UNIVERSAL AUTOMOBILE RKE REPEATER

Sean Kainuma (Electrical Engineering)  Elaine Owens (Electrical Engineering)

Abstract - The remote keyless entry system range on certain model cars is only 15ft. Due to cost and time constraints on automobile manufacturers, the range of these devices are limited. The purpose of this project was to design, build, and test a stand alone repeater for automobile remote keyless entry systems. The intent was to create a device that could operate on numerous cars to extend the range of current RKE systems to greater than 100ft. Emphasis was placed on system design and functionality, and not aesthetics. If this device were to go into commercialization (as planned); meeting FCC rules and regulations is necessary. This has already been factored into the design.

Index Terms - Repeater, Remote Keyless Entry (RKE), Radio Frequency (RF), Automobile Security

I. INTRODUCTION

In the past, remote keyless entry (RKE) systems were present only in higher end car manufacturers and models. As the technology becomes more economically feasible, more automobile manufacturers are including these systems in a wider range of their cars.

To make RKE systems available on many cars, manufacturers have to make them as cheap and long lasting as possible. This is why the range on many cars (from low to high end models) for RKE systems is very limited; usually less than 15 yards. The ranges for older model cars are even less.

The need for a RKE system repeater was due to the very short range of the sponsor’s RKE system for a Saab.

II. NOMENCLATURE

ASK-Amplitude Shift Keying  
$\nu_c$-Modulation carrier frequency  
FCC-Federal Communications Commission  
FIFO-First In First Out  
FSK-Frequency Shift Keying  
Key Fob-Device used for remote operation of a car  
OOK- On Off Keying  
RAM-Random Access Memory  
RKE-Remote Keyless Entry

III. DESIGN OBJECTIVE/SCOPE

The repeater should extend the range of the key fob signal to at least 100ft and 200ft under ideal conditions. To make the repeater marketable, it should also be universal and work for a number of car models. Power and cost should also be taken into account, but is not the main objective.

IV. BACKGROUND

For RKE systems, there is no set standard (FCC or IEEE) unlike the wireless LAN communications standard 802.11b. There are infinite ways to encrypt, encode, and modulate a signal. The only constraint on these signals is the rules and requirements set by the FCC in CFR title 47 part 15. There are however design trends used by automobile manufactures such as commonly used frequencies and modulation schemes.

The most commonly used modulation frequencies for RKE systems are 315MHz in the US and Japan, and 433.92MHz in Europe.
A. Modulation Schemes

There are two modulation schemes that have been identified in use for RKE systems. They are ASK and FSK. ASK modulation modulates a carrier signal by multiplying it by a signal representing the binary data being modulated. Eq. 1 shows the format for a ASK modulated signal.

\[ u(t) = s_m(t) \cos(2\pi f_c t) \]  

\( s_m \) - signal representing binary data  
\( f_c \) - carrier frequency

In general there may be more than 2 signals used to represent the binary data. For example 2 bits can be modulated as shown in Eq. 2,3,4,and 5.

\[ s_0(t) = \sin(t) \Rightarrow "00" \]  
\[ s_1(t) = 2 \sin(t) \Rightarrow "01" \]  
\[ s_2(t) = 3 \sin(t) \Rightarrow "10" \]  
\[ s_3(t) = 4 \sin(t) \Rightarrow "11" \]

The form of ASK modulation used for RKE systems is a specific type called on-off keying. This means that instead of modulating two signals for binary “1” and binary “0” one signal is used, a constant, and the other is zero.

For example, a binary “1” is the carrier signal while a binary “0” is the absence of a signal. This can be seen in Eq. 6 and 7.

\[ u_0 = 0 \]  
\[ u_1 = \cos(2\pi f_c t) \]

Current RKE systems use OOK in an attempt to save power because the transmission of a “0” uses virtually no power.

As may be noticed, the signal may be indistinguishable from noise as long as the message signal (“0” or “1”) is held at “0”. For demodulation purposes this will cause problems because the carrier signal may be lost, and the receiver may not be able to determine if there is a signal at all. One solution to this problem is to use an encoding scheme such as Manchester encoding.

FSK modulation changes the frequency of the carrier signal by some \( \Delta f_c \), a small fraction of \( f_c \). As with ASK, multiple bits can be sent in one signal. The equation for a multiple bits (“b” bits) FSK modulation is shown in Eq. 8.

\[ u_m(t) = \sqrt{\frac{2E_m}{T}} \cos(2\pi f_c t + 2\pi m\Delta f t) \]  

\( m = 0,1,\ldots,M - 1 \)  
\( E_m \) - Energy per symbol (per b bits of data)  
\( T \) - Period of symbol  
\( m \) - Decimal value of b bits  
\( M \) - Number of symbols(2^b)

B. Encoding Schemes

Manchester encoding and Variable pulse width encoding are the most widely used types of encoding for RKE systems.

Manchester encoding is a form of data communication where each bit of data has at least one transition. It is therefore considered to be self-clocking since the clock signal can be embedded into the signal. Each bit is transmitted over a predefined period and there will never be long periods of time without a clock transition. This prevents loss of clock synchronization and bit errors from signal drifting.

The first convention of Manchester encoding published specifies that with a low to high transition (low level for first half of bit period and high level for second half) a 0 is represented. For a high to low transition, a 1 is represented. A sample Manchester encoded signal is shown in Fig. 1.

Figure 1: Encoding of 11011000100 in Manchester

Pulse width modulation is where the width of pulses (duty cycle) are controlled to pass information over a channel. Different pulse width values correspond to specific data values. The pulses are sent at regular intervals, but the length of each pulse varies. An example is shown in Fig. 2.

Figure 2: Example of pulse width modulation
C. Code Hopping

Many car manufacturers now use a code hopping system to encrypt signals before being transmitted to the car. This encryption is done by randomly changing the code that transmits each time you arm or disarm the car alarm. There are numerous methods to accomplish this, but one way is by using a complex algorithm so that the same code never repeats. Both the transmitter on the key fob and the receiver in your car has to use code hopping in order for the system to work.

In response to the need of code hopping technology, Microchip has come up with its own line of code hopping devices under the name brand KEELOQ. KEELOQ is proprietary technology based on random bits generated by a non-linear encryption algorithm (using a 64-bit encryption key) that creates a unique transmission on every use. In RKE systems, the low end fixed encoders are used. The encoders generate a signal for the transmitter with 32 random bits, 28/32 bits serial number (specific to the key fob), and information bits used to tell the car what function to perform. The total transmission can be up to 69 bits long.

When KEELOQ encoders are used on the transmitter side of a RKE device, a KEELOQ decoder needs to be used on the receiving end. This can be done with hardware (Microchip part numbers HCS5XX) or software. The software decoders come as part of a licensing package and needs to be purchased. The price of this package is not advertised but is expected to be very costly.

Each RKE transmission follows a specific format created by the manufacturer. Using the KEELOQ encoding scheme also integrates a code hopping transmission format into the transmitted signal. This makes it easier when decoding the signal since the exact number of bits for a specific function is known and the sequence of data transmission is known.

As with regular pulse width modulation, the variable pulse width modulation used by the KEELOQ encoder varies the duty cycle of the pulses to signify if a bit is 0 or 1. For a 0, the beginning part of the signal is kept high for 2T_e and then pulled low for T_e. For a 1, the beginning part of the signal is kept high for T_e and then pulled low for 2T_e. This can be seen in Fig. 3. T_e is the length of time for a basic pulse element (shortest pulse length used).

![Variable pulse width modulation bit format](image)

**Figure 3: Variable pulse width modulation bit format**

V. HISTORY OF PREVIOUS TEAM

The design concept the previous senior design team decided to follow was to receive the key fob signal, store it, demodulate it to see if it is the user’s key fob signal, and then retransmit the signal.

A learn function was also implemented in the microcontroller so the repeater could learn the serial number of the user’s key fob in order to only repeat the user’s key fob signal. The user would first press a button on the repeater device, and then press a button on the key fob. The microcontroller would then automatically decode the signal and store the serial number of the key fob for future reference.

The design from last year worked only for a 2004 Toyota Corolla operating at 315MHz with ASK modulated signals. The repeater was successful at retransmitting the user’s specific key fob signal, but not at increasing the range of the signal.

The design for the learn function works for only the 2004 Toyota Corolla. This is because you need to know where in the key fob signal the serial number of the car is located when programming the microcontroller. Before this can be accomplished, the signal needs to be demodulated and decrypted. The encoding schemes used by different car manufacturers vary and are not willingly given out since this counter acts the purpose of the encoding and encryption. The team was able to decode and decrypt the Toyota Corolla signal because after opening up the key fob transmitter, they noticed the HCS361 Microchip encoder on the PCB. The datasheet for this chip is available to the public on the Microchip website. On the datasheet, the transmission format including the modulation/demodulation and encryption/decryption scheme is shown. This is not the case for a 2005 Honda Civic and most other cars. Due to this major obstacle, their design concept would not be useable for a universal repeater.

The suggestion made by the past team to allow for universality was to implement a USB connection from the repeater device to a computer. The user would then be able to go to a website and download specific microcontroller code for their car. Through research conducted this year, this would not be feasible for the manufacturer. Creating microcontroller code for every single car model with RKE made to date would be impossible since car manufacturers are not willing to give out their key fob operating specifications.

VI. DESIGN

The overall system level diagram for the universal repeater is shown in Fig. 4.
Using the Microchip receiver demo board and an oscilloscope the key fob signals for a 2005 Honda Civic were captured and analyzed. The screen capture for a lock signal is shown in Fig. 5. The actual signal starts after the long high pulse and ends after the long low pulse.

![Repeater system level diagram](image)

**Figure 4: Repeater system level diagram**

It was found that the signal consisted of constant bits in addition to random portions. Since the key fob used a microcontroller and not a KEELOQ encoder to generate signals, it is impossible to figure out the encoding and encryption scheme. It was obvious that continuing in the path of the previous team was not an option. Although the USB idea of downloading different car model information to a microcontroller is an option, it is not feasible. Car manufacturers giving out information of how to decode their key fob signal would defeat its purpose and allow hackers to break into people’s cars. With these findings a more feasible design concept needed to be made. The new idea was to create a generic repeater that did not have to decode every key fob transmission before repeating it. Instead, it would repeat all transmissions in the correct frequency, but only to a distance of about 10ft. This would allow the repeater to be truly universal and only work for the car that it is placed in.

![Lock command signal for 2005 Honda Civic](image)

**Figure 5: Lock command signal for 2005 Honda Civic**

A. Receiver

To meet the initial design objectives, the receiver was chosen to: minimize power consumption, maximize range and be universal while keeping cost low. A minimal current draw of the receiver while operating and in standby ensures low power consumption. High receiver sensitivity provides a longer range. A receiver that works in multiple modulation schemes with multiple frequencies fulfills the universality objective of this project. Extra functions in the receiver such as polling, where the receiver is left in standby and checks for a signal periodically, also minimize power consumption.

Research on receivers was narrowed down to four receivers that were compatible with 315MHz and 433MHz as well as able to demodulate ASK and FSK signals in one component. Of the four receivers examined in depth, as shown in Table 1, two were chosen for the first design.

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Maxim</th>
<th>Microchip</th>
<th>Chipcon</th>
<th>Atmel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part Number</td>
<td>MAX1471</td>
<td>rM0000420</td>
<td>CC1100</td>
<td>TA0423</td>
</tr>
<tr>
<td>Receiver Sensitivity</td>
<td>-108 dBm</td>
<td>-104 dBm</td>
<td>-110 dBm</td>
<td>-106 dBm</td>
</tr>
<tr>
<td>Current drawn</td>
<td>7mA</td>
<td>8.2 mA</td>
<td>15.6mA</td>
<td>10.5mA</td>
</tr>
<tr>
<td>Modulation</td>
<td>ASK/FSK</td>
<td>ASK/FSK</td>
<td>ASK/FSK</td>
<td>ASK/FSK</td>
</tr>
<tr>
<td>Frequencies (MHz)</td>
<td>315/433</td>
<td>300-450</td>
<td>315/433/968</td>
<td>315/345/433/868/915</td>
</tr>
<tr>
<td>Cost per unit</td>
<td>$5.86</td>
<td>$4.98</td>
<td>$2.49</td>
<td>N/A</td>
</tr>
<tr>
<td>Cost per unit (10000+)</td>
<td>$2.85</td>
<td>$2.79</td>
<td>$1.92</td>
<td>N/A</td>
</tr>
<tr>
<td>Notes</td>
<td>Transceiver</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 1: Comparison of receivers**

The Maxim part, MAX1471, was chosen because it optimized the design objectives. The current draw of the Maxim part is the lowest of all the receivers while operating, and has a very high sensitivity. In the original design the operational current draw was more critical to power consumption than standby current draw. Reexamining this concept, the idle current draw is much more important. Idle current in this sense is the average current drawn while the receiver is waiting for a signal. This means that the receiver needs to either be in a polling type of mode or fully operational, but not in any sort of sleep mode that can not be woken up automatically. The average polling current for the Maxim component is given at 5µA.

The second part chosen was the Chipcon CC1100 component. This device was chosen because it is a transceiver module (having both a receiver and transmitter). If this component fulfills the design objectives it will greatly reduce the number of components needed for this project. The part is also very cheap in high quantity as seen in Table 1. Less components on the board also decreases the cost of the entire board, and if a separate transmitter is not needed the cost of the board may be decreased greatly. The Chipcon part also does not require any sort of external filter as the Maxim and Microchip receivers do, as well as the ceramic filter needed for the transmitter used. Another benefit to having fewer components is...
less power consumption. The polling current for the Chipcon part is 15µA. This component in direct comparison with the Maxim receiver has a slightly better sensitivity but consumes more power. The overall power consumption of the board however may still be less with the Chipcon CC1100 than with the MAX1471 and a separate transmitter. The actual power consumption can only be validated through tests.

B. Transmitter

The transmitter chosen for this design worked for the previous design team. Upon their recommendation the Microchip rfPIC12F675 was used. This allowed efforts to be put towards other areas of the design. The current team also decided that a validated functionality was more critical to the design than transmitting power. The transmitter would be located within the car and would not need a range of more than 10-20ft.

C. Antenna

The Antenna chosen for this design was the TriCOME TCA07F and TCA12B for 433MHz and 315MHz. This part was used by the previous team for the receive antenna, and was recommended to be used in any further designs. Instead of creating a microstrip loop antenna as the previous team did for the transmitter a second TriCOME antenna was used. This decision was made to attempt to save board space. Future design work can be done by creating a three port network (such as a circulator) to route power between the receiver, transmitter, and one antenna. This will save money and real estate. If the Chipcon receiver is chosen in the final design, only one antenna will be needed.

Two inductors, one series and one shunt, make up an impedance matching circuit between the antenna and other components.

D. Microcontroller

Data collected from last year’s design team showed that a 2004 Toyota Corolla had a total signal transmission length of 11mS. The Saab had a total transmission length of 12mS. Data that was collected this year showed that for a 2005 Honda Civic, the total transmission length was around 280mS. Since it is impossible to test every single key fob made, our design assumes that the maximum transmission time that a signal will encounter will be 400mS.

In the background section, $T_e$ was explained as the length of time for a basic pulse element. For the purposes of this section, $T_e$ will be used as the smallest bit time in a transmission signal. The value of $T_e$ determines the frequency the receive signal needs to be sampled at in order to store and retransmit the signal without losing information. For the Toyota Corolla, the minimum bit length was 260uS. No data was provided for the Saab. The Honda Civic had a 550uS bit length. The second assumption made for this project is that the smallest $T_e$ that will be encountered is 150uS. According to Nyquist sampling theory, you want to sample the receive signal at no less than twice the frequency. Calculated in Eq. 9-11 is the amount of RAM needed to sample the signal at different rates.

\[
400mS \cdot \frac{10\text{samples}}{150\mu S} = 26,667\text{samples} (\text{bits})(9)
\]
\[
400mS \cdot \frac{9\text{samples}}{150\mu S} = 24,000\text{samples} (\text{bits})(10)
\]
\[
400mS \cdot \frac{8\text{samples}}{150\mu S} = 21,333\text{samples} (\text{bits})(11)
\]

A sampling frequency of 10 samples/150uS or about 66.7 KHz was chosen and a microcontroller was then chosen accordingly. The microcontroller used for this project is the PIC18F2525 with 3968 bytes of available RAM. The faster sampling rate was chosen to accommodate the worst cast scenario. If it is found that a lower sampling rate can be used, a microcontroller with less RAM, and thus cheaper can be recommended in the future.

The maximum clock frequency of the chosen microcontroller is 40MHz using a 10MHz external crystal with a built in PLL 4x multiplier. The microcontroller also has the ability to provide its own internal 32MHz clock (8MHz with PLL). Initially, the external oscillator design was chosen due to its increased speed over the internal clock. However, while waiting for the external oscillator to be ordered, the internal clock was used for code testing.

E. Software code

A state diagram for the microcontroller code is shown in Fig. 6.

![Figure 6: State diagram for microcontroller](image-url)
On the highest level, the code for the repeater is split up into four states. The first state that is entered on start up is the clear memory state. For security and privacy reasons, on startup and after transmitting a signal, the memory of the microcontroller needs to be cleared. This is to ensure that the repeater device does not act as a code grabber which will store key fob signals in memory to be later accessed illegally to steal a car.

The second state is a wait state. The microcontroller waits in this state (infinite loop) until an interrupt from an external I/O pin connected to the receiver is received. Upon the interrupt, the state is changed to a receive state where a timer is used to sample the receive signal coming from the receiver on an I/O pin.

When the RAM is filled, the receive state is exited and the transmit state is entered. In this state, data is taken from the beginning of the RAM and sent to an I/O pin on the microcontroller to be sent to the transmitter. The microcontroller implements a FIFO process. The data is placed on the I/O pin at the same rate it was sampled from the receiver (to not corrupt the data).

When the end of the signal is reached in RAM, the transmit state is exited and the code repeats itself beginning at the clear memory state.

VII. LEGAL CONCERNS

The whole design concept is based on the assumption that our idea follows the FCC rules and regulations. CFR title 47 Part 15 section 231 pertains to frequencies in the 40.66-40.70 MHz and above 70MHz. It is also for periodic operation in this band. Since our repeater only receives, stores, and retransmits the signal once per press of the key fob, there is no periodic retransmission of the same signal. Based on this information, it was assumed that CFR title 47 Part 15 section 231 does not apply to our situation. Our design is also subject to CFR title 47 part 15 section 209. This rule states the maximum field voltage that the repeater can transmit over a specified distance. We have been in contact with the FCC and were notified that this design meets FCC rules and regulations. The only requirement that needs to be kept track of is the maximum transmission signal strength at a specified distance.

VIII. RESULTS

To test the functionality of the microcontroller code, a test board was set up using LEDs to view the current state of the program. A push button was used to initiate an external interrupt to cause the microcontroller to change from the wait state to the receive state. The microcontroller test board is shown in Fig. 7.

The same Microchip receiver demo board used to initially capture the 2005 Honda Civic RKE signal was used to provide the receive signal input to the microcontroller. The signal coming out of the transmit pin of the microcontroller was then captured using an oscilloscope. In Fig. 8, the top signal is the transmit signal captured using the microcontroller and the bottom signal is the receive signal from the Microchip Receiver. Notice in Fig. 8 that there is approximately a 400mS delay between the receive and transmit signals.

The fabricated prototype board is shown in Fig. 9. The board shown in Fig. 9 was fabricated to test the transmitter functionality. Switches were placed to switch between the Maxim receiver and the Chipcon Transceiver while prototyping to determine which to use in the final design.
IX. CONCLUSION

As more cars are being produced with RKE devices, the 315MHz and 433.92MHz frequencies will not have the operating capacity. This leads to an increased number of RKE operating frequencies, making it harder to create a universal repeater since the repeater will have to work at numerous frequencies.

The functionality of the repeater is feasible however; the power consumption and battery life will be an issue due to the idle current draw of the receiver.

With a total repeater idle current draw of 0.5mA and an operational current draw of 20mA for 1.5 seconds 200 times a day, a battery life of 1800mAH will last approximately 4 months. The assumption of 0.5mA idle current draw may not be feasible due to the frequency of the polling function being able to detect and capture a signal with a total length of only 11mS. With additional circuitry, the design can be easily adapted to run off of the car’s main battery to solve this problem.

ACKNOWLEDGMENTS

The authors would like to thank Dr. Perlman for sponsoring this project for the past two years in addition to identifying the need for this project. The authors would also like to express appreciation to Dr. Phillips, Professor Slack, and Dr. Venkataraman for their coordinating and mentoring efforts.

Jeff Lonneville’s assistance with the assembly of the circuit boards is also greatly appreciated.

The team would also like to thank Jeff Sloane at Jenmat Electronics for his generous donation of both the 315MHz and 433MHz antennas that were used in the repeater.

REFERENCES