Wireless Netw (2019) 25:805–817
https://doi.org/10.1007/s11276-017-1593-z

A frequency hopping method for spatial RFID/WiFi/Bluetooth scheduling in agricultural IoT

Tao Chi[1,2] · **Ming Chen**[1,2]

Published online: 12 October 2017

Abstract Currently, a variety of wireless modules are purposed for different criteria in the area of the agricultural internet of things; however, there is a lack of appropriate methods enabling these wireless modules to operate in the same frequency band. The goal of this paper is to make a very thorough quantitative analysis on the theoretical maximum collision time and collision probability of WiFi or Bluetooth network with RFID interferers. We propose the interference avoidance scheme which requires the knowledge of the theoretical maximum collision time and collision probability between RFID and WiFi/Bluetooth packets. This scheme generates an optimal channel based on the current usage of the adjacent frequency channels thereby reducing the interference. We also propose two solutions from this scheme: a frequency hopping combined with white space exploitation method and an intelligent frequency hopping scheme; for maintaining a quality connection of the WiFi or Bluetooth network in the presence of heavy RFID interferers. We implement a hybrid backscatter-based RFID architecture in existence of the WiFi/Bluetooth infrastructure for efficient operations within the 2.4 GHz ISM band. Results obtained are very encouraging and indicate that quantifying the maximum collision time and collision probability is a vital step for the interference avoidance scheme, which can be adopted in the avoidance of the interference from RFID modules.

✉ Tao Chi
tchi@shou.edu.cn

[1] College of information Technology, Shanghai Ocean University, Shanghai 201306, China

[2] Key Laboratory of Fisheries Information, Ministry of Agriculture, Shanghai 201306, China

Keywords Wireless communication · Agricultural IoT · Coexistence solution · RFID · WiFi · Bluetooth

1 Introduction

Today agriculture is embedded with advance services such as internet of things (IoT), agriculture intelligent products that enable to communicate to each other analyze the data and also exchange data among them [1]. For example, given such RFID, WiFi and Bluetooth as the communication modules of IoT in Agricultural Sector, the agricultural IOT demands an environment characterized by wireless technologies coexistence. Because the physical medium of connectivity is not required in the agricultural IOT, interference can occur with multiple wireless modules operating in the same frequency band. Especially when RFID module transmits more power, it may cause a decrease in the performance of other modules and could even make them lose connectivity. Due to this potential for interference, effective methods are necessary to achieve successful coexistence of RFID and WiFi/Bluetooth modules, in particular in the presence of heavy RFID interferers.

The main contribution of this paper is the exact calculation of the theoretical maximum interference caused by RFID modules sharing a 2.4 GHz band. Information regarding the calculation of these data is available in the ISO 18000 and IEEE standards. In the paper, an interference pattern is established between RFID and WiFi/Bluetooth networks operating in the same 2.4 GHz band. This study performs in-depth analysis on the influence of interference factors, i.e., the spread spectrum, Path Loss, transmission power, antenna gain, RF physical channel, packet format, throughput, and medium access control protocols [2]. To determine the effect of RFID as a source

of interference, the bit error rate (BER) and Path Loss are observed to determine the amount of interference in the physical layer. The BER is calculated to check the accuracy of wireless communication, and Path Loss is calculated to evaluate interference from RFID devices. In addition, a packet collision model for RFID and WiFi packets and a packet collision model for RFID and Bluetooth packets have been constructed in the MAC layer. These models incorporate the collision time in the time domain and the collision probability in the frequency domain.

Our technique is based on a hybrid RFID design that is protocol-compatible with existing WiFi and Bluetooth standards as well as existing RFID standards. Using the hybrid infrastructure, two sets of baseline performance tests of the WiFi/Bluetooth network without interferers and two sets of coexistence performance tests of the WiFi/Bluetooth network with RFID interferers have been performed. These experiments show that when RFID and WiFi/Bluetooth modules are at a reasonable distance from one another, both obtain a large majority of the throughput that would have been obtained with no interference. In addition, these experiments also demonstrate that the interference caused by RFID modules can significantly degrade the performance of the WiFi or Bluetooth network when RFID modules are moved within three meters of the WiFi and Bluetooth modules. To maintain fairness between RFID and WiFi/Bluetooth modules, two solutions are presented in this paper: one is frequency hopping combined with a white space exploitation method for improved coexistence of RFID and WiFi devices; the other is an intelligent frequency hopping scheme for improved coexistence of RFID and Bluetooth devices. The core of the two solutions is the interference avoidance scheme, which requires the knowledge of the theoretical maximum collision time and collision probability between RFID and WiFi/Bluetooth packets. The primary elements of the interference avoidance scheme are the interference detection scheme and smart channel selection. Using the interference avoidance scheme can facilitate optimal interference detection and make the hybrid infrastructure itself determine which channel is the best to use, depending on the current usage of the adjacent frequency channels.

The remainder of this paper is organized as follows: We survey the related wireless coexistence research and explain the novelty of our work in Sect. 2. The causes of the interference with WiFi and Bluetooth networks from RFID interferers are analyzed, and then the packet collision model for RFID and WiFi packets and the packet collision model for RFID and Bluetooth packets are constructed in Sect. 3. Section 4 details a hybrid backscatter-based RFID infrastructure and coexistence testing. Two proposed solutions for achieving successful coexistence are explained in Sect. 5. Finally, Sect. 6 concludes the paper.

2 Related work

Recent work has provided solutions to the problem of modeling interference between wireless devices. For example, in [3], Ivan Howitf has made a general exposition of the interference between WPAN and WLAN and established a complex mathematical model to study the interference caused by the two systems. In [4, 5], Glomie et al. have analyzed the interference between WLAN and Bluetooth and constructed a theoretical model of the impact of interference on the performance of the networks. In [6, 7], the authors made an analysis on the interference between Bluetooth and WLAN and examined all the possible factors that produce the interference. In [8, 9], the authors laid special stress on analyzing the performance of WLAN under interference caused by Zigbee and deduced a formula to calculate the error rate. In [10, 11], Shin et al. did an analysis of the interference caused by WLAN on a Zigbee network, using the error rate as a measure of the performance of the networks. In [12], the authors investigated existing spectrum sharing methods facilitating coexistence of various RF systems. In [13], the authors examined the mutual interference effect of 2.4 GHz devices widely deployed at home via both theoretical analysis and real-life experiment. In [14–16], the authors proposed a dynamic cooperative MAC mechanism (DCMAC) for wireless networks. The IEEE has established an 802.15.2 group to study the problem of the special interference between a WLAN and WPAN, releasing the IEEE 802.15.2 standard. This standard analyzes the interference between WPAN and WLAN and develops a mathematical model of the theoretical interference in the physical layer and MAC layer.

However, the literature published domestically and abroad lacks a thorough study on the interference between RFID and wireless systems. Our work is based on analysis of the existing research results on the interference between various wireless systems; it continues the study of RFID interference, mainly in terms of WiFi/Bluetooth networks. We analyze the causes of the interference between RFID and WiFi/Bluetooth networks and propose a quantitative model for the theoretical maximum collision time and collision probability between RFID and WiFi/Bluetooth packets.

3 Analysis of interference with the wireless network from RFID devices

In this section, the causes of the interference from RFID devices are analyzed in two parts: interference with the WiFi network and interference with the Bluetooth network. Addressing the physical layer and MAC layer, these analyses are premised on Path Loss, interference distance, transmission power, antenna gain, RF physical channel, packet format, traffic load and a medium access control protocol [17–19]. To determine the effect of the interference from RFID devices on the performance of existing wireless network, several parameters, such as BER, PER, average packet delay, and network throughput, are used for quantitative evaluation of RFID interference [20, 21]. The BER and Path Loss for the wireless network are calculated according to the Path Loss Model in the physical layer, and then the causes of the interference are analyzed to quantify the interference from RFID devices. To obtain the theoretical maximum collision time and collision probability between RFID and WiFi or Bluetooth packets, the packet collision model for RFID and WiFi packets and the packet collision model for RFID and Bluetooth packets are established in the MAC layer. These packet collision models include the collision time in the time domain and the collision probability in the frequency domain.

3.1 Analysis of interference with the WiFi network from RFID devices

Using interference distance, transmission power and the path loss model, the BER for the WiFi network with RFID interferers can be obtained; then, Path Loss, which is expressed as a quantitative evaluation of the RFID interference with the WiFi network, is calculated in the physical layer. According to the MAC sub-layer protocol of RFID and WiFi networks, the packet collision model for RFID and WiFi packets has been established. The packet collision model includes the collision time in the time domain and the collision probability in the frequency domain.

(1) Path Loss Model in the Physical Layer

Given scene parameters such as transmitting frequency, distance and antenna gain, Path Loss can be calculated. In this work, the 2.4 GHz Indoor Path Loss Model is used for the theoretical calculation of the WiFi network [22, 23].

$$L_{P,WLAN} = \begin{cases} 40.2 + 20\lg d & 0.5 < d < 8 \\ 58.5 + 33\lg(d/8) & d > 8 \end{cases} \quad (1)$$

Due to near field affect, the model mentioned is a segmented path loss model. Similarly, the path loss model of the 2.45 GHz RFID system is calculated [24] as follows:

$$L_{RFID} = -147.6 + 20\lg d + 20\lg f - 10\lg G_r G_t \quad (2)$$

d is the distance in meters from the interrogator to the tags or to the WiFi receiver. f is the carrier frequency of 2.45 GHz. G_r and G_t are the antenna gains of the receiver and transmitter. When the transmission power and path loss are known, the reception power of the WiFi network is determined by the following formula:

$$P_r = P_t - L_{P,WLAN} \quad (3)$$

P_r is WiFi reception power, and P_t is WiFi transmission power. Given the distance from the RFID interferer to WiFi transmitter, the Path Loss can be calculated using the path loss model of the 2.45 GHz RFID system.

$$P_{rr} = P_{rt} - L_{P,RFID} \quad (4)$$

When the RFID transmitter emits continual wave energy in a frequency-hopping pattern, WiFi devices can be fed with the continual wave. P_{rt} is expressed as RFID transmission power, and P_{rr} is defined as the energy that is transmitted by RFID devices and received by WiFi devices. Because RFID and WiFi devices transmit in different ways using different protocols, these signals which are transmitted by RFID devices and then received by WiFi devices, are the interference signals in terms of the WiFi protocols.

(2) Collision Time in the MAC Layer

The packet collision model for RFID and WiFi packets is constructed in the MAC layer, which involves the collision time in the time domain and the collision probability in the frequency domain.

a. Collision Time in the time domain

Each WiFi network maintains the same frequency usage over time and only utilizes an available subset of 83.5 MHz. The WiFi standard defines 11 possible channels that may be used. Each channel is allocated by its center frequency. The center frequencies are at intervals of 5 MHz from one another. When RFID and WiFi devices operate on the same RF channel or on the adjacent RF channel, there is typically a time-domain collision for some packets on the transmission.

According to the MAC sub-layer protocol of two standards (IEEE 802.11 and ISO/IEC 18000-4), the packet collision model for RFID and WiFi packets is built, as shown in Fig. 1 and Table 1.

In the time domain, the collision time is defined as the overlap in time when an RFID packet is being transmitted while a WiFi packet is also in the transmission. From the IEEE 802.11 standard and the ISO/IEC 18000-4 standard, the payload sizes of the RFID packet and WiFi packet are varied. According to the packet size of the RFID packet

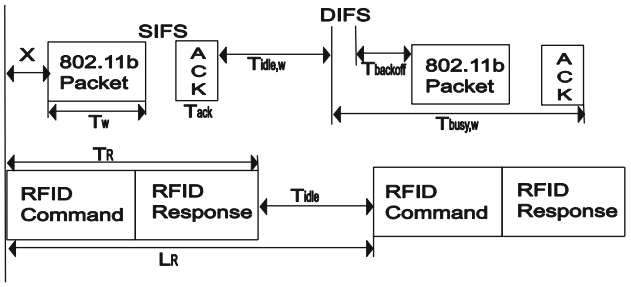

Fig. 1 The packet collision model for RFID and WiFi packets

Table 1 Parameters of the packet collision model for RFID and WiFi packets

Symbols	Specified parameters
T_w	Duration of the WiFi packet
T_{ack}	Duration of the WiFi ACK packet
$T_{backoff}$	Average backoff time of WiFi
$T_{idle,w}$	Idle time between two consecutive packets
$T_{busy,w}$	Duration of a whole packet transmission
T_R	Duration of RFID command and response packet
T_{idle}	Idle time between two RFID packets
L_R	Interarrival time between two RFID packets
DIFS	DCF interframe space of WiFi
SIFS	Short interframe space of WiFi

and WiFi packet, the collision time is detailed in different cases.

The collision time, (T_C), can be expressed as follows:

If $T_W \le T_R \& T_W \le T_{idle}$, then

$$T_C = \begin{cases} T_W & 0 \le X \le T_R - T_W \\ T_R - X & T_R - T_W < X < T_R \\ 0 & T_R \le X < L_R - T_W \\ T_W + X - L_R & L_R - T_W \le X \le L_R \end{cases} \quad (5)$$

If $T_W \le T_R \& T_W > T_{idle}$, then

$$T_C = \begin{cases} T_W & 0 \le X \le T_R - T_W \\ T_R - X & T_R - T_W < X \le L_R - T_W \\ T_W - T_{idle} & L_R - T_W < X \le T_R \\ T_W + X - L_R & T_R \le X \le L_R \end{cases} \quad (6)$$

If $T_R < T_W < T_{idle}$, then

$$T_C = \begin{cases} T_R - X & 0 \le X \le T_R \\ 0 & T_R < X < T_R - T_W \\ T_W + X - L_R & L_R - T_W \le X < L_R + T_R - T_W \\ T_R & L_R + T_R - T_W \le X \le L_R \end{cases} \quad (7)$$

If $T_W > T_R \& T_{idle} \le T_W \le T_R$, then

$$T_C = \begin{cases} T_R - X & 0 \le X \le T_R - T_W \\ T_W - T_{idle} & L_R - T_W < X < T_R \\ T_W + X - L_R & T_R < X \le L_R + T_R - T_W \\ T_R & L_R + T_R - T_W < X \le L_R \end{cases} \quad (8)$$

Since there is no synchronization mechanism between RFID and WiFi networks, we can design a scheme to set the transmission time.

b. Collision Probability in the frequency domain

While Direct Sequence Spread Spectrum technology (DSSS) is used for WiFi devices in the 2.4 GHz ISM band, the RFID system in the 2.4 GHz band utilizes frequency hopping spread spectrum technology (FHSS) to fight multi-path fading and interference. The RFID system can randomly hop over 100 channels, and the internal of each channel is 0.8192 MHz, less than the bandwidth of the channel. Since the bandwidth of the WiFi network is fixed to 22 MHz, interference can occur when the RFID's operating frequency jumps within the bandwidth of the WiFi network. Therefore, the collision probability in the frequency domain between the WiFi and RFID networks can be calculated as follows:

$$P_C = \frac{22}{0.8192 * 100} = 0.268 \quad (9)$$

(3) Performance of the WiFi Network with RFID Interferers

When RFID and WiFi packets do not overlap in the frequency domain, interference does not occur even if there is a collision in the time domain. Therefore, the collision time of the coexistence system between the RFID and WiFi packets can be defined as the product of the collision time in the time domain and the collision probability in the frequency domain.

$$T_{CF} = T_C * P_C = 0.268 T_C \quad (10)$$

Assuming that the offset time is a uniform distribution of 0 to L, the mean interference time can be determined by the following integral function:

$$T_{CE} = E[T_{CF}] = \frac{1}{L_R} \int L_R T_{CF}(x) dx \quad (11)$$

Using the BER and the collision time, the PER of the WiFi network can be calculated, which is a function of the packet length, bit time and collision time. In the following formula, P_{b0} is the BER for the WiFi network with no interference in the physical layer, and P_b is the BER for the WiFi network with RFID interferers in the physical layer.

$$PER = 1 - (1 - P_b)^{\frac{T_{CE}}{T_b}} (1 - P_{b0})^{\frac{(T_W - T_{CE})}{T_b}} \quad (12)$$

In actual application, the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is used for WiFi devices. The CSMA/CA mechanism requires two parameters: the maximum contention window ($W_{\max}$) and the minimum contention window ($W_{\min}$). According to the channel situation, the contention window (W_x) takes a value in $[W_{\min}, W_{\max}]$. Provided that M is a random number of 0 to W_x at an equal probability, the Backoff-avoid-time, ($T_{backoff}$), is the product of a random variable (M) and the slot time

$$T_{backoff} = M * T_{slot} \tag{13}$$

In accordance with IEEE 802.11 standards, the time required for a successful transmission, (T_{succ}), is the sum of DIFS, $T_{backoff}$ and packet length (T_w).

$$T_{succ} = DIFS + T_{backoff} + T_w \tag{14}$$

Similarly, the required time when a packet transmission error occurs, (T_{fail}), is the sum of DIFS, $T_{backoff}$, T_w and the timeout time waiting for an ACK packet.

$$T_{fail} = DIFS + T_{backoff} + T_w + T_{ack-timeout} \tag{15}$$

3.2 Analysis of the interference with the Bluetooth network from RFID devices

Due to the more power transmitted by RFID devices, there is serious interference caused by RFID devices in the Bluetooth network. To determine the effect of RFID as an interferer on the performance of the Bluetooth network, the BER for the Bluetooth network with RFID interferers can be calculated, and then Path Loss, which is expressed as a quantitative evaluation of RFID interference with the Bluetooth network, is obtained in the physical layer. According to the MAC sub-layer protocol of RFID and Bluetooth, the packet collision model for RFID and Bluetooth packets is built. The packet collision model includes the collision time in the time domain and the collision probability in the frequency domain.

(1) Path Loss Model in the Physical Layer

To illustrate the attenuation degree of the electromagnetic wave in propagation space, a 2.4 GHz indoor path loss model is used for the Bluetooth network [25].

$$L_{Bluetooth} = \begin{cases} 40.2 + 20\lg d & 0.5 < d < 8 \\ 58.5 + 33\lg(d/8) & d > 8 \end{cases} \tag{16}$$

The model is a segmented path loss model. Due to the near field effect, the model is not suitable for calculating path loss of < 0.5 m. When the distance is < 8 m, the path loss is the same as the path loss in free space; When the distance exceeds 8 m, the signal is attenuated faster. Similarly, the path model of 2.45 GHz RFID devices is defined as follows:

$$L_{RFID} = -147.6 + 20\lg d + 20\lg f - 10\lg G_r G_t \tag{17}$$

d denotes the distance in meters from the RFID interrogator to the RFID tag or to the Bluetooth receiver. f is the RFID carrier frequency. G_t is transmitter antenna gain, and G_r is receiver antenna gain. Given Bluetooth transmission power P_t and received power P_r, signal attenuation can be calculated as follows:

$$L_{Bluetooth} = P_t - P_r \tag{18}$$

Since the transmission power of RFID is much greater than that of Bluetooth, the Bluetooth device may easily receive the signal transmitted by the RFID device, thus forming the interference signal. The power of interference from the RFID device can be calculated as follows:

$$P_{Interferece} = P_t - L_{RFID} \tag{19}$$

(2) Collision Time in the MAC Layer

The packet collision model for RFID and Bluetooth packets is constructed in the MAC layer, which involves the collision time in the time domain and the collision probability in the frequency domain.

a. Collision Time in the time domain

When RFID devices are operating in the same 2.4 GHz band, there may be overlap in the time domain between RFID and Bluetooth packets. According to the MAC layer protocols of the IEEE 802.15.1 and ISO/IEC 18000-4 standards, the packet collision model for RFID and Bluetooth packets is established, as shown in Fig. 2. The Bluetooth device uses a slotted protocol, and each slot is 625 μs long. Although a transmission can occupy 1, 3 or 5 slots, there is a certain interval between transmissions. Since the RFID's packet cannot be automatically synchronized with the Bluetooth's packet, a time offset is used for setting the starting time of each packet. The minimum time offset is 0, and the maximum time offset is the interval

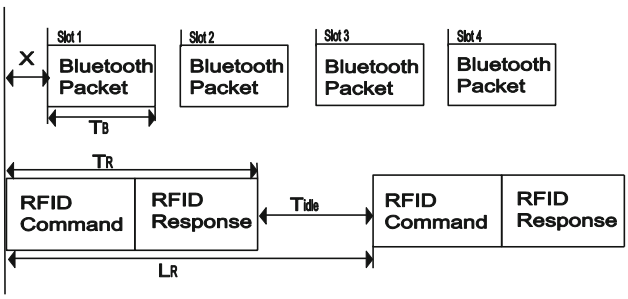

Fig. 2 The packet collision model for RFID and Bluetooth packets

between two continuous packets transmitted by RFID devices.

Collision time is defined as the overlap time between RFID and Bluetooth packet transmissions. According to the ISO/IEC 18000-4 standard, the 2.4 GHz RFID system does not exceed the maximum data rate of 40 kbps. At such a low data rate, the header length of the RFID packet is longer than that of the whole Bluetooth packet. According to the size of the RFID packet and the Bluetooth packet, the collision time is analyzed in different cases.

Collision time, (T_C), can be expressed as follows:

If $T_B \le T_R \& T_B \le T_{idle}$, then

$$T_C = \begin{cases} T_B & 0 \le X \le T_R - T_B \\ T_R - X & T_R - T_B < X < T_R \\ 0 & T_R \le X < L_R - T_B \\ T_B + X - L_R & L_R - T_B \le X \le L_R \end{cases} \quad (20)$$

If $T_B \le T_R \& T_B > T_{idle}$, then

$$T_C = \begin{cases} T_B & 0 \le X \le T_R - T_B \\ T_R - X & T_R - T_B < X < L_R - T_B \\ T_B - T_{idle} & T_R - T_B \le X < T_R \\ T_B + X - L_R & T_R \le X \le L_R \end{cases} \quad (21)$$

In practical applications, the RFID interrogator transmits a carrier modulated with data. The tag can absorb energy from the carrier. When carrier power is adequate, the tag drives the internal chip circuit and then demodulates data from the carrier. RFID interrogators not only transmit a modulated carrier in the return link but also transmit a non-modulated carrier in the forward link to supply energy to the tag. Therefore, whether the RFID interrogator transmits data or receives data, interference transmitted by the RFID interrogator has an important impact on the performance of the Bluetooth network.

b. Collision Probability in the frequency domain

A Bluetooth device uses frequency hopping spread spectrum technology, and each channel occupies 1 MHz bandwidth. The Bluetooth RF channel can be expressed as

$$f = 2402 + k\text{MHz}, k = 0, 1, 2, \ldots, 78 \quad (22)$$

Since a Bluetooth device hops randomly with even probability in the 79 channels in the physical layer, the probability that the Bluetooth device occupies any one channel is 1/79. Although the Bluetooth signal occupies only 1 MHz at any point in the time domain, it actually occupies 79 MHz due to the fact that the Bluetooth device can hop over 79 center frequencies. Therefore, it is not possible to have both RFID and Bluetooth products in the same area without the chance of interference.

Similarly, a 2.4 GHz RFID device utilizes frequency hopping spread spectrum technology and hops over 100 channels of 1 MHz bandwidth. Since the interval of center frequency of each channel is 0.8192 MHz, less than the bandwidth of each channel, there is overlap in adjacent channels of the RFID device. The RFID RF channel can be expressed as

$$f_{RFID} = (2931 + m) * 0.8192, \quad m = 0, 1, 2, \ldots, 99 \quad (23)$$

In Fig. 3, the shaded part of the overlap of the two signals is the interference portion. The collision probability between RFID and Bluetooth signals in the frequency domain is the product of the probability of any occupied channel for the Bluetooth signal and the average probability of an RFID channel overlapped with the Bluetooth channel.

$$P_C = P_{Bluetooth} * \overline{P} \quad (24)$$

(3) Performance of the Bluetooth network with RFID interferers

The collision time of the coexistence system is defined as the product of the collision time in the time domain and the collision probability in the frequency domain.

$$T_{CF} = T_C * P_C = T_C/79 \quad (25)$$

Assuming that P_{b0} is the BER for the Bluetooth network with no interference and P_b is the BER of the Bluetooth network with RFID interferers, the PER of the Bluetooth network can be calculated depending on the BER of the Bluetooth network.

$$PER = 1 - (1 - P_b)^{\frac{T}{T_b}}(1 - P_{b0})^{\frac{(T_B - T)}{T_b}} \quad (26)$$

When a Bluetooth master device needs to exchange data with a slave device, a time division duplex (TDD) is used to achieve full-duplex communication, where two different frequency channels are utilized by the up-link and return-link at the same time. When many slave devices need to exchange data with a master device, time division multiple access (TDMA) is applied to assign multiple channels for many slave devices. Because a Bluetooth packet transmission is synchronized with the allocated slot and each packet is transmitted in each slot time, the device waits until the next slot time and then retransmits the packet

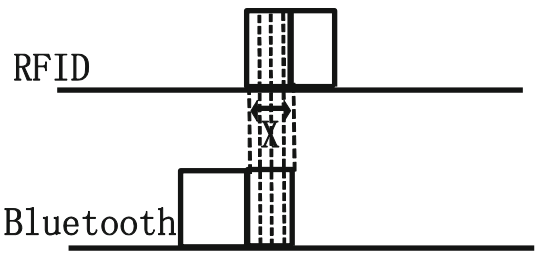

Fig. 3 The frequency collision model for RFID and Bluetooth packets

when a packet error occurs. The interval time from the beginning of the packet transmission to the packet retransmission can be defined as an integer multiple of the slot time.

$$T_{waiting} = iT_{slot} \tag{27}$$

4 Coexistence testing between RFID and wireless networks

In this section, the hardware setup is designed as a hybrid RFID combined with wireless network infrastructure. To demonstrate the impact on the performance of the WiFi or Bluetooth network with RFID interferers, different types of coexistence experiments have been performed. The coexistence tests have been run with actual products to determine their level of coexistence.

4.1 Hardware setup

Our custom hardware design is inspired by Rowitch's patent [26], which is used in the design of an RFID/WiFi/Bluetooth coordinator to target the control of different wireless modes. The hardware contains a coordinator and a set of paired modules such as the RFID, WiFi and Bluetooth modules, which are responsible for their respective initial wireless transmissions. To simulate a strong interference environment in the 2.4 GHz band, the coordinator is designed as a hybrid RFID combined with the wireless network infrastructure, which is a complete embedded system integrating the RFID module, WiFi module and Bluetooth module on a circuit board. In addition, all the protocols on the infrastructure are compatible with existing IEEE 802.11 and Bluetooth standards as well as existing RFID standards. We construct Bluetooth and WiFi protocols compatible with RFID by retaining the frame structures and channel access mechanisms while adding the capability of back-scatter radiation and amplitude-shift keying (ASK) carrier modulation to the RFID front-end. The setup is essentially an RFID solution that can operate within the standardized RFID communication specifications, but it can also operate the WiFi and Bluetooth standards.

The hybrid RFID infrastructure is shown in Fig. 4; it consists of two signal generators: RFID signal generation using Backscatter Radiation mode and WiFi/Bluetooth signal generation using RX/TX Communication mode. The infrastructure can maintain protocol compatibility by switching the antenna impedance in synchronization with a Bluetooth/WiFi frame organized bit stream.

First, the hybrid infrastructure can be automatically switched to Backscatter Radiation mode; a continual radio

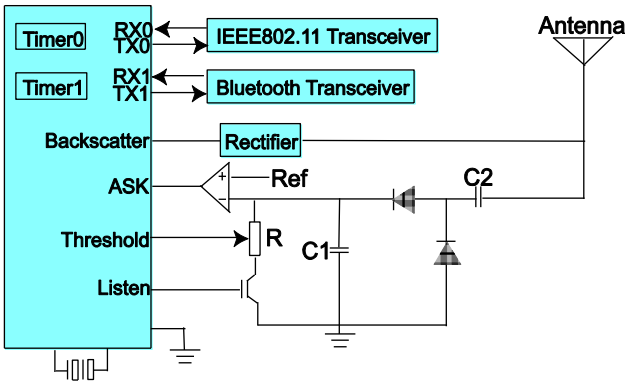

Fig. 4 A hybrid backscatter-based RFID combined with WiFi/Bluetooth infrastructure

wave energy is then emitted in a frequency-hopping pattern. Through their antenna, RFID tags are fed with a continual radio wave that represents a wake-up command. Once a tag wakes up, it can maintain communication with the infrastructure by means of radio waves. To improve the level of coexistence between the RFID and WiFi/Bluetooth networks, an asynchronous wake-up mode is designed whereby the RF signal on the infrastructure antenna is utilized to trigger the RFID chip, WiFi chip, or Bluetooth chip, and then the system records their responses. It is noted that the performance of the wireless devices can be observed by using the described setup.

The final major components of our custom hardware are appropriate RFID/WiFi/Bluetooth transceivers. We design our system with a generic interface suitable for use with a variety of RFID/WiFi/Bluetooth modules. Our choice of RFID/WiFi/Bluetooth modules is dominated by two factors. First, it is fairly easy to integrate from a hardware design perspective. Second, it must provide an integrated 2.4 GHz transceiver. In our experiments, we use the nRF24LE1 module as an RFID module, the TiWi-BLE module as a WiFi module and the Broadcom BCM2046 chip as a Bluetooth module.

4.2 Performed experiments

Using the proposed setup, four sets of major experiments have been performed: two sets of baseline performance tests of the WiFi/Bluetooth network without interferers and two sets of coexistence performance tests of the WiFi/Bluetooth network with RFID interferers. The tests were intended to obtain empirical data on network performance corresponding with certain realistic scenarios in which both RFID and WiFi/Bluetooth connections may coexist.

Experiment 1 (WiFi Baseline Performance) In this experiment, baseline tests for the WiFi network have been performed when there is no interference. The experiment consists of a serial of baseline tests, such as the signal-to-

interference power ratio (SIR), the bit error rate (BER), the packet error ratio (PER), the average delay and throughput. In each baseline test, four communication rates are used in the WiFi network: 1, 2, 5.5 and 11 Mbps. By changing the distance from the WiFi Access Point to the infrastructure, the data SIR, BER, PER, throughput and delay can be measured. This experiment can detail the optimal parameters of the performance of the WiFi network without RFID interferers according to the distance.

Experiment 2 (WiFi Performance with RFID Interferers) This experiment demonstrates the impact on the performance of the WiFi network when RFID devices are operating in a neighboring area. In the experiment, the transmitted power of RFID transmitters is 300 mW, and the transmitted power of WiFi transmitters is 100 mW. The RFID tags were located within ten meters of the WiFi Access Point. By changing the distance from the WiFi Access Point to the infrastructure, the data SIR, BER, PER, delay and throughput are measured. We expect the impact on the performance of the WiFi network to be substantial when RFID interferers are very close to the WiFi Access Point.

Experiment 3 (Bluetooth Baseline Performance) In this experiment, baseline tests for the Bluetooth network are performed when there is no interference in the neighboring area. In analogous fashion to the WiFi baseline performance testing, all testing was performed with Bluetooth devices.

Experiment 4 (Bluetooth Performance with RFID Interferers) This experiment demonstrates the impact on the performance of the Bluetooth network due to interference from RFID devices. In the experiment, the transmitted power of RFID transmitters is 300 mW, and the RFID tags were located within ten meters of the infrastructure. By changing the transmission rate of the RFID transmitters and the distance from the infrastructure to Bluetooth devices, the data SIR, BER, PER, delay and throughput are measured. The results of this experiment show that the performance of the Bluetooth network is impacted when an RFID transmitter is very close to Bluetooth devices (less than 0.5 m). If the RFID transmitter is moved away, the performance of the Bluetooth network can be improved significantly to approximately ninety percent of the baseline performance independent of range.

4.3 The seriousness of the interference

The experiments demonstrate that the seriousness of the interference can be accurately measured by means of several parameters, i.e., SIR, BER, PER, the average delay and throughput. Figure 5 displays the curve of BER versus SIR for the WiFi network with RFID interferers in the case of four different communication rates. It can be seen from the

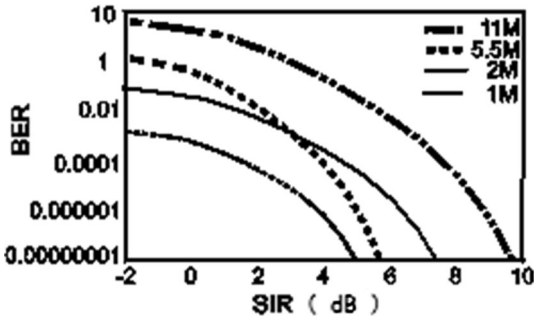

Fig. 5 BER versus SIR for the WiFi network with RFID interferers

curve that the data BER of the WiFi network is minimized when the WiFi network is working at 1 Mbps and at the same time the reliability of the WiFi network is also the highest. When a channel is in deep fading or communicating parties are far apart, the WiFi network can be run at the lowest rate (1 Mbps) to improve the lower performance that arises from interference by RFID devices.

Similarly, the changing curve of BER vs. SIR for the Bluetooth network is shown in Fig. 6. The solid line represents the data BER of the Bluetooth network with the minimum modulation index, and the dashed line denotes the data BER of the Bluetooth network with the maximum modulation index. In the IEEE 802.15.1 standard, the modulation index is a variable in a range of variation where the minimum modulation index is 0.28 and the maximum modulation index is 0.35. According to the experimental circumstance, the modulation index can be set to a specific value.

Although there are some differences in the coexistence tests, the seriousness of the interference from RFID devices remains the same. These experiments show that when RFID and WiFi/Bluetooth devices are located at a reasonable distance from each other, both can obtain a large majority of throughput, and interference is negligible. However, these experiments also demonstrate that the interference from RFID devices can significantly degrade the performance of the WiFi/Bluetooth network if the

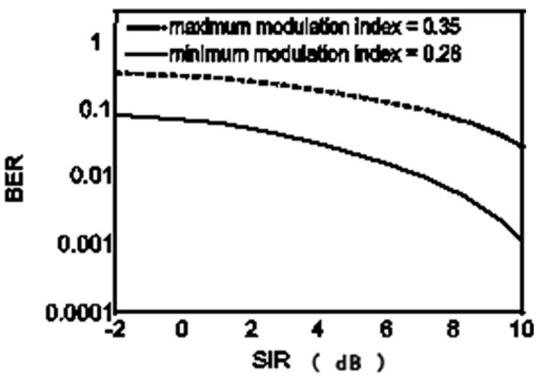

Fig. 6 BER versus SIR for the Bluetooth network with RFID interferers

RFID device is close to the WiFi/Bluetooth devices. In the following sections, the causes of the interference are analyzed in the time domain and in frequency domain, and then two solutions for improved coexistence are proposed.

5 Methods for improved coexistence

To maintain fairness between RFID and WiFi/Bluetooth networks, two approaches to achieving successful coexistence between RFID and WiFi/Bluetooth networks through time division and frequency isolation are presented [27–29]: One is frequency hopping combined with a white space exploitation method for improved coexistence of RFID and WiFi networks; the other is an intelligent frequency hopping scheme for improved coexistence of RFID and Bluetooth networks. The core of the two solutions is the interference avoidance scheme, which requires knowledge of the theoretical maximum collision time and the collision probability for RFID and WiFi/Bluetooth packets. The primary elements of the interference avoidance scheme are the interference detection scheme and smart channel selection. The interference detection scheme is used to facilitate optimal interference detection. Using smart channel selection can make the RFID interrogator itself determine which channel is preferable, depending on the current usage of the adjacent frequency channels.

5.1 Frequency hopping combined with the white space exploitation method for improved coexistence of RFID and WiFi devices

To improve the coexistence level of RFID and WiFi devices, a method that combines frequency hopping with white space exploitation is proposed. This method consists of two parts: the interference avoidance scheme and white space exploitation. The interference avoidance scheme is used for the RFID interrogator to choose the clearest channel and dynamically avoid decreasing the WiFi performance. White space exploitation could auto-size the RFID packet based on the white space length detected in the WiFi traffic.

(1) The Interference Avoidance Scheme

The primary elements of the interference avoidance scheme are the interference detection scheme and smart channel selection. Each RFID interrogator utilizes a response-counter to record the number of failed transmissions (RFID tag) and detects interference using energy detection. If the channel is available, the interrogator transmits the command successfully before the response-counter reaches the threshold value. If the response-counter exceeds the threshold value, the interrogator instructs the tags to perform an energy detection scan for the available channels in accordance with the channel classification table and then selects the channel with the least interference according to feedback from the energy detection scans. Once the channel is determined, the tags perform an active scan to ensure no other RFID device occupies this channel.

a. The Interference Detection Scheme

Due to the RFID's low duty cycle, where transmitting a packet (RFID command/response) only requires a few milliseconds, the RFID interrogator can successfully send an RFID command or response during the retransmission in most situations. To minimize redundant procedures of interference detection for the RFID, it is efficient to use a regular packet rather than signal detection. Therefore, a regular packet can be utilized to detect interference for RFID devices. When the RFID response is not received within the specified timer value, the response-counter can be incremented in values of one, and the interrogator retransmits the command. If the response-counter exceeds the threshold value, the interrogator stops retransmission and performs energy detection to ensure it is interference leading to transmission failure. Once the energy detection result RSSI exceeds the threshold, the interrogator calls the corresponding interference avoidance scheme and then initiates migration to a safe channel.

b. Smart Channel Selection

WiFi uses a 2.4 GHz frequency band, and there are 13 overlapping channels with 22 MHz of bandwidth. Only 3 non-overlapping channels, namely, channels 1, 6, and 11 in the US and channels 6, 7, and 13 in Europe. In the RFID system, data transmission from interrogator to tag is performed in the forward link, and data transmission from tag to interrogator is assigned to the return link. The tests show that when the offset frequency is larger than 8 MHz, the interference with the WiFi network is negligible. When the offset frequency is <3 MHz, the WiFi packet transmission experiences significant interference. The interference avoidance scheme utilizes energy detection and active scans to determine which channel is appropriate for each tag. To improve detection efficiency, the RFID channels are divided into four groups based on offset frequency. Group 1 consists of the channels whose offset frequency is larger than 12 MHz; group 2 consists of the channels whose offset frequency is larger than 8 MHz and smaller than 12 MHz; group 3 consists of the channels whose offset frequency is larger than 3 MHz and smaller than 8 MHz; group 4 consists of the channels whose offset frequency is smaller than 3 MHz. Group 1 has the highest priority, and group 4 has the lowest priority. Upon receipt

of an interference detection report, the interrogator transmits an energy detection scan request to all the devices to check the status of channels from high priority to low priority until an available channel is found.

(2) White Space Exploitation

To obtain high spectral efficiency, resource sharing is necessary. For example, a significant amount of white spaces are left between WiFi frames, as shown in Fig. 7. Using these white spaces, the throughput of an RFID can be maximized while bounding the packet collision probability. White space exploitation involves two components that reside between the physical and MAC layers: the white space modeling component and the packet adaptation component. The white space modeling component can build a white space-aware model based on maximum likelihood estimation. The packet adaptation component can compute the size of a packet that maximizes throughput efficiency while limiting the collision probability.

a. Splitting the Packet and Optimizing Size

If an RFID packet (RFID command/response) cannot finish its transmission before the arrival of the next WiFi packet, the transmission time of the RFID should be shorter than the remaining lifetime of the current WiFi white space in order to reduce the collision probability. The simplest method is to split the packet into sub-packets, and the size of each sub-packet is determined by predicting the remaining lifetime of the white space. Each sub-packet carries a session ID and delimiters.

b. Packet Session Management

When a packet needs to proceed, session management can compute the sizes of all the sub-packets and then start a session to transmit them. Each sub-packet is composed of a 1-byte header and payload. The header includes a 1-bit start session delimiter, 1-bit end session delimiter and 6-bit session ID. Each sub-packet in a session carries the same session ID. The session ID is assigned by the sender. The sender initiates the session by transmitting a session registration frame (SRF), which is identified by setting 1 in the start session delimiter bit. The receiver maintains the states of sub-packets in a session to keep the integrity of the original MAC frame. Due to the criticality of SRF, the collision probability of SRF can be controlled as follows:

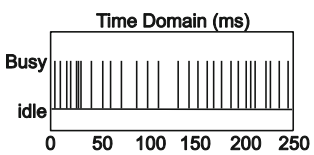

Fig. 7 The channel utilization trace captured in WiFi frames

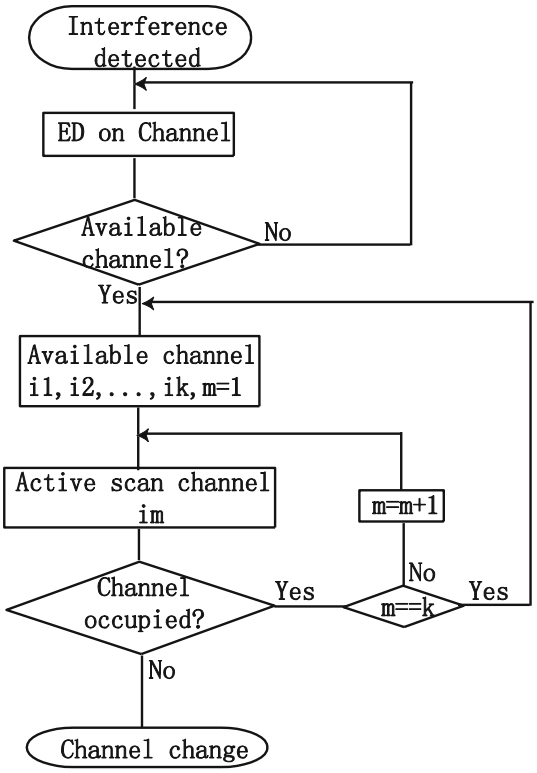

Fig. 8 The Intelligent Frequency Hopping scheme for RFID and Bluetooth devices

When the packet size is smaller than the sum of the physical header, sub-packet header and MAC header, the transmission is deferred by a random backoff, and then the sender repeats this process until it can transmit the entire MAC layer header within one sub-packet.

5.2 An intelligent frequency hopping scheme for improved coexistence of RFID and Bluetooth devices

To improve the coexistence level of RFID and Bluetooth devices, an Intelligent Frequency Hopping scheme is carried out in this section. Because RFID and Bluetooth devices use the frequency hop transceivers based on Frequency Hopping Spread Spectrum (FHSS) structuring, both of them do not continually transmit at the fixed frequency and hop across a given frequency band. Because of the lack of knowledge of the interference in the band, frequency hopping is a blind hop, and it is likely that the transceiver will collide with the transmission of another transceiver at any particular time. If the hop sequences can be designed to actively avoid other devices in the band, the performance of RFID and Bluetooth devices can be improved by hopping through a given sequence rather than hopping randomly.

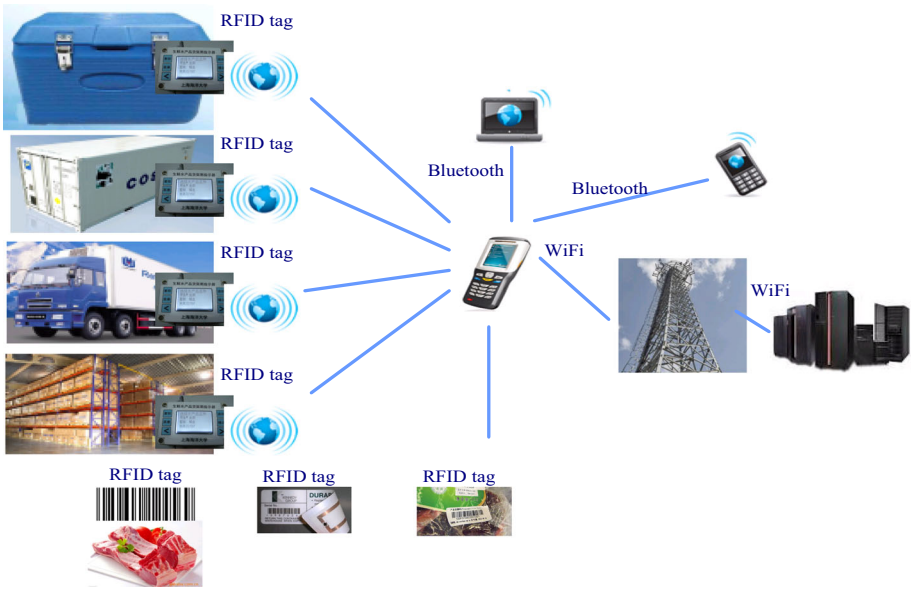

Fig. 9 Communication structure of agriculture of IOT

Table 2 Interference calculated at the transceivers after running SMART channel selection

Transceiver type	Assignment results		
	Frequency assignment (GHz)	Interference (dBm)	Lasting time (S)
RFID	2.471	− 31.7856	31
RFID	2.445	− 28.7621	28
RFID	2.4245	− 23.6732	19
RFID	2.457	− 27.0845	32
Bluetooth	2.407	− 20.6549	17
Bluetooth	2.444	− 27.0123	21
Bluetooth	2.439	− 25.7921	23
Wi-Fi	2.452	− 23.4335	219
Wi-Fi	2.422	− 24.6164	225
Wi-Fi	2.462	− 25.9625	432
Wi-Fi	2.437	− 21.0332	543
Wi-Fi	2.412	− 26.9548	523

Based on the interference avoidance scheme mentioned above, the Intelligent Frequency Hopping scheme adds the active scan process to determine which channel is appropriate for the devices to change to. The scheme consists of energy detection (interference detection), active scan and smart channel selection. To improve hopping efficiency, such hopping sequences are divided into "good" (clear) hop frequencies and "bad" (interfered) hop frequencies. Upon receipt of an interference detection report, the master (Bluetooth device) sends an energy detection scan request to all slaves to check the status of channels till an available channel is found. After completion of the energy detection scan, the slaves commence an active scan on the proposed channel selected by the master, and then the master can send out a slot request to determine whether any other slaves or RFID transceivers are currently active in that channel. If a conflict is detected, the master can select a new channel. The Intelligent Frequency Hopping scheme is detailed in Fig. 8.

5.3 Network performance evaluation with certain realistic scenarios

Place the sensor nodes with RFID, WiFi or Bluetooth modules in the test for farmland in 500 × 800 m, as shown in Fig. 9, according to the characteristics of actual field information collection, information acquisition and the routing process of the scene. In the experimental area, the RFID transmitters transmit power at 300 mV, and the signal wireless transmitting distance is significantly shortened.

The test is divided into two parts: non-prediction channel selection test (direct use of chip's built-in protocol)

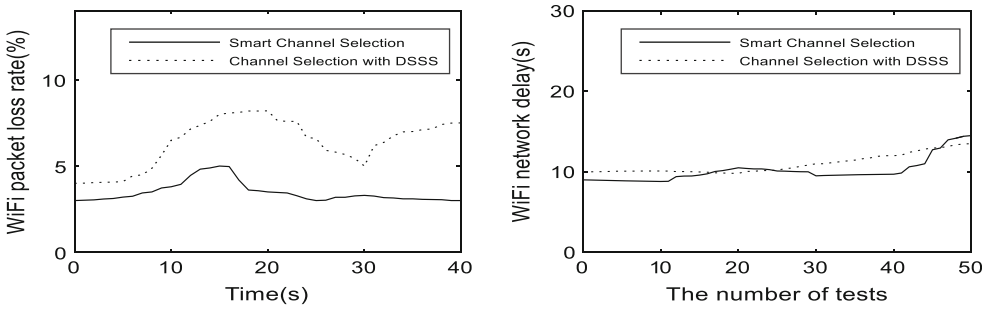

Fig. 10 WiFi network performance test results

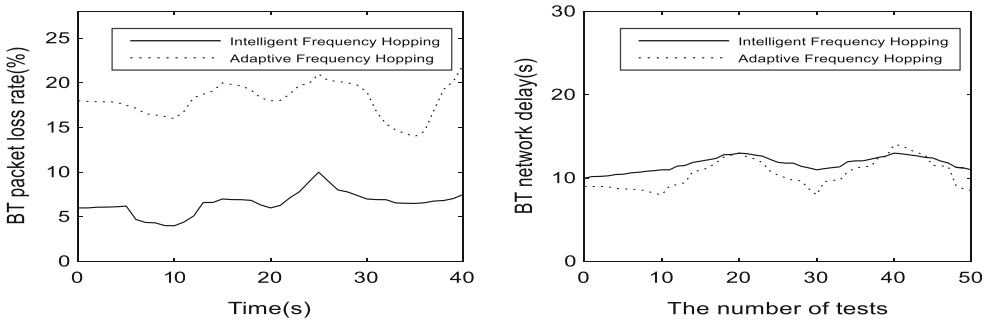

Fig. 11 Bluetooth network performance test results

and SMART channel selection test. The average bandwidth occupied in the three network modes experimental data is presented in Table 2.

Figures 10 and 11 are the network performance test results of two kinds of network modes with RFID interferers. The test results show that the WiFi network with smart channel selection has better performance (P_loss_max = 5%) compared to channel selection with DSSS (P_loss_max = 11%); the network delay of both are similar. The results also show that the performance of the Bluetooth network with intelligent frequency hopping significantly improves from P_loss_max = 21% to P_loss_max = 7%; network delay using intelligent frequency hopping is more than that using Adaptive Frequency Hopping (AFH, a built-in frequency hopping pattern found in most Bluetooth devices today).

6 Conclusion

In this paper, we presented a quantitative analysis of the theoretical maximum collision time and probability for a WiFi or Bluetooth network with RFID interferers. To determine the effect of the interference from RFID devices, the bit error rate of the wireless network and the Loss Path are calculated in the physical layer. The data BER is used to check the accuracy of wireless communication, and Path Loss is the basis of evaluation of the interference from RFID devices in the physical layer. The packet collision model for RFID and WiFi packets and the packet collision model for RFID and Bluetooth packets have been constructed in the MAC layer. Using our hybrid infrastructure, coexistence testing is performed with actual products to determine their level of coexistence. To maintain fairness between RFID and WiFi/Bluetooth devices, two solutions are present in this paper. Frequency hopping combined with the white space exploitation method is used for improved coexistence of RFID and WiFi devices, and an intelligent frequency hopping scheme is used for improved coexistence of RFID and Bluetooth devices. The core of the two solutions is the interference avoidance scheme, which requires knowledge of the theoretical maximum collision time and probability of the RFID and WiFi/Bluetooth packets. The interference avoidance scheme incorporates the interference detection scheme and smart channel selection: The former is used to facilitate optimal interference detection, and the latter can make the interrogator itself determine which channel is the best to use depending on the current usage of the adjacent frequency channels. These coexistence tests show that by using the interference avoidance scheme, the two solutions can aid in the avoidance of interference from RFID devices, making it possible for WiFi and Bluetooth networks to perform well in the presence of heavy RFID interferers.

Acknowledgements The authors would like to thank the TEXAS A&M RFID Sensor Lab for use of its laboratory space, as well as Professor Ben Zoghi (director of RFID/Sensor Lab) for his fruitful discussions and advice. We thank Dr. Feng guofu, Cao Guangpu, Wang Lei and Yan Haowei for their work. Thanks are also to the anonymous reviewers for their insightful suggestions for this work. This work is supported in part by the key program of National Natural Science Foundation of China under Grant No. 61561027, and the

Natural Science Foundation of Shanghai under Grant No. 16ZR1415100.

References

1. Balamurugan, S., Divyabharathi, N., & Jayashruthi, K. (2016). Internet of agriculture: Applying IoT to improve food and farming technology. *International Research Journal of Engineering and Technology (IRJET), 03*(10), 713–719.
2. IEEE Local and Metropolitan Area Network Standards Committee. (1997). Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11-1997, the Institute of Electrical and Electronics Engineers, New York.
3. Howitf, I. (2001). WLAN and WPAN coexistence in UL band. *IEEE Transactions on Vehicular Technology, 50*(4), 1114–1124.
4. Glomie, N., Van Dyck, R. E., Soltanian, A., Tonnerre, A., & Rebala, O. (2003). Interference evaluation of bluetooth and IEEE 802.11b systems. *Wireless Networks, 9,* 201–210.
5. Glomie, N., Van Dyck, R. E. & Soltanian, A. (2011). Interference of bluetooth and IEEE 802.11: Simulation modeling and performance evaluation. In *Proceedings of the fourth ACM international workshop on modeling, analysis, and simulation of wireless and mobile system*, MSWIM'01, Rome, Italy.
6. Cordeiro, C. D. M., & Agrawal, D. P. (2003). Interference modeling and performance of Bluetooth MAC protocol. *IEEE Transactions on Wireless Communications, 2,* 1240–1246.
7. Golmie, N, & Mouveaux, F. (2010). Interference in the 2.4 GHz ISM band: Impact on the Bluetooth access control performance. In *Proceedings of IEEE ICC'01*, Helsinki, Finland.
8. Yoon, D. K., Shin S. Y., & Kwon, W. H. (2006). Packet error rate analysis of IEEE 802.11b under IEEE 802.15.4 interference. In *Proceedings of IEEE vehicular technology conference* (pp. 1186–1190).
9. Myoung, K.-J., & Shin, S.-Y. (2007). IEEE 802.11b performance analysis in the presence of IEEE 802.15.4 interference. *IEICE Transactions on Communications, B*(1), 176–179.
10. Shin, S. Y., & Kwon, W. H. (2005). Packet error rate analysis of IEEE 802.15.4 under IEEE 802.11b Interference. In *Wired/wireless internet commununications* (pp. 279–288).
11. Shin, S. Y., Park, H. S., & Kwon, W. H. (2007). Packet error rate analysis of Zigbee under WLAN and Bluetooth interference. *IEEE Transactions on Wireless Communications, 6*(8), 2825–2830.
12. Han, Y., Ekici, E., Kremo, H., & Altintas, O. (2016). Spectrum sharing methods for the coexistence of multiple RF systems: A survey. *Ad Hoc Networks, 153,* 53–78.
13. Huo, H., Xu, Y., Mikael, G., & Zhang, H. (2010). Coexistence of 2.4 GHz sensor networks in home environment. *Journal of China Universities of Posts and Telecommunications, 17*(1), 9–18.
14. Cao, B., Li, Y., Wang, C., & Feng, G. (2015). Dynamic cooperative media access control for wireless networks. *Wireless Communications and Mobile Computing, 15,* 1759–1772.
14. Li, Y., Cao, B., & Wang, C. (2016). Handover schemes in heterogeneous LTE networks: Challenges and opportunities. *IEEE Wireless Communications, 23*(2), 112–117.
16. Cao, B., Ge, Y., Kim, C. W., Feng, G., Tan, H. P., & Li, Y. (2013). An experimental study for inter-user interference mitigation in wireless body sensor network. *IEEE Sensors Journal, 13*(10), 3585–3595.
17. Hayashi, H. (2015). Standardization of wireless coexistence in industrial automation. In *Proceedings of the society of instrument and control engineers annual conference.*
18. Wireless LAN medium access control (MAC) and physical layer (PHY) specification, IEEE Standard 802.11. June 1999.
19. Wireless LAN medium access control (MAC) and physical layer (PHY) specification: High-speed physical layer extension in the 2.4 GHz band, IEEE Standard 802.11, Sept. 1999.
20. Xiao, Y., & Rosdahl, J. (2002). Throughput and delay limits of WiFi. *IEEE Communications Letters, 6*(8), 355–357.
21. Bing, B. (1999). Measured performance of the WiFi wireless LAN, in Local Computer Networks-LCN'99 (pp. 34–42).
22. Cali, F., Conti, M., & Gregori, E. (1998). WiFi wireless LAN: Capacity analysis and protocol enhancement. In *Prof. of INFOCOM'98, seventeenth annual joint conference of the IEEE computer and communications societies* (vol. 1, pp. 142–149).
23. Tay, Y., & Chua, K. C. (2001). A capacity analysis for WiFi MAC protocol. *Wireless Networks, 7,* 159–171.
24. Won, C., Youn, J. H., Ali, H., & Sharif, H. (2005). Adaptive radio channel allocation for supporting coexistence of 802.15.4 and 802.11b In *Vehicular technology conference*, (vol. 4, pp. 2522–2526).
25. Batra A, Ho, J.-M., & Anim-Appiah, K. (2011). Proposal for intelligent BT frequency hopping for enhanced coexistence, IEEE 802.15-01/082.
26. Rowitch, D. N., Simic, D. N, & Pals, T. P. (2010). Multiple radio device having adaptable mode navigation radio, United States Patent, 7859453.
27. Eliezar, O. (2001). Non-collaborative mechanisms for the enhancement of coexistence performance, IEEE 802.15-01/092.
28. Ryu, E. K., & Takagi, T. (2009). Hybrid approach for privacy-preserving RFID tags. *Computer Standards and Interfaces, 31*(4), 812–815.
29. Hsu, Y.-C., Chen, A.-P., & Wang, C.-H. (2008). A RFID-enabled traceability system for the supply chain of live fish. *IEEE International Conference on Automation and Logistics, ICAL, 2008,* 81–86.

Tao Chi received his Ph.D. in Control Theory and Engineering from Tongji University in 2006. He is currently an Associate Professor in the College of Information Technology, Shanghai Ocean University. His research interests include wireless sensor networks, embedded system and artificial intelligence.

Ming Chen received his Ph.D. in Computer Software and Theory from Fudan University in 2001. He is currently a Professor in the College of Information Technology, Shanghai Ocean University. His research interests include intelligent computing, artificial intelligence, big data and image retrieval.