Research Article

The Methods toward Improving Communication Performance in Transparent Radio Frequency Signals

Nihat Daldal, Majid Nour, and Kemal Polat

1Department of Electrical and Electronics Engineering, Faculty of Engineering, Bolu Abant Izzet Baysal University, 14280 Bolu, Turkey
2Department of Electrical and Computer Engineering, Faculty of Engineering, King Abdulaziz University, Jeddah 21589, Saudi Arabia

Correspondence should be addressed to Kemal Polat; kpolat@ibu.edu.tr

Received 25 February 2020; Accepted 3 April 2020; Published 24 April 2020

1. Introduction

It is well known in FRISS equations for wireless communication that the power received depends on the gain of the transmitter and the loss of the receiver [1]. The received signal strength in free space at a distance \( r \) from the transmitter is expressed in the logarithmic form as

\[
P_r = P_t + G_t + G_r - P_L,
\]

where \( P_t \) is the transmit power, \( G_t \) and \( G_r \) are the gains of the receiver and transmitter antennas, and \( P_L \) is the path loss in dB, which is given by

\[
P_L = 20 \times \log_{10} \left( \frac{4 \pi f \times d}{c} \right) \text{dB},
\]

where \( d \) is the distance between the transmitter and the receiver in meters, \( f \) is the operation frequency in MHz, and \( c \) is the speed of light in a vacuum, \( 3 \times 10^8 \text{ m per second} \).

As a result of the logarithmic expression of FRISS equations, the following equation is used between the sent power and the received power:

\[
\left( \frac{P_R}{P_T} \right)_{\text{dB}} = (G_T)_{\text{dB}} + (G_R)_{\text{dB}} - (32.5 + 20 \log_{10} d + 20 \log_{10} f).
\]

In this equation, the frequency unit is MHz while \( d = \text{km} \). According to FRISS equations, the power of the transmitter in wireless communication, the antenna gain of the transmitter, the antenna gain of the receiver, and the distance are the most important parameters that affect the communication [1, 2].

In short-range radio communication, RF power outputs several microwatts up to 100 milliwatts and the communication range is of several centimeters up to several hundred meters. It uses principally indoor operations and built-
in omnidirectional antennas [3]. According to the classification of the IEEE802.15.4 protocol, the RF 433 MHz network belongs to LR-WPAN (low-rate wireless personal networks). An LR-WPAN network is a simple and low-cost communications network that allows the realization of wireless networking on the premise of limited power dissipation [4, 5].

2. Low-Power RF Transmitter

The communication frequency in low-power transmitters is adjusted by surface acoustic wave (SAW) resonators. These resonators provide reliable, basic mode, quartz frequency stability of fixed frequency transmitters. Figure 1 shows the most widely used SAW resonator transmitter structure. These resonators prevent the shift of the carrier signal frequency and ensure a more stable operation of receiver systems [6, 7].

SDR (software-defined radio) has been used to display the broadcast frequency of the transmitting antennas. Figure 2 shows that SDR and transmitter carrier frequency are approximately 433.9 MHz.

3. Low-Power RF Receivers

Figure 3 shows the RF receiver structure with a diode detector. The simplest method of receiving an RF signal is the envelope receiver structure with a diode detector. The low diode transmission voltage increases the sensitivity of the receiver. It is used to obtain signals from the RF transmitter at short distances [8]. To increase the distance of the detector output, OPAMP amplifier circuits are added. Figure 4 gives the detector output signals.

In Figure 4, the diode detector output has been monitored by sending data with a 433.92 MHz SAW resonator transmitter. When transmitting data from 10 cm to 20 cm distance with 10 MW output, the output of the nongain detector has been displayed. Since the signal strength is extremely weak relative to the distance, high gain is required in receiver circuits.

3.1. Transparent RF Materials

Transparent modules are a wireless wire. The data that are input to the module are used to directly modulate the carrier. There is no wireless protocol built into the module and no buffering or storage of the data. Usually, there are no processors of any kind in these modules, it is just the physical radio [9]. The advantage of this is that the designer has complete control of the over-the-air data. A wireless protocol can be created that is most efficient for the system and is scaled for the amount of data sent by the product or the capabilities of the processor in the product, or both [10]. A company can create a protocol that defines a new market. The products are open so that they can be very dynamic. Figure 5 denotes the 433 MHz RF receivers and transmitters.

In low-power transparent modules, receiver sensitivity is −108 dBm while transmitter power is 10 MW. In the open field, 2400 baud is used in series for the ideal communication while communication is provided at a distance of 100 m. When data are applied at a specific baud rate as serial communication to the transmitter module input, data are taken up to a certain distance on the receiver output. In these modules, preamble and synchronous data are added to the beginning of the data to be sent in order to provide hardware and software synchronization instead of directly sending the data [10].

In this way, the data starting point is determined at the output of the receiver module. The RF receiver module generates a continuous signal from its output in case the data do not arrive. This signal is the noise signal given to the output by the receiver circuit. All transparent receiver modules have this noise signal.

The user must send preamble data before sending data from the transmitter circuit and then send the sensor data. In this case, the receiver can receive the actual data from the output. Transparent modules are asynchronous modules. According to the speed of the module (min. 300 bps-max.), it should organize by calculating 2400 bps. The standard data protocol should be TX: preamble + sencron + data1+⋯+dataX.

In the simplest communication systems, it is almost imperative to use a preamble data to start the message. Preamble data are a sequence of consecutive 1 and 0 bits. 5 bytes can be 0x55 or 0xAA. The times of sending 1 and 0 must be equal. In short, preamble data provide hardware synchronization. Synchronous data help in synchronizing the software [11–18].

Synchronization is required for the correct detection of the starting point of the message. Although the length of this bit array may vary according to application requirements or constraints, it can usually be 5 bytes 0x00 and 5 bytes 0xFF or the user decides the length. When sending data, there must be no space between them, and if so, preamble and synchronous data must be sent again. Preamble data are not checked on the receiving side. Only synchronous data are searched, and then the original data are read. Figure 6 shows the signals to be given to the transmitter module, while the transmitter module RF output, receiver module RF input, and receiver module data output signals are shown.

In Figure 7, the RF receiver module was observed in the oscilloscope in real time when there was no transmitter signal and the transmitter received the signal.

3.2. Basic Transparent RF Module Communication.

In the transparent RF modules, the receiver’s data output is connected to a port of the microprocessor, and the microprocessor listens to the module output continuously. Figure 8 shows the basic data acquisition from the RF transceiver module.

The microcontroller expects continuous synchronous data from the RF module output. In this case, it is difficult for the microcontroller to perform another operation. Also, even if the transmitter does not send data, the presence of continuous noise in the RF receiver output sometimes provides synchronous data and false data retrieval can occur. This problem makes RF communications more insecure. In addition, the extra password is set for this problem, and the length of the data sent is greatly increased.
Figure 1: SAW resonator transmitter (a) and SAW equivalent LC model (b).

Figure 2: Monitoring 433 MHz RF transmitter frequency in spectrum with the SDR radio.

Figure 3: RF receiver and amplifier structure with a diode detector.

Figure 4: Detector output signals.
Figure 5: (a-b) 433 MHz RF receivers and (c) the transmitter.

Figure 6: Transparent RF protocol.

Figure 7: The output signal observed when there are no data in the RF transceiver module and the data arrive.

Figure 8: Main connection of the processor with the transparent RF module.
4. Proposed Transparent RF Communication Systems

In this study, hardware and software recommendations were presented in order to make data retrieval easier and safer from RF transparent modules.

4.1. Listening to Analog Output Pin. In this proposal, a structure is introduced to facilitate data retrieval for modules with the a0 analog output. Some transparent RF modules have extra analog outputs in the receivers, and when the receiver receives the signal, the module generates an analog voltage of ~2 V according to the signal level from this output. If the signal does not arrive, the output voltage is “0.” A valid communication distance is over 0.7 V. Figure 9 shows the proposed connection.

Instead of constantly checking the output data of the RF module, only the microcontroller will read when the data arrive, so it does not need to send long control bits. In addition, the microprocessor can perform other operations in the meantime. When the microprocessor is performing a job, an analog voltage is taken from the output of the RF receiver A0 when the data come in. In this case, the transmitter is active and warns the processor from the interrupt input of the processor. The processor leaves the job and waits for synchronization by branching into the interrupt program and then takes the data and returns to the place where it left off. Compared with conventional data retrieval, the processor does not expect only data from the RF module but can perform different tasks in the meantime. It is also not affected by the noise signal because it only performs the reception when the data come in.

4.2. Getting the Average of the Data Output. In this system, a structure that will facilitate data retrieval for modules that do not have analog outputs has been established. Constant noise is present in the module data output, and a DC voltage is obtained by taking the average of the module output. Moreover, when data are not received from the transmitter, the average value of the noise signal is about DC 1.2 V, and at the moment the data are received, this level falls to DC 0.85 V due to gaps between the data packets. Figure 10 shows the proposed connection.

Even if the sent data value is changed, this voltage remains at almost this value. The comparator OPAMP in the + reference input is set to approximately 0.95 V. When there are no data, the output of the integrator, i.e., the noise voltage, is measured at approximately 1.1 volts. This voltage was applied to the negative input of the comparator OPAMP. In this case, the output of OPAMP is 0 volts.

When data arrive, the integrator output voltage drops below the reference voltage set to approximately 0.85 V, and the OPAMP output goes to + V. In this case, the processor leaves the job and goes to the interrupt program and receives the data from the RF module and returns to the main program again.

Here, the integrator RC circuit output equation is shown in the following equation [19]:

\[
V_{out} = \frac{1}{C} \int \left( \frac{V_{in}}{R} \right) dt = \frac{1}{RC} \int V_{in} dt. \tag{4}
\]

Here, the filter impedance is chosen high so that the module output is not loaded.

4.3. Data Comparison with Differential Pulse-Code Modulation (DPCM). DPCM modulation was introduced in the 1960s based on the idea that digital data transmission could be carried out at least with data transmission. This idea is based on sending the difference between neighboring examples [20]. The basis of DPCM modulation is delta modulation. Since the amplitude differences between successive samples are encoded in this modulation, the coding technique obtained is called differential PCM or DPCM [21, 22]. DPCM communication system is shown in Figure 11.

The difference between the current value of the signal from the transmitter input and the predicted value is

\[
e(i) = S(i) - \tilde{S}(i). \tag{5}
\]

It is expressed with the equation and determines the error value. The error signal can be quantified with a smaller level and then transmitted through the communication channel. This process generates some quantization error Q(I). The quantitative error signal is expressed in the following equation:

\[
e_q(i) = e(i) + q(i). \tag{6}
\]

The S(I) prediction signal is added to the quantitative error EQ(I) signal. The signal s(i) is then transmitted to the estimator and the next incoming input signal is expressed by the following equation:

\[
\tilde{S}(i) = \tilde{S}(i) + e_q(i) \quad \text{s}(i) = \tilde{S}(i) + e(i) + q(i) = S(i) + q(i). \tag{7}
\]

The better the prediction, the smaller the error transmitted and the better the coding process. If the current data are taken as a quantified error value between the predicted data value and the estimated data value, the estimation method is called differential pulse-code modulation (DPCM) [23, 24]. In this technique, the estimated value is added to the value obtained in the previous case on the buyer side, and the new value at that time is obtained [25].

In RF communication, synchronization corruption occurs because the data size to be sent exceeds the specific length. For this reason, there are limitations in a data packet to be sent to a maximum in RF modules [26]. For example, in transparent modules, the packet data size is limited to 20 to 72 bytes according to advanced RF modules. Otherwise, the wrong communication occurs because the synchronization between the receiver and the transmitter is disrupted.

If the difference between the data sent in the packet is less, the sending of the data with DPCM will reduce the total size. Figure 8 shows how to reduce the size of a data array, which is not more than 4 bits different from each other. In the compression algorithm, the 56-bit-length data in the example are converted to 38 bits.
In the conversion process, the first 8-bit data are retrieved. Then from 1 bit, to be guessed 2 reports that information has increased or decreased. The next 4-bit data show the amount of increase or decrease (max 16 must be different for 4 bit). The first 8-bit data are taken in the receiving section, and the next 5-bit data are increased and decreased in the first data, and the data packet is again obtained with a simple algorithm.

An example of this is that the change in ambient heat data is discarded as a package in a given period. Because the temperature does not suddenly make a difference of 16 degrees, if there is too much difference between the data, the number of bits of the difference data can be done more than 4 bits, but the compression rate is reduced. Figure 12 shows the compression of heat data before they are sent. In the example, a 33% reduction in the data size of 7 bytes was achieved.

4.4. Security. When the size of the data packet increases in transparent modules, bad reception starts at the end of the data array. Incorrect data purchases lead to incorrect work in control systems. To prevent this situation, adding BCC (block check character) to the end of the communication packet raises the probability that the entire data array will be received correctly. In the BCC code, the Exor process is executed between all the data to be sent.

After the Exor process, the BCC code is generated for the packet, and at the send, this code is added to the end of the packet. At the end of the package, the BCC code is received along with the recipient-side data. The BCC code is generated again by the Exor process between all received data. Moreover, it is compared with the received BCC code. If the BCC codes are equal, then the data are correctly received and evaluated.

In particular, in the increase of RF communication distance, disturbances in the data series are very frequent. With the addition of the BCC code, the data array that is corrupted is not received, and the array that is nondestructive is received. Since the data sequence is sent more than one time in RF communications, the data packet is received without an error.

In the study, 10 transmissions were made in the data series sent by 30 bytes at long distances (100 m), and 4 data series were corrupted. With the addition of the BCC code, only the correct data array is obtained. Figure 13 shows how to obtain the BCC code for the compressed data package.
In this study, negative conditions in RF communication over transparent RF modules were investigated, and studies for improving communication performance were put forward. The microprocessor’s RF receiver module is prevented from listening continuously while data retrieval is taking place. In this way, the processor can do other tasks. Only when data come in, the processor goes to the interrupt program and receives the data. Also, data compression was provided with the DPCM method for data transmission. In this way, it is shown that the data size can be increased because the data array to be discarded in a package in RF modules is limited. In addition, data sent in long data sequences are corrupted towards the end of the sequence and incorrect communication is provided. Therefore, the BCC code for the data packet is generated and added to the end of the data. The receiving system generates the BCC code by taking the incoming data and compares it to the incoming BCC code. If the BCC codes are equal, the microcontroller in the receiving system receives the data. In this case, incorrect data retrieval is prevented in RF communication.

### Table 1: Comparison of the proposed methods.

<table>
<thead>
<tr>
<th>Proposed first structure: listening to analog output pin</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data can be retrieved from the first packet. The communication speed is high. The microprocessor can perform other operations.</td>
<td>Some RF modules do not have this pin.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proposed second structure: getting the average of the data output</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>The microprocessor can perform other operations. This structure can be used in each RF module.</td>
<td>Data cannot be retrieved in the first pin. It can be taken in other packages. Therefore, the speed is low.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proposed third structure: data compression with DPCM</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>The data size is reduced. More data can be sent in a packet. The speed of communication increases.</td>
<td>As the difference between the data increases, the compression ratio decreases. Software for communication is more difficult.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proposed fourth structure: increasing the communication security</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data cannot be retrieved when data array corruption occurs during communication.</td>
<td>The data length increases by one byte. If data corruption occurs, data cannot be imported in the first package. The communication speed is reduced.</td>
<td></td>
</tr>
</tbody>
</table>

### 5. Conclusions and Future Work

In this study, negative conditions in RF communication over transparent RF modules were investigated, and studies for improving communication performance were put forward. The microprocessor’s RF receiver module is prevented from listening continuously while data retrieval is taking place. In this way, the processor can do other tasks. Only when data come in, the processor goes to the interrupt program and receives the data. Also, data compression was provided with the DPCM method for data transmission. In this way, it is shown that the data size can be increased because the data array to be discarded in a package in RF modules is limited. In addition, data sent in long data sequences are corrupted towards the end of the sequence and incorrect communication is provided. Therefore, the BCC code for the data packet is generated and added to the end of the data. The receiving system generates the BCC code by taking the incoming data and compares it to the incoming BCC code. If the BCC codes are equal, the microcontroller in the receiving system receives the data. In this case, incorrect data retrieval is prevented in RF communication.
communications. In Table 1, the methods proposed in the study have been compared.

**Data Availability**

Data were obtained in real environment with microprocessor in the paper. Since the data are used online in the simulations, the data can be shared at the request of the readers.

**Conflicts of Interest**

The authors of this manuscript have no conflicts of interest related to this work.

**Acknowledgments**

This project was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, Saudi Arabia (the project number is D-585-135-1441). The authors, therefore, gratefully acknowledge DSR technical and financial support.

**References**


