Towards Detecting WiFi Aggregated Interference for Wireless Sensors based on Traffic Modelling

Indika S. A. Dhanapala[1], Ramona Marfievici[1], Piyush Agrawal[2], Dirk Pesch[1]
[1]Nimbus Centre for Embedded Systems Research, Cork Institute of Technology, Cork, Ireland
I.S.A.Dhanapala@mycit.ie, Ramona.Marfievici@cit.ie, Dirk.Pesch@cit.ie
[2]United Technologies Research Centre, Cork, Ireland
AgrawaP@utrc.utc.com

***Abstract*—We present a technique to identify transmission timing for IEEE802.15.4 based Wireless Sensor Networks (WSNs) in the presence of WiFi interference. Our technique is based on modeling WiFi traffic with a Modulated Markov Poisson Process (MMPP) model in order to enable us to predict when WiFi transmissions take place and avoid them. We have evaluated the accuracy of our model in a small test-bed. Results are promising and suggest that our approach can increase the reliability of IEEE802.15.4 transmissions.**

***Index Terms*—Wireless Sensor Networks, Cognitive Radio, Traffic Modelling, Interference Detection**

I. Introduction

Many wireless sensor networks (WSNs) operate in the 2.4GHz unlicensed ISM band, which experiences much radio interference due to an increasing number of devices operating in this radio spectrum. Among the sources of interference, WiFi has been identified as the most dominant interferer for IEEE802.15.4 based WSNs in indoor environments. This is particularly critical in office environments where multiple WiFi Access Points (APs) are deployed utilising much of the 2.4GHz ISM band with transmission powers much higher than IEEE802.15.4 based WSNs. In addition, Bluetooth is another interferer, which can contributes to packet losses in WSNs. However, Bluetooth interference is not considered in this work. Overlapping of multiple WiFi channels with a single IEEE802.15.4 channel generates aggregated interference onto IEEE802.15.4 channels reducing transmission opportunities or increasing interference for wireless sensor nodes and thereby degrading the reliability and lifetime of the WSN [1], [2].

A number of techniques exist for detecting and classifying interference through spectrum sampling [2]–[4] or using corrupt packets [5]. All these, however, do not aim to predict transmission timing for IEEE802.15.4 based WSNs.

Contributions. We propose a technique to model aggregated interference from WiFi on IEEE802.15.4 channels using a Markov Modulated Poisson Process (MMPP). Based on the modelled traffic we predict transmission timing for wireless sensor nodes to increase communication reliability.

TABLE I: Overlapping WiFi and IEEE802.15.4 channels.

IEEE802.15.4 channel	11	12	13	14	15
Overlapping WiFi channels	1	1,2	1,2,3	1,2,3,4	2,3,4,5

II. Overview of the proposed technique

Traffic model. The proposed technique uses a 2^{nd} order MMPP (MMPP(2)) for modelling the packet Inter-Arrival Time (IAT) on individual WiFi channels. MMPP is widely used for traffic modelling as it can capture long range dependency of Internet traffic. MMPP(2) is the simplest model of that kind and is defined by 4 parameters [6], which are obtained by fitting the empirical packet IAT distribution to that of the model. To this end, balanced means and 2^{nd} order Coxian [7] fitting methods are used. The criteria for selecting a fitting method are dependent on the value of the coefficient of variation C of the empirical packet IAT distribution. The balanced means method is chosen if $C > 1$ or otherwise.

Traffic models for generating WiFi aggregated interference are built by taking the superposition of individual MMPP(2) traffic models. For example, WiFi channel 1–4 overlap with the IEEE802.15.4 channel 14 (see Table I). Thus, superposition of 4 MMPP(2) models that each characterise the traffic on those 4 WiFi channels has to be considered in order to model the aggregated interference on the IEEE802.15.4 channel 14. The operator "Kronecker sum" [6] is used for deriving the superposition of multiple MMPP(2) models. This operation increases the number of states in the aggregated traffic model to 2^N, where N is the number of overlapping WiFi channels. Figure 1 depicts the aggregated interference traffic model for 4 overlapping WiFi channels wherein the model generates packets with 16 different arrival rates λ_i $(1 \leq i \leq 16)$ depending on the current state of the traffic model and r_j $(1 \leq j \leq 8)$ denotes transition rates between states. Values of λ_i and r_j are updated dynamically over the time to enhance the performance of the model.

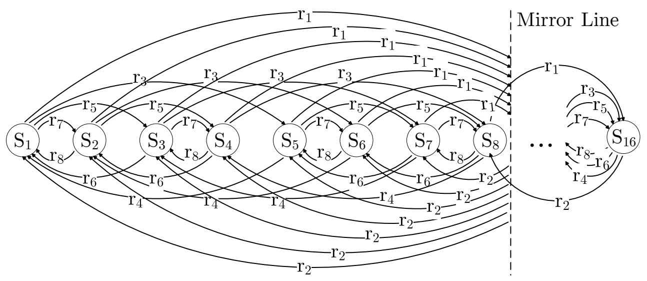


Fig. 1: Traffic model for 4 WiFi channel aggregated interference (each state has distinct packet arrival rate λ_i, $1 \leq i \leq 16$).

Model dynamics. Tuning each MMPP(2) traffic model in regular time intervals is important to keep the traffic models updated to the surrounding dynamic radio environment. To accomplish this, the distribution of WiFi packet IAT is recorded for all WiFi channels, whose statistics such as mean (μ), coefficient of variation (C) and the Hurst parameter (H) are used to obtain MMPP(2) model parameters using the fitting methods mentioned before. The parameters of each MMPP(2) traffic model are updated every 20 minutes.

III. Prediction of WiFi aggregated interference

We evaluate the performance of our approach by comparing our WiFi aggregated interference timing with the actual channel conditions (noise floor traces) we collected in a small-scale test-bed in an office environment with multiple APs.

Experimental setup. We deployed a test-bed composed of 5 TMote Sky nodes (with IEEE802.15.4 compliant radio chip) and 4 WiFi dongles. Motes and dongles were connected to a USB hub linked to a PC (see Figure 2).

Test execution. The collection of noise floor traces was performed by the TMote Sky nodes by sampling the Received Signal Strength Indicator (RSSI) every 1 ms on channels 11–14. The dongles *sniffed* WiFi channels 1–4 in order to obtain packet IAT distributions. Time synchronization is initiated by the PC with a command sent to the base station and dongles. The base station acts as a coordinator towards the rest of the WSN nodes. The results presented are based on the analysis of traces collected on different channels for 24 hours.

Evaluation. The model predicts the IEEE802.15.4 channel status by comparing the aggregated WiFi packet IAT with a predefined threshold of 5 ms (the approximate time required for the transmission of a IEEE802.15.4 packet at a data rate of 250 kbps). Actual channel status throughout the experiment is obtained by comparing the RSSI samples with a predefined threshold of -51 dBm [8]. Finally, the conditions on each channel retrieved by both methods are compared in order to quantify the accuracy of the proposed technique. The MMPP(2) model shows approx. similar performance on each WiFi channel though they have different loading conditions as depicted in Figure 3. WiFi channel 1 exhibits mean error (μ_{m}) of 105 ms and std. dev. (μ_{std}) of 49 ms. The other 3 channels show analogous characteristics with approx. 120 ms and 90 ms for μ_{m} and μ_{std} respectively in the corresponding MMPP(2) models. Figure 4 clearly shows that channel 14 suffers more WiFi traffic than other IEEE802.15.4 channels causing a slight decrease in the accuracy of interference detection. Channel 11 and 12 show 99% and 0.5% as mean and std. dev. of detection accuracy, while the other two IEEE802.15.4 channels exhibit that of 98.5% and 0.8%.

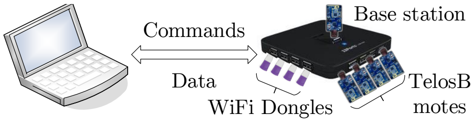
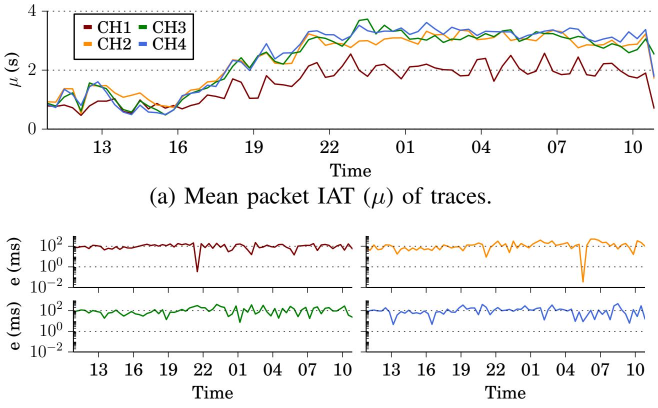


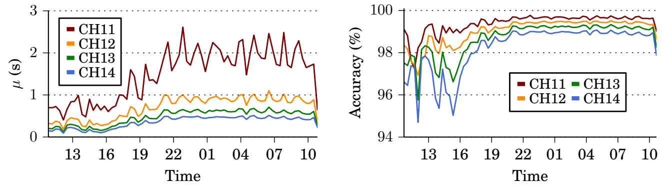
Fig. 2: Experimental setup.



(a) Mean packet IAT (μ) of traces.

(b) Error (e) between model and the trace.

Fig. 3: Validation of the MMPP(2) traffic model.



(a) Mean packet IAT (μ).

(b) Detection accuracy.

Fig. 4: WiFi aggregated interference seen by IEEE802.15.4 channels over 20 minutes time windows.

IV. Conclusions and future work

We present a novel technique to predict transmission opportunities for IEEE802.15.4 based WSNs using the estimate of WiFi packet IAT that can translate into a probability of interference at a certain point in time. This assists with WSN transmission timing. We evaluated the technique in a test-bed showing its high detection accuracy in a saturated WiFi environment. Nevertheless, more experiments are needed to confirm the observations. Future work is focused on advancing the proposed technique with a Hidden Markov Model (HMM) which dynamically selects the best communication channel and optimum transmission parameters for the WSN.

Acknowledgements. We thank Pablo Corbalán Pelegrín for helping with the code, Philip J. Harris and Rodolfo de Paz Alberola for their valuable comments. This work is funded by the Irish Research Council and United Technologies Research Centre Ireland.

References

[1] C.-J. M. Liang *et al.*, “Surviving Wi-Fi Interference in Low Power ZigBee Networks,” in *SenSys*, 2010.

[2] V. Iyer *et al.*, “Detecting and Avoiding Multiple Sources of Interference in the 2.4 GHz Spectrum,” in *EWSN*, 2015.

[3] R. Musaloiu *et al.*, “Minimising the Effect of WiFi Interference in 802.15.4 Wireless Sensor Networks,” *Int. J. Sen. Netw.*, vol. 3(1), 2008.

[4] C. Noda *et al.*, “Quantifying the channel quality for interference-aware wireless sensor networks,” *SIGBED Rev.*, vol. 8, no. 4, 2011.

[5] F. Hermans *et al.*, “SoNIC: Classifying Interference Categories and Subject Descriptors,” in *IPSN*, 2013.

[6] W. Fischer and K. Meier-Hellstern, “The Markov-modulated Poisson Process (MMPP) Cookbook,” *Perform. Eval.*, vol. 18, no. 2, 1993.

[7] I. Adan and J. Resing, *Queueing systems*. Eindhoven University of Technology, 2015.

[8] G. Thonet *et al.*, “ZigBee WiFi Coexistence White Paper and Test Report,” *Schnider Electric*, pp. 1–38, 2008.