UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA-INE
BACHARELADO EM CIÊNCIAS DA COMPUTAÇÃO

Ruan Ramon de Oliveira

Análise de vulnerabilidades em redes ZigBee

Florianópolis
2020

Ruan Ramon de Oliveira

Análise de vulnerabilidades em redes ZigBee

Trabalho de Conclusão de Curso submetido à Universidade Federal de Santa Catarina, como requisito necessário para obtenção do grau de Bacharel em Ciências da Computação.

Orientadora: Profa. Dr. Carla Merkle Westphall

Florianópolis, novembro de 2020

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Oliveira, Ruan Ramon de
Análise de vulnerabilidades em redes ZigBee / Ruan Ramon de Oliveira ; orientador, Carla Merkle Westphall, 2020.
90 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Centro Tecnológico, Graduação em Ciências da Computação, Florianópolis, 2020.

Inclui referências.

1. Ciências da Computação. 2. ZigBee. 3. Segurança. 4. Internet das Coisas. 5. Killerbee. I. Westphall, Carla Merkle. II. Universidade Federal de Santa Catarina. Graduação em Ciências da Computação. III. Título.

UNIVERSIDADE FEDERAL DE SANTA CATARINA

Ruan Ramon de Oliveira

Esta Monografia foi julgada adequada para a obtenção do título de Bacharel em Ciências da Computação, sendo aprovada em sua forma final pela banca examinadora:

Orientador(a): Profa. Dr. Carla Merkle Westphall
Universidade Federal de Santa Catarina - UFSC

Prof. Dr. Carlos Becker Wesphall
Universidade Federal de Santa Catarina - UFSC

Prof. Dr. Jean Everson Martina
Universidade Federal de Santa Catarina - UFSC

Me. Leandro Loffi
Universidade Federal de Santa Catarina - UFSC

Florianópolis, novembro de 2020

Agradecimentos

Agradeço primeiramente e imensamente a minha mãe, dona Angela, a mulher que em tantos momentos colocou as minhas prioridades acima das dela, a mulher que acreditou em mim quando eu não acreditava mais, a mulher que lutou por mim quando eu não tinha mais forças, a mulher que sonhou por mim quando eu já não sonhava mais, a mulher que eu tenho o orgulho e o prazer de poder chamar de mãe.

Agradeço a minha orientadora, Profa. Dra. Carla Merkle Wesphall, pela paciência, compreensão e companheirismo em todo o desenvolvimento deste trabalho. Agradeço também a todos os professores do qual tive o prazer de ter aulas, que me ajudaram não somente com conhecimento mas em muitos casos com ensinamentos de vida.

Agradeço a todos os bons amigos que fiz durante a graduação, que me ajudaram não somente nos aspectos acadêmicos mas também em vários outros aspectos da vida.

"Até mesmo a felicidade cobra seu preço,
você está disposto a pagar o preço pela sua ?.
(EU)

Resumo

Com o segmento de IoT (*Internet of Things*) crescendo de maneira significativa, espera-se que em 2025 hajam bilhões de dispositivos gerando uma grande quantidade de dados. Estes dados serão trafegados utilizando diversos protocolos, dentre eles o ZigBee. Desenvolvido e padronizado pela ZigBee Alliance o protocolo Zigbee apresenta um padrão que possibilita controle seguro, de baixo custo e de baixa potência para redes sem fio, que permite o controle de diversos equipamentos nas áreas de automação, aplicações em telemedicina, entretenimento, entre outras. Em sua maioria os dispositivos IoT tem o objetivo de captar leituras de variáveis do ambiente onde estão instalados, das mais simples como temperatura e umidade até as mais complexas como corrente elétrica, aberturas de portas por sensores de contato seco, entre outras. Diante deste cenário com tantos dados sensíveis trafegando, um algoritmo de segurança é necessário para garantir integridade e confiabilidade dos dados. Assim, este trabalho apresenta um estudo sobre vulnerabilidades do protocolo e a ferramenta KillerBee, utilizada para efetuar ataques contra redes ZigBee. São apresentadas as dificuldades de integração da ferramenta com o hardware necessário para efetuar os ataques e uma nova proposta que visa estudar dispositivos vendidos a varejo, buscando por evidências de que os produtos podem apresentar problemas de segurança. O estudo do protocolo apresenta características importantes, como um sistema completo de segurança com chaves e algoritmos bem definidos para entrada e permanência na rede. O protocolo é bem documentado, contudo um pouco confuso e muito extenso, o que pode ser uma desvantagem na tentativa do seu uso. Por fim, a avaliação dos dispositivos demonstra que a maioria possui pouca documentação sobre os quesitos de segurança, e quando existem, os mecanismos de segurança são implementados parcialmente.

Palavras-chave : IoT, Internet das Coisas, ZigBee, Segurança, KillerBee.

Abstract

With the IoT (*Internet of Things*) segment growing roughly, it is expected that by 2025 there will be billions of devices generating a large amount of data. These data will be transferred using different protocols, among them ZigBee. Developed and standardized by the ZigBee Alliance or Zigbee protocol, it presents a standard that enables secure, low cost and low power control for wireless networks, which allows the control of various equipment in the areas of automation, telemedicine applications, entertainment, among others. Most IoT devices have the objective of capturing readings of environment variables that are installed, from the simplest such as temperature and humidity to the most complex such as electric current, door openings by dry contact sensors, among others. Faced with a scenario with so much data traveling, a security algorithm is necessary to ensure data compliance and reliability. Thus, this work presents a study on protocol vulnerabilities and the KillerBee tool, used to perform against ZigBee networks. There are difficulties such as difficulties in integrating the tool with the necessary hardware to carry out the procedures and a new proposal to study the devices sold at retail, looking for evidence that the products may present security problems. The study of the protocol has important characteristics, such as a complete security system with well-defined keys and algorithms for entering and staying on the network. The protocol is well documented, however a little confusing and very extensive which can be a disadvantage when trying to use it. Finally, the evaluation of the devices shows that the majority have little documentation on the security requirements, and when they exist, the security mechanisms are partially implemented.

Keywords : IoT, Internet of Things, ZigBee, Security, KillerBee.

Lista de ilustrações

Lista de abreviaturas e siglas

AES – Advanced Encryption Standard

APL – Application

APS – Application Support

B2B – Business to Business

CBC-MAC - Cipher Block Chaining Message Authentication Code

CCM – Counter with CBC-MAC

CSMA-CA – Carrier Sense Multiple Access with Collision Avoidance

DDoS – Distributed Denial of Service

DNS – Domain Name Service

DoS – Denial of Service

IoT – Internet of Things

LK – Link Key

MAC – Media Access Control

MK – Master Key

NK – Network Key

NWK – Network

OTA – Over the Air

PAN – Personal Area Network

PHY – Physical

QR – Quick Response

WSN – Wireless Sensor Network

ZCL – ZigBee Cluster Library

ZDO – ZigBee Device Object

ZDP – ZigBee Device Profile

ZTC – ZigBee Trust Center

Sumário

1 Introdução

Pela definição da IEEE Internet of Things journal [IEEE 2015], um sistema IoT (*Internet of Things*) é uma rede de redes, no qual, tipicamente, um grande número de objetos/coisas/sensores/dispositivos são conectados através de uma infra-estrutura de comunicação e informações para fornecer serviços de valor agregado e processamento inteligente de dados e gerenciamento para diferentes aplicações [Porkodi e Bhuvaneswari 2014]

A *Internet of Things* tem evoluído de forma exponencial nas últimas décadas, sendo que alguns especialistas da área estimam que nos próximos anos podemos chegar a quase 50 bilhões de "coisas" conectadas a Internet. Isso se deve ao fato do rápido crescimento tecnológico em sistemas embarcados cada vez menores e mais acessíveis e as redes de sensores sem fio (Wireless Sensor Network – WSN) [Ronen et al. 2017], compostas de elementos conhecidos como nodos. Esses nodos possuem poder computacional, no geral, limitado com foco em sensoriamento de diversas grandezas como : umidade, pressão, calor e vibração [Kocakulak e Butun 2017].

O sensoriamento é feito em diversos segmentos da sociedade em atividades relacionadas ao desenvolvimento e bem-estar das cidades e pessoas como: Cidades Inteligentes, Agricultura Inteligente, Automação Doméstica e Residencial. Em áreas ambientais em atividades relacionadas ao monitoramento e redução de gasto de recursos naturais como: Medição Inteligente, Reciclagem inteligente de água, Alerta de Desastres. Em áreas industriais como em Logística, Aeroespacial e Aviação [Porkodi e Bhuvaneswari 2014].

Com essa diversidade de cenários que demandam características específicas, surge a proposta das redes Zigbee para comunicação entre os dispositivos. Atualmente, na sua versão 3.0, oferece um conjunto de produtos e serviços com foco em usuários e desenvolvedores através de uma padronização em todas as camadas do modelo de rede. O Zigbee 3.0 desenvolvido com base na Zigbee PRO, aprimora o padrão IEEE 802.15.4 adicionando camadas de rede, segurança e uma estrutura de aplicação. Pode ser considerada uma solução completa com foco em dispositivos de baixo consumo de energia, certificável e interoperável, para redes de curto alcance Zigee-Alliance 2019.

Os benefícios advindos do paradigma IoT são inegáveis, contudo existem sérias falhas de segurança. Fatores como o curto tempo para inserção de novos produtos no mercado, associado a pouca legislação relacionada, estimularam muitos fabricantes a ignorar o elemento segurança em suas soluções e projetos, desenvolvendo dispositivos potencialmente vulneráveis. A negligência de várias considerações de segurança permite a exploração de informações sigilosas, que podem variar de *streamings* de vídeos desprotegidos

de monitores de bebês, brinquedos IoT, *upload* de gravações de voz, e-mails e senhas não autorizados, além de dispositivos mal projetados permitirem, em alguns casos, atuação sobre os mesmos, e em casos mais extremos a possibilidade de reprogramação do firmware do dispositivo. Entre casos recentes podemos destacar o ataque lançado pelo malware específico *IoT Mirai* [Neshenko et al. 2019].

Com este cenário em mente este trabalho tem como proposta uma análise de segurança em redes ZigBee/802.15.4. Inicialmente, alguns trabalhos relacionados são comentados. Na sequência, é descrito um estudo aprofundado dos quesitos de segurança nas quatro camadas das redes ZigBee e os tipos de ataques mais comuns efetuados. Por fim, o trabalho propõe a elaboração de uma ambiente controlado para execução de ataques e realiza a verificação dos quesitos de segurança.

1.1 Objetivo

1.1.1 Objetivo Geral

O objetivo geral deste trabalho é prover um estudo sobre vulnerabilidades de segurança em redes ZigBee, amplamente utilizada no ambiente de IoT.

1.1.2 Objetivos Específicos

Considerando o desenvolvimento do trabalho e o objetivo geral apresentado, destacam-se os seguintes objetivos específicos:

- Analisar e compreender o comportamento das redes ZigBee;
- Descrever a ferramenta KillerBee, usada em ambientes IoT, para testes de segurança de redes ZigBee;
- Demonstrar o uso da ferramenta KillerBee em hardwares existentes; e,
- Descrever considerações sobre a segurança de equipamentos disponíveis no mercado que utilizam o protocolo ZigBee.

1.2 Justificativa

De acordo com a IDC 2019, empresa de planejamento estratégico, em 2025 haverá 41,6 bilhões de "coisas" conectadas à Internet. Estes dispositivos não serão de uso geral como smartphones ou computadores pessoais, mas dispositivos de função dedicada como máquinas de venda automática, carros, caminhões, e outros, nas mais diversas áreas.

A IoT terá um grande impacto na economia por transformar muitas empresas em negócios digitais, facilitando novos modelos de negócios, melhorando a eficiência e aumentando o envolvimento dos funcionários e clientes. No entanto, as maneiras pelas quais as empresas podem tomar proveito desses benefícios serão diversos.

A maior barreira para a IoT é que a maior parte das empresas não sabem o que fazer com a tecnologia. E se eles tiverem planos para a IoT, existe uma preocupação sobre quem irá liderar essas iniciativas. Essa necessidade é uma oportunidade para os profissionais preencherem as vagas de liderança de IoT.

Já em McKinsey 2015 calcula-se que a *Internet of Things* terá um potencial impacto econômico de 3,9 trilhões a 11,1 trilhões de dólares, por ano, em 2025. Isso devido a um aumento de produtividade, maior economia de tempo e melhor utilização de ativos. Na ponta superior, o valor desse impacto seria equivalente a onze por cento da economia mundial.

O segmento B2B (*Business to business*) será o maior gerador desse impacto econômico. Com aplicações de IoT, B2B pode criar ainda mais valor do que aplicações unicamente para consumidores. Os usos em B2B podem gerar perto de setenta por cento do valor potencial de IoT, em setores como mineração, petróleo, gás, construção, saúde e agricultura. A *Internet of Things* cria valor por meio de duas alavancas econômicas principais: geração de receita adicional e aumento da eficiência operacional e redução de custos [Ellen 2016].

Contudo, esse cenário trouxe consigo também grandes perigos. No final de 2016, cibercriminosos lançaram grandes ataques de negação de serviço distribuído (DDoS - *Distributed Denial of Service*), causando uma interrupção nos serviços de Internet que afetaram muitas empresas, incluindo Amazon, PayPal, Netflix, Spotify e Twitter. Para isso, o grupo atacante explorou as vulnerabilidades de segurança de milhares de dispositivos IoT, permitindo que eles fossem sequestrados e transformados em criadores de solicitações de DNS (*Domain Name System*) [Ellen 2016].

Com base nessas informações, nos próximos anos, o mercado irá cada vez mais demandar profissionais especializados em IoT, principalmente na área de segurança, pois os segmentos que irão gerar mais renda, serão os segmentos que demandam alto grau de segurança, devido aos tipos de dados gerados.

1.3 Metodologia

A metodologia aplicada a este trabalho teve início com a pesquisa sobre temas associados a segurança e vulnerabilidades em redes WSN, dispositivos IoT e redes Zigbee/802.15.4. As principais fontes de pesquisas para artigos científicos foram : ResearchGate,

IEEE, Nature, ISDN, entre outros; estes serviram como base da fundamentação teórica e para a escrita e desenvolvimento deste trabalho.

Para a etapa prática foi utilizada a ferramenta KillerBee como base e foram feitos testes de configuração da ferramenta em alguns tipos de hardwares disponíveis. Todo o processo foi documentado. Também foram descritos dispositivos comerciais que usam o protocolo ZibBee para realizar uma verificação das características de segurança destes dispositivos.

1.4 Trabalhos Correlatos

Existem vários trabalhos com foco na análise das vulnerabilidades de redes ZigBee. O trabalho de Cao et al. 2016 estuda e implementa um ataque conhecido como ghost-in-ZigBee, no qual o objetivo é gerar mensagens falsas para fazer que um determinado nodo da rede executar operações desnecessárias relacionadas à segurança, para esgotar intencionalmente a energia desse nodo. Após a análise teórica do impacto do ataque na vida útil do nodo vítima foi desenvolvido um modelo analítico para quantificar o impacto de ataques de Negação de Serviço (DoS – *Denial of Service*) em uma rede com vários nodos. Por fim, um algoritmo para detectar e localizar o invasor analisando as variações de fluxo da rede foi proposto, e resultados de simulação em computador demonstraram o impacto do ataque e a eficiência das contramedidas propostas. Além disso, a eficácia do ataque foi validada por meio de experimentos físicos e foram discutidas várias recomendações sobre como suportar o ataque.

Já em Khanji, Iqbal e Hung 2019 é apresentada uma avaliação do desempenho do ZigBee sob a perspectiva de segurança. O artigo introduz uma visão geral das redes Zigbee, apresenta sua arquitetura geral e cada módulo que a compõe, as topologias da rede e os três tipos de nodos que podem ser encontrados na rede. Em seguida são explorados os serviços de segurança integrados do ZigBee como: técnicas de criptografia, sistema de chaves de segurança, tipos de chaves de segurança e o centro de confiança (TC – *Trust Center*). Com base nos resultados da pesquisa são apresentadas questões de vulnerabilidades para as camadas definidas pela Zigbee, ataques passivos, ativos e ataques com foco específico em determinada entidade da rede. Por fim, são apresentados controles de segurança e contramedidas que visam mitigar os cenários de ataques apresentados anteriormente.

1.5 Organização

Este trabalho é dividido em 5 capítulos. O capítulo 1 apresenta a introdução do trabalho, justificativa, metodologia, trabalhos correlatos e objetivos. No capítulo 2 são apresentados os conceitos sobre redes ZigBee, chaves de segurança e vulnerabilidades. O

capítulo 3 apresenta as dificuldades encontradas na proposta inicial e a nova proposta. O capítulo 4 traz a análise da dificuldade para se efetuar um ataque e vulnerabilidades de dispositivos. Já no capítulo 5, é apresentada a conclusão deste estudo, bem como propostas para trabalhos futuros. Por fim, o apêndice A apresenta o artigo gerado a partir deste trabalho.

2 Fundamentação Teórica

Este capítulo tem por objetivo apresentar a base teórica do protocolo ZigBee 802.15.4 em relação aos quesitos de segurança.

2.1 Redes ZigBee

A rede Zigbee é um padrão de redes sem fio para um conjunto de comunicações de alto nível e protocolos de comunicação. Suas principais vantagens são baixa potência, curta distância, baixa complexidade, auto-organização e baixo custo. Inclui um gama completa de dispositivos capazes de realizar medições das mais diversas grandezas como: temperatura, umidade, corrente, sensores de porta, entre outras. São baseadas no padrão 802.15.4 da IEEE que define as 2 camadas inferiores da rede: a camada física (PHY - *Physical*) e a camada de controle de acesso ao meio (MAC – *Media Access Control*). Assim, a ZigBee Alliance baseia-se nestas 2 camadas para fornecer a camada de rede (NWK - *Network*) e uma camada de aplicação (APL - *Application*) padronizada, sendo que a rede é implementada utilizando-se do modelo de pilha de protocolos. A figura 1 ilustra a pilha do protocolos de uma rede ZigBee/802.15.4 [Wang, He e Wan 2011].

A camada física fornece uma interface para o meio físico (por exemplo rádio) e possui 3 intervalos de frequência : 868/915 MHz e 2.4 GHz. A frequência de 868 MHz é utilizada na Europa, a de 915 Mhz na América e a de 2.4 GHz utilizado em todo o mundo. A camada MAC, imediatamente acima, controla o acesso ao canal de rádio, um mecanismo de CSMA-CA (*Carrier Sense Multiple Access with Collision Avoidance*) é usado para transmitir quadros de sinais e sincronização, além de fornecer um meio de comunicação com seus vizinhos imediatos com o intuito de prevenir colisões e melhorar a eficiência, também sendo responsável por compor e decompor os pacotes de dados transmitidos [Dini e Tiloca 2010].

A camada de rede ZigBee tem a responsabilidade de descobrir nodos adjacentes de um salto e armazenar informações relevantes sobre os mesmos, além de permitir que dispositivos entrem e saiam de uma rede ZigBee e encaminhar os quadros de dados aos dispositivos corretos. Por fim, a camada de aplicação especifica o formato dos quadros de dados para transporte e fornece um serviço de dados para aplicações. A segurança envolve tanto a camada de aplicação quanto a camada de rede [Wang, He e Wan 2011].

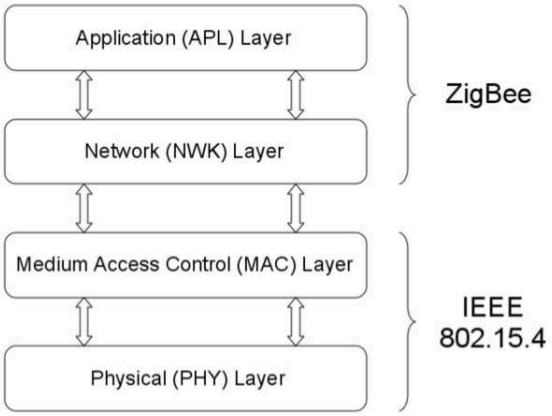


Figura 1 – Camadas da pilha ZigBee [Wang, He e Wan 2011]

2.1.1 Estrutura básica das Redes ZigBee

Uma rede baseada no ZigBee é formada basicamente por um coordenador ZigBee e nodos ZigBee, sendo os nodos diferenciados por roteadores e finais. As redes ZigBee suportam nativamente as topologias estrela e árvore em arquiteturas de malha genérica. Um ponto importante em comum é que em todos os casos a topologia pode possuir somente um concentrador .

A figura 2 apresenta uma topologia do tipo estrela, ou de salto único, neste modelo o coordenador é responsável pela inicialização e pela manutenção da rede. Todos os outros dispositivos da rede são dispositivos finais e se comunicam diretamente com o concentrador. Esta topologia é adequada para redes que se possuam um concentrador centralizado e para aplicações onde o tempo é um fator crítico. Na figura 3 é apresentada uma rede de árvore em cluster, diferentemente da primeira neste modelo os nodos roteadores podem ser utilizados para estender a rede. Os nodos roteadores nesse modelo são responsáveis por controlar o fluxo de dados usando estratégias de roteamento hierárquico e a periodicidade de envio de roteamento definida na 802.15.4. Por fim, a figura 4 apresenta uma rede de malha genérica, neste modelo o concentrador e os nodos roteadores possuem as mesmas funções, uma rede de malha que permite uma comunicação ponto-a-ponto completa, excluindo comunicação entre dois nodos finais diretamente. Neste modelo, o roteamento de dados é descentralizado, para caso um nodo roteador falhe, o nodo final seja capaz de se conectar a outro nodo roteador para continuar enviando dados [Li et al. 2010].

2.1.2 Comissionamento

Comissionamento é o processo de configuração dos nodos de uma rede ZigBee com o intuito de comunicação entre si. Este processo apesar de parecer simples é bem complexo

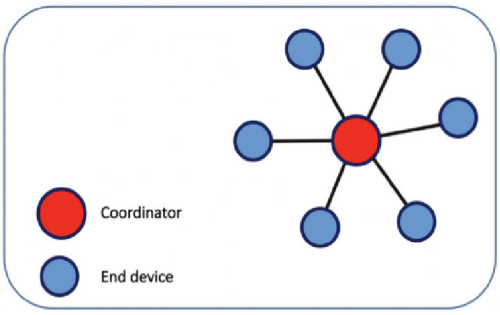


Figura 2 – Topologia em estrela [Alshahrani, Traore e Woungang 2019]

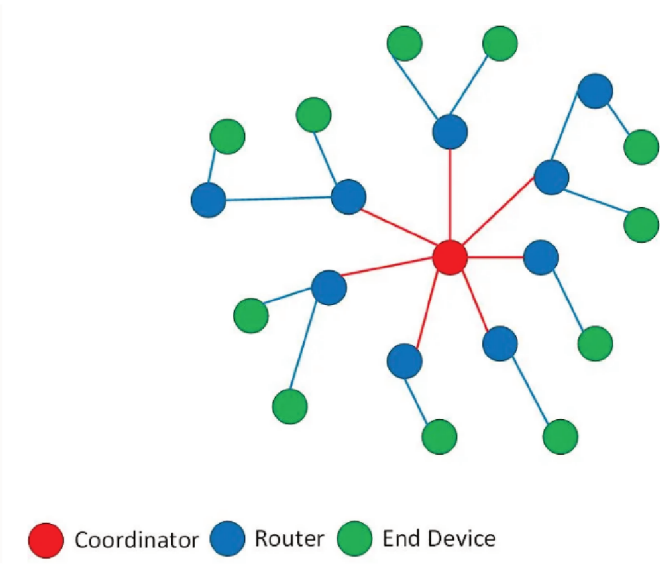


Figura 3 – Topologia de rede Cluster Tree [Alshahrani, Traore e Woungang 2019]

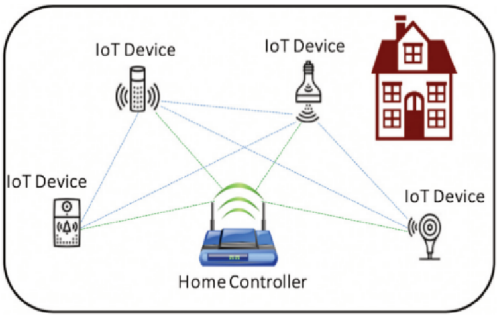


Figura 4 – Topologia de rede mesh [Alshahrani, Traore e Woungang 2019]

e envolve um conjunto de etapas como: procura por uma rede apropriada; conexão com a rede correta; determinar como e com quais nodos da rede ha a possibilidade de comunicação (grupos, ligações ou diretamente); e determinar o que fazer quando a comunicação termina. Uma vez conectado a uma rede são necessários mecanismos de segurança para que redes independentes não se misturem, para envio de comandos para os nodos corretos e para comunicação entre dois nodos de uma mesma rede.

O comissionamento em redes ZigBee é um conceito conhecido como "Modelo Borboleta", que tem por base que um dispositivo seja criado com qualquer informação que possa ser razoavelmente configurada de maneira estática no momento da fabricação. Na sua forma mais básica, e na ausência de outras informações de configuração, um dispositivo novo ingressará na primeira rede disponível. Depois de ingressar, ele receberá as informações que irão prepará-lo para ficar operante e comunicável na rede. Após algumas dessas fases, chega ao estado operacional estável, armazenando essas novas informações da rede em uma memória não volátil, assim, caso haja falha energética quando religado o dispositivo continua operante. Todo dispositivo ZigBee pode ter seu estado regredido ao de fábrica, isso ocorre quando a rede apresenta uma falha ou quando se deseja trocar o dispositivo de rede. As primitivas de comissionamento estão espalhadas em diversas camadas da pilha de protocolos como nas camadas NWK, APS, ZDO, ZDP e a Biblioteca de Clusters ZigBee.

O *ZigBee Device Object* (ZDO) contém os métodos para localizar e associar uma dispositivo a uma rede, efetuando este trabalho juntamente com a camada NWK (Network); O *ZigBee Device Profile* (ZDP) contém o nodo e a aplicação, bem como as funções remotas de gerenciamento de tabelas; O ZigBee Cluster Library (ZCL) fornece um padrão para as principais funcionalidades e gestão de cenários OTA (*Over-the-Air*) como instalação de chaves de segurança, identificação de PAN IDs (*Personal Area Network Identifier*), a máscara de canal e os endereços de outros dispositivos [Gislason 2008].

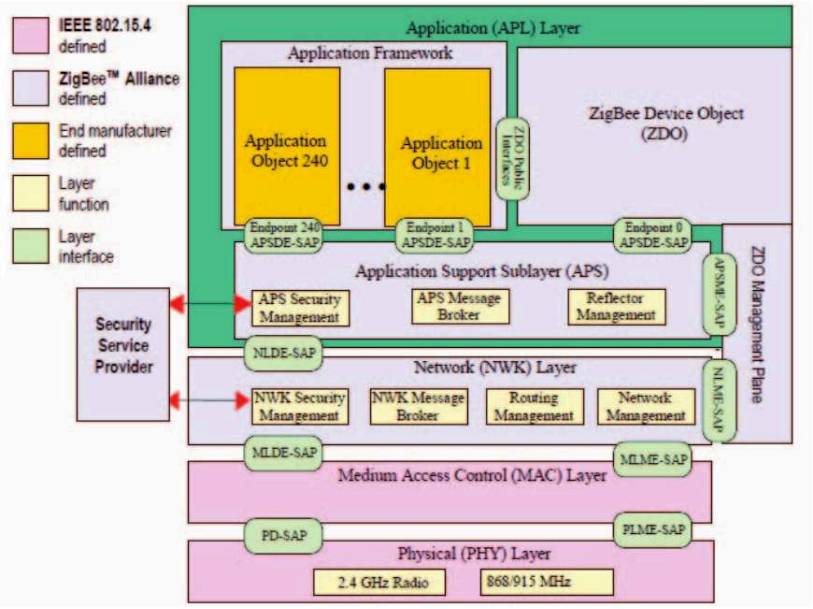


Figura 5 – Arquitetura completa da pilha Zigbee [Wang, He e Wan 2011]

2.1.3 Segurança das Redes ZigBee

O protocolo ZigBee define métodos para implementar serviços de segurança, como estabelecimento de chave criptográfica, transporte de chaves, proteção de quadros e gerenciamento de dispositivos. A arquitetura de segurança do ZigBee inclui mecanismos de segurança em três camadas da pilha de protocolos – MAC, Rede e Aplicação. Cada camada possui serviços definidos para o transporte seguro de seus respectivos quadros.

A camada MAC é responsável por seu próprio processamento de segurança, mas as camadas superiores determinam qual nível de segurança usar. Quando a proteção de integridade da camada MAC é empregada, todo o quadro MAC é protegido, incluindo o cabeçalho MAC que contém os endereços de origem e destino do hardware. Ao ativar a integridade do quadro MAC, o endereço de origem da camada MAC pode ser autenticado. Essa medida pode combater os ataques de falsificação e permitir que um dispositivo processe e compare com mais eficiência um quadro MAC recebido.

A criptografia é baseada no uso de chaves de 128 bits e no padrão de criptografia AES (*Advanced Encryption Standard*). Criptografia, integridade e autenticação podem ser aplicadas nas camadas de Aplicação, Rede e MAC para proteger os quadros, frames e pacotes em cada um dos níveis. Em termos de tipos de chave, o ZigBee especifica o uso das chaves: Mestre (MK – *Master Key*), Link (LK – *Link Key*) e Rede (NK – *Network Key*) para proteger os quadros transmitidos.

Uma chave de Rede é uma chave compartilhada entre todos os nodos em uma rede ZigBee. O padrão também especifica uma Chave de Rede Alternativa como uma forma de rotação de chave que pode ser empregada para fins de atualização de chave. Uma rede deve utilizar uma Chave de Rede comum a todos os dispositivos para proteger todos os quadros de rede (mensagens de roteamento, solicitações de entrada na rede, etc.) e impedir a entrada e uso não autorizado da rede por dispositivos desconhecidos.

As Chaves de Link são chaves de sessão secretas usadas entre dois dispositivos em comunicação e são exclusivas para esses dispositivos. Os dispositivos usam sua Chave Mestra para gerar a chave de Link. A maneira pela qual as chaves Mestra, Link e Chaves de Rede são geradas, armazenadas, processadas e entregues aos dispositivos determina a eficácia e o grau de segurança da implementação geral da rede.

O ZigBee usa o conjunto de segurança CCM* (*Counter with CBC-MAC*) baseado em AES, que é baseado no conjunto de segurança especificado no padrão 802.15.4 e resumido na Figura 6. O CCM* é uma pequena modificação dos modos do CCM no padrão 802.15.4 e oferece recursos somente de criptografia e somente integridade. Os recursos extras no CCM* simplificam a segurança, eliminando a necessidade dos modos CTR e CBC-MAC no conjunto 802.15.4 e também permitem o uso de uma única chave para cada nível de segurança dentro do protocolo. Com o CCM*, as camadas MAC, Rede e Aplicação

podem, opcionalmente, reutilizar a mesma chave para uma implementação mais eficiente, com base nos recursos limitados de armazenamento e processamento do dispositivo.

Identifier	Security level sub domain	Security component	Security attributes	Security services				Data integrity
				access control	data encryption	Frame integrity	Sequence update (optional)	
0x00	000	None	无					M=0
0x01	001	AES-CTR	ENC	X	X		X	M=0
0x02	010	AES-CCM-128	ENC-MIC-128	X	X	X	X	M=16
0x03	011	AES-CCM-64	ENC-MIC-64	X	X	X	X	M=8
0x04	100	AES-CCM-32	ENC-MIC-32	X	X	X	X	M=4
0x05	101	AES-CBC-MAC-128	MIC-128	X		X		M=16
0x06	110	AES-CBC-MAC-64	MIC-64	X		X		M=8
0x07	111	AES-CBC-MAC-32	MIC-32	X		X		M=4

Figura 6 – Componentes de segurança ZigBee [Fan 2017]

O componente central da arquitetura de segurança do ZigBee é o ZigBee *Trust Center* (ZTC). Todos os dispositivos em uma rede reconhecem e confiam em exatamente um ZTC. O ZTC armazena e distribui chaves para dispositivos ZigBee. As funções executadas pelo ZTC são gerenciamento de confiança, gerenciamento de rede e gerenciamento de configuração.

É importante observar que diferentes aplicativos em execução no mesmo dispositivo ZigBee não são separados logicamente (devido a restrições de custo e complexidade). Portanto, aplicativos diferentes também não são criptograficamente separados e deve-se presumir que os aplicativos confiam um no outro porque estão usando o mesmo material de codificação. O ZigBee se refere a ele como um modelo de confiança aberto, no qual, diferentes camadas da pilha de comunicação e todos os aplicativos em execução em um único dispositivo confiam um no outro. A implicação para o uso desse modelo é que todos os dispositivos e aplicativos em uma determinada rede confiam um no outro e que a segurança é realizada de acordo com o dispositivo.

2.1.4 Chaves de Segurança

As redes Zigbee utilizam uma Chave de Rede e Chaves de Link para se comunicar, sendo que o destinatário tem conhecimento das chaves usadas para proteger as mensagens. Uma Chave de Rede possui 128 bits e é compartilhada por todos os dispositivos conectados à rede e é utilizada para transmissões do tipo *broadcasting*. Existem dois tipos: a padrão e a de alta segurança, o tipo da Chave de Rede irá definir como ela é distribuída, pois ela própria deve ser protegida quando é passada ao dispositivo que deseja se conectar.

Para essa criptografia, uma Chave de Link pré-configurada é usada, essa chave é conhecida pelo Trust Center e pelo dispositivo que deseja se conectar no modelo de segurança

centralizada, e é conhecida por todos os nodos no modelo de segurança distribuída.

A Chave de Link é uma chave de 128 bits compartilhada por dois dispositivos, e existem dois tipos: a global e a exclusiva. O tipo da chave determina como o dispositivo lida com mensagens enviadas a partir do *Trust Center*.

No modelo de segurança centralizado, existem três tipos de Chaves de Link: Chave de Link global usada pelo *Trust Center* e todos os nodos da rede; Chave de Link exclusiva usada para uma relação individual entre o *Trust Center* e um nodo específico, posteriormente substituída por uma Chave de Link do *Trust Center*; e a Chave de Link de aplicação usada entre um par de dispositivos. Chaves de link relacionadas ao *Trust Center* geralmente são pré-configuradas usando um método fora de banda, por exemplo, código QR (*Quick Response*) na embalagem, enquanto as chaves de link entre entidades geralmente são geradas pelo Trust Center e criptografadas com a Chave de Rede. Em uma rede de segurança distribuída, as chaves de link existem apenas entre um par de dispositivos. A figura 7 faz um resumo dos modos de segurança, camadas e suas chaves, onde (O) indica opcional.

secret key	layer		mode	
	network layer	application layer	safe mode	High security
Network key	YES	YES	YES	YES
master key	NO	YES	NO	YES(O)
Link key	NO	YES	YES(O)	YES(O)

Figura 7 – Modelos de segurança e chaves [Fan 2017]

2.1.5 Trust Center

O *Trust Center* é o dispositivo que os nodos conectados à rede confiam para distribuir suas chaves, ele tem a função de gerenciar as chaves, configurar a comunicação ponto-a-ponto e estabelecer, manter e atualizar as políticas de segurança para a rede. No modelo de segurança centralizada todos os dispositivos da rede devem saber exatamente quem é o *Trust Center* ativo e deve haver somente um ativo. Neste modelo o *Trust Center* pode estabelecer políticas para ingresso de novos dispositivos, por exemplo, requerer que dispositivos desconhecidos identifiquem-se antes de fornecer a atualização da Chave de Rede; exigir uma Chave de Link pré configurada de fábrica ou exigir que uma Chave de Link seja instalada utilizando uma frequência diferente da padrão.

No modelo de rede distribuída todos os nodos roteadores tem a capacidade de atuar como um *Trust Center*, e distribuir chaves para a segurança da rede. Este modelo é utilizado para distribuição de Chaves de Rede e não para distribuição de Chaves de Link, pois não há um *Trust Center* único na rede. Em algumas aplicações os dispositivos podem

ter o endereço do *Trust Center* e uma Chave de Link configurados na fábrica, em outros casos onde a rede pode tolerar um momento de vulnerabilidade, a Chave da Rede pode ser enviada por meio de de um transporte seguro utilizando as chaves da *Application Support SubLayer* (APS) usando uma Chave de Link conhecida.

Em ambos os modelos para fins de segurança um dispositivo aceita uma Chave de Link do *Trust Center* ou uma Chave de Rede ativa por meio do transporte de chaves. Em uma rede centralizada um dispositivo só vai aceitar uma Chave de Rede ativa inicial e atualizações quando elas estiverem protegidas pela Chave de Link compartilhada com o *Trust Center*. Na configuração um dispositivo só aceita a Chave de Link do seu *Trust Center*, ou por meio de negociação usando um protocolo de mais alto nível entre os dispositivos, este método também é utilizado para adicionar ou trocar Chaves de Link e Chave de Rede. [ZigBee Alliance 2015].

2.1.6 Segurança nas Camadas

Como mostrado na figura 2, o ZigBee define as camadas NWK e APL, e a IEEE 802.15.4 as camadas PHY e MAC. A camada APL é constituída das subcamadas *Application Support* – APS, ZDO e Aplicação. O ZDO é responsável por gerenciar as políticas de segurança e a configuração de um dispositivo enquanto a camada APS fornece uma base para atender as aplicações ZDO e ZigBee. Os mecanismos de segurança estão presentes em três camadas da pilha de protocolos: MAC, NWK e APS. A segurança na camada MAC é baseada na definição da IEEE 802.15.4 e por parte da ZigBee com o algoritmo CCM* [Fan et al. 2017].

A camada MAC usa uma chave única para todos os níveis de segurança do CCM* (CCM* nas camadas MAC, NWK e APS). Esta é responsável por seu próprio processamento de segurança, mas a camada APL acima define quais chaves devem ser utilizadas. A APL define a chave padrão para coincidir com a Chave de Rede ativa e as Chaves de Link da camada MAC para coincidir com as Chaves de Link da Camada de Rede. A figura 8 apresenta um quadro MAC de saída no protocolo Zigbee com seu processamento de segurança [Fan et al. 2017].

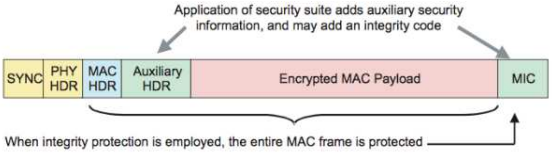


Figura 8 – Quadro ZigBee com segurança na camada MAC [Fan et al. 2017]

A NWK é responsável por prover proteção para as operações da camada MAC e fornece uma interface para a camada APL, ou seja ela é responsável pelo processamento

necessário para transmissão e recebimento dos quadros de forma segura. Quando é necessário segurança nesta camada é utilizado AES-CTR no contador aprimorado com o modo de operação CBC-MAC, as camadas superiores definem quais chaves utilizar, o contador de quadros e qual nível de segurança utilizar. Em alguns casos a camada NWK transmite e recebe mensagens de rota, ao fazer isto usa as Chave de Link, se disponíveis, caso contrário ela utilizará da Chave de Rede ativa. A figura 9 mostra um exemplo de um pacote da camada criptografado [Fan et al. 2017] [Fan 2017].

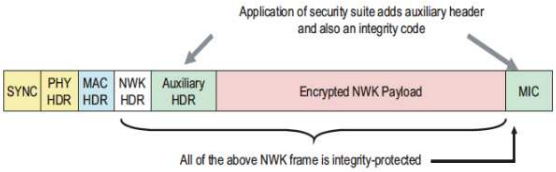


Figura 9 – Quadro ZigBee com segurança na camada NWK [Fan et al. 2017]

A camada APS é quem conduz toda a segurança relacionada as camadas da APL, ela é responsável pelas etapas necessárias para transmitir e receber os quadros com segurança, e gerenciar as chaves de criptografia, sendo que as camadas acima que emitem primitivas para a camada APS para informar o nível de segurança e quais chaves utilizar.

Na ZigBee 3.0 o protocolo pode criar um link seguro no nível da aplicação entre um par de dispositivos, estabelecendo um par de chaves exclusivos utilizando o AES-128 para quando é necessário um maior nível de segurança [Fan et al. 2017]. Este maior grau de segurança pode se utilizado para estabelecer uma Chave de Link ou uma Chave de Rede, para a atualização e status de um dispositivo. Quando um dispositivo conectado em um roteador ZigBee muda (como adicionar ou sair da rede), o roteador ZigBee fornece uma maneira segura de notificar a Central de Confiabilidade (TC - *Trust Center*) sobre a alteração do status do dispositivo. Fornece uma maneira segura para a Central de Confiabilidade notificar o nodo roteador de que um dispositivo filho precisa ser removido da rede. Para que um dispositivo ZigBee forneça uma maneira segura de outro dispositivo solicitar uma Chave de Rede ativa ou uma Chave de Link de aplicativo de ponta a ponta. Fornece uma maneira segura para o TC notificar um NK mútuo de troca de dispositivos [Fan 2017].

Um exemplo de cenário para este caso seria de uma rede doméstica que conecta vários dispositivos, como luzes, termostatos, sensores de presença, travas de portas, sensores de abertura de janelas, portas e portas de garagem. Todos esses dispositivos compartilhariam uma mesma Chave de Rede, assim a criptografia da camada APS pode ser aplicada a dispositivos como travas de portas e de garagem criando assim uma "conexão privada virtual", isso pode limitar a capacidade de um invasor, pois mesmo em posse da Chave de Rede o invasor também necessitaria da chave exclusiva dos dispositivos para atuar sobre eles. [Fan et al. 2017].

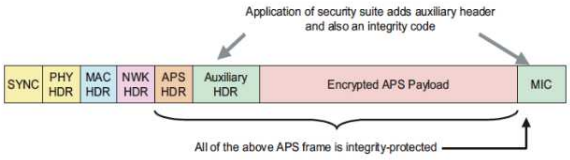


Figura 10 – Quadro ZigBee com segurança na camada APS [Fan et al. 2017]

2.2 Vulnerabilidades da Rede ZigBee

A vulnerabilidade de um nodo ZigBee depende de recursos de segurança do nível lógico tanto quando recursos de segurança incorporados ao design do produto e sua fabricação. Essas decisões juntas constroem o nível de segurança que o dispositivo terá com relação ao seu custo e facilidade de uso [NXP 2019]. Nas duas seções seguintes serão apresentadas inicialmente nove categorias criadas em [Neshenko et al. 2019] que são categorias gerais para vulnerabilidades em diversas redes IoT, e na sequência categorias de ataques voltadas para redes ZigBee.

2.2.1 Vulnerabilidades em redes IoT

Nesta seção serão apresentadas nove categorias de ataques, os ataques não estão em uma ordem de importância ou de efetividade, são apenas categorias gerais que podem ser utilizadas isoladas ou em conjunto. Ao final será apresentada a OWASp e sua classificação de vulnerabilidade para redes IoT .

- Falta de segurança física: A maioria dos dispositivos IoT opera de forma independente em ambientes autônomos. Com pouco esforço, um atacante pode obter informações não autorizadas de forma física, e assim assumir o controle deles. Uma vez com acesso ao dispositivo um invasor poderia causar danos físicos ao dispositivo, possivelmente identificando esquemas criptográficos utilizados, efetuando cópias do firmware do dispositivo usando um nodo malicioso ou corrompendo dados de controle de acesso.

  O acesso físico ao hardware pode permitir que um adversário modifique os parâmetros de inicialização, extraia a senha root, aprenda sobre informações confidenciais e ou privadas e modifique o ID de um dispositivo. Há casos onde pode permitir o roubo de arquivos de atualização, aproveitando a falta de criptografia a nível de dispositivo, e acesso a UART (*Universal Asynchronous Receiver-Transmitter*) que pode permitir acesso total ao sistema do dispositivo caso os algoritmos de hash e criptografia do sistema de arquivos não seja implementado.

- Insuficiência energética: Um fator relevante em dispositivos IoT é a energia, dispositivos têm energia limitada e não possuem necessariamente a tecnologia ou mecanismos para renová-la automaticamente. Um invasor pode direcionar ataques afim de drenar

a energia armazenada gerando inundações de requisições legítimas ou corrompidas de conexão, deixando o dispositivo indisponível para processos ou usuários válidos. Uma solução seria a coleta de energia de fontes humanas, energia elétrica de tomadas, quanto de fontes naturais como solar ou eólica, como um método adequado para capacitar os dispositivos a adotar técnicas de segurança mais complexas.

- Autenticação Inadequada: Energia limitada e poder computacional são dois grandes desafios a implementação de mecanismos complexos de autenticação. Neste caso um invasor pode usar de abordagens de autenticação ineficazes para acrescentar nodos maliciosos ou violar a integridade dos dados, invadindo dispositivos e comunicações da rede. Nesse cenário, as chaves de autenticação trocadas e empregadas também correm o risco de serem perdidas ou corrompidas, nos casos onde as chaves estão sendo armazenadas ou transmitidas com segurança, algoritmos de autenticação sofisticados, ou eficazes, tornam-se insuficientes. Embora em muitos casos a pré-instalação das chaves em cada dispositivo para um determinado modo de segurança seja possível, na realidade, as chaves são transmitidas sem criptografia tornando possível o vazamento de informações confidenciais e permitindo que um adversário obtenha controle sobre os dispositivos. Existem vários ataques que visam ganhar controle ou conduzir negação de serviço em IoT. Uma sugestão para coibir estes ataques é que a aplicação do nível "alta segurança", juntamente com a pré-instalação das chaves, ofereceria suporte à proteção de informações confidenciais.

- Criptografia Imprópria: A criptografia dos dados é de suma importância no paradigma IoT, principalmente nos casos onde operam em locais críticos, como concessionárias de energia, fábricas, automação predial, controle de acesso, etc. A criptografia é um método eficaz para armazenar e transmitir dados de uma maneira que somente usuários autorizados possam utilizá-los. Contudo a força dos sistemas de criptografia depende dos algoritmos implementados, e nesse quesito as limitações de recursos de IoT afetam a robustez, a eficiência e a eficácia de tais algoritmos. Nesse caso um invasor pode contornar as técnicas de criptografia implementadas para revelar informações confidenciais ou controlar operações com esforço limitado e viável.

- Portas Abertas: Diversos dispositivos IoT têm portas desnecessariamente abertas durante a execução de serviços, permitindo que um invasor se conecte e explore uma infinidade de vulnerabilidades.

- Controle de Acesso Insuficiente: O gerenciamento de credenciais deve proteger dispositivos e dados contra acesso não autorizado. Sabe-se que a maioria dos dispositivos IoT em conjunto com suas soluções de gerenciamento em nuvem não força uma senha de complexidade suficiente. Além disso, após a instalação, vários dispositivos não solicitam a alteração das credenciais de usuário padrão, e a maioria dos usuários pos-

sui permissões elevadas. Portanto, um adversário pode obter acesso não autorizado ao dispositivo, pode ameaçar dados e toda a rede.

- Gerenciamento de atualizações: Um sistema para atualização de software/firmware de dispositivos em operação deve ser incorporado, para uma vez identificado um problema, corrigi-los adequadamente para minimizar continuamente os vetores de ataque e aumentar suas capacidades funcionais. No entanto, abundantes casos relatam que muitos fabricantes ou não recorrem a atualizações de segurança ou não possui sistemas automatizados de atualização. Além disso, mesmo as atualizações disponíveis os mecanismos carecem de garantias de integridade, tornando-os susceptível de serem maliciosamente modificados.

- Práticas de Programação Fracas: Embora práticas de programação fortes e injeção de componentes de segurança possam aumentar a resiliência das redes, incontáveis firmwares são lançados com vulnerabilidades conhecidas, como backdoors, usuários root como pontos de acesso principais e a falta de uso do *Secure Socket Layer* (SSL) . Portanto, um adversário pode facilmente explorar os pontos fracos de segurança conhecidos para causar estouros de buffer, modificações de informações ou obter acesso não autorizado ao dispositivo.

- Mecanismos de Auditoria Insuficientes: Uma infinidade de dispositivos de IoT carece de procedimentos completos de registro, tornando possível ocultar atividades maliciosas geradas.

O *Open Web Application Security Project* (OWASP) é uma organização sem fins lucrativos focada em melhorar a segurança de softwares. Com foco em tornar a segurança de softwares algo visível, para que indivíduos e organizações possam tomar decisões com informações. A OWASP fornece informações práticas e imparciais a indivíduos, empresas, universidades, agências governamentais e outras organizações em todo o mundo. Operando como uma comunidade de profissionais com ideias semelhantes, a OWASP emite ferramentas de software e documentação baseada em conhecimento sobre segurança de aplicativos. Qualquer pessoa pode participar da OWASP e todos os materiais estão disponíveis sob uma licença de software aberta e gratuita [OWASP 2019]. A figura 11 apresenta uma comparação entre os dez principais ataques a redes IoT em 2014 e 2018.

Com base na imagem podemos verificar os ataques mais comuns a redes IoT de acordo com o OWASP e a mudança significativa que houve no direcionamento dos ataques de 2014 para 2018. Destaques podem ser visto como a remoção do TOP 1 de 2014 *Insecure Web Interface* e em seu lugar entrando *Weak Guessable*, ou *Hardcoded Passwords*, e o Top 2 de 2018 se tornando *Insecure Network Services* o que mostra que os serviços de redes estão se tornando muito mais inseguros.

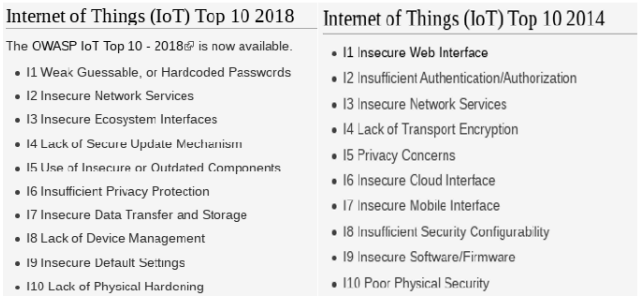


Figura 11 – OWASP TOP 10 - 2018/2014 [OWASP 2019]

2.2.2 Ataques nas Redes ZigBee

Existem dois grandes grupos de ataques, os ataques ativos que requerem um ataque real de interceptação da rede onde o adversário pode modificar os dados ou injetar quadros de falha na rede. Neste modelo a rede é afetada negativamente, além disso a integridade e autenticidade dos dados transmitidos na rede é comprometida. Por sua vez os ataques passivos não buscam a interceptação real da rede mas sim a captura do tráfego, sem a intenção de denegrir as capacidades da rede ou compromete a integridade dos dados. Contudo a confidencialidade das informações é prejudicada uma vez que informações privadas podem ser coletadas para alguma outra finalidade.

Os ataques as camadas visão explorar falhas na sua arquitetura ou comunicação. A camada de transporte é utilizada para oferecer suporte a links de comunicação para dispositivos que acabaram de ingressar na rede. Os ataques podem incluir desde inundações de requisições de entradas a rede, onde o nodo de destino é sobrecarregado por uma grande quantidade de solicitações inválidas de estabelecimento de conexões (ataque de inundação). Até dessincronização onde se forja pacotes para uma ou ambas as extremidades da conexão, para que o host solicite a retransmissão dos quadros de pacotes perdidos. Ambos os ataques visam denegrir a capacidade da camada de transporte, assim impedindo que novos nodos reais entrem na rede, que haja grande perda de pacotes e por conta de todo o processamento requerido a consequente diminuição da vida útil das baterias dos dispositivos.

A camada de rede é responsável pelo processo de roteamento e pelo tráfego de rede. Os ataques podem incluir buracos de minhoca e ataques de encaminhamento seletivo. No ataque do buraco de minhoca; deve haver dois nodos maliciosos localizados em diferentes saltos da rede. Quando um nodo emissor transmite um quadro de dados, um nodo malicioso encapsula esses dados para outro nodo malicioso e pelo qual os envia para os nodos vizinhos. Consequentemente, o nodo remetente é enganado, pois os nodos maliciosos estão próximos de um ou dois saltos, onde esses dois nodos maliciosos podem estar fora do alcance.

Incorpora o cabeçalho MAC que ajuda o receptor a saber o tamanho do pacote, retransmite os quadros em caso de erros e aloca recursos para os nodos recém-ingressados. O atolamento da camada de link é um exemplo de ataques da camada MAC lançados

para criar DoS (*Denial of Service*) interrompendo a troca de mensagens entre nodos de transmissão e recepção. Isso degradaria e reduziria o desempenho da rede. Por fim os ataques a camada física visão explorar principalmente o sinal de rádio comum, bloqueando ou interceptando ou violando os quadros de pacotes de dados.

Por seguinte temos os ataques com alvo, estes modelos de ataques visão buscar uma falha específica da rede como os ataques de afundamento, (do inglês *Sink Attacks*). Podem ocorrer quando um nodo malicioso anuncia uma rota para ser o caminho mais curto e como todos os algoritmos de roteamento selecionam o caminho mais curto, ele atrai mais tráfego de rede para ser direcionado para ele, possibilitando que mais informações sejam capturadas. Geralmente, esse ataque é combinado com um ataque de buraco de minhoca (do inglês *WarmHole*).

Outro modelo de ataque é o de origem, nesses ataques, o adversário compromete um nodo legítimo da rede para atuar como um tipo de nodo do buraco negro; nesse ataque o nodo começa a descartar seletivamente pacotes recebidos ou todos os pacotes recebidos para induzir outros nodos vizinhos a procurar outra rota, como a anterior falhou.

O ataques dos vizinhos explora o processo de descoberta de outros nodos vizinhos das redes transmitindo a mensagem que inicializa o processo de comunicação. Um nodo mal intencionado envia uma mensagem de inicialização de comunicação com alta potência de transmissão e, portanto, os nodos receptores consideram esse nodo como seu vizinho e, em troca, enviarão os dados do pacote detectado. Consequentemente, uma enorme quantidade de energia será desperdiçada e congestionamentos podem ocorrer consequentemente.

Ataques de membros às vezes são chamados de ataques de párias e internos. No caso de ataques de párias; o nodo invasor não faz parte da rede, mas pode ameaçar a rede. Por outro lado, o ataque interno ocorre quando um nodo malicioso faz parte da rede, comprometendo a rede ou quando o atacante carrega um perfil falso e requisita a entrada na rede.

Por fim, os ataques por esgotamento de energia onde o atacante envia mensagens falsas para atrair o nodo a fim de intencionalmente esgotar a energia por cálculos redundantes relacionados à segurança. Isso reduzirá a vida útil do nodo e permitirá que o invasor inicie vários ataques após o esgotamento como DoS.

Vale ressaltar que esses ataques podem ser utilizados isoladamente, contudo frequentemente são utilizados em sequência ou combinados dependendo do grau de complexidade e do modelo de segurança da rede, para que o invasor possa atingir seus objetivos. A figura 12 apresenta um esquema simples para todos os ataques apresentados nesta seção. [Khanji, Iqbal e Hung 2019].

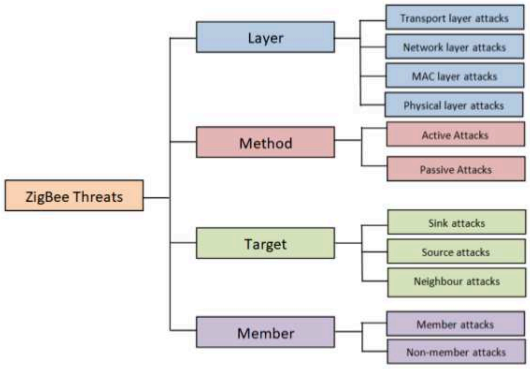


Figura 12 – Modelo de Ameaças ZigBee [Khanji, Iqbal e Hung 2019]

2.3 killerBee

Criado por Joshua Wright o KillerBee é um framwork para efetuar ataques as redes ZigBee e IEEE 802.15.4. Esse framework simplifica a detecção e a injeção de tráfego na rede, ao lado da decodificação e manipulação de pacotes. Fornece um firmware modificado para os transceptores USB ZigBee, uma vez carregado, o usuário tem controle total sobre o stick USB e pode capturar e enviar pacotes ZigBee. Sendo que o framework inclui as seguintes ferramentas :

- zbassocflood: Associa repetidamente ao PANId de destino, em um esforço para causar uma falha no dispositivo devido a muitas requisições de conecção.
- zbconvert: Converte uma captura de pacote da libpcap para o formato Daintree SNA ou vice-versa.
- zbdsniff: captura o tráfego do ZigBee, procurando quadros NWK e provisionamento de chave sem fio. Quando uma chave é encontrada, zbdsniff imprime a chave em stdout.
- zbdump: Uma ferramenta parecida com o tcpdump para capturar quadros IEEE 802.15.4 em um arquivo de captura de pacote libpcap ou Daintree SNA. Não exibe estatísticas em tempo real, como tcpdump, quando não está gravando em um arquivo.
- zbfind: um aplicativo GTK GUI para rastrear a localização de um transmissor IEEE 802.15.4 medindo o RSSI. O Zbfind pode ser passivo na descoberta (apenas escuta pacotes) ou pode estar ativo enviando quadros de solicitação de beacon e gravando as respostas dos coordenadores e coordenadores dos roteadores ZigBee.
- zbgoodfind: implementa uma função de pesquisa de chave usando uma captura de pacote criptografada e despejo de memória de um dispositivo ZigBee ou IEEE 802.15.4 legítimo.

- zbid: identifica interfaces disponíveis que podem ser usadas pelo KillerBee e ferramentas associadas.
- zbreplay: implementa um ataque de repetição, lendo um arquivo de captura de pacote Daintree DCF ou libpcap especificado, retransmitindo os quadros. Os quadros ACK não são retransmitidos.
- zbstumbler: ferramenta ativa de descoberta de rede ZigBee e IEEE 802.15.4. O Zbstumbler envia os quadros de solicitação de beacon ao saltar, gravar e exibir informações resumidas sobre os dispositivos descobertos.

3 Proposta Inicial e Dificuldades no desenvolvimento

Este capítulo apresenta a proposta inicial, as configurações do KillerBee, da placa EFR32 e as dificuldades enfrentadas na configuração da ferramenta.

3.1 Proposta Inicial

Este trabalho teve como objetivo prático a realização de alguns ataques sobre uma rede ZigBee para verificação dos quesitos de segurança implementados. A rede confiável seria construída sobre a topologia de *cluster tree*, contudo, pela limitação de dispositivos, com apenas um cluster. Em relação aos quesitos físicos seria composta por: um gateway ZigBee, um device somente com a capacidade de roteamento, logo ele não atuaria como um *Trust Center* ficando essa responsabilidade somente para o gateway, os dois outros dispositivos fariam apenas o papel de coletores de informações do meio. Ambos os dispositivos teriam duas entradas RJ11 para sondas diversas, uma entrada USB ou duas pilhas do modelo AA para alimentação e um barramento lateral para sondas de extensão, a comunicação entre os dispositivos e entre os dispositivos e o gateway seria feito através do protocolo 802.15.4 definido pela IEEE. A figura 13 exemplifica o modelo da rede.

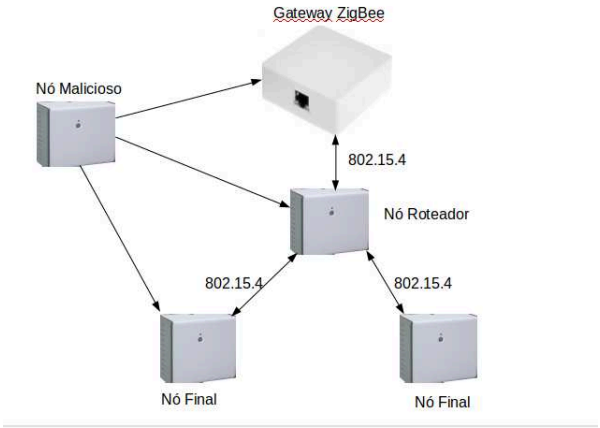


Figura 13 – Modelo da rede do experimento Autor

Com essa rede como base, seria criado um dispositivo malicioso utilizando para isso um Rapberry Pi como base física, a ferramenta killerBee e o sistema operacional Raspbian como base lógica. Uma vez o nodo malicioso construído, um conjunto de ataques seriam executados contra a rede a fim de testar pontos de vulnerabilidades utilizando-se para isto das diversas ferramentas disponibilizadas pelo KillerBee.

3.2 Configuração do KillerBee

A parte prática visava efetuar ataques contra uma rede zigbee, utilizando para isto a ferramenta opensource KillerBee . [Riverloop 2020]. Este software dá suporte, entre outros, a alguns hardwares da Silicom Labs que sejam capazes de executar o Silicon Labs Node Test 2.4GHz e SubGHz. Entre estes hardwares está a EFR32, está o qual o aluno possuía acesso juntamente com um Mighty Gecko SoC 12, rádio que permite o envio de pacotes ZigBee. Uma vez a placa configurada e conectada por micro USB permitiria o envio de comandos a partir do KillerBee para a placa e então a placa passaria os pacotes à rede.

Como descrito pela página do killerBee, é necessário alterar algumas configurações para que a placa possa ser reconhecida. Antes de instalar o programa acesse "killerbee/config.py"e altere para "True"a opção para a sua placa. A figura 14 apresenta a configuração padrão do KillerBee e a figura 15 à configuração que pode ser aplicada. Na configuração da figura 15 irá fazer o KillerBee buscar por todos os dispositivos ao qual a ferramenta dá suporte.

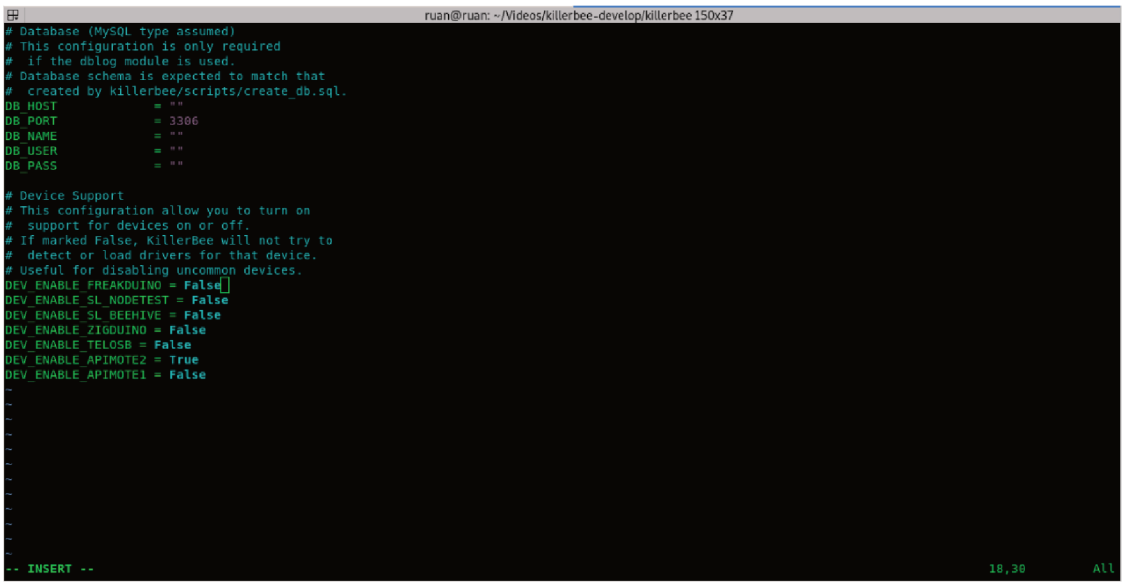


Figura 14 – Configuração padrão do KillerBee Autor

Para instalação utiliza-se o comando “python setup.py install”. Após isso foi iniciado a configuração da placa, visto que a placa não pertencia ao aluno a interação com a mesma foi limitada.

3.3 Configuração da EFR32

A configuração da placa, que inicialmente estava configurada como um dipositivo BLE, iniciou pelo download do SimpliciyStudio [Silicon-Labs 2020], após isto, a instalação

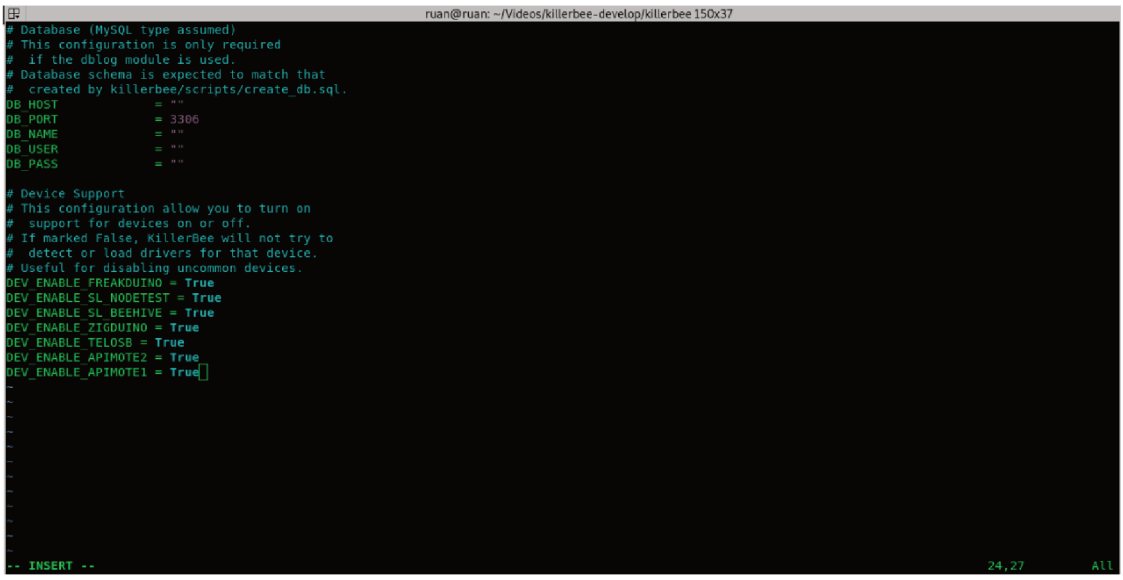


Figura 15 – Configuração alterada do KillerBee Autor

do software de acordo com as preferências do usuário e inicialização. Na primeira inicialização do software é requerido que o usuário faça o login para ter acesso aos softwares proprietários disponibilizados pela empresa, neste caso isso se faz necessário para instalação do pacote que possui a pilha ZigBee nomeada de EmberZNet. O processo de instalação é simples e pode ser feito instalando todo o pacote ZigBee.

Uma vez inicializado é efetuada a conexão da placa pela interface micro USB da EFR32, e o SimplicityStudio já irá reconhecer uma interface, nesse ponto é aconselhável certo cuidado pois o Simplicity Studio pode identificar outros dispositivos conectados ao USB, como um conversor USB-Serial, enquanto um mouse ou teclado não serão listados. A figura 16 apresenta a placa EFR32MG12 e algumas de suas interfaces e a figura 17 apresenta a primeira conexão da placa após os passos citados.

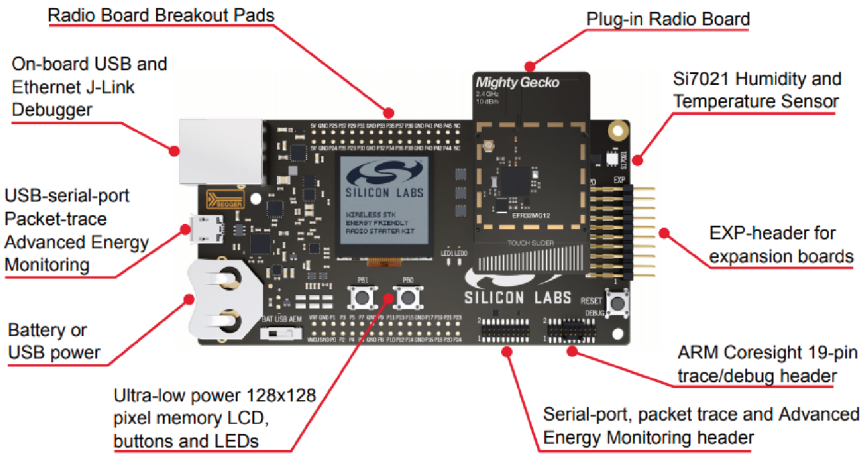


Figura 16 – Placa EFR32MG12 e suas interfaces Autor

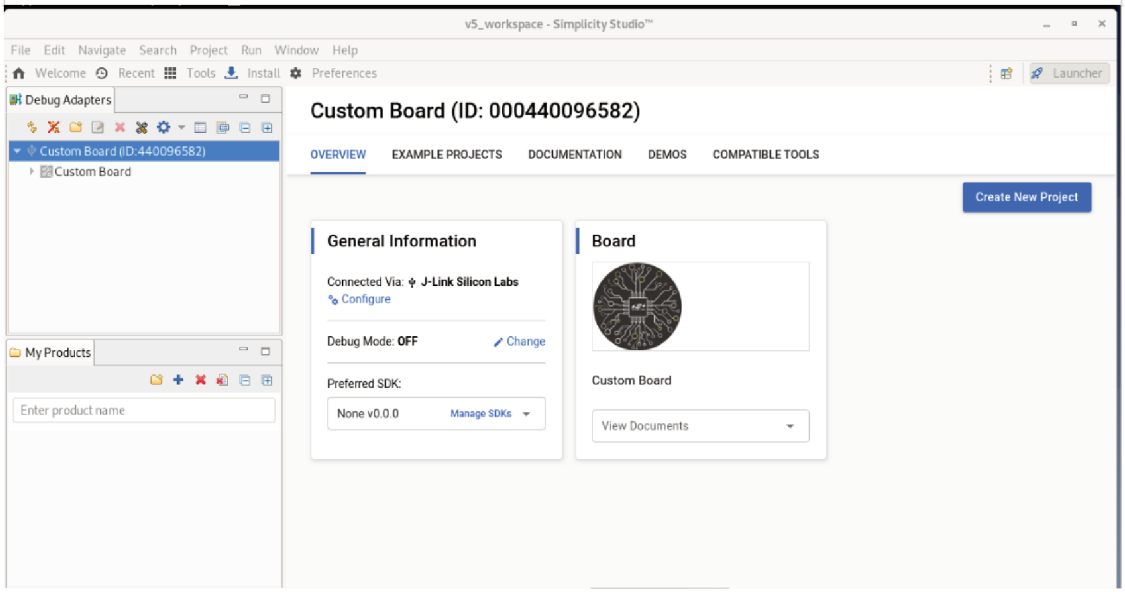


Figura 17 – Identificação Inicial da placa pelo SimplicityStudio Autor

Neste ponto já é possível verificar o número identificador da placa na parte superior da figura 16, contudo o modelo e outras informações não foram identificadas. Isso acontece por que o modo "DEBUG" vem desligado por padrão, assim no quadro "General Information" selecione "Change" ao lado de "Debug Mode OFF" isto irá abrir uma nova tela para configuração do hardware, nas abas superiores selecione a aba "Adapter Configuration" e altere a configuração do campo "DEBUG MODE" para "MCU", a figura 18 apresenta a tela e a configuração.

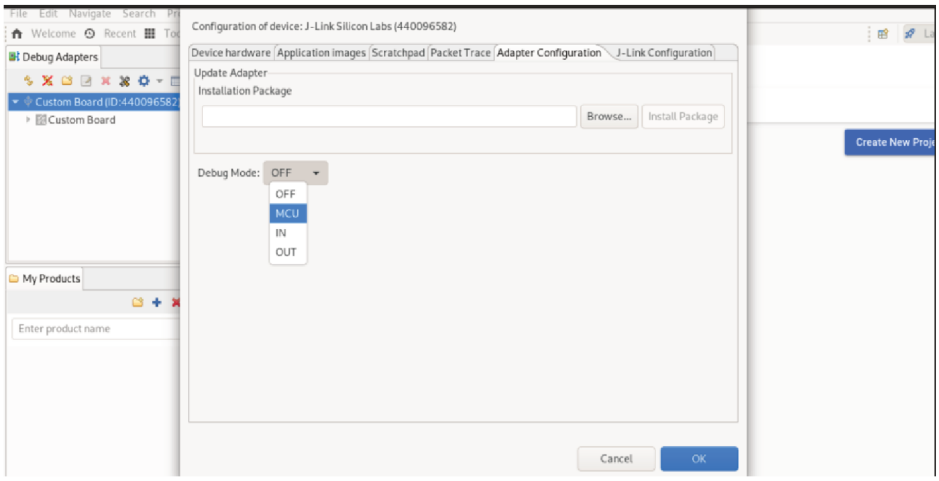


Figura 18 – Configuração do modo de debug Autor

Após a configuração do modo de debug a tela inicial apresenta todas as configurações da placa, figura 18, na parte superior são apresentados a identificação do modelo da placa e as informações do rádio ao invés de "Custom Board" e ao lado esquerdo na aba "Debug Adapters" são apresentadas informações específicas da placa e as possibilidades de

configurações. Ao rolar para baixo a tela central, figura 19, são apresentadas imagens da placa, do rádio do chip.

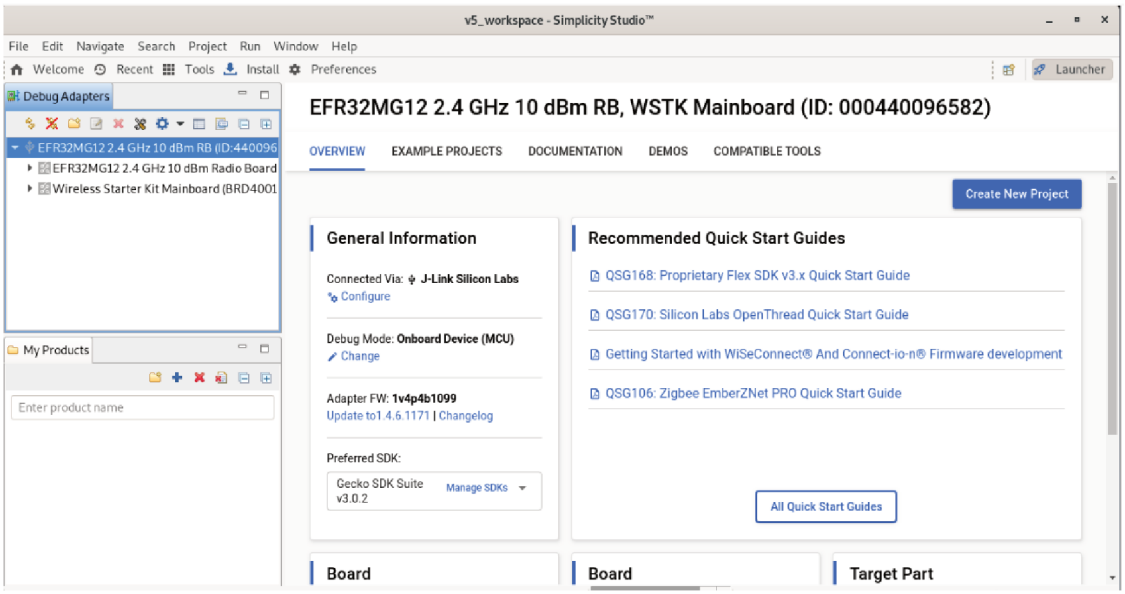


Figura 19 – Identificação das configurações placa Autor

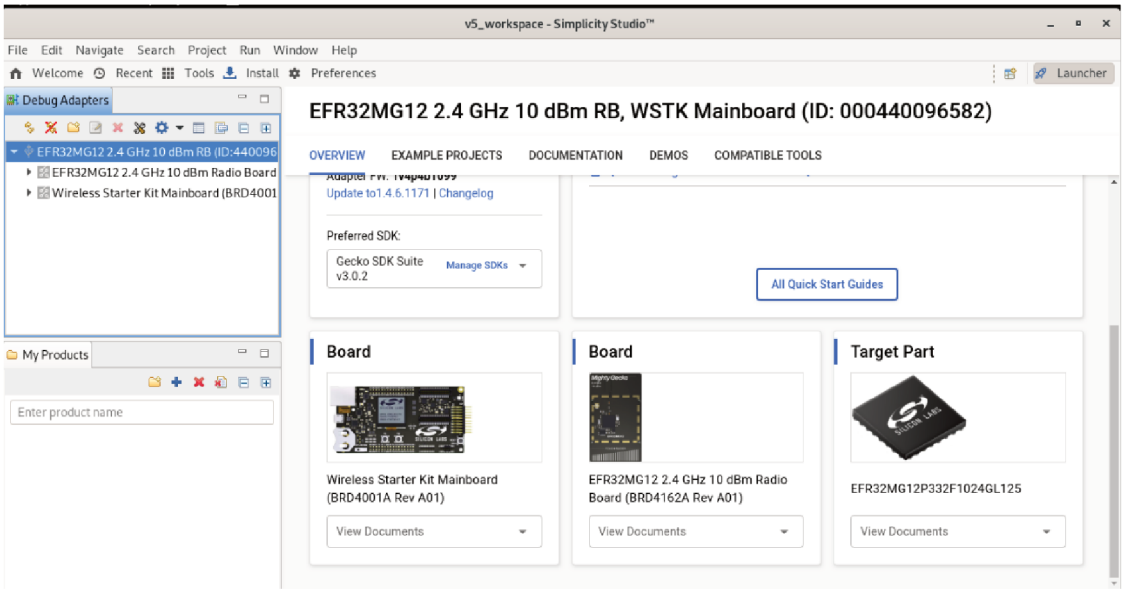


Figura 20 – Caracteríscas de cada componente Autor

Caso haja algum problema em uma instalação inicial do EmberZnet, a guia logo abaixo de “Debug Adapters” selecione “Install”. Na nova tela apresentada selecione a aba “SDKs” e procure por EmberZNet, na parte superior da guia é possível utilizar alguns filtros. A figura 20 apresenta a tela e os filtros selecionados.

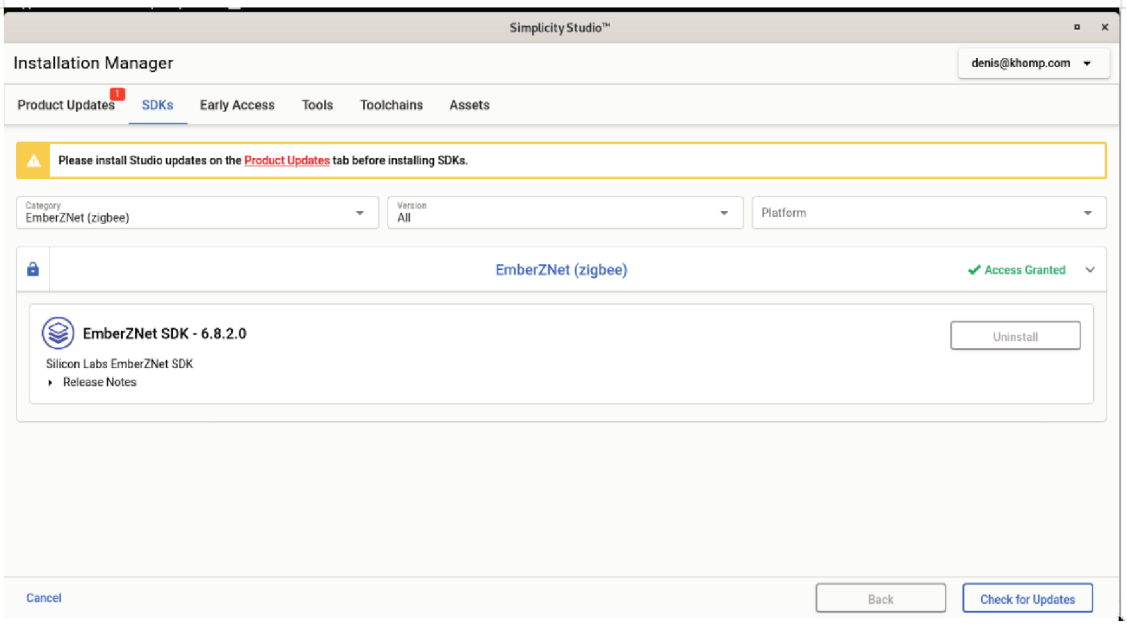


Figura 21 – Instalação do EmberZNet Autor

3.4 Dificuldades

O primeiro problema foi ao tentar gravar o bootloader na placa, a partir da versão 6.1, pois, o EmberZNet não mais prove um bootloader padrão para a a EFR32, sendo assim seria necessário criar um novo . [Silicon-Labs 2020], além disso o tutorial apresenta um exemplo de como criar um bootloader para um modelo semelhante de placa. Após algum estudo sobre as configurações da placa a ser utilizada foi criado e gravado um novo bootloader na placa para dispositivos ZigBee.

Após isso seria necessário gravar o Node Teste, através do tutorial . [Silicon-Labs 2020] apresenta uma sequência de passos para a gravação, contudo ao executar os passos no momento de identificar o Node Test para a EFR32 o mesmo não era mais identificado, apenas eram apresentados corretamente o Node Test para outros modelos de placas, a figura 22 apresenta o momento da tentativa de identificação.

O Node Test é um software proprietário e fechado da Silicom Labs, só é possível acessá-lo através do Simplicity Studio. Uma vez que todos os testes na versão atual não surtiram efeito e a tentativa de encontrar um Node Test compatível em versões mais antigas do EmberZNet falharam. Foi requisitada ajuda a um colega de trabalho que possuía uma versão mais antiga do Silmplicity Studio instalada a fim de verificar se nos arquivos ainda havia o NODE TEST para a EFR32, mas sem sucesso também. Então pelo caminho dos arquivos foi encontrado o que poderia ser o NODE TEST para o modelo da placa, ao executar a gravação e pelos logs foi possível verificar que a placa havia sido gravada. Contudo apesar de todos os testes e tentativas não foi possível fazer com que o KillerBee identificasse ou se comunicasse com a placa através do comando “zbid”, comando utilizado

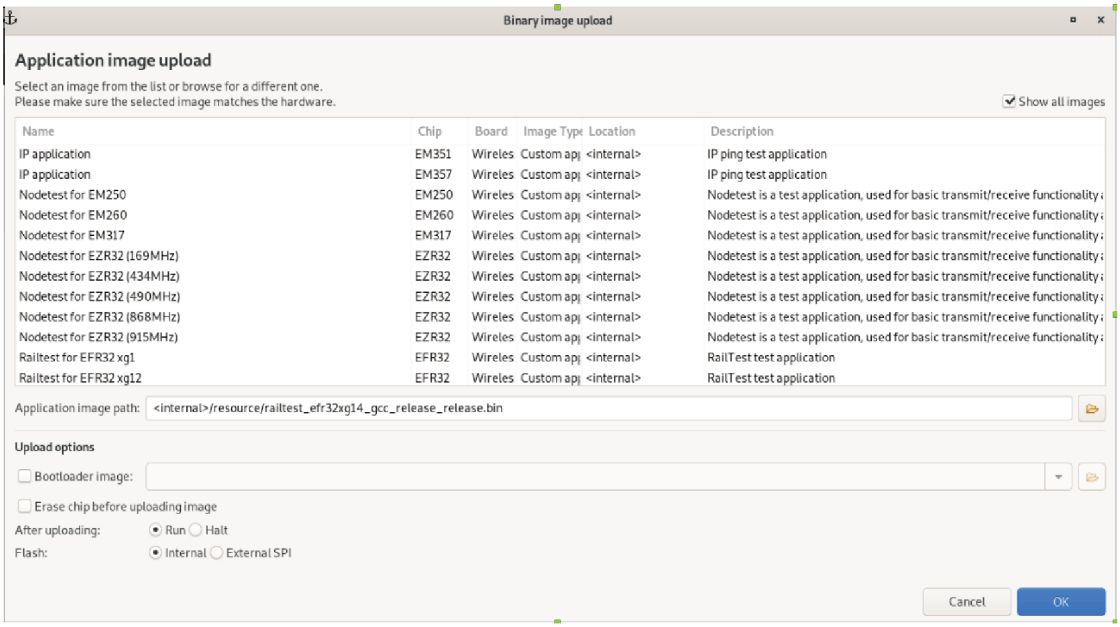


Figura 22 – Apresentação dos Node Test e modelos de placas Autor

para identificar o modelo da placa, utilizar o sniffer de rede ou qualquer outro comando.

Todos estes problemas foram agravados por conta da situação social, a pandemia, que impossibilitou a ida a empresa, uma vez que foi acordado que o aluno poderia utilizar a placa quando ela não estivesse em uso e fora do horário de trabalho. Com o começo do home office por parte das empresas os colabores levaram seus materiais de trabalho para casa, fazendo com que o acesso a placa fosse escasso. Além desses fatores o alto valor agregado da placa limitou os teste por receio de causar alguma avaria ao produto..

3.5 Nova Proposta

Assim o trabalho foi adaptado para apresentar o custo de um ataque feito utilizando a ferramenta KillerBee, mas desta vez utilizando o hardware Atmel RZ Raven USB (Universal Serial Bus) sticks (RZUSBs), o cenário do ataque é apresentado no artigo [Olawumi et al. 2014]. Além disso, será apresentado a busca por dispositivos seguros e como identificar possíveis falhas de segurança para montagem de uma rede ZigBee para uma casa inteligente.

4 Custo e dispositivos

Este capítulo apresenta uma análise de custo e conhecimento necessários para realização de um ataque a uma rede ZigBee, seguindo do estudo de dois dispositivos ZigBee, sendo o primeiro uma câmera inteligente da empresa Lumi United Technology e o segundo o dispositivo multipropósito Echo Plus da Amazon.

4.1 Custo de um ataque

Em [Olawumi et al. 2014] são apresentados três ataques a uma rede zigbee utilizando um Atmel RZ Raven USB (Universal Serial Bus) sticks (RZUSBs), em 2014 quando o artigo foi publicado, é dito que somente o device teve um custo de 40 dólares. O firmware padrão do RZUSB pode ser usado para implementar um sniffer para uma rede ZigBee, atuar como um coordenador de rede de uma PAN – *Personal Area Network* ou como um ZigBee End-Device. Se o invasor usar dois dispositivos RZUSB é possível realizar à detecção e a modificação/injeção de pacotes ao mesmo tempo. Isso requer que o segundo dispositivo RZUSB use um firmware modificado, o KillerBee que suporta modificação e injeção de pacote, a figura 23 apresenta um RZUSB.

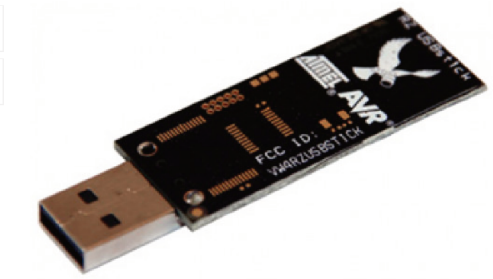


Figura 23 – RZUSB Stick . [Element14 2020]

Atualizar o RZUSB com um novo firmware, que pode realizar outros ataques com o KillerBee, não é um processo simples, pois requer uma outra peça de hardware conhecida como um programador on-chip, como Atmel JTAGICE mkII. O Atmel JTAGICE mkII foi projetado para funcionar com microprocessadores AVR como o AT90USB1287 usado no stick USB Atmel RZ Raven. Apesar de não ser citado o preço do hardware no artigo, em uma pesquisa foi possível encontrar o mesmo hardware por volta de 130 dólares na Amazon. Ao pesquisar o fornecedor oficial, foi identificado que ambos os hardwares pertencem a MicroChip, e que esses produtos não são mais fabricados, como apresentados na figura 24 o RZUSB e na figura 25 o JTAGICE.

Figura 24 – Kit de desenvolvimento RZRAVEN . [MicroChip 2020]

Figura 25 – Gravador On-Cip AVR JTAGICE mkII . [MicroChip 2020]

Assim para realizar um ataque à uma rede Zigbee será necessário um certo investimento, além de algum conhecimento sobre como gravar hardware. É importante ressaltar que o RZUSB é um dispositivo do tipo USB, ou seja é necessita de alimentação, envia e recebe dados por ela. Logo para efetuar um ataque utilizando este dispositivo seria necessário algum outro hardware para acoplar o RZUSB como uma Raspberry. Este investimento financeiro, tempo necessário e as condições para efetuar um ataque já são fatores que podem desestimular um atacante.

4.2 Dispositivos ZigBee

Existem diversos produtos para casas inteligentes, e estes implementam uma vasta quantidade de protocolos. Os protocolos mais comuns na indústria de varejo são : ZigBee, Z-Wave, Bluetooth Low Energy, Bluetooth e Wi-Fi. Existem dispositivos que possuem mais de um protocolo, sendo que quanto mais maneiras de se acessar o dispositivo mais caro ele é, pois necessita de hardware e software mais complexos, e também se tornam vulneráveis a mais tipos de ataques, por outro lado podem ser acessados de várias maneiras facilitando seu uso doméstico.

A escolha do protocolo correto define muito da estrutura da rede da casa, dispositivos ZigBee e Zwave necessitam de um gateway para enviar mensagens a uma nuvem e então através de uma aplicativo acessar as informações, enquanto dispositivos Bluetooth e Wi-Fi não necessitam diretamente de um gateway podendo ser acessados por um smartphone ou por um computador. Dispositivos ZigBee e Z-Wave levam vantagem por um baixo consumo de energia, podendo manter suas funcionalidades por meses ou até mesmo anos utilizando-se de 2 pilhas AA. Esse tempo dependerá de suas configurações e principalmente do tempo entre envio de mensagens, sendo que muitos dispositivos também dispõe de alimentação através de uma entrada externa de energia, sendo as pilhas utilizadas apenas

para suporte em caso de falta de energia. Outro fator importante para redes ZigBee é sua capacidade de se auto organizar e por sua capacidade de trabalhar como redes mesh. Assim apesar de uma alcance restrito, cerca de 30 metros, dispositivos roteadores podem estender a rede, e caso um desses nodos roteadores fique inoperante os dispositivos irão procurar outro caminho para continuar enviando seus dados de forma automática.

Vários desses padrões sem fio usam a mesma frequência (ZigBee, Bluetooth e Wi-Fi) e normalmente interferem uns nos outros. Para pequenos pacotes de dados como a maioria dos sensores envia, isso não representa um problema se o dispositivo específico permanecer em um ambiente doméstico normal.

Na momento da compra dos dispositivos que irão compor à rede doméstica é importante se certificar de que os dispositivos possuam criptografia e de que elas estejam ativadas por padrão, pois a ativação da criptografia pode impedir as tentativas de comprometer dados confidenciais dos dispositivos. Também é importante verificar todas as configurações padrão dos dispositivos e saber como modificá-las, isso permite ao usuário personalizar as características que melhor atendam às suas necessidades, mantendo a sua privacidade e segurança pessoal intacta. É preciso ler com atenção o manual de instalação e funcionamento e buscar mais informações técnicas, se necessário.

Contudo a maior parte dos produtos vendido a varejo não possuem tais informações de maneira fácil e acessível ao público geral, informações das configurações das chaves de segurança ou como alterá-las são ainda mais difíceis de encontrar pois requerem um certo grau de conhecimento por parte do usuário e isso faria com que os produtos fossem menos amigáveis, além da maior parte da população não possuir conhecimento sobre tais configurações e sua importância.

As vantagens do ZigBee neste cenário são que o protocolo não usa endereçamento IP . Portanto, deve haver um gateway ZigBee instalado para se comunicar com a Internet e os serviços em nuvem. Como a maioria dos telefones, tablets e computadores não tem a capacidade de se comunicar com dispositivos Zigbee, os gateways também são necessários para se comunicar com eles. Isso já inclui um maior nível de segurança a rede doméstica, visto que para um atacante conseguir acesso aos dispositivos precisará ter acesso a um rádio ZigBee para efetuar ataques diretos a sua rede, ou conseguir acesso ao gateway da residência. Por outro lado a necessidade de um gateway pode dificultar e encarecer um pouco o custo da rede, por conta disso ao escolher um dispositivo é importante verificar com quais gateways ele é capaz de se comunicar.

Outra característica importante é verificar se o dispositivo tem a capacidade de rotear outros para uma expansão da rede, a versão do dispositivo pois o padrão ZigBee permite diferentes "perfis"como os proprietários do fabricante. Por conta desses perfis nem todos os dispositivos são capazes de se comunicar ou usam os mesmos esquemas de endereçamento. Dispositivos que usam outros perfis ZigBee podem ser capazes de se

conectar à rede, mas suas comunicações podem não ser entendidas, ou eles podem cair frequentemente porque não recebem a mensagem de handshake que estão esperando.

4.3 Câmera Zigbee

Um exemplo de dispositivo é a câmera de segurança ZigBee da Lumi United Technology, apresentada na figura 26, pela tela inicial do produto na Amazon não é possível identificar a versão do protocolo ZigBee implementada, já na na descrição do produto é possível verificar que ela é compatível com o Apple HomeKit, ou utilizando o aplicativo Aqara Home a partir de um dispositivo como smartphone ou tablet, logo é possível acessar as informações da câmera de diversas maneiras. Uma das coisa que chama a atenção nesse dispositivo é a palavra hub na sua descrição que indica que o dispositivo é capaz de rotear informações de outros dispositivos para uma nuvem.

Figura 26 – Câmera de segurança G2h Lumi United Technology . [Lumi-United-Technology 2020]

Com um modelo que satisfaça às necessidades, foi iniciada a busca pelas características específicas do produto, pelo modelo foi possível encontrar o site da fabricante, e no site foi encontrado o manual do usuário do dispositivo . [Lumi-United-Technology 2020].

No página principal da fabricante são apresentadas mais informações do produto, como a capacidade de roteador no máximo outros 64 dispositivos e que todos esses dispositivos devem ser da mesma marca, logo ele não será capaz de rotear dispositivos de outros

fabricantes o que limita a rede a um mesmo fabricante. Na página são apresentados outros dispositivos que podem ser roteados como sensores de vibração, sensores de movimento, sensores de porta e janela e sensores de vazamento de água.

Ao inspecionar o site foi verificado que o produto possui o selo da ZigBee Alliance, esse selo garante que o produto passou por uma série de testes por parte da ZigBee e que foi aprovado recebendo assim esse certificado, produtos que não são certificados pela ZigBee geralmente são apresentados no mercado como compatíveis com 802.15.4 ou como compatíveis com Zigbee, e não podem usar o nome ZigBee, a figura 27 apresenta a figura do dispositivo com o selo ZigBee.

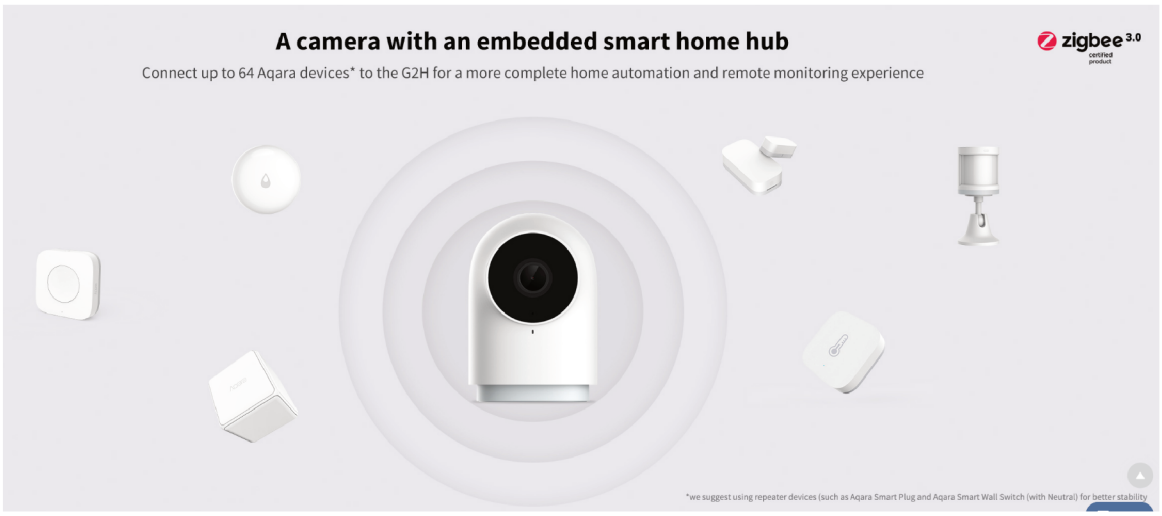


Figura 27 – Câmera de segurança G2h Lumi United Technology com Selo ZigBee . [Lumi-United-Technology 2020]

Na página há algumas informações que necessitam de uma leitura atenta para serem encontradas, como na figura 27, no canto inferior direito é citado a recomendação do uso de outros dispositivos que também tem a capacidade de roteamento para maior estabilidade da rede, isso mostra que é possível montar uma rede no padrão de cluster tree. Em outra parte da página é citado que é necessário IOS, Ipad OS ou tvOS 14 ou superior para acessar informações do dispositivo, indicando que o dispositivo só se conecta a dispositivo Apple. Também é apresentado que o dispositivo possui um sistema de criptografia ponto a ponto e outras funcionalidade de segurança, e que possui a certificação da Apple HomeKit nos quesitos de segurança.

Nesse ponto por conta do produto alegar possuir duas certificações de duas grandes empresas o próximo passo foi a verificação dos certificados . [ZigBee-Alliance 2020]. A ZigBee Alliance disponibiliza em seu site uma página para verificação de produtos certificados, onde uma busca por "G2H" já apresentou o produto. Ao analisar as informações da página, o link disponível do fabricante da câmera leva ao mesmo site onde foi encontrado o manual do usuário, mostrando que a câmera realmente é produzida pela Lumi United Technology.

A figura 28 apresenta o que é retornado pela busca como: o número de certificado na ZigBee Alliance, a data da certificação entre outros.

Camera Hub G2H

By Lumi United Technology Co., Ltd.

The Aqara Camera Hub G2H is a 1080P Full HD Camera with two-way audio and night vision, it is designed to help you look after your home and family even you are away from house. With motion detection and alert system, it helps you keep an eye on what matters in your home.

visit Lumi United Technology Co., Ltd. website.

Specifications

SKU	AC004USW01/AC004EUW01/AC004UKW01
Firmware Version	0x00000001
Hardware Version	0x00000001
Certificate ID	ZIG20276ZB330769-24
Certified Date	10/12/2020
Compliance Document	Download Compliance Document
Product has successfully completed TIS/TRP testing	No

Figura 28 – Certificado ZigBee para a G2H . [ZigBee-Alliance 2020]

O produto possuir um certificado junto a ZigBee Alliance válido mostra que ele passou nos testes e possui as funcionalidades descritas, contudo ao efetuar ao baixar os documentos de conformidade, disponíveis na página do certificado, nenhuma informação sobre quesitos de segurança foi identificado. Além disso os documentos são muito complexo e de difícil leitura o que um usuário sem conhecimentos mais avançados sobre a plataforma não teria.

Voltando a página inicial do produto foi efetuado o download do manual do usuário para verificar se havia alguma informação sobre segurança, contudo no documento não são citadas informações sobre segurança, contudo algumas outras informações sobre o produto são interessantes para as redes ZigBee. O primeiro é que o produto é fixado a sua base por uma base magnética, isso pode ser um pouco perigoso visto que agindo como hub da rede caso ele acabe por cair e se danificar ou mesmo seja retirado manualmente do seu local toda a rede pode ficar comprometida, outro fator nesse sentido é que o produto funciona de -10 à 40 graus Celsius, visto que em alguns estados brasileiros as temperaturas podem ultrapassar a temperatura superior o dispositivo pode para de funcionar.

Outro fator é que não foi encontrado em momento algum no manual alguma informação de como alterar chaves de segurança, apenas de como adicionar um dispositivo a rede que se faz de maneira automática, isso mostra que o dispositivo não possui essa funcionalidade. Não foi encontrado também uma descrição de como atualizar o dispositivo, e nos documentos do certificado ZigBee, foi verificado que o produto não envia as informações de versão do software ou hardware. Com o fato que não haver trocas de chaves acredita-se que todos os dispositivos da linha utilizem as mesma chaves de segurança ou ao menos a

Master Key para uma primeira conexão, o que deixa a rede bem mais insegura visto que caso alguém consiga a chave possa se conectar a sua rede, sendo que a proteção ficaria restrita a abertura da rede. Por fim o trecho que mais chamou a atenção no manual do usuário, apresentado na figura 29, que apesar de vender o produto como para segurança em vários momentos isenta complementa a empresa caso ocorra uma falha no produto nesse sentido.

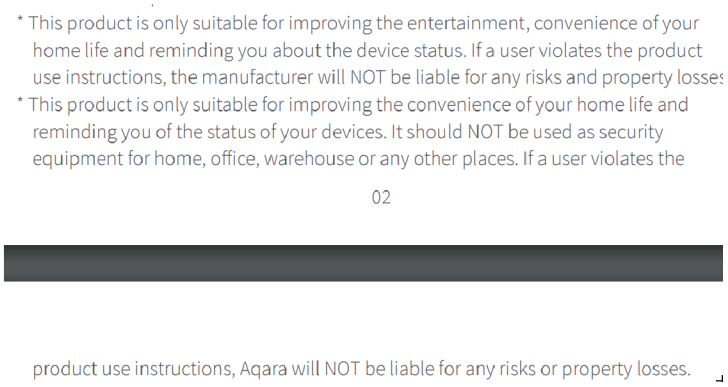


Figura 29 – Manual do usuário do produto . [Lumi-United-Technology 2020]

4.4 Hub ZigBee

O gateway é o dispositivo que irá funcionar como o concentrador, ou seja o elemento da rede que será responsável por intermediar a comunicação entre os dispositivos e o usuário. Logo ele é o principal elemento da rede, é ele quem irá controlar toda a rede, uma vez que os dispositivos tem que entrar na rede gerada pelo concentrador. È ele quem irá gerenciar todo o esquema de chaves e autenticação dos dispositivos na rede, assim escolher um gateway depende de algumas características.

O primeiro fator é verificar se os dispositivos da sua casa utilizam somente o protocolo ZigBee ou também outros, os gateways dedicados são imbatíveis em termos de compatibilidade. Eles podem unificar uma casa inteligente com mais eficiência do que outros gateways e têm opções de programação mais granulares. Ainda assim, do ponto de vista financeiro não vale investir em um gateway inteligente dedicado, a menos que não haja outra maneira de controlar um dispositivo que o usuário deseja em sua casa inteligente. Isso ajuda a economizar dinheiro enquanto simplifica à casa inteligente com menos dispositivos.

O protocolo Zigbee pode ter algumas vantagens sobre o Wi-Fi, mas comprar uma peça extra de hardware (um gateway) não é uma opção econômica e é uma das razões pelas quais a tecnologia doméstica inteligente somente ZigBee não tão populares. Pois como poucos dispositivos têm a capacidade de ler ZigBee, o gateway irá necessariamente possuir algum outro protocolo para comunicação com o usuário, sendo os mais comuns

Wi-Fi e Bluetooth para comunicação direta, e Wi-Fi e ETH para caso os dados necessitem serem enviados a uma nuvem para processamento, o que irá aumentar o valor do produto. Gateways dedicados são um modelo de aplicação antigo e não mais são implementado na indústria para casas inteligentes, tendo seu foco na indústria.

A partir desse cenário os hubs multifuncionais que combinam dois ou mais protocolos para que o usuário possa usá-los para diversas coisas, não apenas para automação residencial. Eles ajudam a entrar no estilo de vida doméstico inteligente porque os dispositivos podem ser adicionados conforme as necessidades e o orçamento permitirem. Eles são a opção mais viáveis para usuários, visto que possibilitam uma maior variedades de dispositivos na rede.

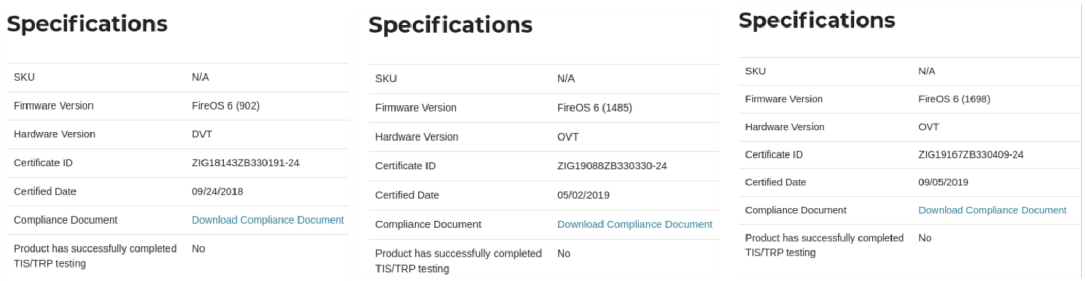
Por exemplo, o Amazon Echo Plus é um alto-falante inteligente onde se pode usar para ouvir músicas, definir temporizadores na cozinha ou verificar o clima do dia. Ele possui a capacidade de controlar dispositivos Zigbee, bem como dispositivos inteligentes que usam Wi-Fi, além disso ele possui a funcionalidade de controles de voz integrados do Amazon Alexa. A figura 30 apresenta a descrição do produto na Amazon.

Figura 30 – Echo Plus e descrição [Amazon 2020]

A busca pelo certificado do produto retornou 3 certificados e com a descrição ligeiramente diferente. A primeira e segunda indica o Echo Plus (2nd Gen) como um *Premium room-filling sound and built-in smart hub*, e a terceira como um *Home Cloud Computing device*, assim já podemos identificar que apesar do nome comercial ser o mesmo, os dispositivos possuem diferenças, a figura 31 apresenta a tela de busca do dispositivo no site de certificações da ZigBee Alliance.

Ao acessar as 3 certificações, apresentadas na figura 32, da esquerda para a direita, é possível verificar que houve uma atualização de software e alteração de hardware, entre a primeira e segunda certificação, que necessitaram ser revalidadas pela Zigbee. E que entre as duas ultimas houve uma atualização de software sendo que a diferença entre as datas de emissão dos certificados é pequena, isso pode indicar problemas de implementação da rede ZigBee ou que a rede ZigBee não apresentava problemas mas que outras funcionalidades do dispositivo poderiam afetar a rede ZigBee. Por fim a página apresenta um link para o

produto, e neste apenas o link da última versão está funcional, o que indica que o produto vendido está na última versão tanto de hardware quanto de firmware.



Specifications

SKU	N/A
Firmware Version	FireOS 6 (902)
Hardware Version	DVT
Certificate ID	ZIG18143ZB330191-24
Certified Date	09/24/2018
Compliance Document	Download Compliance Document
Product has successfully completed TIS/TRP testing	No

Specifications

SKU	N/A
Firmware Version	FireOS 6 (1485)
Hardware Version	OVT
Certificate ID	ZIG19088ZB330330-24
Certified Date	05/02/2019
Compliance Document	Download Compliance Document
Product has successfully completed TIS/TRP testing	No

Specifications

SKU	N/A
Firmware Version	FireOS 6 (1698)
Hardware Version	OVT
Certificate ID	ZIG19167ZB330409-24
Certified Date	09/05/2019
Compliance Document	Download Compliance Document
Product has successfully completed TIS/TRP testing	No

Figura 31 – Certificações do Echo Plus 2º geração . [ZigBee-Alliance 2020]

Ao efetuar o download dos arquivos de conformidade em um dos arquivos são apresentas as informações sobre quais funcionalidades são implementadas. Dentre elas um sistema de OTA – *Over The Air* utilizado para atualização de dispositivo conectados a rede, ainda sim não foram encontradas especificações sobre os protocolos de segurança implementados.

5 Conclusão

Este capítulo apresenta a conclusão do trabalho e trabalhos futuros derivados das dificuldades e aprendizados adquiridos durante a realização do estudo.

5.1 Conclusão

A conclusão desse trabalho é que o protocolo Zigbee/802.15.4, apresenta características importantes, como um sistema completo de segurança com chaves e algoritmos bem definidos para entrada e permanência na rede, sistema para atualização dos dispositivos e para atualização das chaves. Qualquer aplicação que necessite dessas características como um dos fatores de projeto, pode aproveitar o protocolo Zigbee para sua execução.

O protocolo é bem documentado, contudo um pouco confuso e muito extenso, o que pode ser uma desvantagem na tentativa do seu uso. Comparada a outras redes sem fio, a montagem de uma rede ainda possui um custo muito alto, já que é necessário usar um gateway para o funcionamento da rede e nem todos os dispositivos ZibBee se comunicam facilmente.

Porém, seu uso em redes particulares como edifícios, empresas, hospitais, universidades pode ser útil quando é necessário uma rede isolada e de difícil acesso. Para as redes sem fio que atuam em sistemas de controle e automação o ZigBee é uma opção sem fio muito conveniente quando se trata de segurança, visto que o protocolo não utiliza identificação por IP. Seu menor alcance dificulta a captura de pacotes e a necessidade de hardware e conhecimento específicos para conseguir invadir uma rede ZigBee são fatores que desencorajam atacantes. Com relação a trabalhos acadêmicos, e principalmente de pesquisa, o protocolo pode ser muito valioso, pois possui excelentes propostas para os mais diversos cenários.

O protocolo está em constante evolução, teve seu início em 2004 e sua última atualização livre em 2015. Contudo, obter uma certificação ZigBee é um processo atualmente caro, o que desestimula empresas menores a obter suas certificações ou fazer parte da ZigBee Alliance. Por conta disso, o mercado de dispositivos tende a demorar mais para se consolidar.

5.2 Trabalhos Futuros

Este trabalho teve por objetivo inicial, na parte prática, efetuar uma série de ataques contra uma rede Zigbee para estudo dos seus mecanismos de segurança, o que

mais tarde por conta de uma série de problemas não foi possível. Visando a solução desses problemas existem algumas frentes que podem ser exploradas como trabalhos futuros:

- Portar o KillerBee para novos hardwares de baixo custo e mais acessíveis;
- Elaboração de um simulador de redes ZigBee para fins acadêmicos;
- Comparação do modelo de segurança ZigBee com outras tecnologias; e,
- Análise do custo de implementação dos modelos de segurança em hardware e em software.

Referências

ALSHAHRANI, M.; TRAORE, I.; WOUNGANG, I. Anonymous mutual iot interdevice authentication and key agreement scheme based on the zigbee technique. *Internet of Things*, Elsevier, v. 7, p. 100061, 2019. Citado 2 vezes nas páginas 13 e 27.

AMAZON. *Echo Plus*. 2020. Disponível em: <https://www.amazon.com/All-new-Echo-Plus-2nd-built/dp/B0794W1SKP?th=1>. Citado 2 vezes nas páginas 13 e 56.

Cao, X. et al. Ghost-in-zigbee: Energy depletion attack on zigbee-based wireless networks. *IEEE Internet of Things Journal*, v. 3, n. 5, p. 816–829, Oct 2016. Citado na página 22.

Dini, G.; Tiloca, M. Considerations on security in zigbee networks. p. 58–65, June 2010. Citado na página 25.

ELEMENT14. *RZUSB*. 2020. Disponível em: <https://www.element14.com/community/docs/DOC-67532/l/avr-rz-usb-stick-module>. Citado 2 vezes nas páginas 13 e 49.

ELLEN, P. *Internet das coisas já é realidade, porém falta regulamentá-la*. 2016. Disponível em: <https://www.mckinsey.com/br/our-insights/blog-made-in-brazil/internet-das-coisas-ja-e-realidade-porem-falta-regulamenta-la>. Citado na página 21.

Fan, B. Analysis on the security architecture of zigbee based on ieee 802.15.4. In: *2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS)*. [S.l.: s.n.], 2017. p. 241–246. Citado 4 vezes nas páginas 13, 30, 31 e 33.

FAN, X. et al. *Security analysis of zigbee*. [S.l.]: MIT. edu, 2017. Citado 4 vezes nas páginas 13, 32, 33 e 34.

Chapter 8 - commissioning zigbee networks. In: GISLASON, D. (Ed.). *Zigbee Wireless Networking*. Burlington: Newnes, 2008. p. 331 – 350. ISBN 978-0-7506-8597-9. Disponível em: <http://www.sciencedirect.com/science/article/pii/B9780750685979000082>. Citado na página 28.

IDC. *The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast*. 2019. Disponível em: <https://www.idc.com/getdoc.jsp?containerId=prUS45213219>. Citado na página 20.

IEEE. *Towards a definition of the Internet of Things(IoT)*. 2015. Online; accessed 21 September 2019. Citado na página 19.

Khanji, S.; Iqbal, F.; Hung, P. Zigbee security vulnerabilities: Exploration and evaluating. In: *2019 10th International Conference on Information and Communication Systems (ICICS)*. [S.l.: s.n.], 2019. p. 52–57. Citado 4 vezes nas páginas 13, 22, 38 e 39.

Kocakulak, M.; Butun, I. An overview of wireless sensor networks towards internet of things. In: *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*. [S.l.: s.n.], 2017. p. 1–6. Citado na página 19.

Li, J. et al. Study on zigbee network architecture and routing algorithm. v. 2, p. V2–389–V2–393, July 2010. Citado na página 26.

LUMI-UNITED-TECHNOLOGY. *G2h*. 2020. Disponível em: <https://www.amazon.com/stores/Aqara/page/C2BFB250-C977-49DB-99B1-C8392CDC7B7C?ref_=ast_bln>. Citado 3 vezes nas páginas 13, 52 e 53.

LUMI-UNITED-TECHNOLOGY. *G2h*. 2020. Disponível em: <https://www.aqara.com/en/g2h_camera_hub.html>. Citado 3 vezes nas páginas 13, 52 e 55.

MCKINSEY. *THE INTERNET OF THINGS:MAPPING THE VALUE BEYOND THE HYPE*. 2015. Disponível em: <https://www.mckinsey.com/~/media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/High%20Tech/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/The-Internet-of-things-Mapping-the-value-beyond-the-hype.pdf>. Citado na página 21.

MICROCHIP. *JTAGICE*. 2020. Disponível em: <https://www.microchip.com/developmenttools/ProductDetails/PartNO/ATJTAGICE2>. Citado 2 vezes nas páginas 13 e 50.

MICROCHIP. *RZUSB*. 2020. Disponível em: <https://www.microchip.com/developmenttools/ProductDetails/PartNO/ATAVRRZRAVEN>. Citado 2 vezes nas páginas 13 e 50.

Neshenko, N. et al. Demystifying iot security: An exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations. *IEEE Communications Surveys Tutorials*, v. 21, n. 3, p. 2702–2733, thirdquarter 2019. ISSN 1553-877X. Citado 2 vezes nas páginas 20 e 34.

NXP. *MAXIMIZING SECURITY IN ZigBee NETWORKS*. 2019. Disponível em: <https://www.nxp.com/docs/en/supporting-information/MAXSECZBNETART.pdf>. Citado na página 34.

Olawumi, O. et al. Three practical attacks against zigbee security: Attack scenario definitions, practical experiments, countermeasures, and lessons learned. In: *2014 14th International Conference on Hybrid Intelligent Systems*. [S.l.: s.n.], 2014. p. 199–206. Citado 2 vezes nas páginas 47 e 49.

OWASP. *OWASP Foundation*. 2019. Disponível em: <https://www.owasp.org/index.php/Main_Page>. Citado 3 vezes nas páginas 13, 36 e 37.

Porkodi, R.; Bhuvaneswari, V. The internet of things (iot) applications and communication enabling technology standards: An overview. p. 324–329, March 2014. Citado na página 19.

RIVERLOOP. *Riverloop KillerBee*. 2020. Disponível em: <https://github.com/riverloopsec/killerbee>. Citado na página 42.

Ronen, E. et al. Iot goes nuclear: Creating a zigbee chain reaction. p. 195–212, May 2017. ISSN 2375-1207. Citado na página 19.

SILICON-LABS. *SimplicityStudio V5*. 2020. Disponível em: <https://www.silabs.com/products/development-tools/software/simplicity-studio>. Citado na página 42.

SILICON-LABS. *Tutorial-Bootloader*. 2020. Disponível em: <https://www.silabs.com/community/wireless/zigbee-and-thread/knowledge-base.entry.html/2018/04/18/how_to_build_thegec-CcVb>. Citado na página 46.

SILICON-LABS. *Tutorial Upload Node Test*. 2020. Disponível em: <https://docs.silabs.com/simplicity-studio-5-users-guide/1.0/building-and-flashing/flashing/>. Citado na página 46.

Wang, W.; He, G.; Wan, J. Research on zigbee wireless communication technology. p. 1245–1249, Sep. 2011. Citado 4 vezes nas páginas 13, 25, 26 e 28.

ZigBee Alliance. *ZigBee Specification*. 2015. Online; accessed 02 September 2019. Citado na página 32.

ZIGBEE-ALLIANCE. *ZigBee-Alliance-Certification*. 2020. Disponível em: <https://zigbeealliance.org/product_type/certified_product/>. Citado 4 vezes nas páginas 13, 53, 54 e 57.

ZIGEE-ALLIANCE. *Zigbee-Alliance*. 2019. Disponível em: <https://zigbee.org/>. Citado na página 19.

Apêndices

APÊNDICE A – Artigo Formato SBC

Análise de Vulnerabilidades em Redes ZigBee

Ruan Ramon de Oliveira[1]

[1]Departamento de Informática e Estatística – Universidade Federal de Santa Catarina (UFSC)

{ruan.ramon}@grad.ufsc.br

Abstract. *By 2025, billions of devices are expected to generate a large amount of data. Many of these will be sensitive data, so a security algorithm is needed to ensure integrity and reliability. The difficulties of integrating the Killerbee tool with the necessary hardware to carry out the attacks are presented. Then a new proposal to analyze devices sold at retail with respect to security issues. The study of the protocol has important characteristics, such as a complete security system with well-defined keys and algorithms for entering and staying on the network. Finally, the evaluation of the devices shows that the majority have little documentation on the security requirements, and when they exist, the security mechanisms are partially implemented.*

Resumo. *Espera-se que em 2025 hajam bilhões de dispositivos gerando uma grande quantidade de dados. Muitos desses seram dados sensíveis, logo um algoritmo de segurança é necessário para garantir integridade e confiabilidade. São apresentadas as dificuldades de integração da ferramenta Killerbee com o hardware necessário para efetuar os ataques. Em seguida uma nova proposta para analisar dispositivos vendidos a varejo com relação a quesitos de segurança. O estudo do protocolo apresenta características importantes, como um sistema completo de segurança com chaves e algoritmos bem definidos para entrada e permanência na rede. Por fim, a avaliação dos dispositivos demonstra que a maioria possui pouca documentação sobre os quesitos de segurança, e quando existem, os mecanismos de segurança são implementados parcialmente.*

1. Introdução

Pela definição da IEEE Internet of Things journal [IEEE 2015], um sistema IoT (*Internet of Things*) é uma rede de redes, no qual, tipicamente, um grande número de objetos/coisas/sensores/dispositivos são conectados através de uma infraestrutura de comunicação e informações para fornecer serviços de valor agregado e processamento inteligente de dados e gerenciamento para diferentes aplicações [Porkodi and Bhuvaneswari 2014]. Estima-se que nos próximos anos haverão quase 50 bilhões de "coisas" conectadas a Internet. Isso se deve ao fato do rápido crescimento tecnológico em sistemas embarcados cada vez menores e mais acessíveis e as redes de sensores sem fio (Wireless Sensor Network – WSN) [Ronen et al. 2017].

Os benefícios advindos do paradigma IoT são inegáveis, contudo existem sérias falhas de segurança. A negligência de várias considerações de segurança permite a exploração de informações sigilosas, que podem variar de *streamings* de vídeos desprotegidos de monitores de bebês, brinquedos IoT, *upload* de gravações de voz, e-mails e

senhas não autorizados, além de dispositivos mal projetados permitirem, em alguns casos, atuação sobre os mesmos, e em casos mais extremos a possibilidade de reprogramação do firmware do dispositivo. Entre casos recentes podemos destacar o ataque lançado pelo malware específico *IoT Mirai* [Neshenko et al. 2019].

Assim este trabalho tem como a proposta uma análise de segurança em redes ZigBee/802.15.4. Tendo seu início com uma análise do estudo da arte, seguindo por um estudo aprofundado dos quesitos de segurança nas 4 camadas das redes ZigBee e os tipos de ataques mais comuns efetuados. O trabalho propõe a elaboração de uma ambiente controlado para execução de ataques e realiza a verificação dos quesitos de segurança e são apresentadas as dificuldades que impossibilitaram a proposta inicial. Seguindo da apresentação do custo e dificuldades para se realizar um ataque contra um rede Zigbee, e por fim, a análise dos quesitos de segurança de dois dispositivos.

2. Redes ZigBee

O protocolo Zigbee é um padrão de redes sem fio para um conjunto de comunicações. Suas principais características são baixa potência, curta distância, baixa complexidade, auto-organização e baixo custo. Inclui um gama completa de dispositivos capazes de realizar medições das mais diversas grandezas. O protocolo é baseado no padrão 802.15.4 da IEEE que define as 2 camadas inferiores da rede: a camada física (PHY - *Physical*) e a camada de controle de acesso ao meio (MAC – *Media Access Control*). Assim, a ZigBee Alliance baseia-se nestas 2 camadas para fornecer a camada de rede (NWK - *Network*) e uma camada de aplicação (APL - *Application*) padronizada, a figura 1 ilustra a pilha do protocolo ZigBee/802.15.4 [Wang et al. 2011].

A camada física fornece uma interface para o meio físico (por exemplo rádio),. a camada MAC, imediatamente acima, controla o acesso ao canal de rádio, um mecanismo de CSMA-CA (*Carrier Sense Multiple Access with Collision Avoidance*) é usado para transmitir quadros de sinais e sincronização, além de fornecer um meio de comunicação com seus vizinhos imediatos com o intuito de prevenir colisões e melhorar a eficiência, também sendo responsável por compor e decompor os pacotes de dados transmitidos [Dini and Tiloca 2010].

A camada de rede ZigBee tem a responsabilidade de descobrir nodos adjacentes de um salto e armazenar informações relevantes sobre os mesmos, além de permitir que dispositivos entrem e saiam de uma rede ZigBee e encaminhar os quadros de dados aos dispositivos corretos. Por fim, a camada de aplicação especifica o formato dos quadros de dados para transporte e fornece um serviço de dados para aplicações. A segurança envolve tanto a camada de aplicação quanto a camada de rede [Wang et al. 2011]. A figura 1 apresenta a pilha do protocolo ZigBee.

2.1. Estrutura básica das Redes ZigBee

Uma rede baseada no ZigBee é formada basicamente por um coordenador ZigBee e nodos ZigBee, sendo os nodos diferenciados por roteadores e finais. As redes ZigBee suportam nativamente as topologias estrela e árvore em arquiteturas de malha genérica. Um ponto importante em comum é que em todos os casos a topologia pode possuir somente um concentrador .

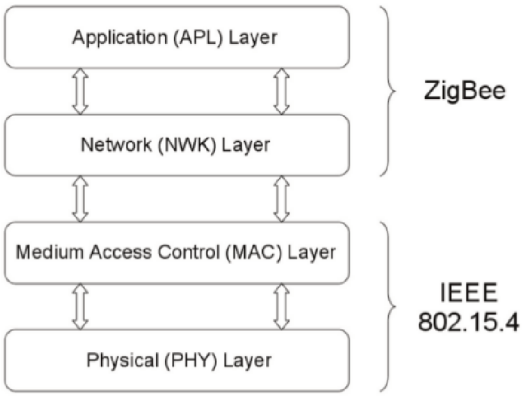


Figura 1. Camadas da pilha ZigBee [Wang et al. 2011]

Na topologia do tipo estrela, ou de salto único, o coordenador é responsável pela inicialização e pela manutenção da rede. Todos os outros dispositivos da rede são dispositivos finais e se comunicam diretamente com o concentrador. Esta topologia é adequada para redes que se possuam um concentrador centralizado e para aplicações onde o tempo é um fator crítico. Outra topologia é a de árvore em cluster, diferentemente da primeira neste modelo os nodos roteadores podem ser utilizados para estender a rede. Os nodos roteadores nesse modelo são responsáveis por controlar o fluxo de dados usando estratégias de roteamento hierárquico e a periodicidade de envio de roteamento definida na 802.15.4. Por fim, a malha genérica, neste modelo o concentrador e os nodos roteadores possuem as mesmas funções, uma rede de malha que permite uma comunicação ponto-a-ponto completa, excluindo comunicação entre dois nodos finais diretamente. Neste modelo, o roteamento de dados é descentralizado, para caso um nodo roteador falhe, o nodo final seja capaz de se conectar a outro nodo roteador para continuar enviando dados[Li et al. 2010]. A figura 2 apresenta um exemplo para cada modelo de topologia.

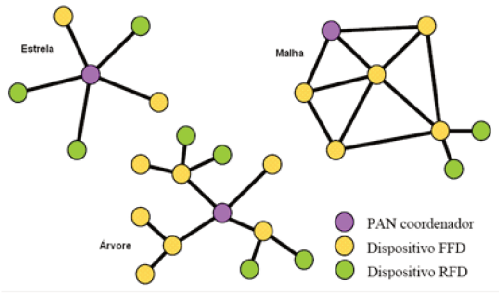


Figura 2. Topologias das redes ZigBee [UFRJ 2020]

2.2. Comissionamento

Comissionamento é o processo de configuração dos nodos de uma rede ZigBee com o intuito de comunicação entre si. Uma vez conectado a uma rede são necessários mecanismos de segurança para que redes independentes não se misturem, para envio de comandos para os nodos corretos e para comunicação entre dois nodos de uma mesma rede. Na sua forma mais básica, e na ausência de outras informações de configuração, um disposi-

tivo novo ingressará na primeira rede disponível. Depois de ingressar, ele receberá as informações que irão prepará-lo para ficar operante e comunicável na rede.

Após algumas dessas fases, chega ao estado operacional estável, armazenando essas novas informações da rede em uma memória não volátil, assim, caso haja falha energética quando religado o dispositivo continua operante. Todo dispositivo ZigBee pode ter seu estado regredido ao de fábrica, isso ocorre quando a rede apresenta uma falha ou quando se deseja trocar o dispositivo de rede. As primitivas de comissionamento estão espalhadas em diversas camadas da pilha de protocolos como nas camadas NWK, APS, ZDO, ZDP e a Biblioteca de Clusters ZigBee.

O *ZigBee Device Object* (ZDO) contém os métodos para localizar e associar uma dispositivo a uma rede, efetuando este trabalho juntamente com a camada NWK (Network); O *ZigBee Device Profile* (ZDP) contém o nodo e a aplicação, bem como as funções remotas de gerenciamento de tabelas; O ZigBee Cluster Library (ZCL) fornece um padrão para as principais funcionalidades e gestão de cenários OTA (*Over-the-Air*) como instalação de chaves de segurança, identificação de PAN IDs (*Personal Area Network Identifier*), a máscara de canal e os endereços de outros dispositivos. A figura 3 apresenta a pilha completa [Gislason 2008].

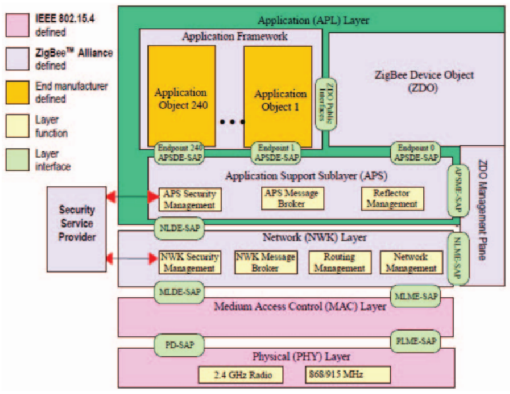


Figura 3. Arquitetura completa da pilha Zigbee [Wang et al. 2011]

2.3. Segurança das Redes ZigBee

O protocolo ZigBee define métodos de estabelecimento de chave criptográfica, transporte de chaves, proteção de quadros e gerenciamento de dispositivos. A arquitetura de segurança do ZigBee inclui mecanismos de segurança em três camadas da pilha de protocolos – MAC, Rede e Aplicação.

A camada MAC é responsável por seu próprio processamento de segurança, mas as camadas superiores determinam qual nível de segurança usar. Quando a proteção de integridade da camada MAC é empregada, todo o quadro MAC é protegido, incluindo o cabeçalho MAC que contém os endereços de origem e destino do hardware. Ao ativar a integridade do quadro MAC, o endereço de origem da camada MAC pode ser autenticado. Essa medida pode combater os ataques de falsificação e permitir que um dispositivo processe e compare com mais eficiência um quadro MAC recebido.

A criptografia é baseada no uso de chaves de 128 bits e no padrão de criptografia AES (*Advanced Encryption Standard*). Criptografia, integridade e autenticação podem

ser aplicadas nas camadas de Aplicação, Rede e MAC para proteger os quadros, frames e pacotes em cada um dos níveis. Em termos de tipos de chave, o ZigBee especifica o uso das chaves: Mestre (MK – *Master Key*), Link (LK – *Link Key*) e Rede (NK – *Network Key*) para proteger os quadros transmitidos.

Uma chave de Rede é uma chave compartilhada entre todos os nodos em uma rede ZigBee. O padrão também especifica uma Chave de Rede Alternativa como uma forma de rotação de chave que pode ser empregada para fins de atualização de chave. Uma rede deve utilizar uma Chave de Rede comum a todos os dispositivos para proteger todos os quadros de rede (mensagens de roteamento, solicitações de entrada na rede, etc.) e impedir a entrada e uso não autorizado da rede por dispositivos desconhecidos.

As Chaves de Link são chaves de sessão secretas usadas entre dois dispositivos em comunicação e são exclusivas para esses dispositivos. Os dispositivos usam sua Chave Mestra para gerar a chave de Link. A maneira pela qual as chaves Mestra, Link e Chaves de Rede são geradas, armazenadas, processadas e entregues aos dispositivos determina a eficácia e o grau de segurança da implementação geral da rede.

O ZigBee usa o conjunto de segurança CCM* (*Counter with CBC-MAC*) baseado em AES, que é baseado no conjunto de segurança especificado no padrão 802.15.4 e resumido na Figura 4. O CCM* é uma pequena modificação dos modos do CCM no padrão 802.15.4 e oferece recursos somente de criptografia e somente integridade. Os recursos extras no CCM* simplificam a segurança, eliminando a necessidade dos modos CTR e CBC-MAC no conjunto 802.15.4 e também permitem o uso de uma única chave para cada nível de segurança dentro do protocolo. Com o CCM*, as camadas MAC, Rede e Aplicação podem, opcionalmente, reutilizar a mesma chave para uma implementação mais eficiente, com base nos recursos limitados de armazenamento e processamento do dispositivo.

Identifier	Security level sub domain	Security component	Security attributes	Security services				Data integrity
				access control	data encryption	Frame integrity	Sequence update (optional)	
0x00	000	None	无					M=0
0x01	001	AES-CTR	ENC	X	X		X	M=0
0x02	010	AES-CCM-128	ENC-MIC-128	X	X	X	X	M=16
0x03	011	AES-CCM-64	ENC-MIC-64	X	X	X	X	M=8
0x04	100	AES-CCM-32	ENC-MIC-32	X	X	X	X	M=4
0x05	101	AES-CBC-MAC-128	MIC-128	X		X		M=16
0x06	110	AES-CBC-MAC-64	MIC-64	X		X		M=8
0x07	111	AES-CBC-MAC-32	MIC-32	X		X		M=4

Figura 4. Componentes de segurança ZigBee [Fan 2017]

O componente central da arquitetura de segurança do ZigBee é o ZigBee *Trust Center* (ZTC). Todos os dispositivos em uma rede reconhecem e confiam em exatamente um ZTC. O ZTC armazena e distribui chaves para dispositivos ZigBee. As funções executadas pelo ZTC são gerenciamento de confiança, gerenciamento de rede e gerenciamento de configuração.

É importante observar que diferentes aplicativos em execução no mesmo dispositivo ZigBee não são separados logicamente (devido a restrições de custo e complexidade). Portanto, aplicativos diferentes também não são criptograficamente separados e deve-se presumir que os aplicativos confiam um no outro porque estão usando o mesmo material

de codificação. O ZigBee se refere a ele como um modelo de confiança aberto, no qual, diferentes camadas da pilha de comunicação e todos os aplicativos em execução em um único dispositivo confiam um no outro. A implicação para o uso desse modelo é que todos os dispositivos e aplicativos em uma determinada rede confiam um no outro e que a segurança é realizada de acordo com o dispositivo.

2.4. Chaves de Segurança

As redes Zigbee utilizam uma Chave de Rede e Chaves de Link para se comunicar, sendo que o destinatário tem conhecimento das chaves usadas. Uma Chave de Rede possui 128 bits e é compartilhada por todos os dispositivos conectados à rede e é utilizada para transmissões do tipo *broadcasting*. Existem dois tipos: a padrão e a de alta segurança, o tipo da Chave de Rede irá definir como ela é distribuída, pois ela própria deve ser protegida quando é passada ao dispositivo que deseja se conectar.

Para essa criptografia, uma Chave de Link pré-configurada é usada, essa chave é conhecida pelo Trust Center e pelo dispositivo que deseja se conectar no modelo de segurança centralizada, e é conhecida por todos os nodos no modelo de segurança distribuída.

A Chave de Link é uma chave de 128 bits compartilhada por dois dispositivos, e existem dois tipos: a global e a exclusiva. O tipo da chave determina como o dispositivo lida com mensagens enviadas a partir do *Trust Center*.

No modelo de segurança centralizado, existem três tipos de Chaves de Link: Chave de Link global usada pelo *Trust Center* e todos os nodos da rede; Chave de Link exclusiva usada para uma relação individual entre o *Trust Center* e um nodo específico, posteriormente substituída por uma Chave de Link do *Trust Center*; e a Chave de Link de aplicação usada entre um par de dispositivos. Chaves de link relacionadas ao *Trust Center* geralmente são pré-configuradas usando um método fora de banda, por exemplo, código QR (*Quick Response*) na embalagem, enquanto as chaves de link entre entidades geralmente são geradas pelo Trust Center e criptografadas com a Chave de Rede. Em uma rede de segurança distribuída, as chaves de link existem apenas entre um par de dispositivos. A figura 5 faz um resumo dos modos de segurança, camadas e suas chaves, onde (O) indica opcional.

secret key	layer		mode	
	network layer	application layer	safe mode	High security
Network key	YES	YES	YES	YES
master key	NO	YES	NO	YES(O)
Link key	NO	YES	YES(O)	YES(O)

Figura 5. Modelos de segurança e chaves [Fan 2017]

2.5. Trust Center

O *Trust Center* é o dispositivo que os nodos conectados à rede confiam para distribuir suas chaves, ele tem a função de gerenciar as chaves, configurar a comunicação ponto-a-ponto e estabelecer, manter e atualizar as políticas de segurança para a rede. No modelo

de segurança centralizada todos os dispositivos da rede devem saber exatamente quem é o *Trust Center* ativo e deve haver somente um ativo. Neste modelo o *Trust Center* pode estabelecer políticas para ingresso de novos dispositivos, por exemplo, requerer que dispositivos desconhecidos identifiquem-se antes de fornecer a atualização da Chave de Rede; exigir uma Chave de Link pré configurada de fábrica ou exigir que uma Chave de Link seja instalada utilizando uma frequência diferente da padrão.

No modelo de rede distribuída todos os nodos roteadores tem a capacidade de atuar como um *Trust Center*, e distribuir chaves para a segurança da rede. Este modelo é utilizado para distribuição de Chaves de Rede e não para distribuição de Chaves de Link, pois não há um *Trust Center* único na rede. Em algumas aplicações os dispositivos podem ter o endereço do *Trust Center* e uma Chave de Link configurados na fábrica, em outros casos onde a rede pode tolerar um momento de vulnerabilidade, a Chave da Rede pode ser enviada por meio de de um transporte seguro utilizando as chaves da *Application Support SubLayer* (APS) usando uma Chave de Link conhecida.

Em ambos os modelos para fins de segurança um dispositivo aceita uma Chave de Link do *Trust Center* ou uma Chave de Rede ativa por meio do transporte de chaves. Em uma rede centralizada um dispositivo só vai aceitar uma Chave de Rede ativa inicial e atualizações quando elas estiverem protegidas pela Chave de Link compartilhada com o *Trust Center*. Na configuração um dispositivo só aceita a Chave de Link do seu *Trust Center*, ou por meio de negociação usando um protocolo de mais alto nível entre os dispositivos, este método também é utilizado para adicionar ou trocar Chaves de Link e Chave de Rede. [ZigBee Alliance 2015].

2.6. Segurança nas Camadas

Os mecanismos de segurança estão presentes em três camadas da pilha de protocolos: MAC, NWK e APS. A segurança na camada MAC é baseada na definição da IEEE 802.15.4 e por parte da ZigBee com o algoritmo CCM* [Fan et al. 2017].

A camada MAC usa uma chave única para todos os níveis de segurança do CCM* (CCM* nas camadas MAC, NWK e APS). Esta é responsável por seu próprio processamento de segurança, mas a camada APL define quais chaves devem ser utilizadas. A APL define a chave padrão para coincidir com a Chave de Rede ativa e as Chaves de Link da camada MAC para coincidir com as Chaves de Link da Camada de Rede [Fan et al. 2017].

A NWK é responsável por prover proteção para as operações da camada MAC e fornece uma interface para a camada APL, ou seja ela é responsável pelo processamento necessário para transmissão e recebimento dos quadros de forma segura. Quando é necessário segurança nesta camada é utilizado AES-CTR no contador aprimorado com o modo de operação CBC-MAC, as camadas superiores definem quais chaves utilizar, o contador de quadros e qual nível de segurança utilizar. Em alguns casos a camada NWK transmite e recebe mensagens de rota, ao fazer isto usa as Chave de Link, se disponíveis, caso contrário ela utilizará da Chave de Rede ativa. A figura 6 mostra um exemplo de um pacote da camada criptografado [Fan et al. 2017] [Fan 2017].

A camada APS é quem conduz toda a segurança relacionada as camadas da APL, ela é responsável pelas etapas necessárias para transmitir e receber os quadros com segurança, e gerenciar as chaves de criptografia, sendo que as camadas acima que emitem primitivas para a camada APS para informar o nível de segurança e quais chaves utilizar.

Na ZigBee 3.0 o protocolo pode criar um link seguro no nível da aplicação entre um par de dispositivos, estabelecendo um par de chaves exclusivos utilizando o AES-128 para quando é necessário um maior nível de segurança [Fan et al. 2017]. Este maior grau de segurança pode se utilizado para estabelecer uma Chave de Link ou uma Chave de Rede, para a atualização e status de um dispositivo. Quando um dispositivo conectado em um roteador ZigBee muda (como adicionar ou sair da rede), o roteador ZigBee fornece uma maneira segura de notificar a Central de Confiabilidade (TC - *Trust Center*) sobre a alteração do status do dispositivo. Fornece uma maneira segura para a Central de Confiabilidade notificar o nodo roteador de que um dispositivo filho precisa ser removido da rede. Para que um dispositivo ZigBee forneça uma maneira segura de outro dispositivo solicitar uma Chave de Rede ativa ou uma Chave de Link de aplicativo de ponta a ponta. Fornece uma maneira segura para o TC notificar um NK mútuo de troca de dispositivos [Fan 2017].

Um exemplo de cenário para este caso seria de uma rede doméstica que conecta vários dispositivos, como luzes, termostatos, sensores de presença, travas de portas, sensores de abertura de janelas, portas e portas de garagem. Todos esses dispositivos compartilhariam uma mesma Chave de Rede, assim a criptografia da camada APS pode ser aplicada a dispositivos como travas de portas e de garagem criando assim uma "conexão privada virtual", isso pode limitar a capacidade de um invasor, pois mesmo em posse da Chave de Rede o invasor também necessitaria da chave exclusiva dos dispositivos para atuar sobre eles. [Fan et al. 2017].

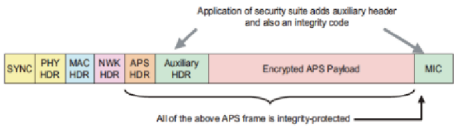


Figura 6. Quadro ZigBee com segurança na camada APS [Fan et al. 2017]

3. Vulnerabilidades das redee IoT

A vulnerabilidade de um nodo ZigBee depende de recursos de segurança do nível lógico tanto quando recursos de segurança incorporados ao design do produto e sua fabricação. Essas decisões juntas constroem o nível de segurança que o dispositivo terá com relação ao seu custo e facilidade de uso [MAXIMIZING-SECURITY-IN-ZigBee-NETWORKS]. Em [Neshenko et al. 2019] são apresentadas categorias gerais para vulnerabilidades em diversas redes IoT, apresentadas abaixo.

- Falta de segurança física: A maioria dos dispositivos IoT opera de forma independente em ambientes autônomos. Com pouco esforço, um atacante pode obter informações não autorizadas de forma física, e assim assumir o controle deles. Uma vez com acesso ao dispositivo um invasor poderia causar danos físicos ao dispositivo, possivelmente identificando esquemas criptográficos utilizados, efetuando cópias do firmware do dispositivo usando um nodo malicioso ou corrompendo dados de controle de acesso. O acesso físico ao hardware pode permitir que um adversário modifique os parâmetros de inicialização, extraia a senha root, aprenda sobre informações confidenciais e ou privadas e modifique o ID de um

dispositivo. Há casos onde pode permitir o roubo de arquivos de atualização, aproveitando a falta de criptografia a nível de dispositivo, e acesso a UART (*Universal Asynchronous Receiver-Transmitter*) que pode permitir acesso total ao sistema do dispositivo caso os algoritmos de hash e criptografia do sistema de arquivos não seja implementado.

- Insuficiência energética: Um fator relevante em dispositivos IoT é a energia, dispositivos têm energia limitada e não possuem necessariamente a tecnologia ou mecanismos para renová-la automaticamente. Um invasor pode direcionar ataques afim de drenar a energia armazenada gerando inundações de requisições legítimas ou corrompidas de conexão, deixando o dispositivo indisponível para processos ou usuários válidos. Uma solução seria a coleta de energia de fontes humanas, energia elétrica de tomadas, quanto de fontes naturais como solar ou eólica, como um método adequado para capacitar os dispositivos a adotar técnicas de segurança mais complexas.
- Autenticação Inadequada: Energia limitada e poder computacional são dois grandes desafios a implementação de mecanismos complexos de autenticação. Neste caso um invasor pode usar de abordagens de autenticação ineficazes para acrescentar nodos maliciosos ou violar a integridade dos dados, invadindo dispositivos e comunicações da rede. Nesse cenário, as chaves de autenticação trocadas e empregadas também correm o risco de serem perdidas ou corrompidas, nos casos onde as chaves estão sendo armazenadas ou transmitidas com segurança, algoritmos de autenticação sofisticados, ou eficazes, tornam-se insuficientes. Embora em muitos casos a pré-instalação das chaves em cada dispositivo para um determinado modo de segurança seja possível, na realidade, as chaves são transmitidas sem criptografia tornando possível o vazamento de informações confidenciais e permitindo que um adversário obtenha controle sobre os dispositivos. Existem vários ataques que visam ganhar controle ou conduzir negação de serviço em IoT. Uma sugestão para coibir estes ataques é que a aplicação do nível ”alta segurança”, juntamente com a pré-instalação das chaves, ofereceria suporte à proteção de informações confidenciais.
- Criptografia Imprópria: A criptografia dos dados é de suma importância no paradigma IoT, principalmente nos casos onde operam em locais críticos, como concessionárias de energia, fábricas, automação predial, controle de acesso, etc. A criptografia é um método eficaz para armazenar e transmitir dados de uma maneira que somente usuários autorizados possam utilizá-los. Contudo a força dos sistemas de criptografia depende dos algoritmos implementados, e nesse quesito as limitações de recursos de IoT afetam a robustez, a eficiência e a eficácia de tais algoritmos. Nesse caso um invasor pode contornar as técnicas de criptografia implementadas para revelar informações confidenciais ou controlar operações com esforço limitado e viável.
- Portas Abertas: Diversos dispositivos IoT têm portas desnecessariamente abertas durante a execução de serviços, permitindo que um invasor se conecte e explore uma infinidade de vulnerabilidades.
- Controle de Acesso Insuficiente: O gerenciamento de credenciais deve proteger dispositivos e dados contra acesso não autorizado. Sabe-se que a maioria dos dispositivos IoT em conjunto com suas soluções de gerenciamento em nuvem não força uma senha de complexidade suficiente. Além disso, após a instalação, vários

dispositivos não solicitam a alteração das credenciais de usuário padrão, e a maioria dos usuários possui permissões elevadas. Portanto, um adversário pode obter acesso não autorizado ao dispositivo, pode ameaçar dados e toda a rede.

- Gerenciamento de atualizações: Um sistema para atualização de software/firmware de dispositivos em operação deve ser incorporado, para uma vez identificado um problema, corrigi-los adequadamente para minimizar continuamente os vetores de ataque e aumentar suas capacidades funcionais. No entanto, abundantes casos relatam que muitos fabricantes ou não recorrem a atualizações de segurança ou não possui sistemas automatizados de atualização. Além disso, mesmo as atualizações disponíveis os mecanismos carecem de garantias de integridade, tornando-os susceptível de serem maliciosamente modificados.
- Práticas de Programação Fracas: Embora práticas de programação fortes e injeção de componentes de segurança possam aumentar a resiliência das redes, incontáveis firmwares são lançados com vulnerabilidades conhecidas, como backdoors, usuários root como pontos de acesso principais e a falta de uso do *Secure Socket Layer* (SSL) . Portanto, um adversário pode facilmente explorar os pontos fracos de segurança conhecidos para causar estouros de buffer, modificações de informações ou obter acesso não autorizado ao dispositivo.
- Mecanismos de Auditoria Insuficientes: Uma infinidade de dispositivos de IoT carece de procedimentos completos de registro, tornando possível ocultar atividades maliciosas geradas.

3.1. Ataques nas Redes ZigBee

Existem dois grandes grupos de ataques, os ataques ativos que requerem um ataque real de interceptação da rede onde o adversário pode modificar os dados ou injetar quadros de falha na rede. Neste modelo a rede é afetada negativamente, além disso a integridade e autenticidade dos dados transmitidos na rede é comprometida. Por sua vez os ataques passivos não buscam a interceptação real da rede mas sim a captura do tráfego, sem a intenção de denegrir as capacidades da rede ou compromete a integridade dos dados. Contudo a confidencialidade das informações é prejudicada uma vez que informações privadas podem ser coletadas para alguma outra finalidade.

Os ataques as camadas visão explorar falhas na sua arquitetura ou comunicação. A camada de transporte é utilizada para oferecer suporte a links de comunicação para dispositivos que acabaram de ingressar na rede. Os ataques podem incluir desde inundações de requisições de entradas a rede, onde o nodo de destino é sobrecarregado por uma grande quantidade de solicitações inválidas de estabelecimento de conexões (ataque de inundação). Até dessincronização onde se forja pacotes para uma ou ambas as extremidades da conexão, para que o host solicite a retransmissão dos quadros de pacotes perdidos. Ambos os ataques visam denegrir a capacidade da camada de transporte, assim impedindo que novos nodos reais entrem na rede, que haja grande perda de pacotes e por conta de todo o processamento requerido a consequente diminuição da vida útil das baterias dos dispositivos.

A camada de rede é responsável pelo processo de roteamento e pelo tráfego de rede. Os ataques podem incluir buracos de minhoca e ataques de encaminhamento seletivo. No ataque do buraco de minhoca; deve haver dois nodos maliciosos localizados em diferentes saltos da rede. Quando um nodo emissor transmite um quadro de dados,

um nodo malicioso encapsula esses dados para outro nodo malicioso e pelo qual os envia para os nodos vizinhos. Consequentemente, o nodo remetente é enganado, pois os nodos maliciosos estão próximos de um ou dois saltos, onde esses dois nodos maliciosos podem estar fora do alcance.

Incorpora o cabeçalho MAC que ajuda o receptor a saber o tamanho do pacote, retransmite os quadros em caso de erros e aloca recursos para os nodos recém-ingressados. O atolamento da camada de link é um exemplo de ataques da camada MAC lançados para criar DoS (*Denial of Service*) interrompendo a troca de mensagens entre nodos de transmissão e recepção. Isso degradaria e reduziria o desempenho da rede. Por fim os ataques a camada física visão explorar principalmente o sinal de rádio comum, bloqueando ou interceptando ou violando os quadros de pacotes de dados.

Por seguinte temos os ataques com alvo, estes modelos de ataques visão buscar uma falha específica da rede como os ataques de afundamento, (do inglês *Sink Attacks*). Podem ocorrer quando um nodo malicioso anuncia uma rota para ser o caminho mais curto e como todos os algoritmos de roteamento selecionam o caminho mais curto, ele atrai mais tráfego de rede para ser direcionado para ele, possibilitando que mais informações sejam capturadas. Geralmente, esse ataque é combinado com um ataque de buraco de minhoca (do inglês *WarmHole*).

Outro modelo de ataque é o de origem, nesses ataques, o adversário compromete um nodo legítimo da rede para atuar como um tipo de nodo do buraco negro; nesse ataque o nodo começa a descartar seletivamente pacotes recebidos ou todos os pacotes recebidos para induzir outros nodos vizinhos a procurar outra rota, como a anterior falhou.

O ataques dos vizinhos explora o processo de descoberta de outros nodos vizinhos das redes transmitindo a mensagem que inicializa o processo de comunicação. Um nodo mal intencionado envia uma mensagem de inicialização de comunicação com alta potência de transmissão e, portanto, os nodos receptores consideram esse nodo como seu vizinho e, em troca, enviarão os dados do pacote detectado. Consequentemente, uma enorme quantidade de energia será desperdiçada e congestionamentos podem ocorrer consequentemente.

Ataques de membros às vezes são chamados de ataques de párias e internos. No caso de ataques de párias; o nodo invasor não faz parte da rede, mas pode ameaçar a rede. Por outro lado, o ataque interno ocorre quando um nodo malicioso faz parte da rede, comprometendo a rede ou quando o atacante carrega um perfil falso e requisita a entrada na rede.

Por fim, os ataques por esgotamento de energia onde o atacante envia mensagens falsas para atrair o nodo a fim de intencionalmente esgotar a energia por cálculos redundantes relacionados à segurança. Isso reduzirá a vida útil do nodo e permitirá que o invasor inicie vários ataques após o esgotamento como DoS.

Vale ressaltar que esses ataques podem ser utilizados isoladamente, contudo frequentemente são utilizados em sequência ou combinados dependendo do grau de complexidade e do modelo de segurança da rede, para que o invasor possa atingir seus objetivos. A figura 7 apresenta um esquema simples para todos os ataques apresentados nesta seção. [Khanji et al. 2019].

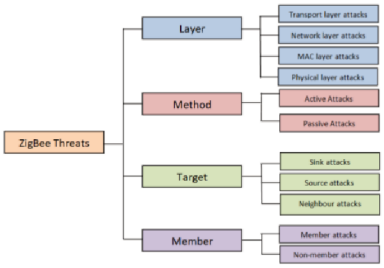


Figura 7. Modelo de Ameaças ZigBee [Khanji et al. 2019]

4. killerBee

Criado por Joshua Wright o KillerBee é um framwork para efetuar ataques as redes ZigBee e IEEE 802.15.4. Esse framework simplifica a detecção e a injeção de tráfego na rede, ao lado da decodificação e manipulação de pacotes. Fornece um firmware modificado para os transceptores USB ZigBee, uma vez carregado, o usuário tem controle total sobre o stick USB e pode capturar e enviar pacotes ZigBee. Sendo que o framework inclui as seguintes ferramentas :

- zbassocflood: Associa repetidamente ao PANId de destino, em um esforço para causar uma falha no dispositivo devido a muitas requisições de conecção.
- zbconvert: Converte uma captura de pacote da libpcap para o formato Daintree SNA ou vice-versa.
- zbdsniff: captura o tráfego do ZigBee, procurando quadros NWK e provisionamento de chave sem fio. Quando uma chave é encontrada, zbdsniff imprime a chave em stdout.
- zbdump: Uma ferramenta parecida com o tcpdump para capturar quadros IEEE 802.15.4 em um arquivo de captura de pacote libpcap ou Daintree SNA. Não exibe estatísticas em tempo real, como tcpdump, quando não está gravando em um arquivo.
- zbfind: um aplicativo GTK GUI para rastrear a localização de um transmissor IEEE 802.15.4 medindo o RSSI. O Zbfind pode ser passivo na descoberta (apenas escuta pacotes) ou pode estar ativo enviando quadros de solicitação de beacon e gravando as respostas dos coordenadores e coordenadores dos roteadores ZigBee.
- zbgoodfind: implementa uma função de pesquisa de chave usando uma captura de pacote criptografada e despejo de memória de um dispositivo ZigBee ou IEEE 802.15.4 legítimo.
- zbid: identifica interfaces disponíveis que podem ser usadas pelo KillerBee e ferramentas associadas.
- zbreplay: implementa um ataque de repetição, lendo um arquivo de captura de pacote Daintree DCF ou libpcap especificado, retransmitindo os quadros. Os quadros ACK não são retransmitidos.
- zbstumbler: ferramenta ativa de descoberta de rede ZigBee e IEEE 802.15.4. O Zbstumbler envia os quadros de solicitação de beacon ao saltar, gravar e exibir informações resumidas sobre os dispositivos descobertos.

5. Proposta

Este trabalho tem como objetivo prático a realização de alguns ataques sobre uma rede ZigBee para verificação dos quesitos de segurança implementados. A rede confiável será construída sobre a topologia de *cluster tree*, contudo pela limitação de dispositivos a rede possuirá apenas um cluster. Em relação aos quesitos físicos será composta por: um gateway ZigBee, um device somente com a capacidade de roteamento, logo ele não atuará como um *Trust Center* ficando essa responsabilidade somente para o gateway, os dois outros dispositivos farão apenas o papel de coletores de informações do meio. Ambos os dispositivos possuem duas entradas RJ11 para sondas diversas, uma entrada USB ou duas pilhas do modelo AA para alimentação e um barramento lateral para sondas de extensão, a comunicação entre os dispositivos e entre os dispositivos e o gateway será feito através do protocolo 802.15.4 definido pela IEEE. A imagem 8 exemplifica o modelo da rede.

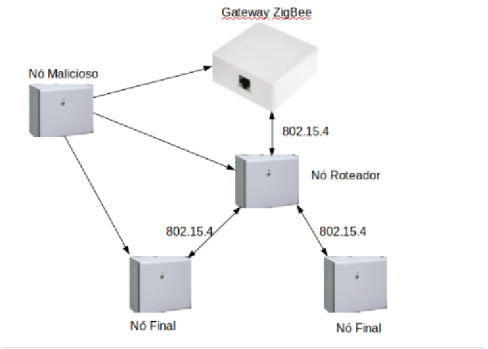


Figura 8. Modelo da rede do experimento Autor

Com essa rede como base, será criado um dispositivo malicioso utilizando para isso um Rapberry Pi como base física, a ferramenta killerBee e o sistema operacional Raspbian como base lógica. Uma vez o nodo malicioso construído, um conjunto de ataques será executado contra a rede a fim de testar pontos de vulnerabilidades utilizando-se para isto das diversas ferramentas disponibilizadas pelo KillerBee.

6. Dificuldades no desenvolvimento

A parte prática visava efetuar ataques contra uma rede zigbee, utilizando para isto a ferramenta opensource KillerBee .[Riverloop 2020]. Este software dá suporte, entre outros, a alguns hardwares da Silicom Labs que sejam capazes de executar o Silicon Labs Node Test 2.4GHz e SubGHz. Entre estes hardwares está a EFR32, está o qual o aluno possuía acesso juntamente com um Mighty Gecko SoC 12, rádio que permite o envio de pacotes ZigBee. Uma vez a placa configurada e conectada por micro USB permitiria o envio de comandos a partir do KillerBee para a placa e então a placa passaria os pacotes à rede.

Como descrito pela página do killerBee, é necessário alterar algumas configurações para que a placa possa ser reconhecida. Antes de instalar o programa acesse "killerbee/config.py" e altere para "True" a opção para a sua placa. Após isso foi iniciado a configuração da placa, visto que a placa não pertencia ao aluno a interação com a mesma foi limitada. O processo de instalação é simples e pode ser feito instalando todo o pacote ZigBee.

Uma vez inicializado é efetuada a conexão da placa pela interface micro USB da EFR32, e o Simplicity Studio já irá reconhecer uma interface, nesse ponto é aconselhável certo cuidado pois o Simplicity Studio pode identificar outros dispositivos conectados ao USB, como um conversor USB-Serial, enquanto um mouse ou teclado não serão listados. A figura 9 apresenta a primeira conexão da placa após os passos citados.

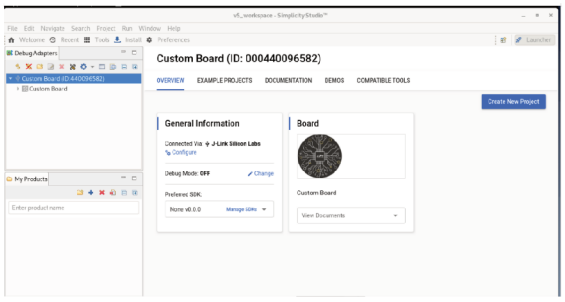


Figura 9. Identificação Inicial da placa pelo SimplicityStudio [Autor]

Neste ponto já é possível verificar o número identificador da placa na parte superior da figura 9, contudo o modelo e outras informações não foram identificadas. Isso acontece por que o modo "DEBUG" vem desligado por padrão, assim no quadro "General Information" selecione "Change" ao lado de "Debug Mode OFF" isto irá abrir uma nova tela para configuração do hardware, nas abas superiores selecione a aba "Adapter Configuration" e altere a configuração do campo "DEBUG MODE" para "MCU".

Após a configuração do modo de debug a tela inicial apresenta todas as configurações da placa, figura 10, na parte superior são apresentados a identificação do modelo da placa e as informações do rádio e ao lado esquerdo na aba "Debug Adapters" são apresentadas informações específicas da placa e as possibilidades de configurações. Ao rolar para baixo a tela central são apresentadas imagens da placa, do rádio do chip.

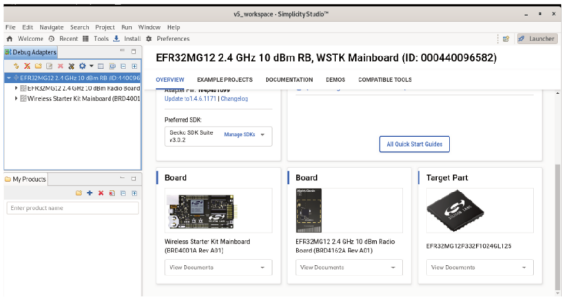


Figura 10. Caracteríscas de cada componente [Autor]

Caso haja algum problema em uma instalação inicial do EmberZnet, a guia logo abaixo de "Debug Adapters" selecione "Install". Após isso seria necessário gravar o Node Teste, através do tutorial .[?] apresenta uma sequência de passos para a gravação, contudo ao executar os passos no momento de identificar o Node Test para a EFR32 o mesmo não era mais identificado, apenas eram apresentados corretamente o Node Test para outros modelos de placas, a figura 11 apresenta o momento da tentativa de identificação.

O Node Test é um software proprietário e fechado da Silicom Labs, só é possível acessá-lo através do Simplicity Studio. Uma vez que todos os testes na versão atual não

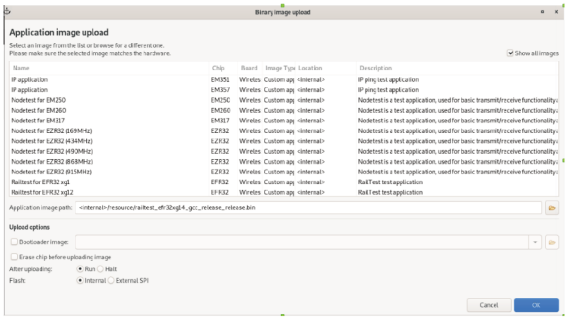


Figura 11. Apresentação dos Node Test e modelos de placas [Autor]

surtiram efeito e a tentativa de encontrar um Node Test compatível em versões mais antigas do EmberZNet falharam. Foi requisitada ajuda a um colega de trabalho que possuía uma versão mais antiga do Silmplicity Studio instalada a fim de verificar se nos arquivos ainda havia o NODE TEST para a EFR32, mas sem sucesso também. Então pelo caminho dos arquivos foi encontrado o que poderia ser o NODE TEST para o modelo da placa, ao executar a gravação e pelos logs foi possível verificar que a placa havia sido gravada. Contudo apesar de todos os testes e tentativas não foi possível fazer com que o KillerBee identificasse ou se comunicasse com a placa através do comando «zbid», comando utilizado para identificar o modelo da placa, utilizar o sniffer de rede ou qualquer outro comando.

Todos estes problemas foram agravados por conta da situação social, a pandemia, que impossibilitou a ida a empresa, uma vez que foi acordado que o aluno poderia utilizar a placa quando ela não estivesse em uso e fora do horário de trabalho.

7. Custo de um ataque

Em [Olawumi et al. 2014] são apresentados três ataques a uma rede zigbee utilizando um Atmel RZ Raven USB sticks, em 2014 quando o artigo foi publicado, é dito que somente o device teve um custo de 40 dólares. O firmware padrão do RZUSB pode ser usado para implementar um sniffer para uma rede ZigBee, atuar como um coordenador de rede de uma PAN – *Personal Area Network* ou como um ZigBee End-Device. Atualizar o RZUSB com um novo firmware, que pode realizar outros ataques com o KillerBee, não é um processo simples, pois requer uma outra peça de hardware conhecida como um programador on-chip, como Atmel JTAGICE mkII. O Atmel JTAGICE mkII foi projetado para funcionar com microprocessadores AVR como o AT90USB1287 usado no stick USB Atmel RZ Raven. Assim para realizar um ataque à uma rede Zigbee será necessário um certo investimento, além de algum conhecimento sobre como gravar hardware. É importante ressaltar que o RZUSB é um dispositivo do tipo USB, ou seja é necessário alimentação. Logo o custo e o conhecimento necessário para se efetuar um ataque pode desistimular um atacante.

8. Dispositivos ZigBee

Existem diversos produtos para casas inteligentes, e estes implementam uma vasta quantidade de protocolos. Os protocolos mais comuns na indústria de varejo são : ZigBee, Z-Wave, Bluetooth Low Energy, Bluetooth e Wi-Fi. Existem dispositivos que possuem

mais de um protocolo, sendo que quanto mais maneiras de se acessar o dispositivo mais caro ele é, pois necessita de hardware e software mais complexos, e também se tornam vulneráveis a mais tipos de ataques, por outro lado podem ser acessados de várias maneiras facilitando seu uso doméstico. A escolha do protocolo correto define muito da estrutura da rede da casa, dispositivos ZigBee e Zwave necessitam de um gateway para enviar mensagens a uma nuvem e então através de uma aplicativo acessar as informações, enquanto dispositivos Bluetooth e Wi-Fi não necessitam diretamente de um gateway podendo ser acessados por um smartphone ou por um computador. Assim apesar de uma alcance restrito, cerca de 30 metros, dispositivos roteadores podem estender a rede, e caso um desses nodos roteadores fique inoperante os dispositivos irão procurar outro caminho para continuar enviando seus dados de forma automática.

Vários desses padrões sem fio usam a mesma frequência e normalmente interferem uns nos outros. Para pequenos pacotes de dados como a maioria dos sensores envia, isso não representa um problema se o dispositivo específico permanecer em um ambiente doméstico normal. Na momento da compra dos dispositivos que irão compor à rede doméstica é importante se certificar de que os dispositivos possuam criptografia e de que elas estejam ativadas por padrão, pois a ativação da criptografia pode impedir as tentativas de comprometer dados confidenciais dos dispositivos. As vantagens do ZigBee neste cenário são que o protocolo não usa endereçamento IP. Portanto, deve haver um gateway ZigBee instalado para se comunicar com a Internet e os serviços em nuvem. Como a maioria dos telefones, tablets e computadores não tem a capacidade de se comunicar com dispositivos Zigbee, os gateways também são necessários para se comunicar com eles. Isso já inclui um maior nível de segurança a rede doméstica, visto que para um atacante conseguir acesso aos dispositivos precisará ter acesso a um rádio ZigBee para efetuar ataques diretos a sua rede, ou conseguir acesso ao gateway da residência.

8.1. Câmera Zigbee

Um exemplo de dispositivo é a câmera de segurança ZigBee da Lumi United Technology, apresentada na figura 12, pela tela inicial do produto na Amazon não é possível identificar a versão do protocolo ZigBee implementada, já na na descrição do produto é possível verificar que ela é compatível com o Apple HomeKit, ou utilizando o aplicativo Aqara Home a partir de um dispositivo como smartphone ou tablet, logo é possível acessar as informações da câmera de diversas maneiras. Com um modelo que satisfaça às necessidades, foi iniciada a busca pelas características específicas do produto, pelo modelo foi possível encontrar o site da fabricante, e no site foi encontrado o manual do usuário do dispositivo. No página principal da fabricante são apresentadas mais informações do produto, como a capacidade de roteador no máximo outros 64 dispositivos e que todos esses dispositivos devem ser da mesma marca, logo ele não será capaz de rotear dispositivos de outros fabricantes o que limita a rede a um mesmo fabricante. Ao inspecionar o site foi verificado que o produto possui o selo da ZigBee Alliance, esse selo garante que o produto passou por uma série de testes por parte da ZigBee e que foi aprovado recebendo assim esse certificado, produtos que não são certificados pela ZigBee geralmente são apresentados no mercado como compatíveis com 802.15.4 ou como compatíveis com Zigbee, e não podem usar o nome ZigBee.

Nesse ponto por conta do produto alegar possuir duas certificações de duas grandes empresas o próximo passo foi a verificação dos certificados. A ZigBee Alliance dispo-

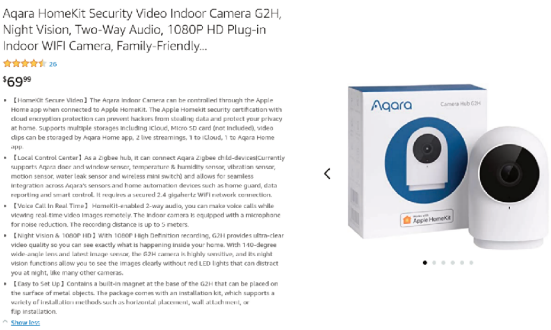


Figura 12. Câmera Zigbee G2h Lumi United Technology.[G2H 2020]

nibiliza em seu site uma página para verificação de produtos certificados, onde uma busca por "G2H" já apresentou o produto. O produto possuir um certificado junto a ZigBee Alliance válido mostra que ele passou nos testes e possui as funcionalidades descritas, contudo ao efetuar ao baixar os documentos de conformidade, disponíveis na página do certificado, nenhuma informação sobre quesitos de segurança foi identificado, a figura 13 apresenta a busca pelo certificado do produto. Voltando a página inicial do produto foi efetuado o download do manual do usuário para verificar se havia alguma informação sobre segurança, contudo no documento não são citadas informações sobre segurança, contudo algumas outras informações sobre o produto são interessantes para as redes ZigBee.

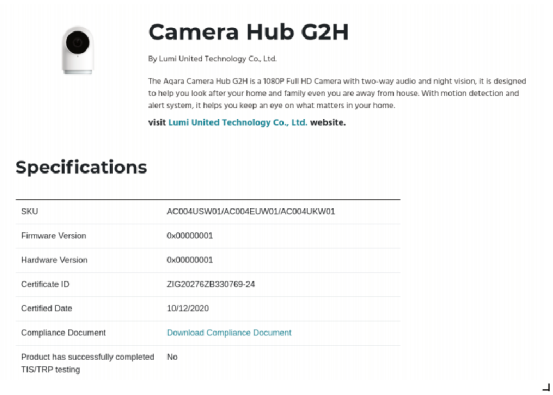


Figura 13. Certificado ZigBee para a G2H .[ZigBee-Alliance 2020]

O primeiro é que o produto é fixado a sua base por uma base magnética, isso pode ser um pouco perigoso visto que agindo como hub da rede caso ele acabe por cair e se danificar ou mesmo seja retirado manualmente do seu local toda a rede pode ficar comprometida, outro fator nesse sentido é que o produto funciona de -10 à 40 graus Celsius, visto que em alguns estados brasileiros as temperaturas podem ultrapassar a temperatura superior o dispositivo pode para de funcionar. Não foi encontrado também uma descrição de como atualizar o dispositivo, e nos documentos do certificado ZigBee,foi verificado que o produto não envia as informações de versão do software ou hardware. Por fim o trecho que mais chamou a atenção no manual do usuário, apresentado na figura 14, que apesar de vender o produto como para segurança em vários momentos isenta complementa a empresa caso ocorra uma falha no produto nesse sentido.

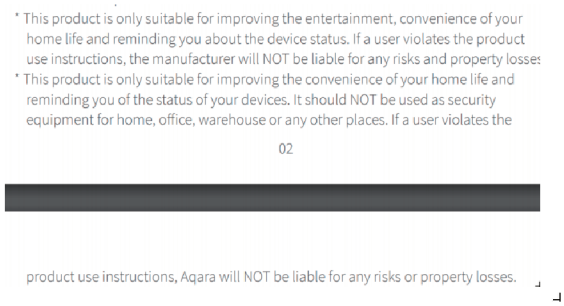


Figura 14. Manual do usuário do produto. [Technology 2020]

8.2. Hub ZigBee

O gateway é o dispositivo que irá funcionar como o concentrador, ou seja o elemento da rede que será responsável por intermediar a comunicação entre os dispositivos e o usuário, uma vez que os dispositivos tem que entrar na rede gerada pelo concentrador. È ele quem irá gerenciar todo o esquema de chaves e autenticação dos dispositivos na rede, assim escolher um gateway depende de algumas características.

O primeiro fator é verificar se os dispositivos da sua casa utilizam somente o protocolo ZigBee ou também outros, os gateways dedicados são imbatíveis em termos de compatibilidade. Eles podem unificar uma casa inteligente com mais eficiência do que outros gateways e têm opções de programação mais granulares. Ainda assim, do ponto de vista financeiro não vale investir em um gateway dedicado, a menos que não haja outra maneira de controlar um dispositivo.

O protocolo Zigbee pode ter algumas vantagens sobre o Wi-Fi, mas comprar uma peça extra de hardware não é uma opção econômica e é uma das razões pelas quais a tecnologia doméstica inteligente somente ZigBee não tão populares. Como poucos dispositivos têm a capacidade de ler ZigBee, o gateway irá necessariamente possuir algum outro protocolo para comunicação com o usuário, sendo os mais comuns Wi-Fi e Bluetooth para comunicação direta, e Wi-Fi e ETH para caso os dados necessitem serem enviados a uma nuvem para processamento, o que irá aumentar o valor do produto. Gateways dedicados são um modelo de aplicação antigo e não mais são implementado na indústria para casas inteligentes, tendo seu foco na indústria.

A partir desse cenário os hubs multifuncionais que combinam dois ou mais protocolos para que o usuário possa usá-los para diversas coisas se tornam mais visados. Eles ajudam a entrar no estilo de vida doméstico inteligente porque os dispositivos podem ser adicionados conforme as necessidades e o orçamento permitirem. Eles são a opção mais viáveis para usuários, visto que possibilitam uma maior variedades de dispositivos na rede.

Por exemplo, o Amazon Echo Plus é um alto-falante inteligente onde se pode usar para ouvir músicas, definir temporizadores na cozinha ou verificar o clima do dia. Ele possui a capacidade de controlar dispositivos Zigbee, bem como dispositivos inteligentes que usam Wi-Fi, além disso ele possui a funcionalidade de controles de voz integrados do Amazon Alexa. A figura 15 apresenta apresenta a descrição do produto na Amazon.

A busca pelo certificado do produto retornou 3 certificados e com a descrição ligeiramente diferente. A primeira e segunda indica o Echo Plus como um *Premium*

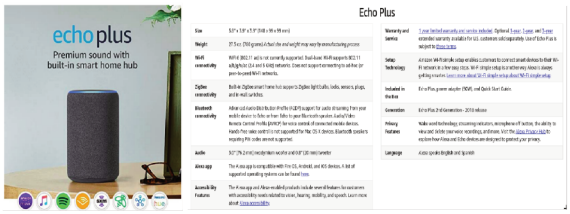


Figura 15. Echo Plus e descrição do produto [Amazon 2020]

room-filling sound and built-in smart hub, e a terceira como um *Home Cloud Computing device*, assim já podemos identificar que apesar do nome comercial ser o mesmo, os dispositivos possuem diferenças, a figura 16 apresenta a tela de busca do dispositivo no site de certificações da ZigBee Alliance.

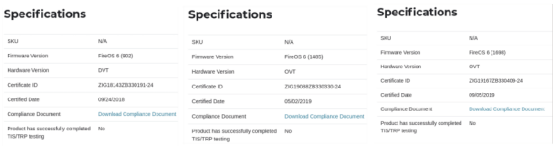


Figura 16. Certificações do Echo Plus 2º geração [ZigBee-Alliance 2020]

Ao acessar as 3 certificações, da esquerda para a direita, é possível verificar que houve uma atualização de software e alteração de hardware, entre a primeira e segunda certificação, que necessitaram ser revalidadas pela Zigbee. E que entre as duas ultimas houve uma atualização de software sendo que a diferença entre as datas de emissão dos certificados é pequena, isso pode indicar problemas de implementação da rede ZigBee ou que a rede ZigBee não apresentava problemas mas que outras funcionalidades do dispositivo poderiam afetar a rede ZigBee. Por fim a página apresenta um link para o produto, e neste apenas o link da última versão está funcional, o que indica que o produto vendido está na última versão tanto de hardware quanto de firmware.

Ao efetuar o download dos arquivos de conformidade as informações sobre quais funcionalidades são implementadas no dispositivo foram encontradas, entre elas a funcionalidade de OTA – Over The Air utilizado para atualização de dispositivo conectados a rede, ainda sim não foram encontradas especificações sobre os protocolos de segurança implementados.

9. Conlusão

A conclusão desse trabalho é que o protocolo Zigbee/802.15.4, apresenta características importantes, como um sistema completo de segurança com chaves e algoritmos bem definidos para entrada e permanência na rede, sistema para atualização dos dispositivos e para atualização das chaves. Comparada a outras redes sem fio, a montagem de uma rede ainda possui um custo muito alto, por conta da atual necessidade de um gateway para funcionamento da rede e por conta de nem todos os dispositivos ZigBee comunicarem-se completamente.

Porém seu uso em redes particulares como edifícios, empresas, hospitais, universidades podem se fazer muito útil quando é necessário uma rede isolada e de difícil

acesso. Seu menor alcance dificulta a captura de pacotes e a necessidade de hardware e conhecimento específicos para conseguir invadir uma rede ZigBee são fatores que desencorajam atacantes. Com relação a trabalhos acadêmicos, e principalmente de pesquisa, o protocolo pode ser muito valioso, pois possui excelentes propostas para os mais diversos cenários.

Este trabalho teve por objetivo inicial, na parte prática, efetuar uma série de ataques contra uma rede Zigbee para estudo dos seus mecanismos de segurança, o que mais tarde por conta de uma série de problemas não foi possível. Visando a solução desses problemas existem algumas frentes que podem ser exploradas como trabalhos futuros: portar o KillerBee para novos hardwares de baixo custo e mais acessíveis; elaboração de um simulador de redes ZigBee para fins acadêmicos; comparação do modelo de segurança ZigBee com outras tecnologias e análise do custo de implementação dos modelos de segurança em hardware e em software.

Referências

Amazon (2020). Echo Plus. `https://www.amazon.com/All-new-Echo-Plus-2nd-built/dp/B0794W1SKP?th=1`. [Online; accessed 11-20-2020].

Dini, G. and Tiloca, M. (2010). Considerations on security in zigbee networks. pages 58–65.

Fan, B. (2017). Analysis on the security architecture of zigbee based on ieee 802.15.4. In *2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS)*, pages 241–246.

Fan, X., Susan, F., Long, W., and Li, S. (2017). Security analysis of zigbee.

G2H, A. (2020). G2H Amazon. `https://www.amazon.com/stores/Aqara/page/C2BFB250-C977-49DB-99B1-C8392CDC7B7C?ref_=ast_bln`. [Online; accessed 11-20-2020].

Gislason, D. (2008). Chapter 8 - commissioning zigbee networks. In Gislason, D., editor, *Zigbee Wireless Networking*, pages 331 – 350. Newnes.

IEEE (2015). Towards a definition of the Internet of Things (IoT). Online; accessed 21 September 2019.

Khanji, S., Iqbal, F., and Hung, P. (2019). Zigbee security vulnerabilities: Exploration and evaluating. In *2019 10th International Conference on Information and Communication Systems (ICICS)*, pages 52–57.

Li, J., Zhu, X., Tang, N., and Sui, J. (2010). Study on zigbee network architecture and routing algorithm. 2:V2–389–V2–393.

Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., and Ghani, N. (2019). Demystifying iot security: An exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations. *IEEE Communications Surveys Tutorials*, 21(3):2702–2733.

Olawumi, O., Haataja, K., Asikainen, M., Vidgren, N., and Toivanen, P. (2014). Three practical attacks against zigbee security: Attack scenario definitions, practical experi-

ments, countermeasures, and lessons learned. In *2014 14th International Conference on Hybrid Intelligent Systems*, pages 199–206.

Porkodi, R. and Bhuvaneswari, V. (2014). The internet of things (iot) applications and communication enabling technology standards: An overview. pages 324–329.

Riverloop (2020). KillerBee. `https://github.com/riverloopsec/killerbee1`. [Online; accessed 08-10-2020].

Ronen, E., Shamir, A., Weingarten, A., and O'Flynn, C. (2017). Iot goes nuclear: Creating a zigbee chain reaction. pages 195–212.

Technology, L. U. (2020). G2H Aqara. `https://www.aqara.com/en/g2h_camera_hub.html`. [Online; accessed 11-19-2020].

UFRJ (2020). Topologia Redes ZigBee. `https://www.gta.ufrj.br/grad/07_1/zigbee/topologias.html`. [Online; accessed 11-20-2020].

Wang, W., He, G., and Wan, J. (2011). Research on zigbee wireless communication technology. pages 1245–1249.

ZigBee Alliance (2015). ZigBee Specification. Online; accessed 02 September 2019.

ZigBee-Alliance (2020). ZigBee Alliance Certification. `https://zigbeealliance.org/product_type/certified_product/`. [Online; accessed 11-19-2020].