University of Turku
Cyber Physical Systems 2015 course

Project proposal - Wireless door opener

Student name: Vu Nguyen (511436)
Lok Khanal

Introduction

The aim of the project is to implement a wireless door opener based on radio communication. It is considered by many people to be inconvenient when they have to leave their cars and open the main entrance door manually, especially during the winter months. They want to stay inside their car and need a device capable of opening the door for them. Nowadays such a device can be found easily on the market. It consists of a remote control and a base station which receives data from the remote control and controls the transceivers accordingly. The wireless communication is based on 433Mhz radio communication with an own designed protocol, usually based on rolling code. The advantage of such a device is easy to design. However, it suffers from security issues as the messages sent over the radio communication which are encrypted using rolling code can be intercepted and hacked [1, 2, 3, 4]. As a replacement for the protocol, we will use AES-128 encryption algorithm to encrypt the messages sent over then radio communication since it has been shown that AES encryption still remains secure for AES key based AES security system [5,6]. The remote control part will be used by a user to open or close the door. The base station will be used to received the encrypted messages send from the remote control and controls the door/gate accordingly.

System description

The system consists of essentially two parts: the remote control and the base station. The remote control includes 4 buttons, an Arduino Uno platform, and a radio transceiver nRF24L01+. The case station part consists of an Intel Galileo platform, a servo motor, and a radio transceiver nRF24L01+. Figure 1 gives an big picture of the system described.

In the remote control part, there are 4 buttons: unlock, lock, open, and close. The lock button is used to disable the functionality of the open and close buttons. This means that when the lock button is pressed, pressing open or close buttons will not send any signal to the base station to open or close the door. By contrast, the unlock button is used for enabling the functionality of the open and close buttons. It does exactly the opposite thing to the lock button. The open and close buttons, as their names imply, are used to open and close the door/gate, respectively. After the open or close button is pressed with unlock function, Arduino

Uno will generate an encrypted message using AES-128 encryption algorithm and send it to the base station by means of the nRF24L01+ radio transceiver.

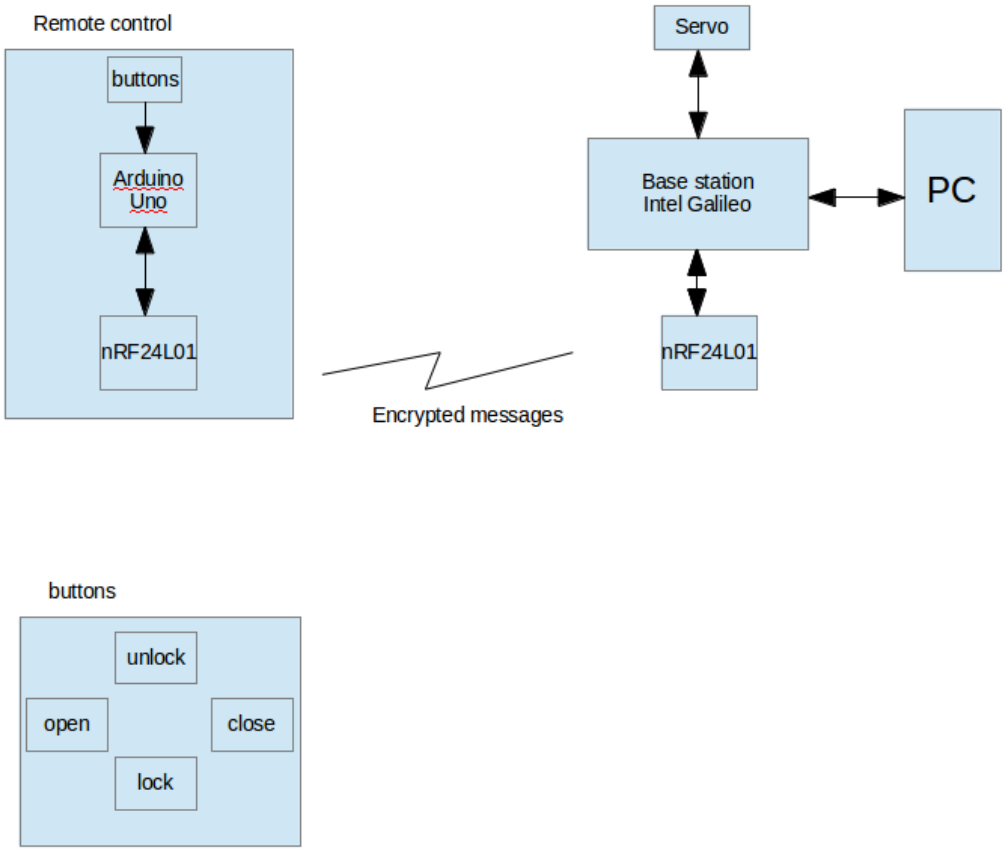

Figure 1. System block diagram

The base station part consists of a servo motor, an nRF24L01+ radio transceiver, and the base station itself which is an Intel Galileo platform. Upon receiving an encrypted message from the nRF24L01+ transceiver, Intel Galileo will decrypt the message and check the identification (ID) of the remote controller. If the right ID is received, the servo motor will open or close the door/gate depending on the content of the received message from the remote controller.

Division of labour

The project group has two team members: Vu Nguyen and Lok Khanal. Vu Nguyen will be responsible for working with the base station part while Lok Khanal will take care of the

remote control part. In particular, Lok Khanal will implement embedded software for the remote control part and make connections for the hardware components in the remote controller. The embedded software for the remote control basically read the state of the buttons, generate encrypted messages using AES-128 encryption algorithm, and send them to the base station. Since the remote control operates using battery. Designing of the embedded software should take care of energy efficiency in mind.

As for the base station part, Vu Nguyen will be responsible for it. Particularly, he will make hardware connections for the base station part, implement embedded software for Intel Galileo so that it receives the encrypted messages from the remote controller, encrypts the messages, and controls the servo motor. In addition, for debugging purposes during project development, Intel Galileo will be connected to the development PC via serial communication.

Hardware components

Remote control part
Buttons (x4)
Arduino Uno (x1)
nRF24L01+ radio transceiver (x1)
Wires
Breadboard (x2)
USB type B to USB type A cable (x1)

Base station part
Intel Galileo Gen 2 (x1)
Servo motor (x1)
nRF24L01+ radio transceiver (x1)
Wires
Breadboard (x1)

Project management

Time budget for the project is 2 to 3 weeks. This can be longer or shorter depending on the difficulty of the problems that may arise during the project. A meeting will be arranged once a week to discuss the status of the project, the problems, and find ways to solve the problems. After 2 weeks, if everything goes smoothly, the testing will be carried out to test the operation of the system. The project report will be done together by the team members after the testing has succeeded. For communication, email and Google docs will be used for writing documentation. A Github will be used to store software as follows
https://github.com/quangng/wireless-door-opener

References

[1] Andy Greenberg. WATCH THIS WIRELESS HACK POP A CAR'S LOCKS IN MINUTES [online]; WIRED 08 April 2014.
http://www.wired.com/2014/08/wireless-car-hack/
Accessed 16 March 2015.

[2] Matthew Sparkes. Hackers can unlock your can with little more than a laptop [online]; The Telegraph 05 August 2014.
http://www.telegraph.co.uk/technology/news/11013062/Hackers-can-unlock-your-car-with-little-more-than-a-laptop.html
Accessed 16 March 2015.

[3] Erica Naone. Car Theft by Antenna [online]; MIT Technology Review 06 January 2011.
http://www.technologyreview.com/news/422298/car-theft-by-antenna/page/1/
Accessed 16 March 2015.

[4] Jam intercept and replay attack against rolling code key fob entry systems using RTL-SDR [online]; 15 March 2014
http://spencerwhyte.blogspot.ca/2014/03/delay-attack-jam-intercept-and-replay.html
Accessed 16 March 2015.

[5] Dave Neal. AES encryption is cracked [online]; theinquirer.net 17 August 2011
http://www.theinquirer.net/inquirer/news/2102435/aes-encryption-cracked
Accessed 16 March 2015.

[6] Alan Kaminsky et al. An Overview of Cryptanalysis Research for the Advanced Encryption Standard; Military Communications Conference 31 October 2010.