

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DAINF — DEPARTAMENTO ACADÊMICO DE INFORMÁTICA
CURSO DE GRADUAÇÃO EM ENGENHARIA DE COMPUTAÇÃO

GUSTAVO LUIZ ANDRADE CORRÊA

**SISTEMA OPEN-SOURCE PARA A ATUALIZAÇÃO DE
FIRMWARE OVER-THE-AIR PARA DISPOSITIVOS DE IOT
BASEADO NAS BIBLIOTECAS LWIP, MBED TLS E FATFS**

TRABALHO DE CONCLUSÃO DE CURSO

PATO BRANCO
2021

GUSTAVO LUIZ ANDRADE CORRÊA

**SISTEMA OPEN-SOURCE PARA A ATUALIZAÇÃO DE
FIRMWARE OVER-THE-AIR PARA DISPOSITIVOS DE IOT
BASEADO NAS BIBLIOTECAS LWIP, MBED TLS E FATFS**

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia de Computação da Universidade Tecnológica Federal do Paraná, como requisito parcial para a obtenção do título de engenheiro de computação.

Orientador: Prof. Dr. Gustavo Weber Denardin
Departamento Acadêmico De Elétrica

PATO BRANCO
2021

Altere este texto inserindo a dedicatória do seu trabalho.

AGRADECIMENTOS

Edite e coloque aqui os agradecimentos às pessoas e/ou instituições que contribuíram para a realização do trabalho.

É obrigatório o agradecimento às instituições de fomento à pesquisa que financiaram total ou parcialmente o trabalho, inclusive no que diz respeito à concessão de bolsas.

Technology is just nature we taught to do cool tricks. (EXURB1A, 2019)

RESUMO

CORRÊA, Gustavo L. Andrade. Sistema *open-source* para a atualização de *firmware Over-The-Air* para dispositivos de IoT baseado nas bibliotecas LwIP, Mbed TLS e FatFs. 2021. [49](#) f. Trabalho de Conclusão de Curso – DAINF — Departamento Acadêmico de Informática , Universidade Tecnológica Federal do Paraná. Pato Branco, 2021.

Com a ampla utilização de internet das coisas, conceito em que dispositivos embarcados estão conectados a internet, surge a necessidade da atualização automática do firmware desses dispositivos para correções ou aperfeiçoamentos. Atualmente existem uma grande variedade de implementações dessa funcionalidade, mas a falta de um padrão dificulta a sua ampla utilização. Assim, esse trabalho propõe uma solução *open-source* de atualização de *firmware Over-The-Air* para dispositivos IoT, utilizando as bibliotecas amplamente difundidas LwIP, FatFs e Mbed TLS. O sistema proposto pretende disponibilizar uma API que pode ser integrada a qualquer plataforma embarcada e um *bootloader* que fazem todo o processo de obtenção e atualização de *firmware*.

Palavras-chave: Atualização. Firmware. Over-The-Air. Portável. IoT.

ABSTRACT

CORRÊA, Gustavo L. Andrade. Open-Source system for firmware OTA (Over-The-Air) update based on the libraries LwIP, Mbed TLS and FatFS. 2021. 49 f. Trabalho de Conclusão de Curso – Curso de Graduação em Engenharia de Computação, Universidade Tecnológica Federal do Paraná. Pato Branco, 2021.

Elemento obrigatório em tese, dissertação, monografia e TCC. É a versão do resumo em português para o idioma de divulgação internacional. Deve ser antecedido pela referência do estudo. Deve aparecer em folha distinta do resumo em língua portuguesa e seguido das palavras representativas do conteúdo do estudo, isto é, das palavras-chave. Sugere-se a elaboração do resumo (Abstract) e das palavras-chave (Keywords) em inglês; para resumos em outras línguas, que não o inglês, consultar o departamento / curso de origem.

Keywords: Word. Second Word. Another word.

LISTA DE FIGURAS

Figura 1 – Processo de inicialização de um sistema embarcado. Fonte: adaptado de (QING, 2003)	5
Figura 2 – Criando um arquivo de imagem para um sistema. Fonte: adaptado de (QING, 2003)	8
Figura 3 – Mapeando uma imagem executável em um sistema alvo. Fonte: adaptado de (QING, 2003)	9
Figura 4 – Alocação do bootloader e firmware nas memórias FLASH e RAM. Fonte: Adaptado de (DAVIS; DURLIN, 2013)	10
Figura 5 – Fluxograma de operações de um bootloader.	11
Figura 6 – Pilha TCP/IP e seus protocolos. Fonte: adaptado de (TANENBAUM, 2003)	12
Figura 7 – Pilha de comunicação. Fonte: adaptado de (DEVINE, 2006)	15
Figura 8 – Alocação encadeada usando tabela de alocação de arquivo. Fonte:(TANENBAUM, 2007)	18
Figura 9 – Posição da biblioteca FatFs na aplicação. Fonte:(CHAN, 2016)	19
Figura 10 – Posição da biblioteca FatFs na aplicação. Fonte:(CHAN, 2016)	21
Figura 11 – Visão geral do funcionamento do sistema de atualização. Fonte: autoria própria.	24
Figura 12 – Diagrama de funcionamento do <i>bootloader</i> . Fonte: autoria própria.	26
Figura 13 – Diagrama de funcionamento da API. Fonte: autoria própria.	28
Figura 14 – Kit de desenvolvimento STM32F746G-Discovery. Fonte:(STMICROELECTRONICS, 2019).	29
Figura 15 – As três mensagens exibidas para diferenciação dos <i>firmware</i> . Fonte: Autoria própria.	30
Figura 16 – As três mensagens exibidas para diferenciação dos <i>firmware</i> . Fonte: Autoria própria.	35
Figura 17 – As três mensagens exibidas para diferenciação dos <i>firmware</i> . Fonte: Autoria própria.	36
Figura 18 – Processo de atualização OTA. Fonte: Autoria própria.	37

Figura 19 – As três mensagens exibidas para diferenciação dos *firmware*.

Fonte: Autoria própria. 38

LISTA DE TABELAS

Tabela 1 – Organização do bloco de memória FLASH do microcontrolador STM32F746NGH6. Adaptado de:(STMICROELECTRONICS, 2019).	31
--	----

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
DECOM	Departamento de Computação

LISTA DE ALGORITMOS

SUMÁRIO

1 – INTRODUÇÃO	1
1.1 OBJETIVO GERAL	3
1.2 OBJETIVOS ESPECÍFICOS	3
2 – REVISÃO DA LITERATURA	4
2.1 PROCESSO DE INICIALIZAÇÃO DO SISTEMA	4
2.1.1 LINKER	6
2.1.2 BOOTLOADER	9
2.2 COMUNICAÇÃO CLIENTE-SERVIDOR	12
2.2.1 LWIP	13
2.2.1.1 Hypertext Transfer Protocol (HTTP)	14
2.2.1.2 Transmission Control Protocol (TCP)	14
2.2.2 MBED TLS	15
2.2.2.1 Transport Layer Security (TLS)	16
2.2.2.2 Função Hash	16
2.3 SISTEMAS DE ARQUIVO	17
2.3.1 SISTEMA DE ARQUIVO FAT	18
2.3.2 FATFS	19
2.4 HARDWARE ABSTRACTION LAYER (HAL)	20
2.4.1 STM32CUBE HAL	20
2.5 TRABALHOS CORRELATOS	21
3 – SISTEMA DE ATUALIZAÇÃO DE FIRMWARE OVER-THE-AIR	23
3.1 VISÃO GERAL	23
3.2 <i>BOOTLOADER</i>	24
3.3 API DE ATUALIZAÇÃO OTA	26
3.3.1 COMUNICAÇÃO COM O SERVIDOR	27
3.3.2 DOWNLOAD E ARMAZENAMENTO DO FIRMWARE	27
3.4 MATERIAIS UTILIZADOS	28
3.4.1 PLATAFORMA STM32F746G-DISCOVERY	29
3.4.2 FIRMWARES DE TESTE PROPOSTOS	30
4 – UTILIZANDO O SISTEMA	31
4.1 PORTANDO O BOOTLOADER	31
4.2 CONFIGURAÇÃO DA API OTA	32
5 – RESULTADOS	35

5.1	PROCESSO DE ATUALIZAÇÃO DE FIRMWARE	35
5.1.1	ESTADO INICIAL DO MICROCONTROLADOR	35
5.1.2	INICIALIZAÇÃO DO BOOTLOADER	36
5.1.3	INICIALIZAÇÃO DO FIRMWARE 1	36
5.1.4	OTA	36
5.1.5	REINICIALIZAÇÃO DO SISTEMA PARA O BOOTLOADER	37
5.1.6	INICIALIZAÇÃO DO FIRMWARE 2	38
5.2	DISCUSSÃO	38
6	CONCLUSÃO	40
6.1	TRABALHOS FUTUROS	40
	Referências	42
	 Apêndices	 44
	APÊNDICE A –Nome do apêndice	45
	APÊNDICE B –Nome do outro apêndice	46
	 Anexos	 47
	ANEXO A –Nome do anexo	48
	ANEXO B –Nome do outro anexo	49

1 INTRODUÇÃO

Com a evolução da microeletrônica e, por consequência, a redução de custo de periféricos e o crescimento do poder computacional de processadores, os sistemas computacionais se tornaram menores e baratos. Devido a isso, processadores e microcontroladores passaram a ser instalados em produtos, o que deu origem ao conceito de sistema embarcado, que são sistemas de processamento de informação embutidos em produtos (MARWEDEL, 2006). A utilização desses sistemas foi disseminada em várias áreas como, a automobilística, aeronáutica, ferroviária, industrial, médica, entre outras, automatizando as mais diversas funções.

Os sistemas computacionais embarcados são compostos pelos mesmos componentes utilizados para a constituição de computadores pessoais, porém com tamanhos, capacidades e custos reduzidos. Tais dispositivos operam de forma independente e geralmente são projetados para realizar tarefas específicas e repetitivas. Sistemas embarcados estão presentes no dia a dia da maioria das pessoas, em micro-ondas, geladeiras, TVs, aparelhos de som, video games e outros produtos eletrônicos (MARWEDEL, 2006), logo, esses dispositivos se distanciam dos computadores de propósito geral, como observamos em *desktops* e *notebooks* atuais.

Com a necessidade cada vez maior da implementação desses sistemas no nosso dia a dia, é imprescindível se obter *hardwares* e *softwares*, cada vez mais robustos e que atendam todas as necessidades dos seus usuários. Assim, o projeto desses produtos devem ser muito bem planejado, e executado de forma a serem entregues produtos de qualidade, à prova de falhas e que possam reagir a erros, de forma a não causar danos a seus utilizadores.

Durante a fase de projeto de um sistema embarcado, deve-se avaliar diversos âmbitos, como desempenho, confiabilidade, consumo de energia, manufaturabilidade, etc. É também necessário validar essas avaliações, com o intuito de verificar se atenderão os requisitos de projeto. Pela necessidade desses produtos serem eficientes, é indispensável que esses sistemas passem por uma fase de otimização, em que mudanças no projeto podem melhorar a eficiência energética do produto ou até mesmo gerar novas funcionalidades a esses equipamentos. Portanto, o projeto todo precisa ser testado para evitar que erros e *bugs* possam vir a permanecer no produto final (MARWEDEL, 2006), criando um ciclo de desenvolvimento que deve ser repetido até se obter um produto eficiente, de qualidade e completo.

Após a venda e instalação de um sistema embarcado para seu cliente, eventualmente pode ser necessária uma nova funcionalidade, uma otimização ou então, podem ser exigidos testes nesse sistema. Logo, é preciso que haja uma forma de se alterar esse produto mesmo após seu lançamento, para assim darmos um maior valor ao produto e confiabilidade ao sistema. A possibilidade de serem feitas manutenções futuras no *software*, que no contexto de sistemas embarcados é chamado de *firmware* (*firmware* é uma classe específica de *software* de computador que fornece controle de baixo nível para o *hardware* específico do dispositivo), é conhecida como atualização OTA (*Over-The-Air*). Esse recurso não é obrigatório no projeto

de um sistema embarcado, mas é muitas vezes necessário, podendo ser uma funcionalidade muito útil dependendo da aplicação do sistema em concepção. A decisão de utilizar ou não a atualização OTA pode influenciar na escolha do *hardware* utilizado no projeto (BALL, 2002), podendo aumentar o custo do produto final. Uma das principais soluções adotadas para a manutenção desses programas é criar métodos de atualização em que, é necessário a presença de um agente humano fisicamente próximo do sistema para fazer a manutenção do *software*, o que acaba aumentando o custo de manutenção do produto e o tornando menos atrativo para os seus compradores.

Os *bootloaders* estão atualmente presentes em todos os computadores pessoais e em alguns sistemas embarcados. Esse *software* prepara a maioria dos *hardwares* presentes na máquina para um sistema operacional ou outro programa é executado. Como é o primeiro programa a ser inicializado após um sistema ser iniciado ou após um *reset*, ele pode ter várias funções, como, realizar checagem de periféricos, verificar se o *firmware* presente na memória não está corrompido, além de poder fazer a troca do *software* presente na memória (DAVIS; DURLIN, 2013), que será sua principal utilização nesse trabalho.

Um dos seus principais usos é em *smartphones*, em que são utilizados para a atualização de sistemas operacionais como *Android* e *iOS*, e como garantia de restauração em caso de erros irreversíveis no sistema operacional. É desenvolvido pelo próprio fabricante do dispositivo, e por padrão é bloqueado para os usuários, evitando a substituição do *software* original do aparelho por uma versão customizada, mas ainda assim existem opções de desbloqueio do *bootloader*, dependendo do modelo do aparelho e do fabricante (SALUTES, 2018).

Internet of things ou IoT é o conceito que se refere à interconexão digital de objetos cotidianos com a internet. A internet das coisas em outras palavras pode ser descrita como uma rede de dispositivos embarcados, como sensores, câmeras, carros e demais objetos do cotidiano, capazes de obter e transmitir dados pela internet. A empresa de consultoria Gartner (GARTNER, INC., 2019) diz que, até 2020, são esperados mais de 20 bilhões de "coisas" conectadas a internet. Essas "coisas" não são dispositivos de uso geral como *smartphones* e PCs, mas objetos de função única.

Esse trabalho de conclusão de curso propõe um método de manutenção desses *firmwares* de forma remota, que possa ser o mais portátil possível. Na solução proposta, o dispositivo embarcado poderá verificar periodicamente um servidor a procura de uma nova versão do seu *firmware*. Quando encontrado, será realizado o *download* do novo *firmware* para a memória interna do dispositivo, para posterior atualização do equipamento. O diferencial da abordagem proposta é basear a solução em bibliotecas amplamente difundidas em sistemas embarcados, como a LwIP (DUNKELS, 2002), Mbed TLS (DEVINE, 2006) e a FatFS (CHAN, 2016). Dessa forma, o código do sistema de atualização é totalmente portátil, desde que a plataforma escolhida tenha suporte a tais bibliotecas. A única peça de *software* que não será totalmente portátil será o *bootloader* que substituirá o *firmware* antigo pelo novo na memória flash do dispositivo, por ser dependente do *hardware* utilizado.

1.1 OBJETIVO GERAL

Esse trabalho tem como objetivo geral o desenvolvimento de um sistema *open-source* para a atualização de *firmwares Over The Air* para dispositivos IoT baseado nas bibliotecas FatFs, LwIP e Mbed TLS.

1.2 OBJETIVOS ESPECÍFICOS

- Desenvolver o *bootloader* que utiliza o sistema de arquivo FAT.
- Implementar uma API que fará a comunicação segura entre o servidor e a plataforma embarcada, verificará a disponibilidade de atualização e fará o *download* da nova versão, se existente. Armazenará o *firmware* recebido em um cartão SD (Secure Digital).
- Comprovar o funcionamento da técnica de atualização remota de *firmware*, utilizando a plataforma embarcada STM32F746G-DISCOVERY.

2 REVISÃO DA LITERATURA

Neste capítulo será feita uma revisão da literatura necessária para o entendimento deste trabalho de conclusão de curso. Serão abordados os temas como: o processo de inicialização de um sistema embarcado, o que é um *bootloader* e o papel do *linker* na criação de um arquivo executável e no mapeamento da memória da aplicação. Também será discutido sobre a comunicação cliente-servidor, a pilha TCP/IP, a biblioteca LwIP e alguns protocolos implementados por ela, assim como a biblioteca Mbed TLS, alguns protocolos e algoritmos de segurança implementados por ela. Será mostrado o que é um sistema de arquivo, o sistema de arquivos FAT e a biblioteca FatFs. Com o conhecimento obtido sobre todos esses temas o leitor será capaz de compreender como será desenvolvido o método de atualização de *firmware* OTA.

2.1 PROCESSO DE INICIALIZAÇÃO DO SISTEMA

Segundo Qing (2003), um processador embarcado, após ser ligado, busca e executa o programa de um endereço pré-definido e gravado permanentemente na memória. A instrução contida nessa localização da memória é geralmente chamada de vetor de reset. O vetor de reset contém diversos ponteiros que apontam para diferentes regiões de memória e dependendo da posição desse ponteiro ele pode apontar para rotinas de inicialização, tratamento de interrupção entre outras rotinas. O ponteiro contido na região de inicialização do vetor de reset geralmente aponta para uma instrução de salto para outro espaço da memória em que a real rotina de inicialização se encontra. A razão deste salto para outra localidade da memória é para manter o vetor de reset pequeno. O vetor de reset pertence a uma pequena área da memória reservada pelo sistema por motivos especiais. O vetor de reset, assim como o código de inicialização do sistema, precisa estar armazenado permanentemente. Por causa deste problema, a rotina de inicialização, chamado de programa *bootstrap*, reside na memória somente de leitura (ROM), na flash ou em outra memória não volátil. O termo *loader* se refere ao subprograma que é responsável por executar o *bootstrap*, fazer o possível *download* de um binário do firmware executável, também conhecido como imagem, de outro local e inicialização da aplicação final.

O conceito é melhor explicado por meio do exemplo criado por Qing (2003). Neste exemplo, assumimos que o *loader* foi desenvolvido e programado na memória flash. Além disso, será assumido que a imagem alvo contém várias seções de programa. Cada seção tem um lugar designado no mapa de memória. O *reset vector* está contido em uma pequena ROM, que está mapeada na localização 0x0h do espaço de endereços. A ROM contém alguns valores iniciais essenciais requeridos pelo processador quando o sistema é reinicializado (*reset*). Esses valores são o *reset vector*, o *stack pointer* (ponteiro de pilha) inicial e o endereço da memória de acesso randômico (RAM).

No exemplo ilustrado na [Figura 1](#), o *reset vector* é uma instrução de salto para o endereço de memória 0x00040h; o *reset vector* transfere o controle do programa para a instrução neste endereço. O código de inicialização do sistema contém, entre outras coisas o programa *loader* da imagem destino e o vetor de exceção padrão do sistema (*exception vector*). O vetor de exceção do sistema aponta para uma instrução que reside na memória flash.

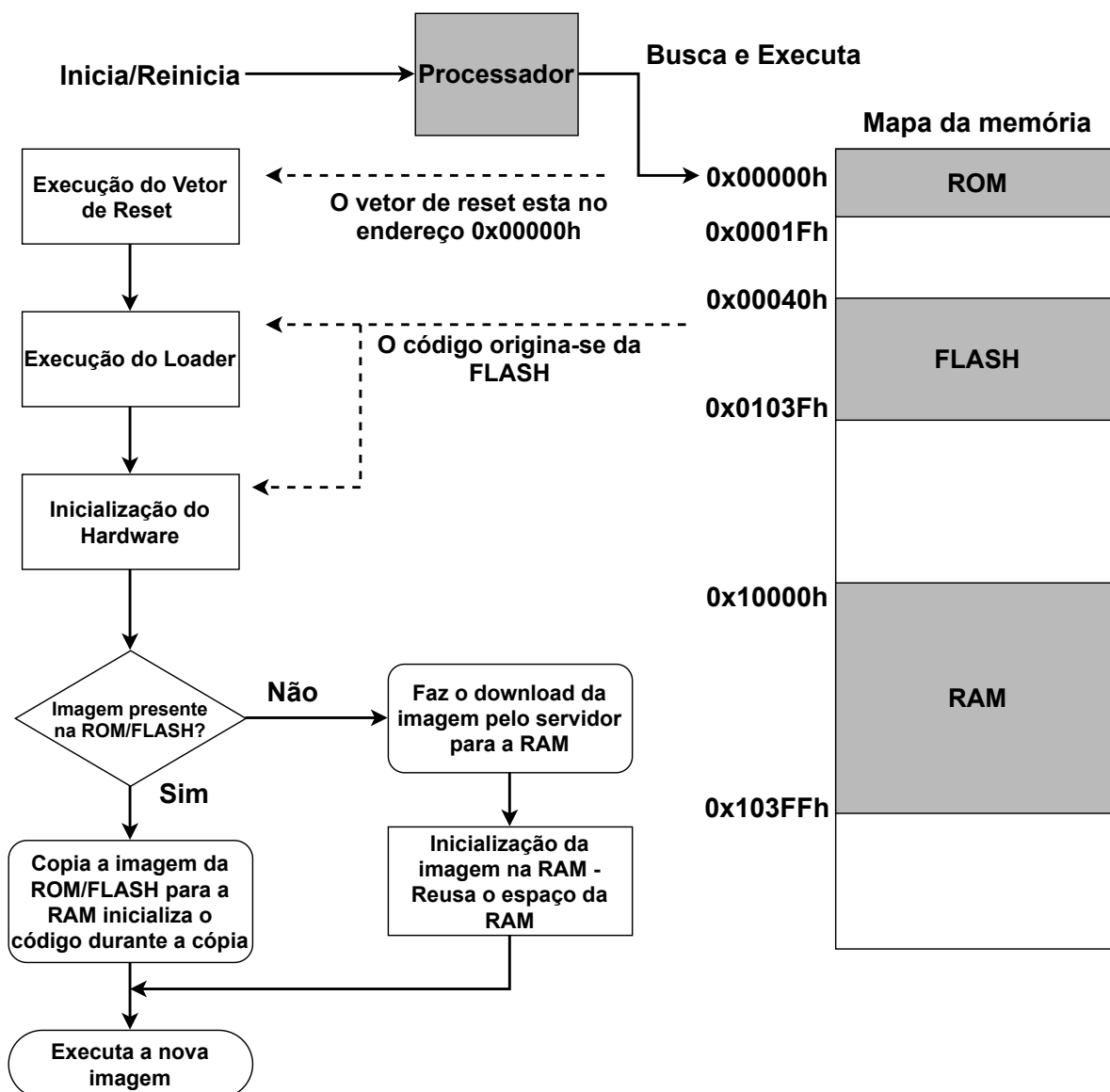


Figura 1 – Processo de inicialização de um sistema embarcado.

Fonte: adaptado de ([QING, 2003](#))

A primeira parte do processo de *bootstrap* do sistema é colocar o sistema em um estado conhecido. São posicionados valores padrões apropriados nos registradores do processador. São colocados no *stack pointer* os valores encontrados na ROM. O *loader* desabilita as interrupções do sistema, pois o sistema ainda não está preparado para lidar com interrupções. O *loader* também inicializa a memória RAM e possivelmente a *cache* (memória transitória)

do processador. Neste ponto, o *loader* executa um diagnóstico de *hardware* limitado nos dispositivos necessários para essas operações.

A execução do programa é mais rápida na RAM quando comparada ao mesmo código executado diretamente na memória flash. O *loader* pode opcionalmente copiar o código da memória flash para a RAM. Por causa dessa capacidade, uma seção de programa pode tanto ter um endereço de carregamento, quanto um endereço de execução. O endereço de carregamento é onde a seção do programa reside, enquanto o endereço de execução é o endereço em que o *loader* copia a seção do programa e a prepara para a execução (QING, 2003).

Uma imagem executável possui seções de dados inicializados e não inicializados. Essas seções são ambas legíveis e graváveis. Essas seções precisam residir na RAM, assim sendo são copiadas da memória flash para a RAM como parte do sistema de inicialização. A seção de dados inicializados (chamadas pelo *linker* de `.data` e `.sdata`) contém os valores iniciais para as variáveis globais e estáticas. O conteúdo dessa seção, portanto, faz parte da imagem executável final e é transferido completamente pelo *loader*. Por outro lado, o conteúdo da seção de dados não inicializado (chamado pelo *linker* de `.bss` e `.sbss`) é vazio. O *linker* reserva espaço para essa seção no mapa de memória. As informações de alocação dessas seções, como o tamanho da seção e o endereço de execução da seção, são parte do cabeçalho da seção. É trabalho do *loader* obter essas informações dos cabeçalhos de seção e alocar a mesma quantidade de memória na RAM durante o processo de carregamento. O *loader* coloca essas seções na RAM de acordo com o endereço de execução das seções.

Uma imagem executável provavelmente possui constantes. Os dados das constantes são parte da seção chamada pelo *linker* de `.const`, que é somente leitura. Sendo assim, é possível manter a seção `.const` na memória somente de leitura durante a execução do programa. Constantes de acesso frequente, como tabelas de *lookup*, necessitam ser transferidas para a RAM para melhorar o desempenho do sistema.

O próximo passo no processo de inicialização do sistema é o *loader* inicializar os dispositivos do sistema. Apenas os dispositivos necessários são inicializados nessa etapa. Em outras palavras, um dispositivo é inicializado na medida em que um subconjunto necessário dos recursos e recursos do dispositivo estejam ativados e operacionais. Geralmente, os dispositivos são parte da interface de entrada e saída do sistema, portanto, esses dispositivos são completamente iniciados quando existe a necessidade de se fazer *download* de uma imagem de outro local.

Agora o *loader* está pronto para transferir a imagem da aplicação para o sistema alvo. A imagem da aplicação pode conter um RTOS, um *kernel*, e os demais códigos das aplicações que o desenvolvedor necessita.

2.1.1 LINKER

Segundo Qing (2003), os arquivos de uma aplicação são processados pelo compilador e *assembler*. Criando assim os arquivos objetos, que contém os códigos de máquina binários

(*machine binary code*) e dados de programa (*program data*). O utilitário de arquivo é um programa que concatena uma coleção de arquivos objetos para formar uma biblioteca. Então o *linker* obtém esses arquivos objetos como entrada e produz ou um arquivo executável, ou um arquivo objeto que pode ser utilizado em outro *linker* com outros arquivos objetos. O arquivo de comandos de *linker* (*linker command file*) orienta o *linker* em como combinar esses diferentes arquivos objetos e em que local da memória colocar o código binário e os dados no sistema embarcado alvo. Em conclusão, a função principal de um *linker* é combinar múltiplos arquivos objetos em um arquivo objeto maior, um arquivo objeto compartilhado ou uma imagem executável final. Esse processo pode ser observado na [Figura 2](#).

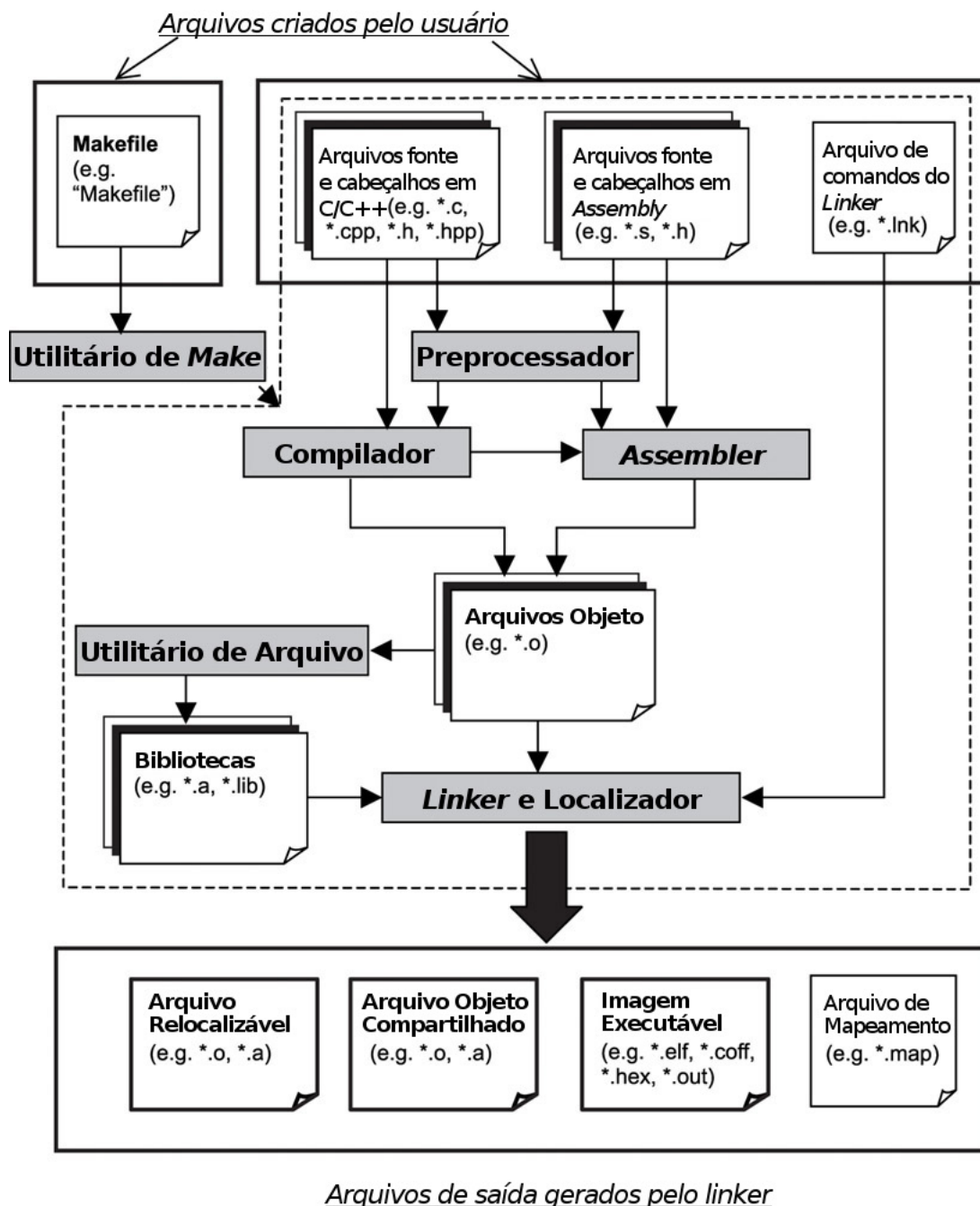


Figura 2 – Criando um arquivo de imagem para um sistema.

Fonte: adaptado de (QING, 2003)

O *linker* precisa combinar esses arquivos objetos e fundir as seções de diferentes arquivos em um segmento de programa. Esse processo cria uma única imagem executável para o sistema embarcado alvo. O desenvolvedor utiliza comandos de *linker* (chamados de *linker directives*) para controlar como o *linker* combina essas seções e aloca seus segmentos no sistema alvo. As diretivas de *linker* ficam contidas no arquivo de comando de *linker*. O objetivo de criar esse arquivo de comando de *linker* é para que o desenvolvedor de sistemas embarcados possa mapear a imagem executável para o *hardware* alvo de forma precisa e eficiente.

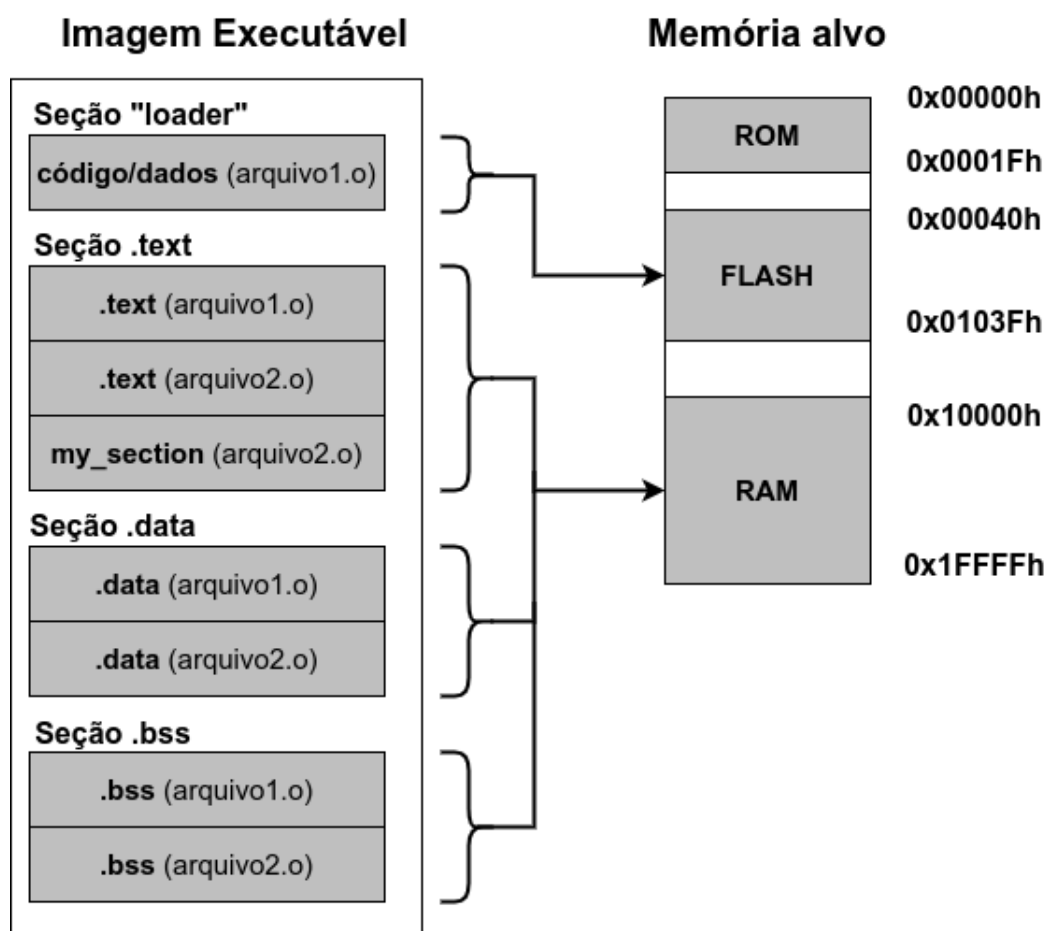


Figura 3 – Mapeando uma imagem executável em um sistema alvo.

Fonte: adaptado de (QING, 2003)

2.1.2 BOOTLOADER

O *bootloader* é um *software* que tem como responsabilidade a atualização do *firmware* do sistema, operação também conhecida como *in-application programming* (IAP). Reside em uma área protegida da memória, geralmente colocado no início da flash ou na ROM, e é o primeiro *software* a ser executado após o *reset* ou iniciação do sistema. É desenvolvido para receber comandos via periféricos de comunicação como: UART, I2C, SPI, CAN e Ethernet, e entender o mapa de memória do microcontrolador (DAVIS; DURLIN, 2013). A Figura 4 mostra como geralmente fica alocado um *bootloader* e o *firmware* na memória.

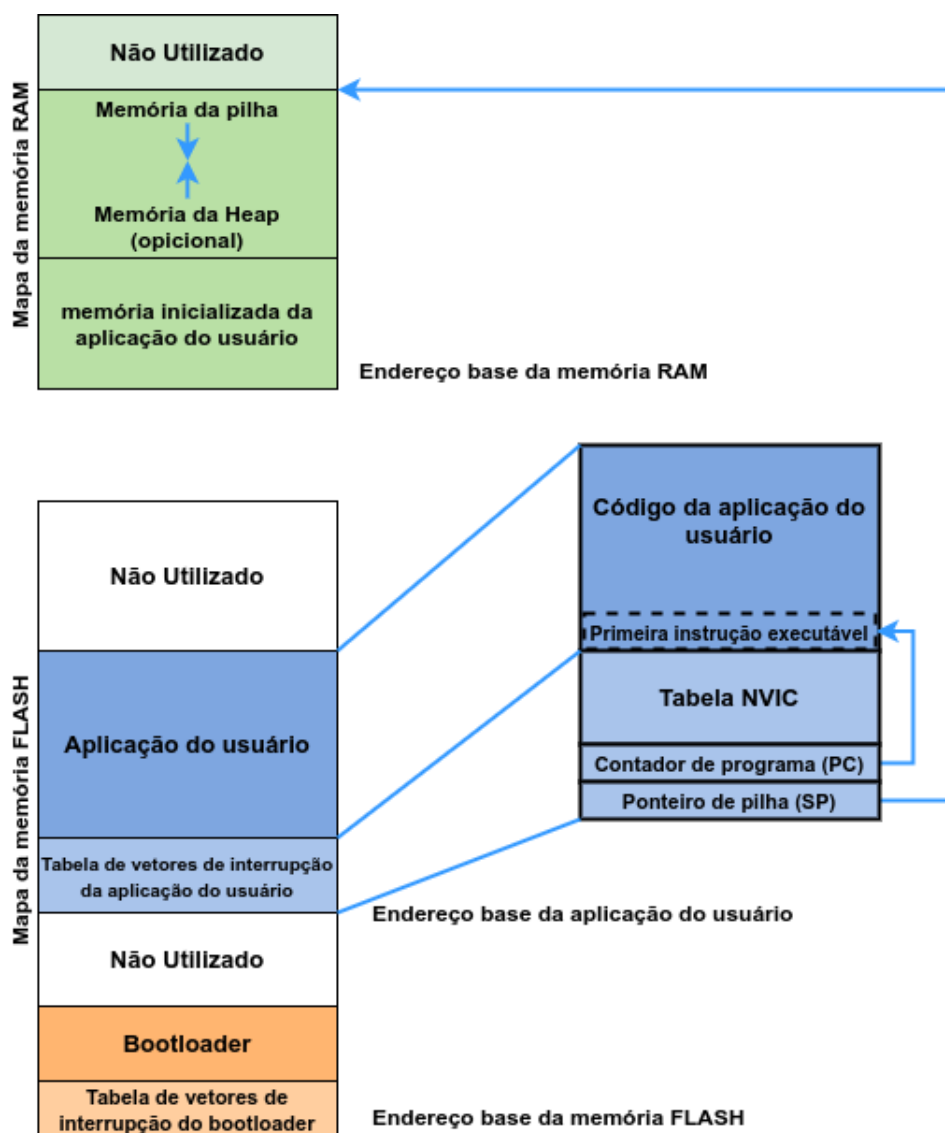


Figura 4 – Alocação do bootloader e firmware nas memórias FLASH e RAM.

Fonte: Adaptado de (DAVIS; DURLIN, 2013)

A função do *bootloader* se resume geralmente a: comunicar-se com outro servidor, ler os arquivos enviados pelo *host*, atualizar o *firmware* de seu microcontrolador, e iniciar esse novo programa. Pode conter instruções e comandos definidos pelo projetista para somente o circuito integrado em uso, impossibilitando a utilização do mesmo código em outras plataformas. Portanto, é uma programa que não é portátil para vários modelos de sistemas embarcados. A Figura 5 mostra o funcionamento de um bootloader padrão.

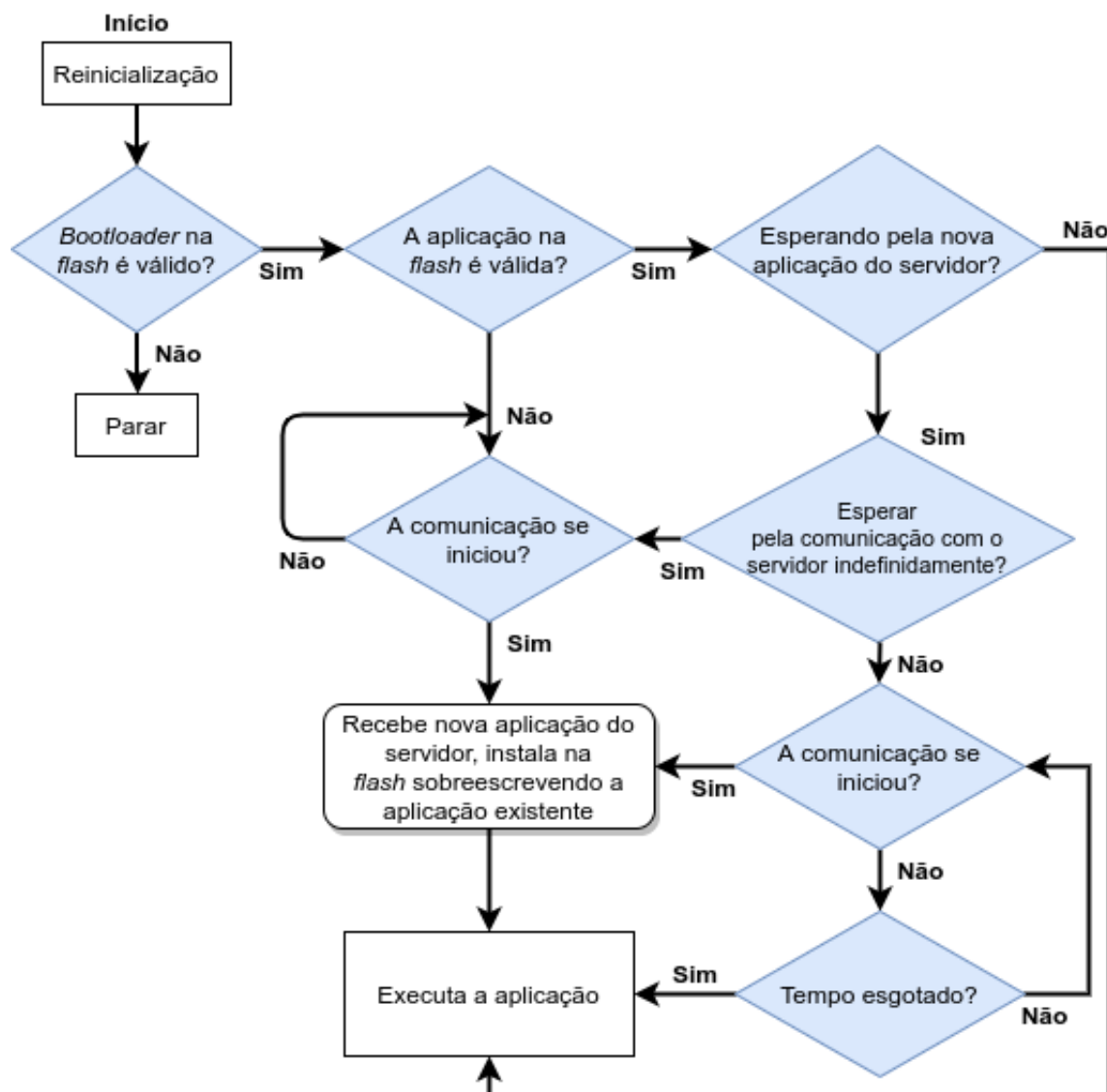


Figura 5 – Fluxograma de operações de um bootloader.

Os microcontroladores da família STM32 desenvolvidos pela empresa ST [STMicroelectronics](#) (2019) possuem um *bootloader* pré programado na ROM desde sua fabricação. Esse *bootloader* pode utilizar diversos periféricos de comunicação, e para cada periférico diferente a ST padronizou diferentes protocolos que permitem várias operações, como: obter o ID do chip, escrever e ler bytes na RAM e memória flash, apagar setores das memórias, ativar áreas de proteção na memória e pular para o código principal do sistema ([NOVIELLO, 2018](#)).

Um *bootloader* customizado pode conter diversas funções adicionais, uma função frequentemente usada é o uso do *bootloader* para descriptografar firmwares que podem chegar via internet, para se garantir a segurança e origem do *firmware*.

2.2 COMUNICAÇÃO CLIENTE-SERVIDOR

Um programa cliente é um programa que funciona em um sistema computacional, que solicita e recebe um serviço de um programa servidor, que funciona em outro sistema final. Uma vez que o programa cliente é executado em um computador e o programa servidor, é executado em outro, aplicações cliente-servidor são, por definição, aplicações distribuídas. Os programas cliente e o servidor interagem enviando mensagens um para o outro, pela internet ou qualquer outra rede local ou remota. Neste nível de abstração, os roteadores, enlaces e outros componentes da internet funcionam como uma caixa-preta que transferem mensagens entre os componentes distribuídos, comunicantes, de uma aplicação (KUROSE; ROSS, 2010).

A comunicação cliente-servidor na internet é feita por meio de diversos protocolos de rede, cujo conjunto de protocolos é conhecido como pilha TCP/IP (*Transmission Control Protocol/Internet Protocol*). Essa pilha é dividida em quatro camadas, em que cada camada é encarregada de realizar uma série de funções, concedendo um grupo de serviços bem definidos para o protocolo da camada superior. A Figura 6 ilustra a pilha TPC/IP e seus protocolos.

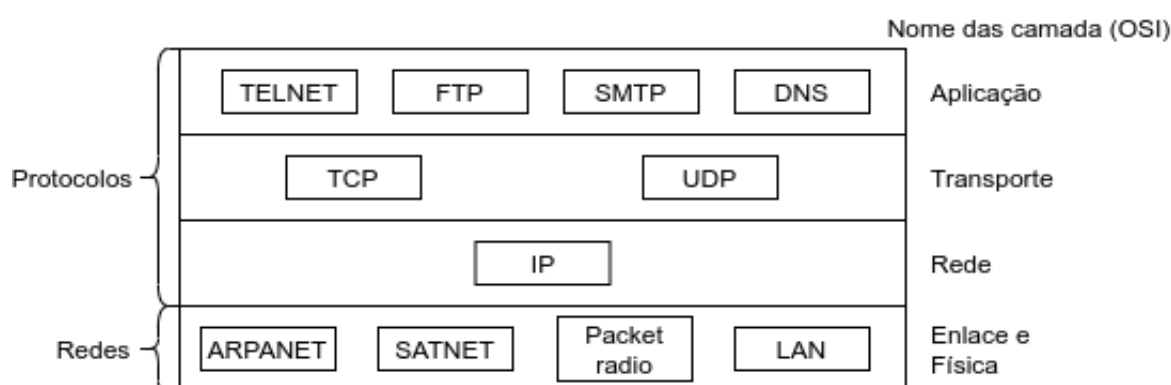


Figura 6 – Pilha TCP/IP e seus protocolos.

Fonte: adaptado de (TANENBAUM, 2003)

Segundo Kurose e Ross (2010), essas camadas são denominadas:

- Camada de aplicação: em que residem os protocolos de nível mais alto. Um protocolo da camada de aplicação é distribuído por diversos sistemas finais, sendo que a aplicação em um sistema usa o protocolo para trocar pacotes de informação com a aplicação em outro sistema. Exemplos de protocolos:
 - HTTP (*Hypertext transfer protocol*).
 - SMTP (*Simple Mail Transfer Protocol*).
 - FTP (*File Transfer protocol*).
 - DNS (*Domain Name System*).
- Camada transporte: em que reside os protocolos que fazem o transporte de dados da camada de aplicação, transportando mensagens entre os lados do cliente e do servidor de uma aplicação. Exemplos de protocolos:

- TCP (*Transmission Control Protocol*).
- UDP (*User Datagram Protocol*).
- Camada de rede: camada que contém o protocolo responsável pela movimentação, de uma máquina para outra, de pacotes de camada de rede conhecidos como datagramas. Um protocolo da camada de transporte passa um segmento TCP ou UDP e um endereço de destino à camada de rede. A camada de rede prove o serviço de entrega do segmento à camada de transporte da máquina destinatária. O protocolo da camada de rede é chamado de IP (*Internet Protocol*).
- Camada de enlace: é a camada que contém os protocolos que ficam responsáveis por enviar datagramas de um nó a outro, ou seja, faz o transporte do datagrama entre elementos da rede, como de uma máquina ao roteador, ou de roteador para roteador. Exemplos de protocolos:
 - Arpanet.
 - LAN (*local area network*).
 - WLAN (*wireless local area network*).

Com a popularização da internet essa comunicação se tornou cada vez mais comum, atingindo bilhões de usuários no mundo todo. Assim a comunicação cliente servidor precisa ser segura. A segurança de redes se preocupa em garantir que pessoas mal-intencionadas não leiam ou modifiquem secretamente mensagens enviadas a outro destinatário. Ela também lida com meio de identificar se uma mensagem recebida é verdadeira e tem uma origem confiável (TANENBAUM, 2003).

2.2.1 LWIP

A Biblioteca LwIP é uma implementação da pilha TCP/IP, focada em ser pequena e portátil, reduzindo a utilização de recursos como memória RAM e ainda tendo um TCP completo, se tornando adequada para sistemas embarcados. Foi originalmente desenvolvida por Adam Dunkels nos laboratórios da *Computer and Networks Architectures* (CNA), no Instituto Sueco de Ciência da Computação (SICS) e agora é desenvolvida e mantida por uma rede mundial de desenvolvedores (DUNKELS, 2002). Possui três *Application Programing Interfaces* (APIs):

- RAW API (API básica): É a API nativa do LwIP, possui melhor desempenho e o menor tamanho de código, porém torna o desenvolvimento de aplicações mais complexo.
- Netconn API: É uma API sequencial de alto nível que requer um sistema operacional de tempo real (RTOS). Habilita operações com múltiplas *threads*.
- BSD Sockets API: API de *sockets* de Berkeley, desenvolvida em cima da API Netconn.

Essas API's implementam diversos protocolos de rede, incluindo:

- HTTP permite a obtenção de recursos, tais como documentos HTML, imagens, scripts e outros tipos de arquivos.

- FTP para o envio e recebimento de arquivos.
- SMTP para o envio de mensagens de correio eletrônico através da internet.
- ICMP (*Internet Control Message Protocol*) para manutenção e *debugging* da rede.
- TCP com controle de congestionamento, estimativa de latência, recuperação e retransmissão rápida.
- IP incluindo o envio de pacotes para múltiplas interfaces de rede.

A seguir serão explanados com mais profundidade alguns dos protocolos implementados pela LwIP que serão utilizados neste trabalho.

2.2.1.1 Hypertext Transfer Protocol (HTTP)

Segundo [Kurose e Ross \(2010\)](#), o protocolo da camada de aplicação HTTP é implementado em dois programas, um programa cliente e outro servidor. Os dois são executados em sistemas finais diferentes, se comunicam entre eles por meio de uma troca de mensagens HTTP. O HTTP define a estrutura dessas mensagens assim como o modo como o cliente e o servidor as trocam.

O HTTP define como clientes requisitam documentos aos servidores e como eles os transferem ao cliente. Ele utiliza o TCP como seu protocolo de transporte subjacente. O cliente HTTP primeiramente inicia uma conexão TCP com o servidor. Após essa conexão ser estabelecida, os processos da aplicação e do servidor acessam o TCP por meio de sua interface de sockets. No lado do cliente a interface de socket é uma porta entre o processo cliente e a conexão TCP. No lado do servidor, ela é uma porta entre o processo servidor e a conexão TCP.

O cliente envia mensagens de requisição HTTP para sua interface de socket e recebe uma mensagem de resposta HTTP de sua interface de socket. De uma maneira parecida acontece do lado do servidor, onde ele recebe mensagens de requisição HTTP de sua interface de socket e envia mensagens respostas a sua interface. Assim a mensagem sai da camada de aplicação e passa para a camada de transporte.

2.2.1.2 Transmission Control Protocol (TCP)

Segundo [Tanenbaum \(2003\)](#), O TCP foi projetado especificamente para oferecer um fluxo de bytes fim a fim confiável em uma inter-rede não-confiável. Uma inter-rede é diferente de uma única rede porque suas diversas partes podem ter topologias, larguras de banda, retardos, tamanhos de pacotes e outros parâmetros totalmente diferentes. O TCP foi projetado para se adaptar dinamicamente às propriedades da inter-rede e ser robusto diante de muitas categorias de falhas que podem ocorrer.

Cada máquina compatível com TCP tem uma entidade de transporte TCP, que pode ser um procedimento de biblioteca, um processo do usuário ou parte do núcleo. Em todos os casos, ele gerencia fluxos e interfaces TCP para a camada IP. Uma entidade TCP aceita fluxos de dados de usuários provenientes de processos locais, divide-os em partes de no máximo 64

kB e envia cada parte em um datagrama IP distinto. Quando os datagramas IP que contêm dados TCP chegam a uma máquina, eles são enviados à entidade TCP, que restaura o fluxo de bytes originais.

A camada IP não oferece garantia que os datagramas serão entregues de forma apropriada, portanto, cabe ao TCP administrar os *timers* e retransmiti-los sempre que necessário. Os datagramas também podem chegar fora de ordem, o TCP também terá que os reorganizar em mensagens na sequência correta.

2.2.2 MBED TLS

A Mbed TLS provê a implementação da camada de segurança para a comunicação com o servidor, que pode evitar que uma versão maliciosa do software seja recebida de uma fonte não confiável. Também nos fornece peças de software contendo algoritmos criptográficos, que podem ser facilmente acoplados a qualquer aplicação. Como é o caso do algoritmo SHA-2 que ficará responsável por fazer a verificação da integridade dos arquivos baixados.

A biblioteca Mbed TLS foi desenvolvida para se integrar facilmente a aplicações embarcadas existentes, e fornecer os blocos de construção para uma comunicação segura, criptografia e gerenciamento de chaves. Como o seu intuito é ser o mais flexível possível, permite que sejam integrados ao sistema somente as funcionalidades necessárias, diminuindo assim o tamanho total que a biblioteca ocuparia no sistema (DEVINE, 2006).

A Figura 7 ilustra como a biblioteca cria uma camada intermediária entre a aplicação final e a camada TCP/IP, chamada de TLS (*Transport Layer Security*). A Mbed TLS pode ser usada para criar um servidor e cliente SSL (*Secure Sockets Layer*)/TLS, fornecendo uma estrutura para a configurar e se comunicar por meio de um canal de comunicação SSL/TLS. A camada TLS criada depende diretamente dos módulos de análise de certificado, criptografia simétrica ou assimétrica e *hash* da biblioteca utilizada.

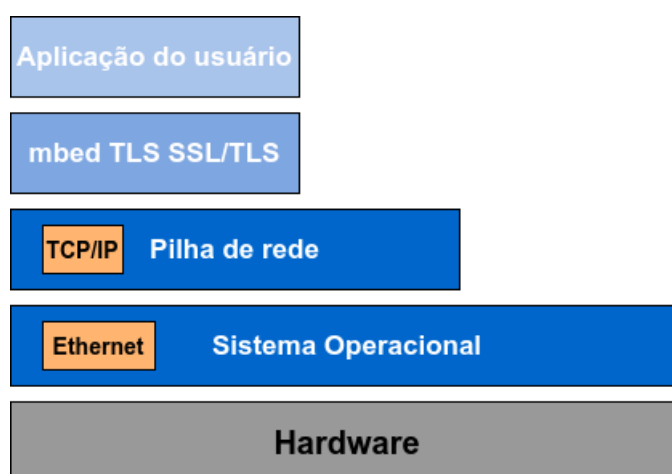


Figura 7 – Pilha de comunicação.

Fonte: adaptado de (DEVINE, 2006)

2.2.2.1 Transport Layer Security (TLS)

A *Transport Layer Security* assim como seu precursor *Secure Sockets Layer*, é um protocolo de segurança projetado para fornecer segurança na comunicação sobre uma rede de computadores. Segundo [Dierks e Rescorla \(2008\)](#), o protocolo TLS visa fornecer privacidade e integridade de dados entre aplicações que se comunicam. Quando uma rede está protegida por TLS, conexões entre um cliente e um servidor devem ter uma ou mais das seguintes propriedades:

- A conexão é privada, pois, utilizada criptografia simétrica para criptografar os dados transmitidos. As chaves para essa criptografia são geradas exclusivamente para cada conexão e são baseadas em um segredo compartilhado que foi negociado no início da sessão (conhecido como *Handshake Protocol*). No protocolo de *Handshake*, o servidor e o cliente negociam qual algoritmo de criptografia e chaves criptográficas usar antes que o primeiro dado seja transmitido. Como a negociação ocorre somente no início da transmissão, qualquer invasor que intercepte a transmissão não poderá decifrar as mensagens, enviar dados e alterar os termos dessa negociação. Então a negociação de um segredo compartilhado é segura e confiável.
- A conexão é confiável, pois cada mensagem transmitida inclui uma verificação de integridade de mensagem, utilizando um código de autenticação de mensagem, como uma *hash* criptográfica, para evitar perda não detectada ou alteração dos dados durante a transmissão.

Uma vantagem do TLS é que ele é independente do protocolo da aplicação. No entanto, ele não especifica como os protocolos adicionam segurança ao TLS, as decisões sobre como iniciar o *handshaking* e como interpretar os certificados de autenticação trocados são deixadas ao critério dos projetistas e desenvolvedores de protocolos executados sobre o TLS.

2.2.2.2 Função Hash

Segundo [Kurose e Ross \(2010\)](#), uma função *hash* é um algoritmo que recebe uma entrada, m , e computa uma cadeia de bits de tamanho fixo $H(m)$ conhecida como *hash*. Uma função de *hash* criptográfica deve apresentar a seguinte propriedade: no processamento, é impraticável encontrar duas mensagens diferentes x e y em que $H(x) = H(y)$.

A SHA-1 (*Secure Hash Algorithm*) é um conjunto de funções *hash* criptográficas projetadas pela NSA ([NSA, 1952](#)). Esse algoritmo, de forma resumida, se baseia em processar um resumo de mensagem de 160 bits por meio de um processo de quatro etapas, formado por uma etapa de enchimento (Adicionando 'uns' seguidos de 'zeros' suficientes, de maneira em que o comprimento da mensagem satisfaça determinados critérios), uma etapa de anexação (anexação de uma representação de alguns bits do comprimento da mensagem antes do enchimento), uma etapa de inicialização de um acumulador e uma etapa final iterativa, em que os blocos de palavras da mensagem são processados (misturados) em quatro rodadas de processamento.

Comparando o *hash* computado (a saída de execução do algoritmo) a um valor de *hash* conhecido e esperado, pode-se determinar a integridade dos dados. Por exemplo, calcular o *hash* de um arquivo baixado e comparar o resultado com um *hash* conhecido, pode comprovar que o arquivo foi modificado ou adulterado.

SHA-2 é um conjunto de funções *hash* criptográficas que contém mudanças significativas de seu antecessor. É composta por seis funções *hash* com valores de *hash* que são de 224, 256, 384 ou 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256.

2.3 SISTEMAS DE ARQUIVO

Segundo [Tanenbaum \(2007\)](#), para resolver diversos problemas com o armazenamento de grandes quantidades de dados, a perda de dados após o fim da execução do processo que os criou e a necessidade de tornar esses dados independentes de quaisquer processos. Existe a necessidade da criação de uma estrutura de armazenamento de informações a longo prazo. Os três requisitos fundamentais para essa estrutura são:

- Deve ser possível armazenar um volume grande de informações;
- Os dados devem sobreviver ao término do processo que os estão utilizando;
- Vários processos devem ser capazes de acessar os dados concomitantemente.

Essa estrutura é chamada de arquivo, e é vastamente utilizada por diversos sistemas. Os arquivos são utilizados para armazenar dados em discos e outras mídias externas. Então os processos podem ler e escrever novos dados quando necessário. As informações armazenadas em arquivos devem ser persistentes, logo, não devem ser afetadas pela criação e pelo término do processo. Um arquivo só deve desaparecer quando o seu criador o apagar ([TANENBAUM, 2007](#)).

O modo como os arquivos são estruturados, nomeados, acessados, usados, protegidos e implementados são definidos geralmente pelo sistema operacional. A parte do sistema operacional responsável por esse gerenciamento é chamada de sistema de arquivos. Os arquivos podem, no caso de sistemas embarcados, ser gerenciados por API's que criam uma camada independente do sistema operacional e gerenciam os arquivos, como é o caso da biblioteca FatFs.

Existem diversas formas de implementar um sistema de arquivo. Nessa implementação é necessário saber como os arquivos e seus diretórios são armazenados, como o espaço em disco é gerenciado e em como fazer tudo funcionar de modo eficiente e confiável. Um dos sistemas de arquivos padrões para o uso em memórias que são divididas em bloco é o FAT32. Um cartão SD é um dispositivo de memória não volátil criado pela SD Card Association ([SD CARD ASSOCIATION, 2016](#)), que possui sua memória dividida em blocos e que por padrão faz uso do sistema de arquivo FAT.

2.3.1 SISTEMA DE ARQUIVO FAT

Segundo [Tanenbaum \(2007\)](#), o sistema de arquivo FAT (*File Allocation Table*) é implementado por meio de uma alocação de memória encadeada usando uma tabela na memória. Nessa organização, o bloco de memória inteiro está disponível para dados. Além disso, o acesso aleatório é muito mais fácil. Mesmo que o encadeamento ainda tenha que ser seguido para encontrar determinado deslocamento dentro do arquivo, ele está inteiramente na memória, de modo que, pode ser seguido sem necessidade nenhuma de referenciar o disco.

A [Figura 8](#) ilustra como é a tabela, mostrando que o arquivo *A* inicia-se no bloco 4 e segue o encadeamento até o seu fim, assim como o arquivo *B* que se inicia no bloco 6. Ambos terminam com um marcador especial que no caso é o número -1.

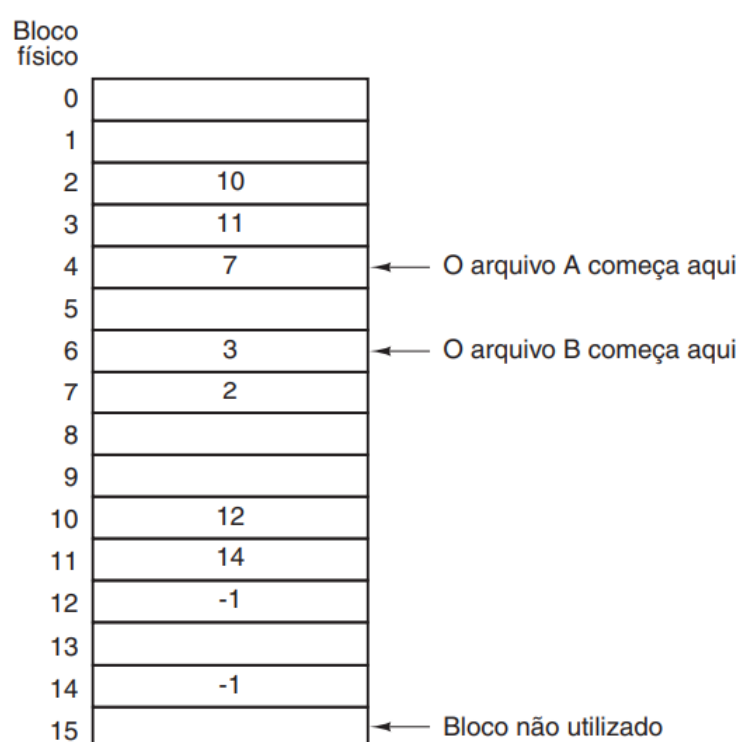


Figura 8 – Alocação encadeada usando tabela de alocação de arquivo.

Fonte: ([TANENBAUM, 2007](#))

A principal desvantagem deste método é que a tabela inteira precisa estar na memória o tempo todo. Com um disco de 20 GB e um tamanho de bloco de 1 KB, a tabela precisa de 20 milhões de entradas, uma para cada um dos 20 milhões de blocos do disco. Cada entrada tem de ter no mínimo 3 bytes para manter o endereço dos blocos. Para facilitar sua pesquisa, as entradas acabam ocupando 4 bytes. Assim, a tabela ocupará 60 MB ou 80 MB de memória principal o tempo todo.

Existe também o sistema de arquivo exFAT que é utilizado para mídias com capacidade de armazenamento maiores que 4 GB, que foi adotada como sistema de arquivo padrão para

cartões de memória (SD card) maiores de 4 GB, pela SD Card Association ([SD CARD ASSOCIATION, 2016](#)).

2.3.2 FATFS

FatFs é um módulo genérico de um sistema de arquivo FAT/exFAT, para pequenos sistemas embarcados com recursos computacionais reduzidos. É escrito em conformidade com a ANSI C (C89) e é completamente separado da camada de entrada e saída do sistema, portanto, é independente da plataforma utilizada. É um *software* livre de código aberto e proporciona a leitura, escrita, criação e remoção de arquivos, além do gerenciamento e navegação de diretórios. A [Figura 9](#) ilustra como o módulo é independente da aplicação e da plataforma utilizada.

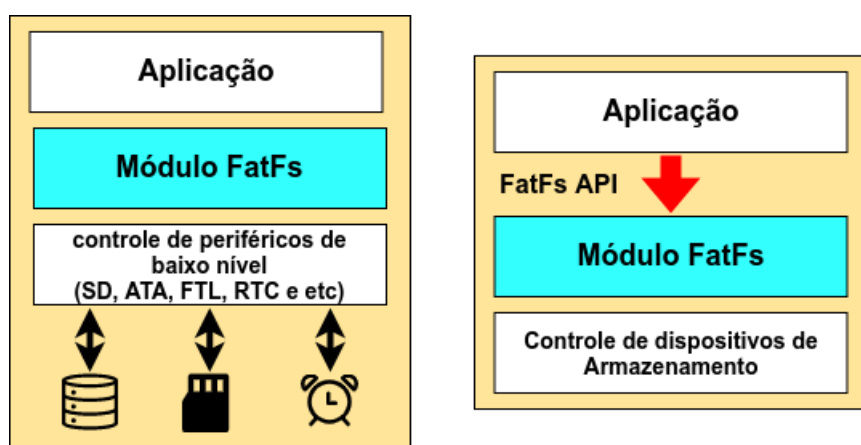


Figura 9 – Posição da biblioteca FatFs na aplicação.

Fonte: ([CHAN, 2016](#))

A FatFs fornece várias funções do sistema de arquivos para a aplicação. Assim pela aplicação é possível gerenciar os arquivos e diretórios, como é ilustrado da [Figura 9](#). As principais funções fornecidas pela FatFs para a aplicação são ([CHAN, 2016](#)):

- Acesso a arquivos.
 - f_open - Abre/Cria um arquivo.
 - f_close - Fecha um arquivo aberto.
 - f_read - Lê os dados de um arquivo.
 - f_write - Escreve dados em um arquivo.
- Acesso a diretórios.
 - f_opendir - Abre um diretório.
 - f_closedir - Fecha um diretório aberto.
- Gerenciamento de arquivos e diretórios.
 - f_stat - Verifica a existência de um arquivo ou diretório.
 - f_unlink - Remove um arquivo ou diretório.
 - f_rename - Renomeia ou move um arquivo, ou diretório.
 - f_mkdir - Cria um diretório.

- `f_chdir` - Muda o diretório atual.
- Gerenciamento de volume e configurações do sistema.
 - `f_mount` - Registra ou remove registro da área de trabalho da partição.
 - `f_mkfs` - Cria uma partição FAT na unidade lógica.
 - `f_fdisk` - Cria uma partição na unidade física.
 - `f_getfree` - Obtém o espaço livre da partição.

2.4 HARDWARE ABSTRACTION LAYER (HAL)

A camada de abstração de hardware (*hardware abstraction layer*) é uma divisão lógica de código que serve como camada de abstração entre o hardware e o software de um sistema computacional. Ele prove uma interface de drivers dos periférico do microcontrolador com o programa, permitindo assim uma comunicação mais fácil entre hardware e software.

O principal objetivo de um HAL é permitir que diferentes arquiteturas de hardwares funcionem com o mesmo software, para isso fazem uso de uma interface uniforme dos periféricos do sistema, mantendo sempre as mesmas chamadas de funções e de periférico desde a sua inicialização até sua utilização.

O HAL está incluído em diversos sistemas operacionais para evitar que se modifiquem o Kernel para que ele possa ser executado em diferentes arquiteturas com diferentes conjuntos de hardwares. Um computador pode possuir uma camada de abstração de hardware dentro do kernel de seu sistema operacional, ou de forma de drivers que garantem uma interface consistente para a aplicação interagir com os periféricos fornecidos pelo hardware disponível.

As vantagens que o HAL fornece são:

- Permite que aplicações extraiam o máximo de desempenho possível dos hardwares.
- Possibilitar que os sistemas operacionais e diversos software funcionem em diferentes arquiteturas de hardware.
- Permite que driver de dispositivos forneçam acesso direto a periféricos do hardware, o que permite que programas sejam independentes dos dispositivos.
- Facilita assim a portabilidade de um software.

2.4.1 STM32CUBE HAL

Segundo a [STMicroelectronics \(2021\)](#), o STM32Cube é uma iniciativa da STMicroelectronics para melhorar significativamente a produtividade do desenvolvedor, reduzindo o esforço, o tempo e o custo de desenvolvimento, e ele cobre toda a linha de produtos da STM32.

É uma ferramenta de desenvolvimento que é composta por um software que permite a geração de códigos em C iniciais de um novo projeto. Nesta ferramenta é possível já fazer as configurações iniciais de periféricos, bibliotecas, configurações de clock entre outras definições necessárias. Todos esses ajustes são feitos a partir de uma interface gráfica facilitando o

entendimento e tornando ainda mais rápido o desenvolvimento. A interface do STM32Cube pode ser vista na [Figura 10](#).

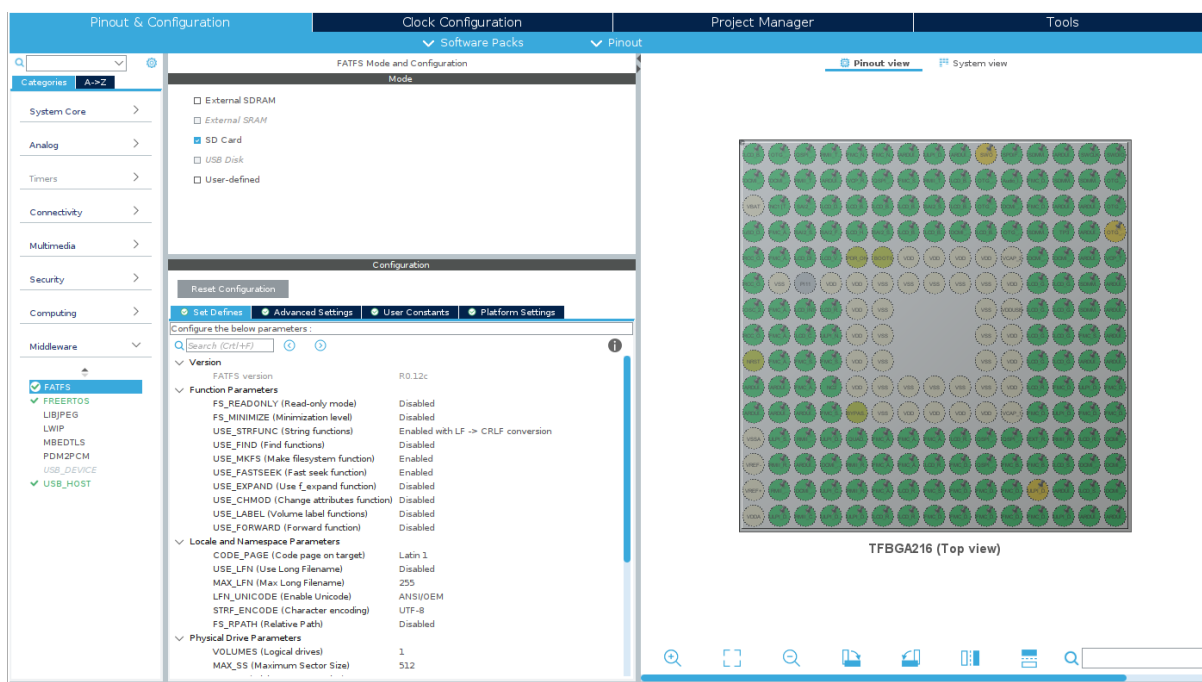


Figura 10 – Posição da biblioteca FatFs na aplicação.
Fonte: (CHAN, 2016)

Segundo a [STMicroelectronics \(2021\)](#), as APIs do driver HAL são divididas em duas categorias: APIs genéricas, que fornecem funções comuns e genéricas para todas as séries STM32 e APIs extendidas, que incluem funções específicas e personalizadas para uma determinada família ou microcontrolador específico. Os drivers HAL incluem um conjunto completo de APIs prontas para uso que simplificam a implementação do aplicativo do usuário. Por exemplo, os periféricos de comunicação contêm APIs para inicializar e configurar-los, gerenciar transferências de dados, lidar com interrupções ou acesso direto a memória e gerenciar erros de comunicação.

2.5 TRABALHOS CORRELATOS

Durante a elaboração desse trabalho foram identificados alguns trabalhos que produzem alguns métodos de atualização OTA para diversas aplicações, que serão explanados a seguir:

- **Firmware over the air for automotive, Fotomotive:** Esse trabalho introduz uma solução para atualização de veículos com a ajuda de fabricantes de equipamentos automotivos para reduzir custos com *recalls* e assim aumentar a qualidade de seus produtos, facilitar as atualizações e controlar melhor a frota de veículos no mercado. Essa solução consiste em atualizar a unidade de controle do motor por meio de métodos OTA, sem a necessidade de uma conexão física com o veículo ([Odat; Ganesan, 2014](#)).

- **Firmware over the air for home cybersecurity in the Internet of Things:** Esse trabalho descreve a utilização de um método de atualização de *firmware* para roteadores caseiros, utilizando sistemas de gerenciamento de rede e de suporte de operações de fornecedores de acesso à *internet* ([Teng et al., 2017](#)).
- **Internet of Things: Over-the-Air (OTA) firmware update in Lightweight mesh network protocol for smart urban development:** Esse trabalho introduz um novo sistema de atualização de *firmware* *Over-The-Air* (OTA) baseado no protocolo de rede *Lightweight mesh*, que prove descoberta de rotas, estabelecimento e um protocolo de malha de baixa potência ([Chandra et al., 2016](#)).

Como observado, todos os trabalhos correlatos tem um objetivo único e diferente para a aplicação de sua atualização OTA, enquanto esse trabalho tem como meta produzir um sistema que pode abranger diferentes aplicações.

3 SISTEMA DE ATUALIZAÇÃO DE FIRMWARE OVER-THE-AIR

Nesse capítulo é retratado como será o funcionamento do sistema que será desenvolvido, mostrada uma visão geral do projeto, listadas as funcionalidades de cada uma das partes do *software*, explicando sua atividade, sua implementação, e as ferramentas utilizadas para o seu teste e os materiais utilizados.

3.1 VISÃO GERAL

O *software* que será desenvolvido nesse trabalho é dividido em duas partes, uma contendo o *bootloader*, com o auxílio da biblioteca FatFs, realizará a comunicação com o cartão SD, que conterá o novo *firmware* previamente recebido. Assim poderá substituir o *software* anterior da aplicação por um novo. Essa parte do *software* ficará armazenada em uma região da memória que dificilmente será reescrita, podendo ser reescrita somente com o auxílio de ferramentas de desenvolvimento como um JTAG e/ou *debugger*, então é uma peça do programa que provavelmente será substituída. Será uma parte que é portátil para todos os microcontroladores da família STM32, pois faz uso direto de funções de escrita na memória flash obtidas por meio do STM32Cube HAL, ficando a cargo do projetista fazer um pequeno porte que posteriormente será explicado neste trabalho.

A outra parte desse trabalho será uma API, contendo as demais funções necessárias para a comunicação com o servidor, que enviará para o sistema o novo *firmware*, por meio do uso da biblioteca LwIP, garantirá a segurança dessa conexão com a utilização de uma camada extra de proteção, com biblioteca Mbed TLS. Essa API irá conectar-se a um servidor, em que verificará a disponibilidade de uma nova versão de *software*.

Após ser confirmada a existência de uma nova versão de *firmware*, a API irá se comunicar novamente com o servidor com o intuito de fazer o *download* dessa nova versão, e a armazenar no cartão SD do sistema. Com o download concluído com sucesso a API se conectará novamente com o servidor para obter o arquivo contendo o hash deste firmware, ela então executará uma função que cria um hash para o *firmware* baixado e o compara com arquivo de hash obtido do servidor, para assim garantir que o firmware está integralmente no cartão sd. Então o *bootloader* entre em ação após uma reinicialização do sistema. De forma geral o funcionamento do sistema pode ser observado na [Figura 11](#)

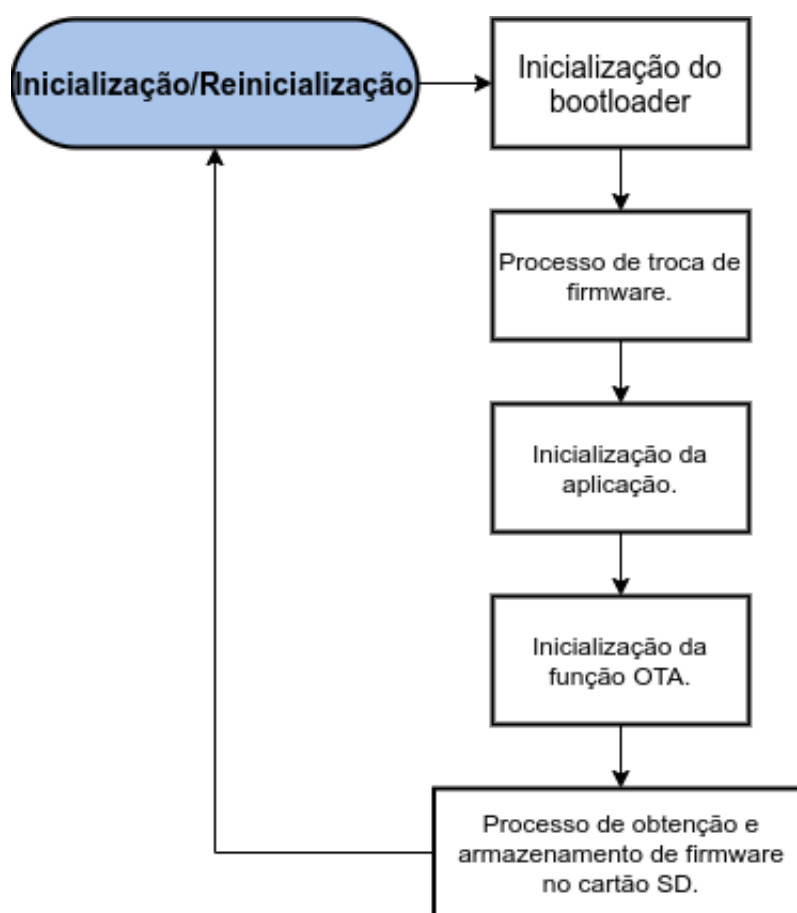


Figura 11 – Visão geral do funcionamento do sistema de atualização.
Fonte: autoria própria.

A API será uma peça de *software* que poderá ser substituída e atualizada em conjunto com as demais aplicações do sistema, como, as bibliotecas LwIP, Mbed TLS, o sistema operacional, entre outras peças de *software* utilizadas pela aplicação. O sistema de atualização OTA utiliza-se de bibliotecas já conhecidas e vastamente utilizadas por desenvolvedores de sistemas embarcados. Assim projetos que necessitem fazer comunicação segura via rede, leitura e escrita de cartões SD, possam utilizar esse sistema de modo a poupar espaço na memória, visando a reutilização dessas bibliotecas. Portanto, o sistema pode ser amplamente utilizado por sistema de IoT.

Em caso de uma falha durante o processo de atualização OTA, o sistema tem a habilidade de se recuperar de forma autónoma. Como não haverá sobreescrita na área em que o *firmware* está posicionado no cartão SD, uma simples reinicialização do sistema pode fazer com que o bootloader seja ativado novamente e refaça o processo de cópia da memória.

3.2 BOOTLOADER

A partir de um arquivo de *linker*, a memória da plataforma será customizada com o intuito de abrigar os arquivos necessários para o *bootloader* e protegê-lo de eventuais sobreescritas

que podem vir a ocorrer. Esse arquivo de *linker*, assim como o próprio *bootloader*, será escrito somente para os microcontroladores da família STM32, visto que cada plataforma tem suas próprias características como, tamanho de memória e endereços diferentes para cada fabricante e/ou arquitetura.

No arquivo de *linker* será especificada uma área especial na memória flash do sistema em que será abrigado o *bootloader*. Também será responsável por fazer com que o *bootloader* seja chamado após a inicialização do sistema. Assim será garantido que o *bootloader* sempre seja executado após a reinicialização do sistema embarcado.

O *bootloader* será responsável em fazer a troca de cada versão de *firmware* instalado no sistema embarcado. Sempre que o sistema for iniciado, o *bootloader* será inicializado e fará a procura de arquivos. Essa busca será possível pelo fato da biblioteca FatFs, que está implementada junto ao *bootloader*, criar um sistema de arquivos no cartão SD do sistema alvo, assim o *bootloader* pode acessar a memória do cartão sem a necessidade da aplicação final ser inicializada.

Se após o *reset* a procura do arquivo contendo a versão do *firmware* novo retornar com um resultado positivo, ele converte o valor contido neste arquivo de uma string para um tipo inteiro e o compara com os quatro últimos bytes da memória flash, posição onde se encontra a versão atual do *firmware*, caso a versão do novo firmware seja maior que a do firmware atual o *bootloader* inicia o processo de atualização.

Nesse processo o *bootloader* substitui completamente o *firmware* e demais bibliotecas e API's em áreas não protegidas na memória, pelo binário do *firmware* presente no cartão SD. Esse processo é implementado com o uso das funções de escrita na memória flash do HAL fornecido pela STM32, onde inicialmente é feito o processo de apagamento massivo dos setores da aplicação da memória flash, dessa forma esses setores são preenchidos com o valor 0xFF em cada byte.

Após o processo de apagamento é iniciado o processo de escrita, em que o arquivo contendo o firmware é lido a cada 512 bytes para um buffer, e a partir deste buffer são escritos 4 bytes por vez na memória flash, assim esse processo se repete até que o arquivo contendo o novo firmware seja completamente escrito na memória. Finalizada a escrita do novo firmware, acontece a escrita da versão nos quatro últimos bytes da memória somente após essa escrita o processo de atualização pode ser considerado concluído com sucesso, e então ele pode apagar do cartão SD os arquivos do firmware e versão.

Caso o *bootloader* seja iniciado e em algum momento detectar que o valor dos quatro últimos bytes são iguais a 0xFFFFFFFF, ele identifica que a última operação de atualização não foi concluída com sucesso. Neste estado o *bootloader* fica sempre tentando encontrar uma nova versão do *firmware* no cartão SD e caso não encontre ele fica reiniciando o microcontrolador, e caso ele encontre ele tenta atualizar novamente como o firmware encontrado, independente da versão dele, garantindo assim que o sistema seja resistente a eventuais erros e eventos não

previstos, como quedas de energia durante o processo. O funcionamento do *bootloader* pode ser observado na Figura 12.

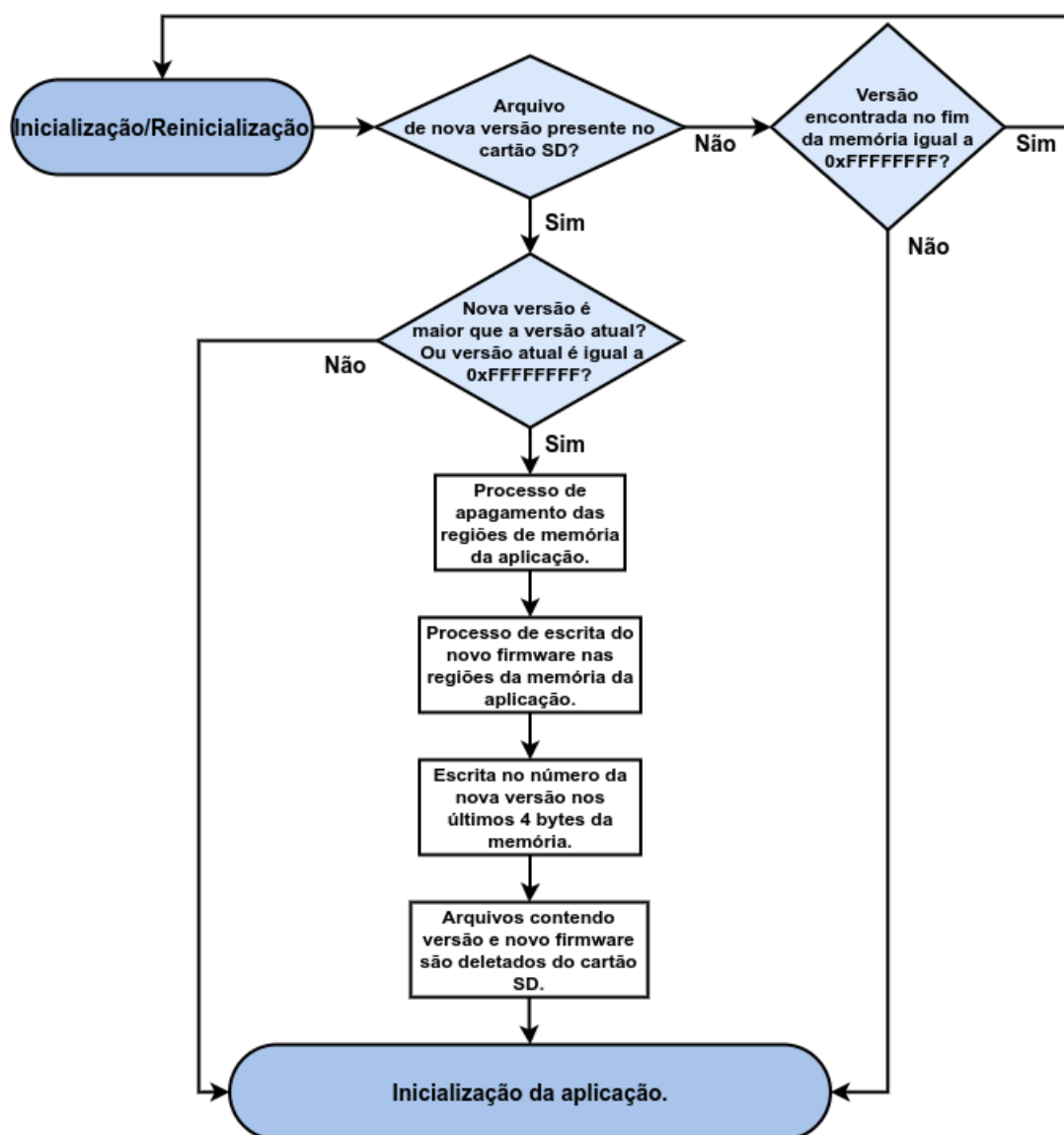


Figura 12 – Diagrama de funcionamento do *bootloader*.
Fonte: autoria própria.

3.3 API DE ATUALIZAÇÃO OTA

A API de atualização OTA que foi desenvolvida nesse trabalho tem o propósito de ser o mais portátil possível, para assim, ser reutilizada por diversos projetos que necessitem da troca de seu *software* e com isso pode ser chamada quando o desenvolvedor necessitar, como após uma interrupção externa ou comando do servidor. Com esse objetivo, serão utilizadas as bibliotecas já bem difundidas, a LwIP para a criação da pilha TCP/IP, a Mbed TLS para criar uma camada de segurança nessa pilha, e a FATFS para a criação de um sistema de arquivos FAT. Assim desenvolvedores podem se aproveitar do fato de que essas bibliotecas já estão

em seus sistemas como padrão para utilizá-las em suas próprias funcionalidades. A seguir será retratado como serão cada uma das funcionalidades necessárias na API.

3.3.1 COMUNICAÇÃO COM O SERVIDOR

Com o uso da biblioteca LwIP e Mbed TLS foi criada uma pilha de comunicação no sistema alvo, que é responsável pela conexão segura com o servidor que fornecerá o novo firmware. Na implementação da pilha de comunicação, foi utilizada a API BSD Sockets, pois, o intuito é deixar o sistema de atualização portátil, e essa API fornece suporte a sistemas operacionais de tempo real entre outras vantagens.

Como a biblioteca Mbed TLS já foi desenvolvida para ser integrada facilmente a várias aplicações embarcadas, ela foi utilizada para criar protocolos de segurança nessa comunicação com o servidor. Foram utilizados padrões SSL/TLS para ser criado um canal criptografado entre o servidor e o sistema alvo, para garantir que todos os dados transmitidos sejam sigilosos e seguros.

A comunicação com o servidor será feita por meio de um servidor HTTP que utilizará o protocolo TCP para garantir que todos os dados obtidos pelo servidor sejam integros, evitando que o novo *firmware* e demais dados obtidos sejam corrompidos.

3.3.2 DOWNLOAD E ARMAZENAMENTO DO FIRMWARE

A partir da utilização da biblioteca FatFs, será criado um sistema de arquivo FAT, que gerenciará a memória presente no cartão SD dentro da aplicação, e ele pode ser utilizado tanto pela aplicação final do sistema embarcado, quanto pela API. Esse sistema de arquivo será utilizado para que se possa identificar a posição na memória em que o *firmware* novo será colocado após o seu *download*, evitando que outros arquivos, pertencentes a aplicação final, sejam colocados com o mesmo nome, e fazendo com que o *bootloader* interprete de forma errada os arquivos gerando erros.

Quando o desenvolvedor iniciar a função OTA, a API iniciará novamente a comunicação com o servidor que contém o *firmware* novo, dessa vez com o propósito de fazer *download* do arquivo contendo o número da nova versão do *software*. Após o *download* a API ainda irá verificar se o valor obtido por meio deste arquivo é maior que o presente nos últimos 4 bytes da memória, para assim verificar se existe a necessidade de se continuar com o processo de atualização.

Caso o valor da nova versão seja maior que a versão atual do firmware a API inicia o *download* do novo firmware, após esse processo a ferramenta inicia a comunicação novamente para obter agora o arquivo contendo o hash do firmware posteriormente baixado, e com isso é feito um teste de integridade neste firmware onde inicialmente se gera um hash a partir do algoritmo SHA-256 fornecido pela biblioteca MBED TLS, e esse hash é comparado com aquele baixado do servidor. Se esse teste retornar com sucesso o processo de atualização é continuado, e o arquivo de hash baixado do servidor é apagado do cartão SD e é iniciado o processo de

reinicialização do microcontrolador com o intuito de se iniciar o bootloader para completar o processo de atualização. A Figura 13 ilustra o funcionamento da API.

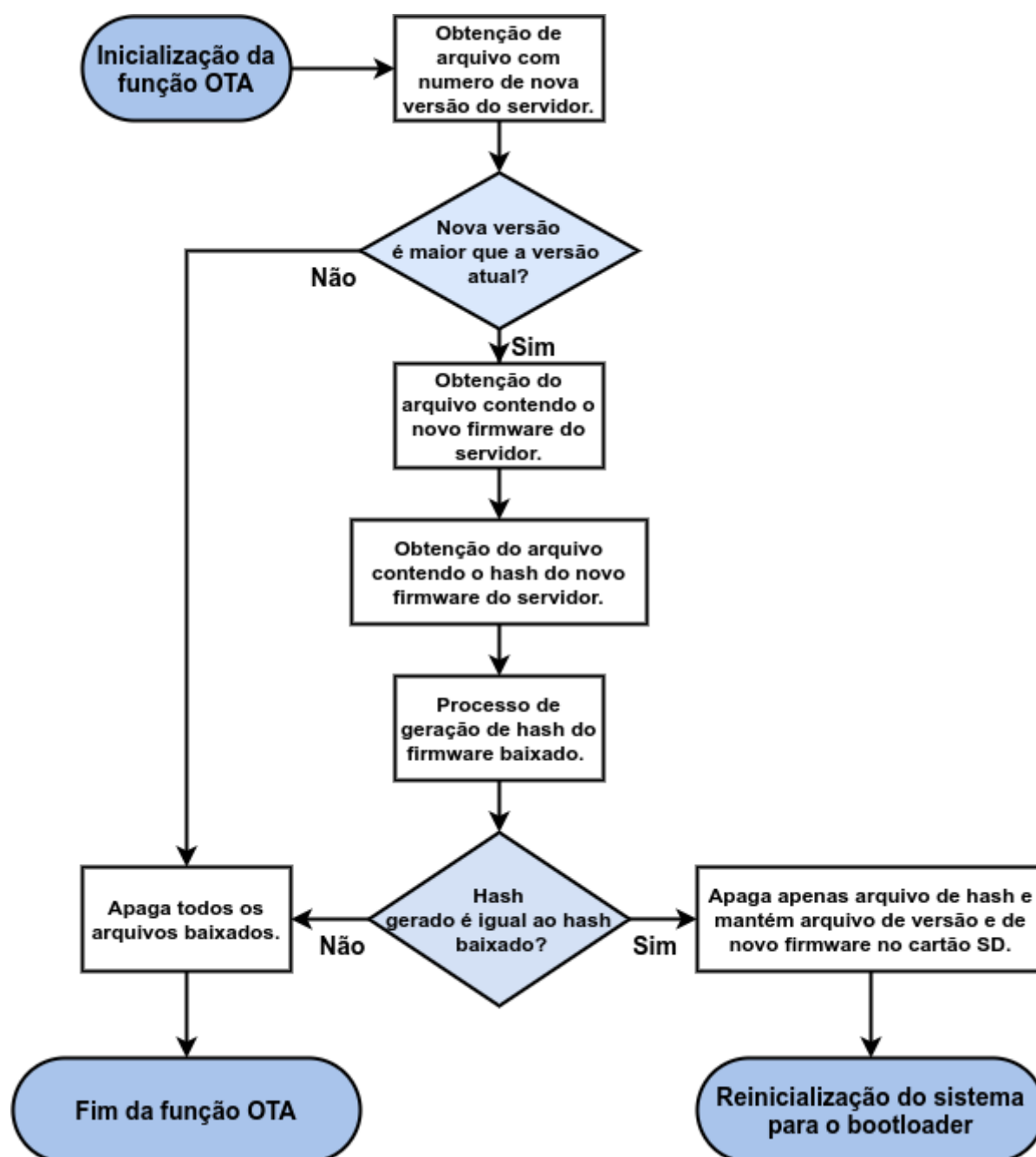


Figura 13 – Diagrama de funcionamento da API.

Fonte: autoria própria.

3.4 MATERIAIS UTILIZADOS

A API e o bootloader foi escrito na linguagem C, enquanto o *linker* será escrito em comandos de *linker*. A escrita desses códigos será feita com o uso do ambiente de desenvolvimento integrado Eclipse ([ECLIPSE FOUNDATION, 2001](#)). O sistema de atualização

OTA desenvolvido nesse trabalho é inicialmente desenvolvido para a plataforma STM32F746G-Discovery.

3.4.1 PLATAFORMA STM32F746G-DISCOVERY

O STM32F7 Discovery é um kit de desenvolvimento que permite ao usuário desenvolver e compartilhar aplicações com toda a série de microcontroladores STM32F7 baseados no processador ARM®Cortex®-M7 core. O kit discovery permite uma ampla diversidade de aplicações que podem se beneficiar de suporte a múltiplos sensores, áudio, tela gráfica, segurança, vídeos e conexões de alta velocidade ([STMICROELECTRONICS, 2019](#)). A [Figura 14](#) ilustra o kit STM32F746NGH6-Discovery.

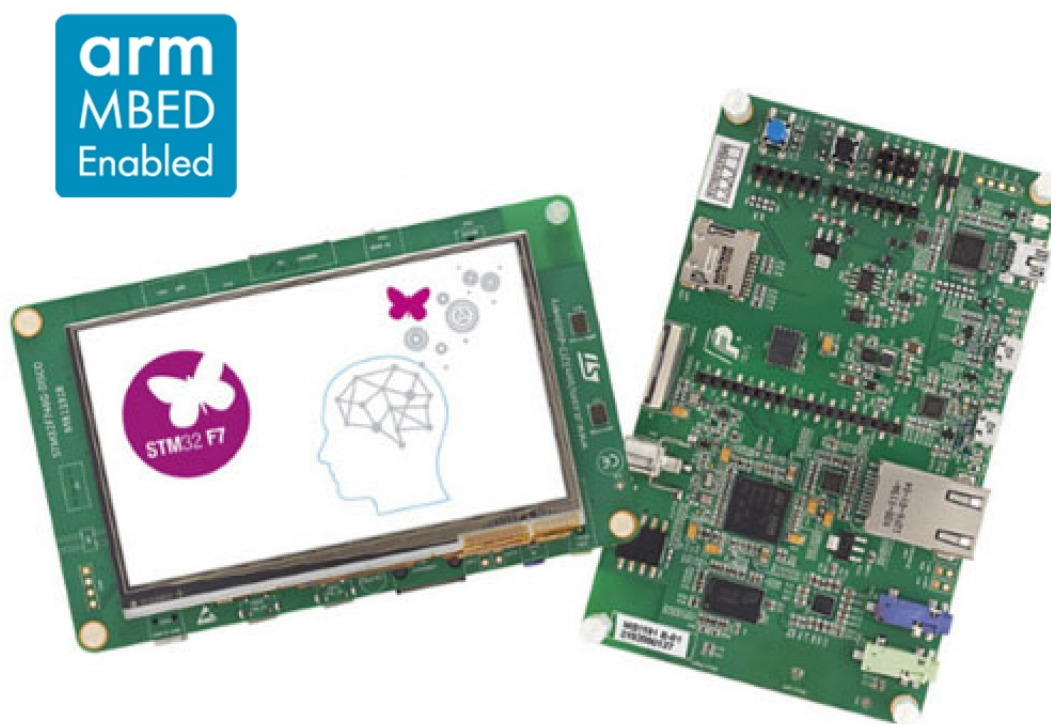


Figura 14 – Kit de desenvolvimento STM32F746G-Discovery.

Fonte: ([STMICROELECTRONICS, 2019](#)).

Algumas de suas principais características são ([STMICROELECTRONICS, 2019](#)):

- Microcontrolador STM32F746NGH6 com 1 Mbytes de memória flash e 340 Kbytes de RAM, em um pacote BGA216.
- 128-Mbit de memória Quad-SPI Flash.
- 128-Mbit SDRAM (Com 64 Mbits Acessível).
- Conector para cartão microSD.
- Conector Ethernet em conformidade com a IEEE-802.3-2002
- Tela LCD de 4,3 polegadas, com resolução de 480x272 com *touch-screen* capacitivo.

3.4.2 FIRMWARES DE TESTE PROPOSTOS

Para os testes apresentados neste trabalho foram desenvolvidos três firmwares muito parecidos, ambos possuem todas as bibliotecas necessárias para que sistema de atualização OTA proposto funcionem corretamente, além de possuírem o sistema operacional de tempo real FreeRTOS. Esses firmwares foram desenvolvido para somente darem suporte ao sistema e não exercerem nenhuma outra função, então temos uma estimativa do tamanho que somente o sistema de atualização, suas bibliotecas e o FreeRTOS ocupam em memória.

Esses firmwares contém em sua função main, além de inicializações necessárias de drivers, bibliotecas e do sistema operacional, uma pequena função que apresenta uma mensagem de apresentação mostrando a versão do firmware atual e uma mensagem de teste somente para fazer uma diferenciação entre as versões e como mostrada na [Figura 15](#).



Figura 15 – As três mensagens exibidas para diferenciação dos *firmware*.
Fonte: Autoria própria.

A função padrão destes firmware é um laço infinito que a cada XXXX segundos inicializa a função OTA que inicializa o processo de atualização, assim temos uma garantia que o firmware ira sempre ficar executando a função OTA.

4 UTILIZANDO O SISTEMA

Com o intuito de fazer a ferramenta criada neste projeto ser facilmente utilizada por diversos desenvolvedores esse capítulo foi criado para facilitar o entendimento de como utilizar o sistema de atualização OTA proposto. Destacando como portar e utilizar o bootloader e toda a API do firmware OTA. Para a utilização de ambos os firmwares desenvolvidos neste trabalho é sempre necessário que as bibliotecas que são utilizadas por eles já estejam incluídas no projeto. Para o bootloader, é necessário somente a biblioteca FATFS, enquanto para o OTA são necessárias as bibliotecas FATFS, LWIP e MBED TLS.

4.1 PORTANDO O BOOTLOADER

Para se utilizar o bootloader proposto em outros sistemas embarcados da família STM32 deve-se primeiramente observar a organização da memória FLASH do sistema microcontrolado que se deseja portar o bootloader. Como podemos observar na [Tabela 1](#) a memória FLASH do microcontrolador STM32F746NGH6 possui oito setores de memória com tamanhos distintos, para esse trabalho foi selecionado o primeiro setor de memória para abrigar o bootloader.

Nome	Endereço do bloco	Tamanho do setor
Setor 0	0x0800 0000 - 0x0800 7FFF	32 Kbytes
Setor 1	0x0800 8000 - 0x0800 FFFF	32 Kbytes
Setor 2	0x0801 0000 - 0x0801 7FFF	32 Kbytes
Setor 3	0x0801 8000 - 0x0801 FFFF	32 Kbytes
Setor 4	0x0802 0000 - 0x0803 FFFF	128 Kbytes
Setor 5	0x0804 0000 - 0x0807 FFFF	256 Kbytes
Setor 6	0x0808 0000 - 0x080B FFFF	256 Kbytes
Setor 7	0x080C 0000 - 0x080F FFFF	256 Kbytes

Tabela 1 – Organização do bloco de memória FLASH do microcontrolador STM32F746NGH6. Adaptado de: ([STMICROELECTRONICS, 2019](#)).

Para isso foi necessário modificar no arquivo de linker o tamanho máximo da memória utilizável para evitar que os dados do bootloader ultrapassem o tamanho que determinamos para ele. Assim no arquivo de linker foi modificado de forma que o tamanho máximo da memória seja de 32Kbytes e iniciada no setor 0. Com isso a configuração de memória do bootloader para o microcontrolador utilizado neste trabalho ficou da seguinte forma:

```
/* Specify the memory areas */
MEMORY
{
RAM (xrw)      : ORIGIN = 0x20000000 , LENGTH = 320K
FLASH (rx)     : ORIGIN = 0x80000000 , LENGTH = 32K
}
```

Como cada microcontrolador tem sua configuração de memória o desenvolvedor deve observar a configuração do sistema alvo e colocar sempre o bootloader no setor 0 de seu microcontrolador.

Feita a modificação no arquivo de linker o desenvolvedor iniciará a alteração do arquivo `bootloader.h` que contem algumas definições dependentes do seu microcontrolador. Neste arquivo as definições que precisam ser alteradas são:

- `FIRMWARE_VERSION_ADDRESS`: Esta definição mostra ao bootloader a posição na memória FLASH em que se deve armazenar a versão atual da aplicação presente na placa e deve ser sempre os quatro últimos bytes da memória, e deve sempre ser o mesmo configurado na API de atualização OTA. No caso do microcontrolador deste trabalho foi utilizada a posição: `0x080FFFC`.
- `FIRMWARE_PATH`: Esta definição mostra qual o caminho do arquivo em que se encontra o novo firmware que foi baixado pela API OTA, deve ser sempre igual ao que será definido na API.
- `FIRMWARE_NEW_VERSION_PATH`: Esta definição mostra qual o caminho do arquivo em que se encontra a versão do novo firmware que foi baixado pela API OTA, deve ser sempre igual ao que será definido na API.
- `APP_START_ADDRESS`: Esta definição mostra ao bootloader a posição na memória FLASH em que se deve armazenar o início da aplicação que será trocada sendo sempre o início do setor 1. No caso do microcontrolador deste trabalho foi utilizada a posição: `0x08008000`.

Com essas alterações já é possível utilizar o bootloader em sistemas embarcados que utilizam microcontroladores da família STM32, restando agora a configuração da aplicação que será utilizada em conjunto com o bootloader e a configuração da API de atualização OTA.

4.2 CONFIGURAÇÃO DA API OTA

Assim como no bootloader, a aplicação também precisa ter seu arquivo de linker modificado para evitar sobrescritas no espaço reservado para o bootloader e reservar o espaço necessário para a variável de versão. Com isso o desenvolvedor deve novamente observar a [Tabela 1](#) e verificar qual posição de memória se inicia sua aplicação e o tamanho total dela deve ser obtido com a seguinte fórmula:

$$\text{Tamanho da aplicacao} = \text{Final da FLASH} - \text{inicio do setor 1 da FLASH} - 4 \text{ bytes} \quad (1)$$

Utilizando a fórmula para o microcontrolador STM32F746NGH6 temos que o início do setor 1 de memória é `0x08008000` e o fim do último setor de memória é `0x080FFFFF`, assim podemos obter os valores de início e tamanho da aplicação e assim configurar o arquivo de linker da aplicação da seguinte forma:

```
/* Specify the memory areas */
```

MEMORY

```
{  
RAM (xrw)      : ORIGIN = 0x20000000 , LENGTH = 320K  
FLASH (rx)     : ORIGIN = 0x08008000 , LENGTH = 0xF7FFB  
}
```

Feitas as alterações necessárias no arquivo de linker o desenvolvedor tem que alterar algumas definições no arquivo `ota_server.h` com o intuito de adequar a API de atualização OTA para a sua aplicação. Neste arquivo as definições que precisam ser alteradas são:

- **FIRMWARE_VERSION_ADDRESS**: Esta definição mostra a aplicação a posição na memória FLASH em que se deve armazenar a versão atual da aplicação presente na placa e deve ser sempre os quatro últimos bytes da memória, e deve sempre ser o mesmo configurado no bootloader. No caso do microcontrolador deste trabalho foi utilizada a posição: `0x080FFFFC`.
- **FIRMWARE_PATH**: Esta definição mostra qual o caminho do arquivo em que se deve armazenar o novo firmware que deverá ser baixado pela API OTA, deve ser sempre igual ao que será definido no bootloader.
- **FIRMWARE_NEW_VERSION_PATH**: Esta definição mostra qual o caminho do arquivo em que se deve armazenar a versão do novo firmware que será baixado pela API OTA, deve ser sempre igual ao que será definido no bootloader.
- **BOOTLOADER_START_ADDRESS**: Esta definição mostra a aplicação a posição na memória FLASH em que está armazenado o início do bootloader sendo sempre o início do setor 0. No caso do microcontrolador deste trabalho foi utilizada a posição: `0x08000000`.
- **FIRMWARE_NEW_VERSION_HASH_PATH**: Esta definição mostra qual o caminho do arquivo em que se deve armazenar o hash do novo firmware para que se compare com o hash gerado pelo firmware baixado, assim fazendo um teste para verificar se o firmware baixado é íntegro.
- **AUTH_SERVER**: Esta definição mostra qual deve ser o endereço do servidor em que se deve obter os arquivos necessários para a atualização de firmware, então deve ser personalizada para cada aplicação.
- **AUTH_PORT**: Esta definição mostra qual deve ser a porta que se deve conectar no servidor, como estamos utilizando uma camada de TLS esta porta deve ser a 443.
- **AUTH_REQUEST_VERSION**: Esta definição mostra qual a requisição HTTP do arquivo contendo o número da nova versão que deverá ser baixada pela API.
- **AUTH_REQUEST_FIRMWARE**: Esta definição mostra qual a requisição HTTP do firmware da nova versão que deverá ser baixada pela API.
- **AUTH_REQUEST_HASH**: Esta definição mostra qual a requisição HTTP do arquivo contendo o hash da nova versão que deverá ser baixada pela API.
- **SSL_CA_PEM**: Esta definição mostra o certificado SSL utilizado na comunicação com o servidor.

Com essas definições corretamente configuradas pode-se utilizar facilmente a API de atualização OTA proposta neste trabalho ficando a cargo do desenvolvedor somente programar em sua aplicação o algoritmos que determina quando a função que inicia a atualização é chamada para que o processo de atualização OTA proposto neste trabalho se encarregue de fazer todo o processo de forma autónoma.

5 RESULTADOS

Este capítulo apresenta o que foi obtido como resultado deste trabalho e as experiências do autor durante o desenvolvimento do sistema de atualização de firmware over-the-air. Primeiro será apresentado os resultados mostrando como é um processo de atualização realizado com sucesso e em seguida discutido o uso e vantagens e desvantagens do sistema.

5.1 PROCESSO DE ATUALIZAÇÃO DE FIRMWARE

Aqui apresentaremos todo o processo de atualização feito para assim comprovar o funcionamento do sistema desenvolvido neste trabalho, com isso é abordado desde a inicialização do firmware que será substituído, a disponibilização de um novo firmware no servidor, a inicialização deste firmware na plataforma embarcada STM32F746G e sua mensagem de apresentação.

5.1.1 ESTADO INICIAL DO MICROCONTROLADOR

Inicialmente é gravado no microcontrolador o bootloader e depois o firmware 1, com isso temos a memória FLASH preenchida separadamente, visto que definimos areas diferentes para aplicação e bootloader no arquivo de linker, assim fica o estado inicial da memória do microcontrolador no inicio do teste.

Com o bootloader e firmware 1 gravados no hardware já é possível fazer a primeira inicialização do sistema, com a reinicialização do hardware o sistema inicializa o bootloader para poder dar sequencia de atualização ou pulo para a aplicação. A [Figura 16](#) mostra a configuração de memória flash do microcontrolador.



Figura 16 – As três mensagens exibidas para diferenciação dos *firmware*.
Fonte: Autoria própria.

5.1.2 INICIALIZAÇÃO DO BOOTLOADER

Após todos processos de inicialização o bootloader é executado, como o intuito é que ele seja pequeno e de forma que se adapte para todos os tipos de microcontroladores da família STM32, não existe nenhum tipo de sinalização durante seus processos, assim sua função principal que é fazer a troca de firmware e pulo para a aplicação é executada de forma que o usuário não é capaz de identificar.

Durante sua execução o bootloader checa a versão do firmware atual e o compara com a versão que está no cartão SD, caso a versão atual for menor ou não seja encontra a nova versão do firmware o bootloader inicializa o firmware que está na memória flash. Como neste caso de teste o cartão SD se encontra vazio, o bootloader assume que não há nenhuma atualização a ser efetuada, assim ele inicializa a sequência de pulo para a aplicação.

5.1.3 INICIALIZAÇÃO DO FIRMWARE 1

Com a inicialização a aplicação efetuada pelo bootloader, são executadas todas as inicializações de drivers, das bibliotecas utilizadas pelo firmware 1, e assim inicializado o sistema operacional FreeRTOS, e exibida via UART a mensagem de confirmação de montagem do driver do cartão SD e a mensagem de apresentação contendo a versão do software atual e o sua frase de identificação como pode ser observado na [Figura 17](#). A partir da impressão dessa frase o sistema operacional iniciará a tarefa OTA.



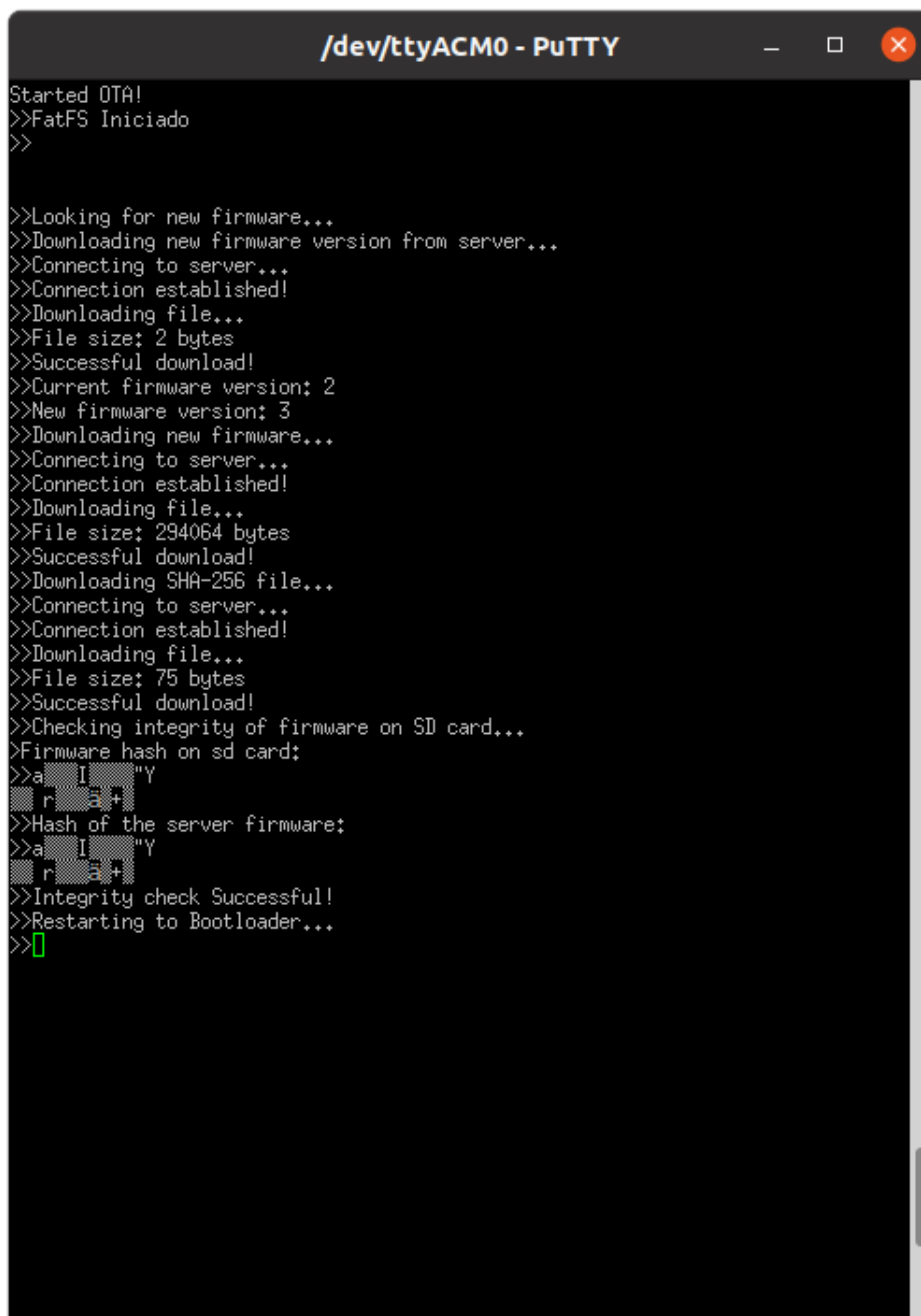
Figura 17 – As três mensagens exibidas para diferenciação dos *firmware*.

Fonte: Autoria própria.

5.1.4 OTA

Ao iniciar a função OTA será buscado no servidor o arquivo contendo a versão do firmware 2, com esse arquivo baixado ele fará a comparação com a versão atual do firmware e caso necessário irá fazer o download do novo firmware, e do arquivo contendo o hash deste firmware, tendo esses arquivos salvos no cartão SD ele irá fazer o hash do firmware baixado e verificar assim a integridade do arquivo baixado. Caso todos os processos ocorram com sucesso

ele irá fazer com que esses arquivos permaneçam no cartão SD e iniciará o processo de pulo para o bootloader, que encerra todos os driver e o sistema operacional e pula para a região do bootloader para o executar. Todo esse processo pode ser visto na [Figura 18](#).



```
/dev/ttyACM0 - PuTTY
Started OTA!
>>FatFS Iniciado
>>

>>Looking for new firmware...
>>Downloading new firmware version from server...
>>Connecting to server...
>>Connection established!
>>Downloading file...
>>File size: 2 bytes
>>Successful download!
>>Current firmware version: 2
>>New firmware version: 3
>>Downloading new firmware...
>>Connecting to server...
>>Connection established!
>>Downloading file...
>>File size: 294064 bytes
>>Successful download!
>>Downloading SHA-256 file...
>>Connecting to server...
>>Connection established!
>>Downloading file...
>>File size: 75 bytes
>>Successful download!
>>Checking integrity of firmware on SD card...
>>Firmware hash on sd card:
>>a I "Y
r A +
>>Hash of the server firmware:
>>a I "Y
r A +
>>Integrity check Successful!
>>Restarting to Bootloader...
>>
```

Figura 18 – Processo de atualização OTA.

Fonte: Autoria própria.

5.1.5 REINICIALIZAÇÃO DO SISTEMA PARA O BOOTLOADER

O bootloader é inicializado novamente, mas agora ele consegue achar um arquivo de versão escrito no cartão SD e com isso fazer a comparação com a versão de firmware e como a

versão encontrada no cartão SD é maior que a escrita na flash ele iniciará o processo de troca de firmware. Após a troca de firmware ele escreverá na última posição da memória a versão do novo firmware, fazendo com que atualização seja concluída com sucesso, assim podendo novamente fazer o processo de pulo para a aplicação.

5.1.6 INICIALIZAÇÃO DO FIRMWARE 2

Após o pulo para aplicação efetuada pelo bootloader após a atualização são executadas todas as inicializações de drivers, das bibliotecas utilizadas pelo firmware 2, e assim inicializado o sistema operacional, exibida a mensagem de confirmação de montagem do driver do cartão SD e a mensagem de apresentação contendo a versão do software atual e o sua nova frase de identificação como pode ser observado na [Figura 19](#). Assim concluindo com sucesso um processo de atualização de firmware.



Figura 19 – As três mensagens exibidas para diferenciação dos *firmware*.
Fonte: Autoria própria.

5.2 DISCUSSÃO

Os resultados obtidos mostraram que o sistema de atualização de firmware Over-The-Air proposto neste trabalho funciona, e que todo o processo desde a verificação de uma aplicação íntegra feita pelo bootloader, seu processo de atualização e as verificações, obtenções e verificações de arquivos da API de atualização OTA ocorrem com sucesso.

Como o bootloader ocupa XX Kbytes de espaço na memória FLASH ele pode ser utilizado por diversas placas da família de microcontroladores STM32 que possuam um setor da memória maior que esse espaço. Com a aplicação que foi utilizada para testar este trabalho que possui em seu código somente a API de atualização, as bibliotecas que são necessárias para este trabalho e o sistema operacional FreeRTOS ocupam juntos cerca de 294 Kbytes, a aplicação do usuário ainda teria um espaço de 674 Kbytes restante na plataforma que utilizamos para teste se contarmos junto o espaço reservado para o bootloader. Esta aplicação ainda não precisaria incluir novamente as bibliotecas FATFS, MBED TLS, LWIP e o sistema operacional FreeRTOS.

Com essa informação sobre o tamanho dos arquivos, é possível notar que este sistema de atualização não é tão portátil quanto se esperava no início deste trabalho, visto que só para ter um sistema de atualização funcional precisamos que o hardware em que se deseja ter esse sistema tenha ao menos 512 Kbytes de memória FLASH, diminuindo muito a quantidade de microcontroladores que poderiam utilizar este sistema.

Ainda assim é possível afirmar que o sistema cumpre com o objetivo geral e específicos propostos, visto que o sistema é capaz de efetuar a atualização da plataforma embarcada STM32F746NGH6 da forma proposta e ainda é capaz de identificar quando houve falhas em seu sistema de atualização e se recuperar de forma autónoma dessas falhas.

6 CONCLUSÃO

O trabalho conseguiu alcançar o objetivo específico de criar um sistema de atualização de firmware Over-The-Air utilizando as bibliotecas FatFs, MBED TLS e LWIP. Todos os objetivos específicos também foram atingidos visto que foi desenvolvido um bootloader que utiliza o sistema de arquivo FAT, foi implementada uma API que faz a comunicação com o servidor e armazena arquivos no cartão SD e assim foi comprovado o funcionamento do sistema na plataforma embarcada STM32F746NGH6-DISCOVERY.

Concluindo o trabalho foi possível observar que o bootloader desenvolvido é muito mais portátil que inicialmente se planejava. Como o processo de troca de firmware foi desenvolvido utilizando o HAL da STM foi possível fazer com que o bootloader funcione para toda a linha de microcontroladores da família STM32 que possuam a biblioteca FatFS e acesso a um cartão SD. Além de ser um bootloader robusto que consegue se recuperar em caso de falhas como quedas de energia durante o processo de troca de firmware.

A API que faz a busca dos arquivos no servidor HTTP e os armazena no cartão SD se mostrou perfeitamente funcional, conseguindo fazer a comparação de versões e a verificação de integridade do firmware baixado a partir de um hash baixado, deixando o sistema muito mais seguro contra falhas, além de conseguir fazer com que todo o sistema seja des-inicializado para fazer com que o bootloader seja executado em sua sequência.

A implementação do sistema de atualização implementado na plataforma embarcada STM32F746NGH6 se mostrou efetuada com sucesso, conseguindo mostrar como diferentes firmwares puderam ser trocados de forma rápida, eficiente e dando ao usuário sinalizações que mostravam cada etapa do sistema.

Um dos revezes deste trabalho foi o fato que o sistema de atualização ocupa um espaço considerável na memória flash dos microcontroladores, fazendo com que o sistema não funcione em hardwares com pouca memória, assim diminuindo a usabilidade do sistema, mas ainda é um ferramenta muito útil e poderosa para sistemas mais robustos. Fazendo que se abra a possibilidade de trabalhos futuros que possam melhorar ainda mais o sistema criado.

6.1 TRABALHOS FUTUROS

Com o intuito de se tornar ainda mais robusto e ocupar uma quantidade de memória menor, este capítulo aborda algumas propostas de melhoria do sistema que podem ser feitas em trabalhos futuros. Essa proposta faz com que o sistema seja mais atrativo para ser utilizado em sistemas com uma quantidade menor de memória.

Uma proposta consiste em utilizar todas as ferramentas já utilizadas no bootloader no próprio firmware em ser atualizado. O firmware pode a partir de ponteiros de função utilizar as funções presentes na biblioteca do FatFS e do HAL que já estão implementadas no bootloader

em sua aplicação, não sendo necessário reimplementa-las no firmware da aplicação, tornando o tamanho final do seu firmware da aplicação menor, assim fazendo com que placas de menor memória possam utilizar o sistema.

Pode-se utilizar outros meios de comunicação para a obtenção do novo firmware, fazendo com que não exista a necessidade de se utilizar toda a comunicação com o servidor e assim diminuindo a quantidade de memória ocupada pelo sistema. Uma implementação possível pode ser o uso de UART para a obtenção do firmware, onde o firmware é dividido em diversos pacotes e esses são enviados aos poucos para o hardware e podem ser conferidos CRCs no final de cada pacote para se obter uma prova de que o firmware obtido é íntegro.

Referências

- BALL, S. **Embedded Microprocessor Systems: Real World Design**. 3rd. ed. Newton, MA, USA: Butterworth-Heinemann, 2002. ISBN 0750675349. Citado na página 2.
- CHAN. **FatFs - Generic FAT File System Module**. 2016. Disponível em: <http://elm-chan.org/fsw/ff/00index_e.html>. Acesso em: 06 de setembro de 2019. Citado 4 vezes nas páginas , 2, 19 e 21.
- Chandra, H. et al. Internet of things: Over-the-air (ota) firmware update in lightweight mesh network protocol for smart urban development. In: **2016 22nd Asia-Pacific Conference on Communications (APCC)**. [S.l.: s.n.], 2016. p. 115–118. Citado na página 22.
- DAVIS, T.; DURLIN, D. **Bootloaders 101: making your embedded design future proof**. 2013. Disponível em: <<https://www.embedded.com/design/prototyping-and-development/4410233/Bootloaders-101--making-your-embedded-design-future-proof>>. Acesso em: 06 de setembro de 2019. Citado 4 vezes nas páginas , 2, 9 e 10.
- DEVINE, C. **SSL Library mbed TLS / PolarSSL**. 2006. Disponível em: <<https://tls.mbed.org>>. Acesso em: 06 de setembro de 2019. Citado 3 vezes nas páginas , 2 e 15.
- DIERKS, T.; RESCORLA, E. **The Transport Layer Security (TLS) Protocol, Version 1.2**. 2008. Disponível em: <<https://tools.ietf.org/html/rfc5246>>. Acesso em: 28 de novembro de 2019. Citado na página 16.
- DUNKELS, A. **lwIP - A Lightweight TCP/IP stack**. 2002. Disponível em: <<https://savannah.nongnu.org/projects/lwip/>>. Acesso em: 06 de setembro de 2019. Citado 2 vezes nas páginas 2 e 13.
- ECLIPSE FOUNDATION. **Eclipse Foundation, Inc.** 2001. Disponível em: <<https://www.eclipse.org/>>. Acesso em: 28 de novembro de 2019. Citado na página 28.
- GARTNER, INC. **Leading the IoT, Gartner Insights on How to Lead in a Connected World**. 2019. Disponível em: <https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf>. Acesso em: 28 de novembro de 2019. Citado na página 2.
- KUROSE, J. F.; ROSS, K. W. **REDES DE COMPUTADORES E A INTERNET - Uma Abordagem Top-Down**. [S.l.]: Pearson Education, inc, 2010. Citado 3 vezes nas páginas 12, 14 e 16.
- MARWEDEL, P. **Embedded System Design**. Berlin, Heidelberg: Springer-Verlag, 2006. ISBN 1402076908. Citado na página 1.
- NOVIELLO, C. **Mastering STM32**. 2018. Disponível em: <<https://leanpub.com/mastering-stm32>>. Acesso em: 06 de setembro de 2019. Citado na página 11.
- NSA. **National Security Agency**. 1952. Disponível em: <<https://www.nsa.gov/>>. Acesso em: 28 de novembro de 2019. Citado na página 16.
- Odat, H. A.; Ganesan, S. Firmware over the air for automotive, fotomotive. In: **IEEE International Conference on Electro/Information Technology**. [S.l.: s.n.], 2014. p. 130–139. Citado na página 21.

QING, Y. C. L. **Real-time concepts for embedded systems**. [S.l.]: CRC Press, 2003. Citado 6 vezes nas páginas , 4, 5, 6, 8 e 9.

SALUTES, B. **Bootloader: o que é e para que serve?** 2018. Disponível em: <(https://www.androidpit.com.br/bootloader-o-que-e-para-que-serve)>. Acesso em: 06 de setembro de 2019. Citado na página 2.

SD CARD ASSOCIATION. **SD Card**. 2016. Disponível em: <(https://www.sdcard.org/)>. Acesso em: 28 de novembro de 2019. Citado 2 vezes nas páginas 17 e 19.

STMICROELECTRONICS. **Discovery kit with STM32F746NG MCU**. 2019. Disponível em: <(https://www.st.com/en/evaluation-tools/32f746gdiscovery.html)>. Acesso em: 15 de novembro de 2019. Citado 4 vezes nas páginas , 11, 29 e 31.

STMICROELECTRONICS. **Description of STM32F7 HAL and low-layer drivers**. 2021. Disponível em: <(https://www.st.com/resource/en/user_manual/dm00189702-description-of-stm32f7-hal-and-lowlayer-drivers-stmicroelectronics.pdf)>. Acesso em: 15 de junho de 2021. Citado 2 vezes nas páginas 20 e 21.

TANENBAUM, A. S. **Computer Networks**. [S.l.]: Pearson Education, inc, 2003. Citado 4 vezes nas páginas , 12, 13 e 14.

TANENBAUM, A. S. **OPERATING SYSTEMS DESIGN AND IMPLEMENTATION**. [S.l.]: Pearson Education, inc, 2007. Citado 3 vezes nas páginas , 17 e 18.

Teng, C. et al. Firmware over the air for home cybersecurity in the internet of things. In: **2017 19th Asia-Pacific Network Operations and Management Symposium (APNOMS)**. [S.l.: s.n.], 2017. p. 123–128. Citado na página 22.

Apêndices

APÊNDICE A – Nome do apêndice

Lembre-se que a diferença entre apêndice e anexo diz respeito à autoria do texto e/ou material ali colocado.

Caso o material ou texto suplementar ou complementar seja de sua autoria, então ele deverá ser colocado como um apêndice. Porém, caso a autoria seja de terceiros, então o material ou texto deverá ser colocado como anexo.

Caso seja conveniente, podem ser criados outros apêndices para o seu trabalho acadêmico. Basta recortar e colar este trecho neste mesmo documento. Lembre-se de alterar o "label" do apêndice.

Não é aconselhável colocar tudo que é complementar em um único apêndice. Organize os apêndices de modo que, em cada um deles, haja um único tipo de conteúdo. Isso facilita a leitura e compreensão para o leitor do trabalho.

APÊNDICE B – Nome do outro apêndice

conteúdo do novo apêndice

Anexos

ANEXO A – Nome do anexo

Lembre-se que a diferença entre apêndice e anexo diz respeito à autoria do texto e/ou material ali colocado.

Caso o material ou texto suplementar ou complementar seja de sua autoria, então ele deverá ser colocado como um apêndice. Porém, caso a autoria seja de terceiros, então o material ou texto deverá ser colocado como anexo.

Caso seja conveniente, podem ser criados outros anexos para o seu trabalho acadêmico. Basta recortar e colar este trecho neste mesmo documento. Lembre-se de alterar o "label" do anexo.

Organize seus anexos de modo a que, em cada um deles, haja um único tipo de conteúdo. Isso facilita a leitura e compreensão para o leitor do trabalho. É para ele que você escreve.

ANEXO B – Nome do outro anexo

conteúdo do outro anexo