%%

%% Capítulo 3: O microcontrolador e o módulo sonar

%%

\mychapter{ O microcontrolador e o módulo sonar}

\label{Cap:picsonar}

\section{O microcontrolador PIC16F628A}

Pode-se dizer que um microcontrolador é um componente eletrônico dotado de uma inteligência programável, utilizado no controle de processos lógicos \cite{pic}.

O controle de processos é o controle de periféricos, tais como LEDs, botões e, no caso deste trabalho, sensores. São chamados de controles lógicos, pois a operação do sistema baseia-se nas ações lógicas que demandam de execução de acordo com o estado das entradas e saídas.

O microcontrolador é programável, pois toda a lógica de operação é estruturada na forma de um programa e gravada dentro do componente. Após o programa ter sido gravado, toda vez que o microcontrolador for alimentado, o programa interno será executado.

\subsection{O PIC16F628A}

Para este projeto foi utilizado o PIC16F628A por ser um microcontrolador versátil, compacto e poderoso. Algumas características desse PIC são:

\begin{itemize}

\item Microcontrolador de 18 pinos, que facilita a montagem de hardwares experimentais;

\item Possui até 16 portas configuráveis como entrada ou saída e dois osciladores internos (4 MHz e 37 kHz);

\item 10 interrupções disponíveis (Timers, Externa, Mudança de Estado, EEPROM, USART, CCP e comparador);

\item Memória de programação FLASH com 2.048 palavras, que permite a gravação do programa diversas vezes no mesmo chip, sem a necessidade de apaga-lo por meio de luz ultravioleta, como acontece nos microcontroladores de janela;

\item Memória EEPROM (não-volátil) interna com 128 bytes;

\item Recursos adicionais avançados: módulo CCP, Comparador interno e USART;

\item Programação com 14 bits e 35 instruções

\end{itemize}

\subsubsection{Nomenclaturas utilizadas}

\begin{figure}[htbp!]

\begin{center}

\fbox{\includegraphics[width=0.5\linewidth]

{figuras/PIC16F628A}}

\caption{Pinagem do PIC16F628A}

\label{Fig:pic16f628a}

\end{center}

\end{figure}

O PIC16F628A possui um total de 16 I/O separados em dois grupos cuja a denominação atende pelo nome de PORTA e PORTB.

O PORTA possui oito pinos que podem ser configurados como entrada ou saída, e seus nomes são definidos como RA0, RA1, RA2, RA3, RA4, RA5, RA6 e RA7. Alguns pinos tem dupla função e para utilizar uma determinada função é necessário abdicar de outra, por exemplo para se utilizar o pino RA5, perdemos o MCLR externo.

O PORTB também possui oito pinos configuráveis como entrada ou saída, indo de RB0 a RB7. O RB0 pode ser utilizado também para gerar interrupção externa.

Para que o microcontrolador possa funcionar, é necessário que o mesmo seja alimentado nos pinos 5 (Vss/GND) e 14 (Vdd/+5Vcc). A tensão nominal para alimentação é de 5Vcc, mas o ranger de variação desta tensão depende do modelo utilizado. No caso do PIC16F628A, ela vai de 2.0 a 5.5Vcc.

Um pino denominado MCLR (barrado) se refere ao Master Clear externo. Para que o PIC funcione, este pino tem que se encontrar em nível lógico baixo (GND). Caso contrário o programa será resetado.

\subsubsection{Opções do PIC}

Foi criada e é mantida pela IEEE (Institute of Electrical and Electronics Engineers). Instituição que tem como finalidade definir padrões para desenvolvimento tecnológico.

O 802.15.4 é, portanto, um protocolo de pacote de dados para rede sem fio. Utiliza como canal de acesso ao meio o protocolo CSMA-CA (Carrier Sense Multiple Access - Collision Avoidance), que é o mesmo utilizado pelo padrão 802.11 (Wi-Fi) e visa a detecção e abstenção de colisão de pacotes. Além do CSMA-CA o 802.15.4 ainda possui time slotting opcional, reconhecimento de mensagem e uma estrutura sinalizadora, chamada \textit{beacon}. A segurança é feita em multicamadas e será abordada mais adiante neste documento.\cite{siteZig}

%Inserir imagem da camada MAC para o padrão 802.15.4

\begin{figure}[htbp!]

\begin{center}

\fbox{\includegraphics[width=0.5\linewidth]

{figuras/padrao802154}}

\caption{Localização do padrão no modelo OSI}

\label{Fig:padrao802154}

\end{center}

\end{figure}

\subsection{Entendendo o padrão 802.15.4}

Como já foi dito anteriormente este protocolo reside no segundo nível do modelo OSI. Esta camada é denominada de Data Link. Aqui os bits contendo as unidades de informação digital são manuseados e organizados de forma se tornarem impulsos eletromagnéticos para a camada física logo abaixo. Esta camada é similar às demais de outros padrões como o 802.11, mais conhecido como Wifi ou o 802.3 (Ethernet). As frequências definidas no padrão são espalhadas através de 27 canais diferentes divididas em três bandas principais: \cite{8vszigbee}

\begin{itemize}

\item Europa - 868.0 à 868.6 MHz (1 canal)

\item EEUU - 902.0 à 928.0 MHz (10 canais)

\item Resto do mundo - 2.40 à 2.48 GHz (16 canais)

\end{itemize}

As taxas de dados são respectivamente:

\begin{itemize}

\item 868.0 à 868.6 MHz - 20/100/250 Kb/s

\item 902.0 à 928.0 MHz - 40/250 Kb/s

\item 2.40 à 2.48 GHz - 250 Kb/s

\end{itemize}

\subsubsection{Por que o 802.15.4 é bom contra ruído?}

O 802.15.4 utiliza DSSS (Direct Sequence Spread Spectrum) que é a sequência direta de espalhamento do espectro. É uma técnica de modulação do espectro de propagação. Utilizada extensamente em aplicações militares, fornece uma densidade espectral da potência muito baixa espalhando a potência do sinal sobre uma faixa de frequência muito larga. Consequentemente este tipo de modulação requer uma largura de faixa muito grande para transmitir diversos Mbits/s.

O 802.15.4 utiliza a DSSS para modular a informação antes dela ser enviada para a camada física. Basicamente, cada bit de informação a ser transmitido é modulado em 4(quatro) diferentes canais. A característica dessa modulação traz como consequência menos interferência nas frequências de banda utilizadas e geram uma melhoria no SNR (Signal to Noise Ratio) no receptor devido ao fato de que é mais fácil detectar e decodificar a mensagem que esta sendo enviada pelo transmissor.

Existem diferentes modulações DSSS dependendo do tipo das limitações físicas do hardware do circuito e o número de símbolos que podem ser processados em um determinado tempo.

%inserir imagem dsss.jpg

\begin{figure}[htbp!]

\begin{center}

\fbox{\includegraphics[width=0.5\linewidth]

{figuras/dsss}}

\caption{Exemplo de modulação de uma onda utilizando a técnica DSSS}

\label{Fig:dsss}

\end{center}

\end{figure}

\subsubsection{Por que o 802.15.4 é bom contra interferências?}

O padrão 802.15.4 utiliza duas técnicas para evitar que os pacotes comecem a ser transmitidos ao mesmo tempo. São elas o CSMA-CA e o GTS.

A mais comum é o CSMA-CA (Carrier Sense Multiple Access - Collision Avoidance). Nesse método, cada nó da rede escuta o meio para poder transmitir caso meio esteja ocioso ou, nesse caso, em baixa energia. Se a energia encontrada é maior em um nível específico, o nó espera durante um tempo randômico e tenta novamente. Existe um parâmetro definido no padrão chamado de \textit{macMinBE} que configura o expoente de \textit{back-off} utilizado para calcular esse time-slot, que é o tempo de espera.

A segunda técnica, GTS (Guarantee Time Slot) utiliza um nó de rede centralizado denominado de coordenador PAN (Personal Area Network) que gera slot de tempo para cada nó para que assim eles saibam quando têm de transmitir. Existem 16 possíveis slots de tempo. Em um primeiro passo um nó deve enviar ao coordenador PAN uma mensagem de requisição GTS, como resposta o coordenador irá enviar uma mensagem de \textit{beacon} contendo o slot alocado e o número de slots cadastrados.

Uma das funcionalidades implementadas no padrão 802.15.4 é o escaneamento de energia do canal (PLME-ED request). A ideia é permitir que se soubesse o quanto de energia (atividade/ruído/interferências) existe em um ou mais canais em detrimento de utilizá-los. Desta forma pode-se economizar energia ao se escolher canais livres quando se configura a rede. Existem três diferentes comportamentos quando se lida com problemas de detecção de energia:

\begin{itemize}

\item \textbf{Energia:} escaneia o canal e reporta a energia encontrada. Não interessa se é causada por outro nó ZigBee, outra tecnologia ou ruído. Apenas irá reportar se o espectro está sendo utilizado. Somente quando o valor recebido se encontrar abaixo de certo parâmetro de threshold, poderá ser realizada a transmissão.

\item \textbf{Carrier Sense (CCA):} escaneia o meio e reporta se existem transmissões no padrão 802.15.4. Somente quando o canal estiver livre a transmissão será realizada.

\item \textbf{CCA + Energia:} escaneia o meio e reporta se existem transmissões no padrão 802.15.4 acima do parâmetro de threshold especificado para então poder transmitir.

\end{itemize}

\subsubsection{Protocolo de baixo consumo}

O protocolo de baixo consumo tem por base o fato de o transceptor poder se encontrar em estado de hibernação (sleep) na maioria do tempo (99\% em média) enquanto que as tarefas de recebimento e envio podem ser configuradas para tomar apenas uma pequena parte da energia do dispositivo. Essa porcentagem depende o tipo de modelo de comunicação utilizado. Se o modo \textit{beacon} é utilizado (redes estrela ou PAN) o montante mínimo de tempo utilizado para transmitir/receber estes frames irá aumentar o tempo total com o qual o transceptor é utilizado.

\subsubsection{Dispositivos da rede}

O padrão 802.15.4 define dois tipos de dispositivos de rede. A primeira é denominada \textbf{Dispositivos de Função Completa (FFD)}. São dispositivos mais complexos e precisam de um hardware mais potente para a implantação da pilha de protocolos, consequentemente, consomem mais energia. Podem funcionar tanto como coordenador de uma rede quanto como um nó comum seja ele roteador ou end device. São implementados em microcontroladores com no mínimo 32KB de memória de programa e necessitam ter uma certa quantidade de memória RAM, para implementações de tabelas de rotas e configurações de parâmetros.

Por outro lado, existem os \textbf{Dispositivos de Função Reduzida (RFD)} que são dispositivos mais simples, onde sua pilha de protocolo pode ser implementada usando os mínimos recursos possíveis de hardware, como por exemplo, em microcontroladores de 8 bits com memória de programa próxima a 6KB, mas só podem se comunicar com dispositivos FFDs (Coordenador ou Roteador). Numa topologia de rede 802.15.4 eles assumem o papel de End Device (dispositivo final). Na prática podem ser: interruptores de iluminação, dimmers, controle de relês, sensores, entre outros.

\subsubsection{Arquitetura de trasporte de dados}

As unidades básicas de transporte de dados são denominadas frames, dos quais existem quatro tipos fundamentais: frames de dados, frames de reconhecimento, frames de \textit{beacon} e frames de comando MAC. Estes tipos de frames proveem um meio termo racional entre simplicidade e robustez. Além do mais, uma estrutura denominada superframe, definida pelo coordenador, pode ser utilizada. Um superframe consiste de 16 slots de mesmo tamanho, que podem ser divididos futuramente em uma parte ativa e uma parte inativa onde o coordenador pode entrar em estado de economia de energia, sem necessidade de controlar sua rede.

\begin{figure}[htbp!]

\begin{center}

\fbox{\includegraphics[width=0.5\linewidth]

{figuras/dataframe}}

\caption{Estrutura do dataframe}

\label{Fig:dataframe}

\end{center}

\end{figure}

A estrutura do Data Frame pode ser vista na figura (\ref{Fig:dataframe}). Esta estrutura é uma das mais básicas e importantes do padrão 802.15.4. Tem capacidade de transferir até 104 bytes por pacote, o que já é o suficiente, se tratando de transferência de informações entre sensores. Para garantir a confiabilidade da entrega dos dados contém um campo com uma numeração sequencial dos dados e um campo de Frame Check Sequence (FCS).

\begin{figure}[htbp!]

\begin{center}

\fbox{\includegraphics[width=0.5\linewidth]

{figuras/ackframe}}

\caption{Estrutura do ACK Frame}

\label{Fig:ackframe}

\end{center}

\end{figure}

No ACK Frame visto na figura \ref{Fig:ackframe}, é enviado um retorno (ACK) eficaz do receptor para o emissor informando que o pacote foi recebido sem erros.

\begin{figure}[htbp!]

\begin{center}

\fbox{\includegraphics[width=0.5\linewidth]

{figuras/maccommandframe}}

\caption{Estrutura do frame de comando MAC}

\label{Fig:maccommandframe}

\end{center}

\end{figure}

A figura \ref{Fig:maccommandframe} mostra o frame que representa um mecanismo para controle e configuração remota de nós da rede, permitindo que uma rede centralizada configure clientes individualmente sem importar o quanto a rede é extensa.

\begin{figure}[htbp!]

\begin{center}

\fbox{\includegraphics[width=0.5\linewidth]

{figuras/beaconframe}}

\caption{Estrutura do frame para o Beacon}

\label{Fig:beaconframe}

\end{center}

\end{figure}

Na figura \ref{Fig:beaconframe} vemos uma estrutura opcional de sinalização. Os dispositivos podem \textit{acordar} somente quando este sinal é transmitido, caso contrário, retornam a \textit{adormecer}. É usado nas topologias de malha e estrela estendida para manter os nós sincronizados sem a necessidade deles consumirem energia por longos períodos de tempo.

\begin{figure}[htbp!]

\begin{center}

\fbox{\includegraphics[width=0.5\linewidth]

{figuras/superframe}}

\caption{Estrutura do superframe}

\label{Fig:superframe}

\end{center}

\end{figure}

A estrutura de frame vista na figura \ref{Fig:superframe} é uma estrutura opcional da camada MAC, ela é definida pelo nó coordenador, utiliza beacons para sinalização, slotting time e Guarantee Time Slotting (GTS) para permitir que um nó continue utilizando o meio de acesso caso esteja mandando uma mensagem com alta prioridade.

A contenção de superframes ocorre entre seus limites, e é resolvida pelo CSMA-CA. Cada transmissão deve terminar antes da chegada do segundo \textit{beacon}. Como mencionado anteriormente, aplicações com largura de banda bem definidas necessitam utilizar acima de sete domínios de um ou mais GTS (Guaranteed Time Slots) à direita no final do superframe. A primeira parte do superframe deve ser suficiente para dar serviço para a estrutura de rede e seus dispositivos. Superframes são tipicamente utilizados no contexto de dispositivos de baixa latência, os quais as associações devem ser mantidas mesmo em um período de tempo inativo ou de longa duração.

Transferência de dados para o coordenador requerem um sincronização de fase de \textit{beacons}, se aplicável, seguida de uma transmissão CSMA-CA. O reconhecimento (acknowledgment) é opcional. Transferência de dados vindas do coordenador usualmente seguem as requisições do dispositivo: Se os \textit{beacons} estão em uso, eles são utilizados para requisições de sinal; o coordenador reconhece a requisição e então envia os dados em pacotes que são reconhecidos pelo dispositivo. O mesmo é feito quando os superframes não estão em uso, somente neste caso não existem beacons para acompanhar as mensagens pendentes.

Redes ponto-a-ponto podem tanto utilizar o CSMA-CA sem slots ou mecanismos de sincronização; neste caso, a comunicação entre quaisquer dois dispositivos é possível, considerando que um dos dispositivos deve ser o coordenador da rede.

Em geral, todos os procedimentos implementados seguem uma arquitetura típica de classificação \textit{requisição-confirmação/indicação-resposta}

\section{O protocolo ZigBee}

O ZigBee nada mais é do que um dos muitos protocolos que utilizam o padrão 802.15.4 em sua camada MAC. É com certeza o mais conhecido dos protocolos utilizados acima da camada física que utiliza o IEEE 802.15.4. A seguir buscaremos entender o funcionamento deste protocolo e suas implementações de segurança.

\subsection{Entendendo o ZigBee}

O ZigBee basicamente oferece quatro tipos diferentes de serviços:

\begin{itemize}

\item \textbf{Serviço de encriptação extra:} chaves de rede e aplicação implementam 128b estre de encriptação AES;

\item \textbf{Associação e autenticação:} somente nós validados podem ingressar na rede;

\item \textbf{Protocolo de roteamento:} \textit{AODV}, um protocolo ad hoc reativo, tem sido implementado para realizar o roteamento de dados

e processo de encaminhamento para qualquer nó na rede

\item \textbf{Serviços de aplicações:} um termo abstrato denominado \textbf{"cluster"} é introduzido. Cada nó pertence a um cluster

pré-definido e pode obter um pré-definido número de ações. Por exemplo: o \textit{cluster do sistema de luz da casa} pode realizar duas

ações; ligar a luz e desligar a luz.

\end{itemize}

O ZigBee é uma camada pensada para organizar a rede. A primeira coisa que um nó, seja ele roteador ou dispositivo final, que deseje ingressar na rede deve fazer é perguntar ao coordenador por um endereço de rede (\textbf{16 bits}), como parte do processo de associação. Toda a informação na rede é roteada utilizando esse endereço e não o endereço de 64 bits da camada MAC. Neste passo, processos de autenticação e encriptação são realizados.

Uma vez que um nó tenha ingressado na rede, ele pode enviar informações para os seus "irmãos" através dos roteadores, os quais estão sempre acordados à espera de pacotes. Quando o roteador recebe o pacote e o destino esta no seu sinal de rádio, o roteador da uma primeira olhada e verifica se o destino final está acordado ou dormindo. Se estiver acordado, o roteador envia o pacote para o destino final, entretanto, em caso contrário, o roteador irá “bufferizar” o pacote até que o dispositivo final acorde e pergunte por um novo roteador.

\subsection{Como trabalha uma rede ZigBee}

No protocolo ZigBee existem três classes de dispositivos lógicos (Coordenador, Roteador e Dispositivo final) que definem a rede:

\begin{itemize}

\item \textbf{Coordenador:} Só pode ser implementado através de um dispositivo FFD. O coordenador é responsável pela inicialização, distribuição de endereços, manutenção da rede, reconhecimento de todos os nós, entre outras funções podendo servir como ponte entre várias outras redes que utilizem o mesmo padrão.

\item \textbf{Roteador:} Só pode ser implementado através de um dispositivo FFD. Tem as características de um nó normal na rede, mas com poderes extras de também exercer a função de roteador intermediário entre nós, sem precisar do coordenador. Por intermédio de um roteador uma rede 802.15.4 pode ser expandida, e assim ter mais alcance. Na prática um roteador pode ser usado para amplificar o sinal da rede entre andares de um prédio.

\item \textbf{Dispositivo Final (End Device):} É onde os atuadores ou sensores serão hospedados. Pode ser implementado através de um dos dispositivos FFD ou RFD. Assim ele é o nó que consome menos energia, pois na maioria das vezes ele fica em modo de hibernação (Sleep).

\end{itemize}

A redes podem ser construídas em topologias tanto ponto-a-ponto quanto estrela. Entretanto, toda rede necessita de ao menos um dispositivo FFD para funcionar como coordenador da rede. Essas redes são, portanto, formadas por grupos de dispositivos separados por uma determinada distância. Cada dispositivo tem um identificador único de 64 bits.\cite{siteZig}

Redes ponto-a-ponto podem formar padrões arbitrários de conexões entre dispositivos, e suas extensões são limitadas apenas pela distância entre cada par de nós. Foram destinados para servir de base para redes ad hoc capazes de realizar autogestão e organização. Uma vez que o padrão não defina uma camada de rede, o roteamento não é diretamente suportado, mas uma camada adicional pode adicionar suporte para uma comunicação \textit{multihop}. Algumas restrições topológicas podem ser adicionadas adiante; o padrão menciona \textit{cluster free} como uma estrutura que pode explorar o fato de que um dispositivo RFD pode apenas se associar com um dispositivo FFD por vez para formar uma rede onde os dispositivos RFDs são exclusivamente as folhas de uma árvore na topologia e a maioria dos nós são FFD. A estrutura também pode ser estendida como uma rede \textit{mesh} genérica onde o nós são aglomerados em árvore da rede com um coordenador local para cada aglomeração, em adição ao coordenador global.

Um padrão mais estruturado seria a topologia em formato estrela, onde o coordenador da rede irá necessariamente ser o nó central. Tal rede pode ser originada quando um dispositivo FFD decide criar o seu próprio PAN e se declara coordenador, após escolher um único identificador PAN. Após isso, outros dispositivos podem se juntar a rede, os quais serão totalmente independentes de todas as outras redes estrela. De forma a simplificar o que já foi escrito, uma rede no padrão 802.15.4 aceita basicamente as seguintes topologias:

\begin{figure}[htbp!]

\begin{center}

\fbox{\includegraphics[width=0.5\linewidth]

{figuras/TopologiaZigBee}}

\caption{Topologias do protocolo ZigBee}

\label{Fig:topologiazigbee}

\end{center}

\end{figure}

\begin{itemize}

\item \textbf{Malha ou Ponto-a-Ponto:} Na topologia em Malha a rede pode se ajustar automaticamente, tanto na sua inicialização como na entrada ou saídas de dispositivos na Rede. A Rede se organiza para otimizar o trafego de dados. Com vários caminhos possíveis para a comunicação entre os nós, este tipo de rede pode abranger em extensão, uma longa área geográfica, podendo ser implementada numa fábrica com vários galpões distantes; controle de irrigação ou mesmo num prédio com vários andares.

\item \textbf{Árvore (Cluster Tree):} Semelhante à topologia de Malha, uma rede em árvore, tem uma hierarquia muito maior e o coordenador assume o papel de nó mestre para a troca de informação entre os nós roteadores e finais.

\item \textbf{Estrela:} É uma das topologias de rede mais simples de serem implantadas, é composta de um nó Coordenador, e quantos nós End Device forem precisos. Este tipo de rede deve ser instalada em locais com poucos obstáculos à transmissão e recepção dos sinais, como por exemplo, em uma sala sem muitas paredes ou locais abertos.

\end{itemize}

\subsection{ZigBee vs ZigBee Pro}

Em 2007, foi lançada uma nova versão do protocolo ZigBee denominada ZigBee Pro. A seguir serão estabelecidas as principais diferenças entre o protocolo ZigBee de 2006 e esse novo modelo.\cite{zigpro}

\begin{itemize}

\item \textbf{Endereçamento Estocástico:} Na primeira implementação do ZigBee, o endereço era escolhido pelo coordenador de acordo com a posição do nó na árvore de rede. Agora o endereço de 16 bits é escolhido de forma randômica. Se os nós escolherem o mesmo endereço, então o endereço é resolvido através do padrão da camada MAC de 64 bits do IEEE 802.15.4;

\item \textbf{Malha de gerenciamento de dados:} No ZigBee convencional, cada nó tinha que manter uma tabela de qualquer uma das rotas de e para o gateway para um dispositivo (se estivesse no caminho de rotas), agora o nós apenas salvam o caminho até chegarem no gateway (reduzindo o espaço de memória necessário). O gateway (um nó que suporta maiores recursos de memória RAM) guarda a rota (com todos os pulos) para algum nó. Quando o gateway tem que enviar um pacote para um nó específico, ele acrescenta a informação a respeito dos passos que tem que ser dados no mesmo pacote. Este procedimento é denominado /textbf{textit{muitos para um}}

\item \textbf{Fragmentação:} Pacotes de dados extensos podem ser facilmente fragmentados.

\item \textbf{Escolha dinâmica do melhor canal:} Os nós irão mudar de canal se o canal em que estão possuir interferências ou ruído seguindo um parâmetro de threshold.

\item \textbf{Conexões assimétricas:} Os links entre os nós nem sempre são simétricos e a qualidade da conexão é diferente de um nó A para um nó B do que de B para A, isto é devido a várias razões que incluem interferências entre canais e ruídos. Por esse motivo a versão PRO tenta levar isso em conta para construir as melhores rotas possíveis.

\item \textbf{Segurança:} Na versão de 2006, a implementação do ZigBee utilizava de 128 bits acima do AES e uma chave de rede global para criar comunicações seguras. A nova versão tem um sistema mais complexo que permite que cada par de nós tenha sua própria chave para que assim a encriptação p2p possa ser realizada. Uma camada peer-to-peer de link de encriptação é adicionada.

\end{itemize}

\subsection{802.15.4 vs ZigBee}

Resumidamente, neste ponto do texto, podemos estabelecer algumas comparações entre o padrão IEEE 802.15.4 e o padrão de protocolo ZigBee:

\begin{itemize}

\item 802.15.4 foi idealizado para ser um protocolo que estabelece comunicações ponto-a-ponto com eficiência de energia.

\item ZigBee define serviços extras (roteamento em topologia estrela, encriptação, serviços de aplicação) acima da camada 802.15.4.

\item ZigBee cria redes semi-centralizadas aonde apenas o dispositivo final pode ficar em estado de hibernação (sleep).

\item Diferentes algoritmos de malha completamente distribuídos estão sendo usados acima do 802.15.4 que é o protocolo usado para criá-los.

\end{itemize}

\section{Segurança no padrão IEEE 802.15.4 e protocolo ZigBee}

Como visto anteriormente neste texto, a camada MAC do padrão IEEE 802.15.4 implementa alguns recursos que são utilizados pelo protocolo ZigBee nas camadas de rede e aplicação. Um desses recursos são os serviços de segurança.

IEEE 802.15.4 define o algoritmo de encriptação para ser usado quando os dados forem cifrados para serem transmitidos, no entanto, o padrão não especifica como as chaves têm de ser gerenciadas ou que tipos de políticas de autenticação têm de ser aplicadas. Esses problemas são tratados nas camadas superiores que são gerenciadas por tecnologias tais como o ZigBee.\cite{segzigbee}

\subsection{Um visão geral da segurança no IEEE 802.15.4}

O algorítmo de encriptação utilizado é o \textbf{AES (Advanced Encryption Standard)} com uma chave de tamanho de 128 bits (16 bytes). É importante contar com um único tipo de método de encriptação devido ao fato de que a maioria dos transceptores 802.15.4/ZigBee têm um design específico de hardware para lidar com esse trabalho em nível eletrônico (dispositivos de baixo recursos embutidos).

\begin{figure}[htbp!]

\begin{center}

\fbox{\includegraphics[width=0.5\linewidth]

{figuras/mac802154\_0med}}

\caption{Quadro MAC do padrão IEEE 802.15.4}

\label{Fig:mac802154\_0med}

\end{center}

\end{figure}

O algoritmo AES não é somente utilizado para encriptar a informação, mas também para validar os dados que estão sendo enviados. Este conceito é denominado de Integridade de Dados e é alcançado utilizando um Código de Integridade de Mensagem, (em inglês MIC) que é adicionado à mensagem. Este código garante integridade no cabeçalho MAC e carga de dados anexada. É criado encriptando partes do frame MAC do IEEE utilizando a chave da rede, assim se for recebida uma mensagem de um nó não confiável, poderá ser analisado que o MIC gerado para a mensagem enviada não corresponde àquele que seria gerado utilizando a mensagem com a chave secreta corrente, e então a mensagem é descartada. O MIC ou MAC (Message Authenticantion Code) pode ter tamanhos distintos: 32, 64, 128 bits, entretanto é sempre criado utilizando o algoritmo AES de 128 bits. Seu tamanho é apenas a quantidade de bits que são anexadas a cada frame. Quanto maior, mais seguro (apesar da menor carga de dados que a mensagem pode ter). A segurança de dados é realizada pela encriptação do campo de carga dados (payload) com a chave de 128 bits.

\subsection{Insights de segurança do 802.15.4}

Existem três campos no frame MAC do padrão IEEE 802.15.4 que são relacionados com a segurança:

\begin{itemize}

\item \textbf{Frame control:} localizado no cabeçalho MAC

\item \textbf{Controle de segurança auxiliar:} localizado no cabeçalho MAC

\item \textbf{Carga(payload) de Dados:} localizada no campo de carga do MAC

\end{itemize}

O frame de \textbf{Controle de Segurança Auxiliar} é habilitado somente se o subcampo de \textbf{Segurança Habilitada} do \textbf{Frame de controle} estiver ligado. Este cabeçalho especial tem 3 campos:

\begin{itemize}

\item \textbf{Controle de Segurança (1B):} especifica que tipo de proteção é utilizada.

\item \textbf{Contador de Frame: (4B)} é um contador fornecido pela fonte do frame atual para proteger a mensagem contra repetição de proteção. Por esta razão cada mensagem tem um único ID de sequência representada por este campo.

\item \textbf{Identificador de chave (0-9B):} especifica a informação necessária para saber que chave nós estamos usando com o nó que estamos nos comunicando.

\end{itemize}

O controle de segurança é o local onde a nossa política de segurança global é configurada. Utilizando os dois primeiros bits (campos de nível de segurança) escolhe-se o que será encriptado e quão longa a chave será:

\begin{figure}[htbp!]

\begin{center}

\fbox{\includegraphics[width=0.5\linewidth]

{figuras/mac8021540med}}

\caption{Segurança na camada MAC do padrão IEEE 802.15.4}

\label{Fig:mac8021540med}

\end{center}

\end{figure}

\begin{table}[htb] % [htb]-> here, top, bottom

\centering % tabela centralizada

\footnotesize % tamanho da fonte

\setlength{\arrayrulewidth}{2\arrayrulewidth} % espessura da linha

\setlength{\belowcaptionskip}{4pt} % espaço entre caption e tabela

\caption{Tabela com as respectivas chaves para o tipo de encriptação de acordo com os bits do nível de segurança}

\begin{tabular}{|l|l|l|l|} % c=center, l=left, r=right

\hline

0x00 & Sem segurança & & Dados não encriptados, autenticidade dos dados não validada\\

\hline

0x01 & AES-CBC-MAC-32 & MIC-32 & Dados não encriptados, autenticidade dos dados validada\\

\hline

0x02 & AES-CBC-MAC-64 & MIC-64 & Dados não encriptados, autenticidade dos dados validada\\

\hline

0x03 & AES-CBC-MAC-128 & MIC-128 & Dados não encriptados, autenticidade dos dados validada\\

\hline

0x04 & AES-CTR & ENC & Dados encriptados, autenticidade dos dados não validada\\

\hline

0x05 & AES-CCM-32 & AES-CCM-32 & Dados encriptados, autenticidade dos dados validada\\

\hline

0x06 & AES-CCM-64 & AES-CCM-64 & Dados encriptados, autenticidade dos dados validada\\

\hline

0x07 & AES-CCM-128 & AES-CCM-128 & Dados encriptados, autenticidade dos dados validada\\

\hline

\end{tabular}

\label{tab:encriptacao}

\end{table}

O valor \textbf{0x00} configura a não encriptação, então nem os dados são encriptados (sem confidencialidade de dados) nem a autenticidade é validada. De \textbf{0x01} à \textbf{0x03} os dados são autenticados utilizando a mensagem de autenticação de código (MAC) encriptada. O valor \textbf{0x04} encripta a carga de dados, certificando a confidencialidade de dados. Os valores de \textbf{0x05} à \textbf{0x07} certificam que os dados tenham confidencialidade e autenticidade.

O subcampo do modo de identificação de chave configura o tipo (implícito ou explícito) que a chave deve ser utilizada pelo destinatário e o remetente. Possíveis valores são:

\begin{figure}[htbp!]

\begin{center}

\fbox{\includegraphics[width=0.5\linewidth]

{figuras/mac802154}}

\caption{Segurança na camada MAC do padrão IEEE 802.15.4}

\label{Fig:mac802154}

\end{center}

\end{figure}

\begin{itemize}

\item \textbf{0:} O ID da chave é implícita para o remetente e destinatário (não é especificada na mensagem).

\item \textbf{1:} O ID da chave é determinada explicitamente pelo index de chave de 1 Byte vindo do campo identificador de chave e do \textbf{macDefaultKeySource}.

\item \textbf{2:} O ID da chave é determinado explicitamente pelo index de chave de 1 Byte e os 4 Bytes da fonte de chave (Key Source).

\item \textbf{2:} O ID da chave é determinado explicitamente pelo index de chave de 1 Byte e os 8 Bytes da fonte de chave (Key Source).

\end{itemize}

Como mencionado anteriormente, o campo \textbf{identificador de chave} é configurado quando o subcampo de modo de identificador de chave é diferente de zero. O subcampo fonte da chave (key source) especifica quem originou o grupo de chave. O index da chave (Subcampo de controle de chave) ajuda a identificar chaves diferentes chaves de uma fonte de chave (key source) específica

O campo de carga de dados (payload data) pode ter três diferentes configurações dos campos de segurança previamente definidos:

\begin{itemize}

\item \textbf{AES-CTR:} Todos os dados são encriptados utilizando a chave definida de 128 bits e o algoritmo AES. O contador de frame configura uma única ID de mensagem, e o contador de chave (key counter) no subcampo de controle de chave é utilizado pela camada de aplicação se o valor máximo do frame counter é atingido.

\item \textbf{AES-CBC-MAC:} O \textbf{MAC} (Código de autenticidade de mensagem) é anexado ao final da carga de dados (data payload). Seu tamanho depende do nível de segurança especificado no campo de política de segurança (Security Policy). O MAC é criado encriptando informação do cabeçalho MAC do 802.15.4 e da carga de dados.

\item \textbf{AES-CCM:} É a mistura dos métodos definidos anteriormente. Os subcampos correspondem com o modo \textbf{AES-CTR} mais o subcampo extra do \textbf{AES-CBC-MAC} encriptado.

\end{itemize}

\subsection{A lista de controle de acesso}

Cada transceptor 802.15.4 tem q gerenciar uma lista de controle para os seus \textit{"irmãos confiáveis"} juntamente com a política de segurança. Por esta razão, cada nó tem que controlar sua própria \textbf{Lista de Controle de Acesso (ACL)} que guarda os seguintes campos:

\begin{itemize}

\item \textbf{Endereço (Address):} Endereço do nó que se deseja comunicar.

\item \textbf{Suite de segurança:} A política de segurança que está sendo utilizada (AEC-CTR, AES-CCM-64, AES-CCM-128,,...).

\item \textbf{Chave:} A chave de 128 bits utilizada no algoritmo AES.

\item \textbf{Último vetor inicial(IV) e contador de repetição:} Ambos estão no mesmo campo. O último IV é utilizado pela fonte e o contador de repetição pelo destino como ID de mensagem em função de se evitar ataques repetidos.

\end{itemize}

Quando um nó quer enviar uma mensagem para um nó específico ou recebe um pacote, ele irá procurar na \textbf{ACL} para verificar se o nó é um \textbf{irmão confiável} ou não. Se for, o nó utilizará o dado contido na coluna específica para aplicar as medidas de segurança. Caso o nó não esteja na lista ou sua mensagem é rejeitada ou um processo de autenticação se dará início.

\subsection{Segurança ZigBee}

O ZigBee implementa duas camadas extras de segurança acima do padrão 802.15.4: as camadas de segurança de \textbf{rede} e \textbf{aplicação}. Todas as políticas de segurança confiam na encriptação do algoritmo AES de 128 bits, assim a arquitetura de hardware previamente implementada para o nível de link (camada MAC) é ainda válida. Existem três tipos de chave: master, link e de rede.

\begin{itemize}

\item \textbf{Master Keys:} São pré-instaladas em cada nó. Sua função é manter confidencial a troca de \textbf{Chaves de Link} entre dois nós no \textbf{Processo de Estabelecimento de Chave (SKKE)}.

\item \textbf{Chaves de Link:} São únicas entre cada par de nós. Essas chaves são gerenciadas pelo nível de aplicação. São utilizadas para encriptar toda a informação entre cada dois dispositivos, por essa razão mais recursos de memória são necessários em cada dispositivo. Geralmente essa chave não costuma ser usada.

\item \textbf{Chaves de Rede:} É uma chave única de 128 bits compartilhada ao longo dos dispositivos na rede. É gerado por um centro de confiança e re-gerada em diferentes intervalos. Casa nó precisa pegar sua chave de rede para ingressar em uma rede. Uma vez que o centro de confiança decida mudar a chave de rede, a nova chave é espalhada na rede utilizando a antiga chave de rede. Uma vez que essa nova chave é atualizada em um dispositivo, seu contador de frame é inicializado em zero. Este centro de confiança é normalmente o coordenador da rede, entretanto, pode ser que seja um dispositivo dedicado. Ele tem apenas que autenticar e validar cada dispositivo que tenta entrar na rede.

\end{itemize}

Cada par de dispositivos podem ter configurados tanto as chaves de rede quanto as de link. Nesse caso a chave de link é sempre utilizada (mais segurança, mais memória é necessária). Existem dois tipos de política de segurança que o centro de confiança pode seguir:

\begin{itemize}

\item \textbf{Modo Comercial:} O centro de confiança compartilha as chaves \textbf{master} e de \textbf{link} com qualquer dispositivo na rede. Este modo requer alto recurso de memória. Oferece um modelo completo e centralizado para controle de segurança de chave.

\item \textbf{Modo Residencial:} O centro de confiança compartilha apenas a \textbf{chave de rede} (é o modo ideal quando dispositivos embarcados tem de lidar com esta tarefa devido aos baixo recursos que eles tem). Este é o modo normalmente escolhido para o modelo de redes de sensores sem fio.

\end{itemize}

\begin{figure}[htbp!]

\begin{center}

\fbox{\includegraphics[width=0.5\linewidth]

{figuras/modocomercial}}

\caption{Política de segurança do modo comercial}

\label{Fig:modocomercial}

\end{center}

\end{figure}

\begin{figure}[htbp!]

\begin{center}

\fbox{\includegraphics[width=0.5\linewidth]

{figuras/modoresidencial}}

\caption{Política de segurança do modo residencial}

\label{Fig:modoresidencial}

\end{center}

\end{figure}