Data Driven Design for Reliability of IoT Applications

Valentina Nejkovic[*], Nenad Milosevic[**], Filip Jelenkovic[*], Zorica Nikolic[**], Milorad Tosic[*]
[*] University of Nis, Faculty of Electronic Engineering, Department of Computer Science, Nis, Serbia
[**] University of Nis, Faculty of Electronic Engineering, Department of Telecommunications, Nis, Serbia
(valentina.nejkovic, nenad.milosevic, filip.jelenkovic, zorica.nikolic, milorad.tosic)@elfak.ni.ac.rs

***Abstract*— The reliability of IoT networks gained its significance during the past several years, mainly due to the harmful coexistence with other technologies operating in the same 2.4 GHz frequency band. IoT applications, using ZigBee, have much lower power than WiFi, the most widespread technology in this frequency band. Such a coexistence results in a significant packet loss in ZigBee networks, which makes them unreliable. The sensor data driven design directions, developed using the massive online IoT testbed SmartSantander, are given in this paper. The interference problems are identified and described, which is the most important step towards the future performance improvement of IoT applications.**

I. Introduction

Modern wireless communications systems are in a great expansion. However, due to the limited spectrum resources, heterogeneous communication systems often operate in the same frequency band. This is the case with widely used the Internet of Things (IoT) [1], [2] networks, based on ZigBee protocol [3], [4], and WiFi networks, both operating in 2.4 GHz frequency band, as shown inf Fig. 1 [5], and interfering with each other. The carrier sensing technology is a part of both standard, and it should provide shared access without interference. However, since ZigBee has much lower transmitting power than WiFi [6]–[8], WiFi devices are not able to detect ZigBee deviecs and the IoT systems suffer from a severe packet loss, making sensor data unreliable. Therefore, in this paper we give design directions for an IoT application, with the respect to the reliability [9], [10], based on the sensor reading data.

The main source of the unreliable sensor data in IoT networks is the interference, the most often with WiFi networks. Thus, the IoT networks should be designed with the reliability in mind. There are proposals that decrease the packet loss in ZigBee networks, based on the modification of ZigBee [11]–[15] or both ZigBee and WiFi [16]. However, these solutions require access to the physical level of ZigBee and WiFi nodes in a network, which is often not available. A methodology to identify problems in an IoT network and to help design it more reliable, is given in this paper.

The research leading to these results are performed within the project "SemantiC Coordination for intelligENT sensors (2CENTs)". This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 643943. The research was performed on SmartSantander testbed.

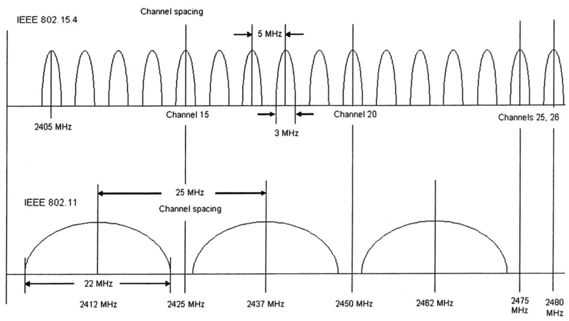

Figure 1. Comparison of IEEE 802.15.4 and 802.11 spectrum occupancy [5]

II. System Model

The analysis of an IoT network may be performed in several different ways. One approach is to create simulation, but it is not always possible due to numerous factors and effects that cannot be theoretically predicted and simulated. The other approach is to conduct an experiment on a deployed commercial network. Again, it is not often suitable because an experiment could interfere with a normal operation of the system. The most appropriate methodology is to run an experiment and acquire data on a massive online testbed. In this paper we will be using SmartSantander [17], an IoT online testbed located in Santander, Spain, which operates within Fiesta-IoT [18] testbed federation. It consists of several

Figure 2. Position and type of several sensors within SmartSantander testbed

thousands of sensors deployed throughout the city. The sensors are connected to a number of gateways using ZigBee network. Finally, gateways are connected, using mobile and WiFi network, to the datacenter. The position of the sensors in one part of the city is shown in Fig. 2. The experiment includes data captured during 37 days from 121 sensors. There were 10,565 measurements per sensor. The data acquired during the experiment is statistically analyzed using correlation analysis, i.e. Pearson correlation coefficient [19].

$$r = \frac{n\sum_{i=1}^{n} x_i y_i - \sum_{i=1}^{n} x_i \sum_{i=1}^{n} y_i}{\sqrt{n\sum_{i=1}^{n} x_i^2 - \left(\sum_{i=1}^{n} x_i\right)^2}\sqrt{n\sum_{i=1}^{n} y_i^2 - \left(\sum_{i=1}^{n} y_i\right)^2}} \quad (1)$$

where x_i and y_i are i-th members of the datasets whose correlation coefficient is needed, and n is the number of samples in each dataset.

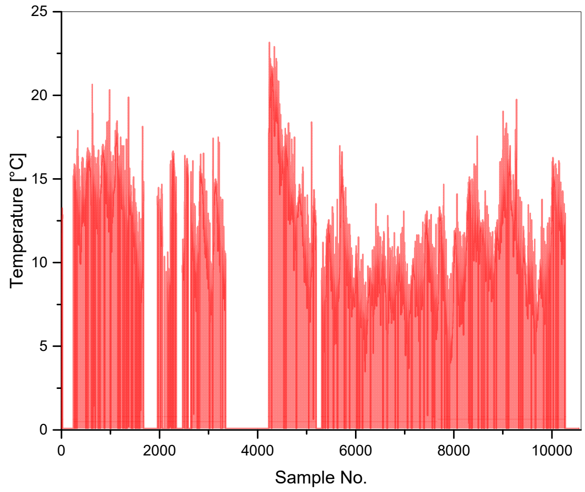

Figure 4. The output of one temperature sensor

The analysis of the sensor's data will give insight into the system operation and will provide the design directions.

III. Results and Discussion

The acquired sensors data analysis is presented in the following figures. Figs. 3 and 4 show the time plot of the data from two different types of the sensors. As can be seen, there are some data voids at some points of time. These missing data are the result of the packet loss due to the interference. This conclusion is confirmed also in the next figures. Figs. 5 and 6 illustrate the Pearson correlation coefficient for the presence or absence of data between all pairs of sensors in the considered part of the testbed, for different distance range. Fig. 5 shows the correlation coefficient between all considered sensors, and Fig. 6 depicts the correlation coefficient for pairs of sensors which are up to 100 meters away from each other. It can be seen that the correlation is generally higher for lower distance, which confirms that the data voids are a consequence of the same WiFi interference at the sensors close to each other. There are some pairs of sensors having low correlation and low distance, as well as relatively high correlation and high distance. It is a result of different operating channels and the presence/absence of the obstacles between the sensors.

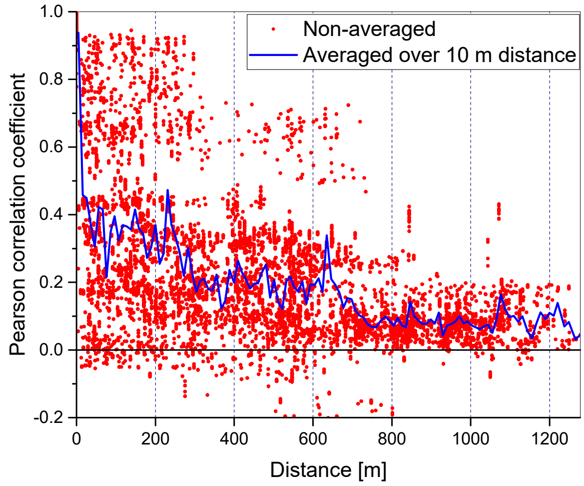

Figure 5. Pearson correlation coefficient as a function of distance between sensors 0 – 1300 m

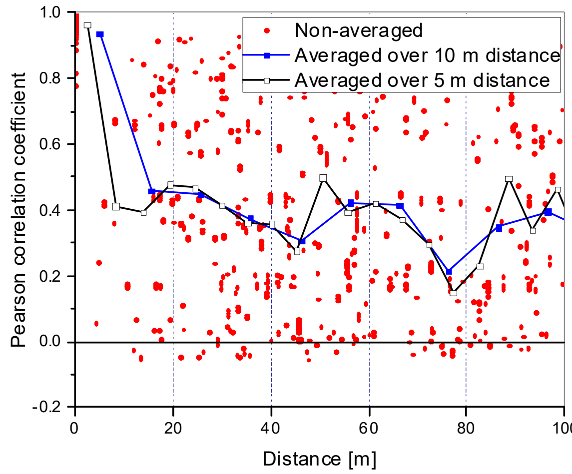

Figure 6. Pearson correlation coefficient as a function of distance between sensors 0 – 100 m

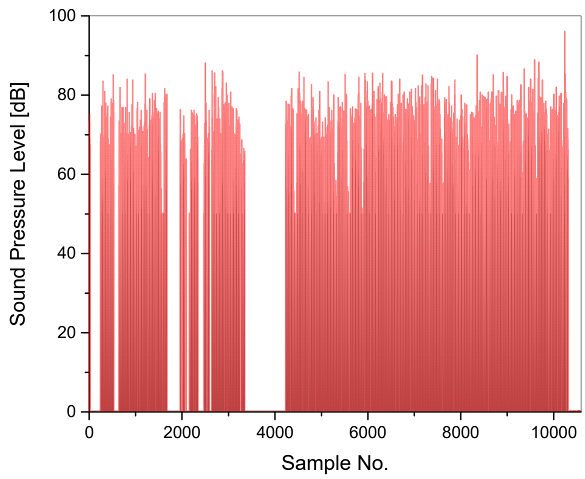

Figure 3. The output of one soud pressure level sensor

In order to avoid the loss of data caused by the interference, some kind of coordinated spectrum access between ZigBee and WiFi should be used. Based on the analysis of the time moments when the data form sensors are missing, it is possible to predict the next moment of the missing data, by employing, for example, a neural network. However, during the experiment, there were not enough data to train the neural network, so it could not be used for the prediction either. But, over the time the amount of data will increase and ti would be achievable to predict the interference and therefore avoid it by proactively changing the operating channel of the ZigBee device being interfered.

IV. Conclusioin

This paper considers the reliability of an IoT network and explores the possibility to incresease the reliability by using data mining and analysis. Namely, IoT networks based on ZigBee standard operate in the same 2.4 GHz frequency band as WiFi networks, which causes interference between them. The interference causes problems in the operation of IoT network and leads to the loss of data from wireless sensors. By analysing the patterns of the previous data loss events, the paper suggests the applicaton of the neural network to predict some future data loss and prevent it by changing the ZigBee device operating frequency in advance.

References

[1] M. R. Palattella *et al.*, “Internet of Things in the 5G Era: Enablers, Architecture, and Business Models,” *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 510–527, 2016.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[3] T. Kumar and P. B. Mane, “ZigBee topology: A survey,” in *2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, 2016, pp. 164–166.

[4] N. V. R. Kumar, C. Bhuvana, and S. Anushya, “Comparison of ZigBee and Bluetooth wireless technologies-survey,” in *2017 International Conference on Information Communication and Embedded Systems (ICICES)*, 2017, pp. 1–4.

[5] Crossbow Inc., “Avoiding RF Interference Between WiFi and Zigbee.” [Online]. Available: https://www.mobiusconsulting.com/papers/ZigBeeandWiFiInterference.pdf.

[6] S. Pollin, I. Tan, B. Hodge, C. Chun, and A. Bahai, “Harmful Coexistence Between 802.15.4 and 802.11: A Measurement-based Study,” in *2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008)*, 2008, pp. 1–6.

[7] J. Huang, G. Xing, G. Zhou, and R. Zhou, “Beyond co-existence: Exploiting WiFi white space for Zigbee performance assurance,” in *The 18th IEEE International Conference on Network Protocols*, 2010, pp. 305–314.

[8] C.-J. M. Liang, N. B. Priyantha, J. Liu, and A. Terzis, “Surviving Wi-fi Interference in Low Power ZigBee Networks,” in *Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems*, 2010, pp. 309–322.

[9] D. Crowe and A. Feinberg, *Design for reliability*, vol. 11. CRC press, 2001.

[10] C. Geiger and G. Sarakakis, “Data driven design for reliability,” in *2016 Annual Reliability and Maintainability Symposium (RAMS)*, 2016, pp. 1–6.

[11] M. S. Kang, J. W. Chong, H. Hyun, S. M. Kim, B. H. Jung, and D. K. Sung, “Adaptive Interference-Aware Multi-Channel Clustering Algorithm in a ZigBee Network in the Presence of WLAN Interference,” in *2007 2nd International Symposium on Wireless Pervasive Computing*, 2007.

[12] S. Pollin *et al.*, “Distributed cognitive coexistence of 802.15.4 with 802.11,” in *2006 1st International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, 2006, pp. 1–5.

[13] R. Musaloiu-E. and A. Terzis, “Minimising the Effect of WiFi Interference in 802.15.4 Wireless Sensor Networks,” *Int. J. Sen. Netw.*, vol. 3, no. 1, pp. 43–54, 2008.

[14] L. Tytgat, O. Yaron, S. Pollin, I. Moerman, and P. Demeester, “Analysis and Experimental Verification of Frequency-Based Interference Avoidance Mechanisms in IEEE 802.15.4,” *IEEE/ACM Trans. Netw.*, vol. 23, no. 2, pp. 369–382, Apr. 2015.

[15] J. W. Chong, C. H. Cho, H. Y. Hwang, and D. K. Sung, “An Adaptive WLAN Interference Mitigation Scheme for ZigBee Sensor Networks,” *Int. J. Distrib. Sen. Netw.*, vol. 2015, p. 159:159--159:159, 2015.

[16] S. Nishikori, K. Kinoshita, Y. Tanigawa, H. Tode, and T. Watanabe, “A cooperative channel control method of ZigBee and WiFi for IoT services,” in *2017 14th IEEE Annual Consumer Communications Networking Conference (CCNC)*, 2017, pp. 1–6.

[17] “SmartSantander.” [Online]. Available: http://www.smartsantander.eu/. [Accessed: 01-Jan-2018].

[18] “Federated Interoperable Semantic IoT Testbeds and Applications (FIESTA-IoT).” [Online]. Available: http://fiesta-iot.eu/.

[19] A. K. Sharma, *Text Book Of Correlations And Regression*. New Delhi: Discovery Publishing House, 2005.