# UMA IMPLEMENTAÇÃO DE CONTROLADOR DE ACESSOS DE BAIXO CUSTO UTILIZANDO CARTÕES RFID

WAGNER LOCH[1]; RAFAEL IANKOWSKI SOARES[2]

[1]*Universidade Federal de Pelotas – wloch@inf.ufpel.edu.br*
[2]*Universidade Federal de Pelotas – rafael.soares@inf.ufpel.edu.br*

## 1. INTRODUÇÃO

Com um enorme tráfego de pessoas, seja em eventos, shows, palestras ou até mesmo em aulas, surge a necessidade de controlar o acesso de seus frequentadores, tanto por motivos de segurança quanto para controle de seus organizadores. Para cada aplicação, existem diferentes tipos de produtos que atendem essa necessidade. Muitas vezes a solução para cada problema possui um alto custo financeiro e precisa ser desenvolvida especificamente para aquele tipo de solução. Por exemplo, a catraca de um ônibus é controlada por um dispositivo leitor de cartões ou por um cobrador, que libera ou impede a passagem de pessoas. Já numa casa de shows, existem pessoas responsáveis pelo recolhimento do ingresso, verificando no ato sua autenticidade.

Utilizando a tecnologia de identificação por radiofrequência ou RFID (do inglês “Radio-Frequency Identification”), que é um método de identificação automática utilizando sinais de rádio através de etiquetas ou cartões de uso pessoal, é possível realizar a identificação e controle de acesso de pessoas ou objetos a lugares restritos, nos mais variados tipos de aplicações. Esta tecnologia pode vir a dispensar o uso de funcionários dedicados a identificar e permitir o acesso de pessoas, por exemplo. “A maior vantagem das etiquetas RFID são o seu pequeno custo e reduzido tamanho (VERMA; TRIPATHI, 2010)”.

Entretanto, assim como em todos os sistemas de identificação pessoal, existem usuários mal intencionados visando encontrar falhas nos sistemas a fim de obter vantagens ilícitas. Neste caso, as questões de segurança também são uma preocupação na implementação do sistema. De acordo com a literatura, o principal problema com as etiquetas RFID são as clonagens que podem ser facilmente realizadas (ZANETTI; FELLMANN; CAPKUN 2010).

Neste trabalho é proposto um sistema de identificação e controle de acesso utilizando tecnologia RFID apresentando uma solução de baixo custo tanto em hardware quanto em software a fim de gerar um produto genérico que pode ser utilizado para controle de acesso em diversas aplicações. O produto obtido além de ter um custo reduzido comparado a outros semelhantes disponíveis no mercado propõe uma solução básica e eficiente para lidar com a clonagem de etiquetas RFIDs baseada na proposta de Zanetti, Fellmann e Capkun.

## 2. METODOLOGIA

O diagrama exibido na Figura 1 demonstra basicamente o funcionamento do sistema proposto. As etiquetas RFID devem ser aproximadas do leitor para que sejam lidas e suas informações enviadas a um microcontrolador, neste exemplo um microcontrolador ATMEGA328 presente na plataforma Arduino UNO. O microcontrolador transmite as informações para um servidor remoto. Neste servidor as informações são processadas de acordo com a aplicação desejada

pelo cliente, como por exemplo o controle de frequência de alunos em uma sala de aula.

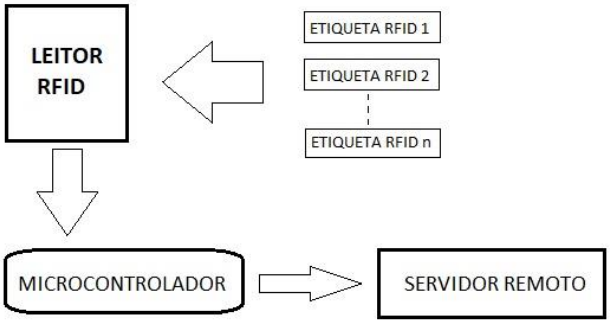


Figura 1: Diagrama do sistema

Inicialmente são propostos experimentos a fim de dominar a tecnologia utilizada no projeto. Com este propósito são realizados experimentos como leitura das etiquetas RFID, extração de informações e verificação de registro de dados. Além disso, são realizados experimentos com os módulos de comunicação para transmissão das informações a um servidor remoto. Esse servidor será responsável por tratar todas as informações lidas e deve ser específico para cada funcionalidade, por exemplo, para o controle de presença em um show, o servidor será diferente do controle de frequência de uma escola, pois cada um tem uma necessidade específica.

O sistema aqui desenvolvido pode ser acoplado com o Sistema Integrado de Gestão Cobalto da Universidade Federal de Pelotas (UFPel) para realizar o controle de frequência dos alunos. O sistema proposto é composto pelos itens especificados na Tabela 1 integrados a um servidor remoto por meio de uma interface da aplicação (do inglês, Application Programming Interface – API). Deste modo, os docentes e discentes podem ter o controle de suas presenças contabilizadas sem a necessidade de interrupções ou atrasos para a checagem de presentes.

Tabela 1: Componentes utilizados no sistema proposto.

| | |
|---|---|
| 1 | Arduino Uno |
| 1 | Leitor/Gravador de Cartões RFID MFRC522 |
| 1 | Módulo de Conexão Ethernet ENC28J60 |
| 2 | Leds |
| 1 | Buzzer |
| 1 | Case de Plástico |
| 1 | Fonte de Alimentação 12v |
| n | Etiquetas RFID |
| n | Cabos para Conexões |

Com o domínio das tecnologias a serem empregadas no sistema é realizada a montagem do hardware conforme o diagrama de ligação mostrado na Figura 2. Com a integração dos módulos e montagem em uma caixa para obtenção do protótipo final, realizam-se experimentos no campo de atuação do sistema. Neste momento, um novo requisito é adicionado ao mesmo, a questão da segurança e autenticação dos usuários. Como as etiquetas são muito comuns

e disponíveis no mercado é possível haver clonagens das mesmas, o que poderia ser um problema para o sistema.

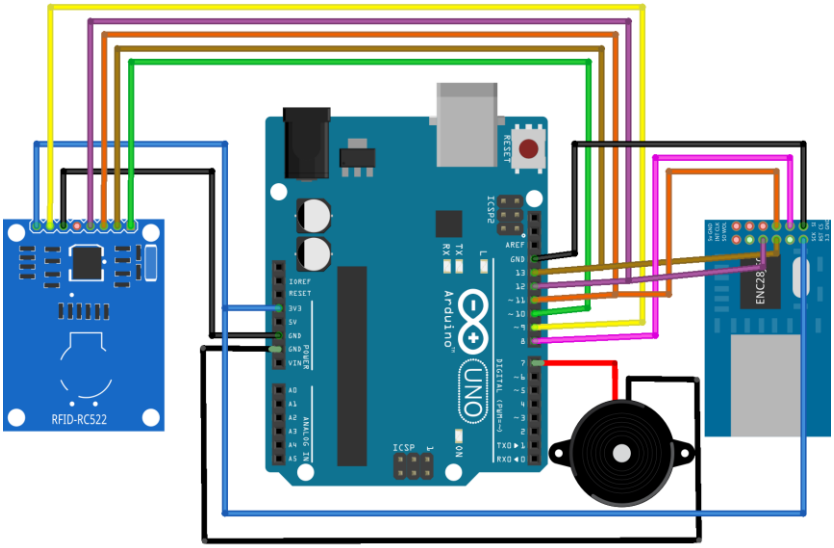


Figura 2: Diagrama de ligação.

Conforme proposto por Zanetti, Fellmann e Capkun, para contornar o problema da clonagem implementa-se um algoritmo que ao mesmo tempo que faz a leitura, realiza-se também a gravação de diversas informações. Essas informações devem ser sincronizadas com o servidor. Dessa maneira, torna-se inútil a clonagem do cartão se o mesmo for utilizado com frequência pois o clone será facilmente detectado. Além disso, é proposto também o uso de um código gerado aleatoriamente. Esse código não deve ser conhecido externamente, a fim de tornar o sistema mais seguro. O fluxograma do algoritmo proposto é exibido na Figura 3.

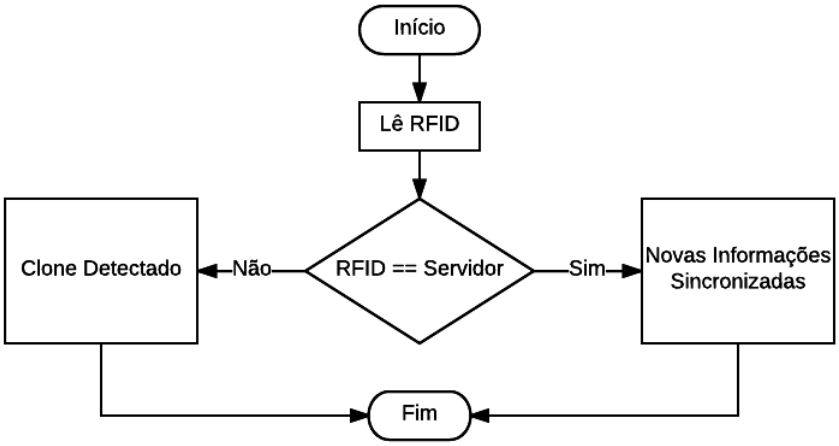


Figura 3: Fluxograma do algoritmo para detecção de clones

## 3. RESULTADOS E DISCUSSÃO

A elaboração desse protótipo teve um custo bastante reduzido se comparado com outros dispositivos no mercado que realizam funções semelhantes.

O Porteiro Eletrônico Xpe 1001 da Intelbras realiza apenas uma função específica, verificar se a etiqueta está cadastrada e liberar acesso. O modelo

apresentado aqui pode realizar essa e muitas outras funções que podem ser implementadas externamente utilizando uma API com um custo cinco vezes inferior. Por outro lado, o sistema proposto necessita estar conectado a uma rede de comunicação para executar suas funcionalidades, podendo essa ser cabeada ou WiFi utilizando o módulo ESP8266. Durante os testes, a rede WiFi não se mostrou muito confiável, tendo problemas de recepção caso o módulo estivesse muito afastado do ponto de conexão. O problema da implementação desse modelo é a sua necessidade de uma API diferente para cada aplicação.

A disposição interna dos componentes proposta neste trabalho mostrada na Figura 4 é apenas um exemplo e pode ser realizada de maneira alternativa, podendo até mesmo economizar espaço interno.

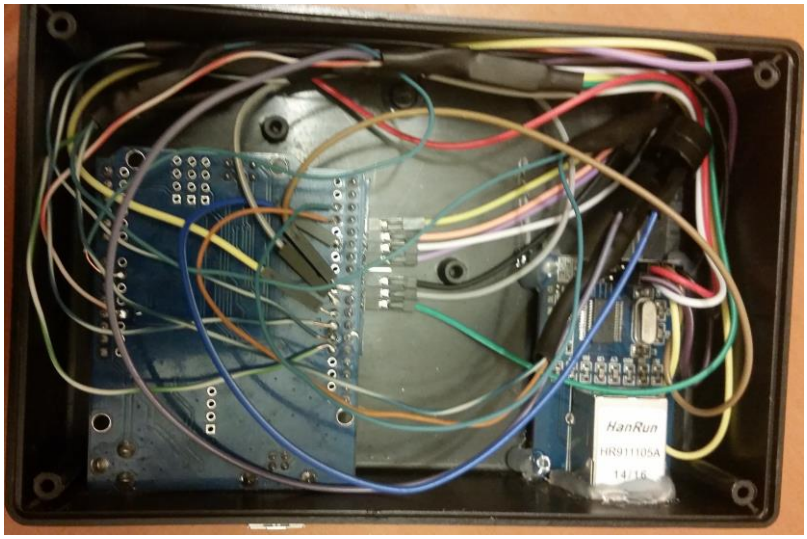


Figura 4: Disposição interna dos componentes na caixa.

## 4. CONCLUSÕES

Neste trabalho foi realizada a implementação e construção de um dispositivo controlador de acessos de propósito geral de baixo custo. Os testes realizados durante a utilização demonstraram que o controlador é eficiente e facilmente configurável, ou seja, pode ser utilizado em diferentes aplicações. Não é possível impedir a clonagem dos cartões, mas é possível alertar as suas utilizações, por isso, o sistema de detecção de clones mostrou-se eficiente em seus testes.

O custo dos materiais aqui apresentados podem ser reduzidos se comprados em grandes quantidades, o valor é irrisório se comparado com outros dispositivos que realizam as mesmas funções, demonstrando que o dispositivo pode ser utilizado em larga escala, como em universidades, eventos etc.

## 5. REFERÊNCIAS BIBLIOGRÁFICAS

VERMA, G. K.; TRIPATHI, P. **A digital security system with door lock system usign rfid technology**. International Journal of Computer Applications, 2010.

ZANETTI, D.; FELLMANN, L.; CAPKUN, S. **Privacy-preserving clone detection for rfid-enabled supply chains**. 2010