Utilizando a plataforma Arduino para a comunicação entre dispositivos embarcados e redes TCP/IP

Alexandre Silva Rodrigues
Colégio Técnico Industrial de Santa Maria
Universidade Federal de Santa Maria, UFSM
Santa Maria, Brasil
alexandre.rodrigues@redes.ufsm.br

Tiago Antonio Rizzetti
Colégio Técnico Industrial de Santa Maria
Universidade Federal de Santa Maria, UFSM
Santa Maria, Brasil
rizzetti@gmail.com

***Resumo*—A crescente expansão da conectividade entre dispositivos na internet e os recursos da plataforma Arduino possibilitam a comunicação entre dispositivos embarcados e redes TCP/IP. Uma grande aplicação desse contexto é um sistema de autenticação de usuários e controle de acesso em ambientes restritos. A Arquitetura ESC apresenta-se como uma proposta para esses aspectos e utiliza a plataforma Arduino para interligar um conjunto de hardware e software por meio de protocolos de comunicação que possibilitam a transferência de informações entre dispositivos embarcados e a rede tradicional de computadores.**

Palavras-chave—Internet das coisas; Arduino; controle de acesso; dispositivos embarcados.

I. INTRODUÇÃO

Conforme a crescente evolução tecnológica, a internet vive um novo momento. Trata-se do conceito de Internet das Coisas (*Internet of Things* ou *IoT*), que proporciona uma vasta gama de recursos a serem explorados e mudanças constantes na forma de comunicação via internet [1].

A Internet das Coisas é formada por uma rede que interconecta objetos (qualquer dispositivo conectado a Internet), onde qualquer objeto pode enviar informações para outros objetos e pessoas [1]. Ou seja, é a interconexão entre objetos físicos e computadores com a internet, transformando tudo que nos cerca em objetos inteligentes (*smart objects*) [2]. A conexão de tais objetos com a internet acontece por meio de endereços IP e URLs, assim como funcionam as páginas Web atuais. Desta forma, os objetos em nosso ambiente tornam-se participantes ativos, ou seja, compartilham informações com outros membros da rede, com capacidade de reconhecer eventos e mudanças no ambiente e de agir de forma autônoma. Com isso, em um mundo onde o real, o digital e o virtual convergem, é possível criar ambientes inteligentes e inúmeras aplicações a serem desenvolvidas [3].

Nesse contexto, a plataforma Arduino desempenha um papel fundamental na interconectividade entre diversos dispositivos. O Arduino é uma plataforma utilizada para programação de microcontroladores responsáveis por processar entradas e saídas entre o dispositivo e os componentes externos conectados a ele. A principal contribuição da plataforma Arduino é facilitar a integração entre dispositivos eletrônicos e a rede tradicional de computadores. Dessa forma, provendo uma nova gama de oportunidades de softwares e hardwares capazes de automatizar diversas atividades cotidianas, desde o controle de portões eletrônicos, via celular, até sistemas complexos para monitoramento de ambientes. Seu hardware consiste em um projeto simples de hardware livre para o controlador, com um processador Atmel AVR e suporte embutido de entrada/ saída. O software consiste de uma linguagem de programação padrão e do *bootloader* que executa na placa [4] [5].

O Arduino pode utilizar diferentes componentes que permitem a comunicação entre dispositivos ou até mesmo entre plataformas embarcadas e qualquer outro dispositivo na rede IP. Por exemplo, a plataforma Arduino pode ser usada para enviar um conjunto de dados de sensores a ele conectados para um cliente qualquer na Web, através do uso do protocolo HTTP [4] [5].

Relacionado com o contexto de conectividade que a Internet das Coisas oferece e utilizando a plataforma Arduino como base de sua arquitetura, o Projeto ESC (desenvolvido pelos autores deste artigo) desenvolve uma arquitetura (denominada Arquitetura ESC) capaz de realizar o gerenciamento de permissões e controle de acesso a ambientes físicos. Este artigo visa apresentar essa arquitetura (hardware e software), abordando o uso da plataforma Arduino para realizar a comunicação entre dispositivos embarcados e redes TCP/IP. Além disso, será descrito um protocolo utilizado para realizar a comunicação entre duas placas via porta serial e serão apresentados resultados de desempenho da arquitetura em questão.

II. ARQUITETURA ESC

Em instituições onde existe uma alta rotatividade de pessoas, um gerenciamento de identidades é fundamental para manter um controle de acesso a ambientes restritos. Esse processo envolve as seguintes ações:

- Autenticação: realiza o teste da identificação de determinado usuário. Pode ocorrer por diferentes métodos: biometria, senhas, cartão, entre outros;
- Autorização: é a capacidade de estabelecer se uma identidade tem a permissão de acessar um local;
- Auditoria: cada evento deve ser registrado para eventuais consultas [6].

Para tanto, é preciso um sistema capaz de realizar tais ações e garantir que apenas pessoas autorizadas possam acessar um ambiente. Com o objetivo de apresentar uma solução para isso, a Arquitetura ESC (*Environment Security Control*) apresenta uma proposta para o controle de tais locais, estabelecendo uma comunicação entre dispositivos de interação com o meio físico e um gerente que centraliza as informações. Essa arquitetura realiza a autenticação de cada usuário que deseja acessar algum ambiente, permitindo ou não o seu acesso. Além disso, é possível gerar relatórios de acesso a cada local ou por usuários, para fins de auditoria. Tais funcionalidades possibilitam uma forma eficiente e segura de controle de acesso a ambientes restritos em instituições, além de substituir o uso de chaves físicas por chaves digitais que identificam cada usuário.

A Arquitetura ESC divide-se em dois subsistemas: o gerente (ESCMA), que aplica as políticas de permissões e realiza a conexão com o sistema; e um conjunto de hardware e software (ESCHA) baseado na plataforma Arduino, que atua como um dispositivo físico para coletar dados que são enviados para o gerente e realiza ações sobre o sistema através de atuadores [7].

A. ESCMA

O gerente atua de forma centralizada sobre os diversos hardwares que compõe o sistema, armazenando informações sobre todo o sistema, o que lhe proporciona flexibilidade e escalabilidade. Um aspecto sobre o gerente é sua arquitetura escalável que permite incluir novos dispositivos físicos e/ou diferentes tipos de dispositivos de entrada de dados (RFID, biometria, teclado, etc.) ao sistema através da inclusão de novos conectores. Cada categoria de dispositivo utiliza uma classe de conectores que recebem os dados do ESCHA e após o processamento, retornam os dados para o ESCHA [8].

Após receber dados do ESCHA, o gerente realiza uma comunicação com sua base de dados, onde ficam cadastrados os usuários do sistema e as respectivas permissões ou restrições, que retorna com o tipo de acesso que determinado usuário possui para o local que está tentando acessar. De acordo com essa resposta, o ESCMA envia para o ESCHA qual ação deve ser realizada. Esta comunicação ocorre por meio de um conector específico. Diferentes bases de dados podem ser utilizadas, pois, para cada base existe uma classe correspondente [8].

A comunicação entre os dois subsistemas da Arquitetura ESC é desenvolvida na camada de aplicação e utiliza a pilha de protocolos TCP/IP, que oferece as funcionalidades necessárias ao tráfego de dados entre os dispositivos e o gerente [7].

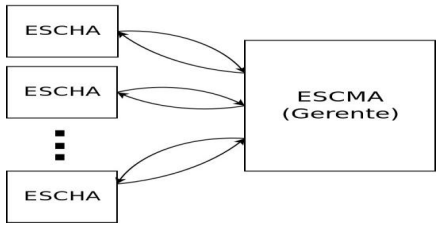

Fig. 1. Arquitetura ESC

B. Interface web e a base de dados

A interface *web* da Arquitetura ESC é responsável pela interação entre o administrador do sistema, o gerente e o hardware. Através dela é possível cadastrar os usuários no sistema com suas devidas permissões de acesso, cadastrar novos dispositivos inseridos no sistema, obter relatórios sobre cada dispositivo ou usuário e realizar ações de forma assíncrona (abertura, bloqueio e desbloqueio de portas).

Todas as informações referentes aos usuários e as permissões para cada porta ficam armazenadas em uma base de dados que pode ser facilmente modificada ou atualizada quando houver necessidade. Além disso, ela mantém informações sobre todos os dispositivos que integram o sistema.

C. Inserção de novos dispositivos ao sistema

A Arquitetura ESC por ser bastante flexível possibilita que novos dispositivos possam ser inseridos com facilidade. Sempre que um novo dispositivo é instalado, ele utiliza um endereço IP padrão e precisa ser configurado. Para isto, basta apenas acessar o endereço IP pré-configurado nele e atribuir um novo endereço IP e o *Mac adress* que utilizará para fazer parte do sistema. Os endereços recebidos serão gravados em uma memória não volátil disponível no microcontrolador (EEPROM).

O administrador do sistema deve cadastrar o novo endereço do dispositivo na base de dados e atribuir o identificador da porta que será controlada. Logo, quando o gerente receber a primeira operação do dispositivo, ele irá atribuir a identificação atribuída para o seu endereço IP.

D. ESCHA

O hardware da Arquitetura ESC utiliza a plataforma Arduino como base, sendo composto por duas placas:

- Placa principal: é uma placa específica, desenvolvida para receber um microcontrolador da Atmel e os seguintes módulos: módulo de interface de rede (*Ethernet Shield*) e um módulo e antenas para leitura e escrita em cartões RFID. Também foram adicionadas relés para o acionamento de dispositivos externos (fechadura eletromagnética, por exemplo);

- Placa auxiliar: contém um microcontrolador Atmel, um módulo de *display* LCD e um módulo e antenas para leitura e escrita em cartões RFID.

A arquitetura do sistema pode ser dividida em quatro partes:

- *Host*: o ESCHA funciona como um servidor *web*, tendo um endereço IP que o identifica na rede e podendo ser acessado via interface *web*;

- Interface Visual: exibe mensagens no visor LCD, proporcionando uma interação do sistema com o usuário;

- Dispositivo de autenticação: é o dispositivo que permite a entrada de dados (leitura de um cartão);

- Interface de rede: permite a comunicação do ESCHA com o gerente [7].

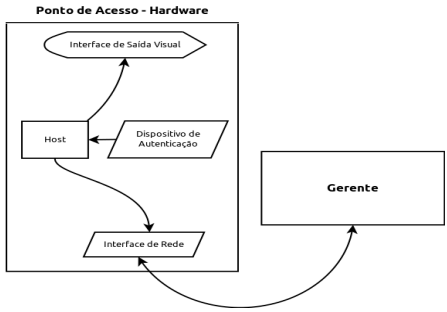

Fig. 2. Conexão do hardware com o gerente

E. Comunicação entre as duas placas do ESCHA

Para realizar a entrada de dados (leitura de cartões), os módulos e antenas RFID de cada placa são interligados, o que permite que ambas possam realizar esta operação. Sua principal aplicação é possibilitar que um local tenha um dispositivo de controle de acesso de entrada e de saída, sem necessitar que os dois dispositivos acessem o gerente de forma independente.

Existe ainda, uma conexão do pino Tx (transmissor) de uma placa ao pino Rx (receptor) da outra e, vice-versa. Esta conexão possibilita a transferência de dados entre ambas. A comunicação entre elas ocorre por meio de um protocolo de comunicação e utiliza a porta serial para a transferência de dados.

Cada placa atua de forma autônoma, controlando seus próprios sensores e atuadores. Entretanto, existe a necessidade de uma comunicação entre ambas. A placa auxiliar, além de realizar a entrada de dados, atua como um dispositivo de saída, exibindo mensagens em um visor LCD. Estas mensagens são obtidas e sincronizadas por meio da comunicação com a placa principal, utilizando a porta serial para realizar esta operação. Desta forma, existe uma interface de interação entre o usuário e o sistema que exibe informações sobre o processo de autenticação de um usuário, indisponibilidade de acesso a um local, possíveis falhas de comunicação com o gerente e atualizações referentes à data e horário. Todas estas informações são atualizadas por meio da comunicação entre gerente e placa principal. Portanto, novamente evidencia-se a importância de não necessitar uma conexão do gerente com cada placa.

F. Protocolo de comunicação da Arquitetura ESC

A Arquitetura ESC além de realizar a comunicação entre gerente e ESCHA por meio de redes TCP/IP, realiza uma a comunicação serial entre as placas principal e auxiliar, e a comunicação entre ESCHA e ESCMA. A Fig. 3 demostra um cenário para aplicação da desta arquitetura e a forma como cada comunicação é realizada.

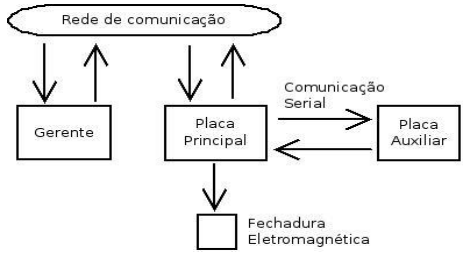

Fig. 3. Cenário de aplicação da Arquitetura ESC

Para estabelecer a transferência de dados entre as placas, por meio da comunicação serial, é necessário um protocolo de comunicação entre elas que diferencie os eventos e as informações que devem ser enviadas. Desta forma, mensagens que serão exibidas são atualizadas instantaneamente.

Cada placa é programada para realizar a operação correspondente ao tipo de dado que está sendo transferido, ou seja, é previsto no código o momento que a placa deve realizar o envio de determinado dado ou a forma que proceder quando receber. Para isso utiliza-se um código para

identificar a ocorrência de determinado evento. Além do código, são enviados os seguintes dados:

- Mensagem: contém a informação a ser exibida no visor LCD. São totalmente flexíveis de acordo com os diferentes eventos que podem ocorrer, por exemplo: autenticação do usuário, travamento de um dispositivo, possível falta de comunicação com o gerente, abertura de uma porta de forma assíncrona, exibição de uma mensagem padrão do sistema;
- Data e hora: mantém a interface de interação com usuário atualizada. Estes dados são enviados pelo gerente na inicialização do sistema e atualizados pela placa principal.

III. RESULTADOS E CONCLUSÕES

Para verificar o funcionamento da arquitetura ESC e analisar o seu desempenho, foram cadastrados alguns usuários na base de dados com diferentes tipos de permissões de acesso. Além disso, foi construído um protótipo com as duas placas que compõem o ESCHA, integrado ao ESCMA e um cenário de testes, simulando o ambiente real de aplicação para esta arquitetura. O cenário construído ilustra o controle de acesso a um local, utilizando uma placa externa (auxiliar) ao ambiente e uma em seu interior (placa principal), conforme pode ser visualizado na Fig. 3. Para realizar a abertura da porta foi utilizada uma relé, responsável pelo acionamento de uma fechadura eletromagnética.

Os primeiros testes realizados serviram para verificar o comportamento do hardware construído e ajustar os códigos desenvolvidos para cada placa. A comunicação entre as placas através da porta serial também foi submetida a vários testes. Durante estas análises, obteve-se um resultado satisfatório, o que permitiu a simulação envolvendo a comunicação via rede com o gerente.

Utilizando o cenário citado anteriormente, foram realizados diversos experimentos para o controle de acesso a um dispositivo (porta). Os testes foram realizados utilizando uma rede local para conectar o ESCHA ao gerente. Um cabo UTP e conectores RJ 45 foram utilizados para conectar a porta serial de uma placa a outra. Uma adaptação na placa, onde os pinos da porta serial foram disponibilizados em um conector RJ 45 femea, permitiu esta forma de conexão.

Os testes foram realizados em três sessões com duração de uma hora cada. Durante cada sessão foram realizadas quarenta tentativas de autenticação de usuário. Os resultados demonstraram que o intervalo de tempo entre processo de autenticação e a resposta do gerente é de aproximadamente 2,2 segundos. Esse tempo é uma média de todas as tentativas realizadas e é independente de qual placa realiza a leitura do cartão, o que confirma que a comunicação serial não causa nenhuma perda de dados ou atraso ao sistema. Testes de estresse foram realizados, mantendo a Arquitetura ESC em funcionamento por diversas horas. Nesses testes, foram realizadas tentativas em tempos aleatórios e verificou-se que 90% das tentativas de autenticação obtiveram uma resposta do gerente. As tentativas sem respostas representam o tempo que o gerente pode estar em modo espera (após determinado tempo sem receber uma operação de autenticação) e possível falha de leitura em algum cartão.

Além disso, a exibição de mensagens no visor LCD ocorreu de forma síncrona e flexível, possibilitando que as informações fossem atualizadas conforme a necessidade de cada evento, podendo ainda ser atualizadas pelo envio de mensagens pela a interface *web* do sistema.

IV. MELHORIAS E PROJETOS FUTUROS

Conforme as constantes mudanças que ocorrem em relação à tecnologia, esta arquitetura precisa ser atualizada ao decorrer do tempo para poder estar de acordos com novos recursos e/ou dispositivos disponíveis.

Visando fazer um melhor aproveitamento dos recursos oferecidos pela comunicação serial e a via rede, trabalha-se com ideia de utilizar tais comunicações para realizar a atualização do software de cada placa por meio do envio dos códigos para todos os dispositivos que integram o sistema.

Além disso, está sendo analisada a ideia de transformar o gerente em um servidor web, que acesse cada dispositivo (cliente) somente quando for solicitado (usuário esta interagindo com o sistema).

REFERÊNCIAS

[1] VERMESAN, Ovidiu; FRIESS, Peter. Internet of Things: Global Technological and Societal Trends. Ed. Aalborg River Publishers, 2011.

[2] ATZORI, Luiz; IERA, Antonio; MORABITO, Giacomo. The Internet of Things: A survey. Computer Networks - Volume 54, Issue 15, 28 October 2010.

[3] SMITH, Ian G. The Internet of Things. New Horizons. 2012

[4] MCROBERTS, Michael. Arduino básico; [tradução Rafael Zanolli]. -- São Paulo: Novatec Editora, 2011.

[5] ARDUINO. Arduino Uno (Online). Disponível na internet. URL: http://www.arduino.cc/en/Main/ArduinoBoardUno, 2013.

[6] SANTOS, A. Gerenciamento de Identidades. Rio de Janeiro, Brasports, 2007.

[7] RAGUZZONI, Jeann C. M.; HEINSCH, Lamarck Ribas; RIZZETTI, Tiago Antonio. Uma arquitetura para desenvolvimento de dispositivos de autenticação e acesso a espaços físicos. 2012.

[8] HEINSCH, Lamarck Ribas; RAGUZZONI, Jeann C. M.; RIZZETTI, Tiago Antonio; PASIN, Marcia. Introduzindo uma arquitetura de Gerenciamento de Segurança física de ambientes baseada em ferramentas livres.