] that have previously shown that the best performance in a crowded spectrum is obtained when disabling both the channel sensing the back-off mechanism of IEEE 802.15.4 devices. To alleviate the problem, King et al. [17] propose to dynamically differentiate CCA to ignore non IEEE 802.15.4 traffic during and before packet transmission, and to immediately re-transmit a packet without a back-off in case no acknowledgement is received and non IEEE 802.15.4 traffic has been detected. Similarly, Yuan et al. [28] have proposed an algorithm that dynamically adapts the CCA threshold to reduce the amount of discarded packets due to channel access failures, and validated it in simulation. In contrast to this body of work, our solution does not focus on channel access failures during transmissions, but instead on improving the efficiency of packet reception in the presence of radio interference.

Adapting the CCA threshold to minimize the number of false wake-ups. A few studies have experimentally shown that false-wake ups caused by a sub-optimal CCA mechanism can significantly affect the energy-efficiency of low-power listening protocols, especially in noisy environments. King et al. [17] have proposed an enhancement of ContikiMAC – Contiki's default MAC protocol – that lets a node keep its radio on to receive a packet only if IEEE 802.15.4 traffic has been detected. The authors exploit the modulation detection of carrier sense (i.e., the one reporting the channel busy only if an IEEE 802.15.4 compliant signal is detected) and ignore any other activities, hence immediately returning the radio to its sleeping state. Sha et al. [24] have designed AEDP, an adaptive energy detection protocol that dynamically adjusts a node's clear channel assessment threshold to improve network reliability and duty cycle based on application-specified bounds. In contrast to the work we describe in this paper, AEDP is a reactive approach that focuses on application-specific requirements (e.g., whether the current ETX is higher than a given threshold) and does not carry out a pro-active enhancement of network performance as soon as (malicious) radio interference is detected in the surroundings.

Adapting the CCA threshold to temperature variations. Researchers have also analyzed the impact of temperature variations on the performance of low-power MAC protocols, highlighting how the functionality of clear channel assessment on traditional low-power listening protocols drastically decreases at high temperatures [4, 10, 23]. In particular, Bannister et al. [1] and Boano et al. [5, 7, 11] have shown that the received signal strength attenuates at high temperatures due to the impact of temperature on the radio's low-noise and power amplifiers, which can cause a complete disruption of a wireless link when static clear channel assessment thresholds are employed. To alleviate the problem, the authors model the attenuation of the received signal strength on common low-power radios as a function of temperature variations, and leverage these models to dynamically adapt the CCA threshold of ContikiMAC. The adaptive algorithm described in this paper is orthogonal to this body of work, and can be combined with the aforementioned adaptive algorithm to maximize the reliability of IoT protocols in the presence of both temperature variations and radio interference in the surroundings.

3 Adjusting the CCA Threshold to Escape Interference

The clear channel assessment algorithm plays a fundamental role in low-power CSMA-CA MAC protocols with respect to reducing the number of wasteful transmissions and preserving the limited energy budget of the nodes in the network. In particular, CCA is traditionally employed for two main tasks:

1. *Collision avoidance during transmission.* Low-power CSMA-CA MAC protocols rely on clear channel assessment to determine whether another device is already transmitting on the same frequency channel, and defer transmissions that may otherwise collide with ongoing communications. In case no ongoing transmissions are detected, a packet is immediately sent, otherwise the MAC protocol defers the transmission using different back-off strategies [9].

2. *Wake-up of nodes.* Duty-cycled protocols such as ContikiMAC [14], B-MAC [21], and X-MAC [12] typically employ CCA to trigger wake-ups, i.e., to determine if a node should stay awake to receive a packet or whether it should remain in low-power mode. Towards this goal, an inexpensive CCA check is performed: If the channel is detected to be busy, the transceiver is kept on in order to receive the incoming packet, otherwise the radio returns to sleep mode.

The CCA check is traditionally carried out using energy detection or carrier sense. The latter consists in sampling the energy level in the wireless channel and comparing the measured signal strength with a given CCA threshold as shown in Figure 2. Most protocols employ fixed CCA thresholds and rely on the default system settings. This typically implies that the default value of the radio device is used, e.g., $-77\,\mathrm{dBm}$ for the widely used TI CC2420 transceiver [7].

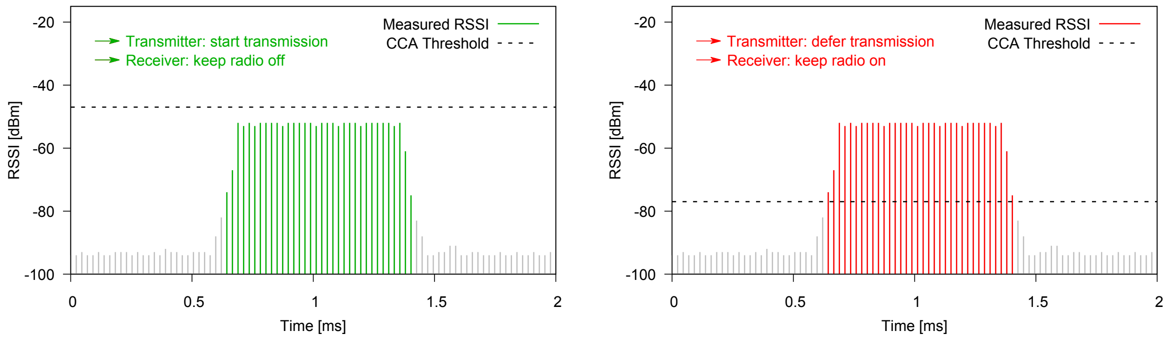
3.1 Varying the CCA threshold

Changing the default CCA threshold can have a strong impact on the performance of duty-cycled CSMA-CA MAC protocols, especially in the presence of interference in the surroundings.

Impact on energy consumption. On the one hand, lowering the CCA threshold, i.e., picking a value closer to the sensitivity threshold of the transceiver, may cause the radio to remain active for a large portion of time and hence reduce the energy efficiency of the system. Having a low CCA threshold maximizes indeed the chances to hear RF noise generated by surrounding devices, which increases the probability of backing-off during transmission as well as the number of false wake-ups during reception (see Figure 2(b)). This applies to RF noise generated by transmissions from other nodes in the same network (internal interference) and to RF noise generated by neighboring devices that do not belong to the same network (external interference) [6].

Impact on network density. On the other hand, increasing the CCA threshold allows to minimize the energy expenditure, but maximizes the risk of having a disconnected network. The CCA threshold has indeed a high impact on network density: If a node K receives packets from a neighbor N with a received signal strength R_S that is lower than the selected CCA threshold C_T, its radio is never woken up from low-power mode and no link can be established (see Figure 2(a)). By decreasing C_T to a value below R_S, Node K can establish a connection with N, but may increase the number of false wake-ups, as previously discussed. Consequently, increasing the CCA threshold helps in minimizing the number of false wake-ups, but may also cause the number of connected links in the network to drastically decrease.

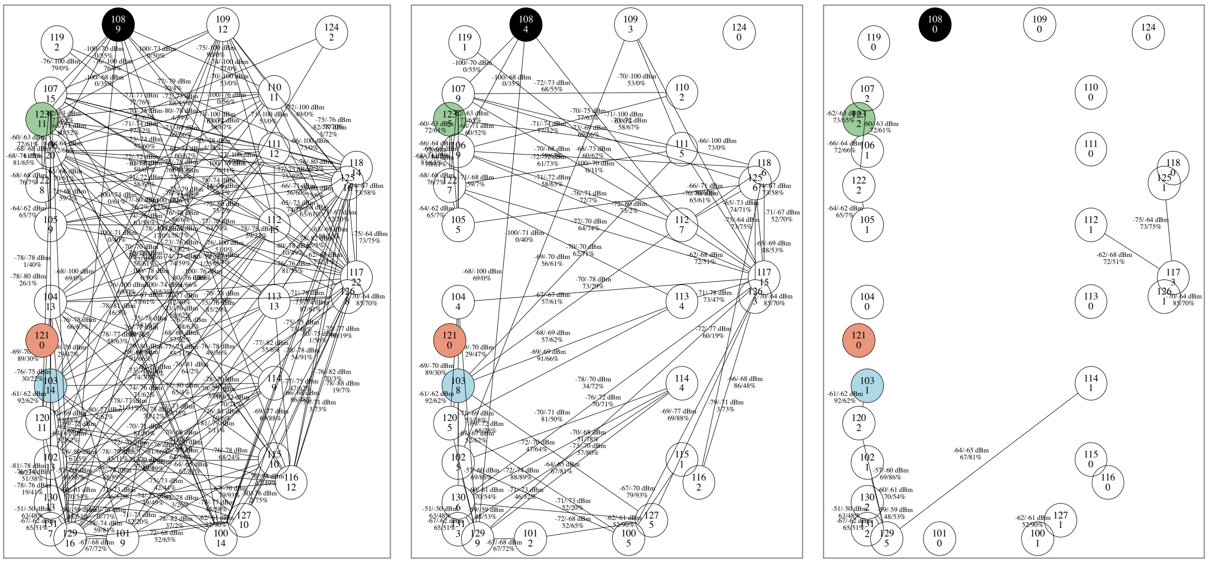
Figure 3 shows the impact of different CCA threshold values on connectivity in a network of 29 Advanticsys MTM-CM5000-MSP nodes (TelosB



(a) Received signal below CCA threshold

(b) Received signal above CCA threshold

Figure 2: The CCA algorithm is traditionally used in low-power CSMA-CA MAC protocols to perform collision avoidance during transmission and to wake-up nodes from their sleep state



(a) CCA threshold: $-80\,\mathrm{dBm}$

(b) CCA threshold: $-73\,\mathrm{dBm}$

(c) CCA threshold: $-65\,\mathrm{dBm}$

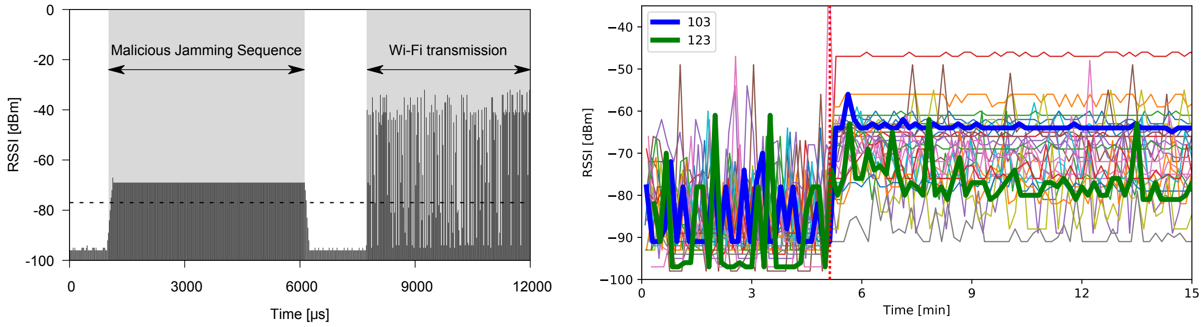
Figure 3: Varying the clear channel assessment threshold has a direct effect on the density of the network

replicas) deployed in an office building and transmitting packets periodically with an output power of $-22\,\mathrm{dBm}$. When selecting a low CCA threshold such as $-80\,\mathrm{dBm}$, the network is fully connected, with a total number of links between all nodes equals to 175 (Figure 3(a)). When increasing the clear channel assessment threshold of all nodes to $-73\,\mathrm{dBm}$, most of the nodes in the network are still connected (with the exception of node 124), but the total number of links is less than half compared to the previous case (Figure 3(b)). If the CCA threshold is increased further (e.g., to $-65\,\mathrm{dBm}$), most of the nodes in the network are isolated and cannot connect to any neighbor (Figure 3(c)).

3.2 Impact of Malicious Interferers on CCA Operation

A notable case is the one in which the selected CCA threshold is equal to or lower than the measured *noise floor*, i.e., the RSSI in absence of packet transmissions. In this case the medium is detected to be busy essentially at all times, postponing all transmissions and keeping the radio unnecessarily active to listen for incoming packets and causing a very quick battery depletion. This is for example the case when a malicious jammer is constantly active in proximity of a node.

This worst-case scenario is depicted in Figure 4(a), which shows the RSSI measured by an Advanticsys



(a) Measured RSSI with different interference sources

(b) Measured RSSI in the presence of a malicious jammer (node 121)

Figure 4: Comparison of the different RSSI measurements obtained in the presence of a malicious jammer and a Wi-Fi station active nearby (a) and RSSI measurements on all nodes in the network in the presence of a malicious jammer placed in their proximity (b)

MTM-CM5000-MSP sensor node in the presence of different types of interference. Initially, the noise floor is close to the sensitivity threshold of the radio (about $-95\,\mathrm{dBm}$, since the TI CC2420 is used). As soon as a malicious jammer is active nearby, the RSSI is persistently increased: If the received signal is above the CCA threshold, we have the aforementioned case in which the medium is detected to be busy essentially at all times. In the presence of Wi-Fi interference, instead, the RSSI is not constantly above the CCA threshold, but only for a fraction of time that is dependent on the type and frequency of Wi-Fi transmissions. It is important to highlight that smart malicious jammers could also emulate Wi-Fi transmissions (e.g., using JamLab [8]), and that it is hence important to be resilient both to a jammer constantly active and to intermittent and bursty interference.

The impact of interference is not the same across a network, as IoT networks can be *very large in scale*. Interference often affects indeed only a portion of the nodes in the network. To observe the spatial impact of a malicious interferer, we reuse the same network used to perform the density experiments shown in Figure 3 to run a data collection using Contiki's RPL, where all nodes forward data to a central sink (node 108, highlighted in black in Figure 3), and where all nodes periodically read their noise floor. One of the nodes in the network (node 121, highlighted in red in Figure 3), acts as a malicious jammer and emits constant noise by means of a continuous carrier [8]. Figure 4(b) shows the increase of noise floor at each of the nodes in the network after the malicious jammer is activated (i.e., after 5 minutes). Node 103 is closer to the jammer and measures an RSSI close to $-60\,\mathrm{dBm}$, whereas node 123 is rather far away and measures an RSSI below $-77\,\mathrm{dBm}$. For example, if the CCA threshold would be selected to be $-77\,\mathrm{dBm}$, Node 103 would be persistently blocked, whereas the operations of Node 123 would not be affected.

Based on the aforementioned observations, to mitigate the impact of interference it is necessary to (i) perform an accurate measurement of the noise floor on *all* nodes in the network, and to (ii) adapt the CCA threshold of each individual node such that most of the interference is avoided, while maintaining connectivity with the rest of the network. The next section presents a lightweight algorithm that dynamically changes the CCA threshold of a node based on the measured noise floor.

4 DynCCA: Design and Implementation

This section describes the design and implementation of DynCCA, an algorithm that dynamically adapts the clear channel assessment threshold of 802.15.4 radios to minimize the impact of malicious or unintentional interference on both network reliability and energy efficiency.

Requirements. As shown in Section 3, setting the CCA threshold just above the noise floor can help in escaping interference. This requires the ability to perform a *periodic* measurement of the noise floor. Such measurement should give an accurate picture of interference in the surroundings, but minimize the amount of time during which the radio is active to maximize energy-efficiency. As interference can occur in different forms, the algorithm to be designed should be *effective* against both malicious jamming and unintentional background interference. Finally, the algorithm to be developed should also be *transparent to the application*, i.e., the adaption of the clear

Algorithm 1: DynCCA's dynamic threshold adaptation

```
procedure DynCCA
    $x_t \leftarrow \text{find\_noise\_floor}(t) + \epsilon$
    $x_t \leftarrow \max(x_t, CCA_{fix})$
    $\text{CCA}_t \leftarrow \min(x_t, x_{t-1}, x_{t-2}, \ldots, x_{t-n-1}) + \beta$
end procedure
```

channel assessment should have minimal impact on the application running on the nodes.

Obtaining a good noise floor estimate. Due to the RSSI readings of low-cost IoT radios being noisy, a high number of RSSI samples at high frequency is traditionally required to get a good estimate of the surrounding interference. To reduce the number of measurements as well as the memory used, but still obtain a good picture of the surrounding interference, we sample RSSI values and build a histogram of the RSSI occurrences. This allows us to easily estimate the noise floor by identifying the highest observed RSSI level, the RSSI value occurring most often, or the minimum RSSI value recorded by at least a given portion of the readings (percentile).

DynCCA algorithm. DynCCA builds on top of the aforementioned RSSI estimation and is sketched in Algorithm 1. After deriving the noise floor x_t at time t from the RSSI measurements, a constant value ϵ is added to it in order to account for the co-channel rejection ability of low-power radios[1]. The chosen noise floor x_t is then capped at to a fixed threshold CCA_{fix}. This is an optional step, but important to reduce the number of false wake-ups in the networks and especially to allow an optimal *tree formation* in data collection protocols. For example, in the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL), the default objective function ETX tries to minimize the number of hops to the sink and hence prefers nodes sustaining a high packet reception ratio that can cover large distances. When selecting very low CCA thresholds, there is an increased chance to create links that are easily affected by radio interference or that can fall in the transitional region [31], causing a large number of parent switches and reducing network performance. Hence, by capping x_t at CCA_{fix}, we make sure to select nodes with an RSSI sufficiently higher than the transitional region. Please note that the selection of CCA_{fix} is especially critical in sparse networks, as high values may lead to a partitioned network (see Section 3.1).

After this step, a filtered baseline CCA_t is calculated and used as a lower bound for the CCA threshold. Filtering the measured noise floor is important to keep the network stable. As only the lower bound is of interest, the filter uses the minimum value of the last n samples. Adding a constant value β to CCA_t can help data collection protocols in selecting better parents by forcing a reduced set of neighbors ($\beta > 0$) or by lowering the CCA threshold to ensure that the network is connected ($\beta < 0$). Obtaining a sufficiently accurate knowledge of the current network performance and the number of neighbors to properly select β may, however, come at a higher communication overhead or energy expenditure, and we therefore keep this feature optional.

Implementation. We implement DynCCA on the popular Contiki operating system, and keep its implementation lightweight and energy efficient, as required to support constrained networked embedded systems. We implement DynCCA as a separate Contiki process, running every 10 s. The current implementation is optimized for Contiki OS' `sky` platform and measures the current noise floor for approximately 50 ms at a sampling frequency of about 20 kHz. It then determines a filtered value by computing the minimum value of the last four measurements. We further optimize the RSSI readings by implementing access to the SPI between the micro-controller and the CC2420 radio in assembler. The array employed to store the RSSI histogram uses 2 bytes per index and stores values in the range [-100,0] dBm.

5 Evaluation

We evaluate the performance of DynCCA experimentally and show that it helps to significantly improve both network reliability and energy efficiency.

5.1 Experimental Setup

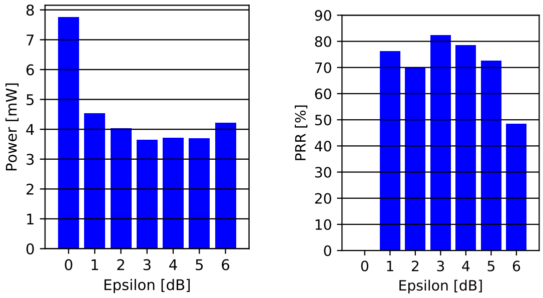
We run a set of experiments on 30 Advanticsys MTM-CM5000-MSP nodes deployed in our local testbed. All nodes run a data collection application using RPL with ETX as objective function and form a mesh network as shown in Figure 3. Each node periodically sends a UDP message with a payload of 46 bytes to the sink (marked in black in Figure 3). Transmissions are scheduled every 10 seconds, with a random offset of ±10 seconds. The transmission power of the nodes has been set to 4 to ensure multiple hops in our dense testbed setup and it is assumed that nodes cannot increase their transmission power to escape interference.

We use Contiki's default MAC protocol, ContikiMAC [14], with a channel check rate (CCR) of 32 Hz to better factor out packet losses due to internal interference. Using a lower CCR would decrease the

[1] Low-power radios can receive a valid packet only if it is higher than the noise floor by a factor specified as co-channel rejection ratio.

Table 1: Summary of our evaluation results

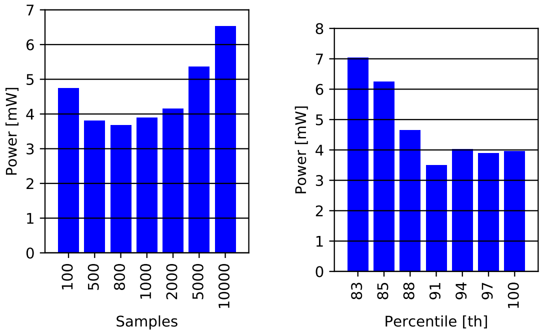
Interference type	**DynCCA active?**	**PRR [%]**	**Power consumption [mW]**	**No. of parent changes / node**	**Nodes with PRR >90%**
None	NO	94	3.45	4.00	27
None	YES	97	3.29	3.83	28
Wi-Fi	NO	86	8.16	13.24	18
Wi-Fi	YES	89	3.53	4.24	25
Malicious	NO	9	14.52	0.52	2
Malicious	YES	61	4.47	10.97	15



(a) Power [mW]

(b) PRR [%]

Figure 5: Performance of DynCCA as a function of ϵ



(a) Impact of number of samples

(b) Impact of noise floor choice

Figure 6: Power consumption of DynCCA as a function of the number of RSSI samples and noise floor choice

energy consumption, but also increase the packet loss and latency. Similar to the setup used in Section 3.2, we run JamLab [8] on node 121 (highlighted in red in Figure 3) at transmission power 11 to emulate either a Wi-Fi device or a malicious interferer. We collect the packet reception rate (PRR) between each node and measure the energy consumption of all the nodes in the network using Energest [15]. We further collect a number of low-level metrics such as the number of parent changes per node and the RSSI of each packet. All experiments last one hour and are repeated multiple times.

5.2 Results

We compare the performance of data collection using RPL in our network with Contiki's default CCA threshold and with DynCCA by performing experiments (i) in absence of controlled interference, (ii) in the presence of emulated Wi-Fi interference, and (iii) in the presence of malicious interference. Table 1 summarizes our results.

Power consumption. The use of DynCCA significantly helps in reducing the false wake-up rate in the presence of Wi-Fi interference. We have measured a decrease in the average power consumption of the nodes in the network from 8.16 mW to 3.53 mW when using DynCCA, i.e., an improvement of 56 %. DynCCA achieves even better results in the presence of malicious interference: The average power consumption in the network is reduced from 14.52 mW to 4.47 mW, i.e., a decrease of 69 %. By comparing the power consumption recorded in absence of interference (3.29 mW), we can also conclude that DynCCA is efficient and does not negatively affect the overall energy consumption.

Packet reception rate. As discussed in Section 4, the use of DynCCA helps RPL in forming an optimal tree by avoiding unreliable links close to or inside the transitional region. This is shown by the improvement in the packet reception rate of 3% in absence of interference as well as in the presence of Wi-Fi interference. In case of malicious interference, Contiki's default performance is very poor, with an average PRR in the network below 10 % and with only two nodes being able to sustain a PRR higher than 90 %. When using DynCCA, the PRR in the network is increased to 61 %, with 15 nodes being able to sustain a PRR higher than 90 %, i.e., DynCCA could allow 13 nodes to escape the malicious jammer by automatically adapting their CCA threshold.

Parent changes. Our experimental results have also shown that, in the presence of Wi-Fi interference, nodes experience a significantly lower number of parent changes per node (from 13.24 down to 4.24), reaching a value very close to the one observed when no interference is present (3.8). This further confirms that the use of DynCCA helps RPL in forming an optimal tree. Please note that in the case of malicious interference, the number of parent changes per node is increased from 0.51 to 10.96 due to the fact that, without DynCCA, the nodes' communication was blocked and thus no parent change could be performed.

Impact of specific parameters. We finally evaluate the performance of DynCCA as a function of specific parameters. First, we run experiments comparing the packet reception rate and power consumption in the network while changing ϵ in the range $[0, 6]$. Figure 5 shows our experimental results. When using $\epsilon = 0$, no packet is being received in the network, whereas selecting $\epsilon = 6$ leads to a less connected network and higher loss. A value of $3\,\mathrm{dB}$ represents the best trade-off, as it minimizes power consumption and maximizes the packet reception rate. This is perhaps not surprising, as $3\,\mathrm{dB}$ is exactly the declared co-channel rejection ratio of the employed radio transceiver – the TI CC2420. Please note that the experiments summarized in Table 1 were conducted with the optimal value of $\epsilon = 3\,\mathrm{dB}$.

We also analyze whether the number of samples or the noise floor percentile used have an influence on the efficiency of the DynCCA algorithm. Our experimental results summarized in Figure 6 show that a higher number of samples increases the accuracy but also the overhead: Using a noise floor percentile higher than the 88th and a number of RSSI samples between 500 and 2000 provides the best trade-off in terms of power consumption. Please note that the experiments summarized in Table 1 were conducted with 1000 RSSI samples and using the 100th percentile.

6 Conclusions

The CCA threshold used by radio-duty-cycled protocols such as ContikiMAC is found to be an adjustable knob to improve network performance under heavy interference. In this paper, we propose and implement DynCCA: An approach to dynamically change the CCA threshold in order to mitigate both unintentional and malicious interference in the surroundings of a node. An experimental evaluation shows that the use of DynCCA can increase the packet reception rate in a network from $9\,\%$ to about $60\,\%$, while also reducing the energy consumption by $69\,\%$. DynCCA is particularly useful for large IoT installations where the deployed nodes are unattended and vulnerable to denial of service attacks and interference from surrounding devices such as Wi-Fi access points.

In the future, we plan to carry out experiments by generating interference using real Wi-Fi devices instead of JamLab. Future work also includes the implementation of β: This would integrate data collected from RPL such as the number of available neighbors into the CCA threshold adaption algorithm to enforce a smaller set of (better) parents.

Acknowledgements

This work was performed within the LEAD-Project "Dependable Internet of Things in Adverse Environments", funded by Graz University of Technology, Austria.

References

[1] K. Bannister, G. Giorgetti, and S. K. Gupta, "Wireless Sensor Networking for Hot Applications: Effects of Temperature on Signal Strength, Data Collection and Localization," in *Proceedings of the* 5^{th} *International Workshop on Embedded Networked Sensors (HotEmNets)*, Jun. 2008.

[2] M. Bertocco, G. Gamba, and A. Sona, "Experimental Optimization of CCA Thresholds in Wireless Sensor Networks in the Presence of Interference," in *Proceedings of the IEEE Europe the Workshop on ElectroMagnetic Compatibility (EMC)*, Jun. 2007.

[3] M. Bertocco, G. Gamba, and A. Sona, "Is CSMA/CA really Efficient against Interference in a Wireless Control System? An Experimental Answer," in *Proceedings of the* 13^{th} *IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, Sep. 2008.

[4] C. A. Boano, "Dependable Wireless Sensor Networks," Ph.D. dissertation, Graz University of Technology, Graz, Austria, Nov. 2014.

[5] C. A. Boano, J. Brown, N. Tsiftes, U. Roedig, and T. Voigt, "The Impact of Temperature on Outdoor Industrial Sensornet Applications," *IEEE Transactions on Industrial Informatics*, vol. 6, no. 3, Aug. 2010.

[6] C. A. Boano and K. Römer, "External Radio Interference," in *Radio Link Quality Estimation in Low-Power Wireless Networks*, ser. SpringerBriefs in Electrical and Computer Engineering - Cooperating Objects. Springer International Publishing, Jul. 2013.

[7] C. A. Boano, K. Römer, and N. Tsiftes, "Mitigating the Adverse Effects of Temperature on Low-Power Wireless Protocols," in *Proceedings of the* 11^{th}

IEEE International Conference on Mobile Ad hoc and Sensor Systems (MASS), Oct. 2014.

[8] C. A. Boano, T. Voigt, C. Noda, K. Römer, and M. A. Zúñiga, "JamLab: Augmenting Sensornet Testbeds with Realistic and Controlled Interference Generation," in *Proceedings of the* 10^{th} *IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, Apr. 2011.

[9] C. A. Boano, T. Voigt, N. Tsiftes, L. Mottola, K. Römer, and M. A. Zúñiga, "Making Sensornet MAC Protocols Robust Against Interference," in *Proceedings of the* 7^{th} *European Conference on Wireless Sensor Networks (EWSN)*, Feb. 2010.

[10] C. A. Boano, H. Wennerström, M. A. Zúñiga, J. Brown, C. Keppitiyagama, F. J. Oppermann, U. Roedig, L.-Å. Nordén, T. Voigt, and K. Römer, "Hot Packets: A Systematic Evaluation of the Effect of Temperature on Low Power Wireless Transceivers," in *Proceedings of the* 5^{th} *Extreme Conference on Communication (ExtremeCom)*, Aug. 2013.

[11] C. A. Boano, M. A. Zúñiga, J. Brown, U. Roedig, C. Keppitiyagama, and K. Römer, "TempLab: A Testbed Infrastructure to Study the Impact of Temperature on Wireless Sensor Networks," in *Proceedings of the* 13^{th} *ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, Apr. 2014.

[12] M. Buettner, G. V. Yee, E. Anderson, and R. Han, "X-MAC: A Short Preamble MAC Protocol for Duty-cycled Wireless Sensor Networks," in *Proceedings of the* 4^{th} *ACM International Conference on Embedded Networked Sensor Systems (SenSys)*, Nov. 2006.

[13] O. Chipara, C. Lu, T. C. Bailey, and R. Gruia-Catalin, "Reliable Clinical Monitoring using Wireless Sensor Networks: Experiences in a Step-down Hospital Unit," in *Proceedings of the* 8^{th} *International Conference on Embedded Networked Sensor Systems (SenSys)*, Nov. 2010.

[14] A. Dunkels, "The ContikiMAC Radio Duty Cycling Protocol," Swedish Institute of Computer Science, Kista, Sweden, Tech. Rep. T2011:13, Dec. 2011.

[15] A. Dunkels, F. Österlind, N. Tsiftes, and Z. He, "Software-based On-line Energy Estimation for Sensor Nodes," in *Proceedings of the* 4^{th} *International Workshop on Embedded Networked Sensors (EmNetS)*, Jun. 2007.

[16] W. Kim, "Short Clear Channel Assessment in Slotted IEEE 802.15.4 Networks," *Wireless Personal Communications*, vol. 71, no. 1, Sep. 2012.

[17] A. King, J. Brown, and U. Roedig, "DCCA: Differentiating Clear Channel Assessment for Improved 802.11/802.15.4 Coexistence," in *Proceedings of the* 10^{th} *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Oct. 2014.

[18] A. Kiryushin, A. Sadkov, and A. Mainwaring, "Real-World Performance of Clear Channel Assessment in 802.15.4 Wireless Sensor Networks," in *Proceedings of the* 2^{nd} *International Conference on Sensor Technologies and Applications (SENSORCOMM)*, Aug. 2008.

[19] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga, "Energy-efficient Link-layer Jamming Attacks Against Wireless Sensor Network MAC Protocols," *ACM Transactions on Sensor Networks*, vol. 5, no. 1, Feb. 2009.

[20] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of Service Attacks in Wireless Networks: The Case of Jammers," *IEEE Communications Surveys Tutorials*, vol. 13, no. 2, May 2010.

[21] J. Polastre, J. L. Hill, and D. E. Culler, "Versatile Low Power Media Access for Wireless Sensor Networks," in *Proceedings of the* 2^{nd} *ACM International Conference on Embedded Networked Sensor Systems (SenSys)*, Nov. 2004.

[22] San Francisco Municipal Transportation Agency, "SFpark: Putting Theory Into Practice," Aug. 2011.

[23] F. Schmidt, M. Ceriotti, N. Hauser, and K. Wehrle, "If You Can't Take the Heat: Temperature Effects on Low-Power Wireless Networks and How to Mitigate Them," in *Proceedings of the* 12^{th} *European Conference on Wireless Sensor Networks (EWSN)*, Feb. 2015.

[24] M. Sha, G. Hackmann, and C. Lu, "Energy-efficient Low Power Listening for Wireless Sensor Networks in Noisy Environments," in *Proceedings of the* 12^{th} *ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, Apr. 2013.

[25] T. Sparber, "Experimental Analysis and Evaluation of RPL under Radio Interference," Master's thesis, Graz University of Technology, Graz, Austria, Jan. 2017.

[26] U. Wetzker, I. Splitt, M. Zimmerling, C. A. Boano, and K. Römer, "Troubleshooting Wireless Coexistence Problems in the Industrial Internet of Things," in *Proceedings of the* 14^{th} *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC)*, Aug. 2016.

[27] C.-M. Wong and W.-P. Hsu, "An Additional Clear Channel Assessment for IEEE 802.15.4 Slotted CSMA/CA Networks," in *Proceedings of the IEEE International Conference on Communication Systems (ICCS)*, Nov. 2010.

[28] W. Yuan, J.-P. M. Linnartz, and I. G. Niemegeers, "Adaptive CCA for IEEE 802.15.4 Wireless Sensor Networks to Mitigate Interference," in *Proceedings of the IEEE Wireless Communication and Networking Conference (WCNC)*, Apr. 2010.

[29] M. Zeghdoud, P. Cordier, and M. Terré, "Impact of Clear Channel Assessment Mode on the Performance of ZigBee Operating in a Wi-Fi Environment," in *Proceedings of the* 1^{st} *IEEE Workshop on Operator-Assisted Wireless-Mesh Community Networks (OpComm)*, Sep. 2006.

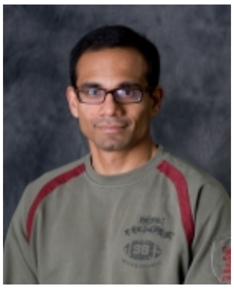
[30] G. Zhou, J. A. Stankovic, and S. H. Son, "Crowded Spectrum in Wireless Sensor Networks," in *Proceedings of the* 3^{rd} *Workshop on Embedded Networked Sensors (EmNets)*, May 2006.

[31] M. A. Zúñiga and B. Krishnamachari, "Analyzing the Transitional Region in Low-Power Wireless Links," in *Proceedings of the* 1^{st} *IEEE International Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, Oct. 2004.

Author Biographies

Tommy Sparber is an embedded software engineer at MEDS in Graz, Austria. He received his Bachelor and Master degree in Information and Computer Engineering from Graz University of Technology in 2013 and 2017, respectively. His Master's thesis analyzed experimentally the performance of RPL under radio interference. His current area of work spans from developing embedded Linux applications to real-time applications on small micro-controllers.

Carlo Alberto Boano is an assistant professor at the Institute for Technical Informatics of Graz University of Technology, Austria. He received a doctoral degree sub-auspiciis praesidentis from Graz University of Technology in 2014 with a thesis on dependable wireless sensor networks, and holds a double Master degree from Politecnico di Torino, Italy, and KTH Stockholm, Sweden. His research interests encompass the design of dependable networked embedded systems and the robustness of networking protocols against environmental influences.



Salil S. Kanhere is an associate professor at the School of Computer Science and Engineering at the University of New South Wales in Sydney, Australia. He obtained his B.E. in Electrical Engineering from VJTI, Bombay, India in 1998 and his M.S. and Ph.D., both in Electrical Engineering from Drexel University in Philadelphia, USA, in 2001 and 2003 respectively. Salil's current research interests are in the areas of sensor networks, mobile networking, vehicular communications and network security.

Kay Römer is a professor and director of the Institute for Technical Informatics at Graz University of Technology, Austria. He held positions of Professor at the University of Lübeck in Germany, and senior researcher at ETH Zürich in Switzerland. Prof. Römer obtained his Doctorate in computer science from ETH Zürich in 2005 with a thesis on wireless sensor networks. His research interests encompass wireless networking, fundamental services, operating systems, programming models, dependability, and deployment methodology of networked embedded systems, in particular Internet of Things, Cyber-Physical Systems, and sensor networks.