TRABALHO DE GRADUAÇÃO

Controle de Portão Robusto para
Longas Distâncias

Sérgio Augusto Barreiros Bittencourt

Brasília, 2019

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

TRABALHO DE GRADUAÇÃO

Controle de Portão Robusto para Longas Distâncias

Sérgio Augusto Barreiros Bittencourt

Relatório submetido ao Departamento de Engenharia Elétrica, como requisito parcial para obtenção do grau de Engenheiro de Redes de Comunicação.

Banca Examinadora

Prof. Ricardo Zelenovsky, Doutor
Orientador

Prof. Georges Daniel Amvame Nze, Doutor
Examinador

Prof. Edson Mintsu Hung, Doutor
Examinador

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

"It does not matter how slowly you go as long as you do not stop."

(Confucius)

DEDICATÓRIA

Dedico este trabalho aos meus pais e às pessoas próximas de mim que me motivaram a concluir este trabalho.

AGRADECIMENTOS

Gostaria de primeiro agradecer meus pais que me apoiaram e me incentivaram por toda esta jornada que foi cursar engenharia.

Ao meu grande amigo Álvaro que me ajudou imensamente neste projeto, graças à ele este projeto conseguiu ser concretizado.

À minha namorada, Ana Luísa, que me apoiou em meus dias mais sombrios e com muita força de vontade me aturou quando eu estava muito estressado e querendo desistir da engenharia.

Agradeço, também, meus outros amigos, especialmente a Karen e o Filipe que se dispuseram a me ajudar quando eu precisava e não me deixaram desistir deste projeto quando os ânimos estavam baixos.

Ao meu orientador, professor Ricardo Zelenovsky, por sua compreensão, grande disposição e pelo seu bom humor.

Finalmente, agradeço à Universidade de Brasília pela oportunidade, pelas boas memórias que o curso me ofereceu e pelo indispensável conhecimento acadêmico.

Sérgio Augusto Barreiros Bittencourt

RESUMO

O objetivo deste trabalho é proporcionar um controle de portão especializado para comandos à longas distâncias, por via de um método de comunicação seguro. O custo do aparelho é baixo, permitindo, assim, o seu amplo acesso. De modo a garantir o funcionamento do controle e a abertura correta do portão, são usados duas porções de hardware; um agindo como controle, ou seja, como transmissor do sinal de abertura do portão e o outro como receptor para este sinal. O maior problema deste modelo é a possível brecha de segurança ao se enviar um sinal em texto claro por distâncias muito grandes, já que a captura do código de abertura do portão por uma entidade maliciosa pode ser efetuada. Para tanto, foi utilizado o algoritmo de criptografia *Advanced Encryption System* (AES-128 bits), que proporciona um nível de segurança adequado para este cenário.

ABSTRACT

The objective of this paper is the creation of a specialized gate control device for emitting commands through long distances. The cost of the device is maintained low for broad commercial availability. To ensure adequate operation and proper gate opening, two types of hardware device are used; one acting as a control device, i.e. as the transmitter for the gate opening signal and the other one as receiver for this signal. The biggest problem with this model is the security breach that occurs when sending a plain-text signal over long distances, since a malicious entity could easily capture the airborne packets and acquire the gate opening signal. For this reason, the AES-128 encryption algorithm was employed, thus providing the solution to this problem.

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

LISTA DE ACRÔNIMOS

ADC	*Analog-to-Digital Converter*
AES	*Advanced Encryption System*
AP	*Access Point*
BPS	*Bits per Second*
CBC	*Cipher Block Chaining*
EIRP	*Effective Isotropic Radiated Power*
GPIO	*General-purpose input/output*
HTML	*HyperText Markup Language*
HTTP	*Hyper Text Transport Protocol*
HTTPS	*Hyper Text Transport Protocol Secure*
IDE	*Integrated Development Enviroment*
IoT	*Internet of Things*
IP	*Internet Protocol*
LED	*Light Emitting Diode*
PWM	*Pulse Width Modulation*
SSID	*Service Set Identifier*
STA	*Station*
TCP	*Transmission Control Protocol*
USB	*Universal Serial Bus*

SUMÁRIO

1 INTRODUÇÃO

O avanço rápido das invenções tecnológicas permite a invasão destas em áreas novas, antes não cogitadas. Com o aumento da dependência da sociedade contemporânea na tecnologia (MUNIZ, 2019) muitos novos problemas surgiram que podem ser solucionados por meio de projeto que requerem um maior grau de sofisticação. Foi por meio de um destes problemas que se originou este trabalho. No Gama existem chácaras extensas onde o morador para receber visitas é obrigado a pegar o seu carro para abrir o portão de entrada da chácara. Este processo é inconveniente para o morador, especialmente quando ele tem uma idade mais avançada, ou recebe um número grande de visitas.

Para estas pessoas, os sistemas convencionais de portões não atendem aos requisitos deste projeto, pois seus controles só agem em distâncias curtas devido à baixa potência destes aparelhos (P.; Reinaldo, 2008). Este tipo de comunicação é inadequado para o ambiente de estudo deste trabalho, logo que nas chácaras do Gama a distância das casas para os portões costuma extrapolar 300m. Considerando ainda que estas chácaras normalmente não são descampadas e, portanto, contém um número significativo de objetos entre o caminho da casa até o portão, sendo, então, amplos campos de interferência para os meios de comunicação. Por conta disso, torna-se necessário desenvolver um sistema para o portão que seja robusto o suficiente para contornar essas limitações.

Outra falha importante dos sistemas de portão convencionais é na questão de informar ao usuário o estado do portão. Ao passar pelo portão, às vezes o indivíduo esquece de fechar o portão, como a distância da casa para este é grande ela pode não perceber o seu erro por um intervalo de tempo muito grande. Em detrimento desta falha pessoas não desejadas podem aproveitar a vulnerabilidade e entrar na propriedade, adquirindo, desta forma, acesso à casa principal da vítima, supondo que o portão da vítima não tenha o seu fechamento temporizado que foi o caso do cliente deste projeto.

Até aqui o cenário das chácaras no Gama recebeu maior destaque, mas estes problemas também ocorrem em outros locais, como, pequenas fazendas e lugares cercados com uma grande distância entre seu centro de operações e o local de acesso.

Tendo estes problemas em mente o projeto deste trabalho foi concebido de forma a suprir essas demandas.

1.1 MOTIVAÇÃO

A motivação deste trabalho surgiu por meio de uma demanda proferida por um morador no Gama. Este morador requisitou uma solução que permitisse a abertura de seu portão externo de dentro da sua casa. O problema surgiu quando este tentou usar controles convencionais para tentar abrir o portão de sua casa localizado a uns 300m de distância de sua casa. Por conta disso,

o controle convencional não foi capaz de suprir as necessidades do cliente devido ao seu baixo alcance.

De forma a resolver o problema dos moradores de chácara no Gama este trabalho criou forma. Entretanto, esta não é a única motivação para este projeto. O projeto também abarca um possível uso nos dispositivos inteligentes, que estão por vir para serem integrados pelo *Internet of Things* (IoT). O dispositivo elaborado neste trabalho torna fácil integração com este conceito de automatização de casas. As Figuras 1 e 2 abaixo evidenciam um pouco mais o local de estudo para o qual este projeto foi desenvolvido, como também mostra as dimensões da chácara.

Figura 1- Portão e chácara do cliente. (Própria, 2019)

Figura 2- Distância do portão até a casa do cliente. (Própria, 2019)

1.2 OBJETIVO

O objetivo deste trabalho é desenvolver um controle remoto de portão que funcione a longas distâncias (maiores que 300m), onde este envie um sinal seguro de tal forma que não seja trivial descobrir o código de abertura do portão por meio de uma técnica de invasão simples, como o *sniffing* por exemplo.

1.3 METODOLOGIA

Para alcançar o objetivo, foi, primeiramente, desenvolvido um dispositivo hardware transmissor, que será efetivamente o controle do portão, para enviar os sinais de mudança de estado para um receptor localizado no portão. Este receptor é responsável por receber este sinal, decodifica-lo e mudar o estado do portão.

Ao construir estes dois dispositivos, seus códigos serão desenvolvidos de acordo com o um nível alto de segurança. De forma a verificar quais parâmetros da antena proporcionam um alcance maior do sinal, foi testada a taxa de transmissão usada no envio do dispositivo.

1.4 ORGANIZAÇÃO DO TRABALHO

Este trabalho foi organizado por meio dos seguintes capítulos: Fundação Teórica, Montagem e Configuração, Ensaios e Conclusão.

No capítulo 2, Fundamentação Teórica, serão discutidas em detalhe todos os conceitos utilizados na confecção deste trabalho, desde as antenas usadas até o protocolo de comunicação empregado na comunicação com o usuário. Este capítulo se divide em: Fundamentos de Antenas, Fundamentos de Criptografia, Hardware e Software. Nos primeiros dois capítulos serão apresentados os conceitos fundamentais para entender os funcionamentos das antenas e da criptografia. Na seção de Hardware serão especificados os componentes escolhidos para engendrar o sistema prometido e, finalmente, na seção de Software será feito algo análogo ao da seção de Hardware, porém, desta vez, discutindo o software encontrado nos componentes.

No capítulo 3, Montagem e Configuração, os processos efetuados para a efetiva criação do sistema e a integração feita entre *hardware* e *software* serão descritos.

Em seguida, no capítulo 4, Ensaios, os testes realizados para auferir o custo do sistema, como também para otimizar o seu funcionamento serão detalhados, apresentando os resultados obtidos para estes ensaios e interpretando-os.

Finalmente, no capítulo 5, Conclusão, será discorrido acerca do resultado final do trabalho e se ele atendeu as expectativas apresentadas acima, como, também, sugestões para trabalhos futuros para melhorar o funcionamento deste sistema.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo serão discutidos os conceitos teóricos fundamentais para entender o desenvolvimento do controle de portão de longa distância. De modo a deixar a compreensão mais clara, este capítulo foi dividido em três seções. A primeira seção discorre acerca dos conceitos mais fundamentais para o entendimento do projeto, como, por exemplo, o funcionamento do sistema em questão e da criptografia empregada. Na segunda seção serão abarcados os conceitos por trás do *hardware* utilizado e uma breve descrição do seu funcionamento e uso atual. Finalmente, a última seção abordará os conceitos de *software* usados para confeccionar este projeto.

2.1 FUNCIONAMENTO DO SISTEMA

De manei geral o sistema tem o seguinte funcionamento, o usuário para mudar o estado do portão aperta o botão do controle. Ao apertar o botão do controle este envia a mensagem via o módulo HC-12 para o dispositivo do portão e este ao receber a mensagem aciona o motor para abrir ou fechar o portão dependendo do seu estado anterior. Enquanto isso, o dispositivo do portão, por meio do seu REED switch, envia qual o estado do portão para o controle. Enfim, este por meio do NodeMCU envia por Wi-Fi o estado do portão ao usuário pelo protocolo HTTP, permitindo, então, que o usuário acesse o estado do portão através do seu celular. A Figura 3 abaixo apresenta um breve esquemático do sistema descrito.

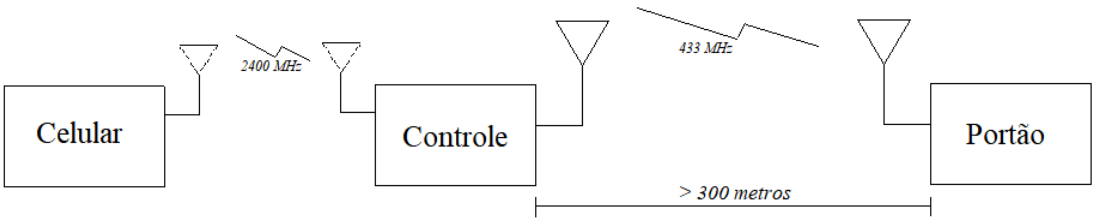

Figura 3- Breve esquemático do funcionamento geral do sistema projetado. (Própria, 2019)

2.2 FUNDAMENTOS DE ANTENAS

Uma antena é definida no dicionário inglês Webster como “um dispositivo metálico (como um bastão ou fio) utilizada para a radiação ou recepção de ondas de rádio”. Outra definição também seria a de um meio para a radiação ou recepção de ondas de rádio (BALANIS,

2016). Considerando estas duas definições acima, se torna evidente que a antena é um componente indispensável para dispositivos que pretendem se comunicar sem fio por meio de ondas eletromagnéticas. O funcionamento destes componentes pode ser resumido da seguinte maneira: uma corrente percorre a parte metálica da antena em um processo de ida e volta. Por conta desta movimentação a corrente que percorre a parte metálica gera um campo elétrico paralelo à corrente e um campo magnético perpendicular a este. Este campo eletromagnético é propagado para fora da antena por meio de uma onda eletromagnética (STROSKI, 2018). O receptor desta onda também é uma antena e funciona da maneira reversa ao que foi explicado anteriormente, a antena primeiro percebe a onda eletromagnética transmitida pela antena transmissora, e ao detectar esta onda uma corrente é gerada na parte condutora da antena receptora, esta corrente é então reconhecida por um aparelho adequado finalizando o processo de transmissão e recepção do sinal (BALANIS, 2016). A Figura 3 abaixo ilustra esse processo de propagação. Em (a) a corrente percorre o fio metálico e consequentemente gera um campo circular em torno do condutor, em (b) é ressaltado que os campos magnético e elétrico são perpendiculares entre si e em (c) este campo magnético é propagado para fora do condutor.

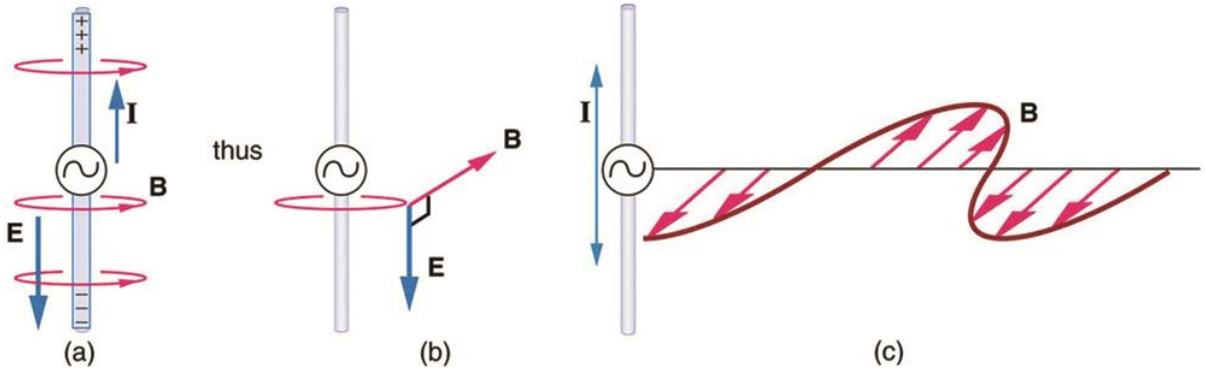

Figura 4- Funcionamento da propagação de uma onda eletromagnética em uma antena. (STROSKI, 2018)

Como visto acima o funcionamento da transmissão sem fio irá depender, quase que exclusivamente, destas antenas e por isso é importante conhecer algumas de suas características.

2.2.1 PARÂMETROS FUNDAMENTAIS DAS ANTENAS

O primeiro parâmetro de uma antena para o qual devemos nos atentar é o seu comprimento. Através do tamanho da antena é que se pode sintonizar a antena para a frequência em que o sinal será enviado (CLOUDE, 1996). Contudo este sempre estará atrelado ao comprimento de sua onda e a relação entre o tamanho da antena e dessa grandeza muda de acordo com o tipo de antena usado. Pode-se encontrar o comprimento de onda por meio da equação da onda, considerando que a onda eletromagnética viaja na velocidade da luz:

$$c = \lambda f$$

- Onde c é a velocidade da luz no vácuo, aproximadamente $3 * 10^6\ m/s$.
- λ é o comprimento da onda.
- f é a frequência de operação, ou de ressonância, da antena.

Outro parâmetro importante é a potência de transmissão da antena, ela determina qual a intensidade do sinal eletromagnético o que permite com que este se desloque por distâncias maiores antes de se degradar significativamente (BALANIS, 2016). Para o cálculo da potência que será recebida na outra antena pode-se utilizar a equação descrita abaixo:

$$P_R = P_{EIRP} * G_R * \left(\frac{\lambda}{4\pi d}\right)^2$$

- Onde P_R é a potência recebida pela antena receptor;
- P_{EIRP} é uma grandeza chamada de *Effective Isotropic Radiated Power* (EIRP), que nada mais é do que a potência de transmissão que é multiplicado pelo ganho da antena transmissora (G_R);

    - É importante comentar que a medida da potência em antenas é feita utilizando a medida *dbi* que nada mais é do que uma medida da potência de uma antena em relação a mesma potência de uma antena isotrópica naquela direção.

- $\left(\frac{\lambda}{4\pi d}\right)^2$ é a fórmula de Friis que modela a perda de potência no espaço livre de uma onde eletromagnética, nota-se que maior a frequência maior a deterioração.

O último parâmetro que será abordado neste projeto é a diretividade da antena. Dependendo de como a antena é construída ela terá um determinado diagrama de radiação. Este diagrama de radiação simplesmente determina para qual direção a antena conseguirá irradiar maior parte da potência. O modelo de antena com diagrama de espectro mais simples é a antena isotrópica que consegue irradiar sua potência de maneira uniforme para todos os ângulos exceto os que estão acima, ou abaixo da antena (BALANIS, 2016). A Figura 4 destacada abaixo apresenta o diagrama de radiação para uma antena dipolo de meia onda que apresenta tal diagrama de maneira isotrópica.

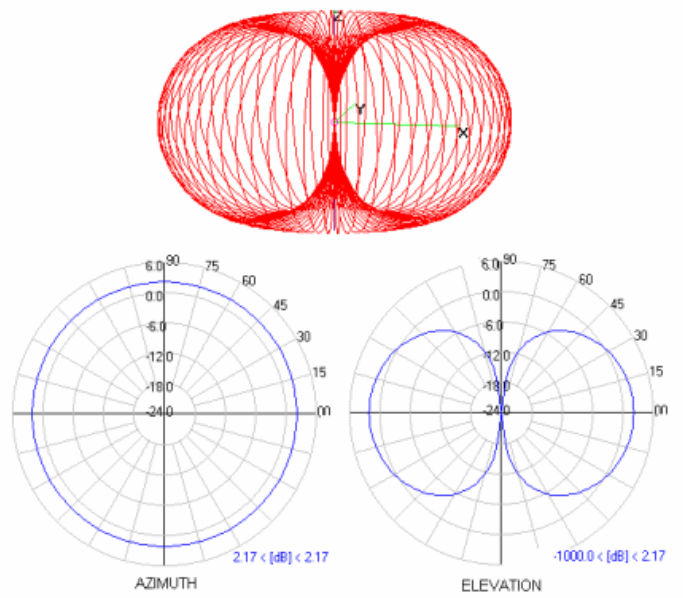

Figura 5- Diagrama de radiação de uma antena dipolo. (LODRO, 2016)

2.2.2 TIPOS DE ANTENAS

Como mencionado anteriormente o formato da antena irá influenciar no seu modo de operação. Por conta disso, existem diversos tipos de antena cada uma adequada para determinada aplicação. A mais simples destas é a antena dipolo de meia onda que pode ser feita por meio de apenas um fio de cobre (CLOUDE, 1996) . Esta simples antena pode não parecer ser uma boa opção, mas dependendo da aplicação, sua irradiação quase perfeitamente isotrópica e seu baixo custo são de suma importância para alguns projetos. Outro tipo de antena também muito utilizado é a helicoidal. Esta antena é bem mais complexa que a dipolo, porém em compensação a antena funciona com uma banda de frequências maior e é mais versátil ao se permitir o seu uso em dois modos diferentes: normal e axial. No modo normal, esta funciona como uma antena dipolo de meia onda. No modo axial a antena irradia com maior diretividade, concentrando a potência em seu lóbulo principal como mostra a Figura 6. Para se trocar o modo de funcionamento da antenna, deve-se ajustar a sua circunferência. Uma das poucas desvantages desta antena seria sua ocupação de espaço maior em relação às outras antenas. Os diversos tipos de antena mais usados estão ilustrados na Figura 5 e como mencionado anteriormente, na Figura 6 são apresentados os diagramas de radiação para os diferentes modos da antena helicoidal.

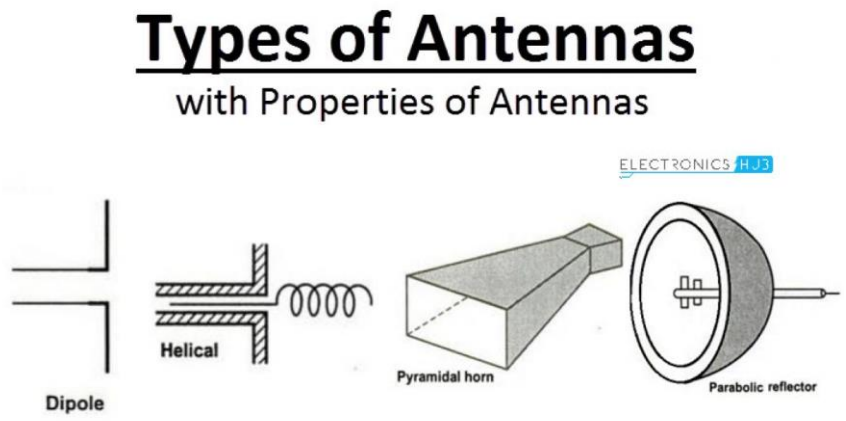

Figura 6- Os diferentes tipos de antena mais usados. (RAVI, 2019)

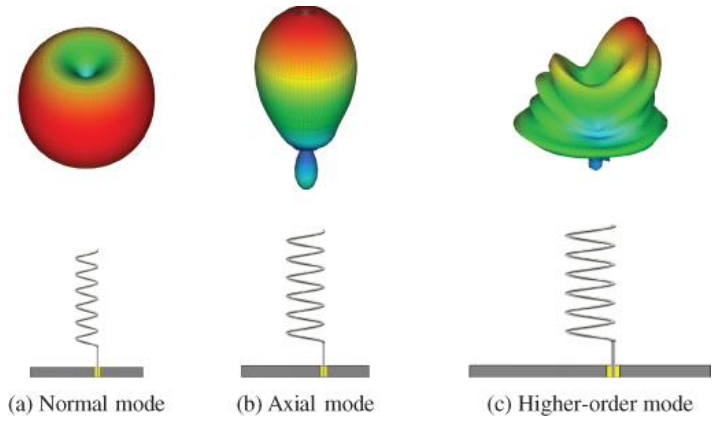

Figura 7- Diagramas de radiação para diferentes modos de operação da antena helicoidal. (LODRO, 2016)

2.3 FUNDAMENTOS DE CRIPTOGRAFIA

A criptografia é o estudo da comunicação segura na presença de invasores, que são comumente chamados de adversários. Estes adversários estão empenhados em tentar obter e interpretar os dados de uma comunicação entre dois agentes. A criptografia difere da criptoanálise, que é o estudo de como se quebrar criptosistemas. As vantagens da criptografia são diversas, contudo, as que merecem maior destaque no presente caso são: confiabilidade na transmissão de dados, autenticação dos dados e integridade dos dados. Um sistema típico de criptografia é apresentado na Figura 7.

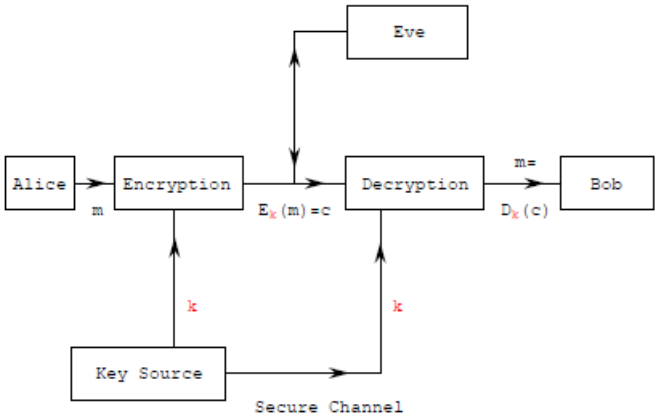

Figura 8- Esquemático do funcionamento de um criptosistema. (TILBORG, 2006)

Em sistemas criptográficos, como o ilustrado na Figura 7, dois agentes chamados de Alice e Bob, desejam comunicar entre si. Porém, um terceiro agente, chamada de Eve se injeta no meio de comunicação entre Alice e Bob para adquirir as mensagens sendo trocadas nesta comunicação, representadas neste diagrama por m. Para não permitir que Eve adquira os dados de Alice e Bob, utiliza-se um método de criptografar a mensagem, representada por $E_k(m)$ para que a mensagem trocada entre Alice e Bob não seja legível sem antes passar pelo processo de decriptografia, que nada mais é que uma função inversa daquela usada na criptografia tal que $D_k\big(E_k(m)\big) = m$ (TILBORG, 2006). De modo a garantir que Eve não conheça as funções usadas na comunicação de Alice e Bob emprega-se as chaves, apenas conhecidas por Alice e Bob, que garantem a unicidade das funções; ou seja, apenas com as chaves é possível ler a mensagem.

2.3.1 CIFRA DE BLOCOS

O sistema apresentado na seção anterior pode ser desenvolvido de diversas maneiras. Neste trabalho em específico usou-se o algoritmo AES-128 que será abordado com mais detalhes na seguinte seção, mas, antes, para a melhor compreensão deste algoritmo deve-se entender que este é do tipo cifra de blocos, ou *block cipher* em inglês. Este é um criptosistema tradicional capaz de manipular um número fixo de símbolos durante determinado tempo utilizando uma chave específica (TILBORG, 2006). Esta criptografia é feita independentemente dos blocos anteriores. Em suma, o modo de funcionamento deste método de criptografia consiste em primeiro separar os dados da mensagem em blocos de igual tamanho a depender do algoritmo utilizando, cifrá-los por meio de uma chave resultando em novos blocos cifrados que precisariam passar pelo processo inverso para poder ser decifrado. A Figura 8 ilustra a operação deste método mais simples que comumente é chamado de método *codebook*.

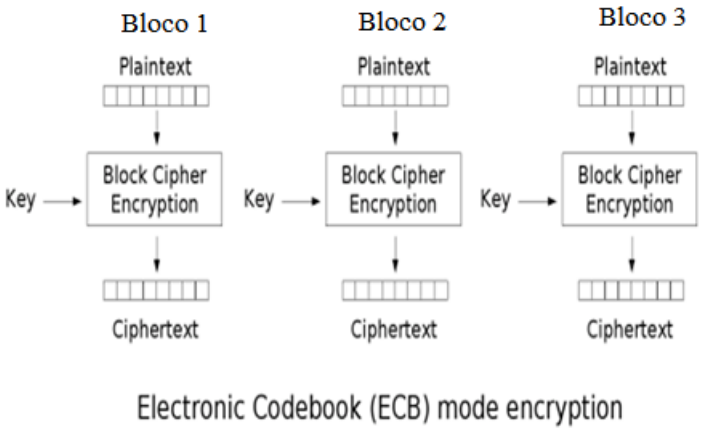

Figura 9- Esquemático do funcionamento da criptografia por cifra de blocos.
(ALTIGANI;BARRY;ELSADIG, 2015)

Contudo, é importante salientar alguns problemas deste método. Primeiro, para cifrar o bloco o algoritmo utiliza uma tabela que precisa ser guardada na memória do dispositivo eletrônico gerada pela chave, consumindo, assim, certa quantidade de memória. Contudo, no caso deste trabalho o problema de memória não é de relevância, pois as mensagens enviadas ao portão são pequenas (16 bytes). Outro problema ocorre ao se cifrar um mesmo bloco com a mesma chave repetidas vezes, logo que o bloco cifrado será sempre o mesmo. Isto é uma grande falha deste método e por conta deste problema é que se criou outros métodos como o *cipher block chaining* (CBC) e o *cipher feedback mode* (TILBORG, 2006). No caso deste trabalho o problema do método *codebook*, assim chamado o método apresentado na Figura 8, não é um problema muito alarmante já que não se espera que se repita a mesma mensagem várias vezes durante um curto período de tempo, portanto optou-se por este modelo devido a sua simplicidade.

Contudo, devido ao uso do modo de operação *codebook* explicado acima, o sistema se torna vulnerável aos ataques do tipo *man-in-the-middle*. Onde, o atacante mesmo não sabendo o conteúdo da mensagem pode interceptar a mensagem criptografada e usar esta para abrir o portão, já que o dispositivo do portão irá decifrar essa mensagem como se viesse do controle. Para contornar este ataque implementou-se um mesmo vetor de 128 bytes nos dois dispositivos, composto por número aleatórios, de tal forma que em um intervalo aleatório de tempo o controle manda para o dispositivo do portão um índice qualquer do vetor para o portão. A partir deste índice os dois dispositivos lerão os próximos 16 bytes do vetor e, daí, formarão com estes uma nova chave. Desta forma, a probabilidade de o ataque *man-in-the-middle* ter êxito diminui drasticamente.

2.3.2 AES-128

O *Advanced Encryption Standard* é um algoritmo de criptografia do método de cifra de blocos usado em alguns departamentos do Estados Unidos da America (EUA) para proteger informação classificada e é largamente utilizada em *softwares* e *hardwares*. O AES é um algoritmo que usa chaves simétricas, ou seja, a chave de um agente deve ser igual à do outro para permitir a conexão. Portanto, estas chaves devem ser conhecidas antes da comunicação. O AES é capaz de manipular blocos de tamanhos de 128, 192 e 256 bits. As vantagens deste algoritmo são: garantir uma segurança maior em relação aos outros algoritmos, custo quase nulo, já que este algoritmo foi lançado de forma a não conter royalties e fácil implementação devido ao seu caráter global e *royalty-free* (MARGARET, ca. 2015).

2.4 PROTOCOLO DE COMUNICAÇÃO: HTTP

O HTTP (*Hypertext Transport Protocol*) é um protocolo da camada de aplicação (no modelo TCP/IP) que é muito utilizado nas comunicações efetuadas na *web* (KUROSE, 2010). O protocolo HTTP tem como utilidade a definição da maneira de como se envia mensagens pela *web*. Além disso, o HTTP utiliza o (Transport Control Protocol) TCP como protocolo na camada de transporte, ou seja, uma conexão HTTP é feita de maneira persistente e os pacotes chegam no cliente de forma integra e respeitando a ordem de envio. Finalmente, o HTTP não guarda informações do cliente, o que o torna um protocolo *stateless* (sem estado), significando que um cliente pode efetuar uma requisição múltiplas vezes usando o protocolo e ele irá informá-la sem registrar quantas vezes estas requisições foram feitas (KUROSE, 2010).

Ultimamente, o HTTP vem sendo substituído pelo HTTPS (*Hyper Text Protocol Secure)* devido ao fato de que o HTTP envia suas mensagens em texto claro, ou seja, o HTTP não é um protocolo seguro, diferente do HTTPS. Contudo, devido às limitações do NodeMCU este se comunica por meio apenas do protocolo HTTP e não tem integração com o HTTPS (HELGESCHNEIDER, 2017). Porém como, neste projeto, as mensagens enviadas pelo HTTP estão criptografadas enviar as mensagens em texto claro não é um problema grave.

2.5 HARDWARE

Nesta seção serão especificados os componentes de *hardware* utilizados para a construção dos dispositivos do sistema de automação residencial. Após vários testes com outros componentes, foi escolhida a composição abaixo por apresentar uma melhor relação entre qualidade e custo.

2.5.1 PLATAFORMA ARDUINO

De acordo com o próprio website do Arduino, este pode ser descrito como uma "plataforma eletrônica de código aberto feita em um hardware e *software* que são fáceis de usar" (ARDUINO, 2015). Esta plataforma tem diversas vantagens, como, por exemplo, o fato de que são relativamente baratos, o seu software Arduino (IDE) pode ser usado em diversas máquinas como Windows, Macintosh OSX e Linux (ARDUINO IDE, 2012). A vantagem desta plataforma é que tanto o seu *hardware* como *software* são *open-source* o que permite que o usuário consiga reutilizar códigos e projetos de outros desenvolvedores. Quanto à sua capacidade de processamento, o Arduino utiliza a família AVR de 8-bits da Atmel que não é um processador de alto desempenho, mas atende aos requisitos de diversos projetos propostos, inclusive o do atual projeto (ARDUINO, 2015). Esta plataforma foi então escolhida devido à sua facilidade na prototipagem de projetos.

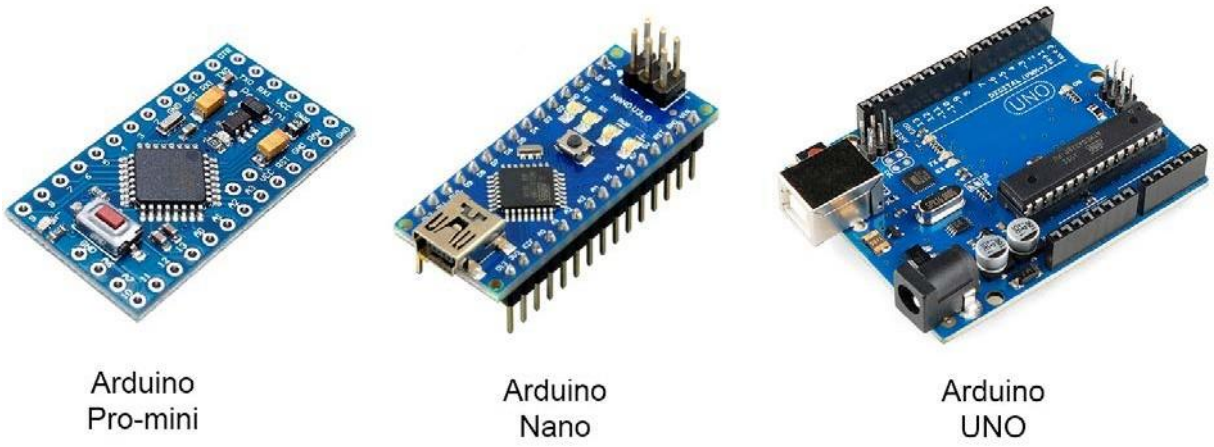

Figura 10 – Versões do Arduino, neste projeto foi utilizado apenas o Arduino Nano (NUNES, 2018)

O Arduino nasceu na Ivrea Interaction Design Institute como uma ferramenta para a criação ágil de protótipos, destinada para estudantes sem conhecimentos prévios em eletrônica, ou programação, daí a sua facilidade de manuseio (ARDUINO, 2015). A partir deste humilde começo a plataforma ganhou maior prestígio e começou a ser usada para fins mais técnicos, como: produtos IoT, os chamados *wearables*, impressão 3D e ambientes integrados. A partir disso começaram a ser produzidos diversas variações da plataforma original para atender estas novas demandas. As versões mais notáveis são: Arduino Pro-Mini, Arduino Nano, Arduino UNO e Arduino Mega.

Neste projeto optou-se por utilizar a versão Arduino Nano, porque o dispositivo elaborado para este trabalho não necessita de um alto poder de processamento e o uso do Arduino Nano acaba por diminuir o custo total do produto desenvolvido. Outra possibilidade era o uso do Pro-Mini, mas a razão do Nano ter sido escolhido em detrimento deste é devido a maior facilidade de manuseio do Nano em relação ao Pro-Mini. Enquanto o Nano contém uma entrada mini USB para o *upload* de códigos para o dispositivo o Pro-Mini não tem entrada USB para esses fins. Portanto, optou-se pela solução mais fácil, embora o custo do projeto tenha sofrido um leve aumento por causa desta escolha. As pinagens do Arduino Nano são explicitadas na Figura 10.

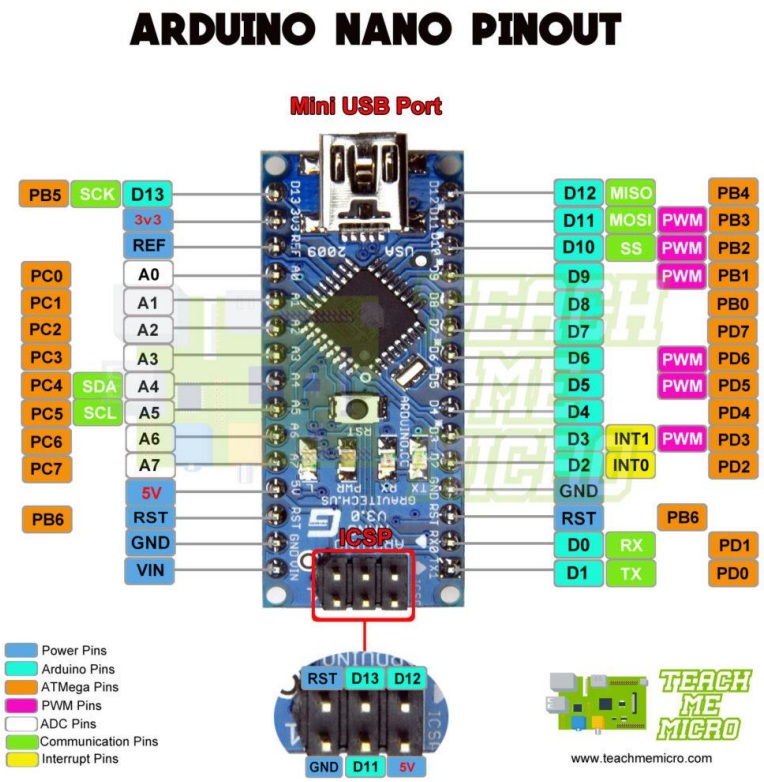

Figura 11– Imagem ilustrativa do *pinout* do Arduio Nano (ARDUINO NANO, 2019)

2.5.2 PLATAFORMA DE INTERNET DAS COISAS NODEMCU

O NodeMCU é uma plataforma IoT de código aberto, o seu firmware é baseado no modelo ESP-12 e, por consequência, executa seu *firmware* em um ESP8266 Wi-Fi SoC da Espressif Systems. O termo “NodeMCU” não se refere ao kit de desenvolvimento, mas sim ao seu *firmware*. Apesar do *firmware* utilizar a linguagem Lua, desenvolvida na PUC-Rio (LUA, 2019), para os seus scripts a IDE do Arduino permite que este seja programável na linguagem C#, necessitando apenas da instalação de algumas bibliotecas para tais fins encontrada em repositórios no GitHub (SZDOIT, 2015).

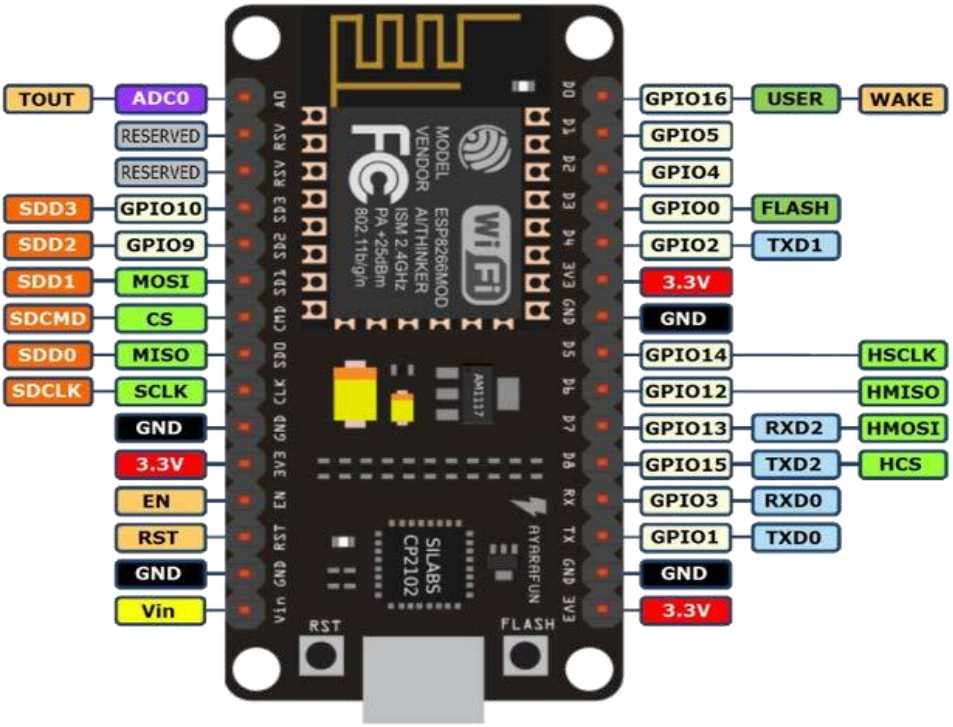

Figura 12- Imagem ilustrativa do *pinout* do NodeMCU 1.0 (HELGESCHNEIDER, 2017)

Com a IDE do Arduino, fica fácil a programação no NodeMCU, que é necessário para realizar a comunicação *wireless* para que o transmissor do controle do portão consiga se comunicar com o receptor. Além disto, o NodeMCU possibilita o controle de relés, parte integral para o funcionamento correto deste projeto. As especificações de *hardware* para esta placa são as seguintes (SZDOIT, 2017):

- 3 modos de funcionamento: Station (STA) / Access Point (AP) / STA + AP;
- Pilha de protocolo Transfer Layer Protocol (TCP) / Internet Protocol (IP) embutida, suporte à conexão de cliente TCP de múltiplos canais (máximo 5);
- 0 ~ D8, SD1 ~ SD3: usado para GPIO, PWM, IIC; A corrente máxima alcançada por pino é de 15mA;
- AD0: ADC unidirecional;
- Entrada de energia: 4.5V ~ 9V (10VMAX), suporta alimentação USB e USB debug;

- Corrente de trabalho: ≈ 70mA (200mA MAX, contínua), em espera <200uA;
- Taxa de dados de transmissão: 110-460800bps;
- Suporta interface de comunicação de dados UART / GPIO;
- Suporta o *firmware* de atualização remotamente (OTA);
- Suporte a Smart Link;
- Temperatura de trabalho: -40 ℃ ~ + 125 ℃;
- Peso: 7g.

2.5.3 MÓDULO HC-12

O HC-12 é um módulo *transceiver half-duplex* usado para comunicação serial *wireless* na faixa de 433.4 – 473. 0 MHz, faixa tipicamente usada em controles de portão convencionais. Utilizando este módulo com uma antena externa é possível de transmitir sinais a distâncias um pouco além de 1 km (ROZEE, 2016). O espectro de frequências do HC-12 pode ser visto na Figura 12, como destacado acima, a frequência de operação do HC-12 está em torno de 433 MHz.

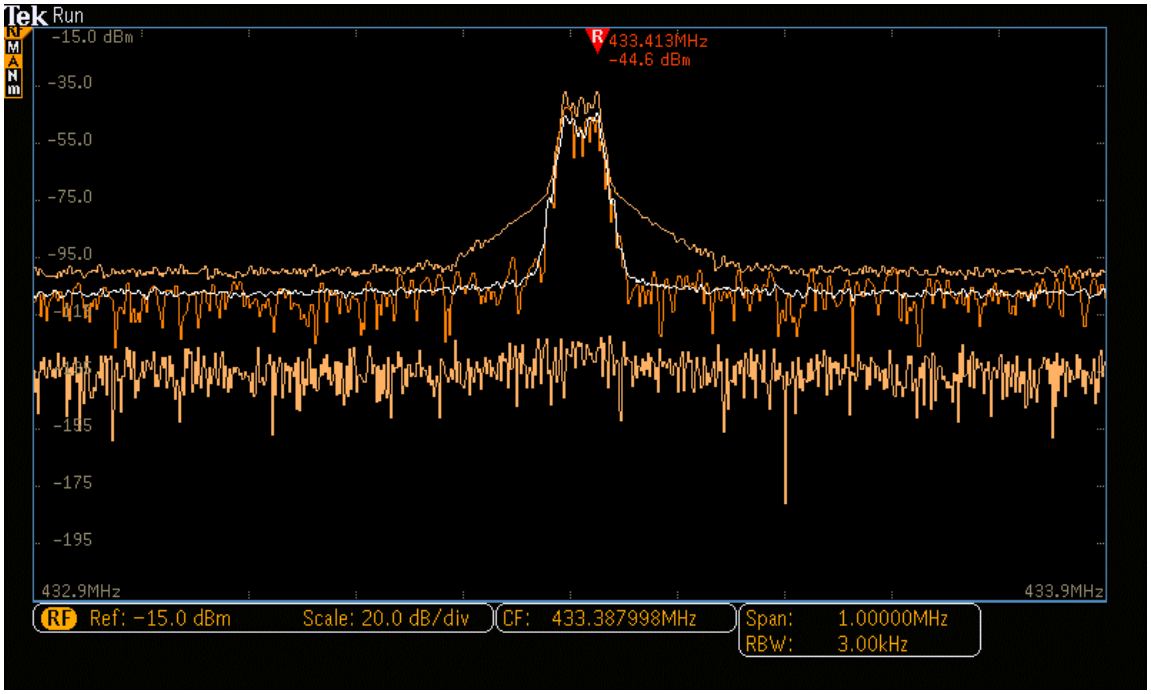

Figura 13- Diagrama espectral da banda de frequência de operação do módulo HC-12. (HUGHES, 2016)

Um componente deste módulo que merece maior atenção é o Si4463 Transceiver que permite uma potência transmissão máxima de 20 dBm (100 mW) com uma sensibilidade de recepção de -129 dBm. Além destas especificações, este módulo também tem outras funcionalidade como operações em múltiplas bandas e saltos de frequência (*frequency hopping*), sendo este último importante no quesito de segurança da mensagem enviada (ROZEE, 2016).

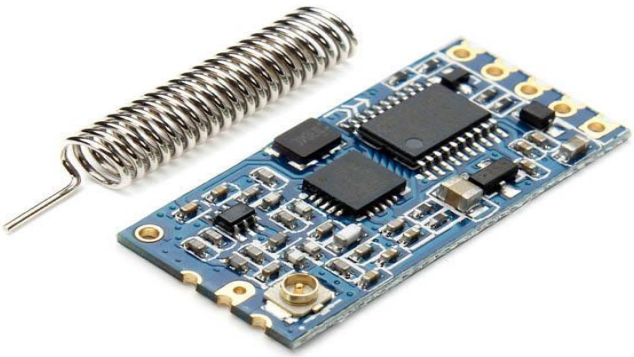

Figura 14- Ilustração do módulo HC-12. (HUGHES, 2016)

2.5.4 MÓDULO RELÉ

Os microcontroladores como o Atmega, PIC e MSP são dispositivos lógicos usados para controlar a inteligência do circuito. Estes microcontroladores usam tensões e correntes baixas para funcionar. Por exemplo, o Arduino UNO é capaz de suportar no máximo 40 mA e fornece uma tensão de no máximo 5V (ARDUINO, 2015). Embora estes valores sejam o suficiente para garantir o funcionamento de dispositivos como o HC-12, não são suficientes para, por exemplo, proporcionar a tensão adequada para o motor do portão.

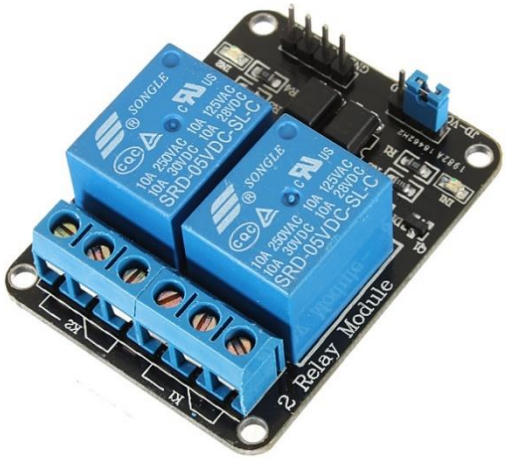

Figura 15- Ilustração de um dispositivo relé. (MOTA, 2017)

Para tal fim se utiliza os módulos relés que servem como um atuador entre dispositivos lógicos de baixa tensão com dispositivos de tensões e corrente maiores. Além disso, o relé funciona como um interruptor através da geração de um campo eletromagnético que faz com que o circuito feche e transfira energia para o dispositivo conectado no relé (MOTA, 2017).

Como comentado anteriormente, este módulo será usado no projeto de forma a garantir a operação do motor do portão, abrindo-o ou fechando-o dependendo do estado em que este se encontra.

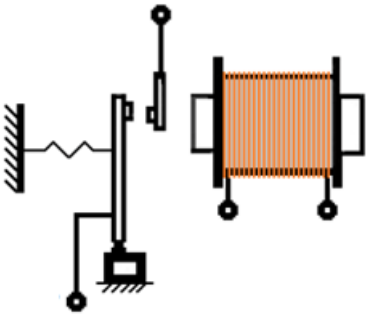

Figura 16- Esquemático do funcionamento de um relé simples. (MOTA, 2017)

2.6 SOFTWARE

O *software* utilizado nesse projeto será descrito de maneira mais detalhada nesta seção. Como neste projeto foi apenas utilizado um *software*, a Arduino IDE, então também serão discutidas as biblioteca usadas para gerar a criptografia das mensagens transmitidas, discutida na subseção 2.2.2.

2.6.1 AMBIENTE DE DESENVOLVIMENTO ARDUINO IDE

A Arduino IDE é uma aplicação que funciona em múltiplas plataformas (Windows, macOS, Linux) que utiliza a linguagem C e C++ para escrever e fazer o *upload* de programas para a placa do Arduino de uma maneira rápida e fácil (ARDUINO IDE, 2012). Atualmente se encontra em sua versão 1.8.10, porém para este trabalho foi utilizada a versão 1.8.7. Apesar de proporcionar uma interface mais amigável para o desenvolvimento na plataforma Arduino, a Arduino IDE não é a única que pode ser usada. Pode-se usar, também, outras IDEs compatíveis com o processador Atmega usado nas placas Arduino. Apesar disso, uma das grandes vantagens deste *software* é que ele, como o resto dos produtos Arduino, é *open-source*; permitindo o acesso a diversos projetos feitos por outros, especialmente por meio de suas bibliotecas de terceiros como a que será abordada a seguir.

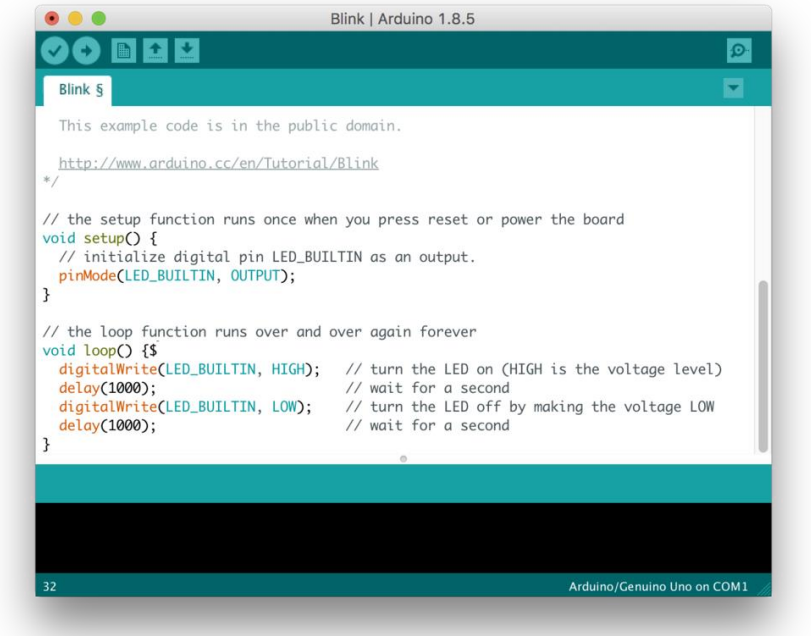

Figura 17- Imagem da interface do Arduino IDE. (ARDUINO IDE, 2012)

2.6.2 BIBLIOTECAS ARDUINO

Neste projeto foram utilizadas três grandes bibliotecas do Arduino de modo a garantir o funcionamento do dispositivo. Estas são as bibliotecas *Thread*, *AESLib* e *ESP8266*.

A primeira biblioteca tenta remediar um problema na plataforma Arduino. As placas Arduino são incapazes por *default* de executar tarefas paralelas por meio de *threads* como é feito em alguns outros microcontroladores e especialmente em comutadores. Como o Arduino não vem com a biblioteca das *threads* como funcionalidade original utilizou-se a função *loop* de tal forma que esta seja executada apenas condicionalmente, criando-se assim uma *protothread*.

A outra biblioteca utilizada foi para o uso do método de criptografia AES-128 no Arduino, garantindo, assim, a segurança na transmissão entre os dispositivos. Esta biblioteca coloca uma quantidade fixa de 128 bits no tamanho do bloco utilizado na criptografia, o que mais que atende a necessidade do projeto. Além disso a biblioteca permite diversas modalidades da criptografia AES-128 como a que utiliza apenas um bloco, ou múltiplo blocos usando CBC com uma ou várias chamadas.

Finalmente, a terceira biblioteca é voltada para a integração da Arduino IDE com o NodeMCU permitindo que este seja codificado por meio daquele.

3 MONTAGEM E CONFIGURAÇÃO

O sistema desenvolvido para o controle do portão compreende duas porções de *hardware* distintos, o primeiro destes é o próprio controle responsável pela transmissão do sinal para a troca de estado do portão. O segundo componente é responsável pela recepção deste sinal e pela mudança efetiva de estado do portão.

O funcionamento deste sistema se inicia com o apertar do botão do controle pelo usuário. Daí, o código de abertura do portão é criptografado e enviado para o receptor que irá decriptografar o sinal e mudar o estado do portão, caso este esteja fechado ele o mudará para aberto. Efetuada a devida mudança, será disponibilizada a mudança de estados do portão para o usuário por meio de um endereço web.

Para a melhor compreensão deste projeto este capítulo irá abordar o processo de montagem do projeto, como também, sua configuração. Primeiramente, será abordado a montagem dos dispositivos previamente mencionados e, em seguida, a configuração destes mesmos será detalhada de forma minuciosa.

3.1 MONTAGEM DOS DISPOSITIVOS

A montagem dos dispositivos foi dividida em duas partes: uma para o dispositivo transmissor / controlador e outra para o dispositivo receptor. Além desses dispositivos, também será apresentado aqui a montagem dos dispositivos usados para os testes de alcance. A Figura 17 apresenta o sistema do portão montado e configurado.

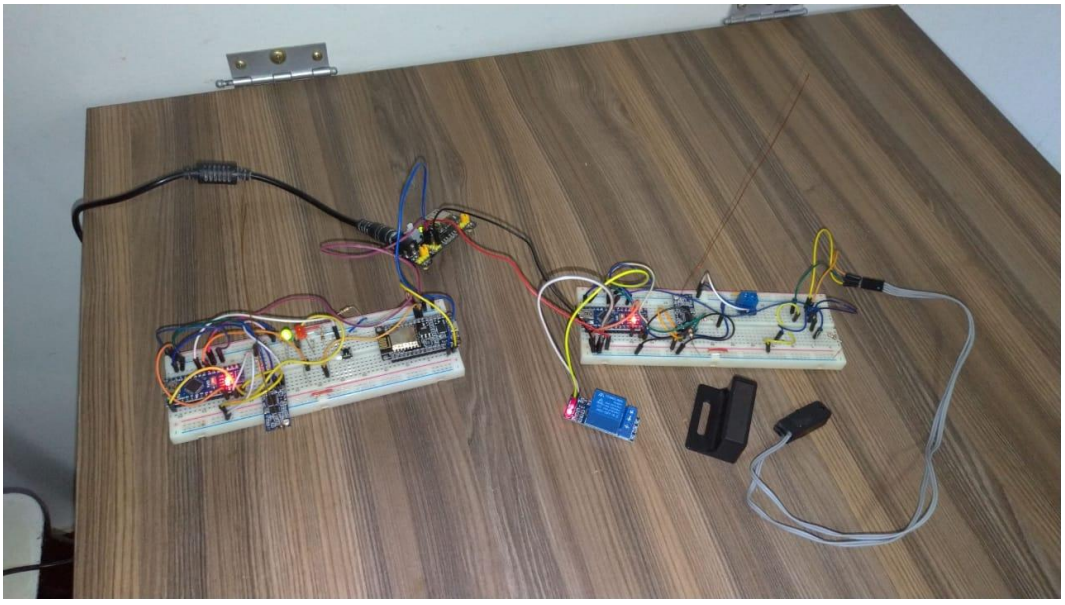

Figura 18- Ilustração do sistema do portão montado. (Própria, 2019)

3.1.1 PLACA DO CONTROLE DO PORTÃO

A montagem da placa do controle do portão foi realizada seguindo o diagrama de blocos ilustrado na Figura 18. Para deixar evidente ao usuário a mudança de estado do portão empregou-se dois *Light Emitting Diodes* (LEDs), um vermelho para denotar que o portão se encontra aberto e um verde indicando que o portão está fechado.

Como o Arduino opera em 5 V, mas o NodeMCU versão 1.0 e o módulo HC-12 operam em 3,3 V então é necessária a utilização de um divisor de tensão de modo a garantir que o Arduino não queime os pinos dos outros módulos. Para tal, utilizou-se um resistor de 4,7 kΩ e outro de 10 kΩ, que neste caso proporcionam na entrada dos pinos uma voltagem de aproximadamente 3,3 V.

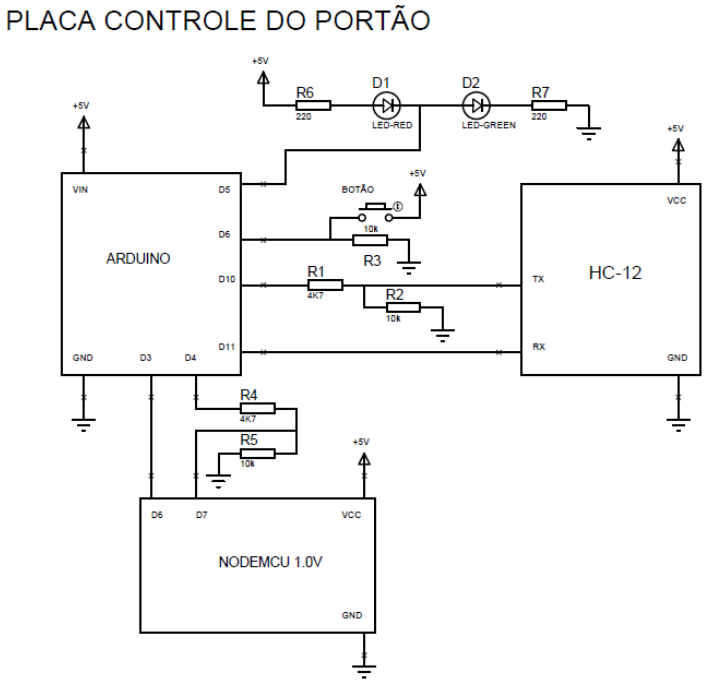

Figura 19- Diagrama de blocos para o controle do portão. (Própria, 2019)

Um detalhe importante da montagem consiste na antena que foi utilizada com o módulo HC-12. De acordo com os testes realizados a antena que proporcionou as maiores distâncias, tanto em ambientes abertos quanto em ambientes com muita interferência foi a antena dipolo feita simplesmente com um fio de cobre desencapado. Para uma antena dipolo, o seu comprimento ideal para o fio metálico é de $\lambda/2$. Calculando o valor de λ para garantir o funcionamento da antena na frequência de 433 MHz, tem-se que o comprimento do cobre deve ser de aproximadamente 6,93 cm para garantir um funcionamento ótimo. O dispositivo do controle do portão montado é ilustrado na Figura 19.

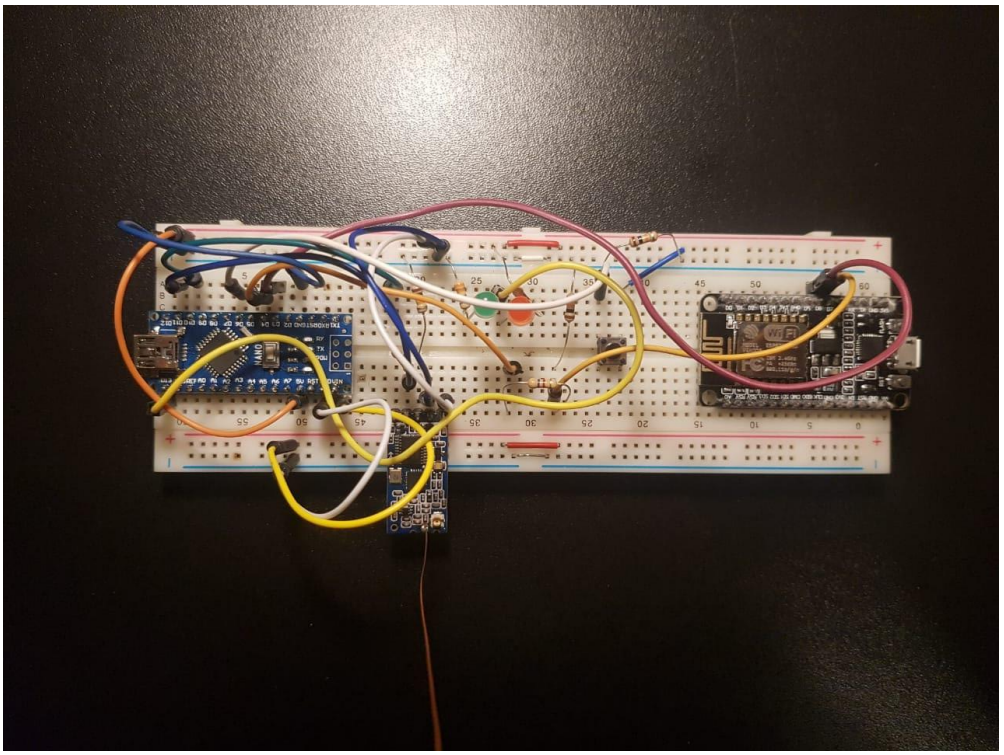

Figura 20- Imagem do controle de portão montado. (Própria, 2019)

3.1.2 PLACA DO PORTÃO

A montagem da placa do portão foi feita de acordo com o diagrama de blocos apresentado na Figura 20. Novamente, o divisor de tensão foi utilizado de modo a garantir a comunicação entre o Arduino e o módulo HC-12.

A placa do portão consiste basicamente em um Arduino Nano, um módulo HC-12, um pequeno sensor REED e um relé utilizado para o controle do motor do portão. Deve-se atentar que o relé não pode ser alimentado com a mesma fonte dos demais componentes, pois requer uma voltagem significativamente maior para o seu funcionamento, neste caso 12 V. Ademais, é importante salientar que o sensor REED neste projeto serve simplesmente como detector de estado do portão. Ao invés do uso destes sensores da forma tradicional, feitas de vidro, optou-se por utilizar um sensor magnético. Contudo, estes funcionam de maneira igual. No caso deste projeto, quando o REED está ligado, significa o portão encontra-se fechado e o LED verde no controle é acesso, caso contrário, o LED vermelho é acesso no controle. A Figura 21 apresenta o dispositivo do portão montado.

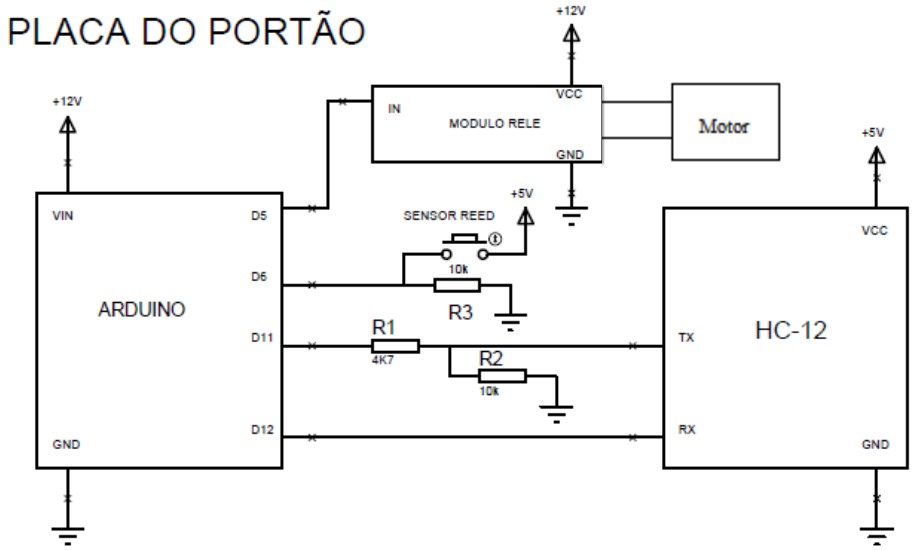

Figura 21- Diagrama de blocos da placa do portão. (Própria, 2019)

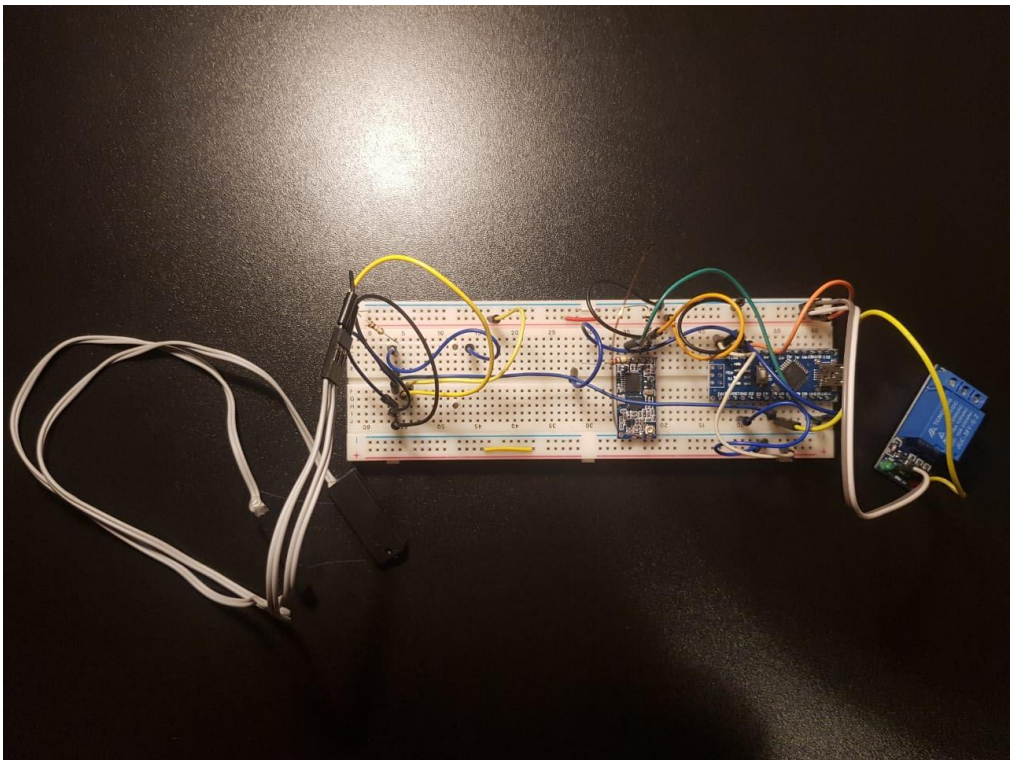

Figura 22- Ilustração da placa do portão montada. (Própria, 2019)

3.1.3 PLACAS DE TESTES

De forma a testar diversas antenas para determinar qual delas apresentava o maior alcance, engendrou-se dois dispositivos de teste com estruturas muito semelhantes. Estes dispositivos são compostos de um Arduino Nano e um HC-12. Para a alimentação do circuito utilizou-se duas pilhas e, para indicar que receptor estava recebendo as mensagens do transmissor, colocou-se um

LED na saída de um dos pinos do Arduino. A Figura 22 abaixo mostra a montagem destes dois dispositivos, como eles não são de grande relevância para o projeto sua montagem e configuração não serão abordadas com maiores detalhes.

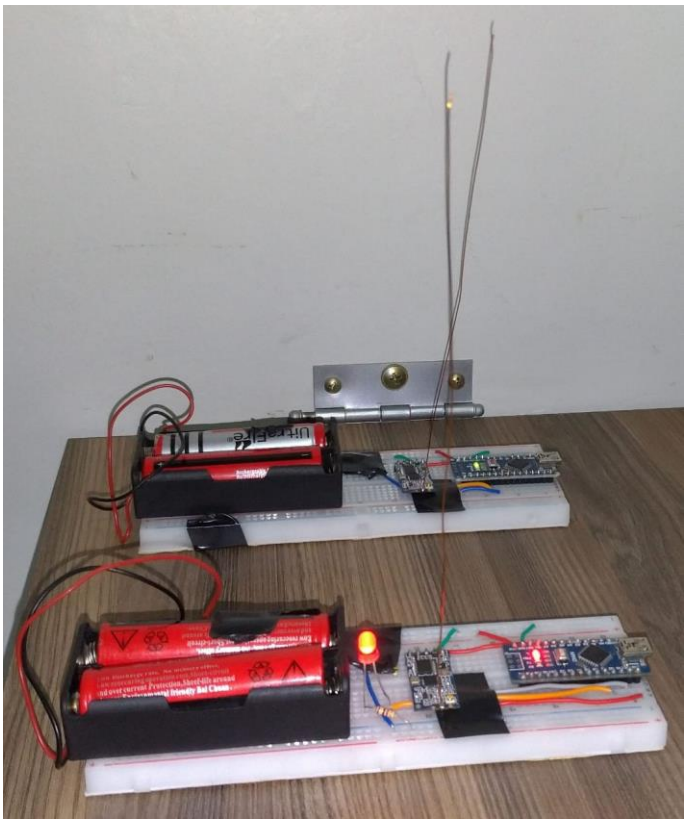

Figura 23- Dispositivos utilizados para o teste de alcance. (Própria, 2019)

3.2 CONFIGURAÇÃO DOS DISPOSITIVOS

Nesta seção serão abordadas as configurações feitas para garantir o funcionamento do projeto. Ou seja, qual a lógica foi utilizada para desenvolver o *software* dos dispositivos usados. Serão detalhadas a lógica do código tanto do Arduino (na placa de controle), como também, o da placa do portão. Ademais, também será evidenciado o código do NodeMCU utilizado.

3.2.1 LÓGICA DO ARDUINO NA PLACA DE CONTROLE DO PORTÃO

A lógica utilizada para a criação do código deste componente segue o fluxograma apresentado n a Figura 23. Primeiro, o componente passa pelo processo de *setup*, onde é definido em qual taxa (em *baud rate*), o dispositivo Arduino e o módulo HC-12 irão se comunicar. Para este trabalho usou-se o default de 9600 bps, porque esta taxa é indicada caso se queira configurar o módulo HC-12 (ROZEE, 2016). Além disso, os pinos usados serão definidos como saída ou entrada de acordo com o diagrama de blocos na Figura 18. Finalmente, ainda no processo inicial, os sinais de controle que serão enviados passam pelo processo de criptografia do AES-128.

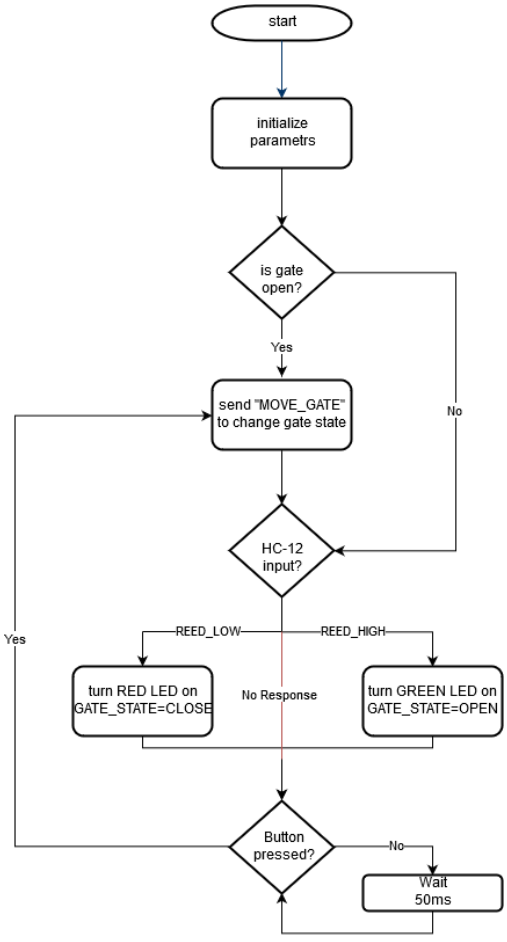

Figura 24- Fluxograma do código embarcado no controle do portão. (Própria, 2019)

Após esse processo de inicialização, o código entre em um laço onde a cada 50 ms o Arduino verifica se o botão foi apertado. Dependendo do estado em que se encontra o portão na hora da ativação do botão o Arduino envia o código para mudar o estado do portão para o HC-12.

3.2.2 LÓGICA DO ARDUINO NA PLACA DO PORTÂO

O fluxograma da Figura 24 descreve a lógica usada neste componente, a lógica entre este componente e o anterior são similares. Novamente, a primeira etapa deste componente é a configuração inicial. Diferente do outro dispositivo a comunicação serial é feita pela taxa de 1200 bps, já que nesta taxa a sensibilidade da antena aumenta, o que acaba por aumentar o alcance dos sinais recebidos do transmissor (ROZEE, 2016).

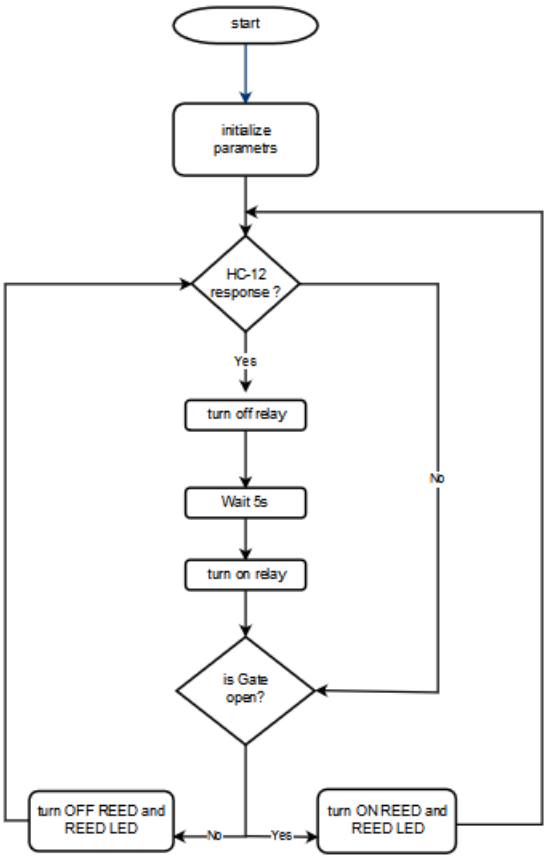

Figura 25- Fluxograma do código embarcado na placa do portão. (Própria, 2019)

Diferente do outro dispositivo, este precisa primeiro esperar para receber a mensagem para depois atuar. Para tanto, o Arduino espera um intervalo de 2,5 segundos para verificar no buffer do módulo HC-12 se alguma mensagem foi enviada. Ao conseguir a mensagem o Arduino, usando a chave pré-estabelecida entre os dois dispositivos, decriptografa a mensagem e a partir desta realiza o comando dado pela mensagem. Este comando é realizado pelo Arduino ao enviar um sinal para o relê. Em seguida, o receptor envia ao transmissor as informações do

sensor REED e, por consequência, o estado do portão.

3.2.3 LÓGICA DO NODEMCU

Como nos casos anteriores, a lógica empregada na configuração do NodeMCU segue o fluxograma apresentado na Figura 25. No processo de inicialização deste dispositivo, o *Service Set Identifier* (SSID) e as credenciais do Wi-Fi são geradas. Neste trabalho utilizou-se a SSID "Portao" e a senha "Portao" simplesmente para fins de teste. Daí, um servidor web é criado usando a porta 8008, com o IP estático que neste trabalho foi definido como 192.168.1.135. Em seguida, os pinos são inicializados para a comunicação com o Arduino e o servidor se inicia.

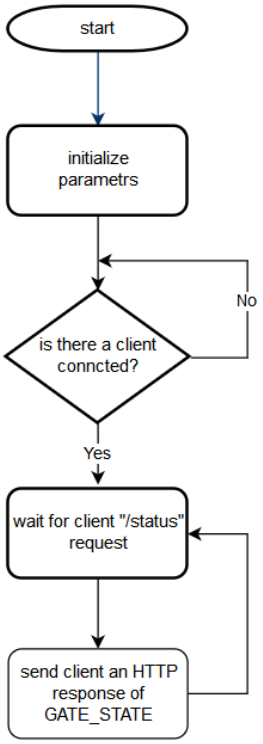

Figura 26- Fluxograma do código embarcado no NodeMCU. (Própria, 2019)

O NodeMCU, a partir da sua conexão com o Arduino, consegue detectar as mensagens enviadas para o HC-12 e partindo ao se conectar com um cliente envia o estado do portão por meio de um HTTP *response*. Deve-se salientar novamente que embora o protocolo HTTP não seja seguro, as mensagens sendo enviadas do HC-12 são todas criptografadas.

Para disponibilizar o estado do portão para o usuário via Wi-Fi, o NodeMCU recebe as mensagens do HC-12 do receptor acerca do estado do sensor REED. De forma a facilitar a visualização do funcionamento do servidor *web* usou-se o aplicativo HTTP Shortcuts que faz apenas um simples HTTP *request* para receber a resposta do NodeMCU. A interface gráfica deste aplicativo é apresentada na Figura 26.

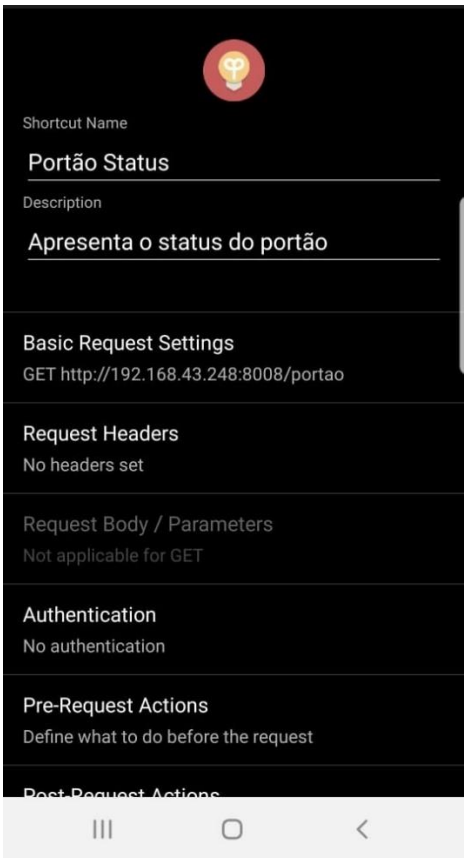

Figura 27- Ilustração do app HTTP Shortcuts usado para descobrir o estado do portão. (Própria, 2019)

4 ENSAIOS

Para se chegar na versão final deste projeto foram feitos alguns ensaios de modo a otimizar a operacionalização do dispositivo e verificar o orçamento necessário para se comprar o sistema.

4.1 TESTE DE ALCANCE

O primeiro ensaio que será discutido é o do teste de alcance com diversas antenas. Como explicado nos capítulos anteriores, este projeto depende do alcance do sinal do transmissor para ser efetivo. Portanto, de forma a melhorar o resultado e obter a máxima distância possível foram testadas algumas configurações com o HC-12, mudando tanto o seu *baud rate* como a antena usada. As antenas que foram testadas são ilustradas na Figura 27 abaixo.

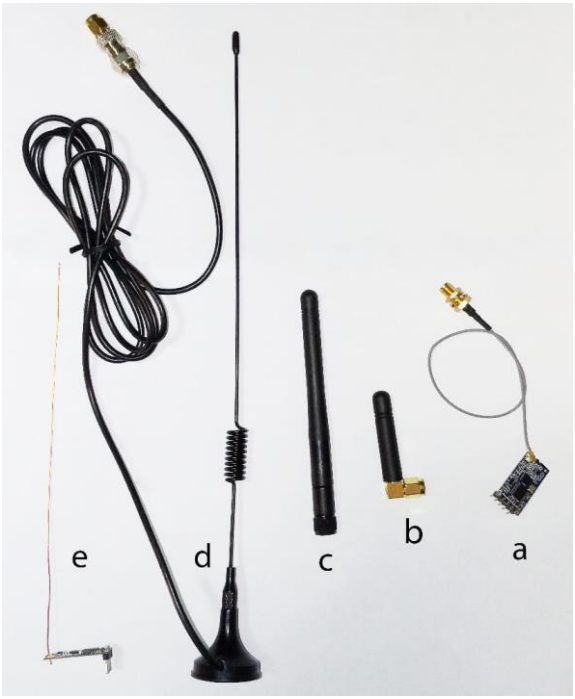

Figura 28- Imagem das antenas usadas na realização do teste de alcance. (Própria, 2019)

O teste do *baud rate* acabou por se tornar inútil, já que como discutido acima um *baud rate* menor significa uma sensibilidade maior para o HC-12. Logo, é melhor manter este em seu valor mais baixo que é 1200 bps.

No teste das antenas nota-se pela Figura 27 que, antenas menores também foram testadas. Estas antenas, correspondidas pelas letras “c” e “b” na Figura 27 não são adequadas para o uso neste sistema, pois são antenas de 2,4 kHz. Estas foram escolhidas pela curiosidade de se verificar o quanto o aumento da frequência é capaz de estancar o alcance do sinal. As antenas que eram candidatas plausíveis eram a antena “e” e a “d”, sendo a “e” um simples fio de cobre

desencapado e a antena ‘d’ uma antena comprada que anunciava um ganho de 12 dBi. O dispositivo “a” na Figura 27 não é uma antena, este é o HC-12 preparado para o encaixe das outras antenas testadas, excluindo o fio de cobre. Os resultados dos testes realizado são encontrados na Tabela 1.

Antena	1200bps Ch01 Rp:20dBm FU3					
	Alcance Área Urbana [metros]		Alcance Área Rural [metros]		Alcance Área Urbana [metros]	
	Parque Olhos D'água		Chácara do Deonézio		DF 002 EIXÃO 214-211	
	22/08/19 14:30 - 15:20		31/08/2019 16:20-18:54		01/09/0219 15:00-17:00	
	Teste 1	Teste 2	Teste 1	Teste 2	Teste 3	Teste 4
1	430	--	300	309	469	-
2	102	--	90	154	212	-
3	353	--	263	295	424	-
4	755	--	305	309	1380	-
ANTENA 1: 433MHz 2dBi | ANTENA 2: 2,4GHz 2dBi | ANTENA 3: 433MHz 12dBi | ANTENA 4: CABO RÍGIDO 17,5 CM						

Tabela 1- Resultado dos testes de alcance. (Própria, 2019)

Estes resultados mostram que o fio de cobre metálico desencapado é a melhor opção para este projeto, pois este conseguiu alcançar a maior distância tanto em um campo aberto quanto em um campo com vários objetos em frente aos comunicadores. A antena comprada de 12 dBi decepcionou tendo resultados bem piores do que o esperado. Um motivo para este acontecimento pode ser devido à diretividade desta antena, que a tornou ineficiente em lugares onde uma radiação isotrópica seria mais vantajosa.

É importante salientar que nos testes feitos para o “Alcance Área Rural” na Chácara do Deonézio o alcance máximo permitido era de 309 metros. Portanto, a antena atingir o alcance máximo neste teste não significa que este é o alcance máximo da antena. Por exemplo, a antena 4 teve um alcance de 309 metros na área rural, ou seja, ela teve o alcance máximo daquela área, porém, pelos testes nas áreas urbanas percebe-se que o seu alcance máximo é mais elevado.

4.2 CUSTO ESTIMADO

Para verificar se um dos objetivos do projeto foi cumprido (o custo baixo do sistema em relação ao mercado) foi feito um orçamento considerando todo o equipamento necessário para a confecção deste dispositivo. O orçamento foi feito com base no sistema inteiro do portão, excluindo da conta apenas o motor do portão, logo que não foi possível encontrar um

preço para este componente isoladamente. O orçamento é apresentado na Tabela 2.

Ref.	Nome	Qtd	Valor Unitário	Total
ADNNANO0000R3	Arduino Nano R3	2	R$ 34,90	R$ 69,80
MDLWIR433HC12	Módulo Transceptor RF 433Mhz SI4463 - HC12	2	R$ 36,90	R$ 73,80
MDLWIFIESP12E	Módulo WiFi ESP8266 ESP-12E	1	R$ 23,44	R$ 23,44
CDTFOESM19AWG	FIO DE COBRE ESMALTADO 19AWG (155?)	2	R$ 1,40	R$ 2,80
PLPFNCM1F2020	PLACA FENOLITE VIRGEM (FACE SIMPLES 20x20cm)	2	R$ 14,60	R$ 29,20
MDLRL5V01CGBK	MÓDULO RELÉ 5V/1CANAL	1	R$ 5,90	R$ 5,90
		Produtos		R$ 204,94
		Frete		R$ 0,00
		Desconto		-R$ 0,00
		TOTAL		R$ 204,94

Tabela 2- Orçamento para o sistema do portão excluindo o motor. (Própria, 2019)

O preço final do sistema foi ligeiramente maior do que o esperado, caso fossem adicionados os trilhos e o motor do portão o preço cotado ultrapassaria a faixa de R$ 300. Contudo, em várias lojas existem portões que por terem algumas funcionalidades a mais, como, por exemplo, um sistema de alarme ao deixar o portão aberto está nessa faixa de preço; enquanto os portões mais sem estas utilidades (só com as básicas) estão abaixo dessa faixa de preço. Portanto, tomando em conta as serventias oferecidas por este sistema, o preço total é relativamente econômico.

5 CONCLUSÃO

O sistema composto pelos dispositivos: controle de portão e portão, desenvolvidos neste projeto atenderam todos os requisitos que foram propostos. O resultado final é capaz não só de garantir a comunicação de longa distância, como também consegue efetuar uma comunicação de modo a prevenir métodos de invasões de privacidade e furto de dados. Além disso, o resultado final é capaz de disponibilizar o estado do portão para o usuário de uma maneira simples, de modo que este não precisaria ter uma visada direta com o portão para saber se este abriu de fato ou não.

O custo final deste projeto ficou um pouco acima do esperada, passando um pouco mais dos R$ 200 sem considerar os custos adicionais do motor. Embora esse preço seja mais alto do que esperado, comparando com o que é ofertado no mercado e considerando as diversas funcionalidades do sistema desenvolvido neste trabalho o preço pode ser considerado competitivo, desde que feitas algumas mudanças que serão explicitadas a seguir.

Este projeto embora tenha cumprido o seu objetivo de forma satisfatória ainda pode ser melhorado para efetivamente se tornar um produto comerciável. Primeiramente, para reduzir os custos do projeto em si deve-se substituir a placa Arduino por um outro microcontrolador mais barato como o MSP430. Além desta modificação a experiência do usuário também poderia ser melhorada drasticamente. Ao invés do usuário ter que se conectar com o NodeMCU a partir de um *app* que apenas mostra os *requests*, seria melhor se o usuário tivesse um simples aplicativo de celular dedicado ao sistema e capaz de mostrar o estado do portão e de disparar um alarme no caso do portão permanecer no estado “aberto” por muito tempo.

Feitas todas as ressalvas acima e exposto todos os melhoramentos desejados para o futuro pode-se concluir que apesar dos problemas enfrentados o projeto consegue suprir a sua demanda e resolver o problema para cujo ele foi criado. Ademais, o projeto foi um sucesso já que o seu *modus operandi* atual satisfaz a demanda do cliente.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] MUNIZ, Eduardo. **Dependência tecnológica, o maior mal desta geração**. [*S. l.*]: Gazeta do Povo, 2019. Disponível em: https://www.gazetadopovo.com.br/opiniao/artigos/dependencia-tecnologica-o-maior-mal-desta-geracao-2r72udomja0wksq5teq16oiq4/. Acesso em: 15 nov. 2019.

[2] P., Reinaldo. **"Regulagem" de alcance portão eletrônico Garen**. [*S. l.*: *s. n.*], 2008. Disponível em: https://www.clubedohardware.com.br/forums/topic/567720-regulagem-de-alcance-port%C3%A3o-eletr%C3%B4nico-garen-fotos/. Acesso em: 5 dez. 2019.

[3] BALANIS, Constantine. **Antenna theory: analysis and design**. 3. ed. [*S. l.*]: John wiley & sons, 2016.

[4] STROSKI, Pedro. **Production of Electromagnetic Waves**. [*S. l.*]: Electrical elibrary, 2018. Disponível em: http://www.electricalelibrary.com/en/2018/09/28/antennas-part-2/. Acesso em: 15 nov. 2019.

[5] CLOUDE, Shane. **An Introduction to Electromagnetic Wave Propagation & Antennas**. [*S. l.*]: John wiley & sons, 1996.

[6] LODRO, Mir. **Antennas and Wave Propagation**. [*S. l.*]: University of Nottingham, 2016.

[7] RAVI. **Different Types of Antennas & Characteristics of Antenna**. [*S. l.*: *s. n.*], 2019. Disponível em: https://www.electronicshub.org/types-of-antennas/. Acesso em: 21 nov. 2019.

[8] TILBORG, Henk. **FUNDAMENTALS OF CRYPTOLOGY**: A Professional Reference and Interactive Tutorial. [*S. l.*]: KLUWER ACADEMIC PUBLISHERS, 2006.

[9] ALTIGANI, Abdelrahman; BARRY, Bazara; ELSADIG, Muawia. **Evaluating AES Performance Using NIST Recommended Block Cipher Modes of Operation**. Langkawi, Malaysia: The 4th International Conference on Computer Science and Computational Mathematics (ICCSCM), 2015.

[10] MARGARET, Rouse. **Advanced Encryption Standard (AES)**. [*S. l.*]: SearchSecurity, ca. 2015. Disponível em: https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard. Acesso em: 7 nov. 2019.

[11] KUROSE, James; ROSS, Keith. **Computer networks: A top down approach featuring the internet**. [*S. l.*]: Peorsoim Addison Wesley, 2010.

[12] HELGESCHNEIDER. Tut02: ESP8266 mit Arduino – Externe LED mit Vorwiderstand schalten. **wvssiot.wordpress.com**, 2017. Disponivel em: <https://wvssiot.wordpress.com/2017/02/03/tut01-esp8266-mit-arduino-externe-led-mit-

vorwiderstand-schalten/>. Acesso em: 28 abr. 2018. il.color.

[13] ARDUINO Nano (V2.3): User Manual. 2.3. ed. [*S. l.*]: Creative Commons Attribution Share-Alike 2.5, ca. 2015. 5 p.

[14] ARDUINO IDE 1.0.1. [*S. l.*]: MeetArduino, 2012. Disponível em: https://meetarduino.wordpress.com/2012/06/12/arduino-ide-1-0-1/. Acesso em: 7 nov. 2019.

[15] NUNES, Álvaro. **ARVIM**: Automação Residencial Via Mobile. [*S. l.*]: Universidade de Brasília, 2018.

[16] ARDUINO NANO Pinout Diagram. [*S. l.*: *s. n.*], 2019. Disponível em: https://www.teachmemicro.com/category/reference/. Acesso em: 7 nov. 2019.

[17] LUA 5.3 Reference Manual. [S. l.: s. n.], 2018. Disponível em: https://www.lua.org/manual/5.3/. Acesso em: 5 dez. 2019.

[18] SZDOIT. User Manual for ESP12E Dev Kit. **smartarduino.gitbooks.io**, 2015. Disponivel em: <https://smartarduino.gitbooks.io/user-manual-for-esp-12e-devkit/content/chapter1.html>. Acesso em: 9 ago. 2017.

[19] HUGHES, Mark. **Understanding and Implementing the HC-12 Wireless Transceiver Module**. [*S. l.*: *s. n.*], 2016. Disponível em: https://www.allaboutcircuits.com/projects/understanding-and-implementing-the-hc-12-wireless-transceiver-module/. Acesso em: 15 nov. 2019.

[20] ROZEE, Robert. **HC-12 Wireless Serial Port Communication Module**: User Manual version 2.3B. 2.3B. ed. [*S. l.*: *s. n.*], 2016. 8 p

[21] MOTA, Allan. **Módulo relé - Acionando cargas com Arduino**. [*S. l.*: *s. n.*], 2017. Disponível em: https://portal.vidadesilicio.com.br/modulo-rele-com-arduino/#Modulo_rele_8211_Acionando_cargas_com_Arduino. Acesso em: 7 nov. 2019.

[22] ARDUINO core for ESP8266 WiFi chip. [*S. l.*: *s. n.*], 2019. Disponível em: https://github.com/esp8266/Arduino. Acesso em: 19 nov. 2019.

APÊNDICE A – ESQUEMÁTICO DAS MONTAGENS

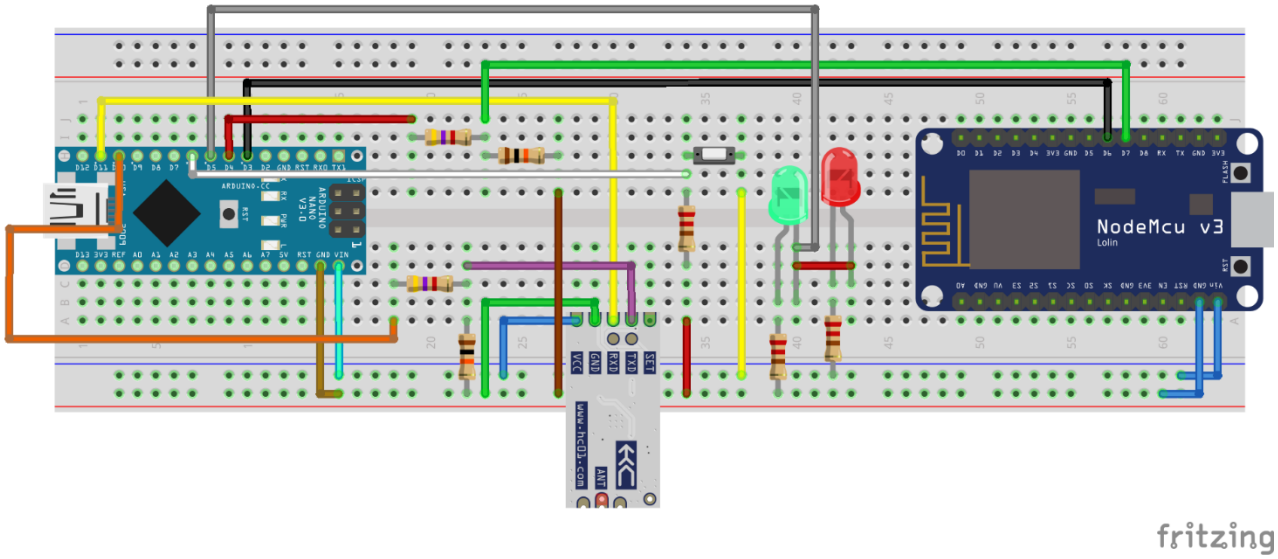

Figura 29- Esquemático da montagem do controle do portão. (Própria, 2019)

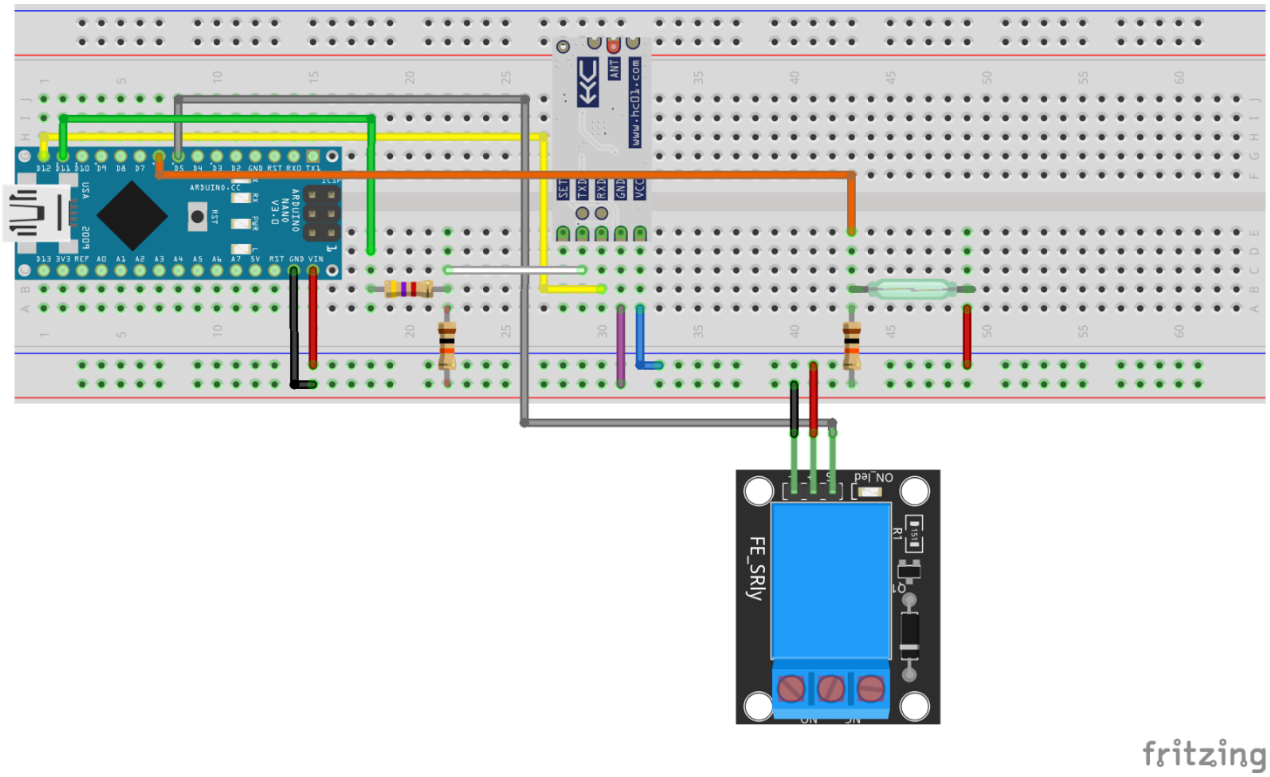

Figura 30- Esquemático da montagem da placa do portão. (Própria, 2019)