Segurança no padrão IEEE 802.15.4 e ZigBee

Iuri Guerra

13 de dezembro de 2010

Sumário

Introdução

- Tecnologias wireless
  - Vantagens e desvantagens

Por que se preocupar com segurança?

- Crescimento no uso da tecnologia
- O meio de transmissão é o ar
- Maior quantidade de dados trafegando a cada dia
- Melhorias na tecnologia para lidar com essa quantidade dados
- Necessidade de garantir segurança e integridade para diversas possibilidades de aplicações

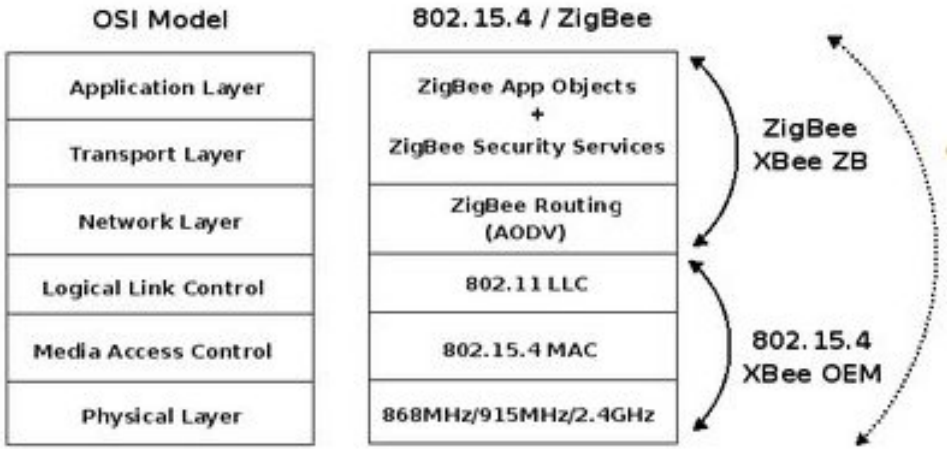
E agora, quem poderá nos defender?

Figura: IEEE 802.15.4 e Zigbee

O padrão IEEE 802.15.4

- Criada pela IEEE e liberada em maio de 2003
- Especifíca a camada física e a camada MAC (Media Access Control) para dispositivos que não precisem de alta taxa de dados e que necessitem de baixa latência e baixo custo de energia
- É, portanto, um protocolo de pacote de dados para rede sem fio

O padrão IEEE 802.15.4



Características

- Utiliza o CSMA-CA para acesso ao meio, o mesmo do WiFi
- Possui estrutura sinalizadora chamada Beacon
- Segurança multi-camada
- Utiliza superframes
- Reconhecimento de mensagem

Frequências e canais

27 canais distribuidos em 3 bandas

- Europa - 868.0 à 868.6 MHz (1 canal)
- EUUU - 902.0 à 928.0 MHz (10 canais)
- Resto do mundo - 2.40 à 2.48 GHz (16 canais)

Taxa de dados

- 868.0 à 868.6 MHz - 20/100/250 Kb/s
- 902.0 à 928.0 MHz - 40/250 Kb/s
- 2.40 à 2.48 GHz - 250 Kb/s

Bom desenpenho contra ruído

- Utiliza DSSS
  - Sequência direta de espalhamento do espectro
  - Fornece uma densidade espectral da potência muito baixa espalhando a potência do sinal sobre uma faixa de frequência muito larga
  - Requer uma largura de faixa muito grande para transmitir diversos Mbits/s.
- Menos interferência de bandas utilizadas
- Melhoria na relação sinal/ruído no receptor

Bom desenpenho contra interferências

- CSMA-CA
- GTS - Garantia de slot de tempo
- Escaneamento de energia
  - Energia
  - CCA (Carrier Sense)
  - CCA + Energia

Baixo consumo

- Sleep em 99% do tempo

Dispositivos da rede

- Dispositivos de Função Completa (FFD)
- Dispositivos de Função Reduzida (RFD)

Arquitetura de transporte de dados

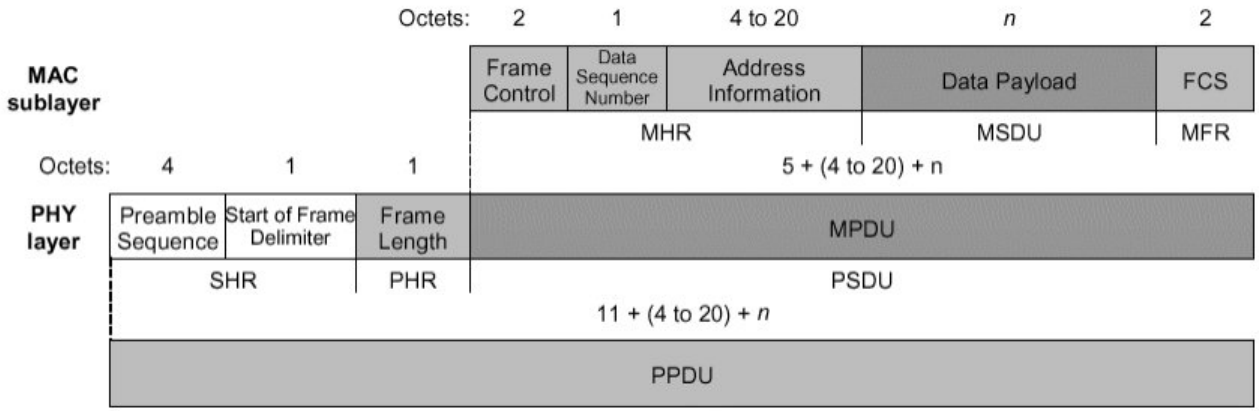


Figura: Dataframe

Arquitetura de transporte de dados

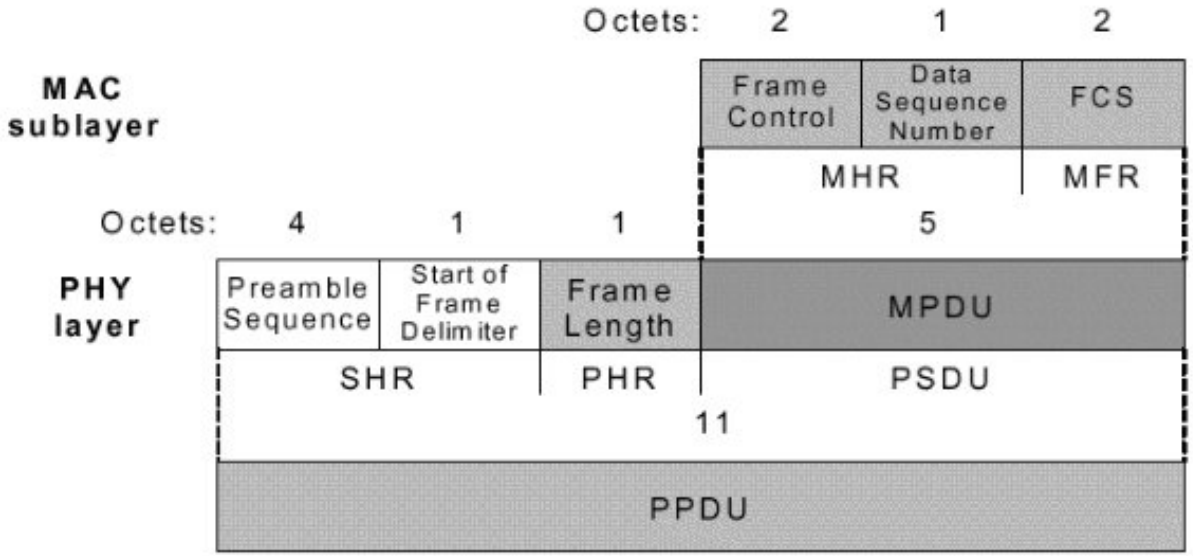


Figura: ACK Frame

Arquitetura de transporte de dados

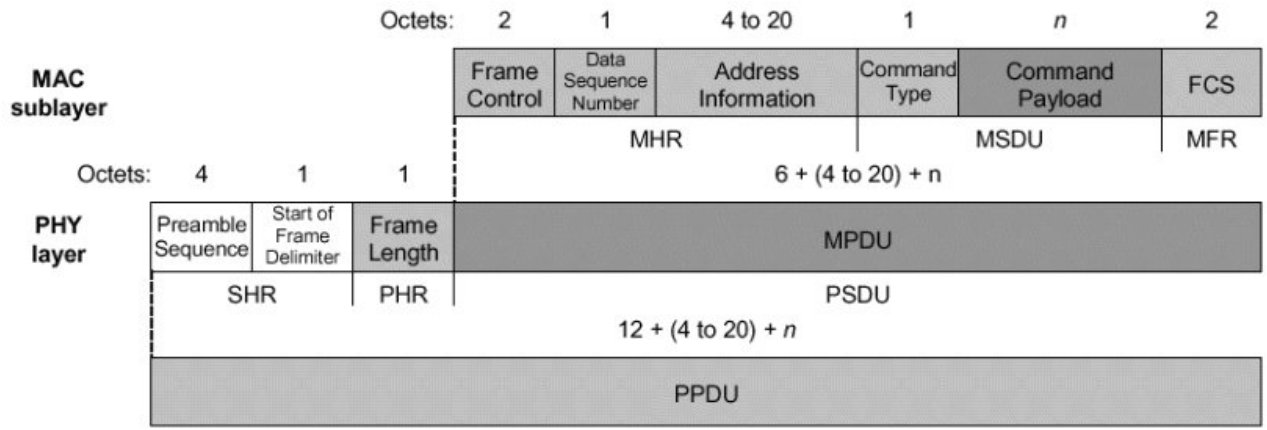


Figura: MAC Command frame

Arquitetura de transporte de dados

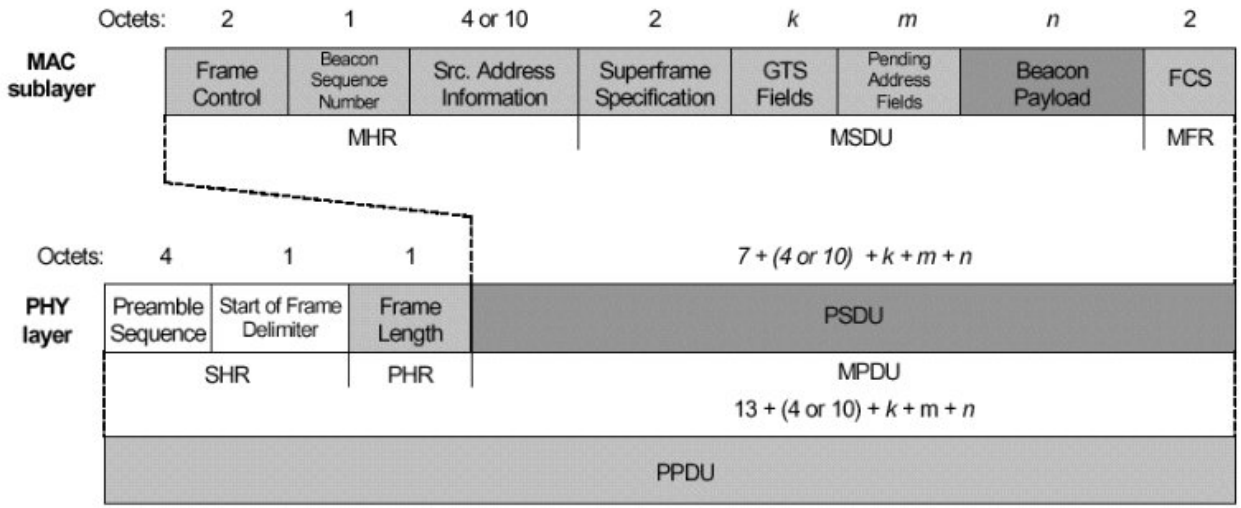


Figura: Beacon frame

Arquitetura de transporte de dados

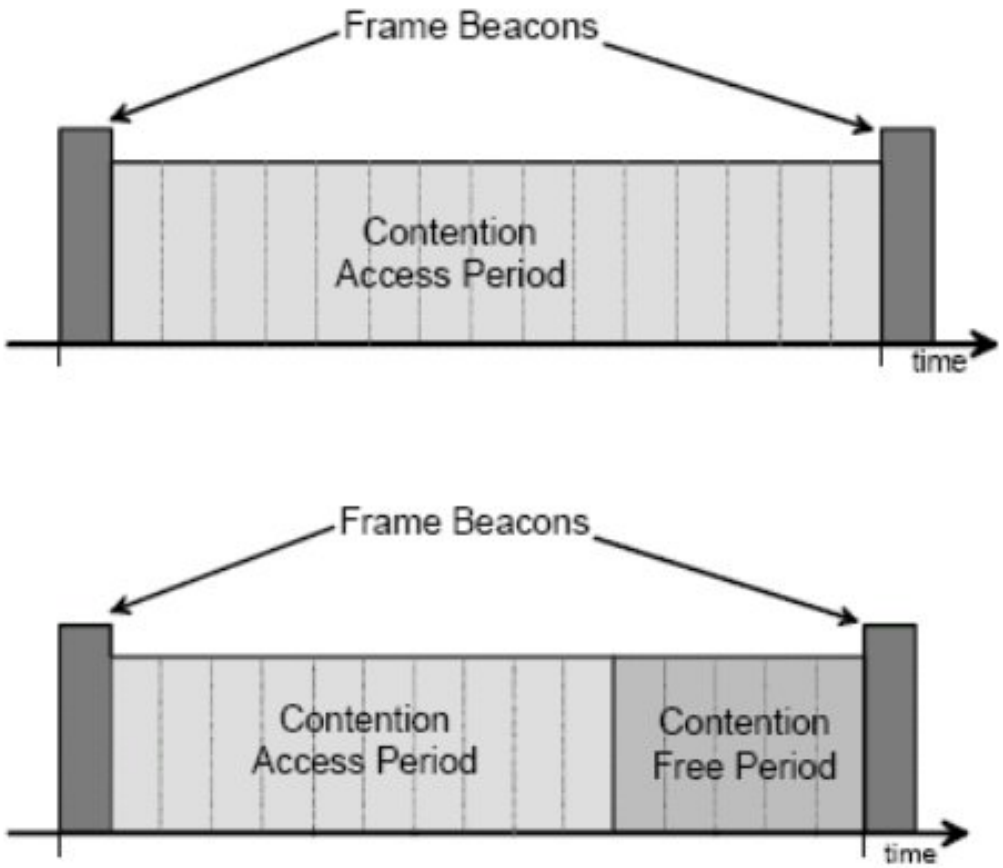


Figura: Super Frame

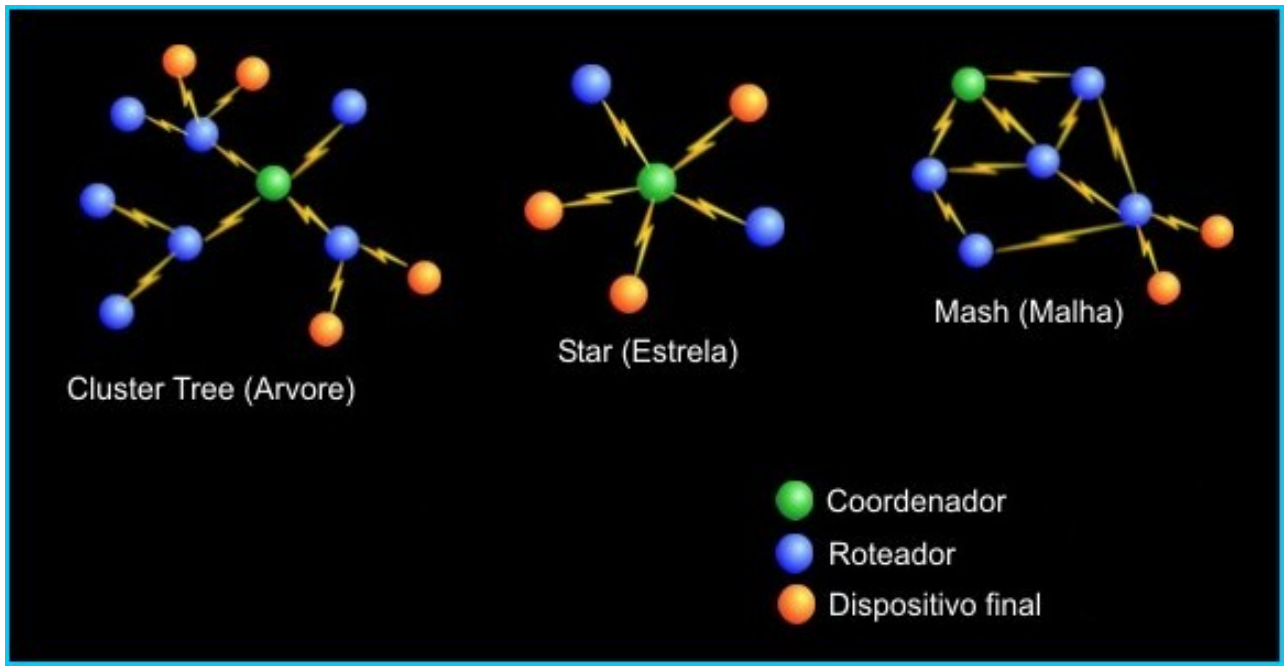
ZigBee

- **Serviço de encriptação extra:** chaves de rede e aplicação implementam 128b de encriptação AES;
- **Associação e autenticação:** somente nós válidados podem ingressar na rede;
- **Protocolo de roteamento:** AODV, um protocolo ad hoc reativo, tem sido implementado para realizar o roteamento de dados e processo de encaminhamento para qualquer nó na rede
- **Serviços de aplicações:** um termo abstrato denominado "cluster"é introduzido. Cada nó pertence a um cluster pré-definido e pode obter um pré-definido número de ações. Por exemplo: o cluster do sistema de luz da casa pode realizar duas ações; ligar a luz e desligar a luz.

Funcionamento de uma rede ZigBee

- Coordenador (FFD)
- Roteador (FFD)
- Dispositivo final (FFD ou RFD)

Topologias de rede ZigBee



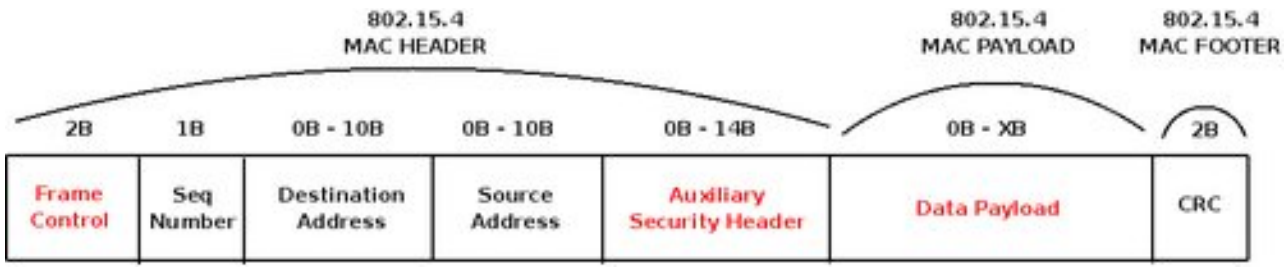
Funcionamento de uma rede ZigBee

- 802.15.4 foi idealizado para ser um protocolo que estabelece comunicações pontoa-ponto com eficiência de energia.
- ZigBee define serviços extras (roteamento em topologia estrela, encriptação, serviços de aplicação) acima da camada 802.15.4.
- ZigBee cria redes semi-centralizadas aonde apenas o dispositivo final pode ficar em estado de hibernação (sleep).

Visão geral

- AES (Advanced Encryption Standard)
- Chave de 128 bits
- Utilizado para encriptar e validar dados
- Código de Integridade de Mensagem

Quadro MAC

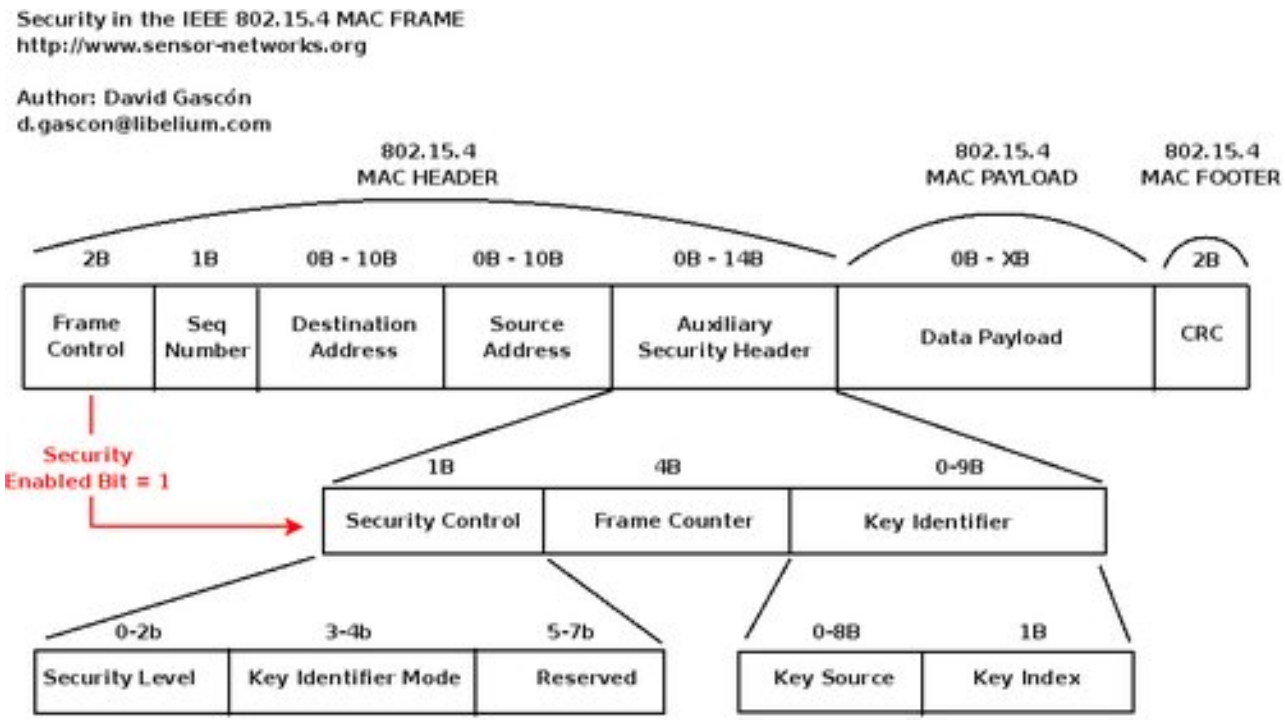

802.15.4
MAC HEADER
802.15.4
MAC PAYLOAD
802.15.4
MAC FOOTER
2B
1B
0B - 10B
0B - 10B
0B - 14B
0B - XB
2B
Frame Control
Seq Number
Destination Address
Source Address
Auxiliary Security Header
Data Payload
CRC

Quadro MAC

O frame de Controle de Segurança Auxiliar é habilitado somente se o subcampo de Segurança Habilitada do Frame de controle estiver ligado. Esse cabeçalho tem 3 campos:

- **Controle de Segurança (1B):** especifica que tipo de proteção é utilizada.
- **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 uma única ID sequência representada por este campo.
- **Identificador de chave (0-9B):** especifica a informação necessária para saber que chave nós estamos usando com o nó que estamos nos comunicando.

Quadro MAC


Security in the IEEE 802.15.4 MAC FRAME
http://www.sensor-networks.org
Author: David Gascón
d.gascon@libelium.com
802.15.4 MAC HEADER
802.15.4 MAC PAYLOAD
802.15.4 MAC FOOTER
2B
1B
0B - 10B
0B - 10B
0B - 14B
0B - XB
2B
Frame Control
Seq Number
Destination Address
Source Address
Auxiliary Security Header
Data Payload
CRC
Security Enabled Bit = 1
1B
4B
0-9B
Security Control
Frame Counter
Key Identifier
0-2b
3-4b
5-7b
0-8B
1B
Security Level
Key Identifier Mode
Reserved
Key Source
Key Index

Controle de Segurança

O controle de segurança é o local onde a nossa política de segurança global é configurada. Utilizando os 2 primeiros bits (campos de nível de segurança) escolhe-se o que será encriptado e quão longa a chave será:

0x00	Sem segurança		DNE*, ANV**
0x01	AES-CBC-MAC-32	MIC-32	DNE, AV****
0x02	AES-CBC-MAC-64	MIC-64	DNE, AV
0x03	AES-CBC-MAC-128	MIC-128	DNE, AV
0x04	AES-CTR	ENC	DE***, ANV
0x05	AES-CCM-32	AES-CCM-32	DE, ANV
0x06	AES-CCM-64	AES-CCM-64	DE, AV
0x07	AES-CCM-128	AES-CCM-128	DE, AV

* Dados não encriptados ** Autenticidade dos dados não validada *** Dados encriptados **** Autenticidade dos dados validada

Controle de Segurança - Identificador de modo de chave

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:

- **0:** O ID da chave é implicita para o remetente e destinatário (não é especificada na mensagem).
- **1:** O ID da chave é determinada explicitamente pelo index de chave de 1 Byte vindo do campo identificador de chave e do macDefaultKeySource.
- **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).
- **3:** O ID da chave é determinado explicitamente pelo index de chave de 1 Byte e os 8 Bytes da fonte de chave (Key Source).

Payload data

- **AES-CTR:** Todos os dados são encriptados utilizando a chave definida de 128 bits e o algorítmo 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.
- **AES-CBC-MAC:** O 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.
- **AES-CCM:** É a mistura dos métodos definidos anteriormente. Os subcampos correspondem com o modo AES-CTR mais o subcampo extra do AES-CBC-MAC encriptado.

Lista de controle de acesso

Quando um nó quer enviar uma mensagem para um nó específico ou recebe um pacote, ele irá procurar na ACL para verificar se o nó é um 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.

Tipos de chave

- **Master Keys:** São pré-instaladas em cada nó. Sua função é manter confidencial a troca de Chaves de Link entre dois nós no Processo de Estabelecimento de Chave (SKKE).
- **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 constuma ser usada.

Tipos de chave

- **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.

Política de segurança

- Modo comercial - compartilha chaves master e link, requer mais recurso de memória e oferece um modelo centralizado
- Modo residencial - compartilha chave de rede, ideal para rede de sensores sem fio

Considerações finais

- Vale a pena?
- Quanto custa?