UNIVERSIDADE D
COIMBRA

Miguel da Silva Rosendo

GESTÃO DINÂMICA DE SEGURANÇA E ENERGIA EM IOT

VOLUME 1

Dissertação no âmbito do Mestrado em Engenharia Informática, especialização em Comunicações, Serviços e Infraestruturas orientada pelo Professor Doutor António Jorge da Costa Granjal e apresentada à Faculdade de Ciências e Tecnologia / Departamento de Engenharia Informática.

Junho de 2020

Esta página foi deliberadamente deixada em branco.

Resumo

A *Internet of Things* (IoT) é conhecida por facilitar inúmeras tarefas, permitindo, por exemplo, a recolha de informação ou a realização de uma ou mais ações remotamente. Isto torna-a numa tecnologia bastante desejável e, aliado ao facto de ser cada vez mais acessível ao público em geral, o número de dispositivos ligados tem crescido exponencialmente, sendo cada vez mais incluído no dia-a-dia da população. Contudo, o consumo crescente de energia e a baixa capacidade das baterias usadas neste tipo de dispositivos são considerados um obstáculo, revelando-se importante chegar a uma forma de equilibrar as necessidades. Para isso, é imperativo dotar esta tecnologia de mecanismos de segurança actualizados que protejam a privacidade da informação transportada nas suas redes e, em simultâneo, não prejudicar gravemente o tempo de vida do dispositivo, evitando que este tenha que ser intervencionado várias vezes. Assim, o objetivo deste trabalho é contribuir para a investigação e desenvolvimento de mecanismos mais robustos em IoT e *Low Power Wide Area Network* (LPWAN) e proteger estas tecnologias, que fazem e farão cada vez mais parte do quotidiano, de ameaças constantes e inovadoras.

Nesta dissertação é apresentado um conjunto de protocolos IoT para LPWAN: *Narrowband Internet of Things* (NB-IoT), *Long Term Evolution* categoria M1 (LTE-M), Sigfox e *Long Range Wide Area Network* (LoRaWAN). Estes protocolos são comparados quanto às suas especificações, ameaças e é avaliada a possibilidade de apresentação de uma proposta de melhoria. Dos protocolos analisados, apenas o LoRaWAN correspondeu às necessidades, visto que, para além de ser bastante usado mundialmente, é um protocolo aberto e que permite alterações no seu funcionamento. Após seleção, foram apresentadas as oportunidades descobertas pela análise de documentos científicos, bem como alternativas que já tenham sido propostas para este protocolo.

A proposta elaborada incidiu sobre o desenvolvimento de um controlador dinâmico de segurança, tendo por objetivo conseguir encontrar um equilíbrio entre segurança e poupança de energia, tentando a todo o custo prolongar o tempo de vida de cada sensor numa infraestrutura LoRaWAN. Mediante as configurações definidas ao nível da aplicação e da avaliação de segurança recebida, é calculado o esquema de segurança que se adequa melhor naquele instante. Depois da apresentação da arquitetura, do algoritmo desenvolvido e dos resultados obtidos nos testes, foi feita a sua análise e comparação, que serviram para tirar conclusões sobre a viabilidade e sucesso desta proposta.

Em suma, este controlador revelou-se uma mais valia ao longo do tempo de funcionamento de um sensor, tendo conseguido mostrar que é possível poupar energia em ambientes com pouco ou nenhum risco de segurança e aumentar a proteção do sistema, aumentando o nível de segurança, contra ameaças graves, caso apareçam.

Palavras-Chave

IoT, LPWAN, Segurança, Energia, LoRa, LoRaWAN, SigFox, NB-IoT, LTE-M

Esta página foi deliberadamente deixada em branco.

Abstract

The *Internet of Things* (IoT) is well known for facilitating tasks, allowing , for example, the collection of information or to perform one or more tasks. This makes it a very desirable technology and, coupled with the fact that it is increasingly accessible to the general public, the number of connected devices has grown exponentially and, being included in the daily lives of the population more often. However, the growing consumption of energy and the low capacity of the batteries used in these types of devices are considered an obstacle, proving to be important to find a way to balance the needs. For that reason, it is imperative to provide this technology with up-to-date security mechanisms that protect the privacy of information carried on the networks and, simultaneously, not severely damaging the lifetime of the device, avoiding the need to be intervened several times. Therefore, the objective of this work is to contribute to the investigation and development of more robust mechanisms in IoT and *Low Power Wide Area Network* (LPWAN) and to protect these technologies, which are and will be part of everyday life, from constant and innovative threats.

In this dissertation, a set of IoT protocols for LPWAN: *Narrowband Internet of Things* (NB-IoT), Long Term Evolution category M1 (LTE-M), Sigfox and *Long Range Wide Area Network* (LoRaWAN). These protocols are compared in terms of their specifications, threats and the possibility of presenting an improvement proposal. Of the protocols that were analyzed, only the LoRaWAN protocol met the needs since, in addition to being widely used worldwide, it is an open protocol that allows changes in its operation. After the selection, the opportunities discovered by the analysis of scientific documents were described as well as proposals that have already been presented for this protocol.

The proposal focused on the development of a dynamic safety controller. aiming to achieve a balance between safety and energy savings, trying at all means to extend the lifetime of each sensor in a LoRaWAN infrastructure. Using the settings defined at the application level and the security assessment received, it is possible to calculate the best-suited security scheme at that moment. After presenting the architecture, the developed algorithm and the results obtained in the tests, its analysis and comparison was made, which are then used to draw conclusions about the feasibility and success of this proposal.

This controller proved to be an asset during the time when the sensor was running, having managed to show that it is possible to save energy in environments with little or no security risks or to increase the protection of the system, raising the level of security, against serious threats.

Keywords

IoT, LPWAN, Security, Energy, LoRa, LoRaWAN, SigFox, NB-IoT, LTE-M

Esta página foi deliberadamente deixada em branco.

Agradecimentos

Em primeiro lugar, quero deixar um agradecimento especial ao Professor Doutor António Jorge da Costa Granjal por toda a dedicação e disponibilidade demonstrada e pelo acompanhamento regular e orientação ao longo destes 10 meses de trabalho, muito importantes para o sucesso desta dissertação.

Quero também deixar um agradecimento à Universidade de Coimbra pelas oportunidades criadas e pela formação académica e pessoal ao longo destes anos.

Por fim, quero deixar uma palavra de agradecimento ao todos os familiares e amigos que, de uma forma ou outra, me acompanharam e apoiaram, presencial ou virtualmente, durante esta nova etapa de trabalho árduo.

Esta página foi deliberadamente deixada em branco.

Conteúdo

Acrónimos

3GPP *3rd Generation Partnership Project*. 5, 6

ABP *Activation by Personification*. 10

AES *Andvanced Encryption Standard*. 24

AS *Application Server*. 9, 13, 17, 18, 26–28

CA *Certificate Authority*. 16

CL-PKC *Certificate-less Public-Key Cryptography*. 17

D-BPSK *Differential Binary Phase-Shift-Keying*. 6, 7

DTLS *Datagram Transport Layer Security*. 16

ECDH *Elliptic Curve Diffie-Hellman*. 17

GFSK *Gaussian Frequency-Shift-Keying*. 7

GSM *Global System for Mobile*. 5, 6

HTTP *Hypertext Transfer Protocol*. 9

IDE *Integrated Development Environment*. 14

IDS *Intrution Detection System*. 24–28, 32, 33

IoT *Internet of Things*. iii, v, 1, 2, 5, 6, 13–15, 17–19, 21, 24, 25, 37, 53

KDF *Key Derivation Function*. 17

LoRaWAN *Long Range Wide Area Network*. iii, v, xiii, xv, 8–10, 12–18, 21–23, 26, 28, 37, 48, 50, 51, 53, 54

LPWA *Low Power Wide Area*. 5, 8, 53

LPWAN *Low Power Wide Area Network*. iii, v, 1, 5, 14, 18

LTE *Long Term Evolution*. 5, 6

LTE-M Long Term Evolution category M1. v

LTE-M *Long Term Evolution* categoria M1. iii, 6, 53

MAC *Media Access Control*. 7, 9

MCU Microcontrolador. 13–16

MIC *Message Integrity Code*. 9, 13

MQTT *Message Queuing Telemetry Transport*. 16

NB-IoT *Narrowband Internet of Things*. iii, v, 5, 6, 53

NS *Network Server*. 9, 10, 13, 15–18, 23, 26, 28, 54

OTAA *Over the Air Activation*. xiii, 10, 11, 18

PKI *Public Key Infrastructure*. 16, 18

PRB *Physical Resource Blocks*. 5

SHA *Secure Hash Algorithms*. 24

SO Sistema Operativo. 15

SSH *Secure Shell*. 16

VPN *Virtual Private Network*. 9, 16

Lista de Figuras

Lista de Tabelas

Esta página foi deliberadamente deixada em branco.

Capítulo 1

Introdução

1.1 Contexto

Internet of Things (IoT) é uma área vasta, com uma aplicabilidade muito diversificada, uma vez que cada rede IoT pode ter o seu propósito, dimensão e arquitectura. Tanto pode englobar pequenos projectos desenvolvidos a título individual, por exemplo a automatização do controlo da rega e humidade do solo das plantas de uma casa, como redes de nível industrial, por exemplo a monitorização da vários tipos de máquinas de uma fábrica. Redes com diferentes dimensões requerem diferentes tipos de arquitetura e protocolos de comunicação que suportem essas exigências e, por isso, existem protocolos para comunicações de curto e longo alcance. O foco deste trabalho incide sobre os protocolos de longo alcance que surgem para passar a área de IoT de uma escala local, como o ambiente doméstico, para uma escala mais ampla, como complexos industriais, cidades ou até mesmo países.

As redes criadas com este tipo de protocolos são designadas *Low Power Wide Area Network* (LPWAN), uma área que tem despertado a atenção de investigadores e industria com o intuito de a evoluir [5]. Por esta razão, o tema da segurança é cada vez mais relevante, dado o rápido crescimento desta área. Dadas a limitações que um dispositivo IoT tem, o aspecto da segurança torna-se um grande desafio, pois é preciso criar as condições necessárias à inclusão de sistemas de segurança robustos, sem comprometer o dispositivo em termos de longevidade da bateria, consumo de memória ou poder computacional, ambos muito reduzidos.

1.2 Abordagem

Depois de escolhidos os protocolos IoT de baixa energia que vão ser estudados e comparados, será procurada toda a informação referente às suas especificações, funcionamento e vulnerabilidade que possam existir. Após a comparação, será escolhido o protocolo que apresente uma oportunidade para inovar. Com o foco definido, serão procuradas melhorias já propostas pela comunidade científica para assim perceber que caminho tomar. Com o objectivo estabelecido, o trabalho irá incidir sobre a elaboração da nova proposta e o desenvolvimento e execução de testes para que seja feita uma análise dos resultados e tiradas as devidas conclusões quanto à abordagem sugerida.

1.3 Objetivos

Os objetivos da realização deste trabalho são:

- Melhorar a relação Segurança-Poupança de energia, arranjando um equilíbrio que permita poupar bateria sem que se ponha em risco a segurança dos dados;
- Otimizar o nível de segurança em comunicações IoT;
- Apresentação de um método que crie ou melhore esta propriedade no protocolo seleccionado;

1.4 Calendarização

Esta secção apresenta o planeamento do trabalho realizado ao longo da dissertação. Na figura 1.1 é possível observar o planeamento do trabalho que foi realizado ao longo do primeiro semestre.

Figura 1.1: Planeamento para a primeira parte da dissertação

Para o segundo semestre, o planeamento é apresentado no capítulo 3.

1.5 Estrutura

O documento encontra-se dividido em sete capítulos, que integram todo o trabalho realizado.

O capítulo 1 inicia o relatório com a introdução, onde é contextualizado o propósito do projeto, apresentada a abordagem a adotar e os seus objetivos, bem como a calendarização do primeiro semestre e a estrutura do documento.

O capítulo 2 corresponde ao Estado da Arte e está dividido em duas partes, sendo que na primeira secção são apresentados os vários protocolos importantes na área de IoT e de baixa energia e é feita uma comparação entre eles, e na segunda são apresentadas propostas de alteração existentes no meio científico e oportunidades de investigação com base na análise feita anteriormente.

No capítulo 3 refere-se à linha de investigação do segundo semestre incide, detalhando a proposta de trabalho.

O capítulo 4 expõe a arquitetura proposta para o controlador, assim como as decisões tomadas.

O capítulo 5 diz respeito ao processo de desenvolvimento do algoritmo.

No capítulo 6 são apresentados os testes realizados ao controlador e o seu *setup*, discutidos os seus resultados e ilustrado o seu comportamento e as diferentes respostas consoante as configurações definidas.

Por fim, o capítulo 7 aborda as conclusões tiradas e o trabalho futuro.

Esta página foi deliberadamente deixada em branco.

Capítulo 2

Estado da Arte

Neste capítulo é feita uma apresentação de todos os protocolos inseridos na categoria *Low Power Wide Area* (LPWA) que foram considerados mais relevantes, tendo sido escolhidas tecnologias recentes ou amplamente conhecidas e usadas em IoT. Após a apresentação das suas características, estas são comparadas para se perceber qual dos protocolos apresenta oportunidades de melhoria.

2.1 Tecnologias IoT de baixa energia

2.1.1 NB-IoT

O *Narrowband Internet of Things* (NB-IoT) é uma tecnologia do tipo LPWAN desenvolvida a partir das funcionalidades *Long Term Evolution* (LTE) pela *3rd Generation Partnership Project* (3GPP), organização criada por 5 empresas a nível mundial que visa padronizar novas tecnologias do ramo das telecomunicações. Foi criado com o intuito de se conseguirem dispositivos pouco complexos para comunicações de longo alcance, tendo a particularidade de ter também como objetivo a comunicação dentro de edifícios e para isso a sua potência de transmissão foi aumentada em 20 dB em comparação com a cobertura GPRS (uma tecnologia que melhora as comunicações *Global System for Mobile* (GSM) aumentando a taxa de transmissão dos pacotes de voz).

Este protocolo tem 3 modos de operação para que haja uma flexibilidade perante os recursos que existem para a sua implementação: 1)Modo Stand-alone: este protocolo é usado como alternativa ao GSM, permitindo o reaproveitamento da infraestrutura e do espectro. Neste modo a largura de banda usada é de 200kHz. 2)Modo Guard-Band: neste modo o protocolo é utilizado em paralelo com o LTE, utilizando a banda do canal não ocupada para transmissão, ao qual se chama Guard Band. Neste modo é usada uma largura de banda de 180kHz. 3)Modo In-Band: aqui o NB-IoT terá um ou mais *Physical Resource Blocks* (PRB) do LTE para usar, partilhando assim a gama útil da largura de banda do canal. Isto faz com que a potência da estação seja partilhada entre estas duas tecnologias.

O NB-IoT tem um tamanho de mensagem que pode variar entre 2 a 125 Bytes e é constituído por vários canais, derivados dos existentes no LTE com modificações para que se adequem à pequena largura de banda deste protocolo. Para o envio de mensagens (Uplink) existem dois canais: Narrowband Physical Uplink Shared Channel (NPUSCH) e Narrowband Physical Uplink Shared Channel (NPUSCH). Para a receção de mensagens (Downlink) existem 4 canais: Narrowband Physical Downlink Control Channel (NPDCCH), Nar-

rowband Physical Downlink Shared Channel (NPDSCH), Narrowband Physical Broadcast Channel (NPBCH), Narrowband Synchronization Signal (NPSS/NSSS).

Como NB-IoT pode ser parte integrante da rede principal de LTE, este garante mecanismos de segurança, autenticação, entre outros.

Uma vez que foi desenvolvido com base no LTE e o seu funcionamento envolve a utilização de infraestruturas de redes de comunicação móvel, é considerada uma tecnologia muito atrativa para as operadoras de telecomunicações que pretendam ter serviços IoT na sua oferta. [6, 7]

Apesar da atratividade e do facto de ser inovadora, existe pouca informação disponível no meio académico que nos dê informações mais detalhadas relativamente a esta tecnologia, possivelmente justificado pelo facto de ser proprietária.

2.1.2 LTE-M

Este é um protocolo também desenvolvido pela organização 3GPP e corresponde à abreviatura de LTE Cat-M1, ou seja, Long Term Evolution da categoria M1. É um protocolo para redes IoT muito semelhante ao NB-IoT uma vez que foi desenvolvido pela mesma organização e também tem por base os standards LTE. No entanto este protocolo tem uma particularidade que é a possibilidade de suportar a troca de mensagens de voz e vídeo, algo que pode ser considerado uma vantagem em relação aos outros protocolos.

O protocolo tem dois modos em que pode operar: reutilizando a infraestrutura e o canal GSM, ficando como seu substituto, ou utilizando a banda guardada do espectro que não é utilizada para comunicações LTE, chamado o modo Guard-band. Em ambos os modos é usado um *Data Rate* de 200Kbps e uma largura de banda que pode chegar até 1.4MHz (superior aos valores usados por outros protocolos incluindo o NB-IoT, porém muito inferior à frequência usada nos standards LTE de 10MHz).

O LTE-M é constituído por vários canais para o envio e receção de mensagens. Para Uplink existem 3 canais: Physical Uplink Shared Channel(PUSCH), Physical Random Access Channel (PRACH), Physical Uplink Control Channel (PUCCH). Para Downlink existem 4 canais: Enhanced Physical Downlink Control Channel (EPDCCH), Physical Downlink Shared Channel (PDSCH), Physical Broadcast Channel (PBCH), Synchronization Signal (PSS/SSS).

Uma vez que assenta nos standards LTE, os dispositivos de qualquer rede IoT que utilize este protocolo podem ligar-se directamente a uma infraestrutura 4G já existente para comunicar com os servidores, sem que seja necessária a implementação de *gateways* para suportar essa comunicação. Também por essa razão, todos os mecanismos de segurança, autenticação e outros são atribuídos ao LTE [8, 9, 10].

Assim como acontece com a tecnologia NB-IoT, também o *Long Term Evolution* categoria M1 (LTE-M) não dispõe de informação disponível muito detalhada.

2.1.3 Sigfox

O SigFox usa modelação *Differential Binary Phase-Shift-Keying* (D-BPSK) para transmitir dados. Funciona com 200kHz de banda e o *Bit Rate* pode variar entre dois valors, 100bps e 600bps, dependendo da região onde opera. Cada mensagem enviada tem um tamanho pequeno (26 Bytes) que garante um baixo consumo de energia e por consequên-

cia, uma grande durabilidade. Nesta arquitectura de rede, os dispositivos finais (sensores) comunicam com uma estação implementada pela empresa (SigFoz S.A.) que filtra o ruído das mensagens recebidas e redirecciona-as pela Internet até à SigFox Cloud. Estando na nuvem, os clientes podem aceder e interagir com toda a informação recolhida pelos sensores que é enviada para as suas plataformas e serviços. Este software é vendido como um serviço pela empresa responsável e pode ser usado em *Smart Cities*, no auxilia à agricultura ou automação de habitações, entre outros. No entanto, exige uma subscrição e trabalho directo com os responsáveis para a construção de uma rede SigFox. Isto faz com que este protocolo seja fechado a novas abordagens [11].

Segurança

A comunicação bidireccional não é feita de forma convencional, pois o cliente apenas pode comunicar com o sensor quando este o informar que estará à espera de uma resposta, estando apenas à escuta de mensagens quando esse pedido for enviado à rede. Este mecanismo previne que os dispositivos finais escutem mensagens de terceiros que poderão ter como objectivo a sua captura, alteração de informação, realização de acções, etc. Para além do aspecto de segurança, também aumenta a autonomia do dispositivo. Em termos de segurança na transição dos dados pela rede Sigfox, são usados vários mecanismos para manter a confidencialidade e integridade das mensagens trocadas. Entre os dispositivos finais e as estações onde os dados são tratados é usado um método de encriptação ponto-a-ponto com uma chave secreta. Esta é mantida numa parte da memória de cada dispositivo não acessível com permissões apenas de leitura, sendo usada para gerar uma assinatura que é única por mensagem e servirá para identificar o remetente. Esta assinatura contém um identificador numérico que é incluído no *frame* enviado pela rede e que impede que a mensagem seja duplicada. Para além deste mecanismo de encriptação, cada mensagem de um sensor é enviada 3 vezes em frequências distintas escolhidas aleatoriamente. Assim, a probabilidade de um atacante realizar *sniffing* é muito reduzida dadas as baixas hipóteses que tem de conseguir acertar nas frequências escolhidas. Entre as estações e a *cloud*, a comunicação é feita por um túnel VPN encriptado. A *cloud* corresponde a um conjunto de servidores seguros e distribuídos. Por fim, a troca de informação entre os clientes e a *cloud* é feita por HTTPS [11].

Abordagem Protocolar

Este protocolo está incutido nos sensores com o intuito de modular os *frames* de dados e transmiti-los, utiliza as 4 primeiras camadas do modelo OSI (Física, Ligação de Dados, Rede e Transporte) e é constituída pelas camadas: Frame, *Media Access Control* (MAC) e Física. Na camada Frame, o *payload* é recebido da camada de Aplicação e gera uma frame radio onde é adicionado o indicador numérico referido anteriormente. Na camada MAC, são adicionadas informações para a identificação do dispositivo que remete a mensagem e um conjunto de outros parâmetros *standard*. Nesta camada foi removida a parte do *signaling* para simplificar o protocolo, uma vez que se trata da troca de pequenas mensagens. Por fim, na camada Física, os sinais são sintetizados usando o modelo D-BPSK, para comunicações enviadas para a rede SigFox, e *Gaussian Frequency-Shift-Keying* (GFSK), para mensagens recebidas dessa rede. Aqui são geridos alguns parâmetros da transmissão das mensagens, como o Bit-Rate, que pode ser de 100 ou 600 bps, a força do sinal, 140dBm, e a frequência de transmissão, de 868MHz. Os valores de Bit-Rate e Frequência correspondem aos usados na Europa, sendo diferentes noutras partes do mundo [11].

2.1.4 LoRaWAN

Long Range Wide Area Network (LoRaWAN) é uma das tecnologias LPWA mais utilizadas e é considerado um *Open Standard* (protocolo que, apesar de estar definido por uma entidade, permite que lhe sejam feitas alterações por terceiros sem autorização previa). Tem flexibilidade para se adaptar a um determinado caso de uso e usa mecanismos de encriptação para garantir a confidencialidade e integridade da rede e da informação que nela circula.

Os principais pontos fortes do LoRaWAN destacados em [12, 13] são:

1. Não ser necessária uma subscrição de um serviço como acontece com SigFox e NB-IoT.
2. Diminuição dos custos, uma vez que é possível usar recursos fornecidos por outras entidades.
3. Ter uma cobertura grande utilizando um número reduzido de dispositivos.
4. Fácil instalação.
5. Suporte de comunicações bidireccionais.

Os seus pontos fracos são:

1. Problemas de segurança.
2. Funcionamento precário em redes com congestionamento de tráfego.

A especificação deste protocolo apenas define os aspectos técnicos, não impondo nenhum modelo para a sua implementação. As *gateways* usadas numa rede LoRa têm um custo reduzido e podem ser adquiridas por qualquer pessoa, permitindo que sejam criadas e geridas redes privadas conforme as necessidades dos utilizadores [13, 14].

Os *End-devices* podem ser divididos em 3 categoria: classe A, classe B e classe C. Cada uma destas classes define um tipo de comportamento para os sensores. Na configuração do tipo A, o sensor é sempre quem inicia, a qualquer altura, a comunicação para o servidor (*uplink*), seguindo-se de duas janelas para a recepção de comunicações do servidor (*downlink*) para a comunicação bidireccional. Neste modo, os dispositivos também podem hibernar para reduzir os consumos de bateria em alturas que não seja necessário comunicar com a rede. Assim, é considerada a classe mais eficiente em termos de consumo de energia, conferindo às baterias usadas a maior longevidade. É considerada a classe *default*, portanto todos os dispositivos LoRaWAN devem suportá-la. A Classe B resulta de um acrescento na classe anterior, sendo que nesta há sincronização de sensores na rede e janelas de *downlink* em alturas definidas. A possibilidade de serem enviadas mensagens do servidor para os sensores de uma forma mais sistemática aumenta o consumo de energia, no entanto neste tipo de configuração é mantida uma alimentação com recurso a baterias. Por fim, a Classe C é a que mais energia consome, por isso é recomendado que apenas seja utilizada por dispositivos que tenham acesso à rede eléctrica para um fornecimento constante. Este elevando consumo deve-se ao facto de que neste tipo de configuração os dispositivos ficarão constantemente à escuta de comunicações, tornando possível o envio de mensagens pelo servidor a qualquer altura, eliminando a latência comum neste tipo de comunicações

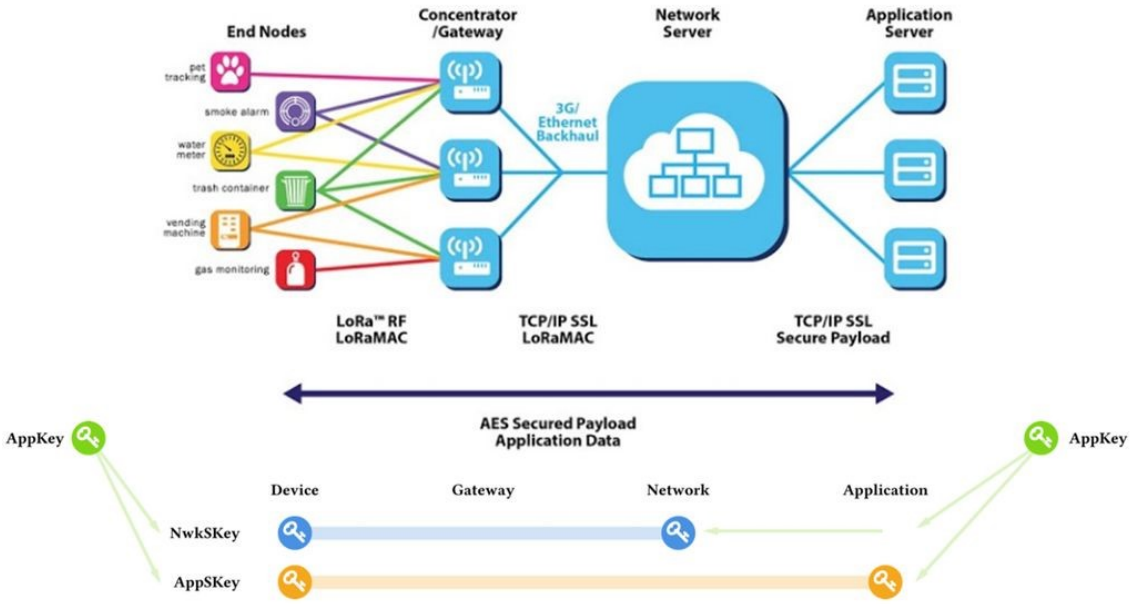

Figura 2.1: Arquitectura de uma rede LoRaWAN e os dois níveis de encriptação [1]

Mecanismos de segurança do protocolo LoRaWAN

São usados algoritmos AES para garantir a autenticidade e a integridade dos dados enviados para o servidor e a encriptação ponto a ponto ao nível da aplicação. Cada dispositivo LoRaWAN é pré-configurado com um identificador global único e uma chave AES única de 128bits (AppKey). Desta chave, também conhecida pela rede, derivam duas chaves de sessão: uma chave da rede (NwkSKey) para garantir a confidencialidade e provar a integridade e autenticidade da informação trocada entre sensores e servidores da rede, *Network Server* (NS); uma chave da aplicação (AppSKey) que garante a encriptação e integridade do *payload* ponto a ponto na infraestrutura, ou seja, desde os sensores até ao servidor da aplicação, *Application Server* (AS). Estas 3 chaves referidas são armazenadas em memória contra violações de um dispositivo cuja segurança física é crucial para garantir que as chaves não serão acessíveis ou extraídas. Um problema apresentado para esta metodologia é o facto de o fabricante ter acesso à AppKey, uma vez que esta é incluída no dispositivo LoRaWAN aquando do fabrico. Com acesso a esta chave, o fabricante pode gerar as duas chaves de sessão usadas nos mecanismos de segurança do protocolo e aceder à informação partilhada na rede.

Na prática, como mostra a figura 2.2, cada conjunto de dados, *payload*, é encriptado por AES-CTR usando a AppSKey. A este juntam-se um identificador do *payload* a enviar para impedir duplicação de mensagens e o *header* do protocolo, MAC *Header*. Por fim, é gerado um código de integridade, *Message Integrity Code* (MIC), por AES_CMAC usando a NwkSKey que impede alteração de informação.

Este mecanismo de encriptação que garante a integridade e protege as mensagens contra a sua duplicação juntamente com utilização de autenticação mútua na rede asseguram que os dados que circulam pela rede são confidenciais e têm como remetente um dispositivo autorizado e fidedigno. Para a segurança das interfaces de *Backend*, que envolvem a troca de informação sobre a rede e os dados recolhidos, são usadas as tecnologias *Hypertext Transfer Protocol* (HTTP) e *Virtual Private Network* (VPN) para garantir comunicações seguras [2].

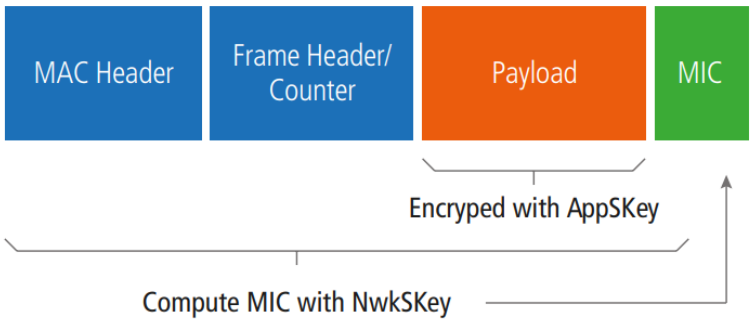

Figura 2.2: Estrutura de um pacote LoRaWAN [2]

Gestão de chaves

As chaves do sistema de segurança proposto para o LoRaWAN podem ser geradas de duas formas distintas, dependendo do processo escolhido para a activação dos sensores.

De um lado temos a activação por personalização, *Activation by Personification* (ABP). Um processo que consiste na inclusão das duas chaves de sessão, da rede e da aplicação, assim como um identificador único de cada dispositivo durante o processo de fabrico do mesmo. Como ambas as partes já possuem todos os elementos do mecanismo de segurança, chaves de encriptação e identificadores, quando o sensor é ligado pela primeira vez pode começar logo a transmitir informação.

Do outro temos a activação aérea, *Over the Air Activation* (OTAA), representada na figura 2.3. Apesar de ter uma complexidade maior, permite que os dispositivos alternem a rede onde são incluídos sem um acordo prévio entre o gestor da rede e o fabricante, como acontece na ABP. Para que a troca dos elementos necessários na criação das chaves de sessão seja realizada em segurança, é necessário utilizar uma outra chave, a Appkey, introduzida previamente no dispositivo. Quando um dispositivo LoRa se junta a uma rede, envia um JOIN_REQUEST encriptado com a chave Appkey. Este JOIN_REQUEST inclui o identificador único do *hardware* (DevUI), o identificador da aplicação (AppUI) que é incluido no sensor previamente à activação e um número gerado aleatoriamente (DevNonce). No NS, é recebido o pedido e são calculadas as chaves de sessão usando a AppKey, um número gerado aleatoriamente no servidor (AppNonce), o identificador do servidor da rede (NetID) e o DevNonce recebido. Assim são geradas: a AppSKey, a chave de sessão do nivel da aplicação, e a NwkSKey, a chave de sessão do nível da rede.

Posteriormente, é enviado um JOIN_ACCEPT em resposta ao pedido que inclui o AppNonce, o NetID, o identificador do dispositivo (DevAddr) que são encriptados com a AppKey. Quando o Sensor recebe a resposta, usa a informação recolhida juntamente com a informação que já tinha para gerar também as duas chaves de sessão necessárias. Estas serão iguais às que foram criadas no NS. No fim deste processo pode ser iniciada a comunicação com chaves simétricas entre sensores e o NS através das *gateways* [13].

Análise de risco e ataques ao protocolo LoRaWAN

Uma análise formal [5] feita ao protocolo LoRaWAN usando a ferramenta Scyther (realiza análises formais a protocolos de comunicação e segurança) concluiu que a versão 1.0 tem uma vulnerabilidade que resulta da falta de sincronização entre dispositivos. Este problema

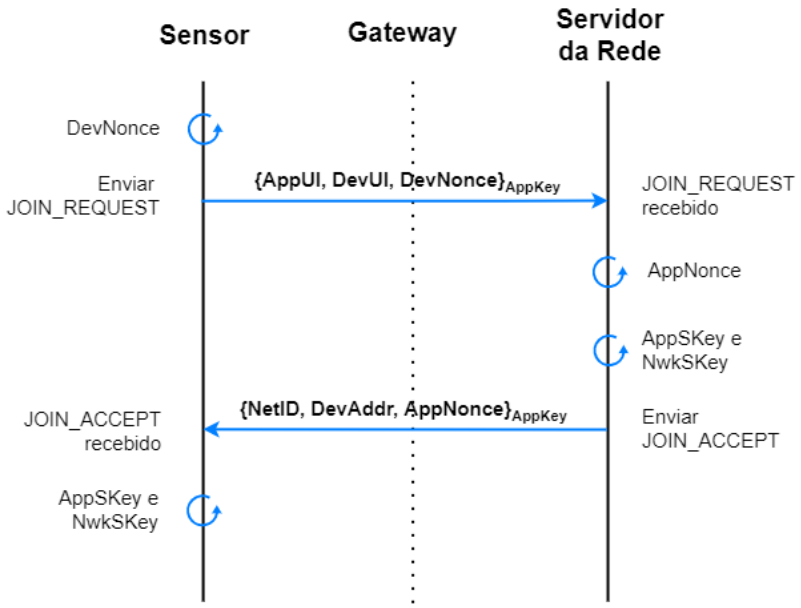

Figura 2.3: Troca de informação para a geração das chaves de sessão por OTAA [3]

expõe o protocolo a um tipo de ataque conhecido: *Replay Attack* (Um ataque do tipo *Man in the middle* feito através da rede, que consiste no atraso ou repetição de um conjunto de dados [15]).

Este protocolo foi melhorado com a introdução da versão 1.1 que veio corrigir algumas das falhas da versão anterior. No entanto, não colmatou todos os problemas, introduzindo novas ameaças à segurança com a nova *framework* de segurança ou por não especificar detalhadamente alguns aspectos do protocolo, o que leva a implementações com falhas de segurança. Estas falhas de segurança têm impacto na disponibilidade da rede e integridade e confidencialidade dos dados, sendo por isso um tema tão importante para o bom funcionamento do protocolo. Depois de ser feita uma categorização de vários ataques com base no impacto, dimensão e probabilidade para cada um, é dada especial atenção a 3 ameaças: *End-device Physical Capture*, *Rogue Gateway* e *Replay Attacks* [12].

2.1.5 Comparação entre Protocolos

Expostos os protocolos que foram considerados relevantes analisar, fazemos agora uma análise mais objectiva com recurso a tabelas para comparar os valores/respostas de cada protocolo para um determinado parâmetro [16, 17, 18, 19, 20, 21].

	LoRaWAN	SigFox	NB-IoT	LTE-M
Largura de banda	125 a 500 KHz	100 KHz	180 KHz ou 200 KHz	1.4 MHz
Data Rate Máximo	50 kbps (Adaptativa)	100 bps	200 kbps	1 Mbps
Limite de mensagens	Sem limite	Diário: 140 (enviar), 4 (receber)	Sem limite	Sem limite
Tamanho máximo de uma mensagem	243 Bytes	12 B (enviar), 8 B (receber)	1600 Bytes	1000 Byte
Comunicação	Half-duplex	Half-duplex com restrições	Half-duplex	Half-duplex
Alcance	5 a 20 km	10 a 40 km	1 a 10 km	11 km
Modos de Operação	Único	Único	In-Band; Guard-Band; Stand-Alone	Guard-Band; Stand-Alone
Modulação	CSS	BPSK	QPSK	QPSK
Rede Privada	Sim	Não	Não	Não
Responsavel	LoRa Allience	SigFox	3GPP	3GPP
Abertura	Semi-Industrial/ Semi-Proprietária	Industrial/ Proprietária	Industrial/ Proprietária	Industrial/ Proprietária

Tabela 2.1: Comparação geral dos protocolos

<table>
<tr><th></th><th>LoRaWAN</th><th>SigFox</th><th>NB-IoT</th><th>LTE-M</th></tr>
<tr><td>Confidencialidade</td><td>Sim, AES(128) pré configurada</td><td>Sim, mas Opcional</td><td>Sim, LTE</td><td>Sim, LTE</td></tr>
<tr><td>Integridade</td><td>Ao nível da rede Sim, para cada mensagem é gerado um MIC com a chave de sessão da rede; Ao nível da aplicação, depende do facto de ser implementado um mecanismo adicional que garanta que o NS não tem acesso ao payload destinado ao AS</td><td>Sim, cada mensagem é enviada em 3 frequências diferentes</td><td>Sim</td><td>Sim</td></tr>
<tr><td>Autenticação</td><td rowspan="2">Sim, com a chave de sessão da rede é gerada uma assinatura por cada dispositivo</td><td rowspan="2">Sim, é criada uma assinatura por cada mensagem de um dispositivo</td><td>Sim</td><td>Sim</td></tr>
<tr><td>Não repudiação</td><td>Sim</td><td>Sim</td></tr>
</table>

Tabela 2.2: Comparação dos protocolos a nível de segurança

2.1.6 Plataformas e Hardware de Desenvolvimento

Nesta secção são apresentadas informações sobre diversos dispositivos, plataformas e sistemas operativos usados para o desenvolvimento e teste de aplicações IoT que usam o protocolo LoRaWAN. Esta informação servirá para definir qual o dispositivo, plataforma e sistema operativo é mais adequado para a realização de avaliações experimentais, caso exista.

Arquitectura geral de um dispositivo LoRaWAN

Os dispositivos que suportam LoRaWAN são normalmente compostos por: um Microcontrolador (MCU), onde se encontra o CPU e a memória e é responsável por executar o programa incluído no dispositivo; uma Fonte de energia; um conjunto de Periféricos, normalmente sensores para recolha de informação, por exemplo sensores de humidade, temperatura ou presença; um módulo Rádio LoRa, modulação e desmodulação da infor-

mação, ou seja, transformar a informação binária em ondas electromagnéticas e vice-versa; uma Antena para possibilitar a recepção ou transmissão.

Para este tipo de dispositivos existem 3 tipos de arquitetura. Um primeiro onde o protocolo LoRaWAN corre no MCU principal e o Módulo LoRa é um componente distinto, um segundo em que o Módulo LoRa tem um MCU adicional incorporado para que o protocolo LoRaWAN não seja aplicado no MCU principal e um terceiro tipo em que o MCU principal contem o protocolo LoRaWAN e é incorporado com o Módulo de Rádio LoRa.

Hardware de Desenvolvimento

1. **B-L072Z-LRWAN1** é um dispositivo de desenvolvimento usado na plataforma IoT-Labs para simular ambientes IoT com o protocolo LoRaWAN, criado pela Murata Manufacturing. É constituído por um MCU STM32L072CZ, onde se encontram o CPU e a memória e é responsável por processar os comando incluidos no dispositivo. Inclui também um chip SX1276 (*transceiver*) desenvolvido pela Semtech, um módulo de radio LoRa responsável pela modulação e transmissão a longas distâncias da informação recolhida. Este dispositivo tem à disposição um conjunto de periféricos, usados para a recolha de dados, assim como a possibilidade de outros serem incluídos e usados de forma conjunta. Também suporta os 3 tipos de classes, classe-A, classe-B e classe-C, descritos no protocolo LoRaWAN [22, 23].

2. **LoPY**: Um dispositivo compacto para MicroPython que suporta LoRa, Wifi e BLE usado como uma ferramenta de desenvolvimento na plataforma The Things Network. É constituído por um MCU dedicado apenas à aplicação implementada e um chip LoRa SX1276 onde é incluído o protocolo LoRaWAN. Este dispositivo está desenvolvido de forma a suportar tanto o papel de *End-device* como o de *gateway* numa rede LoRaWAN [24, 25].

3. **FiPy**: É um dispositivo compacto para desenvolvimento e testes que usa MicroPython e muito semelhante ao LoPy. Suporta WiFi, Bluetooth e um vasto número de protocolos LPWAN como LoRaWAN, Sigfox, LTE_M CAT M1 e NB-IoT, sendo que estes dois últimos se inserem na categoria dos protocolos IoT celulares. Permite um alcance máximo de 50 Km, que irá variar consoante o protocolo usado e sua funcionalidade, inclui também um Chip LoRa SX1272 e o MCU principal apenas processa aplicação, sendo o protocolo LoRaWAN remetido para o chip usado [26].

4. **The Things Uno**: Este dispositivo é um dos recomendados pela plataforma The Things Network para o inicio de projectos de IoT com o protocolo LoRaWAN. Por ser considerado uma boa forma de iniciação na área, existem tutoriais e documentação disponibilizados pela plataforma referida. É composto por Arduino Leonardo ao qual se junta um Chip LoRa para a transmissão dos dados a longo alcance. Por pertencer à família dos Arduinos, é compatível com o *Integrated Development Environment* (IDE) desta marca e com *hardware* usado para expandir as funcionalidades e capacidades de uma placa, conhecido como *shields* [27].

5. **The Things Node**: Este segundo dispositivo da familia The Things é recomendado para quem é iniciante na área de IoT e LoRa mas também em electrónica. O The Things Node resulta da conjugação de um MCU compativel com Arduino, um módulo de radio LoRa para as transmissões de sinal e um conjunto de *hardware* pronto a ser usado, como sensores de luz e temperatura, leds e um botão. Tudo isto é alimentado apenas por 3 baterias que irão dar energia ao dispositivo por vários meses. Por ser

um dispositivo recomendado pela The Things Network, esta plataforma dispõe de documentação para ajudar a desenvolver projectos com este dispositivo [28].

6. **RAK811 WisNode LoRa Module**: É um dispositivo de desenvolvimento compatível com um Arduino Uno que tanto pode ser usado como um acessório deste ou como uma ferramenta independente. Apenas suporta o protocolo LoRaWAN e é constituído por um MCU STM32, para que possa processar uma aplicação de forma independente, e um chip LoRa SX1276 para a transmissão de pacotes segundo esse protocolo [29].

	B-L072Z-LRWAN1	LoPy	FiPy	The Things UNO	The Things Node
Memória Flash	129 KB	8 MB	8 MB	32 KB	32 KB
RAM	20 KB	4MB	4 MB	2,5 KB	2,5 KB
Chip LoRa	SX1276	SX1276	SX1276	RN2483	RN2483
Classes Suportadas	A, B e C	A e C	A e C	A	A

Tabela 2.3: Comparação entre dispositivos que suportam LoRaWAN

Plataformas

Existem duas plataformas que suportam o desenvolvimento e teste de infraestruturas LoRaWAN.

Uma delas é o **IoT-LAB**, uma plataforma científica de testes em larga escala que permite ao utilizador desenvolver a sua própria aplicação para usar nos dispositivos (sensores) suportados. O utilizador tem um controlo total sobre os sensores usados e tem a possibilidade de aceder às *gateways* que os seus dispositivos usam no processo de comunicação. Com os ambientes de teste usados também é possível ter acesso a resultados e à monitorização do comportamento da infraestrutura, podendo recolher diversas métricas sobre a rede (*End-to-End delay*, interferências, entre outras) ou consumo de energia. o IoT-LAB suporta um vasto número de dispositivos e sistemas operativos do ramo de IoT [30].

A segunda é o **The Things Network**, uma plataforma que pertence e contribui para a LoRa Allience. Funciona exclusivamente para a criação e desenvolvimento de redes IoT que usem o protocolo LoRaWAN, reunindo a informação sobe todas as *gateways* disponíveis a nível mundial que possam ser usadas para a implementação de uma rede LoRaWAN. Isto torna o desenvolvimento mais acessível a todos, tornando a implementação mais económica. O utilizador pode optar por adquirir o equipamento necessário ou usar uma infraestrutura já existente para se ligar a um NS que irá passar a sua informação para aplicação pretendida [31].

Sistemas Operativos e Linguagens de Programação

Riot: É um Sistema Operativo (SO) *Open Source* usado na área da IoT. Foi desenvolvido por uma comunidade que inclui universidades, empresas e programadores a titulo individual. Suporta um grande número de arquitecturas quer de MCU como de dispositivos. Para perceber melhor o papel deste SO é usada a analogia dizendo que este é tão importante para a IoT como o Linux é para a Internet [32].

MicroPython: É uma linguagem de programação escrita em C99, compatível com o Python 3. Contem um pequeno conjunto de bibliotecas Python e é optimizado de forma a poder ser usada num MCU. É possível utilizá-lo segundo a licença do MIT, alterar ou adaptar para um fim comercial ou pessoal, sem qualquer custo. É o mais próximo da linguagem Python possível para facilitar a conversão de código para ser utilizado num MCU e a programação neste novo formato, pois quem já sabe programar em Python saberá utilizar o MicroPython [33].

2.2 Melhorias já propostas para o protocolo LoRaWAN

Aqui são apresentadas as propostas de investigação existentes no meio académico cujo foco é melhorar a segurança do protocolo LoRaWAN. Estas vêm sugerir métodos alternativos de funcionamento para problemas que consideram relevantes.

A arquitectura proposta em [34] usa uma infraestrutura de chave publica, *Public Key Infrastructure* (PKI). É atribuído a cada componente da rede um certificado gerado pela Autoridade de Certificação, *Certificate Authority* (CA), da rede, que é usado para a realização de comunicações dentro desta infraestrutura. Assim é garantida a confidencialidade e integridade dos dados por via da encriptação na troca de dados. Para além disto, foram implementadas regras na IPTables em cada dispositivo da rede para que apenas se realizem as comunicações necessárias ao bom funcionamento da aplicação e sejam permitidas comunicações *Secure Shell* (SSH) para actualizações e manutenção à rede. Como as *gateways* são consideradas pontos não fidedignos por se encontrarem fora da área controlada, os autores propõem a utilização de um servidor de VPN, usando a ferramenta OpenVPN, que atribui a cada *gateway* um certificado que esta usa para se autenticar nas comunicações com a rede interna. Este mecanismo, associado a uma lista de IPs das respectivas *gateways* usadas na rede, previne que o sistema seja acedido por dispositivos não autorizados. Já dentro da rede interna do sistema proposto, a comunicação entre as *gateways* e os *Brokers* (transporta as mensagens dos dispositivos finais enviadas através de *gateways* até às camadas superiores da rede) usa *Datagram Transport Layer Security* (DTLS) para tornar seguras as comunicações via UDP. Deste ponto, é usado o protocolo *Message Queuing Telemetry Transport* (MQTT), implementado nos Brokes, para que a informação transmitida por TCP chegue aos Servidores da Rede de forma segura. No que toca ao Network Server, é recomendado que a implementação do mecanismo de gestão de chaves seja meticulosamente bem implementada visto que é um ponto critico de gestão da infraestrutura e recepção de informação numa arquitectura LoRaWAN.

Em [35] é proposta a adição de um quarto elemento na arquitectura do LoRaWAN, gerido de forma independente e que seria responsável pela gestão das chaves de encriptação, gerar e distribuir correctamente as chaves para que os diferentes dispositivos apenas tenham conhecimento da sua respectiva chave de sessão. Isto previne que o NS consiga saber a chave de sessão da aplicação e assim ter acesso à informação que deveria apensa ser visível para o servidor da aplicação. Para além disto, é proposto que a AppKey seja diferente a cada sessão para dificultar o comprometimento das chaves de sessão geradas, a NwkSKey e AppSKey. Outra alteração é a utilização de um *timestamp* em vez de números aleatório usados para gerar as chaves criptográficas. Cada dispositivo guarda o último *timestamp* recebido e compara-o com o recebido na próxima mensagem, se a diferença for menor que o esperado então a mensagem é descartada. Isto é utilizado para prevenir *Replay Attack*.

Os autores de [36] propõe a utilização de Blockchain para melhorar a confiança do servidor de rede e a segurança de toda a infraestrutura. Esta alteração é aplicada ao NS por ser o

único elemento do protocolo LoRaWAN com capacidade e recursos para a sua implementação, uma vez que tanto a *gateway* como os dispositivos finais não dispõem de capacidade computacional para suportar Blockchain. Esta proposta consiste na inclusão, no NS, de um "Blockchain Management component"[36] que é responsável por fazer a ponte com outros servidores para colocar em funcionamento este protocolo. Aqui a mensagem é empacotada, é criada a *hash* desse pacote, é verificado, é criado o bloco e incluído na Blockchain para ser armazenado. O mecanismo apresentado garante um sistema seguro e confiável que tem a capacidade de verificar que uma determinada mensagem foi transmitida pela rede num momento especifico. Os autores afirmam que, para seu conhecimento, esta proposta de integração de Blockchain é a primeira a aparecer.

Em [37] podemos ler que independentemente do processo de activação escolhido no LoRaWAN, todas as chaves são fixas, não havendo uma renovação periódica que aumentaria o nível de segurança deste protocolo. Seria uma mais valia poder actualizar as chaves de sessão num determinado período de tempo para assim aumentar o nível de segurança das comunicações no LoRaWAN. A proposta é utilizar EDHOC, um protocolo de gestão de chaves simétricas entre dois dispositivos que é baseado no SIGMA-I e implementa o algoritmo *Elliptic Curve Diffie-Hellman* (ECDH) com a curva P-256. Este novo mecanismo será usado para renovar as chaves de sessão assim que o dispositivo estiver activado, acrescentando uma flexibilidade a todo o processo de gestão de chaves. Para isso, "apenas são trocadas 3 mensagens entre o sensor e o NS para actualizar"[37] as duas chaves de sessão, da rede e da aplicação. Para a geração das novas chaves é na mesma usado o algoritmo AES com 128 bits e acrescenta-se o uso de *Key Derivation Function* (KDF) para garantir a total independência entre as novas chaves de encriptação e as que serão substituídas.

Outra alternativa apresentada em [38] propõe que a gestão de chaves seja feita através de chaves publicas sem o uso de certificados, implementando *Certificate-less Public-Key Cryptography* (CL-PKC). Este é um método leve em termos de memória e computação e por isso é considerado uma boa escolha para redes IoT dada a baixa capacidade de memória RAM e flash característica deste tipo de dispositivos.

Em [39] é proposto o uso de duas chaves de activação. Este método é muito semelhante ao especificado pela LoRa Alliance no entanto usa mais uma chave pré configurada para separar a gestão de chaves das duas camadas da arquitectura, a camada de rede e da aplicação. Esta abordagem usa uma chave, *AppKey*, para gerar uma chave de sessão entre o dispositivo final e o AS e outra, *NwkKwey*, para gerar a chave de sessão entre o dispositivo final e o NS. Desta forma, o problema do NS ter acesso à chave de sessão do nível da aplicação é solucionado. Também é proposto um mecanismo de actualização das chaves de sessão, para aumentar a segurança do sistema. Esta actualização usa as actuais chaves de sessão de cada camada para auxiliar a criação das novas chaves de sessão, descartando no final a chave de sessão anterior para que não haja forma de um atacante conseguir obter as novas chaves geradas.

Após a análise de cada uma das propostas apresentada, é perceptível que cada uma apresenta uma solução para resolver os problemas apresentados, relacionados com confidencialidade e gestão de chaves. Isto vem reforçar as lacunas existentes neste protocolo, identificando diversas oportunidades de melhoria no LoRaWAN.

2.3 Oportunidades de Investigação

Nesta secção serão apresentadas as oportunidades encontradas para o protocolo LoRaWAN. Estas oportunidades surgem da análise de propostas existentes no meio científico, apresen-

tadas na secção 2.2, que identificam possíveis falhas nos *standards* do protocolo LoRaWAN, identificando, assim, caminhos de investigação que poderão ser seguidos.

1. Gestão das chaves: Como foi explicado anteriormente, o protocolo LoRaWAN tem uma chave pré-configurada a partir da qual são geradas duas chaves de sessão para garantir dois níveis de encriptação, da rede e da aplicação. No entanto, ambas as chaves de encriptação são geradas no NS, o que faz com que seja possível aceder através deste servidor às mensagens destinadas apenas ao AS. Isto é considerado um problema quando ambos os servidores não são geridos pela mesma entidade. Uma alternativa para solucionar este problema passa por transferir a gestão das chaves para uma entidade externa, não permitindo que as chaves sejam todas partilhadas com uma ou mais entidades.

2. Confidencialidade: A criação das chaves criptográficas de sessão durante a activação de um sensor é um processo complexo. Tanto pode envolver a troca directa das mesmas entre as entidades responsáveis por pré configurar os sensores e os servidores, como pode envolver a troca de informação, ainda que encriptada, para que seja possível gerá-las, tanto em cada sensor como no NS, o que envolve alguns riscos. Em alternativa, poderia ser usada uma PKI para que apenas fossem transferidas as chaves públicas, a que qualquer entidade pode ter acesso, tornando o acesso à informação impossível sem a respectiva chave privada, que apenas será do conhecimento de cada entidade. Com esta abordagem, continua a ser possível implementar dois níveis de encriptação, da rede e da aplicação, sem que o NS tenha conhecimento da chave do nível da aplicação, resolvendo também o problema da gestão de chaves apresentado no ponto anterior.

3. *Frame Counter*: Este é um mecanismo utilizado pelo LoRaWAN como forma de controlar as mensagens, prevenindo a sua repetição ou a recepção de informação desactualizada. No entanto, a inclusão deste mecanismo no sistema de segurança usado para cada rede IoT é opcional e pode tornar todo o sistema vulnerável a *Replay Attacks*.

4. Número Aleatório: Conforme explicado no ponto 2.1.4, a criação das chaves usando o método OTAA envolve, entre outras informações, a troca de um número gerado aleatoriamente que irá identificar o dispositivo que o utilizou. Portanto, dois diapositivos da mesma rede não poderão utilizar o mesmo número aleatório para a geração das chaves criptográficas sob pena de um deles não ser admitido na rede por não poder ser activado. Assim, este ponto é assinalado como um alerta a ter em conta aquando da criação de uma rede IoT usando LoRaWAN com OTAA. É importante que o número aleatório seja gerado com o maior número de bits possível para diminuir a probabilidade de dois dispositivos finais chegarem ao mesmo resultado, impedindo assim que um deles se junte à rede.

2.4 Conclusão

Apresentados e analisados os vários protocolos IoT para LPWAN, o protocolo LoRaWAN revelou ser o mais promissor, tendo sido a sua abertura um fator preponderante nesta decisão. Após esta escolha, foram comparadas as propostas já existentes para este protocolo, bem como as respetivas oportunidades de investigação encontradas, surgiram várias hipóteses para o trabalho a desenvolver, como por exemplo a proposta de um novo mecanismo de gestão de chaves ou o reforço da confidencialidade. No entanto, sendo a energia um

tema importante para a tecnologia, tanto em IoT, como para futuros sistemas 5G, uma proposta de trabalho sobre gestão combinada de energia e segurança é também uma hipótese relevante, pondendo eventualmente ser combinada com o assunto da confidencialidade.

Esta página foi deliberadamente deixada em branco.

Capítulo 3

Proposta de Trabalho

Neste capítulo é apresentada a proposta de trabalho para a segunda parte da dissertação, assim como o seu planeamento.

3.1 Introdução

Após a análise apresentada no capítulo 2 e as reflexões apresentadas na secção 2.4, a proposta de trabalho escolhida incidiu sobre Gestão Dinâmica de Segurança. A razão que levou à escolha deste tema prende-se com o facto de a energia e a poupança de bateria serem temas fulcrais em IoT. Ao longo dos anos a tecnologia tem tido uma evolução rápida, o que implica custos energético maiores. No entanto, as baterias não têm acompanhado essa evolução, sendo preciso colmatar essa falta com o auxílio de software capaz de criar um equilíbrio entre um bom funcionamento do sistema e a poupança de bateria. Uma vez que o desejo de prolongar o tempo de vida das baterias usadas nos sensores tem que ser conjugado com a desvantagem de estes não suportarem baterias com capacidades muito grandes, dado o seu tamanho reduzido, esta proposta de trabalho é feita com o objetivo de encontrar um equilíbrio entre a segurança e a poupança de energia, tentando ao máximo aumentar o tempo de vida de um sensor sem pôr em causa a segurança dos dados da infraestrutura. Em contraste com infraestruturas LoRaWAN que usam normalmente um esquema de segurança fixo, esta proposta tanto permite que se aumente o nível de segurança a usar para combater ataques mais graves, como se diminua esse mesmo nível para poupar bateria em alturas menos críticas para a segurança.

3.2 Objetivos de investigação

Nesta secção, são apresentados os detalhes da proposta de trabalho que foi realizada na segunda metade da dissertação.

Propostas

A proposta consiste no desenvolvimento de um mecanismo que permite a alteração de forma dinâmica do esquema de segurança de uma rede IoT com LoRaWAN. Isto permite que uma rede adapte o seu esquema de segurança usado consoante factores como o nível de bateria, prolongando a sua vida útil. Para isto, foi necessário dividir o trabalho em

duas fases: uma primeira, onde o controlador foi pensado e desenvolvido, propondo uma arquitetura e elaborando o seu algoritmo; uma segunda, correspondente à planificação e realização de testes, tendo sido necessário fazer um estudo prévio sobre o impacto que cada mecanismo de segurança e a transmissão de mensagens tem no consumo de energia dos dispositivos da rede. Por fim, a comparação dos resultados obtidos com o *standadrd* do LoRaWAN serviu para tirar conclusões sobre o comportamento do controlador, a sua viabilidade e o cumprimento ou não dos objetivos.

O procedimento realizado para esta proposta tem as seguintes tarefas:

- Proposta de uma arquitetura que inclui o controlador;
- Desenvolvimento e adaptação do algoritmo que incorpora o adaptador;
- Estudo do impacto energético dos mecanismos de segurança (AES e SHA) e da transmissão de mensagens numa redeLoRaWAN;
- Implementação e avaliação;
- Análise dos resultados;
- Demonstração do comportamento do controlador.

3.2.1 Planeamento

A figura 3.1 apresenta o planeamento da segunda parte da dissertação. As barras cinzentas correspondem à previsão feita no início da segunda fase para o trabalho a desenvolver, enquanto que as barras pretas correspondem ao momento em que cada tarefa foi efetivamente realizada.

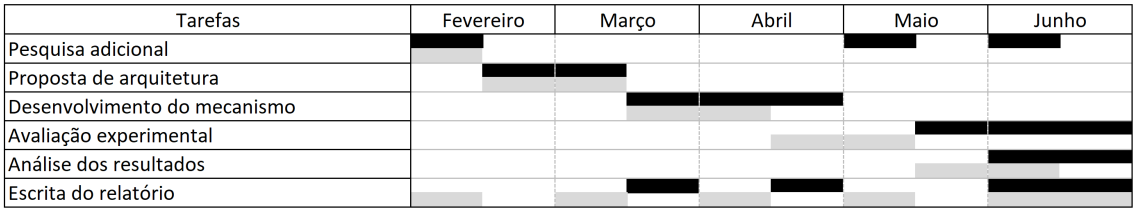

Figura 3.1: Planeamento previsto para a segunda metade da dissertação

Capítulo 4

Arquitetura

Neste capítulo é apresentada a arquitetura do controlador dinâmico de segurança desenvolvido, proporcionando uma visão geral do seu funcionamento, bem como uma abordagem mais específica ao nível do sistema e do protocolo.

4.1 Visão geral

O controlador dinâmico de segurança permite que uma rede LoRaWAN altere o esquema de segurança em uso, para que haja uma gestão mais articulada entre o nível de segurança e o consumo de energia, prolongando assim a vida útil das baterias que alimentam os sensores e gerindo a segurança de forma dinâmica e inteligente, por forma a fazer face a possíveis ameaças internas ou externas à segurança das comunicações.

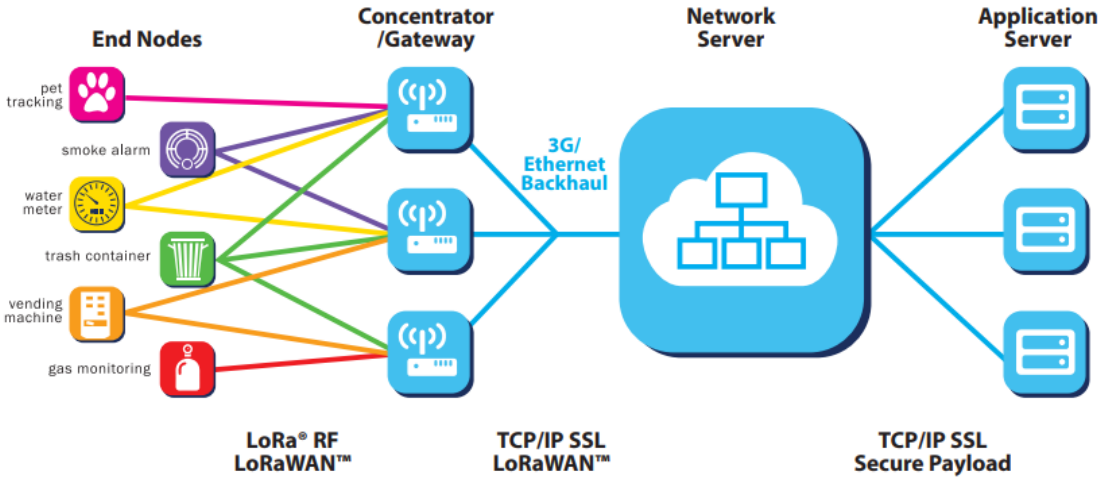

Figura 4.1: Visão geral da arquitetura

No caso do desenvolvimento do controlador dinâmico de segurança não será preciso alterar a arquitetura *standard* de uma rede LoRaWAN, apresentada na figura 4.1.

O controlador será colocado no NS por se tratar do componente central de rede LoRaWAN e, como tal, tem acesso a toda a informação que nela circula.

4.2 Requisitos Funcionais

4.2.1 Input

Para que seja feita a análise do estado da rede e proposta a alteração do mecanismo de segurança que irá proteger as comunicações de ataques externos, o controlador precisa de um conjunto de informação de vários pontos da rede. Assim, os parâmetros definidos como *input* são:

- Percentagem de bateria do sensor;
- Nível de segurança inicial/desejável para a rede, apresentado na tabela 4.1;
- Nível mínimo de segurança permitido na rede, apresentado na tabela 4.1;
- Fator preferencial, entre segurança ou longevidade das baterias, apresentado por um valor numa escala de 0 a 100, representando uma percentagem;
- Análise de segurança, feita pelo *Intrution Detection System* (IDS), que reporta um determinado ataque que seja detectado usando uma escala numérica. Esta escala inicia-se em 1 e o máximo é definido pelo utilizador, que também atribui um ataque a um índice;
- Perfil de segurança, uma tabela definida ao nível da aplicação e configuração do controlador que faz a correspondência entre o índice reportado pelo IDS e a percentagem de impacto que esse ataque externo tem para o sistema IoT.

4.2.2 Output

O *output* será um esquema de segurança adequado consoante as informações que cheguem ao controlador. Cada esquema de segurança conjuga um determinado nível de confidencialidade (para o qual será usado o algoritmo de encriptação *Andvanced Encryption Standard* (AES)) com outro de integridade (usando a função de *hash Secure Hash Algorithms* (SHA)). O resultado pode ser um de cinco níveis disponíveis, apresentados na tabela 4.1.

4.2.3 Requisitos de Comportamento

Para que o controlador atinja os resultados pretendidos, é necessário garantir que um conjunto de ações se realizam:

- Alteração do nível de segurança perante um novo registo de percentagem de impacto diferente da anterior;
- Diferenciação dos valores calculados perante diferentes fatores preferenciais;
- Atenuação do esquema de segurança sugerido conforme vai ocorrendo o desgaste da bateria;
- Não sugerir esquemas de segurança abaixo do nível mínimo definido ao nível da aplicação.

4.3 Tabelas de níveis

Para compreender melhor o controlador e algumas variáveis essenciais ao seu funcionamento, apresentamos tabelas exemplificativas dos níveis de segurança a usar e de ataques, definidas ao nível da aplicação e necessárias para que o controlador faça os cálculos pretendidos.

Segurança

A tabela 4.1 ilustra um exemplo de esquemas de segurança definidos pelo utilizador, onde a cada nível de segurança está associado um índice para que seja facilmente identificado e, quanto maior o índice, mais forte o esquema de segurança. A informação desta tabela é enviada às várias entidades do sistema para que saibam que esquema de segurança corresponde à resposta do controlador.

Nível	Esquema de Segurança		Poupança de bateria	Protecção
	Confidencialidade	Integridade		
1	-	-	Muito Forte	Fraca
2	-	SHA1	Forte	Moderada
3	AES128	-	Forte	Moderada
4	AES128	SHA1	Moderada	Forte
5	AES258	SHA2(258)	Fraca	Muito Forte

Tabela 4.1: Níveis de segurança

Ataques

A tabela 4.2 é um exemplo de uma tabela definida ao nível da configuração do controlador que será usada pelo IDS para converter um ataque no seu respetivo índice, que o identifica no sistema. Esse índice será depois usado para perceber qual o impacto desse ataque para esta estrutura IoT.

Índice	Ataque
1	Spoofing
2	Hijacking

Tabela 4.2: Tipos de Ataques

A tabela 4.3 é um exemplo de uma tabela de Perfil de Segurança, criada para fazer a relação entre cada índice que representa um ataque e a respetiva percentagem de impacto definida pelo utilizador.

Índice	Percentagem de Impacto
1	45%
2	10%

Tabela 4.3: Perfil de segurança

Esta abordagem permite que o controlador dinâmico de segurança seja usado em diferentes sistemas e arquiteturas IoT, uma vez que permite que o mesmo ataque tenha diferentes

tipos de impacto consoante o objetivo do utilizador para o sistema, não sendo necessário fazer alterações ao esquema ou ao código fonte do controlador.

4.4 Visão de sistema

A visão de sistema pretende mostrar o local de cada componente na arquitetura e as comunicações que existem entre eles.

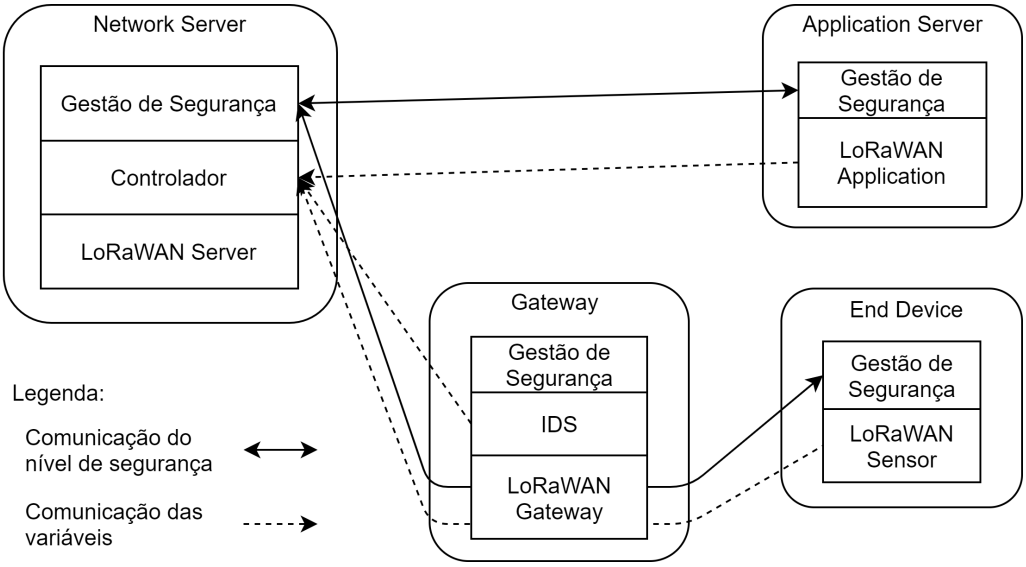

Figura 4.2: Visão de sistema da arquitetura proposta

Como ilustra a figura 4.2, todos os componentes da rede LoRaWAN mantêm as suas funcionalidades originais, sendo apenas acrescentadas outras funções ao NS e às *Gateways*. No caso do NS, este componente mantém a funcionalidade base de um servidor de rede LoRaWAN (filtragem da informação vinda dos sensores e encaminhamento dos respetivos *payloads* para o AS) e é adicionado o controlador dinâmico de segurança. Nas *Gateways* é adicionado um IDS para auxiliar o controlador, permitindo a avaliação do estado da rede no que se relaciona com as intrusões e ataques externos com base na análise das comunicações. Esta informação irá ajudar o controlador a decidir qual o esquema de segurança que deve ser implementado, aumentando o nível de segurança caso a rede esteja sobre ataque ou, caso contrario, diminuindo-o, preservando as baterias dos sensores.

Em todos os elementos da arquitetura LoRaWAN será adicionado um componente para a gestão de segurança que irá ser responsável por enviar informações sobre o esquema de segurança em uso ou receber informações para a implementação do novo esquema sugerido pelo controlador.

4.5 Visão Protocolar

Nesta secção é apresentada a troca de informação necessária ao funcionamento do controlador, estando dividida em duas fases: a de *setup* e a do comportamento normal do controlador dinâmico de segurança.

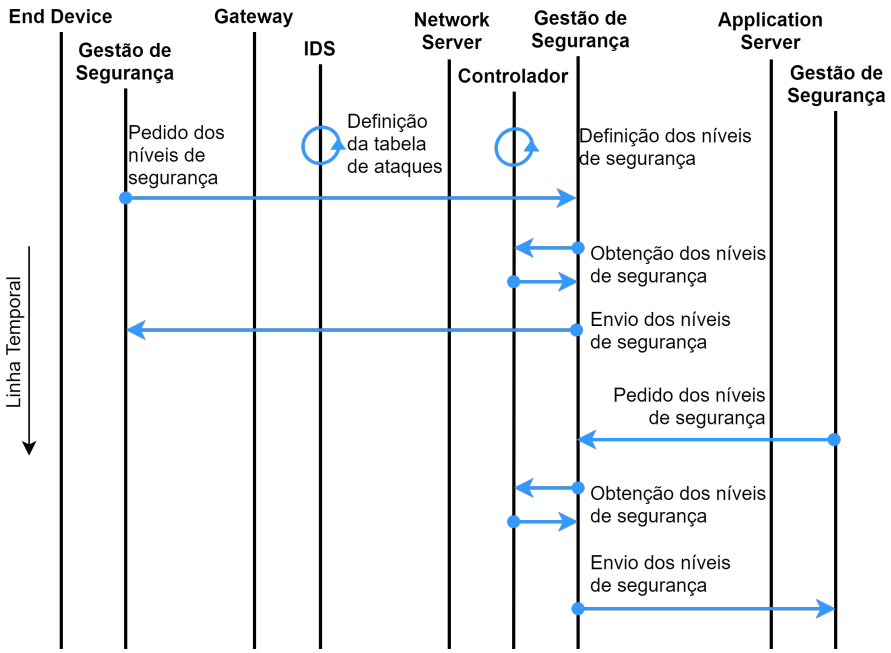

Figura 4.3: Visão protocolar de *Setup* da arquitetura proposta

Na figura 4.3 são apresentados os fluxos de dados, a sua origem e o seu destino para a configuração inicial do controlador. Esse processo consiste na partilha dos níveis de segurança adicionados ao controlador com os restantes elementos que precisam dessa informação, os sensores e o AS, a definição da tabela de ataques e da tabela de perfil de segurança, necessárias para compreender e adaptar a informação obtida e enviada pelo IDS.

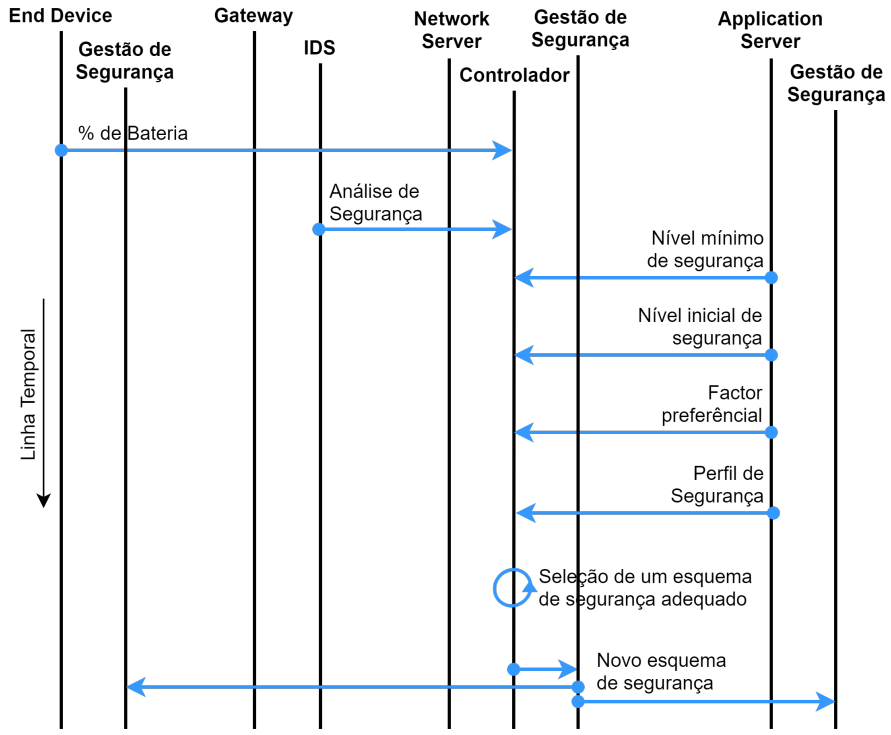

Figura 4.4: Visão protocolar da arquitetura proposta

Na figura 4.4 é apresentado o esquema de troca de informação no decorrer do funcionamento do controlador, onde este recebe um conjunto de informação de vários componentes da rede. A percentagem de bateria é enviada pelo sensor e a análise de segurança é retirada do IDS. As restantes mensagens são enviadas pelo AS, dando a conhecer o nível mínimo de segurança que a rede tem de ter, o nível desejável e o fator preferencial da rede (segurança ou bateria). Após reunida toda a informação necessária, o controlador analisa-a e selecciona um esquema de segurança adequado. Este esquema é depois dado a conhecer ao sensor, ao NS e ao AS, uma vez que o LoRaWAN prevê encriptação ao nível da rede e da aplicação.

4.6 Conclusão

Com a apresentação da arquitectura proposta para o controlador dinâmico de segurança e a identificação das variáveis e processo de funcionamento, é possível entender melhor qual a proposta trabalhada, assim como a função e objetivos deste controlador. Esclarecido o seu funcionamento e o seu papel numa arquitetura LoRaWAN, é possível passar à apresentação do processo de desenvolvimento do algoritmo que o irá integrar.

É também importante referir que o trabalho incide sobre o controlador, com o desenvolvimento e teste do respetivo algoritmo. No entanto, este depende de outros componentes apresentados neste capítulo aos quais não é dado destaque, mas que fornecem informações essenciais, como é o caso do IDS, Gestor de Segurança e dos restates elementos que integram a arquitetura padrão do LoRaWAN.

Capítulo 5

Implementação

Depois de apresentada a arquitetura e funcionamento geral do controlador, neste capítulo são abordados os pontos relativos ao desenvolvimento do algoritmo.

5.1 Decisões de Implementação

O algoritmo foi desenvolvido com recurso a operações aritméticas simples (somas, subtracções, multiplicações e divisões), médias e funções quadráticas.

Para calcular o nível de segurança mais apropriado, foram utilizadas 3 variáveis: fator preferencial, percentagem de impacto de um ataque e percentagem de bateria de um sensor. Destas, apenas a primeira variável tem uma relação inversamente proporcional com o resultado, ou seja, uma vez que o fator preferencial demonstra a importância que o utilizador quer dar à bateria em detrimento da segurança, quanto maior este fator, maior será a preferência pela poupança da bateria e, por isso, menor terá de ser o nível de segurança sugerido.

Esta formula foi criada em várias etapas para controlar e facilitar o seu desenvolvimento. Numa primeira fase foram apenas tidas em conta duas variáveis, o fator preferencial e a percentagem de impacto do ataque. Após obter resultados satisfatórios e com o objetivo de poupar bateria, foi incluída a percentagem de bateria como um fator atenuante desse resultado.

Para que o algoritmo tenha uma resposta mais adequada, foram definidos intervalos para duas variáveis fundamentais. Para o fator preferencial foram definidos 4 intervalos, apresentados na tabela 5.1, sendo que quanto mais perto de 100% se encontrar o valor será preferida a poupança da bateria em detrimento da segurança e o contrário caso se aproxime de 0%. Quanto à percentagem de bateria do sensor, são definidos 3 intervalos (0-25%, 25-75%, 75-100%), feitos com base na curva de descarga de uma bateria alcalina exemplificada na figura 5.1 permitindo, assim, comportamentos mais ou menos agressivos.

Intervalos do fator preferencial					
0 %	]0;20[%	[20;50[%	[50;80[%	[80;100[%	100 %
Segurança Total	Segurança Forte	Segurança Fraca	Poupança Fraca	Poupança Forte	Poupança Total

Tabela 5.1: Intervalos do fator preferencial

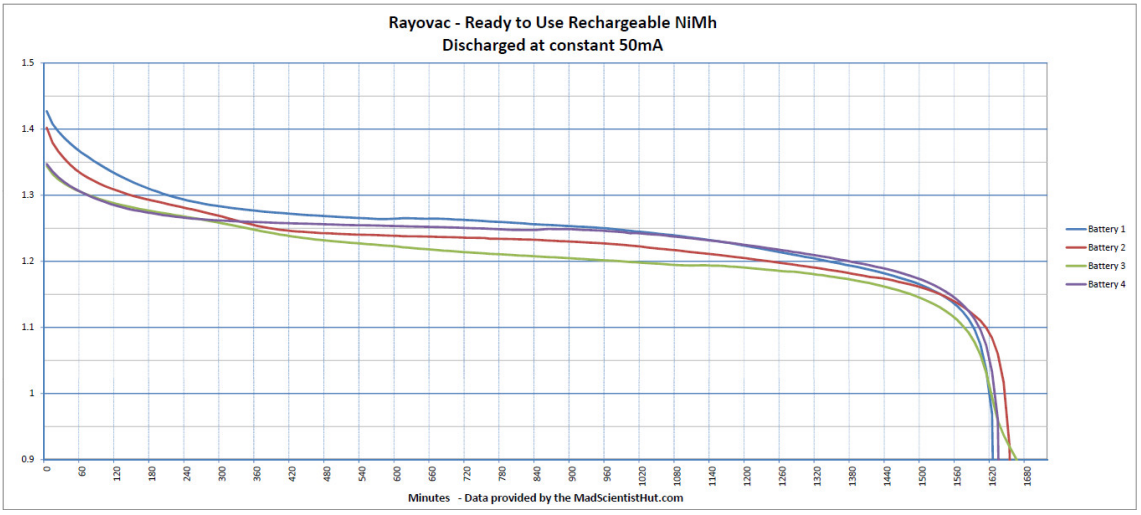

Figura 5.1: Gráfico de descarga de uma bateria [4]

5.2 Lógica do Controlador

Aqui é apresentado o algoritmo desenvolvido para fazer a gestão de dinâmica segurança, com o fluxograma é ilustrada a lógica do algoritmo e com o pseudocódigo apresentamos o código desenvolvido para testar o comportamento da lógica apresentada.

5.2.1 Fluxograma

A figura 5.2 mostra o fluxograma representativo do algoritmo desenvolvido que permite perceber como é obtido o esquema de segurança a ser sugerido pelo controlador.

Depois de receber todas as variáveis necessárias, indicadas na secção 4.2, a primeira decisão é sobre o fator preferencial definido. Isto vai decidir a forma como é calculado o novo esquema de segurança, uma vez que, por cada intervalo definido para esta variável, existe uma fórmula diferente. Após o calculo do esquema de segurança a ser sugerido, é verificado o nível de bateria do sensor nesse momento para aplicar a devida atenuação. Assim como acontece com o fator preferencial, também a percentagem de bateria tem intervalos que definem diferentes atenuações. O resultado deste processo é o novo nível de segurança a ser adotado pelo sistema.

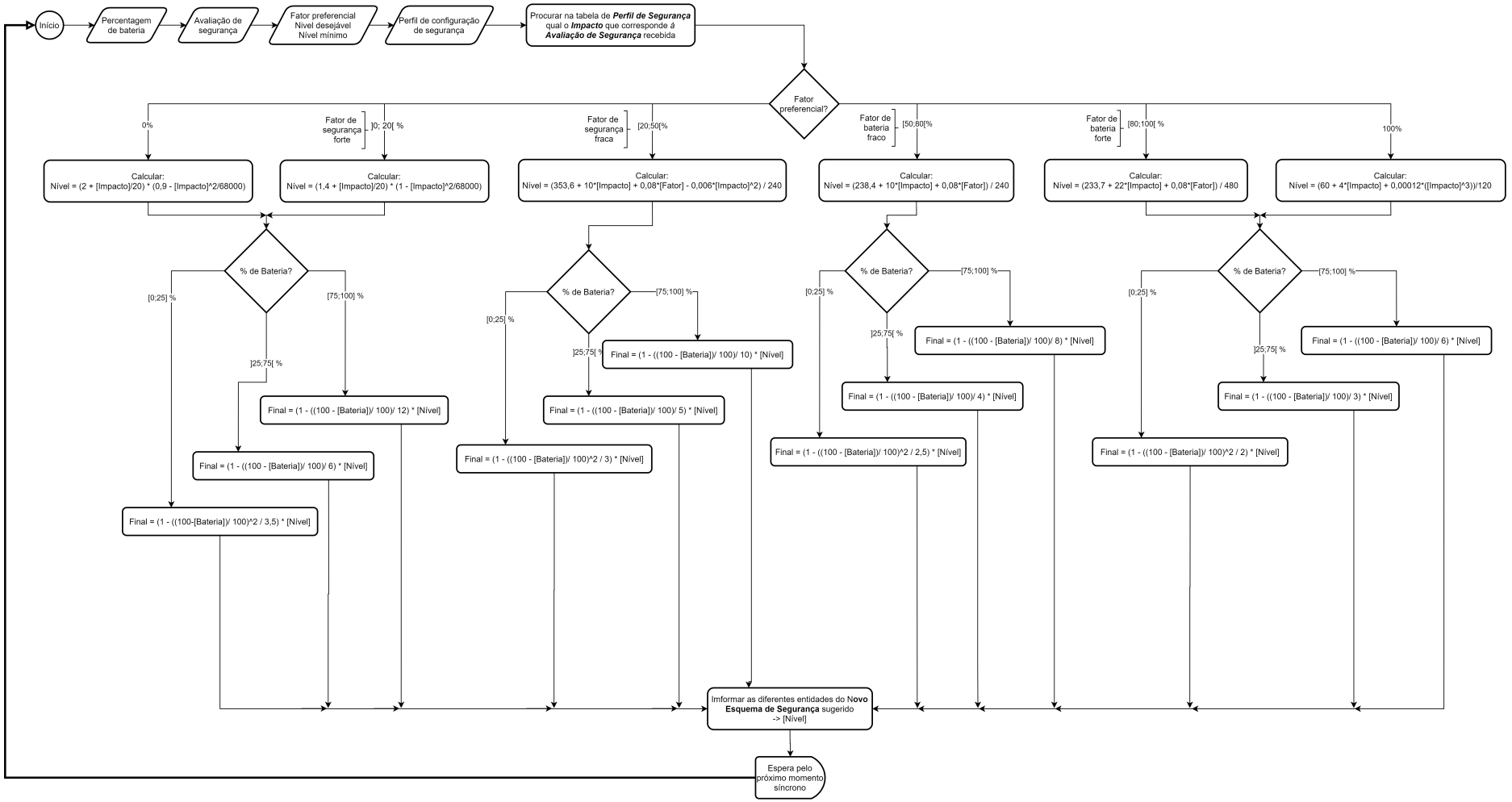

Figura 5.2: Fluxograma que representa o algoritmo

5.2.2 Pseudocódigo

Com o objetivo de testar a prestação do algoritmo construído foi planeada a sua implementação usando pseudocódigo. Para isso, foram criadas duas abordagens: a primeira, Lógica, é uma transposição direta do algoritmo criado; a segunda, Lógica Delta, é uma alternativa, que tem por base a primeira, onde foi acrescentado um mecanismo para filtrar avaliações de segurança que esporadicamente possam ser mal recolhidas.

Lógica

A primeira opção de pseudocódigo retrata diretamente o que foi apresentado na figura 5.2.

```
Declarar variáveis principais
Declara variáveis auxiliares
Ler configuração inicial de var.txt
Alocar memória necessária
Iniciar ficheiros de escrita de resultados
Escrever configuração inicial nos ficheiros de resultados
Aplicar gasto energético do nível inicial
Ciclo até percentagem de bateria diminuir 5%
    Calcular nova percentagem de bateria
    Obter avaliação de segurança
    Calcular nível de segurança a sugerir
    Aplicar atenuação dependendo do nível de bateria
    Retirar custo energético da nova segurança
    Guardar os dados no respetivo ficheiro
    Aumentar contador do número de ciclo
Fim de ciclo
Apresentar número de ciclos
Libertar espaço e fechar escrita de ficheiros
```

Tabela 5.2: Pseudocódigo da primeira abordagem de teste do algoritmo desenvolvido

Lógica Delta

A segunda alternativa, que tem por base a primeira, representa uma melhoria onde é acrescentado um armazenamento de um número de avaliações de segurança, definido pelo utilizador. Sempre que é recebida uma nova avaliação de segurança pelo IDS, esta é guardada nesse *buffer*, sendo depois selecionada a avaliação mais elevada para realizar os cálculos necessários.

Esta melhoria foi criada com vista à absorção de pequenas anomalias na avaliação de segurança feita pelo IDS para que não afete o esquema sugerido. Concretizando com um exemplo: num cenário onde estão constantemente a ser detetados ataques com um impacto elevado, se por alguma razão for enviado ao controlador uma avaliação cujo impacto seja baixo ou nulo, este *buffer* vai impedir que haja uma mudança desnecessária no nível de segurança, não gastando energia adicional.

```
Declarar variáveis principais
Declara variáveis auxiliares
Ler configuração inicial de var.txt
Alocar memória necessária
Iniciar ficheiros de escrita de resultados
Escrever configuração inicial nos ficheiros de resultados
Aplicar gasto energético do nível inicial
Ciclo até percentagem de bateria diminuir 5%
    Calcular nova percentagem de bateria
    Obter avaliação de segurança
    Guardar no buffer e escolher o valor mais alto
    Calcular nível de segurança a sugerir
    Aplicar atenuação dependendo do nível de bateria
    Retirar custo energético da nova segurança
    Guardar os dados no respetivo ficheiro
    Aumentar contador do número de ciclo
Fim de ciclo
Apresentar número de ciclos
Libertar espaço e fechar escrita de ficheiros
```

Tabela 5.3: Pseudocódigo da segunda abordagem de teste do algoritmo desenvolvido

5.3 Conclusão

Dado a conhecer algoritmo, ilustrando-o num fluxograma, e todo o processo do seu desenvolvimento, torna-se mais simples fazer uma análise à arquitetura proposta e perceber porque determinados componentes são adicionados, como é o caso do IDS. A preparação da avaliação, apresentando as duas versões de pseudocódigo usadas nos testes realizados prepara a fase seguinte do documento que irá incidir sobre a apresentação e discussão dos resultados obtidos nestes testes e sobre a ilustração do comportamento do controlador, sendo possível observar e comparar visualmente o resultado obtido consoante as condições do momento de decisão.

Esta página foi deliberadamente deixada em branco.

Capítulo 6

Avaliação

Neste capítulo são apresentadas as duas avaliações feitas ao algoritmo desenvolvido, referindo o *setup* necessário, os resultados e a discussão dos mesmos. Por fim, é ilustrado o comportamento do controlador com o auxílio de gráficos para que sejam percetíves as suas ações no decorrer da execução.

6.1 Avaliação analítica do comportamento do controlador

Com vista à obtenção de conclusões sobre as propostas de avaliação elaboradas, foram feitos testes analíticos sobre o custo da segurança na energia do sensor, não sendo para já considerados quaisquer custos relativos a transmissão de dados e aplicação. Esta secção pretende expor os diferentes cenários de teste, as inúmeras configurações iniciais e os resultados obtidos.

6.1.1 Setup Experimental

Para testar o comportamento do Controlador foram criados vários cenários com diferentes configurações iniciais. Cada teste corresponde a uma combinação destes dois pontos e, para além disto, foi definido para cada mensagem um tamanho de 127 Bytes, tamanho de referência usado no padrão 802.15.4, e o envio de duas mensagens por cada execução.

O fator preferencial, o nível mínimo e o nível inicial são as variáveis alteradas nas configurações iniciais de cada teste e a tabela 6.1 ilustra os respetivos valores.

	Fator Preferencial	Nível Mínimo	Nível Inicial
1	80%	2	4
2	20%		
3	80%	1	4
4	20%		
5	80%	2	3
6	20%		

Tabela 6.1: Configurações iniciais escolhidas

Os diferentes cenários usados correspondem: a um cenário aleatório que está mais próximo da realidade, 2 cenários com 20% de ocorrência de ataques cuja percentagem de impacto

é considerada elevada, 80% e 90%, um cenário com 20% de ataques com impacto médio, 40%, e um cenário com 20% de ataques com impacto considerado baixo, 20%.

No que diz respeito à avaliação, foram desenvolvidos 2 códigos na linguagem de programação C para as duas abordagens apresentadas na secção 5.2.2, com o objetivo de estudar o impacto da segurança na energia. Para esse estudo, os valores do custo energético de cada esquema de segurança utilizado foram retirados de [40] e estão representados tabela 6.2. Quanto à capacidade da bateria do sensor, foi usada uma pilha alcalina LR6 (conhecida em linguagem corrente como Pilha AA) com uma capacidade de 1,8Ah e tensão de 1,5V, equivalendo a uma quantidade de energia gerada igual a 2,7Wh. Uma vez que 1Wh corresponde a 3600J de energia [41], podemos afirmar que esta bateria tem 9720 Joules.

Nível	Esquema de Segurança		Custo energético (microJ/B)
	Confidencialidade	Integridade	
1	-	-	0
2	-	SHA256	0,043
3	AES128	-	0,245
4	AES128	SHA256	0,288
5	AES258	SHA512	0,375

Tabela 6.2: Custo energético de cada nível de segurança

Cada código na linguagem C testou cada cenário, nos quais foram usadas as 6 combinações de configurações iniciais apresentadas na tabela 6.1, num total 60 testes. Dado o elevado tempo necessário para a realização de cada um, foram feitas medições apenas em 3 intervalos de bateria, de 100% a 95%, de 75% a 70% e de 25% a 20%. Esta decisão foi tomada tendo em consideração o comportamento diferente do algoritmo nas 3 fases do nível de bateria. Os valores finais correspondem a uma extrapolação dos valores obtidos nestes 3 intervalo.

6.1.2 Resultados

A tabela 6.3 apresenta os valores obtidos em cada um dos testes, representando o número de ciclos que foi possível executar para uma determinada abordagem de testes, cenário e configuração inicial. Como anteriormente referido, estes números são uma extrapolação feita através dos valores obtidos, usando a função 5 x [Valor de primeiro intervalo] + 10 x [Valor de segundo intervalo] + 5 x [Valor de terceiro intervalo]. Cada peso dos diferentes intervalos equivale à quantidade de vezes que cada intervalo incorpora 5% de bateria, ou seja, entre 100% e 75% ou entre 25% e 0% há 5 intervalos de 5% e entre 75% e 25% há 10 intervalos de 5%.

		Configuração Inicial					
Cenário	Código	1	2	3	4	5	6
Aleatório	Lógica	306698115	208301610	306698150	208301610	379677515	224068215
	Lógica Delta	148947695	117738690	148947770	117738710	149992340	117797305
Alto 90%	Lógica	398231705	362629505	398231705	362629475	623803770	539511990
	Lógica Delta	157904815	137406450	157904925	137406470	165193705	142853115
Alto 80%	Lógica	468039540	390846515	468039545	390846515	1124969280	604671550
	Lógica Delta	254661730	153298930	254661750	153298950	297894645	160122900
Médio 40%	Lógica	889946800	553140925	889946820	553140930	3337300455	1660158380
	Lógica Delta	889946660	360221480	889946780	360221720	883662985	439623500
Baixo 20%	Lógica	17798937782	17798937782	17798937858	17798937858		88994688908
	Lógica Delta	17798937782	17798937782	17798937858	17798937858		

Tabela 6.3: Resultados obtidos nos testes, representando o número de ciclos corridos em cada teste

Nota: As células em branco da tabela corresponde a valores que são impossíveis de obter uma vez que as configurações permitem a utilização do nível 1 de segurança que corresponde a não usar nenhum esquema de segurança, conforme é definido na tabela 4.1.

6.1.3 Análise dos Resultados

Os *standars* que definem uma arquitetura IoT para LoRaWAN apenas preveem a utilização de um único esquema de segurança durante todo o seu funcionamento. Assim, a primeira comparação a fazer é com um cenário onde o esquema de segurança usado seja fixo, o que irá ajudar a perceber se os objetivos deste trabalho, poupar bateria e estender o tempo de utilização de um sensor numa rede IoT, foram atingidos.

Para o cenário de esquema de segurança fixo definiu-se a utilização do nível de segurança 4 definido na tabela 4.1. Recorrendo à tabela 6.2, é possível visualizar o custo energético por Byte inerente à utilização do nível 4 de segurança. Usando as mesmas configurações dos testes anteriormente apresentados ou seja, um tamanho de mensagem igual a 127 Bytes e o envio de duas mensagens por ciclo executado, podemos chegar ao custo energético por ciclo de execução de 0,073152 mJ e assim calcular o número de ciclos que é possível executar segundo este cenário de nível de segurança fixo, que são 132874016.

Na tabela 6.4 é apresentada a comparação de forma percentual entre os valores obtidos nos testes e o valor calculado anteriormente. Valores percentuais positivos correspondem a um ganho em relação ao número de ciclos executados em esquema de segurança fixo, enquanto que valores negativos correspondem a uma perda. Ao analisar esta tabela concluímos que 55 dos 58 testes têm valores superiores ao pretendido, provando que o Controlador dinâmico de segurança tem um impacto positivo na poupança de bateria de um sensor. Os 3 resultados que ficaram aquém do esperado correspondem a testes cuja preferência foi pela segurança dos dados em detrimento da poupança de bateria.

		configurações Iniciais					
Cenário	Código	1	2	3	4	5	6
Aleatório	Lógica	306698115 131%	208301610 57%	306698150 131%	208301610 57%	379677515 186%	224068215 69%
	Lógica Delta	148947695 12%	117738690 -11%	148947770 12%	117738710 -11%	149992340 13%	117797305 -11%
Alto 90%	Lógica	398231705 200%	362629505 173%	398231705 200%	362629475 173%	623803770 369%	539511990 306%
	Lógica Delta	157904815 19%	137406450 3%	157904925 19%	137406470 3%	165193705 24%	142853115 8%
Alto 80%	Lógica	468039540 252%	390846515 194%	468039545 252%	390846515 194%	1124969280 747%	604671550 355%
	Lógica Delta	254661730 92%	153298930 15%	254661750 92%	153298950 15%	297894645 124%	160122900 21%
Médio 40%	Lógica	889946800 570%	553140925 316%	889946820 570%	553140930 316%	3337300455 2412%	1660158380 1149%
	Lógica Delta	889946660 570%	360221480 171%	889946780 570%	360221720 171%	883662985 565%	439623500 231%
Baixo 20%	Lógica	17798937782 13295%	17798937782 13295%	17798937858 13295%	17798937858 13295%		88994688908 66877%
	Lógica Delta	17798937782 13295%	17798937782 13295%	17798937858 13295%	17798937858 13295%		0 -100%

Tabela 6.4: Comparação dos resultados dos testes com o valor calculado para o cenário com segurança fixa

A comparação de resultados entre fatores preferenciais diferentes é feita na tabela 6.5. Os testes cujo fator preferencial é igual a 20%, correspondendo a uma importância forte da segurança, obtêm resultados inferiores aos testes com fator preferencial igual a 80%, ilustrando a poupança que estes últimos conseguem em relação aos primeiros.

		configurações Iniciais								
Cenário	Código	1	2		3	4		5	6	
Aleatório	Lógica	306698115	208301610	-32,08%	306698150	208301610	-32,08%	379677515	224068215	-40,98%
	Lógica Delta	148947695	117738690	-20,95%	148947770	117738710	-20,95%	149992340	117797305	-21,46%
Alto 90%	Lógica	398231705	362629505	-8,94%	398231705	362629475	-8,94%	623803770	539511990	-13,51%
	Lógica Delta	157904815	137406450	-12,98%	157904925	137406470	-12,98%	165193705	142853115	-13,52%
Alto 80%	Lógica	468039540	390846515	-16,49%	468039545	390846515	-16,49%	1124969280	604671550	-46,25%
	Lógica Delta	254661730	153298930	-39,80%	254661750	153298950	-39,80%	297894645	160122900	-46,25%
Médio 40%	Lógica	889946800	553140925	-37,85%	889946820	553140930	-37,85%	3337300455	1660158380	-50,25%
	Lógica Delta	889946660	360221480	-59,52%	889946780	360221720	-59,52%	883662985	439623500	-50,25%
Baixo 20%	Lógica	17798937782	17798937782	0,00%	17798937858	17798937858	0,00%		88994688908	
	Lógica Delta	17798937782	17798937782	0,00%	17798937858	17798937858	0,00%		0	

Tabela 6.5: Comparação dos resultados para valores de fator preferencial diferentes no mesmo cenário

Na figura 6.6 são comparados os valores do mesmo cenário e valor de fator preferencial, mas com as restantes configurações iniciais diferentes. O intuito desta análise prende-se ao estudo do impacto energético de níveis mínimos e iniciais diferentes. Como se pode constatar, os testes 5 e 6 onde o valor do nível mínimo de segurança é 1 (o mais pequeno) registam uma subida nos resultados obtidos em relação ao testes base (1 e 2) em que o nível mínimo de segurança é 2. Já para os testes 3 e 4, em que o nível de segurança inicial está um patamar abaixo em relação ao dos testes de referência, não se registaram aumentos significativos uma vez que as diferenças não ascendem a 100 unidades.

		Configurações Iniciais									
Cenário	Código	1	2	3		4		5		6	
Aleatório	Lógica	306698115	208301610	306698150	0,00%	208301610	0,00%	379677515	24%	224068215	7,57%
	Lógica Delta	148947695	117738690	148947770	0,00%	117738710	0,00%	149992340	1%	117797305	0,05%
Alto 90%	Lógica	398231705	362629505	398231705	0,00%	362629475	0,00%	623803770	57%	539511990	48,78%
	Lógica Delta	157904815	137406450	157904925	0,00%	137406470	0,00%	165193705	5%	142853115	3,96%
Alto 80%	Lógica	468039540	390846515	468039545	0,00%	390846515	0,00%	1124969280	140%	604671550	54,71%
	Lógica Delta	254661730	153298930	254661750	0,00%	153298950	0,00%	297894645	17%	160122900	4,45%
Médio 40%	Lógica	889946800	553140925	889946820	0,00%	553140930	0,00%	3337300455	275%	1660158380	200,13%
	Lógica Delta	889946660	360221480	889946780	0,00%	360221720	0,00%	883662985	-1%	439623500	22,04%
Baixo 20%	Lógica	17798937782	17798937782	17798937858	0,00%	17798937858	0,00%			88994688908	400,00%
	Lógica Delta	17798937782	17798937782	17798937858	0,00%	17798937858	0,00%			0	

Tabela 6.6: Comparação dos resultados entre configurações iniciais diferentes no mesmo cenário

Por último, a figura 6.7 ilustra a comparação entre as duas abordagens testadas para o mesmo cenário e conjunto de configurações iniciais.

Como seria de esperar, o código Lógica Delta apresenta resultados menores nos testes realizados em cenário Aleatório, em ambos os cenários com 20% de ataques altos e em alguns testes realizados com cenário com 20% de ataques médios. Isto deve-se ao facto de esta abordagem tomar uma decisão com base nas últimas 5 avaliações de segurança e utilizar o valor mais alto de percentagem de impacto registado, contrastando com a decisão imediata que acontece na abordagem com o nome Lógica. Assim, é mantido um esquema de segurança mais elevado durante mais tempo, levando a que haja um impacto energético mais acentuado tendo isso repercussão no número de ciclos que são executados, diminuindo esse valor. Os restantes testes têm os mesmos resultados visto que o esquema de segurança surgido pelo algoritmo é menor do que o nível mínimo de segurança permitidos nas configurações iniciais, levando a que todos esses testes acabem por usar ao longo do tempo sempre o mesmo nível de segurança, o nível mínimo.

		configurações Iniciais					
Cenário	Código	1	2	3	4	5	6
Aleatório	Lógica	306698115	208301610	306698150	208301610	379677515	224068215
	Lógica Delta	148947695 -51%	117738690 -43%	148947770 -51%	117738710 -43%	149992340 -60%	117797305 -47%
Alto 90%	Lógica	398231705	362629505	398231705	362629475	623803770	539511990
	Lógica Delta	157904815 -60%	137406450 -62%	157904925 -60%	137406470 -62%	165193705 -74%	142853115 -74%
Alto 80%	Lógica	468039540	390846515	468039545	390846515	1124969280	604671550
	Lógica Delta	254661730 -46%	153298930 -61%	254661750 -46%	153298950 -61%	297894645 -74%	160122900 -74%
Médio 40%	Lógica	889946800	553140925	889946820	553140930	3337300455	1660158380
	Lógica Delta	889946660 0%	360221480 -35%	889946780 0%	360221720 -35%	883662985 -74%	439623500 -74%
Baixo 20%	Lógica	17798937782	17798937782	17798937858	17798937858		88994688908
	Lógica Delta	17798937782 0%	17798937782 0%	17798937858 0%	17798937858 0%		0

Tabela 6.7: Comparação entre diferentes códigos para o mesmo cenário e configurações inicias

6.2 Comportamento do Controlador

Esta secção expõe o comportamento do Controlador nos testes realizados à primeira abordagem do algoritmo, Lógica, onde é possível perceber qual o resultado do algoritmo num determinado momento, para cada tipo de cenário, Ataque Alto, Ataque Baixos e Aleatório, e a influência que a alteração de uma variável pode ter no esquema de segurança sugerido pelo controlador.

O resultado final difere consoante a alteração de uma determinada variável com o objetivo de poupar bateria e prolongar o tempo de vida do sensor. O impacto do nível de bateria ou a diferença do fator preferencial servem para fazer uma gestão ativa da energia que lhe resta.

6.2.1 Cenário com 20% de Ataque com Impacto de 80%

O gráfico da figura 6.1 demonstra o comportamento do Controlador dinâmico de segurança num cenário com 20% de ataques cujo impacto é de 80%, com um nível de bateria de 100%, um fator preferencial igual a 80% (que perfere a poupança de energia em detrimento da segurança), nível mínimo de segurança permitida 2 e nível inicial de segurança 4. Como se pode ver, sempre que há a deteção da presença de um ataque, o esquema de segurança sugerido pelo controlador sobe para o nível 4 e desce para o nível 2, o mínimo permitido, na sua ausência. Esta figura servirá de base de comparação com os gráficos seguintes a fim de mostrar a diferenciação que é feita no valor final sugerido pelo controlador para diferentes configurações e valores recebidos dentro do mesmo cenário.

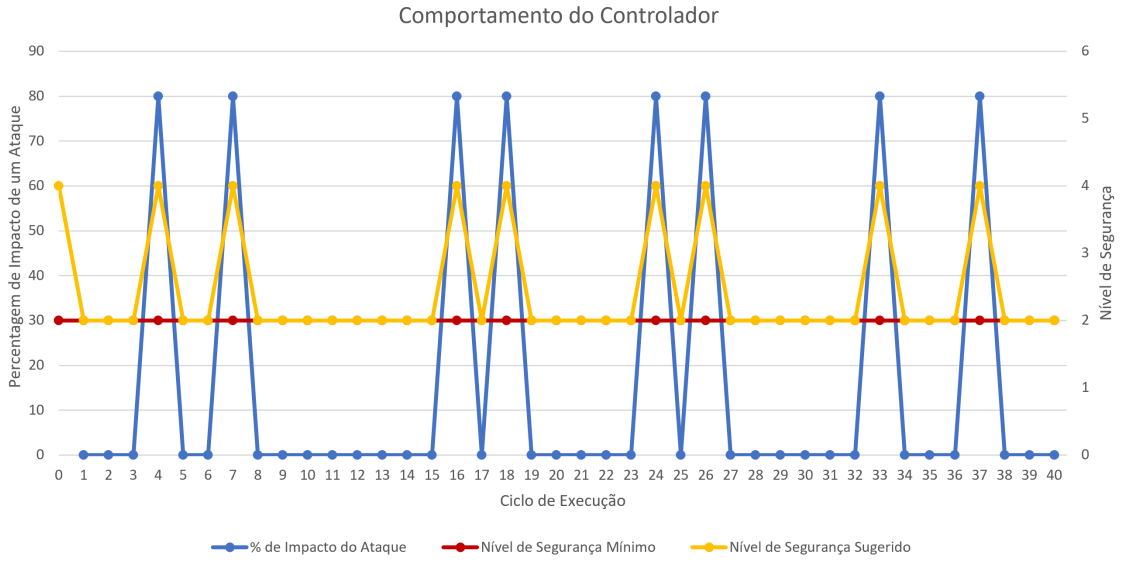

Figura 6.1: Gráfico que representa o comportamento do controlador com 100% de bateria e Fator Preferencial de 80%

Percentagens de bateria diferentes

Numa comparação entre o comportamento do Controlador dinâmico de segurança com diferentes percentagens de bateria, é possível ver que os valores apresentados são diferentes. Na figura 6.1, o nível de segurança reportado pelo Controlador na presença de um ataque é 4, no entanto o nível desce para 3 caso o estado da bateria se situe nos 25%, como é

mostrado na figura 6.2. Já na ausência de ataque, em ambos os casos o nível de segurança desce até ao mínimo permitido, que, neste caso, é o nível de segurança 2.

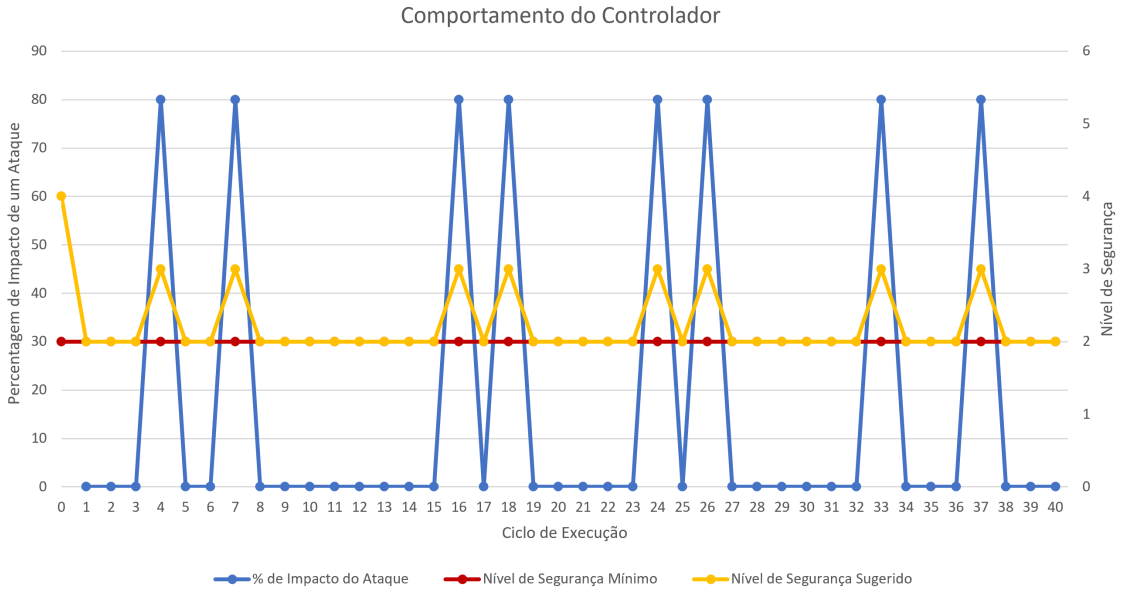

Figura 6.2: Gráfico que representa o comportamento do controlador com 25% de bateria e fator preferencial de 80%

Fatores preferenciais diferentes

Comparando as diferenças de resultado para diferentes fatores preferenciais, podemos constatar que o nível de segurança sugerido é maior caso este se aproxime de 0. As figuras 6.1 e 6.3 representam dois testes feitos para as mesmas configurações, variando apenas o fator preferencial de 80 para 20, respetivamente. Ou seja, o utilizador primeiro dá importância à poupança de bateria e depois à segurança, o que explica o aumento do valor sugerido de 4 para 5 no nível de segurança.

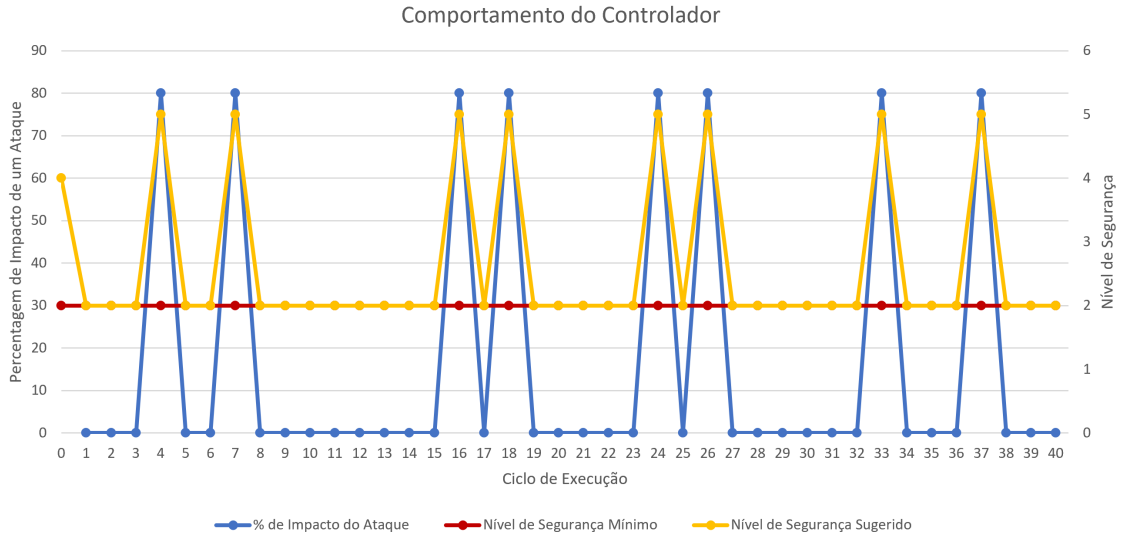

Figura 6.3: Gráfico que representa o comportamento do controlador com 100% de bateria e fator preferencial de 20%

Níveis mínimos diferentes

Nas figuras 6.1 e 6.4 é possível observar a diferença do comportamento do Controlador para níveis mínimos de segurança diferentes. Sempre que não é detetada a presença de um ataque, o nível mínimo a que se pode descer no segundo teste é menor que o do primeiro caso referido, permitindo assim uma maior poupança de bateria ao longo do tempo uma vez que o gasto energético passa a ser menor. Em ambos os casos o nível sugerido sempre que surge um ataque é igual, o nível 4 de segurança.

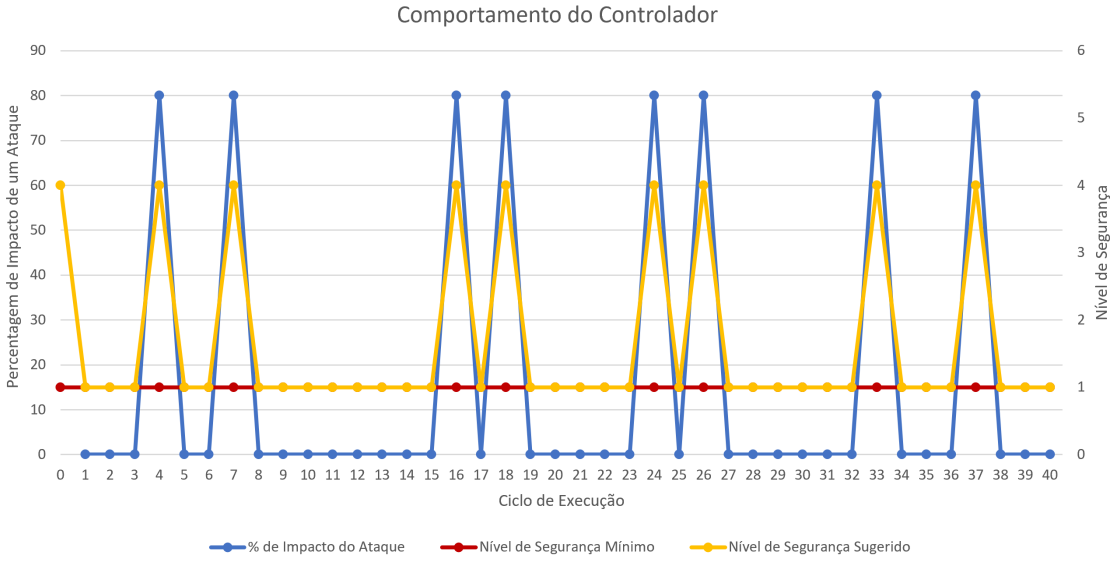

Figura 6.4: Gráfico que representa o comportamento do controlador com 100% de bateria, fator preferencial de 80% e nível mínimo de segurança 1

6.2.2 Cenário com 20% de Ataques Baixos

Na figura 6.5 é ilustrado o comportamento do Controlador em cenário de 20% de ataques com impacto reduzido para um estado de bateria de 100%, poupança de bateria como fator preferencial, nível mínimo de segurança 2 e inicial igual a 4. Dadas as condições, o esquema de segurança sugerido pelo Controlador aquando de um ataque é o nível 2, como este também é o nível mínimo de segurança permitido, é usado sempre o mesmo esquema de segurança ao longo do tempo. Este gráfico servirá de referência para a comparação dos diferentes resultados, conforme as configurações iniciais e as avaliações de segurança recebidas.

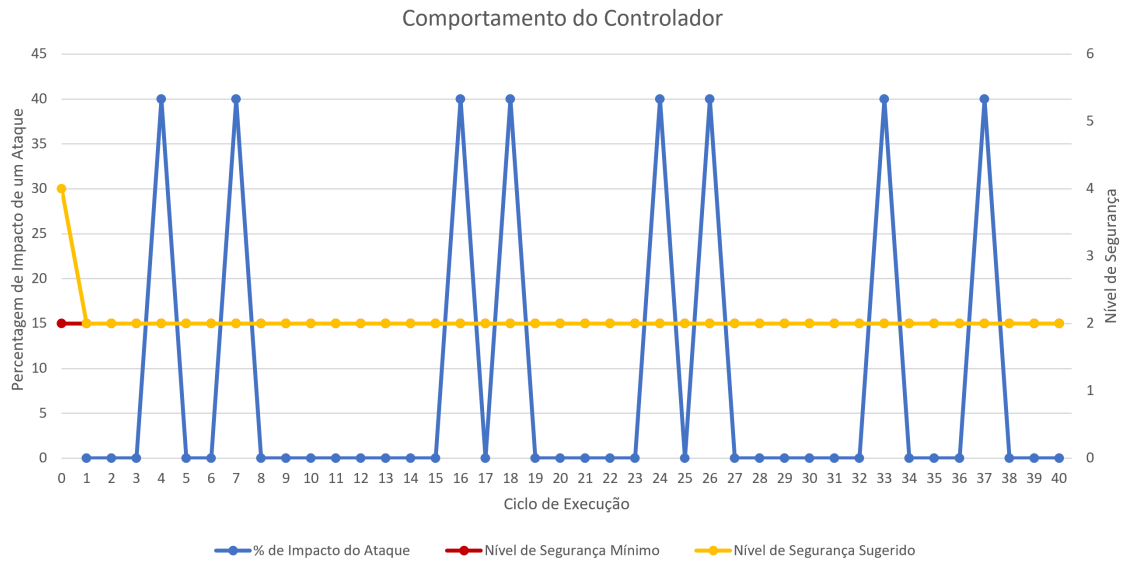

Figura 6.5: Gráfico que representa o comportamento do controlador com 100% de bateria, fator preferencial de 80% e nível mínimo de segurança 2

Percentagens de bateria diferentes

Na figura 6.6 é apresentado o teste para o cenário em questão, fator preferencial de 80%, nível de bateria de 25% e nível mínimo de segurança de 2. Ao longo do tempo de execução não visíveis quaisquer alteração ao nível de segurança, pois o valor calculado pelo Controlador é inferior ao valor mínimo permitido.

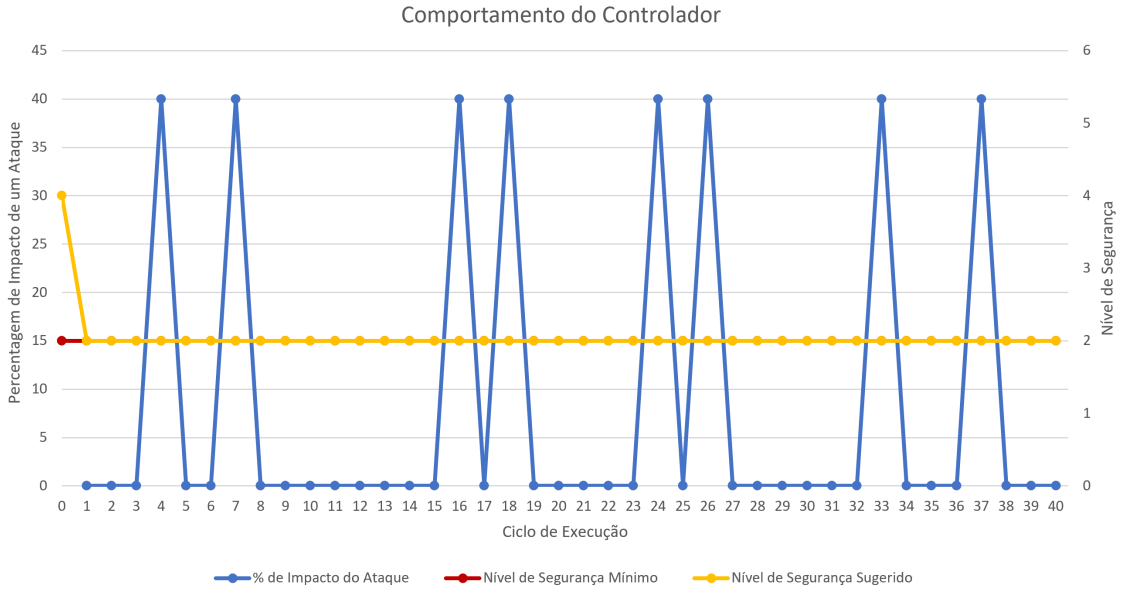

Figura 6.6: Gráfico que representa o comportamento do controlador com 25% de bateria e fator preferencial de 80%

Fatores preferenciais diferentes

No gráfico 6.7 é apresentado o resultado do teste num cenário com 20% de ataques com importância baixa com fator preferencial de 20%, bateria a 100% e nível mínimo de segurança 2. Aqui, na presença de ataque, o nível sugerido sobe para 3, voltando para o mínimo permitido de 2 na sua ausência. Comparando com a figura 6.5, é possível constatar a diferença do nível sugerido aquando da ocorrência de um ataque para valores de fator preferencial diferentes, sendo esse resultado superior.

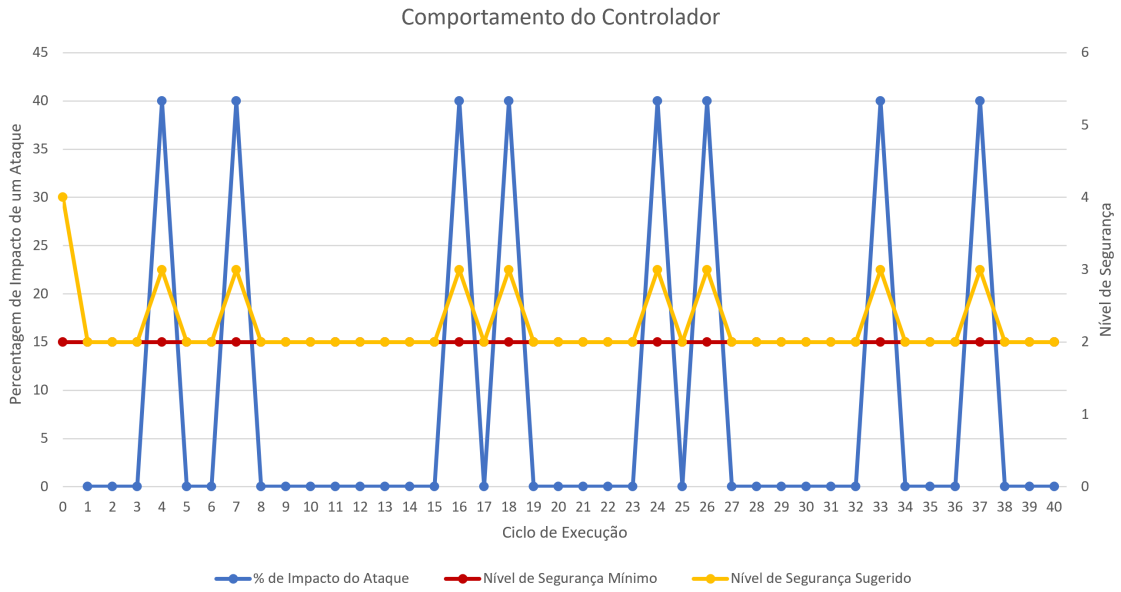

Figura 6.7: Gráfico que representa o comportamento do controlador com 100% de bateria e fator preferencial de 20%

Níveis mínimos diferentes

A figura 6.8 ilustra um teste idêntico ao apresentado na figura 6.5, mas para níveis mínimos de segurança diferentes. Nesta figura, o nível mínimo é de 1, sendo possível ver a diferença entre o resultado do controlador com e sem a presença de um ataque, algo que não é possível observar na figura 6.5, uma vez que nesse caso o nível mínimo é igual ao sugerido durante um ataque.

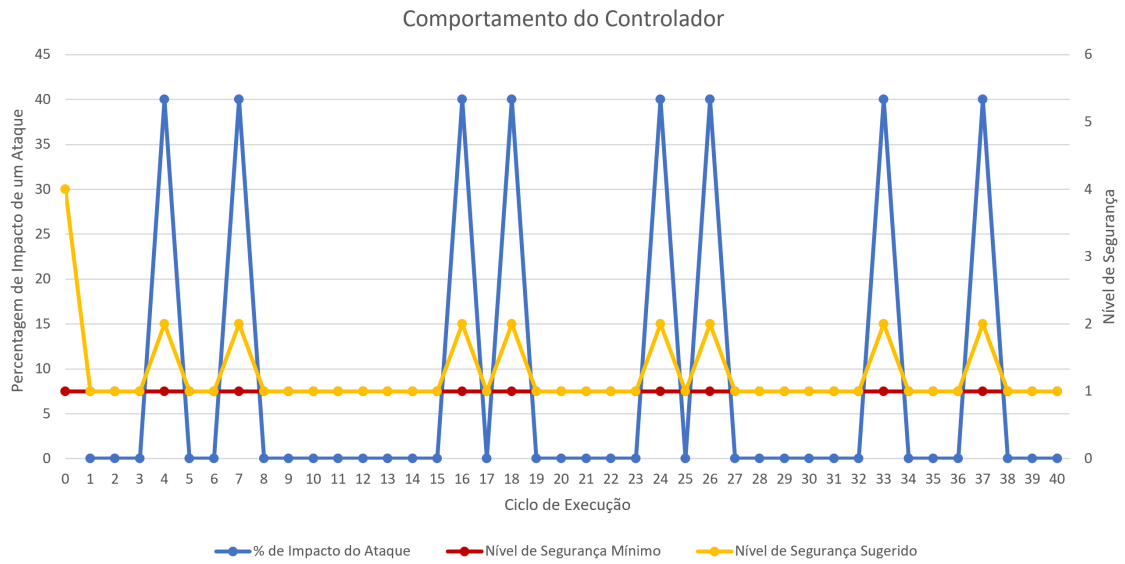

Figura 6.8: Gráfico que representa o comportamento do controlador com 100% de bateria, fator preferencial de 80% e nível mínimo de segurança 1

6.2.3 Cenário Aleatório

A figura 6.9 representa o teste realizado em cenário aleatório, o mais idêntico à realidade uma vez que não há forma de prever se existirá ou não um ataque e qual o seu tipo, quantidade e duração, para um fator preferencial de 80%, bateria a 100%, nível mínimo de segurança 2 e inicial igual a 4. Aqui pode-se perceber que o valor sugerido pelo Controlador acompanha as alterações do impacto dos ataques detetados. Apesar de haver ataques detetados cuja percentagem de impacto é baixa, o esquema de segurança nunca é inferior ao mínimo permitido.

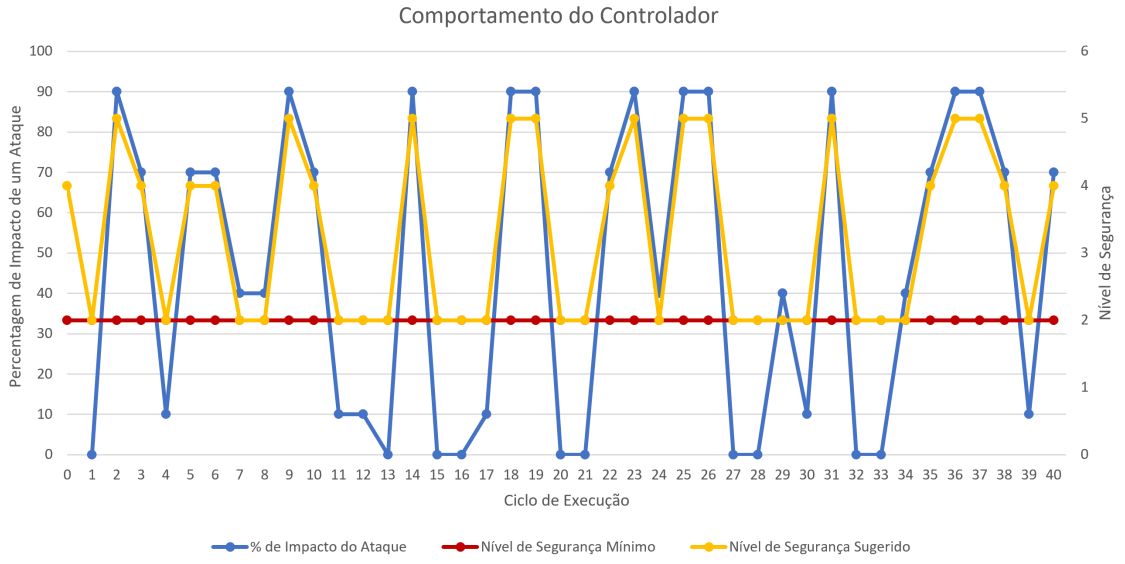

Figura 6.9: Gráfico que representa o comportamento do controlador com 100% de bateria, fator preferencial de 80% e nível mínimo de segurança 2

Percentagens de bateria diferentes

Os gráficos ilustrados nas figuras 6.10 e 6.11 representam testes feitos nas mesmas condições, mudando apenas a percentagem de bateria, de 75% e 25% respetivamente. Nesta comparação, e incluindo também a figura 6.9, é possível perceber a diferença de resultados para os vários estados de bateria, sendo que quanto mais perto a bateria se encontra do fim de vida, menor será o valor reportado pelo Controlador face ao mesmo valor de impacto de um ataque.

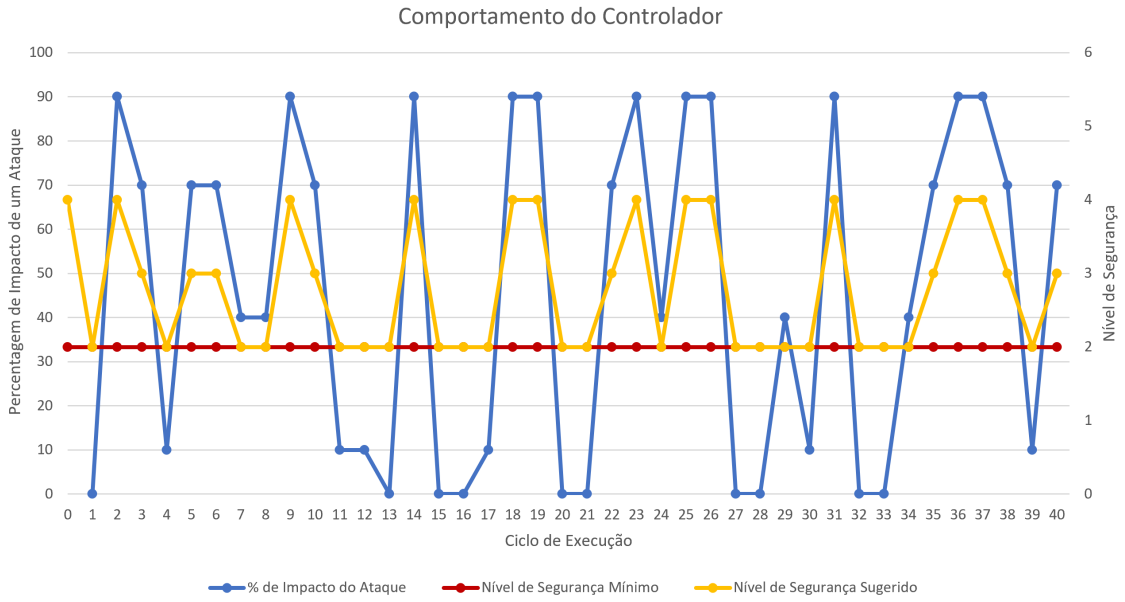

Figura 6.10: Gráfico que representa o comportamento do controlador com 75% de bateria, fator preferencial de 80% e nível mínimo de segurança 2

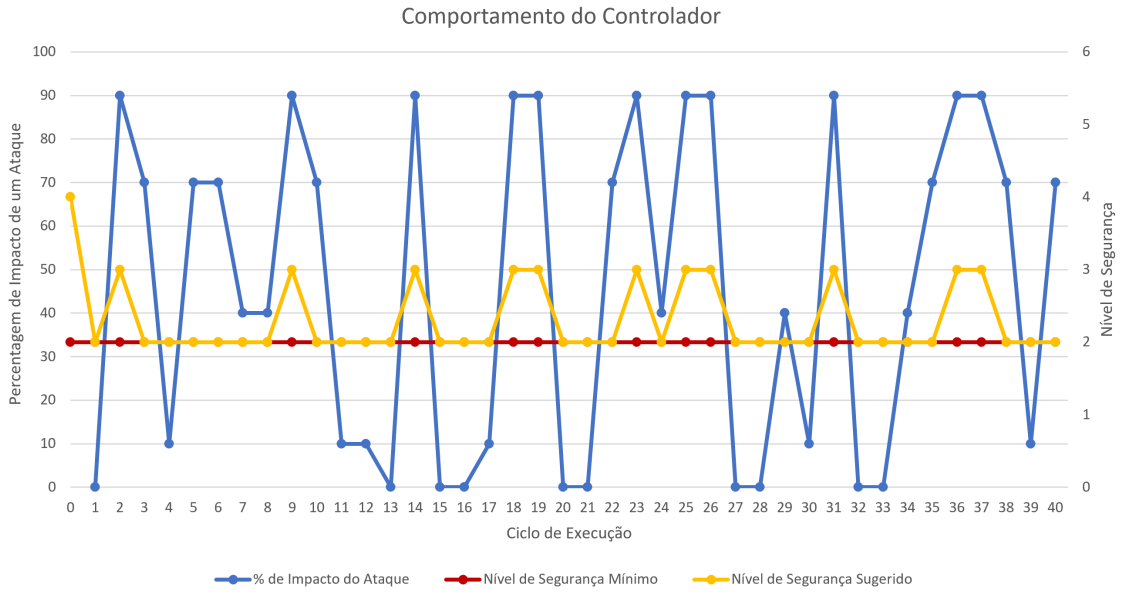

Figura 6.11: Gráfico que representa o comportamento do controlador com 25% de bateria, fator preferencial de 80% e nível mínimo de segurança 2

Fatores preferenciais diferentes

Comparando os gráficos das figuras 6.12 e 6.9, é possível perceber algumas alterações ao resultado com percentagens de impacto de segurança médias.

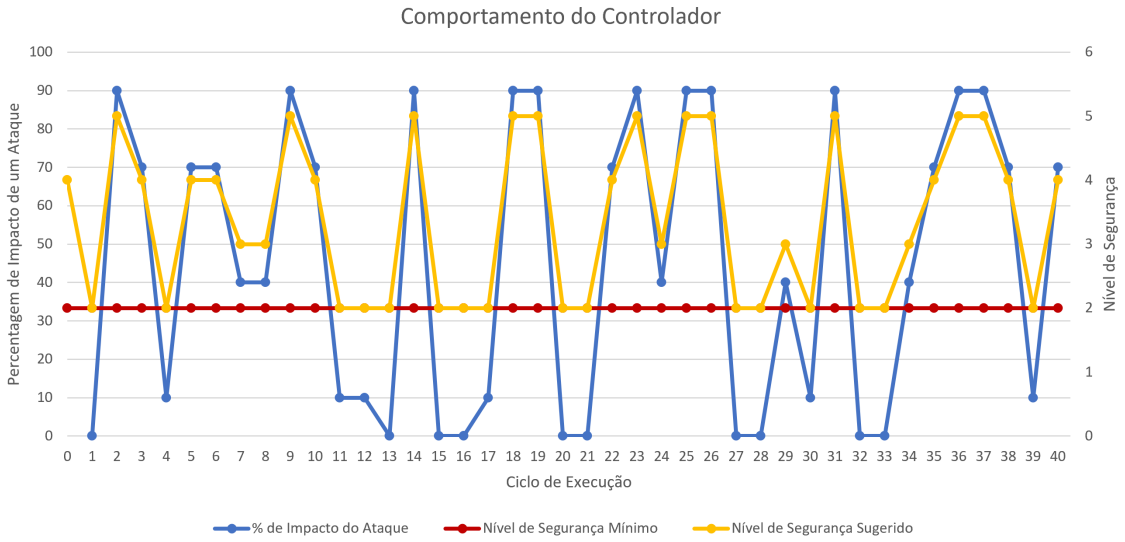

Figura 6.12: Gráfico que representa o comportamento do controlador com 100% de bateria, fator preferencial de 20% e nível mínimo de segurança 2

Níveis mínimos diferentes

Na Comparação entre testes com níveis mínimos de segurança diferentes é possível ver maior diversidade de respostas por parte do controlador visto que existem mais hipóteses de sugestão, como ilustra a figura 6.13. O impacto que esta mudança tem na longevidade da bateria não é diretamente percetível através dos gráficos mencionados, mas a diminuição deste nível irá aumentar o tempo de funcionamento do sensor.

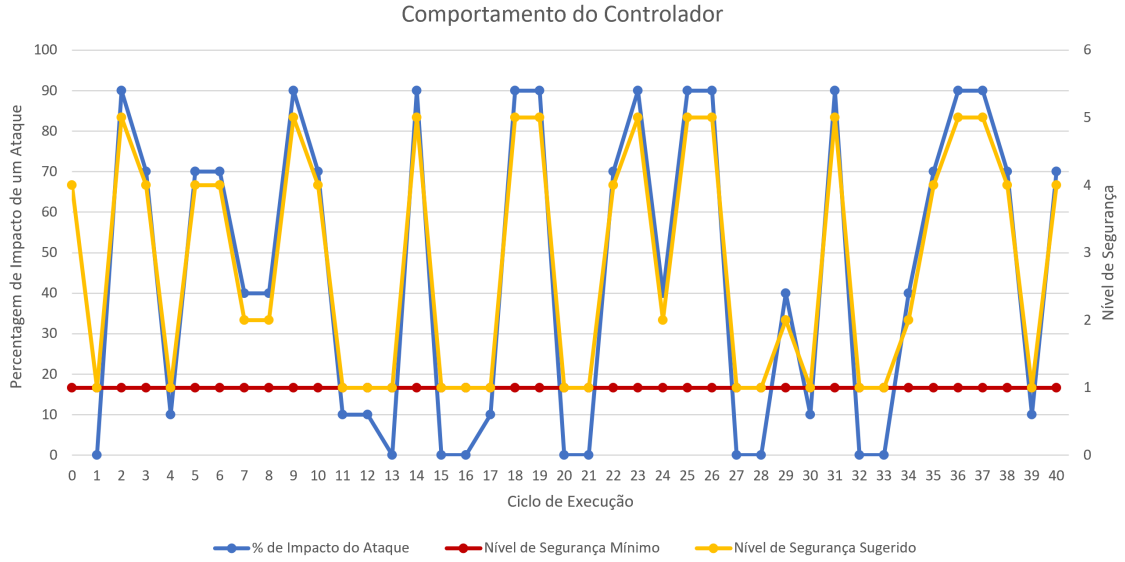

Figura 6.13: Gráfico que representa o comportamento do controlador com 100% de bateria, fator preferencial de 80% e nível mínimo de segurança 1

6.3 Avaliação analítica no contexto do LoRaWAN

Esta segunda avaliação tem em vista a apresentação de resultados no contexto de uma aplicação prática descrita em [42], uma vez que conjuga o custo energético da utilização dos diferentes níveis de segurança assim como o custo de transmissão das mensagens. O custo energético inerente à aplicação usada por um sensor não foi considerado, uma vez que esse valor depende muito de aplicação para aplicação.

6.3.1 Configuração da aplicação e do controlador

Para a concretização desta análise foi necessário, em primeiro lugar, definir os cenários a serem testados, as suas configurações inicias e o código a usar. Assim, foram testados dois cenários diferentes: um onde não são registados ataques ao sistema; outro onde se registam ataques constantes às comunicações, cada um deles com um impacto alto, de 80% . Quanto às configurações inicias, o fator preferencial, que representa a importância dada à poupança de bateria, foi testado com os valores de 80%, que dá prevalência à poupança de bateria em detrimento da segurança, e 20%, onde acontece o contrário, e o nível mínimo de segurança para o nível 1 e 2. O tamanho de cada mensagem mantém-se igual ao dos testes anteriores, 127 Bytes e a taxa de envio é de uma mensagem a cada meio minuto. As características da bateria também se mantém, sendo usado o mesmo tipo e com a mesma capacidade de 9720 Joules.

O valor do custo de energia da transmissão foi retirado de [42] e ilustra o valor medido para um transmissor LoRa SX1272, comum em sensores usados em ambientes LoRaWAN e que é incluído em alguns dispositivos apresentados na secção 2.1.6. Os valores usados para o custo energético da segurança são os mesmo usados para os testes anteriores, apresentados na figura 6.2.

Também foi analisado o caso em que a segurança do sistema é fixa, tendo sido escolhido o esquema de segurança 4 da tabela 4.1, com o objetivo de comparar os restantes resultados com o cenário atualmente mais comum de uma rede LoRaWAN. Aqui não se aplicam as configurações de fator preferencial e nível mínimo de segurança, uma vez que estas são apenas variáveis utilizadas pelo controlador.

6.3.2 Resultados

Na tabela 6.8 são apresentados os resultados obtidos para cada um dos testes realizados.

Com base nos custos energéticos de transmissão e segurança dos dados, foi possível fazer a avaliação analítica extrapolada através de valores experimentais. Para isso, cada combinação de cenário e configuração inicial foi analisada para determinar os intervalos da percentagem de bateria onde cada nível de segurança seria sugerido, apresentado na quinta e sexta colunas da tabela 6.8. Com essa divisão, foi possível calcular os diferentes gastos de energia ao longo do tempo para a vida da bateria e assim chegar ao tempo de execução de cada teste.

O custo energético da transmissão retirado de [42] é de 0,59 mJ por bit. Assim, fazendo a conversão desse valor para Bytes e multiplicando pelo tamanho de mensagem usado, chegamos ao valor apresentado na oitava coluna da figura 6.8 de 14,986 mJ por cada ciclo de execução.

Cenários	Configuração inicial			Intervalo de bateria	Nível de segurança	Custo energético da segurança (mJ)	Custo energético da transmissão (mJ)	Número total de ciclos executados		Tempo total de execução (minutos)	Tempo total de execução convertido
	Fator preferencial	Nível mínimo de segurança	Nível inicial								
Segurança Fixa	Não aplicavel	Não aplicavel	4	100%-0%	3	0,0311	14,986	647261		323630	224d 17h 50m
Ataques constantes com 80% de impacto cada	80%	1		100%-59%	4	0,288		265281	647413	323707	224d 19h 6m
				59%-22%	3	0,245		239487			
				22%-2%	2	0,043		129674			
				2%-0%	1	0		12972			
		2		100%-59%	4	0,288		265281	647408	323704	224d 19h 4m
				59%-22%	3	0,245		239487			
				22%-0%	2	0,043		142641			
	20%	1		100%-74%	5	0,375		168103	646951	323476	224d 15h 15m
				74%-21%	4	0,288		342924			
				21%-0%	3	0,245		135925			
		2		100%-74%	5	0,375		168103	646951	323476	224d 15h 15m
				74%-21%	4	0,288		342924			
				21%-0%	3	0,245		135925			
Sem ataques	Indiferente	1		100%-0%	1	0		648605		324303	225d 3h 5m
		2		100%-0%	2	0,0055		648369		324185	225d 3h 5m

Tabela 6.8: Resultados dos testes para estudo do tempo de vida de um sensor tendo em conta o custo energético da segurança e transmissão demensagens

6.3.3 Análise de resultados

Na figura 6.9 é apresentada uma comparação, em valor percentual, entre os valores obtidos nos testes feitos aos diferentes cenários e um ambiente em que o esquema de segurança usado é fixo. Os valores percentuais positivos representam um ganho no tempo de vida do sensor e os valores negativos representam uma perda no tempo de execução.

Cenários	Configuração inicial		Número total de ciclos executados	Tempo total de execução (minutos)	Comparação
	Fator preferencial	Nível mínimo de segurança			
Segurança Fixa	Não aplicável	Não aplicável	647261	323630	-
Impacto de 80%	80%	1	647413	323706	0,02%
		2	647408	323704	0,02%
	20%	1	646951	323475	-0,05%
		2	646951	323475	-0,05%
Sem ataques	Indiferente	1	648561	324281	0,24%
		2	648558	324279	0,21%

Tabela 6.9: Comparação dos resultados do estudo do tempo de vida de um sensor tendo em conta o custo energético da segurança e transmissão de mensagens

Os valores percentuais baixos são explicados pela relação direta com a quantidade limitada de informação transmitida pelos pressupostos dos cálculos no estudo analítico.

Analisando a comparação apresentada, é possível perceber que apenas 2 testes em 6 revelaram valores percentuais negativos, sendo possível afirmar novamente que o controlador desempenha um papel importante na gestão dinâmica de energia e segurança de uma infraestrutura LoRaWAN.

Observando as configurações iniciais e o cenário desses 2 testes é perceptível a razão pela qual existem esses valores negativos, uma vez que se trata de um cenário com ataques constantes, cujo impacto é elevado na proteção dos dados, e pelo facto de o fator preferencial escolhido ser 20%, ou seja, neste caso é preferida a segurança dos dados à poupança de bateria. Isto resulta num aumento do nível de segurança do sistema e, consequentemente, num aumento da exigência energética para assegurar essa proteção. Assim, estes dois testes foram realizados num tempo menor de execução, porém têm um nível de segurança geral superior, quando comparados com um esquema de segurança fixa, tendo sido usados os níveis 3, 4 e 5 de segurança para responde a ataques detetados em contraste com o uso fixo do quarto nível de segurança apresentado na tabela 4.1.

Os diferentes valores obtidos dentro do mesmo cenário são o resultado da aplicação das diferentes condições e algoritmos, reforçando a existência de uma diferenciação no tratamento da segurança e da poupança de energia dependendo dos valores de *input* definidos. O maior ganho é sempre registado com um fator preferencial de 80% e um nível mínimo de segurança de 1, o que significa que o algoritmo vai escolher poupar bateria em detrimento da segurança e abster-se de proteger os dados nos casos que considerar oportunos. Por sua vez, o menor ganho ou prejuízo é registado quando o fator preferencial é igual a 20% e o nível mínimo de segurança é 2, o que irá representar uma abordagem do controlador virada para a segurança em vez da poupança de bateria e onde existirá um esquema de segurança mesmo quando não forem registados ataques ao sistema, o que obviamente acarreta maiores custos energéticos.

Existem alguns fatores que podem influenciar o ganho obtido pelo uso do controlador, como por exemplo as configurações de teste: tamanho de cada mensagem, frequência de envio e energia disponível. A diminuição doas duas primeiras variáveis enumeradas ou o aumento da terceira irá contribuir para o aumento da diferença de tempos de execução.

6.4 Conclusão

Neste capítulo foram apresentados todos os testes feitos ao algoritmo proposto, comparando-os entre si, mas mais importante ainda, comparando-os com o resultado esperado para um sistema que use o mecanismo de segurança especificado pelo protocolo LoRaWAN. Esta comparação permitiu perceber a vantagem que existem em usar um controlador dinâmico de segurança, pois são atingidos dois propósitos: o de poupar bateria, estendendo o tempo de execução do sensor, quando não são detetados ataques ou quando estes têm um impacto reduzido nas comunicações; e o de aumentar a segurança do sistema, caso o meio envolvente seja hostil e haja deteção de ataques com um impacto elevando para o sistema.

Esta página foi deliberadamente deixada em branco.

Capítulo 7

Considerações finais

Neste capítulo é feita uma reflexão de todo o trabalho realizado e são apresentadas propostas de trabalho futuro.

7.1 Conclusões

A IoT é uma tema atual e que desperta muita atenção, tanto no meio académico, como no industrial. A acessibilidade cada vez maior faz com que surja um vasto número de projetos e por isso é necessário garantir que os mecanismos de segurança dos dados se mantém atualizados. No entanto, com a necessidade de mecanismos robustos de segurança surgem os aumentos nos consumos da bateria, o que se revela um problema para dispositivos, como os sensores, que não possuem a capacidade de armazenar grandes quantidades de energia para a sua alimentação. Surge, assim, a necessidade de dotar estes equipamentos de uma capacidade de gestão de energia sem comprometer a segurança do sistema. É neste âmbito que surge o trabalho apresentado, estudando a gestão de energia e segurança em IoT.

Nesta área há um vasto leque de opções no que diz respeito a tecnologias e protocolos, por isso são apenas focados os protocolos do tipo LPWA, capazes de estabelecer comunicações entre longas distancias e que os diferenciam de outros protocolos de âmbito mais local ou pessoal. Assim, os protocolos analisados foram: NB-IoT, LTE-M, Sigfox e LoRaWAN. Todos eles foram analisados, apresentando as suas especificações, e comparados entre si com o objetivo de encontrar um protocolo para o qual fosse possível propor melhorias. O LoRaWAN foi o selecionado dada a sua vasta utilização e pelo facto de ser o único com a abertura necessária, uma vez os restantes são protocolos industriais.

Conjugando a tecnologia escolhida com o âmbito do trabalho, foi proposto o desenvolvimento de um controlador dinâmico de segurança. O objetivo foi criar um método que permitisse ao sistema poupar bateria sempre que possível, aumentando o tempo de vida de cada dispositivo. Para isso, foi proposta uma arquitetura que tem por base a do protocolo LoRaWAN, onde são acrescentados o controlador e módulos de auxilio ao controlador. Esta arquitetura foi definida de forma a ser genérica para que seja possível a sua implementação em aplicações com diferentes requisitos de gestão de segurança e energia.

Após conhecida a arquitetura, foram apresentados o algoritmo que incorpora o controlador e que calcula o esquema de segurança adequado num dado momento, os testes que avaliaram o seu comportamento e os resultados desses teste e foi feita a sua apreciação.

Concluindo, os resultados obtidos ao testar o comportamento do sensor foram satisfatórios,

uma vez que são apresentados ganhos no tempo de vida do sensor em relação a um sistema com esquema de segurança fixo, como definem as especificações do LoRaWAN. Quanto aos testes em que foi detetada uma perda no tempo de vida de bateria, os resultados também podem ser considerados benéficos no âmbito da segurança, uma vez que essa perda acontece devido ao aumento do nível de segurança em comparação, novamente, com um sistema de segurança fixo. Assim, pode ser afirmado que o controlador dinâmico de segurança cumpriu os objetivos que foram traçados, o de poupar bateria, sempre que possível, para aumentar o tempo de vida o sensor ou fortalecer a segurança caso seja necessário. Para além disso, também é importante referir que o controlador se adaptou sempre às configurações da aplicação, não sendo algo definido de forma fixa e por isso pode ser adaptado a diferentes contextos de aplicação ou tecnologias.

7.2 Trabalho futuro

Com este trabalho provou-se analiticamente que a utilização do controlador apresenta melhorias, tanto na proteção, como na poupança de energia numa infraestrutura LoRaWAN. No entanto, continuam a existir diferentes forma de avaliar o controlador proposto, havendo espaço para trabalho futuro:

- A realização de uma avaliação experimental, implementando a arquitetura proposta num ambiente real, testando-a para diferentes requisitos do sistema.
- Estudo comparativo entre arquiteturas semelhantes que façam uso do controlador em diferentes posições (NS, *Gateway*, Sensor, etc.), chegando assim a uma conclusão sobre o melhor local onde incorporar este elemento.

Referências

[1] [Online]. Available: https://www.instructables.com/id/ESP32-Lora-Changing-Frequency/

[2] A. Gemalto and S. And, "LoRaWAN ™ SECURITY A WHITE PAPER PREPARED FOR THE LoRa ALLIANCE™ FULL END-TO-END ENCRYPTION FOR IoT APPLICATION PROVIDERS," LoRa Alliance, Tech. Rep., 2017. [Online]. Available: https://lora-alliance.org/sites/default/files/2019-05/lorawan{_}security{_}whitepaper.pdf

[3] X. Yang, "LoRaWAN: Vulnerability Analysis and Practical Exploitation," Delf University of Tecnology, Tech. Rep., 2017. [Online]. Available: http://repository.tudelft.nl/.

[4] "AA Battery Discharge Curves." [Online]. Available: http://madscientisthut.com/wordpress/daily-blog/aa-battery-discharge-curves/

[5] M. Eldefrawy, I. Butun, N. Pereira, and M. Gidlund, "Formal security analysis of LoRaWAN," *Computer Networks*, vol. 148, pp. 328–339, jan 2019. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1389128618306145

[6] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, and A. Ghosh, "NB-IoT system for M2M communication," in *2016 IEEE Wireless Communications and Networking Conference Workshops, WCNCW 2016*. Institute of Electrical and Electronics Engineers Inc., aug 2016, pp. 428–432. [Online]. Available: https://ieeexplore.ieee.org/document/7552737

[7] R. Ratasuk, N. Mangalvedhe, Y. Zhang, M. Robert, and J. P. Koskinen, "Overview of narrowband IoT in LTE Rel-13," in *2016 IEEE Conference on Standards for Communications and Networking, CSCN 2016*. Institute of Electrical and Electronics Engineers Inc., dec 2016. [Online]. Available: https://ieeexplore.ieee.org/document/7785170

[8] "LTE-M - Wikipedia." [Online]. Available: https://en.wikipedia.org/wiki/LTE-M

[9] R. Ratasuk, N. Mangalvedhe, A. Ghosh, and B. Vejlgaard, "Narrowband LTE-M system for M2M communication," in *IEEE Vehicular Technology Conference*. Institute of Electrical and Electronics Engineers Inc., nov 2014. [Online]. Available: https://ieeexplore.ieee.org/document/6966070

[10] R. Ratasuk, N. Mangalvedhe, D. Bhatoolaul, and A. Ghosh, "LTE-M Evolution Towards 5G Massive MTC," in *2017 IEEE Globecom Workshops, GC Wkshps 2017 - Proceedings*, vol. 2018-Janua. Institute of Electrical and Electronics Engineers Inc., jan 2018, pp. 1–6.

[11] "Sigfox Technology Overview | Sigfox." [Online]. Available: https://www.sigfox.com/en/sigfox-iot-technology-overview

[12] I. Butun, N. Pereira, and M. Gidlund, "Security Risk Analysis of LoRaWAN and Future Directions," *Future Internet*, vol. 11, no. 1, p. 3, dec 2018. [Online]. Available: http://www.mdpi.com/1999-5903/11/1/3

[13] "About LoRaWAN® | LoRa Alliance™." [Online]. Available: https://lora-alliance.org/about-lorawan

[14] L. Alliance, "A technical overview of LoRa ® and LoRaWAN ™ What is it?" LoRa Alliance, Tech. Rep., 2015. [Online]. Available: https://lora-alliance.org/sites/default/files/2018-04/what-is-lorawan.pdf

[15] "Replay attack - wikipedia." [Online]. Available: https://en.wikipedia.org/wiki/Replay_attack

[16] S. Chacko and M. D. Job, "Security mechanisms and Vulnerabilities in LPWAN," in *IOP Conference Series: Materials Science and Engineering*, vol. 396, no. 1. Institute of Physics Publishing, aug 2018.

[17] R. S. Sinha, Y. Wei, and S. H. Hwang, "A survey on LPWA technology: LoRa and NB-IoT," pp. 14–21, mar 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405959517300061

[18] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "Overview of Cellular LPWAN Technologies for IoT Deployment: Sigfox, LoRaWAN, and NB-IoT," in *2018 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2018*. Institute of Electrical and Electronics Engineers Inc., oct 2018, pp. 197–202. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8480255

[19] ——, "A comparative study of LPWAN technologies for large-scale IoT deployment," *ICT Express*, vol. 5, no. 1, pp. 1–7, mar 2019.

[20] A. Ikpehai, B. Adebisi, K. M. Rabie, K. Anoh, R. E. Ande, M. Hammoudeh, H. Gacanin, and U. M. Mbanaso, "Low-power wide area network technologies for internet-of-things: A comparative review," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2225–2240, apr 2019. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8550722

[21] Y. Rama and M. Alper Ozpmar, "A Comparison of Long-Range Licensed and Unlicensed LPWAN Technologies According to Their Geolocation Services and Commercial Opportunities," in *Mediterranean Microwave Symposium*, vol. 2018-Octob. IEEE Computer Society, jan 2019, pp. 398–403.

[22] "Hardware • FIT/IoT-LAB." [Online]. Available: https://www.iot-lab.info/hardware/

[23] "B-L072Z-LRWAN1 - STM32L0 Discovery kit LoRa, Sigfox, low-power wireless - STMicroelectronics." [Online]. Available: https://www.st.com/en/evaluation-tools/b-l072z-lrwan1.html/{#}overview

[24] "LoPy | The Things Network." [Online]. Available: https://www.thethingsnetwork.org/docs/devices/lopy/

[25] "The LoPy4 is a quadruple bearer MicroPython enabled development board including LoRa, Sigfox, WiFi and Bluetooth." [Online]. Available: https://pycom.io/product/lopy4/

[26] "FiPy - Pycom - Five Network Development Board with LTE-M, LoRa, Sigfox, WiFi and Bluetooth." [Online]. Available: https://pycom.io/product/fipy/

[27] "The Things Uno | The Things Network." [Online]. Available: https://www.thethingsnetwork.org/docs/devices/uno/

[28] "The Things Node | The Things Network." [Online]. Available: https://www.thethingsnetwork.org/docs/devices/node/

[29] "RAK811 WisNode LoRa Module | The Things Network." [Online]. Available: https://www.thethingsnetwork.org/docs/devices/rak811-wisnode-lora-module/{#}product-background

[30] "FIT/IoT-LAB • Very large scale open wireless sensor network testbed." [Online]. Available: https://www.iot-lab.info/

[31] "The things network."

[32] "RIOT - The friendly Operating System for the Internet of Things." [Online]. Available: http://www.riot-os.org/

[33] "MicroPython - Python for microcontrollers." [Online]. Available: https://micropython.org/

[34] B. Oniga, V. Dadarlat, E. De Poorter, and A. Munteanu, "A secure LoRaWAN sensor network architecture," in *Proceedings of IEEE Sensors*, vol. 2017-Decem. Institute of Electrical and Electronics Engineers Inc., dec 2017, pp. 1–3. [Online]. Available: https://ieeexplore.ieee.org/document/8233990

[35] S. Naoui, M. E. Elhdhili, and L. A. Saidane, "Trusted third party based key management for enhancing LoRaWAN security," in *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, vol. 2017-Octob. IEEE Computer Society, mar 2018, pp. 1306–1313. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8308441

[36] J. Lin, Z. Shen, and C. Miao, "Using blockchain technology to build trust in sharing LoRaWAN IoT," in *ACM International Conference Proceeding Series*, vol. Part F1306. Association for Computing Machinery, jul 2017, pp. 38–43. [Online]. Available: https://dl.acm.org/citation.cfm?id=3126980

[37] R. Sanchez-Iborra, J. Sánchez-Gómez, S. Pérez, P. Fernández, J. Santa, J. Hernández-Ramos, and A. Skarmeta, "Enhancing LoRaWAN Security through a Lightweight and Authenticated Key Management Approach," *Sensors*, vol. 18, no. 6, p. 1833, jun 2018. [Online]. Available: http://www.mdpi.com/1424-8220/18/6/1833

[38] S. Tiwari, H. B. Patel, and B. Shrimali, "A Survey on Certificate-Less Public Key Encryption for Authentication in a Smart IoT-Based LoRaWAN," IOSR Journal of Engineering, Tech. Rep., 2018. [Online]. Available: www.iosrjen.org

[39] J. Kim and J. S. Song, "A dual key-based activation scheme for secure LoRaWAN," *Wireless Communications and Mobile Computing*, vol. 2017, 2017. [Online]. Available: https://www.hindawi.com/journals/wcmc/2017/6590713/abs/

[40] U. Banerjee, "Energy-Efficient Protocols and Hardware Architectures for Transport Layer Security," Massachusetts Institute of Technology, Tech. Rep., jun 2017. [Online]. Available: https://dspace.mit.edu/handle/1721.1/111861

[41] "Kilowatt-hour - Wikipedia." [Online]. Available: https://en.wikipedia.org/wiki/Kilowatt-hour

[42] T. Bouguera, J.-F. Diouris, J.-J. Chaillout, R. Jaouadi, and G. Andrieux, "Energy Consumption Model for Sensor Nodes Based on LoRa and LoRaWAN," *Sensors*, vol. 18, no. 7, p. 2104, jun 2018. [Online]. Available: http://www.mdpi.com/1424-8220/18/7/2104