Transmission Control to Suppress Interference Between Periodic and Non-Periodic

Traffic in Wireless Coexistence Scenarios

Ryota Ikeuchi and Hiroyuki Yomo Graduate School of Engineering Science, Kansai University 3-3-35 Yamate-cho, Suita, Osaka, 564-8680 Japan e-mail: {k097114, yomo}@kansai-u.ac.jp

Abstract—In this paper, we consider a wireless coexistence scenario where multi-radio platforms are employed to simultaneously support periodic and non-periodic traffic. Considering a scenario where wireless terminals generating periodic traffic over one frequency band change their operating band to the other band after detecting long-term communication failures, we consider how to suppress mutual interference between periodic and non-periodic traffic over the shared channel. In this paper, we propose a transmission control alleviating negative impact of mutual interference by exploiting interface heterogeneity, traffic periodicity, and queue management. The proposed scheme realizes high packet delivery ratio of periodic traffic by suppressing transmissions of terminals with non-periodic traffic at the timing when periodic traffic is expected to be transmitted by their hidden terminals. With computer simulations and experiments, we investigate the practicality and effectiveness of the proposed scheme.

Keywords—Wireless Coexistence, Factory Automation, IEEE 802.11, IEEE 802.15.4, Internet of Things

I. INTRODUCTION

The proliferation of diverse wireless access technologies, such as LTE, WiFi, ZigBee, Bluetooth, etc., has been accelerated during the last decade to support heterogenous traffic with different requirements. Today, we have an option to simultaneously exploit these technologies with multi–radio platforms [1][2]: for instance, small, low–price IoT devices, which are equipped with multiple interfaces operating over different frequency bands, such as 2.4/5GHz and 920MHz, are commercially available [3].

In this paper, we exploit multi-radio platforms to enhance robustness of wireless networks in a highly noisy environment. A typical use-case is factory [4], where there are many metal objects blocking communication links between transmitters and receivers [5]. Furthermore, there can be noise emitted from industrial machines, as well as interference from many radio equipment around a factory. The resulting instability of communication channels causes temporal communication failure, which can last for a long period of time. If we employ wireless devices with a single interface operating over a specific frequency band in such an unstable environment, we cannot offer reliable transmissions of data: once blocking, noise or interference is generated over an operating frequency band, each device has no way to avoid them. The lack of reliability for data transmissions in a factory can result in serious incidents that could even cause human life to be in danger. Therefore, in our work, we focus on the usage of wireless devices equipped with multiple radio interfaces operating

at different frequency bands, called Flexible Terminal (FT). With FT, even if noise or interference is generated over one frequency band, its operating band can be changed to the other frequency band, which enables us to avoid communication failures due to noise and interference. More specifically, we employ radio standards operating at unlicensed frequency bands: IEEE 802.11 at 2.4 GHz and IEEE 802.15.4g at 920MHz since these standards are widely employed in many industrial fields [6].

Besides the heterogeneity of radio interface, the heterogeneity of communication traffic has become a common trend in current wireless networks. In addition to non-periodic (bursty) traffic generated by classical applications, such as Internet access and video/image transfer, more deterministic and periodic traffic has become a dominant pattern especially in a scenario with sensor devices deployed for monitoring purpose [7][8]. In general, small amount of data is generated by sensor devices, for which 920MHz radio supporting low data rate with large coverage is a favorable option. On the other hand, 2.4GHz commonly used by WiFi offers higher data rate with smaller coverage than 920MHz, which makes it suited for supporting Internet access and transfer of largesize image/video files. In this work, we employ FTs to simultaneously support periodic and non-periodic traffic. In a normal operation mode without any noise or interference, FTs with non-periodic traffic employ an interface operating at 2.4 GHz while FTs with periodic traffic use an interface operating at 920MHz. Then, we consider a scenario where noise or interference is generated by surrounding devices/machines over 920MHz, and each FT with periodic traffic changes its operating interface to that at 2.4GHz. In this case, there is mutual interference between FTs with periodic traffic and FTs with non-periodic traffic. In this work, we propose a transmission control, which suppresses mutual interference by exploiting interface heterogeneity, traffic periodicity, and queue management. In the proposed scheme, FTs with nonperiodic traffic detect possible hidden FTs with periodic traffic by using difference of propagation characteristics of different frequency bands. Then, FTs with non-periodic traffic predict the transmission timing of FTs with periodic traffic, and suppress their packet transmissions at the predicted timing with adaptive queue management. With computer simulations and experiments, we investigate the practicality and possible gain of the proposed scheme.

The rest of the paper is organized as follows. After describing the system model and problem definition in Section II, we

present our proposed transmission control in Section III. After showing and discussing some numerical results in Section IV, Section V concludes the paper with several future work.

II. SYSTEM MODEL AND PROBLEM DEFINITION

In this section, we first describe the system model considered in this paper, followed by the problem formulation.

A. System Model

In this work, we employ FTs with interfaces operating at 2.4GHz and 920MHz. In general, 920MHz signals have larger propagation distance than 2.4 GHz while the former achieves lower data rate than the latter. We consider a factory-like indoor area where FTs and a single Flexible Gateway (FG), which is in charge of aggregating data generated by FTs, are deployed as shown in Figure 1. The FG is also equipped with 2.4GHz and 920MHz interfaces to receive data from FTs. Some FTs are supposed to generate non-periodic, bursty, and heavy-load traffic, which are called NP-FTs. Since this type of traffic is in general supported by higher PHY rate at 2.4GHz that has limited communication range, we assume that NP-FTs are deployed near FG. On the other hand, FTs except for NP-FTs are assumed to generate periodic, light-load traffic, which are called P-FTs. A typical example of P-FT is a sensor device generating monitoring data of industrial machines and/or a given environment, which are deployed at various places within an area. This requires P-FTs to employ an interface and/or parameters realizing a larger communication range, for which 920MHz is more favorable option. We assume that the information on period of P-FT's traffic is known and shared by all FTs/FG. This is a reasonable assumption since these terminals and gateway are considered to be deployed by a single administrator of a factory. Furthermore, the timing of packet-generations of P-FTs are controlled to be equally separated over time so that they are not overlapped. This enables us to avoid contention among P-FTs. In a normal operation mode, NP-FTs employ 2.4GHz interface while P-FTs utilize 920MHz interface. Here, 2.4 GHz interface is supposed to follow IEEE 802.11 PHY/MAC protocol while 920MHz interface is in accordance with IEEE 802.15.4g/e PHY/MAC protocol. Note that both of these standards employ CSMA/CA protocol. The FG receives data from both NP-FTs and P-FTs by using its two interfaces. It is assumed that the carrier-sense range of 2.4GHz interface is smaller than that of 920MHz as shown in Figure 1: for example, carrier-sense range of NP-FT1 in Figure 1 over 920MHz is sufficiently large to detect signals transmitted by all terminals while it can only sense signals transmitted by a part of terminals over 2.4GHz.

B. Problem Definition

In this work, we consider a scenario where severe noise/interference is caused over 920MHz, which can be emitted from industrial machines and/or radio devices deployed inside/outside a factory area, and 920MHz interface suffers from continuous communication failures for a long period of time. As mentioned in Section I, FTs are able to switch

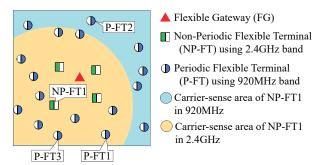


Figure 1. The considered, factory-like system model.

their operating interface. Therefore, P-FTs, which operate with 920MHz interface in a normal operation mode, can switch their operating interface to 2.4GHz, e.g., after detecting continuous packet errors or after receiving some instruction if there is a central entity to monitor the radio environment. Here, each P-FT is assumed to employ low PHY rate (e.g., 1Mbps) at 2.4GHz, which enables each P-FT to achieve sufficiently large communication range to transmit data to FG. However, when P-FTs and NP-FTs share the same 2.4GHz frequency band, another problem can occur, which is a hidden terminal problem. For example, as shown in Figure 1, NP-FT1 and P-FT2 cannot sense their signals with each other at 2.4GHz. Therefore, CSMA/CA mechanisms do not work properly among these nodes after P-FT2 changes its operating band to 2.4GHz, which can cause packet losses at FG, thereby degrading packet delivery ratio and throughput.

A well-known solution to hidden terminal problem is RTS/CTS handshake defined in IEEE 802.11. However, it has been reported that the efficiency of RTS/CTS handshake is low when short packets, such as small amount of data generated by P-FTs in our scenario, are involved in data transmissions [9]. Furthermore, RTS/CTS mechanism does not fundamentally solve problems on collisions among hidden terminals: RTS frames transmitted by hidden terminals can collide with high probability. Another requirement specific to industrial applications is more strict and deterministic protection for sensing data in comparison to Internet access/file transfer [10], which is difficult to achieve with RTS/CTS handshake even with QoS differentiation defined in IEEE 802.11e [11]. Therefore, in this work, we propose a mechanism to deterministically suppress transmissions of NP-FTs to avoid interference with hidden P-FTs without resorting to RTS/CTS mechanisms by exploiting interface heterogeneity, traffic periodicity, and adaptive queue management.

III. PROPOSED TRANSMISSION CONTROL

The proposed scheme controls packet transmissions of NP–FTs in order to suppress interference with their hidden P–FTs.

A. Mechanism to Detect Hidden Terminals

The NP-FTs first need to identify possible hidden terminals in order to suppress their mutual interference. This is achieved by exploiting the heterogeneity of interface. Each NP-FT observes traffic over 920MHz and 2.4GHz while they are not

transmitting their own data. In the normal operation mode, P-FTs transmit data at 920MHz. In this case, each NP-FT finds packets of all P-FTs over 920MHz since they can easily reach each NP-FT thanks to a large communication range of 920MHz. For example, NP-FT1 shown in Figure 1 observes periodic receptions of all P-FTs at 920MHz interface in a normal operation mode. After P-FTs detect noise/interference at 920MHz, they switch their interface to 2.4GHz, where NP-FT1 receives packets only from P-FTs located within its communication range over 2.4GHz. Thus, in the example of Figure 1, NP-FT1 cannot receive packets transmitted by P-FT2 since P-FT2 is out of carrier-sense/communication range of NP-FT1. Then, NP-FT1 finds that it has a hidden terminal of P-FT2 over 2.4GHz. At this timing, NP-FTs can also find that P-FTs have changed their operating band to 2.4GHz. Thus, by comparing packet receptions at 920MHz and 2.4GHz, each NP-FT can identify its hidden terminals over 2.4GHz, whose packets can cause collisions against itself.

B. Basic Idea of Proposed Transmission Control

While receiving packets from P–FTs in the normal operation mode, each NP–FT records the reception timing of each P–FT. Based on this information and pre–knowledge of the period of packet transmissions of each P–FT, each NP–FT predicts the timing of periodic packet transmissions. Then, each NP–FT suppresses its packet transmissions when the transmissions of its hidden P–FTs are expected. This is achieved by our proposed Transmission Control (TC), which executes queue management to control timing to pass upper–layer packets to MAC layer module.

The basic idea of the proposed TC is shown in Figure 2. Here, the blue solid arrow shows the predicted transmission timing of a hidden P-FT. With the proposed TC, a duration called Suspending Duration (SD), which consists of Pre-SD (before the predicted timing) and Post-SD (after the predicted timing) is prepared. A NP-FT attempts to suspend its packet transmission over SD, i.e., even if packets are generated at upper layer, it stores them into its upper-layer queue, and does not pass them to MAC layer module. In Figure 2, the dashed green arrow represents the timing when packets are generated at upper layer of NP-FT. Once SD is over, NP-FT passes the stored packets to MAC layer module, which are then transmitted by MAC layer module over the air. Note that packets generated at non-SD duration can be immediately passed to MAC layer module and transmitted as in the packet P4 in Figure 2. The flowchart of these operations of the proposed transmission control is shown in Figure 3. The duration of Pre-SD and Post-SD are decided considering trade-off between achievable Packet Delivery Ratio (PDR) of P-FTs and throughput of NP-FTs as discussed in Section IV-B in more detail.

With the above operation of TC, we can prevent NP–FTs from passing their packets to MAC layer module at the timing when hidden terminals are expected to transmit their packets, thereby suppressing interference. However, the queue management at upper layer has difficulty to precisely control the timing when signals are actually transmitted at

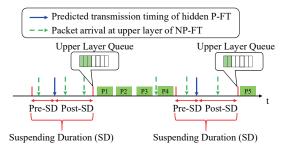


Figure 2. Basic idea of the proposed transmission control.

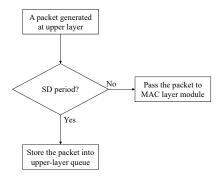


Figure 3. A flowchart of basic operations of the proposed transmission control.

PHY/MAC level. This problem is explained in an example shown in Figure 4. Here, a NP-FT suspends passing packets to MAC layer module during the first SD, and three packets are stored in the upper-layer queue. These packets are passed to MAC layer module after the first SD is over, which are then stored in lower-layer PHY/MAC queue. The transmissions of packets in PHY/MAC queue are managed by PHY/MAC module, which are in general hard to control since it requires the modification of firmware installed into WiFi module/chip. The packets are transmitted if they win contentions against the other terminals. In the example of Figure 4, it is supposed that NP-FT succeeds in transmitting a packet P1 by winning the contention. However, it fails to transmit packets P2 and P3 due to the lost contentions with BackGround (BG) traffic. Then, these 2 packets remain in PHY/MAC queue in the beginning of the next SD. As mentioned above, it is impossible to control the transmissions of these lower-layer packets, therefore, they can be transmitted even during SD, which can cause a collision with packets transmitted by hidden P-FTs.

A possible solution to the above–mentioned problem is to control the number of packets to be passed to MAC layer module based on the congestion level over the channel, i.e., each NP–FT controls the number of packets passed to MAC layer module in the end of SD in such a way that these packets can be transmitted in the following non–SD period at the PHY/MAC level. This requires each NP–FT to continuously monitor the congestion level over the operating channel. Note that background traffic at 2.4GHz are not necessarily generated by WiFi terminals, whose packets can be decoded by NP–FT, but generated by the other radio equipment, e.g., Bluetooth or Microwave oven. In this case, each NP–FT needs to monitor the congestion level without decoding each background signal.

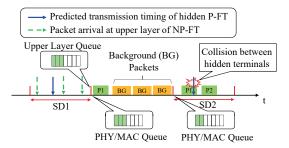


Figure 4. An example of problem on controlling packet transmissions with SD.

Therefore, in the following subsection, we first investigate whether it is practically possible for a WiFi terminal to conduct real-time monitoring of busy rate (i.e., fraction of time during which the channel is occupied by radio signals) of a channel.

C. Feasibility to Monitor Congestion Level

We found a parameter called CCAcount in a device driver of an off-the-shelf WiFi module (Buffalo WL-U3-866DS [12]). The parameter seems to be related to busy rate of a channel, however, there was no evidence that this parameter represents our desired information on busy rate. Therefore, we conducted experiments to check the relationship between CCAcount and busy rate of a channel. In the experiments, we prepared 3 laptop PCs with USB dongles of WL-US-866DS. A laptop PC (Tx PC) was configured to be a transmitter of packets, which are directed to Rx laptop PC. A laptop PC to observe CCAcount was located at a sufficiently close position to Tx PC. The busy rate was varied by changing the number of packets transmitted per a unit time, for which the output of CCAcount was monitored at the observing PC. The PHY rate, packet size, and ACK size of packet transmissions were respectively set to be 54Mbps, 1496Bytes, and 46Bytes. The busy rate for each traffic load can be calculated based on these parameters. The measurements were conducted inside a shielded room.

Figure 5 shows the output of CCAcount against traffic load (packets/s). From this figure, we can see that CCAcount increases as traffic load increases, which saturates over the range of high traffic load. There is a maximum traffic load that can be generated by a single WiFi terminal, which depends on back—off parameters and Inter—Frame Space (IFS) of IEEE 802.11, where the saturation is observed. From this figure, we can confirm that there is a direct relationship between CCAcount and traffic load, i.e., busy rate of the channel, which enables us to employ CCAcount as a measure of busy rate of the channel.

D. Proposed Adaptive Transmission Control

In this work, we design an Adaptive TC (ATC), which controls the number of packets to be passed to MAC layer module based on the observed CCAcount. In ATC, each NP-FT observes CCAcount during each non-SD period. The output of CCAcount is converted to the traffic load by using a

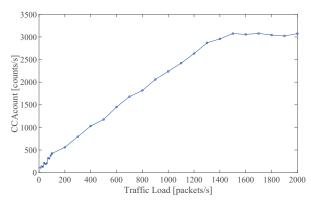


Figure 5. Experimental results on CCAcount against traffic

linear equation approximating the relationship between CCA-count and traffic load over the load range of [0:1500] packets/s in Figure 5, which is used to calculate the busy rate. Based on the derived busy rate, the maximum number of packets permitted to be passed to MAC layer module at the next non–SD period, N_{max} , is decided. N_{max} is calculated as follows:

$$N_{max} = \frac{(1 - B_{ave})T_{NSD}}{T_D \cdot \alpha}.$$
 (1)

Here, T_{NSD} is the duration of next non–SD period, T_D is the duration required to transmit a single data frame including SIFS and ACK duration, and α is a parameter to vary effective number of N_{max} , and B_{ave} is average busy rate calculated as

$$B_{ave} = \frac{\sum_{i=1}^{W} B_i}{W},\tag{2}$$

where B_i is busy rate calculated for the i-th last non–SD period, and W is the window size (number of non–SDs) used for calculating average busy rate. N_{max} calculated with (1) represents the estimated (effective) number of packets that can be transmitted by a single NP–FT during free period in the following non–SD period. Note that α is introduced in order to take the impact of back–off duration and number of contending FTs into account. With smaller (larger) α , the estimation of N_{max} becomes more optimistic (pessimistic). The range of α considered in this paper is set to [0.4, 6.0].

The proposed ATC is executed in the end of every SD period. For instance, in the end of SD1 in Figure 4, N_{max} is calculated by using busy rate over the last W non–SD periods. Then, if the number of packets stored in the upper-layer queue is equal to or more than N_{max} , only N_{max} packets out of stored packets are passed to MAC layer module, and no more packets are passed to MAC layer module during the following non–SD period. Otherwise if the number of packets stored in the upper–layer queue is less than N_{max} , all stored packets are passed to MAC layer module. Then, newly arriving packets in the following non–SD period can be passed to MAC layer module as long as the total number of packets passed to MAC layer module does not exceed N_{max} . With these operations, we can reduce the probability that packets remain in PHY/MAC queue in the end of each non–SD period.

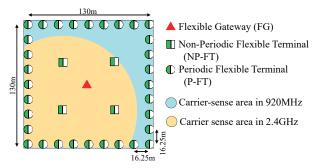


Figure 6. Simulation Model.

TABLE I: Simulation Parameters

	NP-FT	P–FT
PHY rate	54Mbps	1Mbps
Communication range	75m	100m
Carrier-Sense Range	100m	100m
Packet generation	Poisson (mean λ)	period = 1s
Data size	2000Bytes	200Bytes
ACK size	30Bytes	
DIFS	$28\mu s$	
SIFS	$10\mu s$	
Slot time	$20\mu s$	
Max. Num. of Retransmissions	3	
Min. Contention Window	31	
Simulation Duration	20s	

IV. SIMULATION MODEL AND RESULTS

In this section, we provide numerical results obtained by our computer simulations, and discuss the benefit brought by the proposed transmission control in detail.

A. Simulation Model

The simulation model is shown in Figure 6. The layout given in Figure 6 is selected since it can increase the number of hidden terminals, which allows us to consider a worstcase scenario. In the simulations, communication performance after P-FTs change their operating frequency band to 2.4GHz is evaluated. The main parameters used in simulations are shown in Table I. Most of the parameters are taken from the IEEE 802.11g standard [13]. The P-FTs generate packets with period of 1s, and their generation timing are scheduled so that they do not overlap with each other. In the evaluation, since there are 32 P-FTs, a period of 1s is divided into 32 sections, and the beginning of each section is randomly assigned to each P-FT as its generation timing. Each NP-FT applies the proposed TC/ATC to its hidden P-FTs. We use the application-level PDR of P-FT and throughput of NP-FT as performance measures. A packet is decided to be lost and discarded once the number of retransmissions reaches the maximum value. For simplicity, packet errors are assumed to occur only due to collisions. The throughput is defined as the amount of data successfully delivered by NP-FTs to FG. The simulation is conducted by a custom-made simulator developed with Matlab software.

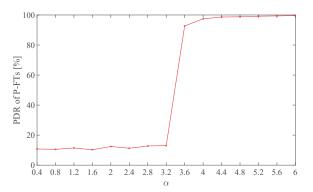


Figure 7. PDR of NP-FTs against α for ATC.

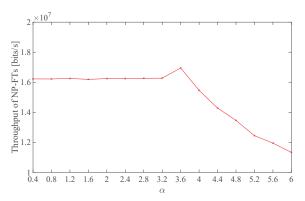


Figure 8. Throughput of NP-FTs against α for ATC.

B. Simulation Results

Below, we show simulation results averaged over 5 simulation trials. Figure 7 shows PDR of P-FTs against the parameter of α in (1) when the proposed ATC is employed with Pre–SD = 2ms, Post–SD = 6ms, W = 10, and λ = 400 [packets/s]. From Figure 7, we can see that PDR of P-FT is degraded with smaller α . With smaller α , each NP-FT passes a larger number of packets to MAC layer module in the end of SD as calculated by (1), which exceeds the number of packets that can be transmitted at PHY/MAC layer during the next non-SD period. In this case, packets remained in PHY/MAC queue can be transmitted simultaneously with hidden P-FTs, which causes collisions with high probability. This problem is alleviated by increasing the value of α where the number of packets passed to MAC layer module is reduced. Therefore, PDR of P-FT is improved with larger value of α . However, larger values of α force each NP-FT to keep more packets in its upper-layer queue, and degrade its throughput performance. This is confirmed in Figure 8, where throughput of NP-FTs against α is shown. The throughput of NP-FTs is largely degraded with too large α , i.e., the range of α exceeding 3.6. From these results, we can see that there is an appropriate value of α to be employed to achieve both high PDR of P-FTs and high throughput of NP-FTs. In the following evaluations, we employ $\alpha = 3.6$ based on the above results.

Next, we investigate the impact of SD length on the achievable performance of the proposed ATC. Figures 9 and 10 respectively show PDR of P-FTs and throughput of NP-

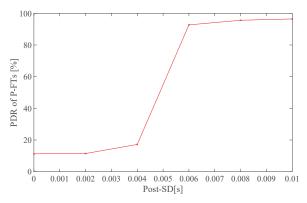


Figure 9. PDR of P-FTs against Post-SD for ATC.

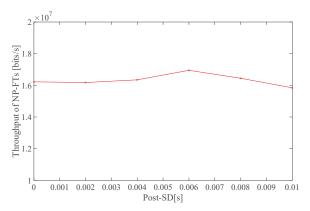


Figure 10. Throughput of NP-FTs against Post-SD for ATC.

FTs against the length of Post-SD, where Pre-SD is fixed to be 2ms, W = 10, $\alpha = 3.6$, and $\lambda = 400$ [packets/s]. First, from Figure 9, we can see that a sufficiently large value of Post-SD is required to achieve high PDR of P-FTs. Each packet generated at P-FT is transmitted with CSMA/CA protocol, where its actual transmission timing at PHY/MAC level can be delayed due to contentions with the other NP-FTs and P-FTs within its carrier-sense range. Therefore, if NP-FT employs too small Post-SD, it can transmit packets with hidden P-FTs whose transmissions are delayed due to CSMA/CA operations. The increase of Post-SD also offers the improvement on throughput as shown in Figure 10 thanks to higher probability to avoid mutual collisions, however, too large Post-SD leads to the reduction of throughput of NP-FTs since it can reduce the duration for NP-FTs to be able to transmit their packets. From these figures, we can see that Post-SD of 6ms is an appropriate choice in our considered settings.

Finally, we respectively show PDR of P–FTs and throughput of NP–FTs against traffic load of NP–FTs for different schemes in Figures 11 and 12. Here, we set Pre–SD = 2ms, Post–SD = 6ms, W=10, and $\alpha=3.6$. In these figures, we also show upper–bounds, which are obtained if we can ideally stop/start the transmission of packets at PHY/MAC level according to the schedule of SD and non–SD. Note that the performance of these upper–bounds can be obtained only if we can modify PHY/MAC module so that we can arbitrarily

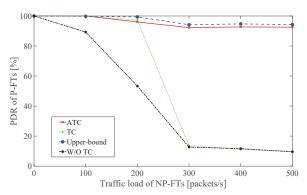


Figure 11. PDR of P-FTs against traffic load of NP-FTs.

control transmission timing at PHY/MAC level. On the other hand, our proposed ATC only requires the modification of a device driver of WiFi module. The results of W/O TC in these figures represent achievable performance of an existing scheme, which follows conventional IEEE 802.11 MAC protocol without employing our proposed TC. From Figure 11, we can first see that PDR of P-FTs is largely degraded if we do not employ TC. This is due to packet collisions between NP-FTs and their hidden P-FTs. By introducing TC with SD, PDR of P-FTs can be improved, however, we can obtain gain only over the range of small traffic load of NP-FTs. As the traffic load of NP-FTs increases, more packets are stored in the upper-layer queue in the end of each SD, which can exceed the number of packets that can be handled at PHY/MAC level during the following non-SD period. Therefore, more collisions occur for larger traffic of NP-FTs, which degrades PDR of P-FTs. On the other hand, it can be seen that the proposed ATC achieves high PDR of P-FTs even for larger traffic load of NP-FTs thanks to the adjustment of number of packets passed to PHY/MAC queue, which is adapted to the observed traffic load. We can see that the proposed ATC achieves PDR close to the upperbound. Next, from Figure 12, we can see that the proposed ATC does not degrade throughput of NP-FTs even with the introduction of SD. The avoidance of collisions eventually leads to throughput improvement in comparison to the other schemes. With the proposed ATC, packets are stored in the upper-layer queue according to the estimated traffic load. If the actual traffic load is smaller than the estimated value, all packets passed to PHY/MAC queue can be transmitted at early timing within a non-SD period, after which no packet is transmitted since there is no packet in PHY/MAC queue. This problem does not occur with upper-bound, therefore, throughput of the proposed ATC does not reach close to the upper-bound. However, from these results, we can confirm that the proposed ATC can significantly improve PDR of P-FTs while achieving slightly better throughput of NP-FTs in comparison to the other schemes.

V. CONCLUSIONS

In this paper, focusing on a wireless coexistence scenario where multi-radio platforms are employed to support heterogenous traffic, we proposed an Adaptive Transmission

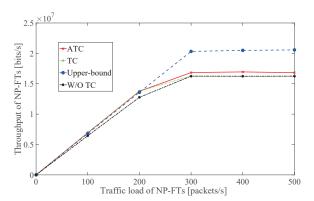


Figure 12. Throughput of NP-FTs against traffic load of NP-FTs.

Control (ATC), which suppresses mutual interference between hidden terminals generating periodic and non–periodic traffic. The proposed ATC exploits interface heterogeneity, traffic periodicity, and queue management adapting to the observed congestion level. We first confirmed with experiments the practicality for WiFi device to monitor congestion level in a real–time manner. Then, we evaluated the gain of the proposed ATC in terms of packet delivery ratio and throughput by computer simulations. Our numerical results showed that the proposed ATC significantly improves PDR of periodic traffic while slightly improving throughput of non–periodic traffic in comparison to reference schemes.

Our future work includes experimental evaluations of the proposed ATC with actual multi-radio platforms. More extensive verifications of simulation results, e.g., with a larger number of simulation trials and comparison with theoretical results, are also our future work. Furthermore, in this paper, it is assumed that the transmission timing of P–FTs can be ideally estimated by NP–FTs. However, in practice, this estimation can be incomplete, which can shift SD from the desired duration. This causes degradation of PDR of P–FTs and throughput of NP–FTs, therefore, we need to evaluate the impact of estimation error on the achievable performance of the proposed transmission control.

ACKNOWLEDGEMENT

This work is supported by the Ministry of Internal Affairs and Communications for the project entitled "R&D on Technologies to Densely and Efficiently Utilize Radio Resources of Unlicensed Bands in Dedicated Areas."

REFERENCES

- J. Gummeson, D. Ganesan, M. D. Corner, and P. Shenoy, "An Adaptive Link Layer for Heterogenous Multi-Radio Mobile Sensor Networks," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 7, pp. 1094–1104, Sept. 2010.
- [2] D. K. Tosh and S. Sengupta, "Heterogenous Access Network(s) Selection in Multi-Interface Radio Devices," *IEEE International Workshop on Managing Ubiquitous Communications and Services*, pp. 117–122, 2015.
- [3] "Smart Energy Gateway CUBE, NextDrive Co." accessed: 2020-01-07.[Online]. Available: https://www.nextdrive.io/en/productNew/Cube

- [4] S. Dietrich, G. May, O. Wetter, H. Heeren, and G. Fohler, "Performance indicators and use case analysis for wireless networks in factory automation," in 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Sep. 2017, pp. 1–8.
- [5] M. Dungen et al., "Channel measurement campaigns for wireless industrial automation," Automatisierungstechnik, vol. 67, no. 1, pp. 7– 28, 2019.
- [6] A. Varghese and D. Tandur, "Wireless requirements and challenges in Industry 4.0," Proc. of 2014 International Conference on Contemporary Computing and Informatics (IC3I), pp. 634–638, 2014.
- [7] M. Sansoni et al., "Comparison of M2M Traffic Models Against Real World Data Sets," Proc. of IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pp. 1–6, 2018.
- [8] X. Cao, J. Chen, Y. Cheng, X. X. Shen, and Y. Sun, "An Analytical MAC Model for IEEE 802.15.4 Enabled Wireless Networks With Periodic Traffic," *IEEE Transactions on Wireless Communications*, vol. 14, no. 10, pp. 5261–5273, Oct. 2015.
- [9] L. Zhang et al., "Signal Strength Assistant Grouping for Lower Hidden Node Collision Probability in 802.11ah," Proc. of 9th International Conference on Wireless Communications and Signal Processing (WCSP), pp. 1–6, Oct. 2017.
- [10] A. A. K. S., K. Ovsthus, and L. M. Kristensen, "An Industrial Perspective on Wireless Sensor Networks: A Survey of Requirements, Protocols, and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1391–1412, Third Quarter 2014.
- [11] "Ieee standard for information technology-local and metropolitan area networks-specific requirements-part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications - amendment 8: Medium access control (mac) quality of service enhancements," *IEEE* Std 802.11e-2005 (Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003), pp. 1–212, 2005.
- [12] "BUFFALO, WI-U3-866DS," accessed: 2020-01-07. [Online]. Available: https://www.buffalo.jp/product/detail/wi-u3-866ds.html
- [13] D. Vassis, G. Kormentzas, A. Rouskas, and I. Maglogiannis, "The ieee 802.11g standard for high data rate wlans," *IEEE Network*, vol. 19, no. 3, pp. 21–26, May 2005.