TELKOMNIKA Telecommunication, Computing, Electronics and Control
Vol. 18, No. 4, August 2020, pp. 1762~1770
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v18i4.14879

Machine learning based lightweight interference mitigation scheme for wireless sensor network

Ali Suzain, Rozeha A. Rashid, M. A. Sarijari, A. Shahidan Abdullah, Omar A. Aziz
School of Electrical Engineering, Faculty of Engineering, Universiti Teknologi Malaysia, Malaysia

Article Info

Article history:

Received Aug 9, 2019
Revised Mar 31, 2020
Accepted Apr 12, 2020

Keywords:

Interference
Machine learning
RSSI

ABSTRACT

The interference issue is most vibrant on low-powered networks like wireless sensor network (WSN). In some cases, the heavy interference on WSN from different technologies and devices result in life threatening situations. In this paper, a machine learning (ML) based lightweight interference mitigation scheme for WSN is proposed. The scheme detects and identifies heterogeneous interference like Wifi, bluetooth and microwave oven using a lightweight feature extraction method and ML lightweight decision tree. It also provides WSN an adaptive interference mitigation solution by helping to choose packet scheduling, Acknowledgement (ACK)-retransmission or channel switching as the best countermeasure. The scheme is simulated with test data to evaluate the accuracy performance and the memory consumption. Evaluation of the proposed scheme's memory profile shows a 14% memory saving compared to a fast fourier transform (FFT) based periodicity estimation technique and 3% less memory compared to logistic regression-based ML model, hence proving the scheme is lightweight. The validation test shows the scheme has a high accuracy at 95.24%. It shows a precision of 100% in detecting WiFi and microwave oven interference while a 90% precision in detecting bluetooth interference.

Corresponding Author:

Rozeha A. Rashid,
School of Electrical Engineering, Faculty of Engineering,
Universiti Teknologi Malaysia,
81310 UTM Johor Bahru, Johor, Malaysia.
Email: rozeha@utm.my

1. INTRODUCTION

Wireless sensor network (WSN) is a low-powered, small and embedded network deployed in industrial, scientific and medical (ISM) band [1, 2]. In future, WSN will have a rapid usage expansion due to Internet of Things (IoT). IoT demand for low powered networks is increasing and WSN is the most suitable candidate to fulfil the aim of connecting large number of sensors. WSN deploying IEEE802.15.4 (2003) standard operates in three unlicensed ISM bands. It provides 27 channels which include 1 at 868 MHz, 10 at 915 MHz and 16 at 2.4 GHz. The most commonly used one is 2.4 GHz band. The band is used by various technologies and devices including WiFi, Bluetooth and microwave oven [3-5].

Recent advancement in wireless communication have increased the number of devices operating in 2.4 GHz ISM band. This leads to congestion of the unlicensed band and different communication challenges such as co-existence and interference. Traditional methods like spectrum fragmentation and carrier sensing to solve interference problem in ISM band do not work anymore as these solutions were designed for low spatial density and presence of only a few radio technologies [6]. So, interference and coexistence are becoming major problems in the ISM band, especially for WSN. The increase in the number of various wireless technologies operating in ISM band leads to collision and congestion on the shared channels. This will cause critical repercussions in the communication of WSNs. Hence, there is a need for agile methods that assess the channel conditions and apply actions to maximize communication success. The interference from various sources changes quickly due to reasons like mobility and changes in configuration. Therefore, the interference mitigating methods need to be adaptive and self-aware to the changes in the interference. Moreover, due to WSN being a small, embedded, low-power network, interference mitigating methods need to be lightweight.

2. RELATED WORKS

The topic of interference identification and mitigation are becoming popular in recent years in the field of WSN due to overcrowding of ISM band and increasing use of WSN especially as a sub platform for IoT applications. Different interference classification and mitigation schemes are found in the literatures. Most of them focused only on interference classification. Few schemes are found that identify the interference and suggest mitigation strategy. Research works in [6-8] propose algorithms to identify type of interference. Studies in [7, 8] decide on features of interfering signal by evaluating RSSI values. Then, with a fixed set of conditions, the signal is classified as bluetooth, WiFi or microwave interference. In both cases, the classification accuracy is below 90%. A method to calculate the percentage of the interference in the wireless link and distance of the interfering source is provided in [9]. Interference identification methods through supervised learning and machine learning are proposed in [10-12]. Each of these works lack an adaptive method that can mitigate the effect of the interference. Work in [13] proposes a scheme that identifies mitigation strategy with the help of decision tree but does not identify the type of interference. Authors in [14] propose Specksense, which identifies WiFi, periodic and non-periodic traffic. The scheme also helps to mitigate interference by channel black listing. However, the scheme is limited to the type of identified interference only.

Majority of these works found in the literature use energy detection (ED) approach to detect and identify the interference type. ED approach uses received signal strength indicator (RSSI) value to evaluate the interference. Few use packet probing and link quality indicator (LQI). Motivated from these works, this paper proposes a lightweight interference mitigation scheme to reduce the effect of interference on WSN. The scheme is made self-aware by using a lightweight feature extraction method and a ML model that can extract features of interfered signal and identify the type of interference. In order to make the scheme adaptive, a look-up table that chooses packet scheduling, ACK-retransmission and channel switching as countermeasures to mitigate the detected interference is deployed.

3. BACKGROUND AND TECHNOLOGIES IN ISM BAND

The wireless medium is vulnerable to interference from various sources due to its broadcast nature. These interferences degrade the communication and sometimes even block it by making it difficult for receiver to decode the received signal. The interference can be from a similar technology, different technology operating in the same band or noise. Many research have been carried out and various mechanisms have been proposed to overcome the effect of interference within the same technology. All these mechanism lack the ability to reduce or manage interference among different technologies as they have been designed without considering the issue of coexistence. Moreover, it is proven to be difficult to have interoperable interference mitigation among various wireless technologies as they lack the feasibility of communication among themselves. Therefore, interference mitigation from different technologies or cross technology interference (CTI) mitigation is becoming one of the demanding topics in communication [14]. The unlicensed ISM band is the most crowded band with the largest number of different technologies operating in it. This make ISM band as the most vulnerable band to CTI.

3.1. ISM band technologies

Microwave oven heats food by changing absorbed microwave at 2.4 GHz frequency to atomic vibration. When operating at this frequency, some amount of the waves are leaked to the surrounding. This results in interference to other devices that utilize this frequency band. The average output power of microwave oven is 800 Watt and emitted wave has a bandwidth of approximately 5 MHz. Therefore, if a WSN operates at a frequency close to the center frequency of 2.4 GHz, it will experience an enlarged packet drop due to interference from microwave leakage. However, the interference from microwave would last only for the heating period, which typically range from 30 minutes to 1 hour [8].

IEEE 802.15.4 standard uses offset quadrature phase-shift keying (O-QPSK) modulation with a half pulse shaping. The transmission occurs in one of the 27 non overlapping channels. 16 of them with 2 MHz bandwidth and 5 MHz channel spacing are in 2.5 GHz band, while the remaining 11 channels are in sub-GHz band. The standard has many different MAC layer protocols defined over various version. The simplest one uses the carrier sense multiple access with clear channel (CSMA/CA) communication. At the beginning of any transmission, nodes will make sure the channel is idle by using clear channel assessment (CCA). If the channel is found to be busy, it defers the communication for a certain period of time [15-19].

IEEE802.15.1, commonly known as Bluetooth, is a wireless specification for wireless personal area network (WPAN). It is being used by variety of devices for short range communication. Some example include data transferring between mobiles, laptops and tablets [20]. Bluetooth operates in 2.4 GHz frequency band with 76 distinct channels, each 1MHz wide. It uses frequency hopping spread spectrum (FHSS) which causes a change of the center frequency of the signal at a rate of 1600Hz. This helps it to avoid interference but forces it to occupy 76 MHz of the 2.4 GHz band over majority of the time. FHSS is later improved to an upgraded version known as adaptive frequency hopping (AFH) algorithm which allows bluetooth devices to categorize occupied channels by WSN as “bad” channels and will be ignored during channel selection. However, this is unlikely to happen in most of the cases as the WSN signals are low powered in nature.

In IEEE802.11 standard, the carrier sense multiple access (CSMA) and CSMA/CA algorithm are used to tacle coexistence interference [20]. However, a study by Huang et al. [21] shows that the due to the bursty nature of the WiFi, CSMA scheme is not able to completely use the WiFi white spaces (unused spaces between Wi Fi frames). Moreover, WiFi transmitters are unable to identify the WSN signals as the clear channel assessment (CCA) in CSMA only senses the carrier of IEEE802.11 signals. Hence, it depends on the CCA mode being used [22, 23].

4. SYSTEM DESIGN

The scheme proposed in this paper is based on four main modules, namely, interference estimation, feature extraction, ML classification and look-up table. Figure 1 presents the overall architecture of the scheme with these modules. The scheme takes sampled RSSI traces from PHY layer and stores them for processing. The first process involved is interference estimation carried out by the interference estimation module. If this module detects presence of any interference, feature extraction is executed on the trace using lightweight feature extraction module. If no interference is detected, the message is passed to the look-up table directly. The extracted feature vector of the RSSI trace is the input to the ML classification model [24] which classifies the interfering signal into one of the classes, Bluetooth, WiFi or microwave oven. The classification output which is the type of interference, is passed to the look-up table in order to carry out decision on the countermeasure to be used for detected interference [25]. The mitigation countermeasure information is passed to MAC layer to take the action. The proceeding sections describe in detail the designing process by explaining the design of each module in depth.

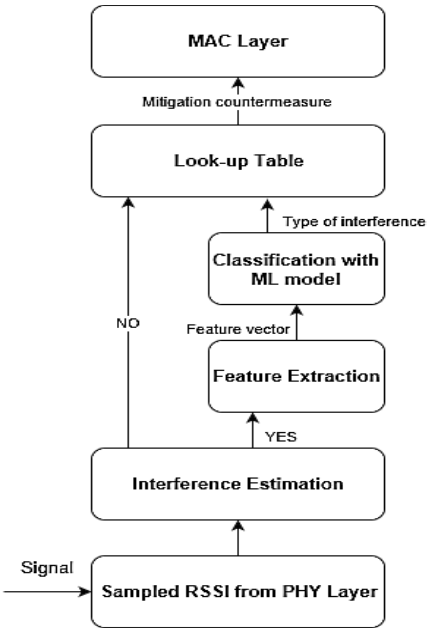

Figure 1. Overall architecture of the scheme

4.1. Signal sampling

The developed scheme uses ED approach to extract features and identify the type of interference. The ED value is commonly known as RSSI value and roughly represents the power of received signal at the receiver radio. In developing the proposed scheme, RSSI values from experiments carried out in [13] are used. These readings are already sampled RSSI values for different interfering technologies in ISM band namely, WiFi, Bluetooth and microwave oven obtained every 16 µs in a controlled experiment. Figure 2 depicts the controlled experimental setup used in [13] to measure the RSSI for different interfering technologies.

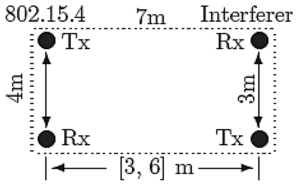

Figure 2. Controlled experimental setup used in [13]

4.2. Interference estimation

Interference estimation module is concerned with detection of any interference in the sampled RSSI trace received from PHY layer. The interference estimation module reads serially the '1s' of the RSSI trace and performs interference estimation using a threshold. First, the RSSI values are converted to dBm by adding an offset of -45 to each serially read RSSI value. Next step involves finding the interference threshold. This is done by finding the power level of the received signal without interference. When the signal is exposed to interference, the power level increases as the interference is additive. Analysis of RSSI trace for different interference source shows that the power level of the received signal without interference is the most repeated RSSI value. Therefore, this value is taken to be the threshold.

The trace plots also show there are some values with variation of less than 1 dBm from threshold. These values are not subject to interference from the interfering source but the variation is due to the environmental conditions like multipath propagation. With this information, the series are converted to a binary trace in the following step. Any value having a variation less than 1dBm from the threshold or any value below the threshold is converted to 0. The rest are converted to 1. Therefore, in the resulting binary trace, 1 represents samples subject to interference while 0 represents samples without interference. In the last stage of the module, active ratio of the binary trace is calculated using (1). If the active ratio is greater than 0, the module estimates that the received signal is exposed to interference. If the active ratio is equal to 0, it decides that the signal is not subject to any interference.

$$active\ ratio = \frac{number\ of\ samples\ converted\ as\ 1}{total\ number\ of\ samples} \tag{1}$$

4.3. Feature extraction

This module aims at finding the temporal features of the generated binary signal from interference estimation module. The features extracted in this project are listed in the following.

- Maximum channel usage duration
- Maximum channel clear duration
- Channel usage ratio
- Periodicity which describes a unique transmission pattern of a wireless signal

Two models are created to extract these features and the one with a lesser memory consumption is selected to be used in the final scheme. In both models, the same methods are used to find the first three features but different methods are used to find the last feature, periodicity. Model 1 uses Fast Fourier Transform (FFT) to estimate the periodicity of the binary signal while the proposed lightweight method is used to estimate the periodicity in model 2. The methods for the feature extraction are further described in the following:

- Maximum channel usage duration: This represents the maximum duration for which the signal is exposed to external interference. It is found by calculating the maximum duration for which the binary signal continues with the value 1.
- Maximum channel clear duration: This represents the maximum duration for which the signal is not exposed to external interference. It is found by calculating the maximum duration for which the binary signal continues with the value 0.

- Channel usage ratio: This is the same as the active ratio calculated in interference estimation module. So, the value for active ratio is used instead of calculating it again in order to save the computation and memory.
- Proposed lightweight method to estimate periodicity: This method estimates the periodicity by determining the number of repeated duty cycles in the binary signal. The binary plots for microwave oven interference shows that the duty cycle consists of regular time interval of busy channel and idle channel. Analysis of the binary traces for WiFi shows that it has regularly transmitted beacons. Even if there is a data traffic, the transmitted data is usually around the beacons. So, during and around a beacon transmission, the channel is subject to interference, while the duration between beacons, the channel is clear of the interference. Bluetooth traces show regularly transmitted spikes. During and around these spikes, the channel is subjected to interference. Other than that, it is free of interference. Therefore, the duty cycle for each interfering technology consists of channel clear duration and channel busy duration. Hence, (2) is used to calculate the number of repeated duty cycles or periodicity in binary signal.

$$Periodicity = \frac{total\ duration\ of\ the\ binary\ signal}{channel\ busy\ time + channel\ ideal\ time} \tag{2}$$

The default beacon interval for WiFi is 102.4ms [7]. The sum of maximum channel clear duration and maximum channel busy duration (duty cycle duration) for WiFi should not exceed this value. The Bluetooth and microwave oven traces show their duty cycle durations are always less than this value. Under heavy data traffic, the duty cycle for WiFi exceeds this value. Therefore, in order to keep the duty cycle always within this limit, the following condition is used while calculating the periodicity. If the sum of maximum channel busy time and maximum channel clear time > 102.4ms, periodicity is given by (3):

$$Periodicity = \frac{total\ duration\ of\ the\ binary\ signal}{102.4\ ms} \tag{3}$$

From computation, the proposed lightweight method is found to be more accurate in estimating periodicity. Moreover, the memory profile of the method shows it consumes less memory compared to FFT. Hence, the proposed method is proven to be lightweight.

4.4. Machine learning model-decision tree

The scheme proposed in this paper needs to classify the type of interfering signal for an extracted feature set. Therefore, a supervised learning model is needed. The first requirement to develop a supervised machine learning model is to have an appropriate dataset. In order to generate the required dataset, feature extraction is carried out using the developed feature extraction method on 70 different traces. Once the dataset is generated, the ML model development procedure is carried out. Firstly, the dataset is randomly split into train data and test data. 70% of the dataset is split as train data and 30% into test data. The train data is used for developing and training the model while test data is used for validating the developed model. Two models, namely, decision tree model and logistic regression model are developed separately. For the final scheme, the model with the least memory consumption and high accuracy is used. In both models, the four numeric attributes of the dataset (periodicity, busy time, channel utilization and idle time) will be used as inputs to the models. The decision tree is built using CART algorithm with attribute selection measures (ASM) as gini index. Figure 3 presents the generated trained decision tree. From simulation, it is found that the decision tree is more accurate and lightweight compared to logistic regression model. Hence, the decision tree is considered to be the ML model in the final scheme.

4.5. Lookup table

The look-up table takes ML classification model output as its input and chooses the most appropriate countermeasure for the type of input interference. The table is created from observations stated in [7, 8] on different countermeasures for interference in WSN. These observations state that each interfering technology shapes the interfered channel in a particular way. So different countermeasures will work for different types of interference. For instance, microwave oven utilizes the channel heavily with a slow but steady and timely transmission. The transmission has regular on-off periods. So, the transmission or interference periods can be avoided by sending the packets in a regularly scheduled manner [7] or in other words, by using packet schedule transmission. Hence, if the input to the look-up table is microwave oven interference, it will choose packet scheduling as the countermeasure.

On the other hand, WiFi utilizes the channel very deeply for a long period of time with heavy data traffic. Unlike microwave oven transmission, it does not have a regular on-off transmission pattern. So, the best method to avoid WiFi interference would be to change the current transmitting channel [8]. Therefore, the look-up table decides channel switching as the most appropriate countermeasure when the type of input interference is WiFi. Unlike WiFi and microwave oven, bluetooth has the least interference effect on WSN signal. In addition, bluetooth interference occurs randomly as it uses adaptive frequency hopping mechanism to transmit data on channels. So, the best way to avoid bluetooth interference would be to remain in the channel and retransmit if a packet collision occurs [7]. The packet collision can be detected by using ACKs. Hence, if the detected interference is Bluetooth, the look-up table will choose retransmission with ACK as the countermeasure. Table 1 illustrates the look-up table used in the developed scheme.

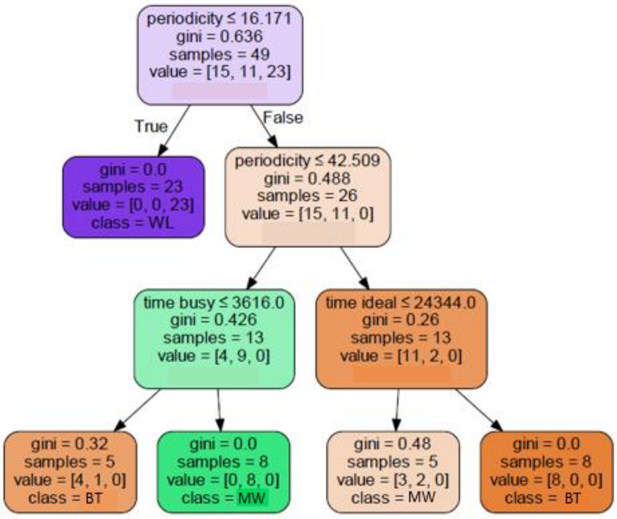

Figure 3. Trained decision tree

Table 1. Look-up table

Interference type	Mitigation strategy
WiFi	Channel switching
Microwave oven	Packet scheduling
Bluetooth	ACK - retransmission

5. SCHEME EVALUATION

In addition to the proposed scheme, two more schemes were constructed. One of them was developed with FFT feature extraction method and decision tree classification model. The other one uses proposed lightweight feature extraction method, but logistic regression as the ML model. In order to prove the proposed scheme is lightweight, an analysis of memory consumption is considered. The analysis is done first by profiling the running memory for the developed scheme and other constructed schemes. In addition to this memory profiling, different feature extraction methods used are also compared to search for the most lightweight one.

Figure 4 shows memory profiles for feature extraction methods used to develop the scheme. The red line plot in the graph shows memory profile for feature extraction method using FFT. The green line shows the profile for the proposed light weight method to extract features. From the figure, it can be observed that the FFT method has a running memory of 68MiB while the proposed lightweight method consumes 37 MiB of memory. The 31 MiB reduction of memory consumption shows that the proposed method is more lightweight than the FFT method. The complexity of FFT makes it more memory intensive and slow compared to the proposed lightweight method.

Figure 5 shows memory profiles for different schemes created. It can be observed that the developed scheme has a memory of 75.9 MiB, the scheme with logistic regression has a memory of 78.3 MiB and the scheme with FFT has 88.2 MiB memory. So, the developed scheme (in red colour) has 14% memory improvement compared to the scheme with FFT as feature extraction method. This improvement is due to the lesser memory consumption of the proposed lightweight method used for feature extraction in the developed scheme. As mentioned in the previous section, FFT uses intensive calculations and is more complex compared to the proposed lightweight method.

From Figure 5, the comparison of memory used between the scheme with logistic regression as ML model and the proposed scheme illustrates that the proposed scheme consumes 3% less memory. This shows that decision tree model used in the proposed scheme is more lightweight than the logistic regression model. Logistic regression model involves finding logits, probability and cross-entropy function for each input attribute which makes it computationally intensive. Hence, it consumes more memory than the simple decision tree. The decision tree has 1 root node and 3 internal nodes, so, it is fairly simple and uses less memory to make classification.

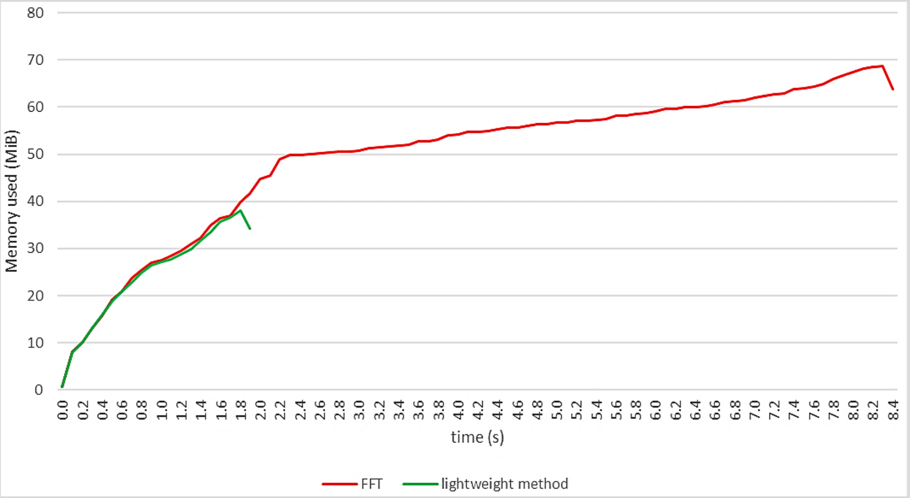

Figure 4. Memory profiles for feature extraction methods

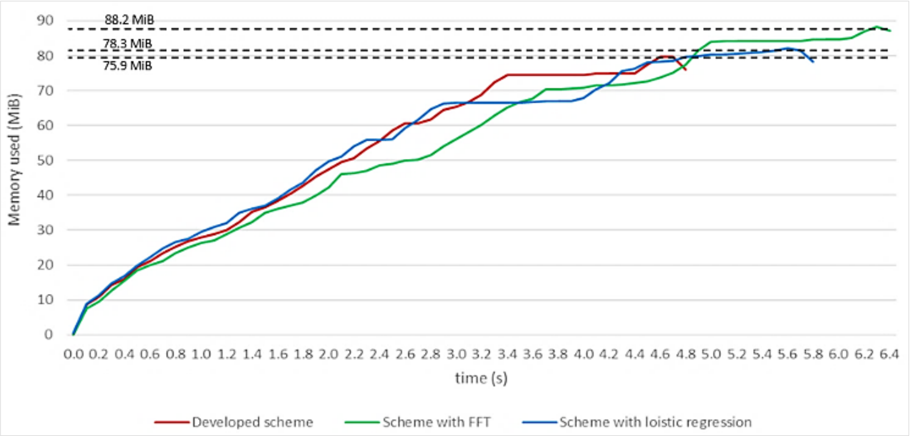

Figure 5. Memory profile for different schemes created

In order to evaluate the performance of the proposed scheme, its validation and precision accuracy is compared with schemes in [7, 8] and [13]. Table 2 depicts this comparison. In [8] and [13], the scheme precision accuracy for different classes were not given so the precision is only compared with scheme in [7]. As can be seen, the proposed scheme has a precision of 100% in detecting WiFi and Microwave oven interference while a 90% precision in detecting Bluetooth interference. The scheme in [2] has a precision of 99.05% in detecting WiFi, 100% in detecting Microwave oven interference and a 90% precision in detecting Bluetooth interference. This shows that the precisions are almost similar for both schemes except for Bluetooth. In both schemes, Bluetooth has less precision compared to other classes. Bluetooth uses adaptive frequency hopping (AFH) and changes to unused or less used channels when many collisions are detected on a channel. Therefore, a detection of Bluetooth is more challenging compared to microwave oven which emits radiation in a regular on-off pattern while WiFi periodicity is always less than around 16μs. So, they are easier to identify.

Table 2. Performance comparison of the developed scheme

Scheme	Bluetooth Precision	WiFi Precision	Microwave oven Precision	Validation accuracy
Proposed scheme	90%	100%	100%	95.24%
[7]	97.41%	99.05%	100%	96.46%
[13]	-	-	-	92.9%
[8]	-	-	-	70%

The scheme in [8] has a low validation accuracy of 70% while scheme in [13] has 92.9% accuracy. Scheme in [8] is only an interference classification scheme. It is not accompanied with any mitigation strategy. The scheme in [13] is a mitigation scheme which chooses different countermeasures for detected interference. As can be seen from the table, the developed scheme has 95.24% accuracy which is high compared to other two schemes. Scheme in [7] has a validation accuracy of 96.46%, which is higher than the proposed scheme. However, the scheme in [7] uses fixed set of rules to build decision tree for classification. The proposed scheme uses a trained decision tree from a dataset to make the classification. This means the developed scheme can be trained for different datasets. It can be made adaptive to changes in the wireless environment. This cannot be possible with scheme in [7] as it uses fixed decision tree. So, the scheme proposed is more adaptive than the one in [7]. This guarantees the proposed scheme to deliver a good performance accuracy irrespective of the wireless environment.

6. CONCLUSION

In this paper, a ML based lightweight interference migration scheme for WSN is presented. The scheme uses a lightweight method to estimate the interfering signal features and a lightweight decision tree to identify the type of interference. This information is fed to a look-up table to decide the best mitigation strategy for the detected interference. Evaluation of the proposed scheme's memory profile shows a 14% memory saving compared to a scheme with FFT as periodicity estimation technique and 3% less memory when compared to logistic regression as ML model. This proves the developed scheme is lightweight. The validation test using test data shows the proposed scheme is very accurate with an accuracy of 95.24%. Due to the use of trained decision tree, the proposed scheme is able to deliver a good performance accuracy irrespective of the wireless environment.

ACKNOWLEDGEMENT

The authors wish to express their gratitude to Ministry of Higher Education (MOHE), Malaysia and Research Management Center (RMC), Universiti Teknologi Malaysia for the financial support of this project under FRGS/1/2019/TK04/UTM/02/44 grant no: RJ130000.7851.5F174 titled Machine Learning based Interference Mitigation Scheme in Wireless Sensor Network for Internet-of-Things (IoT) Applications.

REFERENCES

[1] F. Yao, S. H. Yang, W. Zheng, "Mitigating interference caused by IEEE 802.11 b in the IEEE 802.15. 4 WSN within the environment of smart house," *2010 IEEE International Conference on Systems, Man and Cybernetics*, pp. 2800-2807, 2010.

[2] N. H. Mahalin, H. S. Sharifah, S. K. S. Yusof, N. Fisal, and R. A. Rashid, "RSSI measurements for enabling IEEE802.15.4 coexistence with IEEE802.11b/g.," *TENCON 2009-2009 IEEE Region 10 Conference,* 2009.

[3] M. A. Sarijari, Anthony Lo, M. S. Abdullah, S. H. De Groot, I. G. M. M. Niemegeers, Rozeha A. Rashid, "Coexistence of Heterogeneous and Homogeneous Technologies in Smart Grid Home Area Network," *2013 International Conference on Parallel and Distributed Systems*, Seoul, South Korea, 15-18 Dec 2013.

[4] Rozeha A. Rashid, M. Rezan Resat, M. A. Sarijari, N. Mahalin, M. S. Abdullah, A. H. F. A. Hamid, "Performance Investigations on Frequency Agile Enabled TelosB Testbed in Home Area Network," 2014 *IEEE 2nd International Symposium on Telecommunication Technologies (ISTT),* Langkawi, Malaysia, 24-26 November, 2014.

[5] A. H. F. A. Hamid, Rozeha A. Rashid, Lye Kong Weng, N. Fisal, "IEEE802.11 Interference Management for Wirelss Sensor Node," *International Conference on Power, Energy, and Communication Systems (IPECS),* Perlis, Malaysia, 24-25 August, 2015.

[6] K. R. Chowdhury and I. F. Akyildiz, "Interferer classification, channel selection and transmission adaptation for wireless sensor networks," *2009 IEEE International Conference on Communications*, pp. 1-5, Jun 2009.

[7] S. Zacharias, T. Newe, S. O'Keeffe, and E. Lewis, "A lightweight classification algorithm for external sources of interference in IEEE 802.15.4-based wireless sesor networks," *International Journal of Distributed Sensor Network*, vol. 10, no. 9, pp. 265-286, 2014.

[8] Meng Hou, Fengyuang Ren, Chuang Lin, Mao Miao, "HEIR: Heterogeneous Interference Recognition for Wireless Sensor Network," *Proceedings of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, Sydney, NSW, Australia, 09 October 2014.

[9] S. Diaz, D. Mendez and R. Kraemer, "ICI-Interference characterization and identification for WSN," *2017 Wireless Telecommunications Symposium (WTS),* Chicago, IL, pp. 1-7, 2017.

[10] Simone Grimaldi, Aamir Mahmood, "Real-time Interference Identification via Supervised Learning: A Coexistence Framework for Massive IoT Networks," arXiv preprint arXiv:1809.10085, Sept 2018.

[11] S. Grimaldi, A. Mahmood, and M. Gidlund, "An SVM-based method for classification of external interference in industrial wireless sensor and actuator networks," *Journal of Sensor and Actuator Networks*, vol. 6, no. 2, 2017.

[12] M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1-23, May 2014.

[13] Anwar Hithnawi, Hossein Shafagh, "TIIM: Technology-Independent Interference Mitigation for Low-power Wireless Networks," *Proceedings of the 14th International Conference on Information Processing in Sensor Networks*, 2015.

[14] Iyer V., Hermans F., Voigt T., "Detecting and Avoiding Multiple Sources of Interference in the 2.4 GHz Spectrum," *European Conference on Wireless Sensor Networks*, vol. 8965, pp. 35-51, Springer, 2015.

[15] Anwar Hithnawi, "Low-power Wireless Systems Coexistence," Thesis, Doctor of Science, ETH Zurich, 2016.

[16] S. Zacharias, "Effects, classification and mitigation of external interference in IEEE 802.15.4 based sensor networks," Thesis, Doctor oF Science, University of Limerick, 2014.

[17] W. Yuan, J. P. M. G. Linnartz, and I. G. M. M. Niemegeers, *"*Adaptive CCA for IEEE802.15. 4 wireless sensor networks to mitigate interference," *Proceedings of the 2010 IEEE Wireless Communications and Networking Conference (WCNC),* Sydney, New South Wales, pp. 1-5, 18-21 April 2010.

[18] A. King and U. Roedig, "Differentiating clear channel assessment using transmit power variation," *ACM Transaction on Sensor Network*, vol. 14, no. 2, pp. 1-15, May 2018.

[19] P. Du and G. Roussos, "Adaptive time slotted channel hopping for wireless sensor networks," *2012 4th Computer Science and Electronic Engineering Conference (CEEC)*, pp. 29-34, 2012.

[20] N. Azmi, L. M. Kamarudin, "Interference Issues and Mitigation Method in WSN 2.4GHz ISM Band: A Survey," *2014 2nd International Conference on Electronic Design (ICED)*, 2014.

[21] J. Huang, G. Xing, G. Zhou, R. Zhou, "Beyond co-existence: Exploiting WiFi white space for Zigbee performance assurance," *18th IEEE Int. Conf. Network Protocol*, pp. 305-314, Oct 2010.

[22] Liang, C. J, Priyantha, "Surviving wifi interference in low powered zigbee network," *Proceeding of the 18th ACM conference on Embedded Networked Sensor Systems*, pp 309-322, Nov 2015. https://doi.org/10.1145/ 1869983.1870014.

[23] J. W. Branch, C. Giannella, B. Szymanski, R. Wolff, and H. Kargupta, "In-network outlier detection in wireless sensor networks," *Knowledge and Information Systems,* vol. 34, no. 1, pp. 23-54, Jul. 2013.

[24] T. O. Ayodele, "Types of Machine Learning Algorithms," Portsmouth, U.K., *InTech*, February 2010.

[25] Hossein Fotouhi, Mário Alves, Marco Zuniga, Nouha Baccour, Claro Noda, Thiemo Voigt, Kay Romer, and Carlo Boano, "Radio Link Quality Estimation in Low-Power Wireless Networks," *Springer International Publishing,* Heidelberg, July 2013.