



Universidade do Minho
Escola de Engenharia
Departamento de Informática

Tese de Mestrado em Informática

**Desenvolvimento de um
Sistema de Localização baseado em Tecnologia RFID**

Mauro Nuno Barbosa de Castro

Orientador:

Prof. António Joaquim André Esteves
Departamento de Informática
Universidade do Minho

Braga, 31 de Outubro de 2011

AGRADECIMENTOS

Ao professor António Esteves, orientador da minha dissertação, agradeço o grande apoio, a partilha do saber, a paciência, a compreensão pelas minhas limitações e a grande entrega. Sem ele, este trabalho não seria possível.

Queria agradecer também aos meus pais, porque são o meu porto seguro. Foram eles que, ao longo de todos estes anos, me proporcionaram todas as condições necessárias para a minha formação.

À minha irmã, que também deu o seu contributo.

À minha namorada, Sandra, a pessoa que me fez sorrir, que aturou as minhas angústias, que me deu força nos momentos menos bons e que me ajudou muito.

O meu profundo agradecimento a todos que contribuíram para a concretização deste trabalho, estimulando-me intelectual e emocionalmente, pois não é fácil viver no silêncio.

RESUMO

Atualmente existem várias soluções comerciais que utilizam a tecnologia RFID para diversos fins aplicativos. Na literatura estão também documentados várias abordagens e algoritmos para localização de dispositivos RFID. Partindo deste contexto, o objetivo principal da presente dissertação era modelar e conceber uma solução global de monitorização/localização baseada na tecnologia RFID (pontos de acesso e etiquetas), que fosse adequada para vários tipos de organismos/empresas. Ou seja, nunca foi intenção desta dissertação propor novos algoritmos de localização por RFID.

Seguindo uma metodologia de desenvolvimento de *software* orientada aos modelos, e apoiada na tecnologia UML, o desenvolvimento do sistema percorreu as seguintes fases: (i) levantamento e documentação de requisitos, baseados na identificação das necessidades de três tipos de organismos/empresas e utilizando o modelo de Volere, (ii) identificação dos utilizadores do sistema, (iii) conceção do sistema, tarefa que incluiu a elaboração de casos de uso detalhados, diagramas de sequência ao nível do sistema, o modelo de dados persistentes do sistema, diagrama de classes e diagramas de sequência ao nível da implementação, (iv) implementação de um protótipo em Java e (iv) realização de testes com o protótipo.

Muito mais do que um algoritmo, ou conjunto de algoritmos, de localização, o sistema desenvolvido é uma solução integrada de localização baseada na tecnologia RFID. A estratégia seguida no desenvolvimento do sistema assenta em 3 princípios: (1) uma dada empresa ou organização deseja monitorizar pessoas e bens, de forma impedir/permitir o acesso a determinadas zonas do espaço físico do edifício dessa empresa, (2) uma das tecnologias mais versátil para este atingir este fim é a RFID, (3) combinando a potência do sinal RF, enviado pela mesma etiqueta RFID, e recebido em pelo menos três pontos de acesso, é possível obter uma estimativa da localização do emissor desse sinal RF. Deste modo, o sistema desenvolvido pressupõe que existem 3 pontos de acesso (conjunto de APs) em cada local de acesso a zonas críticas do edifício, geometricamente localizados de forma a facilitar a trilateração de medições do sinal RF. Entre as funcionalidades do sistema de localização desenvolvido incluem-se: acesso ao sistema controlado, gestão de utilizadores do sistema, gestão de etiquetas RFID (atribuição, recolha, programação), definição da geometria de cada piso do edifício (usando os

conceitos de ponto, segmento e zona), definição das zonas permitidas e interditas a cada tipo de utilizador, gestão dos pontos de acesso e dos conjuntos de pontos de acesso, localização de etiquetas RFID por trilateração e emissão de alertas, para uma ou mais entidades de segurança, nos casos em que ocorrer a “invasão” de uma zona interdita.

Em termos de resultados, pode dizer-se que se concebeu um protótipo funcional que cumpre a maioria dos requisitos propostos, possui uma interface fácil de utilizar e é suficientemente genérico para poder ser usado por empresas de tipos diferentes. Dado que o código e os modelos estão perfeitamente sincronizados, alterar ou adicionar funcionalidades ao sistema é relativamente seguro e com um custo moderado. Em termos da qualidade das estimativas da localização, os resultados não são muito positivos. Duas alternativas para melhorar este aspeto passariam por (i) melhorar o algoritmo de localização e (ii) usar um tipo de *hardware* RFID mais sofisticado e vocacionado para ser aplicado num sistema de localização.

ABSTRACT

Currently there are several commercial solutions that use the RFID technology for different applications. In the literature we can find several approaches and algorithms for the localization of RFID devices. In this context, the main objective of this dissertation is to model and design a global monitoring/locating solution based on the RFID technology (access points and tags), that would be adequate for several kinds of organizations/companies. In other words, it was never the intention of this dissertation to propose new RFID localization algorithms.

Following a model-based software development methodology, supported by the UML technology, the system development has taken the following steps: (i) requirements analysis and documentation, based on the identification of the needs of three types of organizations/companies, and using the Volere template, (ii) identification of the system users, (iii) system design, a task that includes the development of a detailed specification for each use case, system-level sequence diagrams, the persistent data model of the system, class diagram and implementation-level sequence diagrams, (iv) implementation of a Java prototype and (v) testing the prototype.

Much more than an algorithm, or a set of localization algorithms, the developed system is an RFID-based integrated solution for localization. The strategy followed on the system development is based in three principles: (1) a company or organization wants to monitor people and needs, so they could forbid/allow the access to certain zones of the physical space of the building, (2) one of the most versatile technologies to achieve this goal it is the RFID, (3) combining the strength of the RF signal, sent by the same RFID tag, and received at least in three access points, it's possible to achieve an estimate for the localization of the RF signal emitter. In this way, the developed system requires that there are three access points (an AP set) in the access to each critical zone of the building, geometrically located in such a way to facilitate the trilateration of the RF signal measurements. The localization system includes the following features: controlled access to the system, management of the system users, management of RFID tags (assignment, collecting, programming), definition of the geometry of each floor of the building (using the point, segment and zone concepts), defining the allowed and forbidden zones to each type of user, management of access points and sets of access

points, localization of RFID tags by trilateration, and emission of alerts for one or more security entities, in the cases that occur the “invasion” of one forbidden zone.

In terms of results, we may say that it was conceived a functional prototype that meets most of the proposed requirements, it has a user friendly interface and it is generic enough to be used by different types of companies. Since the code and the models are perfectly synchronized, alter or add functionalities to the system is relatively safe and with moderate cost. In terms of the quality of the localization estimates, the results are not very positive. Two alternatives for improving this aspect would be (i) improve the localization algorithm, and (ii) use a more sophisticated RFID hardware, geared to be applied in a localization system.

Índice

AGRADECIMENTOS	ii
RESUMO	iii
ABSTRACT	v
Índice de Figuras	xii
Índice de Tabelas	xvi
Índice de Equações	xvi
Acrónimos	xviii
Estruturas de dados	xix
<i>Capítulo 1 Introdução</i>	<i>1</i>
1.1. Objetivos	2
1.2. Estrutura da Tese	3
<i>Capítulo 2 Estado da Arte</i>	<i>5</i>
2.1. História da Tecnologia RFID	5
2.2. Definição de RFID	7
2.3. Funcionamento de um Sistema RFID	8
2.4. Tipos de Etiqueta de Acordo com a sua Autonomia	9
2.4.1. Etiquetas Passivas	9
2.4.2. Etiquetas Ativas	10
2.4.3. Comparação entre etiquetas ativas e passivas	11
2.4.4. Etiquetas Semi-passivas	11
2.5. Exemplos de Aplicação da Tecnologia RFID	11
2.5.1. Área da Saúde	11
2.5.2. Área das Bibliotecas	13
2.5.3. Área da Segurança	15
2.5.4. Área da Identificação Animal	15
<i>Capítulo 3 Análise e Modelação de Requisitos</i>	<i>17</i>
3.1. Levantamento de Necessidades	17
3.1.1. Resultados dos Inquéritos a Hospitais e Maternidades	19
3.1.2. Resultados dos Inquéritos a Bibliotecas	20
3.1.3. Resultados dos Inquéritos a Armazéns	21
3.1.4. Especificidades de um Sistema de Localização para Hospitais/Lares	22
3.1.5. Especificidades de um Sistema de Localização para Armazéns	25
3.1.6. Especificidades dum Sistema de Localização para Bibliotecas	26
3.2. Requisitos do Sistema	26
3.2.1. Requisitos Não Funcionais	32
3.3. Utilizadores de Sistema	33
<i>Capítulo 4 Conceção do Sistema</i>	<i>34</i>
4.1. Diagrama de Contexto do Sistema	35
4.2. Princípio de Funcionamento do Método de Localização	36
4.3. Estruturas de Dados de Apoio à Localização	40
4.4. Atores Intervenientes	46
4.5. Diagrama Geral de Casos de Uso	47
4.5.1. Diagrama de Casos de Uso “Sistema Central”	47
4.5.2. Diagrama de Casos de Uso do Ponto de Acesso (AP)	54

4.6.	Diagramas de sequência ao nível do sistema	55
4.7.	Modelo dos Dados Persistentes	56
4.8.	Diagrama de Classes	59
4.9.	Diagramas de sequência ao nível da implementação	65
<i>Capítulo 5 Implementação</i>		68
5.1.	Tecnologias	68
5.2.	Integração entre o código da implementação e os modelos UML	69
5.3.	Algoritmos	70
5.3.1.	Cálculo da menor distância dum ponto P a um segmento de reta	70
5.3.2.	Algoritmo para definir a zona em que se localiza um ponto P	72
5.3.3.	Algoritmo para calcular a localização duma etiqueta RFID	73
5.3.4.	Algoritmo para calcular a interceção entre duas circunferências	75
5.3.5.	Algoritmo para calcular a interceção entre dois segmentos de reta	77
5.4.	Pontos de Acesso Utilizados	78
5.4.1.	Comunicação entre pontos de acesso e sistema central por TCP/IP	79
5.4.2.	Comunicação entre etiquetas RFID e pontos de acesso	79
5.4.3.	Protocolo de comunicação entre ponto de acesso e sistema central	81
5.4.4.	Protocolo utilizado no caso de uso “Receber pacote de AP por TCP/IP”	81
5.4.5.	Protocolo utilizado no caso de uso “Configurar AP”	82
5.4.6.	Protocolo utilizado no caso de uso “Enviar Comando ao AP para Ler a Configuração”	83
5.5.	Protótipo do Sistema Desenvolvido	84
5.5.1.	Operações sobre Pontos de Acesso (APs)	85
5.5.2.	Operações sobre conjuntos de pontos de acesso	89
5.5.3.	Emissão de alertas quando um utilizador de etiqueta RFID entra numa zona interdita	91
5.5.4.	Criar e gerir utilizadores do sistema, incluindo administrador do sistema	92
5.5.5.	Autenticação de um utilizador registado	93
5.5.6.	Definir as zonas dum edifício	93
5.5.7.	Criar e gerir as listas de zonas dum edifício permitidas e interditas a cada tipo de utilizador	94
5.5.8.	Operações sobre etiquetas RFID: atribuir, recolher e listar etiquetas atribuídas	96
5.5.9.	Localizar utilizadores de etiqueta RFID	97
5.5.10.	Simular o envio de pacotes para se efetuar a trilateração entre medições de RSSI	99
<i>Capítulo 6 Testes Efetuados e Resultados</i>		102
6.1.	<i>Hardware</i> utilizado nos testes	102
6.2.	Calibração do <i>hardware</i> utilizado nos testes	102
6.3.	Resultados da calibração do <i>hardware</i> usado nos testes	104
6.4.	Teste do protótipo desenvolvido	110
<i>Capítulo 7 Conclusões e Trabalho Futuro</i>		112
7.1.	Conclusões	112
7.2.	Trabalho Futuro	116
Bibliografia		118
Anexos		121
Anexo I	Inquérito para Armazéns	121
Anexo II	Inquérito aos bibliotecários	125
Anexo III	Inquérito aos profissionais de saúde	129

Anexo IV	Implementação do Intervalo de Tolerância nas Medições (DELTAT) entre 0 e 2 Segundos	133
Anexo V	Descrição textual dos casos de uso do Sistema Central	135
1.	Descrição Textual do caso de uso “Imprimir Etiqueta de Papel para Etiqueta_RFID”	135
2.	Descrição Textual do caso de uso “Atribuir etiqueta_RFID”	136
3.	Descrição Textual do caso de uso “Programar etiqueta_RFID”	137
4.	Descrição Textual do caso de uso “Recolher etiqueta_RFID”	139
5.	Descrição textual do caso de uso “Listar as etiquetas atribuídas aos utilizadores”	140
6.	Descrição Textual do caso de uso “Login”	141
7.	Descrição Textual do caso de uso “Logout”	142
8.	Descrição Textual do caso de uso “Inicializar a lista de acessos às zonas do edifício”	142
9.	Descrição Textual do caso de uso “Alterar a lista de acessos às zonas do edifício”	144
10.	Descrição Textual do caso de uso “Registar utilizador do sistema”	145
11.	Descrição Textual do caso de uso “Criar perfil de administrador do sistema”	146
12.	Descrição textual do caso de uso “Emitir sinal de alerta”	148
13.	Descrição textual do caso de uso “Configurar AP”	149
14.	Descrição textual do caso de uso “Criar dados do AP”	152
15.	Descrição textual do caso de uso “Alterar dados do AP”	154
16.	Descrição textual do caso de uso “Remover AP do sistema”	156
17.	Descrição textual do caso de uso “Receber pacote de AP por TCP/IP”	157
18.	Descrição textual do caso de uso “Guardar pacote recebido dum AP”	158
19.	Descrição textual do caso de uso “Listar descrição do AP”	159
20.	Descrição textual do caso de uso “Criar conjunto de APs”	160
21.	Descrição textual do caso de uso “Adicionar AP a um conjunto de APs”	161
22.	Descrição textual do caso de uso “Remover AP do conjunto de APs”	162
23.	Descrição textual do caso de uso “Eliminar conjunto de APs”	162
24.	Descrição textual do caso de uso “Listar descrição do Conjunto de APs”	163
25.	Descrição textual do caso de uso “Enviar Comando ao AP para Ler a Configuração”	164
26.	Descrição textual do caso de uso “Calcular localização duma TAG”	165

27.	Descrição textual do caso de uso “Calcular zona de localização”	166
28.	Descrição textual do caso de uso “Definir Zonas”	167
29.	Descrição textual do caso de uso “Definir segmentos”	169
Anexo VI Descrição textual dos casos de uso do Ponto de Acesso (AP)		171
1.	Descrição textual do caso de uso “Receção de mensagem de etiqueta_RFID”	171
2.	Descrição textual do caso de uso “Enviar pacote construído para o sistema central”	171
3.	Descrição textual do caso de uso “Responder a pedidos de leitura da configuração”	172
4.	Descrição textual do caso de uso “Efetuar configuração do AP”	173
Anexo VII Diagramas de Sequência ao Nível do Sistema		175
1.	Diagrama de Sequência “Imprimir Etiqueta de Papel para Etiqueta_RFID”	175
2.	Diagrama de Sequência “Atribuir etiqueta_RFID”	176
3.	Diagrama de Sequência “Programar etiqueta_RFID”	177
4.	Diagrama de Sequência “Recolher etiqueta_RFID”	178
5.	Diagrama de Sequência “Login”	178
6.	Diagrama de Sequência “Logout”	179
7.	Diagrama de Sequência "Inicializar a lista de acessos às zonas do edifício"	180
8.	Diagrama de Sequência "Alterar a lista de acessos às zonas do edifício"	181
9.	Diagrama de Sequência "Registrar utilizador do Sistema / Criar perfil de administrador do sistema"	182
10.	Diagrama de Sequência "Emitir sinal de alerta”	183
11.	Diagrama de Sequência "Configurar AP”	184
12.	Diagrama de Sequência "Erro: Configurar AP”	185
13.	Diagrama de Sequência "Criar Dados de AP”	186
14.	Diagrama de Sequência "Introduzir Coordenadas de Localização de um AP”	187
15.	Diagrama de Sequência "Gravar Dados de AP”	187
16.	Diagrama de Sequência "Alterar Dados de AP”	188
17.	Diagrama de Sequência "Alterar Coordenadas de Localização de um AP”	189
18.	Diagrama de Sequência "Gravar Coordenadas de Localização de um AP”	190

19.	Diagrama de Sequência "Guardar novo valor de conjunto do AP "	190
20.	Diagrama de Sequência "Remover AP do sistema"	191
21.	Diagrama de Sequência "Apagar ID_AP"	192
22.	Diagrama de Sequência "Adicionar AP a um conjunto de APs"	192
23.	Diagrama de Sequência "Criar Conjunto de APs"	193
24.	Diagrama de Sequência "Introduzir ID do conjunto"	193
25.	Diagrama de Sequência "Gravar Conjunto de APs"	194
26.	Diagrama de Sequência "Eliminar conjunto de APs"	194
27.	Diagrama de Sequência "Remover AP do conjunto de APs"	195
28.	Diagrama de Sequência "Listar Descrição do AP"	195
29.	Diagrama de Sequência "Listar Descrição do Conjunto de APs"	196
30.	Diagrama de Sequência "Enviar Comando ao AP Ler a Configuração"	196
31.	Diagrama de Sequência "Guardar pacote recebido dum AP"	197
32.	Diagrama de Sequência "Gravar pacote recebido dum AP"	198
33.	Diagrama de Sequência "Calcular localização dum TAG"	198
34.	Diagrama de Sequência "Receber pacote de AP por TCP/IP"	199
35.	Diagrama de Sequência "Guardar ultima pacote para o numero do posição de AP_ID de um TAG_ID"	200
36.	Diagrama de Sequência "Receção de mensagem de etiqueta_RFID"	200
37.	Diagrama de Sequência "Enviar pacote construído para o sistema central"	201
38.	Diagrama de Sequência "Responder a pedidos de leitura de configuração"	201
39.	Diagrama de Sequência "Efetuar Configuração do AP"	202
Anexo VIII Protocolo de Comunicação entre o(s) Ponto(s) de Acesso e o Sistema Central		203
1.	Protocolo utilizado no caso de uso "Configurar AP"	203
2.	Protocolo utilizado no caso de uso "Enviar Comando ao AP para Ler a Configuração"	205

Índice de Figuras

Figura 1 - Antigos sistemas de Radar [4].	6
Figura 2 - Etiqueta, leitor e servidor [6].	8
Figura 3 - Exemplos de etiquetas [6].	8
Figura 4 - Leitor de Dispositivos RFID [6].	9
Figura 5 - Exemplos de etiquetas passivas [12].	10
Figura 6 - Exemplos de etiquetas ativas [11] [13].	10
Figura 7 - Chip RFID para implante em pessoas [2].	12
Figura 8 - Cartão Active Tag [22].	24
Figura 9 - Pulseira RFID [22].	25
Figura 10 - Pulseira RFID [22].	25
Figura 11 – Modelo para a especificação de requisitos [23].	27
Figura 12 - Diagrama de contexto do sistema estruturado em 3 camadas.	35
Figura 13 - Arquitetura física do edifício e do sistema de localização.	37
Figura 14 - Exemplo da planta de um piso de um edifício para ilustrar o princípio de funcionamento do método de localização.	39
Figura 15 - Estrutura de dados packet que guarda um pacote recebido.	40
<i>Figura 16 - Estrutura de dados APdata que guarda os dados dum AP.</i>	40
Figura 17 - Estrutura de dados listAPs que guardam os conjuntos de APdata.	41
Figura 18 - Estruturas de dados setAPs e listSetAPs que guardam os conjuntos de APs.	41
Figura 19 - Estruturas de dados EtiquetaRFID e listaEtiquetaRFID que guardam os dados das etiquetas RFID.	42
Figura 20 - Estrutura de dados PacksLastPosTAG que guarda a lista de pacotes relativos à última posição de cada etiqueta RFID.	43
Figura 21 - Estruturas de dados Segment e listSegments .	44

Figura 22 - Estruturas de dados Zone e listZones utilizadas para guardar a geometria das zonas do edifício.	45
Figura 23 - Diagrama de casos de uso global do sistema.....	48
Figura 24 - Caso de Uso "Enviar Ordem para efetuar uma operação sobre etiqueta". ..	53
Figura 25 – Diagrama de casos de uso do Ponto de Acesso (AP).....	54
Figura 26 - Modelo dos dados persistentes.	58
Figura 27 - Diagrama de classes do sistema.....	64
Figura 28 - Diagrama de sequência “Atribuir etiqueta RFID”.....	65
Figura 29 - Diagrama de sequência "Guardar pacote recebido dum AP".	66
Figura 30 - Diagrama de sequência "Calcular localização dum TAG".	66
Figura 31 - Diagrama de sequência "Receber pacote de AP por TCP/IP".	67
Figura 32 - Arquitetura da JDBC.	68
Figura 33 – Exemplo de integração entre o modelo UML e a implementação em Java para a classe “etiqueta_RFID”.	69
Figura 34 - Ilustração do cálculo da menor distância dum ponto a um segmento de reta (ou a uma reta).....	70
Figura 35 - Ilustração do funcionamento do algoritmo que calcula a zona dum localização P, em especial a definição da vizinhança Sviz(Patual).	73
Figura 36 - Fundamento do algoritmo utilizado para calcular a localização dum etiqueta RFID	75
Figura 37 - Ilustração da metodologia utilizada para calcular os pontos de interceção (E e F) entre duas circunferências.....	76
Figura 38 - Interseção entre dois segmentos de reta.....	78
Figura 39 - Arquitetura do hardware utilizada na modelação e validação do sistema desenvolvido.....	79
Figura 40 - Comunicação entre um ponto de acesso (recetor) e as etiquetas RFID.....	80
Figura 41 - Estrutura do protótipo do sistema.	84
Figura 42 - Arquitetura do protótipo.	85
Figura 43 - Formulário referente às operações sobre um AP.....	86
Figura 44 – Formulário referente à operação de edição dos dados dum AP.	87

Figura 45 - Formulário referente à operação de configuração dum AP (no modo TCP Client).....	88
Figura 46 - Formulário relativo ao processo “Enviar um comando ao AP para ler a configuração”.....	88
Figura 47 – Caixa de diálogo referente à operação de remover um AP do sistema.....	89
Figura 48 – Formulário utilizado para executar operações sobre conjuntos de APs.....	89
Figura 49 - Formulário de dados referente ao processo de "Adicionar AP a um conjunto de APs" que está a ser criado.	90
Figura 50 - Formulário de dados referente ao processo de inserção de mais APs no mesmo conjunto.	90
Figura 51 - Caixa de diálogo "Pretende guardar os dados do conjunto?".	90
Figura 52 - Formulário de dados referente ao processo de alteração de um conjunto de APs previamente criado.	91
Figura 53 – Caixa de diálogo para mostrar a composição dum conjunto de APs.....	91
Figura 54 - Seção da interface do protótipo relativa à emissão de alertas.....	92
Figura 55 - Formulário relativo ao registo dum utilizador do sistema.....	92
Figura 56 - Formulário para um utilizador registado se autenticar perante o sistema....	93
Figura 57 – Esquema ilustrativo da definição de uma zona dum edifício.....	94
Figura 58 - Interface utilizada para definir uma zona dum edifício.....	94
Figura 59 - Interface concebida para criar e alterar as listas de zonas permitidas e interditas do edifício.....	95
Figura 60 - Formulário referente ao processo “Configurar tipo de alerta”.	95
Figura 61 – Caixa de diálogo para registar a atribuição dum etiqueta RFID a um utilizador.....	96
Figura 62 - Caixa de diálogo para registar a recolha dum etiqueta RFID entregue a um utilizador.....	97
Figura 63 – Interface com o utilizador que mostra o conteúdo da lista PacksLastPosTAG (D5).	98
Figura 64 – Interface que mostra ao utilizador informação sobre os últimos pacotes recebidos.....	98
Figura 65 – Interface com o utilizador que mostra informação sobre a localização de utilizadores de etiqueta RFID.....	99

Figura 66 - Interface com o utilizador que permite simular o envio de pacotes para se efetuar a trilateração entre medições de RSSI.....	100
Figura 67 – Interface que mostra alguns detalhes relativos aos cálculos envolvidos na estimação da localização de etiquetas RFID.....	101
Figura 68 – Cenários que podem ocorrer no cálculo da localização duma etiqueta, no que diz respeito à interceção dum par de circunferências.....	101
Figura 69 – Medição de RSSI no recetor, com a etiqueta RFID emissora colocada em diferentes distâncias e ângulos (posições assinaladas por uma carta na figura). ..	103
<i>Figura 70 - Medição de RSSI em função da distância, com a etiqueta colocada numa direção de 45 graus.....</i>	<i>106</i>
<i>Figura 71 - Erro entre os valores de RSSI medidos e calculados com a equação 3, com a etiqueta colocada numa direção de 45 graus.</i>	<i>106</i>
<i>Figura 72 - Medição de RSSI em função da distância, com a etiqueta colocada numa direção de 90 graus.....</i>	<i>107</i>
<i>Figura 73 - Erro entre os valores de RSSI medidos e calculados com a equação 3, com a etiqueta colocada numa direção de 90 graus.</i>	<i>108</i>
Figura 74 - Medição de RSSI em função da distância, com a etiqueta colocada numa direção de 135 graus.....	109
<i>Figura 75 - Erro entre os valores de RSSI medidos e calculados com a equação 3, com a etiqueta colocada numa direção de 135 graus.</i>	<i>109</i>
<i>Figura 76 - Comparação das medições de RSSI, em função da distância, para 3 direções distintas (45, 90 e 135 graus).</i>	<i>110</i>
Figura 77 – Parte da interface com o utilizador que reúne o acesso às funcionalidades do protótipo mais diretamente ligadas com a localização de etiquetas RFID.....	111

Índice de Tabelas

Tabela 1 - Evolução do RFID [5]	7
Tabela 2 - Comparação entre etiquetas ativas e passivas [5].	11
Tabela 3 - Resultados da medição de RSSI para várias distâncias, com a etiqueta colocada numa direção de 45 graus.....	105
Tabela 4 - Resultados da medição de RSSI para várias distâncias, com a etiqueta colocada numa direção de 90 graus.....	107
Tabela 5 - Resultados da medição de RSSI para várias distâncias, com a etiqueta colocada numa direção de 135 graus.....	108

Índice de Equações

Equação 1	37
Equação 2	38
Equação 3	38
Equação 4	38
Equação 5	39
Equação 6	39
Equação 7	70
Equação 8	70
Equação 9	71
Equação 10	71
Equação 11	71
Equação 12	71
Equação 13	71
Equação 14	71

Equação 15	71
Equação 16	71
Equação 17	71
Equação 18	75
Equação 19	76
Equação 20	76
Equação 21	76
Equação 22	76
Equação 23	76
Equação 24	77
Equação 25	77
Equação 26	77
Equação 27	77
Equação 28	77
Equação 29	77
Equação 30	77
Equação 31	77

Acrónimos

RFID - *Radio-Frequency IDentification* (Identificação por Rádio Frequência).

IBM - *International Business Machines*.

CI - Circuito Integrado.

RF - Rádio Frequência.

TCP/IP - *Transmission Control Protocol*.

ID - Número de Identificação.

UML - *Unified Modeling Language*.

AP – *Access Point* (Ponto de Acesso).

RSSI - *Received Signal Strength Indicator*.

TAG – Etiqueta RFID.

JDBC - *Java DataBase Connectivity*.

LQI - *Link Quality* (É um indicador de qualidade da ligação entre um leitor e uma etiqueta RFID).

SN – Referência da etiqueta RFID (número de série).

MMQ – Método dos mínimos quadrados.

Estruturas de dados

D1 – Um pacote recebido.

D2 - Dados de um AP.

D3 - Lista com os conjuntos de APs.

D4 – Dados de uma etiqueta RFID.

D4L - Lista com os dados das várias etiquetas RFID.

D5 - Lista de pacotes relativos à última posição de cada etiqueta RFID.

D6 - Lista com os dados dos vários APs.

D7 - Conjunto de APs.

D8 – Lista de segmentos.

D9 – Lista de zonas.

D10 – Lista com a associação entre utilizadores e etiquetas RFID.

Capítulo 1 Introdução

Sabemos que a evolução tecnológica é como uma bola de neve, isto é, cresce a cada dia, e a ausência desse conhecimento faz-nos distanciar gradualmente do mundo real. Para nos localizarmos um pouco mais, vejamos o que se considera ser tecnologia. Goodman & Sproull [1] definem tecnologia como sendo o conhecimento de relações causa-efeito contido (embutido) nas máquinas e equipamentos utilizados para realizar um serviço ou fabricar um produto. Para um leigo, a tecnologia pode ser vista como o conjunto particular de dispositivos, máquinas e outros aparelhos utilizados numa empresa para a produção do seu resultado.

Podemos também definir tecnologia de uma forma muito diferente, como sendo um pacote de informações de tipos diversos, organizadas, provenientes de várias fontes e obtidas através de diversos métodos, utilizado na produção de bens.

Para Gonçalves Lima [2], a tecnologia é muito mais que apenas equipamentos, máquinas e computadores. A organização funciona a partir da operação de dois sistemas que dependem um do outro de maneira variada. Existe um sistema técnico, formado pelas técnicas e ferramentas, utilizadas para realizar cada tarefa. Existe também um sistema social, com suas necessidades, expectativas e sentimentos sobre o trabalho. Os dois sistemas são simultaneamente otimizados quando os requisitos da tecnologia e as necessidades das pessoas são atendidos conjuntamente. Assim, é possível distinguir entre tecnologia (conhecimento) e sistema técnico (combinação específica de máquinas e métodos empregues para obter um resultado desejado).

Neste caso, podemos concluir que a tecnologia seria representada por um conjunto de características específicas do sistema técnico no cenário em que a mesma funciona. É notório, portanto, o uso de novas tecnologias pelo indivíduo na organização dos seus negócios, nos quais há a necessidade de deslocar grandes quantidades de mercadorias bem como de acompanhar o seu estado ao longo da cadeia de consumo, desde o produtor até ao consumidor. Existe também cada vez mais a necessidade de localizar e identificar bens e pessoas. Esta necessidade de saber rapidamente, em tempo real ou não, onde se encontra um determinado item pode reduzir drasticamente o tempo de ação de um determinado negócio. Desta forma, podem ser diminuídos tempos de resposta, refletindo-se no aumento da eficácia e eficiência dos negócios.

As telecomunicações têm dado as ferramentas necessárias a este crescente ritmo e têm evoluído cada vez mais na crescente necessidade de localizar e identificar bens e pessoas.

Não só se pretende localizar pessoas, usando tipicamente para esse processo as redes móveis, como cada vez mais se torna imperativo localizar objetos, mercadorias, meios de transporte e até mesmo animais selvagens por meio de sistemas cada vez mais simples e pouco dispendiosos. Desde os mais simples objetos (fixos dentro de uma garagem ou armazém) até aos mais complexos (automóveis ou animais em locais longínquos, por exemplo), os sistemas de localização são hoje uma tecnologia apetejada pela indústria eletrónica.

1.1. Objetivos

O principal objetivo do presente trabalho é desenvolver um sistema para monitorizar a localização de bens, funcionários e visitantes numa empresa (ou seja, do edifício da empresa) através de etiquetas e recetores RFID. Para atingir este objetivo deve ser possível configurar a comunicação entre os recetores e o sistema central. Também deve ser possível inserir, remover, mudar de local e descrever os recetores perante sistema.

Outra funcionalidade necessária é a gestão das etiquetas RFID, onde se inclui saber em cada momento qual a etiqueta associada a cada utilizador, bem como associar e remover a associação entre etiquetas e utilizadores.

Outro grande objetivo é poder restringir o acesso de pessoas e bens a determinadas zonas do edifício da empresa, sendo emitidos alertas quando as zonas interditas forem acedidas por utilizadores cujo acesso esteja negado. Para atingir este objetivo deve ser possível definir zonas permitidas e interditas para cada tipo de utilizador e quais os tipos de alerta a emitir no caso de ocorrer o acesso a zonas interditas. Por questões de segurança deve haver alternativas para o tipo de alerta.

O sistema deve ainda ter um acesso controlado, estando apenas acessível a utilizadores registados. Deve haver a possibilidade de diferenciar as funcionalidades acessíveis a cada tipo de utilizador do sistema.

Pretende-se que a solução a desenvolver seja útil para diferentes tipos de empresas ou organismos. Deste modo, a conceção deve ser o mais modular e parametrizável possível.

1.2. Estrutura da Tese

Este documento descreve o trabalho realizado no âmbito da dissertação de Mestrado em Engenharia Informática, o qual se encontra organizado em capítulos.

No primeiro capítulo faz-se uma introdução à tecnologia RFID e enunciam-se os objetivos da dissertação e a estrutura do documento.

No capítulo 2 é feito o levantamento do estado de arte. Aqui é dada uma retrospectiva histórica da tecnologia RFID e é apresentado o modo de funcionamento desta tecnologia. Também são apresentados e comparados vários tipos de etiquetas RFID, uma vez que é com base nesta tecnologia que se irá projetar o sistema. Para finalizar são dados alguns exemplos de aplicação da tecnologia RFID, nas áreas da saúde, arquivo documental e segurança.

No capítulo 3 é apresentado o problema que foi proposto resolver e depois faz-se o levantamento e modelação dos requisitos do sistema. Para ajudar na captura dos requisitos do sistema, elaboram-se inquéritos que foram entregues a várias pessoas de 3 instituições tipo que foram alvo de estudo: hospitais, armazéns e bibliotecas. Com base nos resultados destes inquéritos procedeu-se à identificação, análise prioritização e documentação da lista de requisitos funcionais e não funcionais do sistema.

No capítulo 4 é detalhada a conceção do sistema, recorrendo para isso a vários digramas do UML: diagrama de casos de uso e descrição textual de cada caso de uso, diagramas de sequência e diagrama de classes. Será ainda concebido o modelo dos dados persistentes. Antes de elaborar o diagrama de casos de uso são apresentados (i) o diagrama de contexto, que permite identificar os atores envolvidos, (ii) o princípio de funcionamento do método de localização por RFID e (iii) as estruturas de dados que se revelaram fundamentais para conceber o sistema de localização.

O capítulo 5 descreve a implementação de um protótipo do sistema de localização. Começa-se por identificar as tecnologias de *software* utilizadas no desenvolvimento do protótipo e a abordagem seguida para manter o código da implementação e os modelos UML sincronizados. Depois disto descrevem-se os

algoritmos mais importantes do processo de localização das etiquetas RFID. A fase seguinte consistiu em resumir as características dos pontos de acesso (APs), nomeadamente no que diz respeito à comunicação entre os APs e o sistema hospedeiro e entre os APs e as etiquetas RFID. Por fim, é apresentada a interface do protótipo desenvolvido com o utilizador do sistema. É ainda apresentada uma funcionalidade que permite simular o envio de pacotes a partir de etiquetas RFID para se poder testar todo o processo de localização por trilateração de medições.

No capítulo 6 são descritos o equipamento e os procedimentos utilizados durante a fase de testes do protótipo desenvolvido. Nos procedimentos é de salientar a calibração do equipamento. Aborda-se também a funcionalidade do protótipo desenvolvida para facilitar os testes e apresentam-se, de uma forma clara e objetiva, os resultados obtidos nos testes efetuados.

Por último, o capítulo 7 expõe as conclusões e considerações finais a que se chegou com a realização deste trabalho. Abordam-se também as limitações e possibilidades de melhoria do trabalho desenvolvido, que podem ser vistas como possibilidades de trabalho futuro na continuidade do trabalho realizado.

Capítulo 2 Estado da Arte

2.1. História da Tecnologia RFID

A tecnologia *Radio Frequency IDentification* (RFID) tem as suas raízes nos sistemas de radares utilizados na Segunda Guerra Mundial (2ª GM). Os alemães, japoneses, americanos e ingleses utilizavam radares – que foram descobertos em 1937 por *Sir Robert Alexander Watson-Watt* [3], um físico escocês – para avisá-los com antecedência de aviões, quando eles ainda estavam bem distantes. O problema era identificar, de entre esses aviões, qual era inimigo e qual era aliado. Os alemães descobriram então que se os seus pilotos girassem os aviões quando estivessem de regresso à base iriam modificar o sinal de rádio que seria refletido (de volta) para o radar. Esse método simples alertava os técnicos responsáveis pelo radar que se tratava de um avião alemão. Este foi, essencialmente, o primeiro sistema passivo RFID.

No decorrer da 2ª GM ocorreram evoluções no que respeita ao sistema de radar. Este tornou-se capaz de detetar não só navios e aviões, mas também aviões a voar a baixa altitude. Com o desenvolvimento da tecnologia, surgiram também melhoramentos no alcance e na frequência de operação dos radares, usando comprimentos de onda mais curtos que permitiam maior alcance. Este sistema de radar passou a ser conhecido como o radar de micro-ondas. Com estes avanços tecnológicos tornou-se possível seguir as rotas de navios e aviões, calcular a sua velocidade e, mais importante, identificá-los. Deste modo, conseguia-se saber se o objeto detetado era aliado ou inimigo. A necessidade de distinguir entre os vários objetos ao alcance do radar conduziu ao modelo de identificação “*Identify: Friend or Foe?*”. Este modelo foi posteriormente chamado de “*squawk*” e consistia num código de quatro letras que se introduz manualmente no *transponder* do avião, o qual ao ser interrogado sobre quem é, devolve automaticamente este código.

O RFID está de certa forma ligado ao radar, dado que as etiquetas (*tags*) passivas se assemelham aos objetos que o radar tenta encontrar. Quando uma etiqueta passiva se encontra dentro do raio de alcance de um determinado recetor, esta vai receber energia proveniente do recetor. Desta forma, a energia oriunda do recetor vai ativar a etiqueta e permite que ela emita um sinal que poderá ser lido pelo recetor. Embora o sinal emitido pela etiqueta não seja a reflexão do sinal emitido pelo recetor, o

princípio mantém-se idêntico ao radar, dado que a emissão de energia leva a que haja um sinal de resposta que pode ser lido por um dispositivo à escuta.

Na década de 60 e 70 surgem os primeiros estudos e implementações de sistemas RFID. Os primeiros sistemas eram bastante simples, poderiam ser apenas etiquetas de 1 bit que permitiam saber se um dado item de uma loja que estava a atravessar a porta de saída teria sido pago ou teria sido roubado. Desta forma, seria possível detetar furtos de lojas. Ao pagar os itens as etiquetas seriam desativadas e desta forma não ativariam o alarme à saída. Pelo contrário, um item não pago (roubado) ativaria um alarme. Surgem também etiquetas em formato de cartão, usadas pelo exército para fazer controlo de acessos.

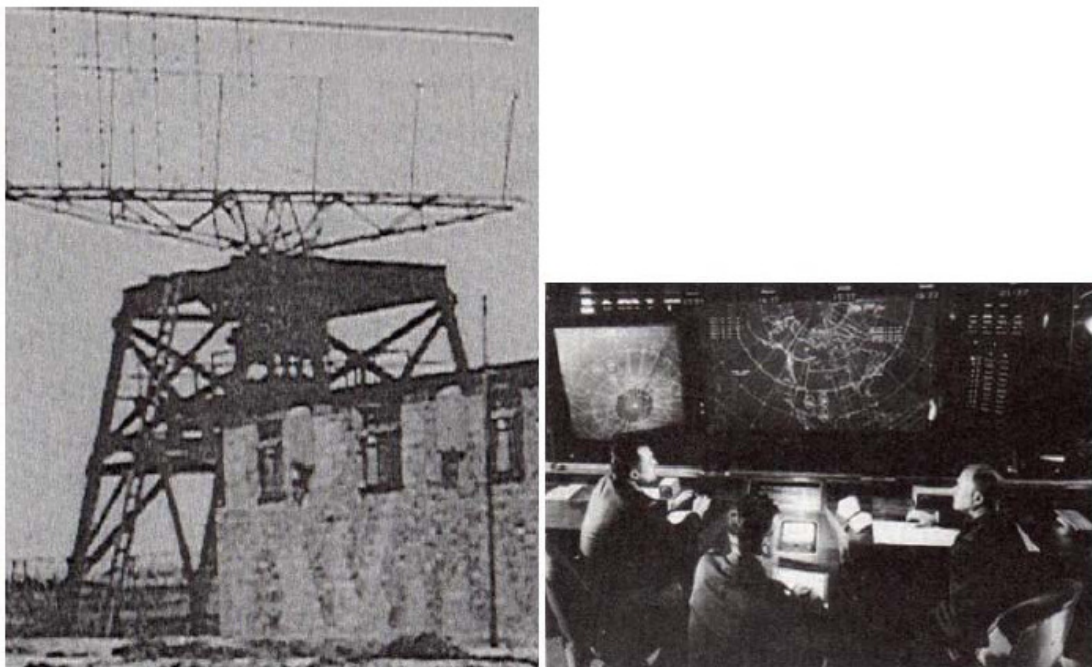


Figura 1 - Antigos sistemas de Radar [4].

A primeira etiqueta RFID surge em 1969 resultante de uma conversa entre Mário Cardullo e um engenheiro da *International Business Machines* (IBM). A IBM tinha em mãos a implementação de um sistema ótico chamado de CARTRAK para os comboios. Este sistema era baseado num código de barras multicolor na lateral de cada carruagem. Ao passarem pelos leitores, as carruagens seriam então identificadas através da leitura do código de barras. Este sistema traria imensos problemas de leitura resultantes da sujidade, da luz intensa, ou dos danos na etiqueta que continha o código. Cardullo apercebe-se dos problemas associados a este projeto e propõe um sistema que

incluía um transmissor, um recetor, uma pequena quantidade de memória interna e uma fonte de alimentação. Cardullo continuaria a trabalhar nesta área e uns anos mais tarde surge um sistema de pagamento automático de portagens.

Década	Eventos
1940-1950	Invenção e rápido desenvolvimento do radar durante a 2ª Guerra Mundial O princípio de funcionamento do RFID em 1948
1950-1960	Primeiras explorações da RFID e experimentações laboratoriais
1960-1970	Desenvolvimento da teoria da RFID Primeiras aplicações experimentais no terreno
1970-1980	Explosão no desenvolvimento da RFID Aceleração dos testes Implementações embrionárias de RFID
1980-1990	Aplicações comerciais de RFID entram no mercado
1990-2000	Surgimento de standards RFID é largamente utilizado começando a fazer parte da vida de cada um.

Tabela 1 - Evolução do RFID [5].

2.2. Definição de RFID

A identificação por ondas rádio, mais conhecida por RFID (*Radio Frequency Identification*) consiste genericamente no armazenamento e posterior envio de informação por meio de ondas eletromagnéticas para circuitos integrados compatíveis com rádio frequência. Este sistema permite não só a identificação mas também a localização, a monitorização de pessoas ou objetos recorrendo a ondas rádio. Sumariamente, a RFID permite efetuar a identificação de itens através de ondas rádio.

Os atuais sistemas de RFID, que possuem grande capacidade de identificação e de localização de bens ou pessoas, levaram a que esta tecnologia assumisse um papel importante na indústria e no comércio. Com efeito, no futuro podem imaginar-se diversas aplicações para esta tecnologia nas mais variadas áreas, desde a identificação e localização de objetos dentro de armazéns (minimizando o tempo gasto na procura de *stocks*), controlo e armazenamento de mercadorias, monitorização de pessoas e bens, entre outros. Existem ainda aplicações de RFID para fins de diagnóstico médico, na indústria química, farmacêutica, têxtil ou em simples lojas de roupa ou bibliotecas.

2.3. Funcionamento de um Sistema RFID

Na tecnologia RFID, o funcionamento dum sistema é visto de forma global, e não cada parte a funcionar de forma isolada. Este tipo de sistema utiliza o espectro eletromagnético para transmitir a informação. A RFID também pode ser definida como uma tecnologia de identificação que utiliza a radiofrequência para a troca de dados, permitindo realizar remotamente o armazenamento e recuperação de informação utilizando um dispositivo chamado *transponder*, que é um pequeno objeto que poderá ser fixado ou integrado num produto, num bem ou inclusive num ser vivo. É uma tecnologia que utiliza ondas eletromagnéticas (sinais de rádio) para transmitir dados armazenados num *microchip*. Este dispositivo (*microchip*) está associado a um dos componentes básicos dos sistemas RFID e é designado de *e-tag*, *tag RFID*, *transponder*, etiqueta eletrónica, etiqueta inteligente, ou simplesmente etiqueta.

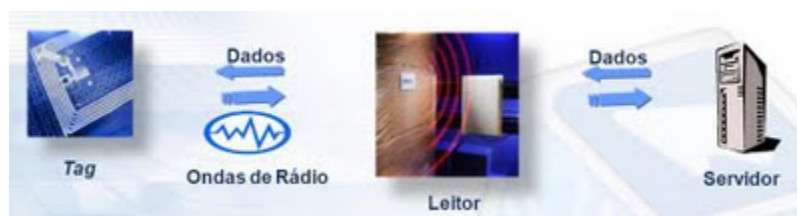


Figura 2 - Etiqueta, leitor e servidor [6].

Os sistemas RFID que se encontram atualmente no mercado têm uma arquitetura bastante simples, e que se baseia em três componentes básicos:

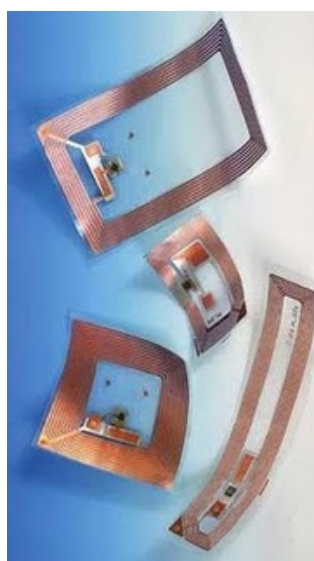


Figura 3 - Exemplos de etiquetas [6].

- Etiqueta (*transponder*): é um componente essencial para qualquer sistema RFID. Está associado ao recurso que se pretende identificar. Contém circuitos integrados e antena que lhe permitem responder aos sinais de rádio enviados por uma base transmissora.
- Sistema de leitura (leitor e antena): o leitor é um componente obrigatório responsável pela leitura da informação enviada pela etiqueta. A antena do leitor é facultativa. Muitos dos leitores não possuem uma antena incorporada, mas os leitores mais recentes já possuem antena incorporada, o que incrementa o seu raio de ação.



Figura 4 - Leitor de Dispositivos RFID [6].

- Servidor e *software (middleware)*: teoricamente, qualquer sistema RFID pode operar sem estes componentes, mas nesse caso torna-se praticamente inútil.

2.4. Tipos de Etiqueta de Acordo com a sua Autonomia

2.4.1. Etiquetas Passivas

Este tipo de etiqueta não possui qualquer tipo de alimentação [7] [8] [9]. Quando se encontram numa zona de leitura, são ativadas pela potência emitida pelo leitor, reaproveitando essa energia para retransmitir informação [10] [7].

Devido à ausência de bateria, o tamanho é cada vez menor, sendo este tipo de etiquetas as menos dispendiosas. Podem ainda assumir qualquer forma física desejada. Pelo facto

de não terem bateria, podem manter-se em funcionamento sem necessitarem de manutenção durante um tempo longo.

As etiquetas são geralmente feitas à base de silício, mas existem atualmente etiquetas feitas de materiais poliméricos. Futuramente pretende-se que as etiquetas possam ser impressas, como um simples código de barras, tornando-as assim economicamente comparáveis ao código de barras [11].

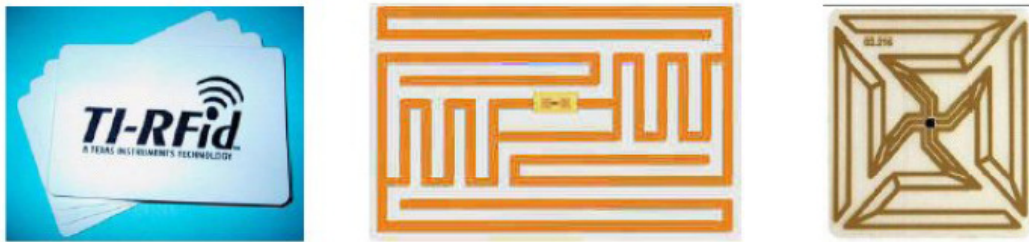


Figura 5 - Exemplos de etiquetas passivas [12].

2.4.2. Etiquetas Ativas

As etiquetas ativas possuem uma fonte de energia interna, bateria [5] [8], que alimenta o seu circuito integrado e fornece energia para o envio de dados para o leitor [5]. Como possuem bateria, para além de terem um alcance atual de dezenas de metros, podem estar ativas continuamente e necessitam de pouca potência para comunicarem. Apesar de tudo, têm algumas desvantagens, comparativamente com as etiquetas passivas: são maiores, o tempo de vida útil sem manutenção é consideravelmente menor (cerca de 10 anos) e os custos são substancialmente superiores [5].



SYTAG245-TM-AA1

Figura 6 - Exemplos de etiquetas ativas [11] [13].

2.4.3. Comparação entre etiquetas ativas e passivas

Na tabela seguinte é efetuada a comparação entre etiquetas ativas e passivas.

	Etiqueta RFID Ativa	Etiqueta RFID Passiva
Bateria	Sim	Não
Potência na etiqueta	Continua	Só quando está ao alcance do leitor
Sinal no leitor/etiqueta	Fraco/Forte	Forte/Fraco
Alcance	Longo (12m)	Curto (3m)
Acesso múltiplo	Sim	Limitado
Atualização	Permanente	Quando perto do leitor
Memória	Acima de 128KB	128 bytes
Segurança	Sofisticada	Básica
Monitorização de área	Sim	Não
Aplicações comuns	Processos comerciais dinâmicos, segurança e sensibilidade, armazenamento de dados (<i>logging</i>)	Processos comerciais fixos, segurança reduzida, fraca capacidade de armazenamento de dados

Tabela 2 - Comparação entre etiquetas ativas e passivas [5].

2.4.4. Etiquetas Semi-passivas

As etiquetas semi-passivas são um híbrido da tecnologia dos dois tipos de etiqueta anteriores, com a vantagem de serem bastante menos dispendiosas que as etiquetas ativas [11]. Apesar de possuírem bateria não estão permanentemente ativas e precisam de receber um sinal elétrico de uma antena para que possam estabelecer uma comunicação [5] [8] [11]. Este tipo de etiqueta não possui um modulador de rádio frequência. A sua alimentação interna apenas alimenta os circuitos internos, não gerando o sinal RF para o leitor [12], isto é, não usa a sua energia interna para reenviar o sinal RF [5] [8].

2.5. Exemplos de Aplicação da Tecnologia RFID

A tecnologia RFID já está no nosso dia-a-dia e muitos utilizadores desta tecnologia nem sabem que na realidade a estão a usar. Desta forma, será interessante ver algumas das suas aplicações.

2.5.1. Área da Saúde

Investigadores da área da saúde sugerem que um dia um pequeno CI RFID, implantado debaixo da pele, poderá transmitir um número de identificação de um

determinado utente e automaticamente aceder ao registo completo da saúde do mesmo. Funcionários de um hospital, remédios e equipamentos também podem ser etiquetados, criando um potencial de administração automática, reduzindo erros e aumentando a segurança. Uma outra interação com a área médica pode ser no uso de lentes especiais com um *transponder* implantado no olho de um paciente com glaucoma.

Muitos hospitais começaram a adotar sistemas RFID ativos com o objetivo de localizar peças de equipamento quando o pessoal médico necessita delas. Esta capacidade de seguir objetos serve dois propósitos. Primeiro, o pessoal médico, especialmente enfermeiros, poderá gastar menos tempo a procurar o equipamento de que precisa, o que faz com que dediquem proporcionalmente mais atenção direta aos pacientes. Em segundo lugar, os hospitais podem utilizar de forma mais eficiente os equipamentos que têm, gerando menos despesas relativas ao aluguer e aquisição de equipamentos adicionais.

Este tipo de sistemas RFID tem sido chamado de "sistemas de localização interna". Outros hospitais começaram a adotar dispositivos de RFID ativos para identificar e localizar os pacientes e os membros da equipa médica. Por exemplo, dispositivos RFID foram incorporados em pulseiras de identificação de pacientes para que o pessoal médico possa identificá-los eletronicamente antes das cirurgias, transfusões sanguíneas e administração de medicamentos. Além disso, estes sistemas foram implementados com o objetivo de localizar e acompanhar o movimento e fluxo de pacientes e de materiais no hospital. Da mesma forma, os médicos podem usar etiquetas RFID ativas, incorporadas em crachás, para recolher dados de assiduidade e encontrar ineficiências nas operações hospitalares. Este tipo de sistema tem sido implementado principalmente em serviços de urgência e centros cirúrgicos, que são locais onde há grandes volumes de pacientes e riscos elevados de erro médico.



Figura 7 - Chip RFID para implante em pessoas [2].

O implante de *chips* RFID, já aplicados em animais, está atualmente a ser utilizada em humanos. Uma experiência feita com implantes RFID foi liderada pelo professor britânico de cibernética Kevin Warwick [12] [14] que implantou um chip no seu próprio braço em 1998. A empresa *Applied Digital Solutions* propôs *chips* de "formato único para debaixo da pele" como uma solução para identificar fraudes, aumentar a segurança no acesso a determinados locais, computadores, bases de dados de medicamentos, iniciativas anti-sequestro, entre outros.

Numa outra área, o *Baja Beach Club*, uma casa noturna em Barcelona e em Roterdão usa *chips* implantados em alguns dos seus frequentadores para os identificar como *VIPs*.

Em 2004, um escritório de uma firma mexicana implantou dezoito *chips* em alguns dos seus funcionários, com o objetivo de controlar o acesso dos mesmos à sala da base de dados.

Recentemente, a *Applied Digital Solutions* anunciou o *VeriPay*, um *chip* com o mesmo propósito do *Speedpass*, com a diferença de que este é implantado sob a pele. Nesse caso, quando alguém for a uma caixa eletrónica, bastará fornecer o código pessoal e um *scanner* irá varrer o corpo do cliente de modo a captar os sinais de RD (*Rede Digital*), os quais transmitem os dados do cartão de crédito desse mesmo cliente [15].

No entanto, especialistas em segurança estão alertar contra o uso de RFID para autenticação de pessoas devido ao risco de roubo de identidade. Seria possível, por exemplo, alguém roubar a identidade de uma pessoa em tempo real. Devido a alto custo, é praticamente impossível encontrar mecanismos de proteção contra esses ataques, pois seriam necessários protocolos muito complexos para saber a distância a que se encontra o Circuito Integrado (CI).

2.5.2. Área das Bibliotecas

Nas bibliotecas e centros de informação, a tecnologia RFID é utilizada para a identificação do fundo documental, possibilitando a leitura e o acompanhamento dos exemplares físicos das obras. O sistema funciona através da fixação nesses exemplares de uma etiqueta RFID plana (de 1 a 2 mm), adesiva, de dimensões reduzidas

(50x50 mm em média), contendo no centro um *micro-chip* e ao redor deste uma antena metálica em espiral. Inclui, também um conjunto com sensores especiais e dispositivos fixos (portais), de mesa ou portáteis (manuais). Estes possibilitam a codificação e leitura dos dados dos exemplares na mesma, principalmente o código identificador dos exemplares, anteriormente registado em códigos de barras.

A etiqueta é inserida normalmente na contracapa dos livros, perto da lombada, dentro das revistas e sobre os materiais multimédia (como CDs ou DVDs), de modo a ser lida à distância. É possível converter facilmente os códigos identificadores atuais, sob a forma de código de barras, para etiquetas RFID, através de equipamentos próprios para esta conversão.

Algumas aplicações em bibliotecas:

- Auto atendimento;
- Controle de acesso de funcionários e utilizadores;
- Devolução;
- Empréstimo;
- Estatística de consulta local;
- Leitura de estante para inventário do fundo documental;
- Localização de exemplares indevidamente ordenados no fundo documental;
- Localização de exemplares noutras bibliotecas da rede;
- Re-catalogação.

É ainda possível utilizar as etiquetas RFID para evitar o furto de exemplares do fundo documental. Algumas etiquetas permitem gravar num bit de segurança informação sobre o facto de um determinado exemplar estar ou não emprestado. O metal pode bloquear os sinais de rádio, impossibilitando a leitura da etiqueta. Ao contrário do sistema tradicional de segurança eletromagnético (vulgo EM), adotado em bibliotecas, que é facilmente anulado com um magneto e exige apenas um par de hastes EAS (sistema de vigilância eletrónica de artigos) [16] [17], um sistema de deteção de furto baseado em etiquetas RFID apenas necessita de uma haste (na sua configuração mais simples).

2.5.3. Área da Segurança

Além do controlo de acessos, um sistema RFID poderá fornecer à área da segurança outros serviços. Um exemplo são os sistemas de imobilização. No início dos anos 90 o roubo de carros disparou, tornando o mercado de segurança para carros, alarmes e sistemas de imobilização, um mercado promissor. Os controlos de alarme com alcance de 5 a 20 metros estão no mercado há anos, e são pequenos transmissores de rádio frequência que operam na frequência de 433.92 MHz. Neste tipo de sistema de segurança para carros, é somente este controlo que poderá acionar o desbloqueamento do carro, permitindo que ele seja aberto sem que o alarme dispare e as portas sejam destrancadas. Permitir que o carro possa ser ligado é trabalho do sistema de imobilização. O problema é que, se o controle que o desbloqueia sofrer uma avaria, o carro poderá ser aberto através das chaves, por um processo mecânico. Contudo, não há forma de o sistema detetar se a chave inserida é genuína, se é uma ferramenta específica para assalto de carros, ou se é uma chave-mestra. A tecnologia dos *transponders* RFID pode intervir justamente neste ponto, verificando a autenticidade da chave. Assim, o sistema antigo trata da parte do alarme e desbloqueamento, e a etiqueta RFID trata da imobilização. Se uma chave não original tentar ligar o carro, ele será imobilizado, mesmo que o alarme tenha sido desligado e as portas abertas. Mobilização Eletrónica é o nome dado a este sistema, onde o sistema de ignição é combinado com um *transponder*, incorporado diretamente no topo da chave.

Os dispositivos de RFID são ainda utilizados no controlo de acesso a centros comerciais, condomínios residenciais, zonas comerciais e empresariais, bem como para controlar a passagem de peões nas estradas, facilitando o fluxo dos veículos.

2.5.4. Área da Identificação Animal

Os sistemas usados na identificação de animais facilitam a gestão da sua transferência entre empresas, permitem controlar epidemias, funcionam como garantia de qualidade e procedência. A identificação de animais por sistemas RFID pode ser feita de quatro maneiras diferentes: através de colares, brincos, injetáveis ou digeríveis *bolus*. Os colares são fáceis de aplicar e de transferir de um animal para o outro, sendo usados, geralmente apenas dentro da mesma empresa. Os brincos são as etiquetas de menor custo e podem ser lidas a uma distância inferior a um metro. As etiquetas injetáveis, que são usadas há cerca de 10 anos, são colocadas sob a pele do animal com

uma ferramenta especial, um aplicador parecido com uma seringa. A etiqueta digerível, ou bolus (*microchip* implantável) tem a forma de um comprimido de grandes dimensões, é revestido geralmente por um material cerâmico resistente a ácido e possui uma forma cilíndrica, podendo permanecer no estômago do animal durante toda a vida. O acompanhamento de animais será exigido cada vez em mais situações, nomeadamente, no que respeita à entrada da sua carne em mercados que exijam garantias da origem de proveniência dos alimentos vendidos. Já há vários problemas para a exportação de carne para países europeus, devido à não utilização de tecnologia que permite acompanhar os animais desde o nascimento até ao abate.

Capítulo 3 Análise e Modelação de Requisitos

Este capítulo começa por efetuar o levantamento das necessidades, relacionadas com a monitorização da localização de pessoas e bens, em 3 tipos de empresas/organizações usadas como referência: hospitais e maternidades, bibliotecas e armazéns. Este levantamento teve por base os inquéritos efetuados nas empresas/organizações. Com base nos resultados dos inquéritos efetuados são identificadas as especificidades dum sistema de localização para cada um dos 3 tipos de empresa/organização. Na fase seguinte são apresentados os requisitos funcionais e não funcionais que resultaram da fase de levantamento. Para concluir apresenta-se uma primeira visão dos utilizadores do sistema de localização.

Para atingir os objetivos deste capítulo é necessário efetuar as seguintes tarefas:

- Identificar as pessoas que vão ajudar a especificar os requisitos (*stakeholders*) [18].
- Identificar o equipamento necessário ao sistema de localização.
- Efetuar o levantamento de requisitos.
- Documentar os requisitos funcionais e não funcionais.
- Definir os utilizadores do sistema.

3.1. Levantamento de Necessidades

Atualmente existe uma necessidade e interesse crescentes por parte dos principais responsáveis das empresas em saber com exatidão a localização dos seus bens/produtos e funcionários, bem como, obter informações acerca de tudo o que se passa no interior de um ou vários edifícios da mesma (como armazém, escritórios, etc.). Estas questões poderão ter resposta através do desenvolvimento de uma metodologia capaz de apresentar uma solução única face às solicitações de vários tipos de empresas (como por exemplo, bibliotecas, armazéns e lares/hospitais) [19] [20].

O processo de desenvolvimento de um *software* é um ato complexo envolvendo, as múltiplas variáveis, sendo inúmeras vezes efetuado com abordagens que conduzem a soluções de baixa qualidade ultrapassado os prazos e os orçamentos previstos. Cada processo deverá ser adaptado e configurado conforme o perfil das empresas envolvidas.

Neste trabalho recorrer-se-á à utilização de UML, para desenhar os diagramas de contexto do sistema, o que permitirá uma melhor explicação dos seus atores.

Ao desenvolver um sistema para a solução parametrizável, é capaz de resolver qualquer tipo de problema que este consiga identificar os diferentes tipos de objetos, bem como os funcionários que entram e saem do edifício da empresa. Para tal, cada funcionário deverá registar a respetiva data e hora de entrada/saída, num sistema de controlo de acessos.

Mais especificamente, no que refere a bens/produtos de uma empresa é possível, através de recetores, identificar e localizar os objetos. Cada objeto terá uma etiqueta afixada, permitindo ao recetor identificar a sua localização e o código associado a esse objeto. Esta funcionalidade é particularmente útil no caso dos armazéns, em que o funcionário poderá ter que entregar um determinado objeto a um cliente ou instituição (Cliente, Revendedor, Fornecedor, etc.). Durante esse processo, o utilizador do sistema deverá identificar o código do objeto, através de um leitor de código de barras, associando-o ao seu código do funcionário. Após o pedido ser processado pelo sistema, o objeto estará autorizado sair da zona não permitida, ou seja, da zona restritiva.

Relativamente à entrada de objetos na empresa, o funcionário deverá registar a referência dos objetos em questão através do dispositivo (RFID), deverá imprimir etiqueta com o código que identifica o objeto e afixá-la na no seu exterior. No caso de conflitos de objetos iguais, a etiqueta poderá resolver o problema, criando um número de etiqueta ao qual é associado o número de código de objeto. Desse modo, cada novo objeto registado fica associado ao número do funcionário que é responsável pelo processamento da base de dados.

Um utilizador do sistema poderá localizar os vários objetos existentes numa ou em várias zonas, contudo a determinação da localização do objeto poderá ser feita por vários recetores. Assim, poderão levantar-se alguns problemas na deteção de objetos e/ou de pessoas (como por exemplo doentes, médicos, enfermeiros, etc.), por haver múltiplos recetores a localizar o mesmo objeto podendo ocorrer situações em que o objeto não seja detetado como sendo o mesmo.

No processo de desenvolvimento do sistema em questão, é necessário implementar a possibilidade de configurar os recetores, uma vez que existem os dispositivos RFID bastante distintos. Assim, na configuração do dispositivo deverá ser possível escolher os fabricantes compatíveis e introduzir valores desejados nos parâmetros de configuração (como por exemplo, ligação *Transmission Control Protocol* - TCP/IP -, via porta série ou USB).

Os produtos existentes em armazém, deverão ser organizados/agrupados de acordo com a respetiva categoria, de modo a não confundir a zona da sua localização, usando uma etiqueta mais estrutura que terá três partes diferentes: a classe do objeto (Pessoa/Produto/Animal), o ID do Tipo de Objeto (por exemplo, Mala/Embalagem/Caixas) e o ID do Objeto (código utilizado para distinguir os objetos com as mesmas características (por exemplo, disco rígido), ou seja, o código de barras. No caso de produtos que tenham o mesmo fabricante e o mesmo modelo, o número de referência do produto poderá ser o mesmo ou não, mas o número das etiquetas deverá ser necessariamente diferente. Como tal, não se deve duplicar o mesmo número de etiqueta nos vários produtos iguais, mas antes usar números de etiqueta.

Para efetuar o levantamento de requisitos prepararam-se inquéritos que foram entregues a várias pessoas das instituições em estudo. O objetivo destes inquéritos era recolher dados relevantes para a implementação do referido sistema e apresentou os resultados descritos nas próximas 3 secções [12] [21].

3.1.1. Resultados dos Inquéritos a Hospitais e Maternidades

- 1- Os alvos dos inquéritos foram hospitais com Maternidade que já possuíam o respetivo sistema de monitorização nas unidades de Psiquiatria e Maternidade, com um valor aproximado de 25000 doentes por ano, 1200 visitantes por dia, 1800 funcionários permanentes e 20 temporários.
- 2- Foram inquiridos 1 enfermeiro, 1 médico e 1 gestor, com idades compreendidas entre os 50 e os 58 anos de idade.
- 3- Todos eles consideraram o sistema eficaz e suportável em termos financeiros.
- 4- A importância da monitorização foi direcionada maioritariamente para os doentes e segurança, tendo achado em dois casos ser, também, a monitorização dos visitantes e vendedores e 1 dos inquiridos incluiu, ainda, os trabalhadores temporários.
- 5- Relativamente ao tipo de alerta desejado quando ocorrer uma situação anómala, 2 dos inquiridos preferem o toque de uma sirene. Enquanto outro achou mais adequado ativar uma central de vigilância.
- 6- Em relação à forma de alertar os funcionários, os 3 inquiridos preferem o alarme através de um BIP, enviado pela central de vigilância.

- 7- Todos os inquiridos acharam importante monitorizar as entradas, saídas, bem como, o movimento na Maternidade e Psiquiatria.
- 8- Foi distribuído 1 inquérito num hospital com Maternidade onde o referido sistema ainda não está implementado, com um número anual aproximado de 25000 doentes, 2791 partos, 1200 visitantes, 1900 funcionários e 50 trabalhadores temporários.
- 9- Foi inquirida 1 enfermeira, de 25 anos de idade.
- 10- A inquirida desconhece se já foram tomadas medidas para a implementação do referido sistema, embora ache a sua adoção muito pertinente.
- 11- Em termos financeiros acha-o suportável.
- 12- Considerou mais importante monitorizar os doentes e visitantes.
- 13- Achou o toque da sirene mais adequado em caso de situação anómala.
- 14- Em relação à forma de alerta dos funcionários, preferiu o aviso sonoro no local do funcionário.
- 15- Relativamente às áreas monitorizadas, apontou a entrada e saída da Maternidade e a Psiquiatria.

3.1.2. Resultados dos Inquéritos a Bibliotecas

- 16- Os alvos do inquérito foram as Bibliotecas da Universidade do Minho e de uma Escola Superior de Enfermagem, que não dispõem do respetivo sistema.
- 17- Foram inquiridos 2 funcionários, com idades compreendidas entre os 30 e os 46 anos de idade.
- 18- Segundo os inquiridos, são bibliotecas muito frequentadas por alunos e professores, estimando-se um valor de 200 utentes diários, bem como, um valor aproximado de 9300 documentos e 6 funcionários. Dispõem de livros na área da saúde, investigação, educação, gestão e psicologia.
- 19- No que respeita a situações anómalas registadas no local de trabalho, 2 dos inquiridos apontam a danificação dos livros como a mais frequente. As outras anomalias mais registadas são a perda de registos, bem como, ocorrem dois registos iguais.

- 20- Questionados sobre a pertinência da aquisição deste tipo de tecnologia, os 3 inquiridos responderam que sim, referindo que já ocorreram situações que poderiam ter sido evitadas se existisse o sistema de segurança.
- 21- Em termos financeiros consideraram-no muito dispendioso.
- 22- Relativamente ao fundo documental que importa monitorizar, foram referidos: livros, revistas e CDS.
- 23- Quanto ao tipo de alerta desejado em caso da existência de situações anómalas, 2 dos inquiridos manifestaram preferência pelo toque da sirene, tendo o outro apontando o registo num LOG.
- 24- Já na alternativa da forma de alerta aos funcionários houve unanimidade na preferência da mensagem e-mail tendo, um referido também o aviso sonoro no local do funcionário.
- 25- No que se refere a situações que importa monitorizar, foi referido que o furto é a principal, embora 2 dos inquiridos apontassem também a consulta de livros e o inventário.
- 26- Inquérito a uma Biblioteca da Universidade do Minho, que já dispõe do respetivo sistema de monitorização.

3.1.3. Resultados dos Inquéritos a Armazéns

- 27- Os destinatários do inquérito foram armazéns que não estão equipados com o referido sistema de segurança e cujos produtos existentes são: caixas, embalagens veículos e produtos informáticos.
- 28- Foram inquiridos 3 funcionários; um gerente, um diretor comercial e um diretor de logística, com idades compreendidas entre 30 e 56 anos de idade.
- 29- Segundo os inquiridos, dois destes armazéns apresentam um valor aproximado de 50 clientes diário e no do 3º armazém, um valor de 100 clientes.
- 30- Relativamente ao número aproximado de bens em armazém, apenas um dos inquiridos referiu 2000. Os outros não responderam.
- 31- Todos os inquiridos referiram já terem sentido necessidade de melhorar as operações do seu armazém.
- 32- Sobre a forma de melhorar as mesmas operações, um dos inquiridos nomeou o rastreio de ativos ou a localização de equipamentos de alto valor, a melhora do

prazo de entrega e a redução de gastos. Um segundo inquirido achou importante a informação em tempo real da situação das vendas, permitindo-lhe melhorar as reposições. Enquanto o terceiro inquirido, considerou importante as soluções logísticas que permitam acelerar o ritmo dos seus inventários e manter os produtos em constante movimento até eles chegarem às mãos dos consumidores.

- 33- Dois inquiridos foram unânimes ao responder que já ocorreram situações que poderiam ter sido evitadas se existisse um sistema eficaz de segurança, enquanto outro, não indicou ocorrências desse tipo.
- 34- A resposta dos 3 inquiridos sobre o facto de já terem sido tomadas medidas para a implementação do referido sistema foi negativa, embora todos o achem suportável em termos financeiros.
- 35- Ao nível do que consideram mais importante monitorizar, a preferência dos 3 inquiridos foi para os bens, incluindo também os clientes e funcionários num dos casos.
- 36- Do ponto de vista da monitorização de situações anómalas, 2 dos inquiridos optaram pelo registo num LOG como sinal de alerta, enquanto o outro inquirido manifestou preferência pelo toque de sirene.
- 37- Ainda a nível de monitorização, mas no que concerne à forma de alerta dos funcionários, as mensagens SMS para telemóvel e o e-mail, foram as preferidas. Enquanto o aviso sonoro no local do funcionário mereceu a preferência de um dos inquiridos.
- 38- No que respeita ao tipo de situações que importa monitorizar, a entrada e saída do edifício foi a mais preferida. O movimento das pessoas foi apontado por um dos inquiridos.

3.1.4. Especificidades de um Sistema de Localização para Hospitais/Lares

No caso de o sistema ser utilizado num “Hospital/Lar”, o objetivo do mesmo será localizar os doentes, médicos, enfermeiros, pessoal de apoio, visitantes e qualquer outro tipo de funcionário. A cada tipo de pessoa pertencerá uma etiqueta.

No entanto, levantam-se alguns problemas em relação aos visitantes. Neste caso, podem definir-se vários cenários.

Num **primeiro cenário**, o funcionário do Hospital/Lar terá que pedir o número do bilhete de identidade ou do cartão de cidadão da pessoa que visita essa instituição. Posteriormente, esse dado será introduzido no sistema, sendo criado um registo, no qual ficarão guardadas, também, informações relativas à hora de entrada do visitante no Hospital/Lar e à etiqueta que lhe será entregue/atribuída. De seguida, a etiqueta é entregue ao visitante, que antes de sair do Hospital/Lar, a deverá devolver ao funcionário.

Num **segundo cenário**, quando uma pessoa visita o Hospital/Lar, o funcionário terá que pedir e introduzir no sistema o número do bilhete de identidade ou do cartão de cidadão do visitante e imprimir a etiqueta, não sendo necessário devolvê-la quando sair do hospital.

Num **terceiro cenário**, quando uma pessoa visita o Hospital/Lar, o funcionário lê de forma automática o número do cartão de cidadão do visitante, através dum dispositivo de leitura de códigos de barras. Posteriormente, poderá escolher entre duas opções: introduzir o número de etiqueta (Cenário 1) ou imprimir a etiqueta (Cenário 2).

Um sistema de localização para um Hospital deve conseguir determinar com rapidez e fiabilidade a localização de um paciente, assim como, evitar o acesso a determinadas áreas restritas.

Hospitais e Serviços Médicos de Emergência, estão constantemente a enfrentar desafios quotidianos, especialmente nas respostas em emergência. Eles precisam ser capazes de gerir um grande número de doentes em situação de emergência de forma eficaz e eficiente. A instituição, é responsável pelos cuidados e segurança dos doentes a seu cargo. Se algum destes pacientes “desaparecer”, será sem dúvida, uma má imagem, sem falar das consequências ao nível da justiça e obviamente financeiras.

A Maternidade é um lugar de alegria e festa. Toda a família e amigos querem partilhar o momento de felicidade e dar as boas vindas ao(s) recém-nascido(s). Contudo, se as visitas não forem cuidadosamente programadas, ou seja, caso não ocorra a gestão de visitas por recém-nascido, poderá gerar-se alguma confusão. Além disso, eventuais complicações ao nível do parto ou pós parto podem levar a uma separação entre o recém-nascido e a mãe. Nestes casos, a confusão gerada pelo *stress* e outros eventuais problemas, poderão levar a inevitáveis trocas de bebés. Com as nossas soluções, ajudaremos a resolver estas duas situações críticas.

A monitorização através das Pulseiras RFID não só garante segurança, como aumenta a facilidade de identificar e verificar cada paciente de forma segura e eficaz em Tempo Real. Especificando:

- As Pulseiras RFID podem ser usadas pelos pacientes. Uma pulseira RFID pode ser lida através de leitores RFID sem fios, de modo que os doentes não sejam incomodados enquanto dormem.
- Os doentes podem ser geo-referenciados usando pulseiras RFID, com recurso a Leitores fixos em determinadas portas e corredores, para garantir que os pacientes não se dispersam para além de um determinado perímetro.
- As Pulseiras RFID podem conter todas as informações do paciente, sendo que a informação global reside num computador central [22].



Figura 8 - Cartão Active Tag [22].

A todas as visitas é dado um cartão TAG de visita (o visitante não sabe que é um dispositivo de segurança) e a partir desse momento, a pessoa é “seguida” em Tempo Real. Caso não se dirija para o seu local de destino, pode gerar-se um alarme ou envio de SMS para segurança.

O cartão ACTIVE TAG, é ideal para gestão de visitas e pacientes. Na realidade, o visitante desconhece que através deste cartão, poderá ser monitorizado em tempo real no interior das instalações hospital. Poderão ser criados diferentes perímetros consoante as autorizações para cada cartão, evitando assim, que as visitas andem em locais não autorizados.



Figura 9 - Pulseira RFID [22].

Entre outras soluções, existe também uma pulseira de última geração com tecnologia ativa. Duas vantagens desta pulseira são:

1. Em caso quebra ou abertura sem permissão, é imediatamente enviado um sinal de alerta.
2. Inclui um botão de pânico. Caso o paciente precise de cuidados urgentes, basta pressionar o botão, para que seja emitido um sinal de alerta.



Figura 10 - Pulseira RFID [22]

3.1.5. Especificidades de um Sistema de Localização para Armazéns

No contexto de um armazém, poderão surgir outros problemas especificamente relacionados com o **movimento de produtos/pessoas no armazém**:

- É possível que se verifiquem alguns problemas em localizar o(s) produto(s);
- Quando um funcionário ou cliente (ao qual corresponde uma etiqueta de identificação) pegar num produto (com uma etiqueta de identificação), o sistema deverá identificar quem é o funcionário ou cliente, bem como, qual o produto em questão;
- O sistema deverá permitir localizar os funcionários da empresa;
- O sistema deverá possibilitar a identificação de eventuais mudanças na localização dos objetos;
- Na empresa poderão existir zonas mistas, como é o caso das farmácias, em que há uma zona com produtos em que os clientes podem pegar e outra zona à qual os clientes não têm acesso. Deste modo, é necessário criar níveis de segurança diferentes em função do produto em questão e da sua localização.

3.1.6. Especificidades dum Sistema de Localização para Bibliotecas

Caso o contexto seja uma biblioteca as necessidades estão relacionados com o **movimento de objetos** (livros/revistas/CDs/DVDs):

- O funcionário consulta o sistema que lhe indica onde estão o(s) livro(s);
- O funcionário identifica as mudanças dos livros.

3.2. Requisitos do Sistema

Uma das tarefas mais importantes para obter uma solução correta para um determinado problema proposto, no nosso caso um problema de engenharia de *software*, é compreendê-lo. Esta tarefa primordial pode ser concretizada através do levantamento e documentação dos requisitos para a solução desse problema. Como tal, nesta secção serão elencados e documentados os requisitos funcionais e não funcionais do problema em estudo.

Para especificar os requisitos funcionais será utilizado o modelo descrito em “*Volere-Requirements Specification Template* [23], que é sintetizado na Figura 11.

List of events /
use cases that
need this
requirement

Requirement #: Unique id	Event/use case #'s:
Description: A one sentence statement of the intention of the requirement	
Rationale: A justification of the requirement	
Originator: The person who raised this requirement	
Fit Criterion: A measurement of the requirement such that it is possible to test if the solution matches the original requirement	
Priority: A rating of the customer value	

Degree of stakeholder happiness if this requirement is successfully implemented.
Scale from 1 = uninterested to 5 = extremely pleased.

Volere
Copyright © Atlantic Systems Guild

Figura 11 – Modelo para a especificação de requisitos [23].

Requisito: 1

Descrição: Gerir a comunicação entre os Pontos de Acesso (APs) e o sistema central.

Casos de uso: “Receber pacote de AP por TCPIP”, “Configurar AP” e “Enviar comando ao AP para ler a configuração”.

Racional: O sistema deve ser capaz de gerir a comunicação bidirecional entre o sistema central e os APs. A comunicação pode ser (i) recepção de pacotes provenientes dum AP contendo dados do próprio AP, (ii) recepção de pacotes originados por etiquetas RFID mas reencaminhados por um AP, (iii) envio de comandos para um AP de forma a configurar esse AP ou para ler a sua configuração atual. A recepção de pacotes com origem nas etiquetas RFID permitirá monitorizar a localização dos utilizadores das etiquetas (bens, pessoas ou animais).

Fit criterion: O sistema consegue receber, processar e armazenar corretamente pacotes enviados pelos APs. O sistema consegue enviar comandos que os APs interpretam de forma correta, e que permitem configurar os APs ou ler a sua configuração.

Prioridade: 5

Requisito: 2

Descrição: Configurar pontos de acesso (APs).

Casos de uso: “Criar dados do AP”, “Remover AP do sistema”, “Alterar dados do AP” e “Listar descrição do AP”.

Racional: Para localizar as etiquetas RFID é necessário configurar os pontos de acesso que recebem o sinal RF por elas emitido periodicamente. Para esse fim, o sistema deve dispor das funcionalidades de inserção, eliminação, alteração e listagem dos pontos de acesso que comunicam com o sistema central. Parte importante da inserção de um AP no sistema é a definição do tipo de comunicação entre esse AP e o sistema central.

Fit criterion: O sistema consegue criar, eliminar, alterar e listar corretamente os dados relativos a um ponto de acesso.

Prioridade: 5

Requisito: 3

Descrição: Formar e gerir conjuntos de pontos de acesso.

Casos de uso: “Criar conjunto de APs”, “Eliminar conjunto de APs”, “Adicionar AP a um conjunto de APs”, “Remover AP do conjunto de APs” e “Listar descrição do conjunto de APs”.

Racional: Para localizar etiquetas RFID de forma correta e em todos os cenários, aplicando um método de triangulação, é preciso dispor de pelo menos 3 estimativas da posição da etiqueta em cada momento. Para isso, introduziu-se o conceito de *conjunto de pontos de acesso*, que mais não é do que um conjunto de pontos de acesso, próximos em termos de localização, e que atuam em conjunto para localizar as etiquetas. Deste modo, o sistema deve dispor das funcionalidades de criação, eliminação, alteração e listagem dos conjuntos de pontos de acesso. A alteração de um conjunto consiste em adicionar ou remover um AP desse conjunto.

Fit criterion: O sistema consegue criar, eliminar, alterar e descrever a composição de cada conjunto de pontos de acesso, de forma correta.

Prioridade: 5

Requisito: 4

Descrição: Localizar utilizadores de etiqueta RFID.

Casos de uso: “Receber pacote de AP por TCPIP”, “Calcular localização duma TAG”, “Calcular zona da localização”.

Racional: Com base no sinal RF emitido por uma etiqueta RFID, e captado por um ou mais APs, o Sistema Central deve ser capaz de determinar a zona em que essa etiqueta se encontra. O sistema deve conseguir aproximar a localização dos vários utilizadores de etiquetas RFID e em modo *quase tempo real*. Para cumprir este requisito, o sistema deve conseguir (i) receber pacotes dos APs, contendo informação sobre as etiquetas RFID, (ii) obter uma estimativa da localização dessas etiquetas, com base na informação desses pacotes e num método de triangulação, e (iii) calcular a zona do edifício correspondente a essa localização, conhecida a geometria dos espaços do edifício.

Fit criterion: O Sistema consegue calcular com uma precisão aceitável e em modo quase de tempo real, a zona do edifício em que cada utilizador de etiqueta RFID se localiza.

Prioridade: 5**Requisito: 5**

Descrição: Emitir alertas nas situações em que um utilizador de etiqueta RFID entra numa zona que lhe é interdita.

Casos de uso: “Emitir sinal de alerta”.

Racional: Após determinar a zona em que uma etiqueta RFID se encontra, caso a zona seja interdita ao (tipo de) utilizador dessa etiqueta, o sistema deve enviar alertas, de um ou mais tipos, para os seguranças. Os tipos e a ordem de envio dos alertas devem ser configuráveis.

Fit criterion: Os alertas, pré-definidos para cada tipo de utilizador e de zona, são enviados para os seguranças quando um utilizador desse tipo se localizar numa zona definida como interdita.

Prioridade: 5

Requisito: 6

Descrição: Criar e gerir utilizadores do sistema, incluindo o administrador do sistema.

Casos de uso: “Registrar utilizador do sistema” e “Criar perfil de administrador do sistema”.

Racional: De forma a diferenciar o tipo de acesso às funcionalidades do sistema, por parte dos seus utilizadores, o sistema deve permitir criar, alterar e remover utilizadores com determinado perfil. O perfil de acesso menos restringido, administrador do sistema, será criado apenas pelo administrador da empresa. Um administrador do sistema poderá criar, alterar e remover utilizadores registados com qualquer outro tipo perfil mais limitado que o seu. A criação de um utilizador pressupõe a atribuição de um *login* e uma palavra-passe.

Fit criterion: O sistema permite criar, alterar e remover utilizadores. Apenas o administrador da empresa consegue criar utilizadores com perfil de administrador do sistema. Um administrador do sistema consegue criar, alterar e remover utilizadores com qualquer outro tipo perfil mais limitado que o seu.

Prioridade: 4

Requisito: 7

Descrição: Permitir a um utilizador autenticar-se perante o sistema e encerrar uma sessão de trabalho.

Casos de uso: “Login” e “Logout”.

Racional: O sistema deve permitir que um utilizador se autentique, sendo para isso necessário introduzir o nome de utilizador (*login*) e a palavra-passe atribuídos no acto de registo. Caso a autenticação decorra com sucesso, o sistema deverá então dar acesso às funcionalidades pré-definidas para o tipo de perfil correspondente a este utilizador. Uma funcionalidade que tem que estar presente em todos os perfis será a de encerrar uma sessão de trabalho (*logout*) no sistema. Após o fecho duma sessão de trabalho, o sistema desativa todas as funcionalidades exceto a de autenticação (*login*).

Fit criterion: Para cada tipo de perfil de utilizador definido, o sistema apenas dá acesso às funcionalidades correspondentes a esse perfil e apenas enquanto o utilizador estiver autenticado. Um utilizador não autenticado apenas tem acesso à funcionalidade de autenticação.

Prioridade: 4

Requisito: 8

Descrição: Definir as zonas do edifício.

Casos de uso: “Definir zonas” e “Definir segmentos.

Racional: Para dotar o sistema da capacidade de reconhecer em que local do edifício se encontram os utilizadores de etiquetas RFID, e poder assim emitir alertas no caso em que se verifique o acesso a zonas interditas, o sistema tem que conhecer a geometria dos espaços físicos (zonas) do edifício. Para isso, tem que ser possível definir o polígono que caracteriza a geometria de cada zona. Por sua vez, para definir as zonas é necessário especificar os segmentos (equivalentes a paredes físicas) do edifício. Por motivos de simplificação, estamos a assumir uma representação 2D de cada piso do edifício.

Fit criterion: O sistema permite editar, validar e guardar a geometria dos vários espaços/zonas do edifício, usando para isso a geometria dos segmentos/paredes do edifício.

Prioridade: 4

Requisito: 9

Descrição: Criar e gerir as listas de zonas do edifício permitidas e interditas a cada tipo de utilizador.

Casos de uso: “Inicializar a lista de acessos às zonas do edifício” e “Alterar a lista de acessos às zonas do edifício”.

Racional: Para cada zona do edifício deve ser possível especificar e alterar os tipos de utilizador que estão autorizados a entrar nessa zona, e por omissão especificar os tipos de utilizador proibidos de entrar nessa zona. Nos casos de interdição, dum dado tipo de utilizador a uma determinada zona, deve ainda ser possível escolher os tipos de alerta e emitir quando ocorrer uma violação dessa interdição. Os alertas serão preferencialmente enviados para alguém responsável pela segurança.

Fit criterion: Quando um dado tipo de utilizador é localizado numa dada zona, o sistema consegue determinar se deve emitir ou não sinais de alerta, o tipo dos alertas e a ordem de envio. O sistema consegue definir/alterar estes alertas, para cada tipo de utilizador e para cada zona.

Prioridade: 4

Requisito: 10

Descrição: Monitorizar a associação entre etiquetas RFID e utilizadores.

Casos de uso: “Atribuir etiqueta_RFID”, “Recolher etiqueta_RFID” e “Listar as etiquetas atribuídas aos utilizadores”.

Racional: O sistema deve permitir monitorizar que utilizador é portador de qual etiqueta RFID, em dado momento. Deste modo, a pessoa responsável pela gestão de etiquetas RFID deve ser capaz de (i) registar a entrega duma etiqueta a um utilizador, (ii) remover esse registo quando a etiqueta é devolvida e (iii) listar todas as etiquetas atribuídas em dado momento.

Fit criterion: O gestor de etiquetas RFID consegue registar, remover e mostrar a atribuição de etiquetas a utilizadores.

Prioridade: 5

Requisito: 11

Descrição: Efetuar operações sobre etiquetas RFID.

Casos de uso: “Enviar ordem para efetuar uma operação sobre a etiqueta”.

Racional: O sistema deve permitir ao responsável pela gestão de etiquetas RFID efetuar operações sobre essas etiquetas. Entre as operações a disponibilizar incluem-se: imprimir os dados da etiqueta em papel e programar uma etiqueta.

Fit criterion: O sistema consegue efetuar com sucesso a operação solicitada pelo gestor de etiquetas RFID, ou então informa-o do motivo do insucesso.

Prioridade: 3

3.2.1. Requisitos Não Funcionais

Os requisitos não funcionais identificados são os seguintes:

- 1) A interface com o utilizador deverá ser fácil de usar, intuitiva, não ter várias formas de fazer a mesma coisa, ergonómica e gráfica.
- 2) Na comunicação entre componentes do sistema serão utilizadas normas, nomeadamente *Ethernet* e TCP/IP, de forma a facilitar a gestão global do sistema e a tornar possível a utilização da estrutura da rede informática existente [24] [25].

- 3) O produto final deve ser robusto.
- 4) A utilização do sistema deve ser segura.
- 5) A manutenção/alteração do código deve ser simplificada e possível a pessoas diferentes das que desenvolveram o sistema.
- 6) As tecnologias a usar são Java, MySQL e UML.

3.3. Utilizadores de Sistema

Os tipos de utilizador inicialmente identificados são os seguintes:

Administrador da empresa: Tem acesso completo a todas as funções do sistema, mas também tem a tarefa especial de criar o perfil de administrador do sistema.

Administrador do sistema: Tem acesso completo a todas as funções do sistema, exceto criar perfis de administrador do sistema. O administrador do sistema é responsável por: (i) efetuar as operações de criação, eliminação e alteração (CRUD) de utilizadores do sistema, (ii) definir a geometria do edifício, utilizando para isso zonas, que por sua vez usam segmentos, (iii) efetuar operações sobre os recetores (APs), nomeadamente configuração, (iv) efetuar operações sobre os conjunto de APs, (v) gerir as lista de zonas permitidas e interditas a cada tipo de utilizador.

Gestor de etiquetas RFID: É o utilizador responsável por efetuar operações sobre as etiquetas RFID: entregar, recolher e programar etiquetas.

Capítulo 4 Conceção do Sistema

Para conceber o sistema vai ser necessário começar por obter um diagrama de contexto que permita de identificar os atores do sistema, bem como, as ações envolvidas nas interações entre sistema e atores. O próximo passo consiste em conceber o diagrama de casos de uso global do sistema de forma a identificar e descrever todos os cenários de interação entre sistema, sensores/atuadores e atores/sistemas externos. Cada caso de uso será posteriormente modelado com outros casos de uso, se a sua complexidade o justificar, ou então será descrito de forma textual com um cenário principal e possivelmente com vários cenários alternativos. Posteriormente, a estrutura do sistema será modelada através de diagramas de classe do UML. Finalmente, para verificar se a estrutura obtida implementa a funcionalidade descrita nos casos de uso, serão utilizados diagramas de sequência do UML, ao nível da implementação.

Para atingir os objetivos propostos é necessário efetuar as seguintes tarefas:

- Identificar os atores;
- Identificar as possíveis relações de herança entre atores;
- Identificar os casos de uso;
- Estabelecer as interligações entre casos de uso utilizando relações do tipo *extend*, *includes* e generalização/especialização;
- Descrever cada caso de uso com um subdiagrama de casos de uso ou com uma descrição textual;
- Modelar a estrutura do sistema com diagramas de classe;
- Desenhar o modelo de dados persistentes;
- Validar a estrutura obtida com os diagramas de classe, em relação à funcionalidade descrita nos casos de uso, através de diagramas de sequência.

4.1. Diagrama de Contexto do Sistema

Depois de obter os requisitos do sistema, a primeira tarefa da conceção consiste na modelação com os diagramas de Casos de Uso do UML. Para isso começa-se por identificar os atores do sistema, bem como, as funções de cada um [26].

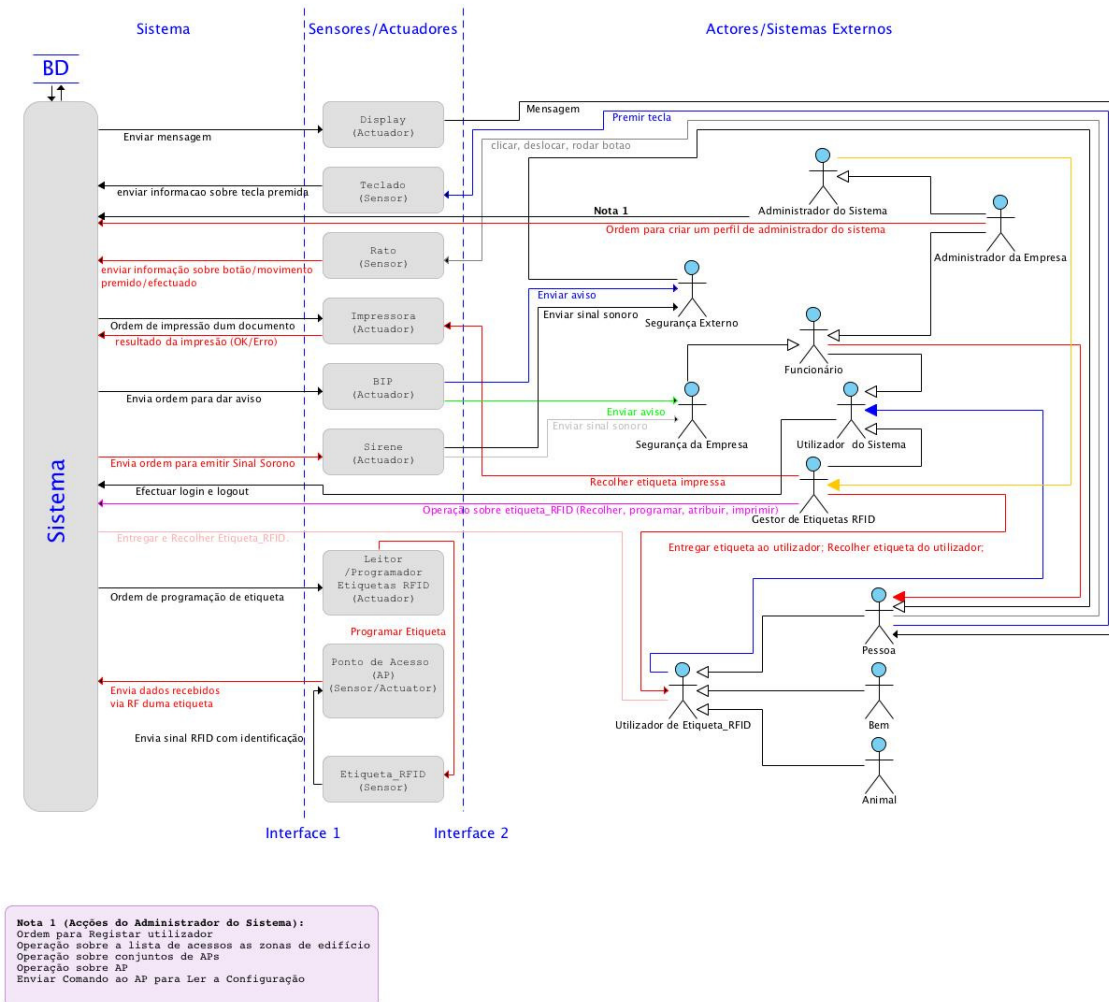


Figura 12 - Diagrama de contexto do sistema estruturado em 3 camadas.

O diagrama de contexto apresentado na Figura 12 mostra a visão global do sistema, estruturada em 3 camadas: (i) sistema, (ii) sensores/actuadores e (iii) actores/sistemas externos.

4.2. Princípio de Funcionamento do Método de Localização

Além da informação que consta no diagrama de contexto, um diagrama de casos de uso global do sistema procura adicionar mais informação resultante da fase de análise, ou seja, procura **identificar e descrever todos os cenários de interação** entre sistema, sensores/atuadores (como por exemplo *display*, ponto de acesso (AP), ou leitor de etiquetas RFID) e atores/sistemas externos (como por exemplo Segurança, Pessoa, Animal ou Bem). Numa perspetiva alargada, é necessário descrever todas as interações que ocorrem nas duas interfaces identificadas na Figura 12, mas em determinado projeto ou contexto podemos limitar-nos a modelar um subconjunto das interações relevantes nesse contexto. É o que faremos no presente trabalho, onde não nos iremos concentrar em modelar tudo, mas apenas o essencial de um sistema de deteção por RFID.

Tendo como objetivo monitorizar a entrada/saída em determinadas zonas de um edifício, é necessário instalar vários pontos de acesso que vão permitir localizar as etiquetas RFID transportadas pelos utilizadores. O **princípio de funcionamento da localização** terá por base o facto de haver uma correlação entre a distância, de um emissor de sinal RF a um dado AP, e a potência do sinal recebido nesse AP (RSSI) [27] [28]. O sistema central começa por receber os pacotes $P_{j,i}$ de cada AP_i e insere-os na estrutura de dados D1 (*Packet*). De seguida armazena esses dados de forma permanente numa base de dados e finalmente processa os dados de cada pacote $P_{j,i}$ para calcular a localização atual da etiqueta T_j que enviou o pacote. Para que a localização seja calculada com precisão exige-se medições da potência do sinal RF provenientes de pelo menos 3 APs. Com base na localização obtida, no tipo de utilizador da etiqueta detetada e no tipo de zona (permitida ou interdita) correspondente à localização, é possível emitir um alerta caso ocorra uma situação anómala.

A Figura 13 mostra-se um exemplo da arquitetura de um edifício e dos componentes físicos fundamentais do sistema de localização. O edifício é dividido em zonas (1 a 8 na Figura 13), às quais será atribuído um tipo de permissão de acesso para cada tipo de utilizador. Os componentes físicos fundamentais do sistema de localização serão (i) o sistema central, (ii) um conjunto de pontos de acesso (APs) colocados em zonas estratégicas para o processo de localização e (iii) as etiquetas RFID transportadas por cada utilizador. Convém referir que se decidiu que não se iria tentar localizar as etiquetas na totalidade do espaço do edifício, mas sim apenas nas áreas de acesso às

zonas críticas. Esta opção deve-se ao facto de ser complicado e dispendioso, sem obtenção de vantagens significativas, cobrir o espaço todo dum edifício.

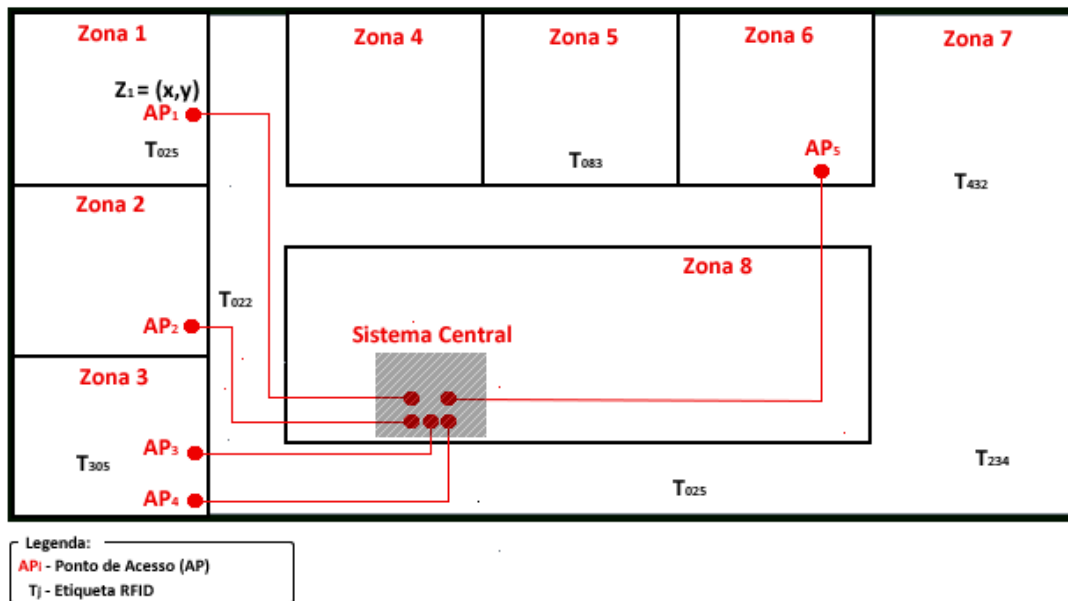


Figura 13 - Arquitetura física do edifício e do sistema de localização.

Para ajudar à explicação do processo de localização seguido, introduziu-se o conceito de **conjunto de APs**. Um conjunto de APs será composto normalmente por 3 APs, afixados de forma correta numa área crítica para a monitorização. Na prática, as áreas críticas coincidirão com portas de acesso às zonas a monitorizar (ver Figura 14). Cada conjunto de APs permitirá a localização de etiquetas RFID numa área crítica, aplicando o princípio de triangulação.

A distância entre um recetor e um emissor RF é estimada com base num modelo de propagação que descreve a relação entre a potência do sinal RF recebido e a distância [29]:

$$P = \frac{K}{D^2} \quad (\text{Equação 1})$$

onde P representa a potência do sinal recebido a uma distância D do emissor e K é uma constante que depende do meio de propagação.

Aplicar a Equação 1 (a qual corresponde à lei do *Inverso do Quadrado da Distância*), com valores RSSI é o ponto de partida de qualquer método de localização

baseado na potência do sinal RF. Contudo, como o RSSI fornece normalmente uma estimativa da atenuação do sinal em vez da potência do sinal, o modelo descrito na Equação 1 deve ser reescrito em termos das medições do RSSI:

$$RSSI_{dBm} = 10 * \log_{10}(K/D^2) \quad (\text{Equação 2})$$

onde $RSSI_{dBm}$ consiste na atenuação do sinal, em milidecibéis, de um sinal emitido com uma potência de 1mW.

No modelo de propagação de rádio que é usado em [29], a distância D é calculada pela Equação 3, obtida a partir da Equação 2 (a qual corresponde o *modelo de Propagação de Rádio em termos de Milidecibéis*).

$$D = \sqrt{K/10^{(RSSI_{dBm}/10)}} \quad (\text{Equação 3})$$

Em ambientes reais existem múltiplas interferências e múltiplos caminhos, os quais dificultam a correlação entre os parâmetros do sinal RF e a distância. Utilizando um método empírico é possível estimar o valor de K . Para isso, divide-se o espaço em pequenas áreas, mede-se o valor de RSSI para várias distâncias e aplica-se um Método dos Mínimos Quadrados para ajustar o parâmetro K . A distância d_{pi} entre cada uma destas áreas p e um recetor i é calculada com a Equação 4 (a qual corresponde à distância entre dois pontos num sistema cartesiano).

$$d_{pi} = \sqrt{(x_{mi} - x_p)^2 + (y_{mi} - y_p)^2} \quad (\text{Equação 4})$$

Onde:

- (x_{mi}, y_{mi}) define a posição conhecida (por medição) do recetor i ;
- (x_p, y_p) define o centro da área de p (onde se encontra o emissor RF).

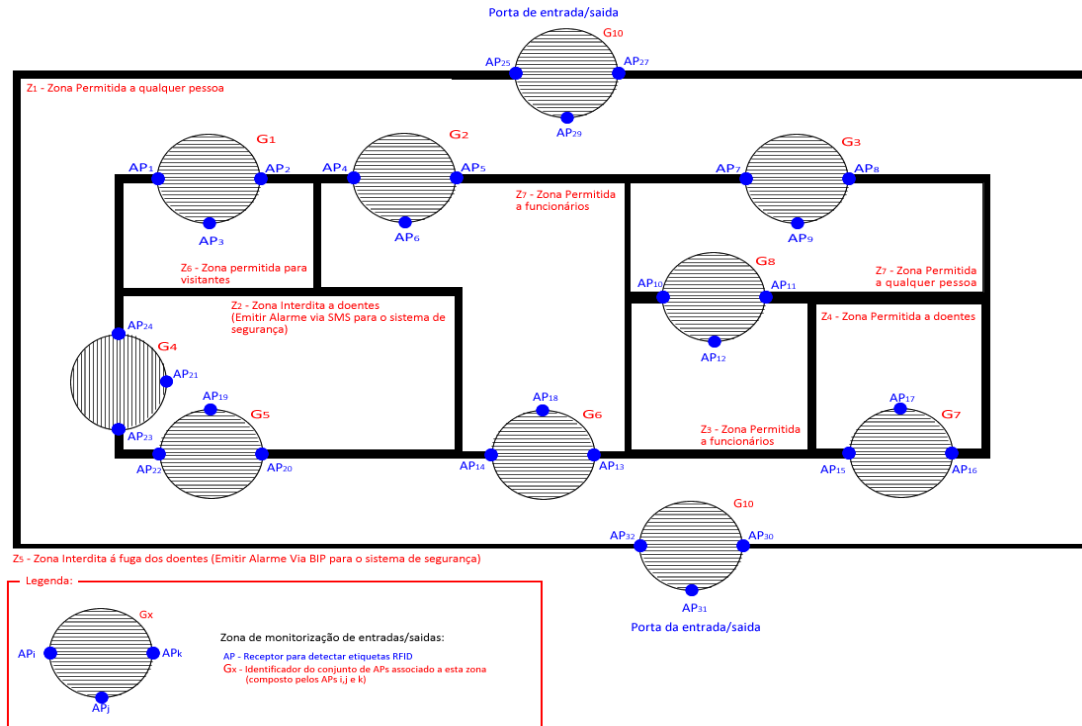


Figura 14 - Exemplo da planta de um piso de um edifício para ilustrar o princípio de funcionamento do método de localização.

Para calcular o valor de K pode aplicar-se o Método dos Mínimos Quadrados sobre as medições do RSSI. O ponto de partida deste método é fazer com que o erro entre as medições (y_i) e os valores calculados pela Equação 2 seja mínimo, ou seja, a derivada do erro deve ser nula:

$$\frac{\partial}{\partial K} \left\{ \sum_{i=1}^N \left[y_i - 10 * \log_{10} \left(\frac{K}{x_i^2} \right) \right]^2 \right\} = \quad (\text{Equação 5})$$

em que os valores de x_i ($1 \leq i \leq N$) são as várias distâncias para as quais se possui medição de RSSI (y_i) em dBm. Manipulando esta derivada chega-se à expressão de K que é apresentada na Equação 6.

$$K = 10^{\frac{\sum_{i=1}^N y_i + 10 * \sum_{i=1}^N \log_{10} x_i^2}{10 * N}} \quad (\text{Equação 6})$$

4.3. Estruturas de Dados de Apoio à Localização

Nesta secção apresentam-se as principais estruturas de dados que ajudaram a conceção dos casos de uso. Dada a complexidade de alguns casos de uso e do problema a modelar, foi necessário recorrer a estas estruturas de dados “conceptuais” para descrever corretamente alguns casos de uso.

- **D1 (*packet*) – Um pacote recebido**

A estrutura *packet* armazena os dados de um pacote recebido de um AP e inclui o identificador do pacote (PACK_ID), o identificador do AP que enviou o pacote (AP_ID), o identificador da etiqueta RFID que está na origem do pacote (TAG_ID), a potência do sinal RF recebido no AP (RSSI_RX), a data (DATE) e hora (TIME) da receção desse sinal RF no AP. Esta estrutura é preenchida com os dados provenientes do caso de uso “Receber pacote de AP por TCP/IP”.

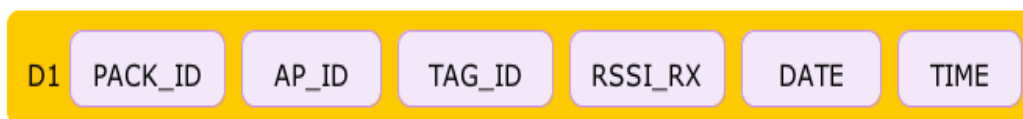


Figura 15 - Estrutura de dados *packet* que guarda um pacote recebido.

- **D2 (*APdata*) – Dados dum AP**

- **D6 (*listAPs*) – Lista com dados dos vários APs**

A estrutura *APdata* é uma espécie de configuração dos APs, pois para cada AP inclui o seu identificador (AP_ID), a localização (AP_X, AP_Y e AP_Z), a descrição (AP_DESCRIPTION), o conjunto de APs em que está inserido (AP_SET) e o endereço TCPIP atribuído ao AP (TCPIP). Em dado momento o AP_SET pode não estar definido. A estrutura *APdata* é preenchida com os dados referentes ao caso de uso “Operação sobre AP”.

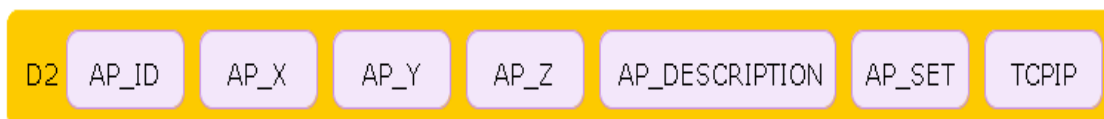


Figura 16 - Estrutura de dados *APdata* que guarda os dados dum AP.

A estrutura *listAPs* é simplesmente a lista com os dados de todos os APs, ou seja, é uma lista de elementos *APdata*. Esta tabela será eficientemente implementada com a classe *HashMap<AP_ID_x,APdata_x>*. Esta estrutura D2 é preenchida com os dados provenientes do caso de uso “Operação sobre AP”.

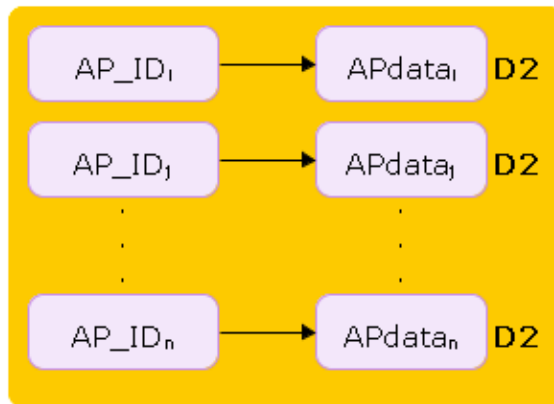


Figura 17 - Estrutura de dados *listAPs* que guardam os conjuntos de *APdata*.

- **D7 (*setAPs*) – Conjunto de APs**
- **D3 (*listSetAPs*) – Lista com os conjuntos de APs**

A estrutura *listSetAPs* guarda a composição dos vários conjuntos de APs (*setAPs*) a colocar em cada ponto estratégico do edifício. Em princípio cada conjunto terá uma cardinalidade de 3 APs, de forma a permitir efetuar a localização de etiquetas RFID por um método de triangulação. Para cada conjunto, identificado pelo seu identificador (*SET_ID*), a tabela guarda a lista com a identificação dos vários APs desse conjunto (*AP_ID_i*, *AP_ID_j*, *AP_ID_k*). As estruturas *setAPs* e *listSetAPs* são preenchidas com os dados provenientes do caso de uso “Operação sobre Conjuntos de APs”.

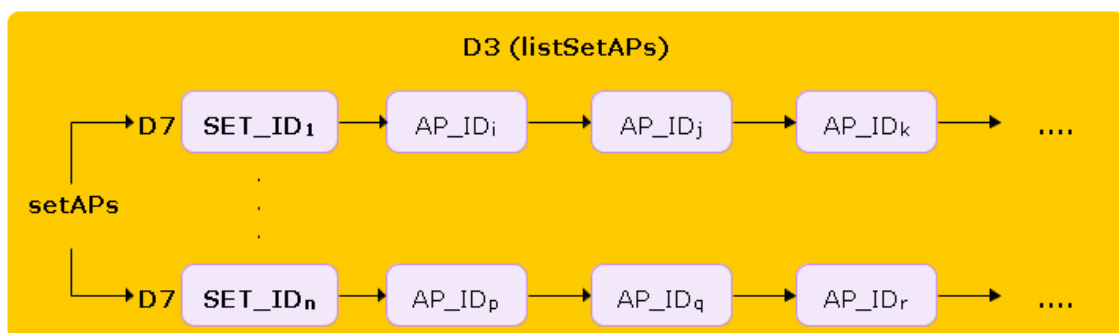


Figura 18 - Estruturas de dados *setAPs* e *listSetAPs* que guardam os conjuntos de APs.

- **D4 (*EtiquetaRFID*) – Dados duma etiqueta RFID**
- **D4L (*listaEtiquetaRFID*) – Lista com os dados das várias etiquetas RFID**

A estrutura *listaEtiquetaRFID* é simplesmente a lista com todas as etiquetas RFID (*EtiquetaRFID*). Esta tabela será eficientemente implementada com a classe *List<EtiquetaRFID>*, onde cada classe *EtiquetaRFID* inclui o identificador da etiqueta RFID (*ID_TAG*), a indicação se está ativa ou não (*Activa*) e uma referência que pode ser usada para descrever o tipo de etiqueta (*Referencia*).

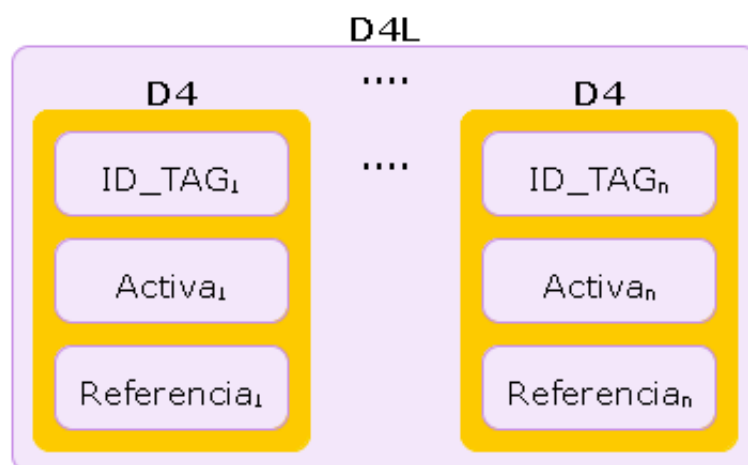


Figura 19 - Estruturas de dados *EtiquetaRFID* e *listaEtiquetaRFID* que guardam os dados das etiquetas RFID.

- **D5 (*PacksLastPosTAG*) – Lista de pacotes relativos à última posição de cada TAG**

Para cada etiqueta RFID *t*, a estrutura *PacksLastPosTAG* permite guardar os pacotes mais recentes relativos à localização dessa etiqueta *t* e que foram recebidos por APs pertencentes ao mesmo conjunto de APs. Quando a deteção de uma etiqueta muda de um conjunto para outro, a lista de pacotes mais recentes é limpa.

Para estimar a localização duma etiqueta, num dado instante *T*, com base em pacotes relativos a um dado conjunto de APs, os 3 pacotes a usar são os que apresentem um tempo de chegada mais próximo de *T*. Os 3 pacotes têm que se enquadrar ainda num intervalo $[-\delta T, +\delta T]$ em relação ao tempo *T* (ver o Anexo IV), em que δT pode ser da ordem de 2 segundos. Um pacote usado permanece na lista *PacksLastPosTAG* enquanto não surgir um mais recente que ele,

proveniente do mesmo AP. Com esta abordagem tenta-se minimizar os problemas causados pela receção assíncrona de pacotes nos vários APs. Esta estrutura é preenchida com os dados provenientes do caso de uso “Calcular localização duma TAG”.

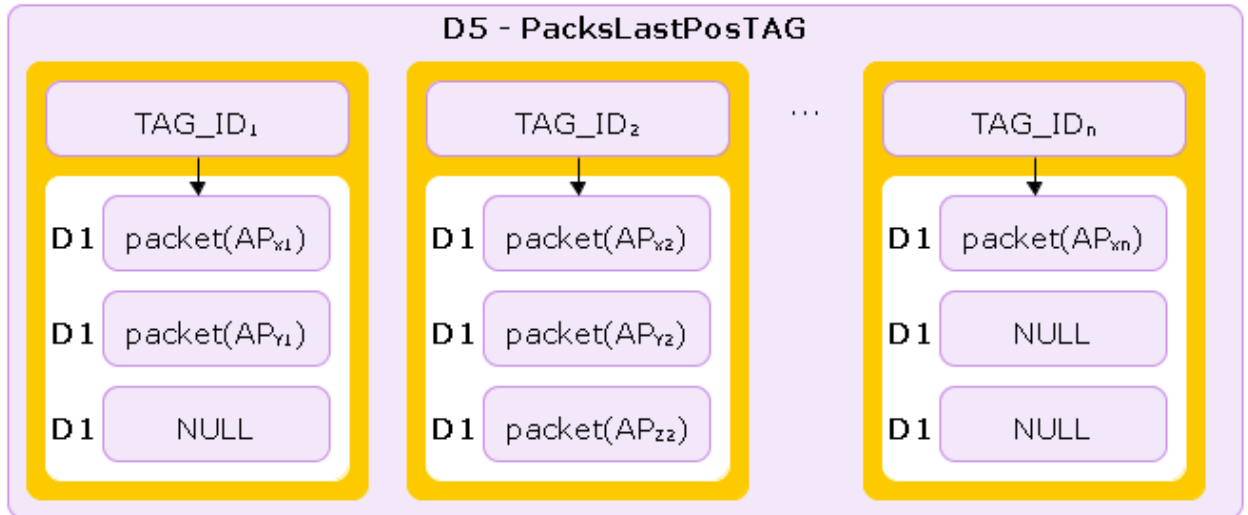


Figura 20 - Estrutura de dados **PacksLastPosTAG** que guarda a lista de pacotes relativos à última posição de cada etiqueta RFID.

- **D8 (Segment) – Segmento**
- **D8L (listSegments) – Lista de segmentos**

A estrutura **Segment (D8)**, que guarda os dados dum segmento/parede do edifício, é definida pelos dois pontos extremos do segmento ($POINT_i$ e $POINT_f$) e pela direção (**DIRECTION**). A direção é calculada com base nos dois pontos anteriores. Cada ponto (classe **POINT**) inclui as coordenadas X, Y e Z. Esta estrutura é preenchida com os dados provenientes do caso de uso “Definir segmentos”. A estrutura **listSegments (D8L)** é simplesmente uma lista com todos os segmentos definidos. Esta estrutura será eficientemente implementada com a classe `HashMap<S_id,Segment>`.

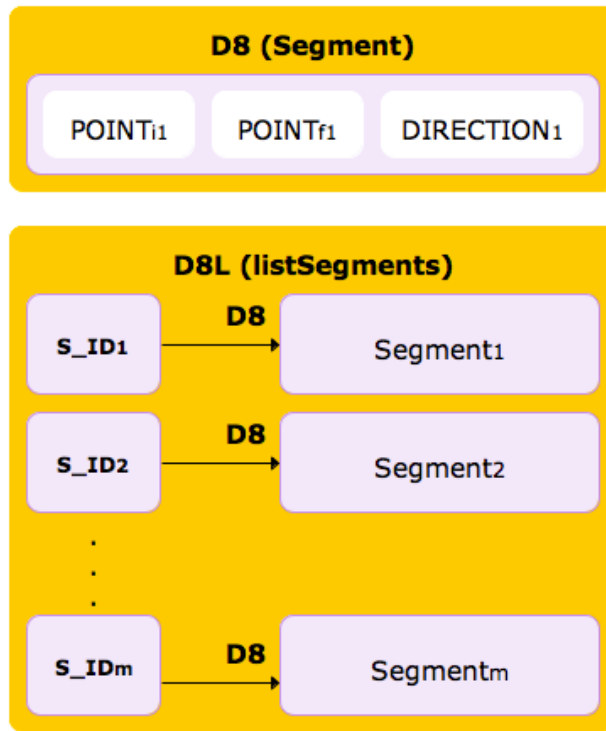


Figura 21 - Estruturas de dados *Segment* e *listSegments*.

- **D9 (Zone) – Zona do edifício**
- **D9L (listZones) – Lista de zonas do edifício**

A estrutura **Zone (D9)**, que guarda a geometria duma zona/espço do edifício, é definida pelo conjunto de segmentos que delimitam essa zona. O valor mínimo do número de segmentos duma zona é 3, definindo dessa forma uma zona triangular. A estrutura **Zone** é preenchida com os dados provenientes do caso de uso “Definir zonas”. Por sua vez, a estrutura **listZones (D9L)** é a lista com todas as zonas definidas para o edifício. Esta estrutura será eficientemente implementada com a classe *HashMap<Z_id,Zone>*.

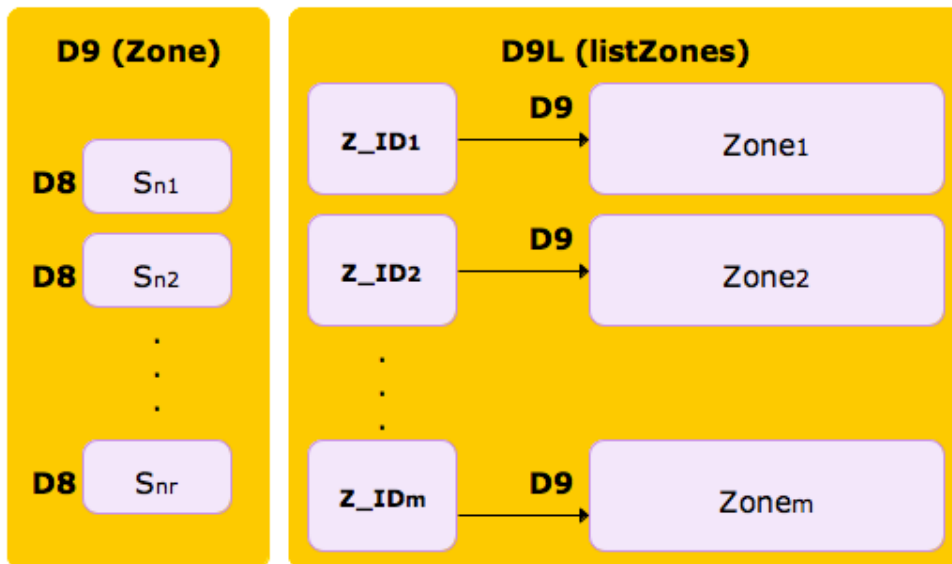


Figura 22 - Estruturas de dados *Zone* e *listZones* utilizadas para guardar a geometria das zonas do edifício.

- **D10 (*UserOfTag*) – Lista de etiquetas atribuídas aos utilizadores**

A estrutura de dados *UserOfTag* é simplesmente uma lista onde se regista a associação entre cada etiqueta RFID e os dados do utilizador a quem foi atribuída. Esta estrutura será eficientemente implementada com a classe *HashMap<tagID,userData>*, em que a chave é o identificador da etiqueta RFID (*tagID*) e o valor contém os dados do utilizador: identificador do utilizador (*userId*), o tipo de utilizador (*userType*) e uma descrição do utilizador (*userDescription*).

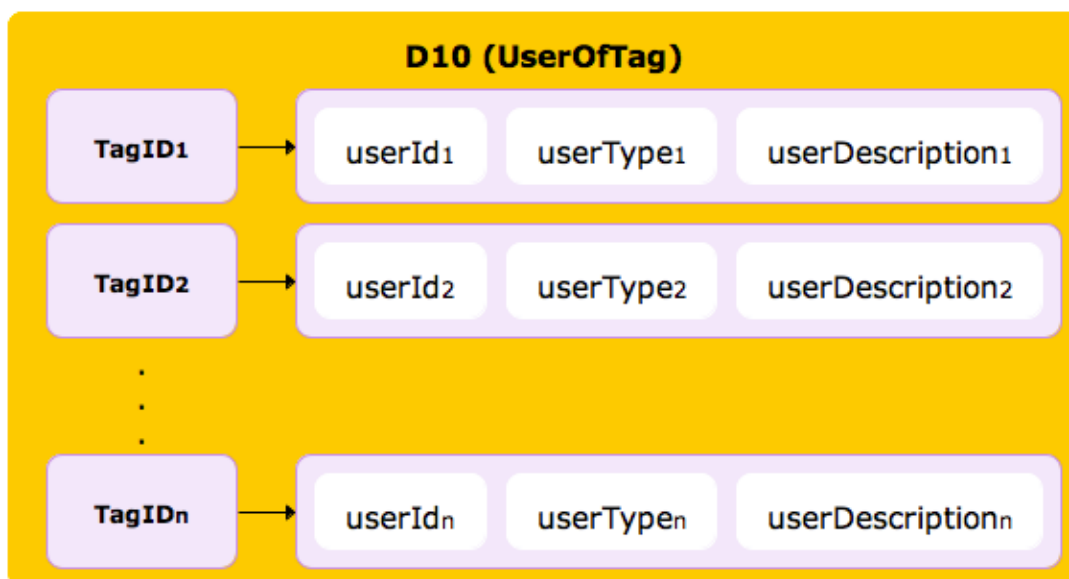


Figura 23 - Estrutura de dados *UserOfTag* que contém as etiquetas atribuídas a utilizadores.

4.4. Atores Intervenientes

A partir do diagrama de contexto do sistema, obtido na fase de levantamento de requisitos, refinou-se a lista de atores do sistema.

- O ator **Utilizador do Sistema** é um utilizador normal do sistema.
- O ator **Gestor de Etiquetas RFID** é um utilizador do sistema responsável pelas operações e gestão de informação relativas às etiquetas RFID.
- O ator **Administrador do Sistema** é um utilizador do sistema que tem acesso a todas as funcionalidades do sistema.
- O ator **Administrador da empresa**, é um supervisor do sistema que gere os perfis de administrador do sistema.
- O ator **Impressora** imprime em papel etiquetas RFID.
- O ator **Leitor/Programador** é responsável por programar e ler informação de configuração duma etiqueta RFID.
- O ator **Utilizador de Etiqueta RFID** é um portador de uma etiqueta RFID.
- O ator **Pessoa** é uma especialização do ator Utilizador de etiqueta RFID.
- O ator **Bem** é especialização do ator Utilizador de etiqueta RFID. Representa todo o tipo de utilizadores de etiquetas RFID que não são pessoas nem animais.
- O ator **Animal** é uma especialização do ator Utilizador de etiqueta RFID.
- O ator **BD com dados utilizadores registados** contém as credenciais de acesso ao sistema por parte de utilizadores registados e autorizados pelo administrador do sistema.
- O ator **AP** (*ponto de acesso*) corresponde a um dispositivo de *hardware* e *software* que estabelece a comunicação entre as etiquetas RFID e o sistema central.
- O ator **Etiqueta RFID** é utilizado para identificar pessoas, animais ou bens. Exemplos: calçado, peças de roupa, livros, revistas, CDs/DVDs, doentes, produtos de armazém, sacos de frutas.
- O ator **Segurança Externa**, especialização do ator Pessoa, como o próprio nome indica, é um segurança que não faz parte dos funcionários da empresa. Pode pertencer a organismos públicos, como polícia ou bombeiros, e será alertado sempre que a sua atuação se justifique.
- O ator **Segurança da Empresa** é uma especialização do ator Pessoa e corresponde a um segurança que é funcionário da empresa. Este ator será

alertado, por exemplo, através do envio de um sinal sonoro, sempre que a sua atuação se justifique.

4.5. Diagrama Geral de Casos de Uso

O diagrama geral de casos de uso visa modelar os requisitos capturados na fase anterior do projeto, conjuntamente com o diagrama de contexto do sistema estruturado em 3 camadas. Com a modelação espera-se que permita obter uma solução parametrizável para o problema de localização por RFID.

Com os diagramas de caso de uso do UML pretende-se representar os vários cenários de funcionamento do sistema, de uma forma simples e que pode ser usada para discutir a solução a implementar com as diversas partes interessadas no sistema (*stakeholders*) [18]. Além disso, as funcionalidades modeladas devem cobrir, como se disse, todos os requisitos identificados.

O diagrama de casos de uso global do sistema é apresentado na Figura 23. Como se pode ver, foram identificados 2 subsistemas: o **Sistema Central** e o **AP** (ponto de acesso). Uma breve explicação dos casos de uso, bem como, a sua descrição textual detalhada, serão apresentados nas próximas subsecções.

4.5.1. Diagrama de Casos de Uso “Sistema Central”

1) Caso de Uso “*Login*”

Modela as atividades envolvidas na identificação de um utilizador perante o sistema, de forma a iniciar o acesso às funcionalidades correspondentes ao tipo de utilizador em causa.

2) Caso de Uso “*Logout*”

Modela as atividades envolvidas no fecho da sessão de trabalho no sistema, por parte de um utilizador, e tem como resultado o terminar do acesso a todas as funcionalidades, exceto efetuar *login*.

3) Caso de Uso “Registrar utilizador do sistema”

Modela as atividades envolvidas na introdução de informação necessária para registar um utilizador do sistema. Nesta informação inclui-se a seleção do tipo de utilizador. O acesso a esta funcionalidade está reservado ao ator “Administrador do Sistema”.

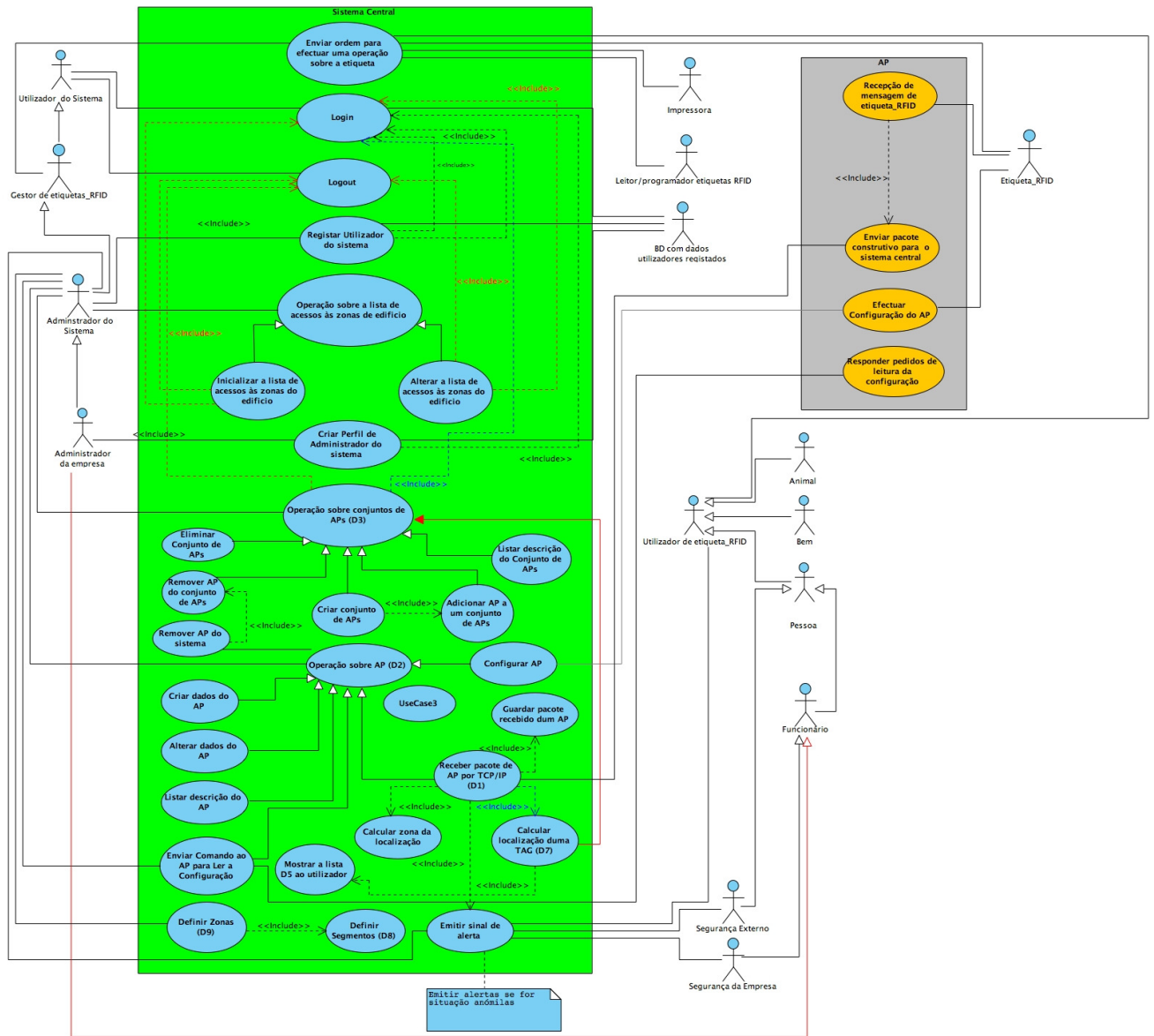


Figura 23 - Diagrama de casos de uso global do sistema.

4) Caso de Uso “Operação sobre a lista de acessos às zonas de edifício”

Este caso de uso não tem funcionalidade própria, foi apenas incluído para funcionar como uma generalização dos diferentes tipos de operação sobre a lista de acessos às zonas do edifício.

5) Caso de Uso “Inicializar a lista de acessos às zonas do edifício”

Modela as atividades envolvidas na inicialização da lista que define, para cada tipo de utilizador, qual o tipo de acesso que tem a cada zona do edifício. Se a zona for interdita, é preciso especificar o tipo de alarme a emitir quando essa interdição for violada.

6) Caso de Uso “Alterar a lista de acessos às zonas do edifício”

Modela as atividades necessárias para trocar o tipo de acesso a uma certa zona do edifício (permitido/interdito) por parte de um dado utilizador, atualizando as listas de acesso em causa.

7) Caso de Uso “Criar um perfil de administrador do sistema”

Modela as atividades necessárias para o administrador da empresa introduzir os dados relativos a um novo administrador do sistema.

8) Caso de Uso “Operação sobre conjuntos de APs”

Este caso de uso não tem funcionalidade própria, foi apenas incluído para funcionar como uma generalização dos diferentes tipos de operação (criar, editar ou eliminar) sobre um conjunto de APs.

9) Caso de Uso “Criar conjunto de APs”

Modela as atividades envolvidas na criação dum conjunto de APs com identificador *SET_ID*. A informação resultante é guardada na estrutura **D7**, que por sua vez é um elemento da lista **D3**. Cada conjunto, a tabela **D7** guarda a lista com a identificação dos vários APs desse conjunto.

10) Caso de Uso “Adicionar AP a um conjunto de APs”

Modela as atividades necessárias para inserir um AP num determinado conjunto de APs. O identificador desse AP é inserido no conjunto com o identificador pretendido (estrutura **D7**, que é um elemento da lista **D3**). Em consequência da inserção do AP no novo conjunto, é preciso alterar o conjunto a que pertence esse AP (campo *AP_SET* da estrutura **D2**).

11) Caso de Uso “Remover AP do conjunto de APs”

Modela as atividades necessárias para remover um AP (*APid*) do conjunto em que está inserido. Utilizando como referência o identificador do AP, procura-se na estrutura **D2** qual o conjunto a que pertence (*setAP*). Assim pode eliminar-se o elemento *APid* do

conjunto *setAP* (estrutura **D7**). Para terminar, marca-se o AP como a indicação de que não pertence a qualquer conjunto (campo *AP_SET=NULL* na estrutura **D2**).

12) Caso de Uso “Eliminar conjunto de APs”

Modela as atividades envolvidas na eliminação dum conjunto de APs. Ou seja, remove a entrada (estrutura **D7**), correspondente a esse conjunto *APset*, na lista de conjuntos de APs (lista **D3**). Elimina ainda todas as entradas relativas a esse conjunto *APset* na estrutura **D5**, a qual indica o último conjunto em que cada etiqueta foi detetada.

13) Caso de Uso “Remover AP do Sistema”

Modela as atividades envolvidas na eliminação da informação relativa a um determinado AP do sistema. Começa-se por remover a entrada relativa a esse AP no conjunto de APs em que está inserido (**D7**). Posteriormente remove-se a entrada desse AP (elemento **D2**) da lista de APs (**D6**). Por fim, eliminam-se todos os pacotes provenientes desse AP e que se encontrem na lista *PacksLastPosTAG* (**D5**).

14) Caso de Uso “Operação sobre AP”

Este caso de uso não tem funcionalidade própria, foi apenas incluído para funcionar como uma generalização dos diferentes tipos de operação (criar, alterar, eliminar, listar, receber pacotes de etiquetas RFID, responder a comandos de configuração) sobre um AP.

15) Caso de Uso “Criar dados do AP”

Modela as atividades envolvidas na introdução de informação que descreve um AP. Esta informação inclui os vários campos da tabela *APdata* (**D2**), que será depois inserida na lista **D6**. Se o campo *AP_SET* for preenchido com um dado valor *APset*, será necessário inserir o identificador do AP criado (*AP_ID*) no conjunto *APset* (**D7**).

16) Caso de Uso “Alterar dados do AP”

Modela as atividades envolvidas na alteração da informação que descreve um AP. Pode alterar-se qualquer dos campos da estrutura **D2** (exceto o identificador). Se o campo alterado for uma das coordenadas da posição do AP, a nova posição será validada para não coincidir com a posição de outro AP. Se o campo alterado for o conjunto do AP, isso implicará eliminar em **D7** a referência ao AP no conjunto antigo e inserir a referência ao AP no novo conjunto. A informação alterada (**D2**) será reinserida em **D6**.

17) Caso de Uso “Receber pacote de AP por TCP/IP”

Modela as atividades que permitem guardar os dados incluídos num pacote, recebido dum AP, numa estrutura *packet* (**D1**). Além dos campos provenientes do pacote, a estrutura *packet* precisa ainda da data e hora de receção do pacote e um identificador único atribuído a esse pacote. Este caso de uso recorre ainda à funcionalidade dos casos de uso “Guardar pacote recebido dum AP”, “Calcular localização dum TAG” e “Calcular zona da localização”.

18) Caso de Uso “Guardar pacote recebido dum AP”

Este caso de uso modela as atividades necessárias para inserir um pacote, originado numa etiqueta RFID e enviado por um AP, na lista *PacksLastPosTAG* (**D5**). Para executar esta tarefa é preciso:

- 1) Extrair do pacote o identificador da etiqueta (*tagId*),
- 2) Obter o anterior conjunto de APs que detetou a etiqueta (*prevSet*),
- 3) Extrair do pacote o identificador do AP que o enviou (*APid*),
- 4) Obter o conjunto em que está inserido o AP que enviou o pacote (*newSet*); se a etiqueta *tagId* passou a ser detetada por um conjunto diferente do anterior (*newSet* é diferente de *prevSet*), todos os pacotes relativos à última posição de etiqueta serão apagados de **D5**,
- 5) Obter a posição do AP que enviou o pacote dentro da lista de APs que formam o novo conjunto que passou a detetar a etiqueta (*apPos*),
- 6) Inserir o pacote recebido na lista *PacksLastPosTAG* (**D5**) na posição (*tagId,apPos*).

19) Caso de Uso “Calcular localização dum TAG”

Modela as atividades necessárias para localizar uma etiqueta RFID, combinando a estimativa da distância a que se encontra essa etiqueta de vários APs. As posições dos APs são conhecidas e fixas. Começa-se por verificar se existem, na estrutura **D5**, 3 pacotes provenientes da etiqueta RFID em causa. Seguidamente, verifica-se se todos os pacotes são válidos para o cálculo da localização. Para critério de validação utiliza-se o tempo de receção dos pacotes. Só serão aceites pacotes cuja diferença no tempo de receção se encontra num certo intervalo $[-\delta T, \delta T]$ em torno do tempo a que se refere o cálculo da localização. Com base em 3 localizações (ou pacotes) válidas, para a mesma etiqueta, estima-se a sua localização, usando por exemplo um método de triangulação. Quando um pacote é antigo demais, é eliminado da lista, mas enquanto se mantiver “atual” pode ser reutilizado no cálculo da localização da etiqueta.

20) Caso de Uso “Calcular zona da localização”

Este caso de uso modela as atividades necessárias para calcular a zona do edifício que corresponde à posição (P) estimada para uma etiqueta RFID. O resultado do caso de uso será o identificador de uma zona, que é definida por um conjunto de segmentos. Começa-se por procurar o segmento do edifício (S_{atual}) que se encontra à menor distância de P (ver secção 5.3.1). Este segmento inicia a geometria da zona procurada. Um dos pontos extremos de S_{atual} será designado P_{atual} e o outro P_{final} . Pegando em P_{atual} , define-se o conjunto dos segmentos (vizinhança) que ligam a esse ponto e calcula-se a direção de cada segmento desta vizinhança. O próximo passo é identificar qual o segmento (S_{next}), de entre os segmentos desta vizinhança, que será adicionada à geometria da zona procurada. Com base nas direções calculadas, o segmento S_{next} a escolher é aquele que garante que o segmento, definido pelos pontos P e P_{atual} , tem como segmentos vizinhos S_{atual} e S_{next} . Adiciona-se S_{next} à geometria da zona procurada e S_{next} passa a ser o novo S_{atual} . Considerando o extremo de S_{atual} que é diferente de P_{atual} , o novo P_{atual} , repete-se o processo até que P_{atual} seja igual a P_{final} . Concluída a geometria da zona procurada, resta comparar esta geometria com a geometria das zonas definidas na lista *listZones* e devolver o identificador da zona que possui os mesmos segmentos. O algoritmo que descreve este caso de uso pormenorizadamente é apresentado na secção 5.3.2.

21) Caso de uso “Definir zonas”

Este caso de uso modela as atividades envolvidas na definição da geometria das zonas do edifício. A geometria de uma zona consistirá num conjunto de segmentos que delimitam uma zona fechada. Depois de escolher o identificador da zona, o administrador do sistema seleciona um conjunto de segmentos disponíveis na lista *listSegment*. Após concluir a introdução dos segmentos, o conjunto será validado de forma a garantir que define uma zona com geometria válida. As características que uma zona válida deve possuir são: (i) forma um único polígono (fechado), (ii) o número de segmentos é superior ou igual a 3, (iii) não possui segmentos desligados num ou nos 2 extremos. Se a geometria for inválida, o administrador poderá remover ou adicionar mais segmentos. A geometria das zonas será guardada na lista *listZones*.

22) Caso de uso “Definir segmentos”

Este caso de uso modela as atividades necessárias para definir os segmentos a utilizar na caracterização da geometria das zonas do edifício. O administrador do sistema começa por escolher o identificador do segmento. Depois introduz as

coordenadas dos dois extremos desse segmento: $Pi=(Pix, Piy, Piz)$ e $Pf=(Pfx, Pfy, Pfz)$. Com base nestes dois extremos, Pi e Pf , o sistema calcula a direção do segmento. Os dados do segmento ($Pi, Pf, direção$) são guardados na lista *listSegments*.

23) Caso de Uso “Emitir sinal de alerta”

Modela as atividades necessárias para que numa situação de violação da regra de interdição numa zona, por parte de utilizador de etiqueta RFID, seja emitido um alerta para os seguranças. Para esse efeito é preciso consultar as prioridades dos diferentes tipos de alarme (sirene, mensagem para o BIP, mensagem para o telemóvel) associadas ao utilizador em causa.

24) Caso de uso “Enviar ordem para efetuar uma operação sobre etiqueta”

Este caso de uso é modelado com um subdiagrama que inclui um caso de uso para cada tipo de operação que é permitido efetuar sobre as etiquetas RFID.

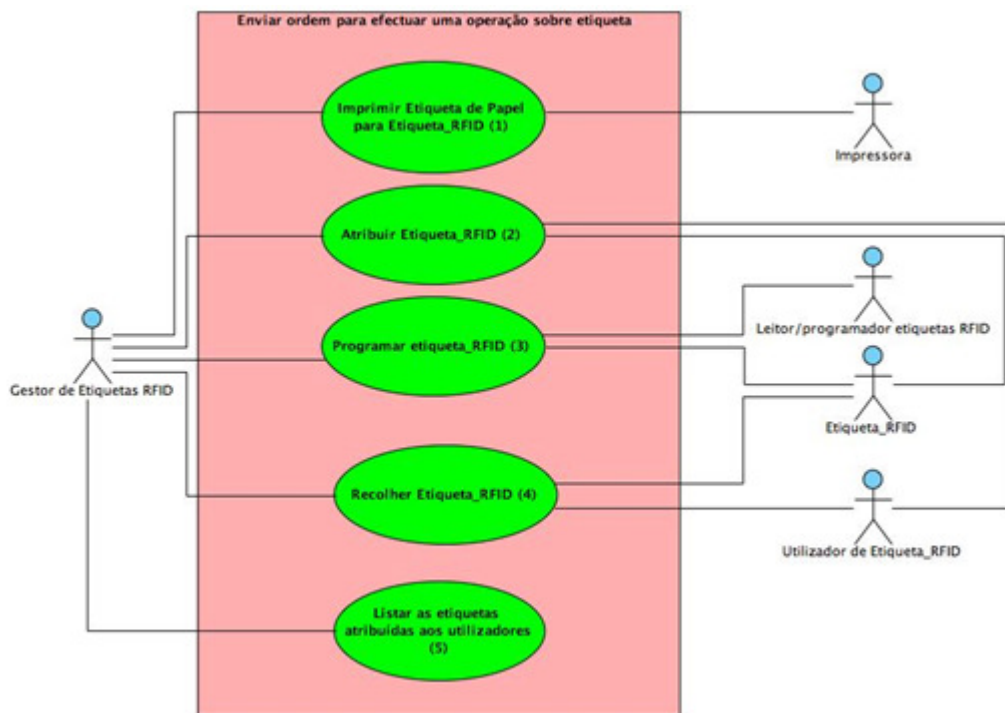


Figura 24 - Caso de Uso "Enviar Ordem para efetuar uma operação sobre etiqueta".

24.1) Caso de uso “Imprimir etiqueta de papel para etiqueta_RFID”

Modela as atividades necessárias para que o gestor de etiquetas RFID imprima uma etiqueta em papel para colar numa etiqueta RFID.

24.2) Caso de uso “Atribuir Etiqueta_RFID”

Modela as atividades envolvidas na atribuição de uma etiqueta RFID a um utilizador que a requisita, e no conseqüente registo desse facto na base de dados. No caso em que o gestor de etiquetas RFID entrega uma etiqueta ao utilizador, é registada a associação (etiqueta, utilizador, tipo de utilizador) na base de dados.

24.3) Caso de uso “Programar etiqueta_RFID”

Modela as atividades necessárias para que, sob ordem do gestor de etiquetas RFID, uma etiqueta RFID seja programada num leitor/programador. Se a etiqueta constar como já programada o gestor poderá optar por a reprogramar ou cancelar a reprogramação.

24.4) Caso de uso “Recolher etiqueta_RFID”

Modela as atividades necessárias para que o gestor de etiquetas RFID recolha uma etiqueta entregue a um utilizador. A correspondente associação (etiqueta, utilizador, tipo de utilizador) é removida na base de dados.

24.5) Caso de uso “Listar as etiquetas atribuídas aos utilizadores”

Modela as atividades que permitem ao gestor de etiquetas RFID visualizar a lista de todas as etiquetas atribuídas a utilizadores em dado momento.

4.5.2. Diagrama de Casos de Uso do Ponto de Acesso (AP)

O Ponto de Acesso, não sendo o alvo principal da modelação nesta tese, será descrito de uma forma bastante sintética através de 4 casos de uso. Os casos de uso incluídos são apenas os necessários para ter um protótipo global do sistema de localização.

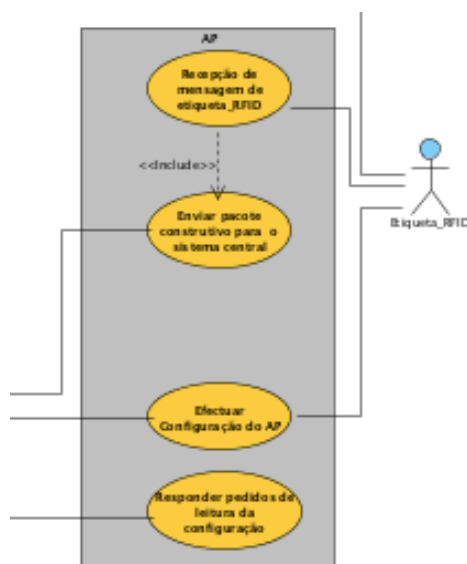


Figura 25 – Diagrama de casos de uso do Ponto de Acesso (AP).

1) Caso de uso “Receção de mensagem de etiqueta_RFID”

Modela as atividades necessárias para que o ponto de acesso esteja à espera de receber mensagem de uma etiqueta RFID detetado. Mais além, enviou o pacote construído para o sistema central.

2) Caso de uso “Enviar pacote construído para o sistema central”

Modela as atividades necessárias para que o ponto de acesso prepare o processo de construção da mensagem que unir os campos do TAG (ID, RSSI, *Link quality* e estado). Por conseguinte, foram convertidos para o pacote e logo a seguir, enviou o pacote construído para o sistema central.

3) Caso de uso “Responder a pedidos de leitura da configuração”

Modela as atividades necessárias para que o AP tenha duas alternativas para responder o pedido de leitura da configuração do ponto de acesso ou etiqueta RFID. Em relação ao ponto de acesso, somente descodifica qual o tipo de dados pretendido (dados duma TAG, S/N duma TAG, S/N do AP, ID da rede do AP, dados do utilizador, versão do *firmware* do AP) e envia um pacote contendo o tipo de dados do AP pedidos para o sistema central. Em comparação da etiqueta RFID, depende do tipo de dados pedido relacionados com uma etiqueta RFID, após executar a tarefa espera uma mensagem dessa TAG via sinal RFID e envia para o sistema central um pacote contendo os dados recebidos dessa TAG.

4) Caso de uso “Efetuar configuração do AP”

Este caso de uso modela as atividades necessárias para efetuar a configuração do AP de acordo com os comandos recebidos do sistema central. O sistema central pretende configurar um AP e recebe do sistema central os comandos relativos à configuração das funcionalidades desse AP. O ponto de acesso efetua a configuração de cada uma das funcionalidades definidas pelos comandos recebidos do sistema central e envia ao sistema central uma resposta indicando sucesso na execução da configuração do AP.

4.6. Diagramas de sequência ao nível do sistema

Com base na descrição textual de cada caso de uso foi elaborado um diagrama de sequência ao nível do sistema. Em cada um destes diagramas, o sistema é representado por um único objeto. Os outros objetos intervenientes são sistemas

externos ou atores. Dada a quantidade de diagramas de sequência elaborados, eles foram incluídos no Anexo VII.

4.7. Modelo dos Dados Persistentes

Esta secção apresenta um resumo dos dados persistentes guardados na base de dados.

A tabela *APdata* do modelo de dados implementa as tabelas *APdata* (D2) e *listAPs* (D6) auxiliares, utilizadas na explicação dos casos de uso. Ou seja, guarda os dados dos vários APs.

Por seu lado, a tabela *setAPs* do modelo de dados implementa as tabelas *setAPs* (D7) e *listSetAPs* (D3) utilizadas na explicação dos casos de uso. Esta tabela guarda a composição dos vários conjuntos de APs.

As tabelas *ListAllowed* e *ListForbidden* especificam quais as zonas permitidas e interditas a cada tipo de utilizador (tabela *TypeUser*), respetivamente. A tabela *ListForbidden* também se liga à tabela *Alarm*, pois é ela que contém os dados sobre o(s) alerta(s) a emitir quando um dado tipo de utilizador entrar numa zona que lhe é proibida.

A tabela *TagRFID* implementa as tabelas *EtiquetaRFID* (D4) e *listaEtiquetaRFID* (D4L) utilizadas na explicação dos casos de uso. Ou seja, guarda os dados de cada etiqueta RFID.

A tabela *SEGMENT* implementa as tabelas *Segment* (D8) e *listSegments* (D8L) utilizadas na explicação dos casos de uso. Deste modo, esta tabela guarda os dados dos vários segmentos (paredes) do edifício, em que cada segmento é definido por dois pontos e uma direção.

A tabela *Zone*, que guarda informação sobre a geometria duma zona/espço do edifício, em conjunto com as tabelas *ZONES_SEGMENTS* e *SEGMENT* implementam as tabelas *Zone* (D9) e *listZones* (D9L) utilizadas na explicação dos casos de uso. A tabela *ZONES_SEGMENTS* permite estabelecer uma relação N:N entre as tabelas *Zone* e *SEGMENT*.

A tabela **UserTagRFID**, que armazena os vários utilizadores de etiquetas RFID, estabelece a associação entre os utilizadores e as etiquetas. Um utilizador de etiqueta RFID pode ser do tipo **Person**, **Animal** ou **Stuff**. Em conjunto, as tabelas **UserTagRFID** e **TagRFID** implementam a tabela **UserOfTag** (D10) utilizada na explicação dos casos de uso. Um animal é de um dos tipos especificados na tabela **TypeAnimal**. Similarmente, um bem (*Stuff*) é de um dos tipos especificados na tabela **TypeStuff**. Uma pessoa (*Person*) pode ser do tipo **Employee**, **Visitor** ou **Collaborator**. A pessoa pode ainda ter animais associados. Por seu lado, um empregado pode ser também um utilizador do sistema (*SystemUser*). A tabela **SystemUser** guarda os dados de acesso ao sistema por parte de um utilizador registado. Um dos campos desta tabela é o tipo de utilizador (**TypeUser**), que mais não é do que uma categoria como por exemplo administrador, utilizador normal, diretor da empresa, etc.

A tabela **Anomaly**, é utilizada para registar anomalias que ocorram na entrega ou recolha de etiquetas RFID. Nomeadamente, tentar entregar uma etiqueta que conste como atribuída. Ou seja, ocorreu uma recolha prévia de uma etiqueta em que não se apagou do sistema o registo que indicava que essa etiqueta estava atribuída.

Convém referir que os dados relativos aos pacotes recebidos dos APs, guardados nas estruturas *packet* (D1) e *PacksLastPosTAG* (D5), não são guardados em base de dados.

O modelo de dados persistentes apresentado na Figura 26 é constituído por um conjunto de tabelas entidade-relacionamento desenhadas de acordo com o levantamento de requisitos e os casos de uso apresentados. Este modelo de dados foi desenhado na aplicação *MySQLWorkbench*¹.

¹ <http://wb.mysql.com>

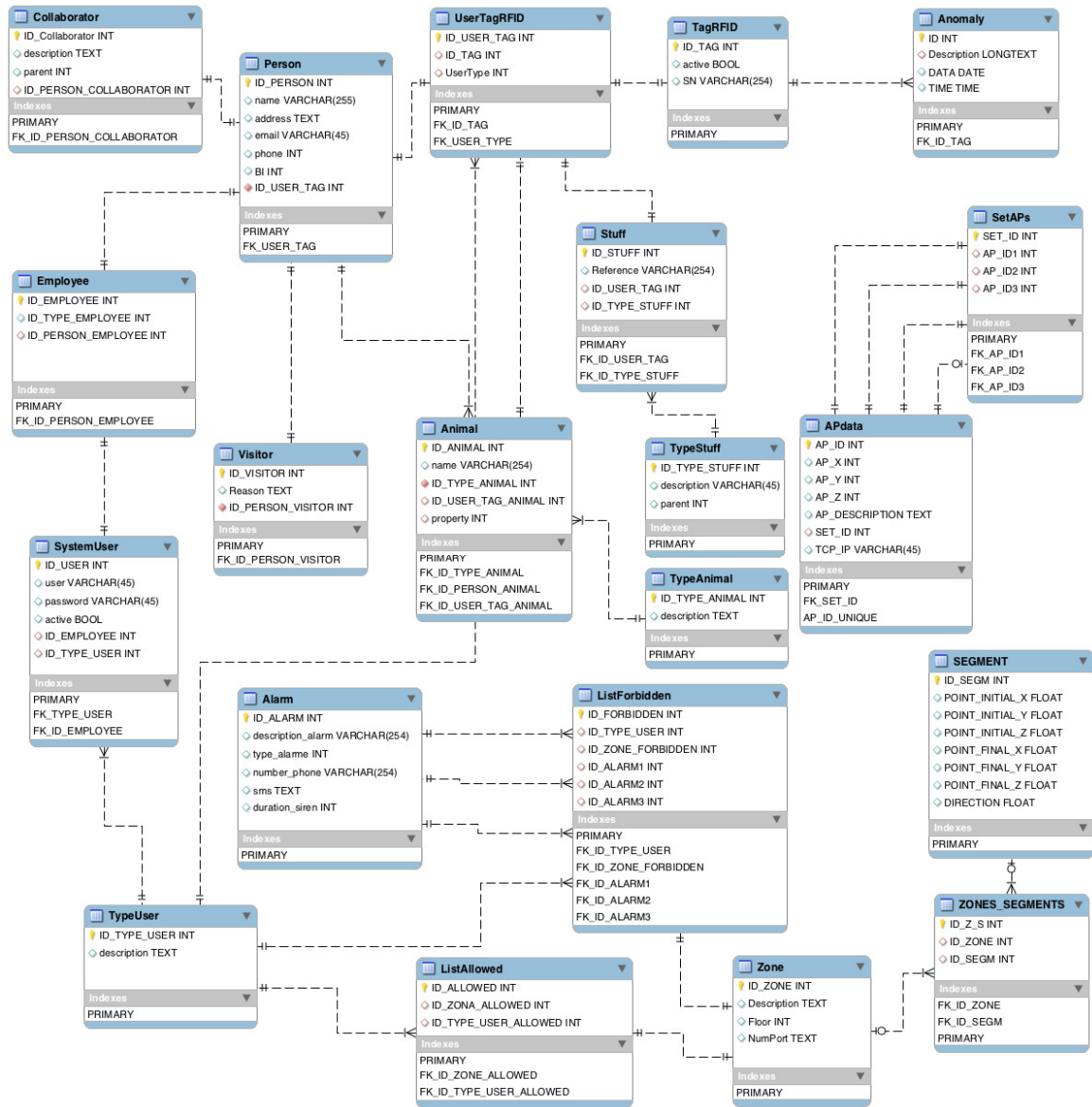


Figura 26 - Modelo dos dados persistentes.

4.8. Diagrama de Classes

Com base na descrição textual dos casos de uso, nos diagramas de sequência e no modelo de dados persistentes foi elaborado o diagrama de classes do sistema (ver Figura 27). As classes e os seus atributos resultam essencialmente do modelo de dados, enquanto os métodos são fundamentalmente obtidos a partir da descrição textual dos casos de uso e dos diagramas de sequência. Apresenta-se a seguir um resumo das várias classes do sistema.

1) Classe *SystemUser*

Os atributos desta classe são equivalentes à tabela *SystemUser* do modelo de dados e possui métodos para validar e remover um utilizador do sistema.

2) Classes *Person*, *Animal* e *Stuff*

Os atributos destas classes são equivalentes aos das tabelas com o mesmo nome no modelo de dados. Cada uma destas classes possui métodos para remover e listar os dados dum objeto do tipo da classe respetiva.

3) Classes *TypeUser*, *TypeAnimal* e *TypeStuff*

Os atributos destas classes são equivalentes aos das tabelas com o mesmo nome no modelo de dados. Cada uma destas classes possui métodos para criar e listar os dados dum objeto do tipo da classe respetiva. A classe *TypeUser* possui métodos adicionais para remover e validar o tipo de utilizador.

4) Classes *Employee*, *Collaborator* e *Visitor*

Estas classes são uma especialização da classe *Person*.

5) Classe *TagRFID*

Os atributos desta classe são equivalentes aos da tabela *TagRFID* do modelo de dados e possui métodos para atribuir, recolher, programar, imprimir, criar, eliminar e listar os dados duma etiqueta RFID.

6) Classe *UserTagRFID*

Os atributos da classe são equivalentes aos da tabela *UserTagRFID* do modelo de dados e possui métodos para consultar, eliminar, listar, autorizar e não autorizar a utilização duma etiqueta RFID.

7) Classe *RFIDUserType*

Esta classe serve apenas para classificar o tipo de utilizador de etiqueta RFID. É uma generalização de *TypeUser*, *TypeVisitor*, *TypeAnimal* e *TypeStuff*.

8) Classe “Packet”

A classe *packet* é utilizada para guardar os dados recebidos no sistema central a partir dum AP. Os atributos da classe correspondem aos da estrutura de dados D1: identificador do pacote, identificador do AP que enviou o pacote, identificador da etiqueta RFID que está na origem do pacote, a potência do sinal RF recebido no AP, a data e hora da receção dos dados (por RF) no AP. Esta classe inclui alguns métodos relevantes, tais como: (i) *ReceivePacket*, que recebe um pacote dum AP por TCP/IP, (ii) *Validate*, que verifica se o pacote recebido é válido ou não. Se for inválido não será utilizado nos cálculos da localização da etiqueta RFID; (iii) *CalcDbmTagLocalization*, converte o valor do RSSI, na gama 0:255, para milidecibéis (dBm); (iv) *CalcDistanceTagLocalization*, calcula uma estimativa para a distância a que se encontra a etiqueta RFID que enviou o pacote, utilizando a Equação 3.

9) Classe *PacksLastPosTag*

A classe *PacksLastPosTag*, com atributos equivalente aos da estrutura de dados D5, é uma lista com os pacotes relativos à última posição de cada TAG. Possui alguns métodos que vale a pena referenciar: (i) *TagLocalization*, que calcula a localização (x,y,z) da etiqueta RFID, (ii) *ZoneLocalization*, que determina qual a zona do edifício a que corresponde a localização da etiqueta, e (iii) *Verify3PacksAvailable*, que verifica se existem 3 pacotes, provenientes da mesma etiqueta, válidos para efetuar a trilateração.

10) Classe *SetAPs*

Os atributos desta classe são equivalentes aos da tabela *SetAPs* do modelo de dados (estrutura D7) e possui métodos para criar, validar, remover e listar um conjunto de APs.

11) Classe *ListSetAPS*

A classe *ListSetAPS* é uma lista de conjuntos de APs. Possui atributos equivalentes aos da estrutura de dados D3 e métodos para adicionar, validar, remover e listar um conjunto de APs da lista.

12) Classe *APdata*

A classe *APdata* guarda os dados dos pontos de acesso, os seus atributos são

equivalentes aos da tabela *APdata* do modelo de dados (e da estrutura de dados D2) e possui métodos para criar, alterar os dados, remover do sistema, remover dum conjunto de APs, listar e validar os dados, configurar e enviar um comando ao AP.

13) Classe *Zone*

Esta classe, que guarda a geometria duma zona do edifício, possui atributos equivalentes aos da tabela *Zone* do modelo de dados e os métodos para ler e escrever cada atributo.

14) Classe *ForbiddenZone*

Esta classe estende a classe *Zone*, acrescentando-lhe atributos necessários para definir a zona como interdita a um determinado tipo de utilizador, nomeadamente atributos que especificam os tipos de alerta a emitir quando o tipo de utilizador entrar nessa zona. Possui apenas os métodos para ler e escrever cada atributo.

15) Classe *Segment*

Os atributos desta classe são equivalentes aos da tabela *Segment* do modelo de dados e possui apenas os métodos para ler e escrever cada atributo.

16) Classe *POINT*

A classe *Point* define um ponto num edifício através das coordenadas X, Y e Z. Inclui o método *equals* que permite verificar se dois objetos do tipo *POINT* são iguais.

17) Classe *ListAllowed*

Esta classe guarda a lista de zonas permitidas a cada tipo de utilizador e é implementa com um *HashMap<int,HashMap<int,Zone>>*. Possui métodos para adicionar e remover uma zona, inicializar a lista e mover uma zona para a lista de zonas interditas.

18) Classe *ListForbidden*

Esta classe guarda a lista de zonas interditas a cada tipo de utilizador e é implementa com um *HashMap<int,HashMap<int, ForbiddenZone>>*. Possui métodos para adicionar e remover uma zona, inicializar a lista e mover uma zona para a lista de zonas permitidas.

19) Classe *Alarm*

A classe *Alarm* contém os dados sobre o(s) alerta(s) a emitir quando um dado tipo de utilizador entrar numa zona interdita. Os seus atributos são equivalentes aos da

tabela *Alarm* do modelo de dados e possui métodos para consultar, emitir e listar alertas.

20) Classes *Siren*, *SMS* e *BIP*

São especializações da classe *Alarm*, guardando informação sobre um tipo de alerta diferente: um sinal sonoro, um SMS a enviar para um telemóvel e um aviso a enviar para um BIP, respetivamente.

21) Classe *TagLocalization*

A classe *TagLocalization* contém os métodos necessários para estimar a localização duma etiqueta RFID com base em 3 distâncias que foram estimadas a partir das medições de RSSI em 3 APs do mesmo conjunto. Os métodos relevantes da classe são:

- *CalcPosDistanceMin* calcula a circunferência com raio mínimo de entre uma lista de 3.
- *APsCalcLocalizationTag* calcula a localização duma etiqueta RFID, com base nos valores estimados para a distância a que ela se encontra de 3 APs e conhecida a localização dos 3 APs.
- *CalcIntercept2Circles* calcula os pontos de interceção entre 2 circunferências (0, 1 ou 2 pontos).
- *CalcIntersept2Lines* calcula o ponto de interceção entre 2 segmentos de reta.
- *CalcFirstPairCircumference* obtém o primeiro par de circunferências, em que uma delas é a que possui o raio mínimo e a outra é a primeira que encontrar distinta dela, de entre uma lista de 3 circunferências. Depois calcula os 2 pontos de interceção desse par de circunferências.
- *CalcSecondPairCircumference* obtém o segundo par de circunferências, em que uma delas é a que possui o raio mínimo e a outra é a segunda que encontrar distinta dela, de entre uma lista de 3 circunferências. Depois calcula os 2 pontos de interceção desse par de circunferências.
- *CalcPointLineDist* calcula a distância mínima dum ponto a um segmento de reta.
- *CalcDirectionPoint* calcula o ângulo formado entre o vetor que liga um dado ponto $P=(x,y)$ à origem das coordenadas e o eixo dos XX.
- *CalcDirectionSegment* calcula a direção dum segmento definido por dois pontos.
- *FindSegmentDistanceMin* determina qual o segmento, de entre uma lista de segmentos, se encontra mais próximo dum dado ponto.
- *CalcZoneLocalization* identifica qual a zona em que se inclui uma determinada localização dada por $P=(x,y,z)$.

22) Classes *Circumference* e *PointDouble*

A classe *Circumference* define uma circunferência centrada num dado ponto e com um certo raio. A classe *PointDouble* define um ponto usando coordenadas do tipo *double*.

23) Classe *BDInterface*

Esta classe implementa a interface entre o sistema de localização e a base de dados que guarda os dados persistentes. Inclui atributos como as credenciais de acesso, o endereço do hospedeiro e o nome da base de dados. Possui métodos para ligar e desligar a ligação à base de dados, para ler os parâmetros de configuração, para inserir, alterar, remover e listar valores da base de dados.

24) Classe *AP*

A classe *AP*, que foi projetado para ser apenas um protótipo básico dum ponto de acesso e permitir assim testar o sistema de localização, inclui atributos que correspondem aos parâmetros de configuração do AP e possui métodos para estabelecer uma ligação com o AP, desligar a ligação, ler o estado do AP, configurar o AP, programar uma etiqueta RFID a partir do AP, enviar um comando ao AP para ler a sua configuração, receber uma mensagem do sistema central durante o tempo de repouso, receber uma mensagem duma etiqueta RFID e enviar um pacote para o sistema central.

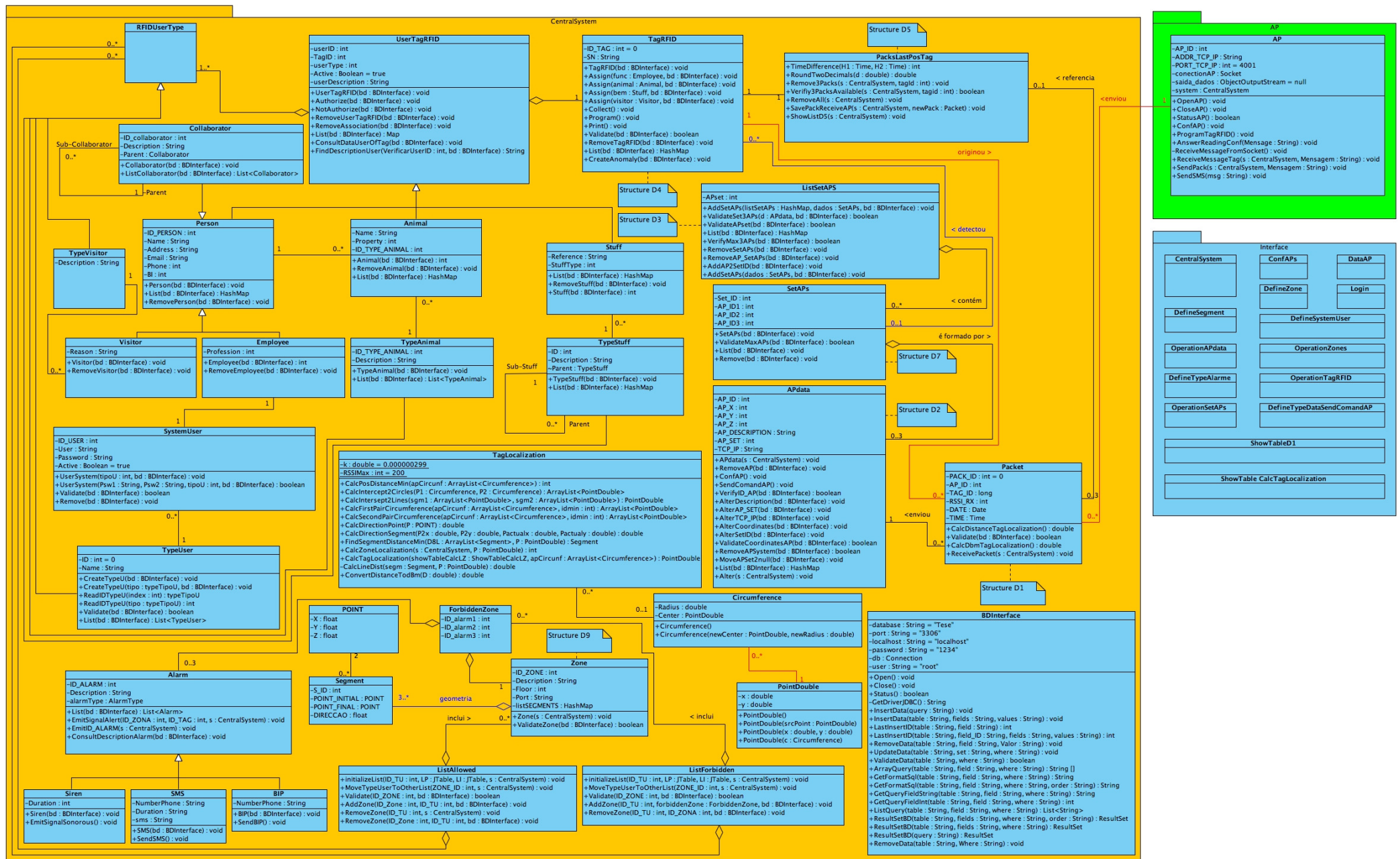


Figura 27 - Diagrama de classes do sistema.

4.9. Diagramas de sequência ao nível da implementação

Depois de concluir o modelo de dados persistentes e o diagrama de classes, elaboram-se os diagramas de sequência ao nível da implementação. Estes diagramas permitem verificar se a implementação respeita a conceção, ou seja, implementa a funcionalidade descrita nos casos de uso. Dada a dimensão do problema, apresenta-se nesta secção apenas um subconjunto dos diagramas de sequência ao nível da implementação. Concretamente, apresentam-se apenas diagramas relevantes e suficientemente ilustrativos do modelo do sistema:

- Diagrama de sequência que descreve a tarefa de atribuição de uma etiqueta RFID a um utilizador (Figura 28).
- Diagrama de sequência relativo à tarefa em que se guardam os dados de um pacote recebido de um AP (Figura 29).
- Diagrama de sequência associado com o cálculo da localização de uma etiqueta RFID (Figura 30).
- Diagrama de sequência relativo à receção de um pacote de um AP por TCP/IP (Figura 31).

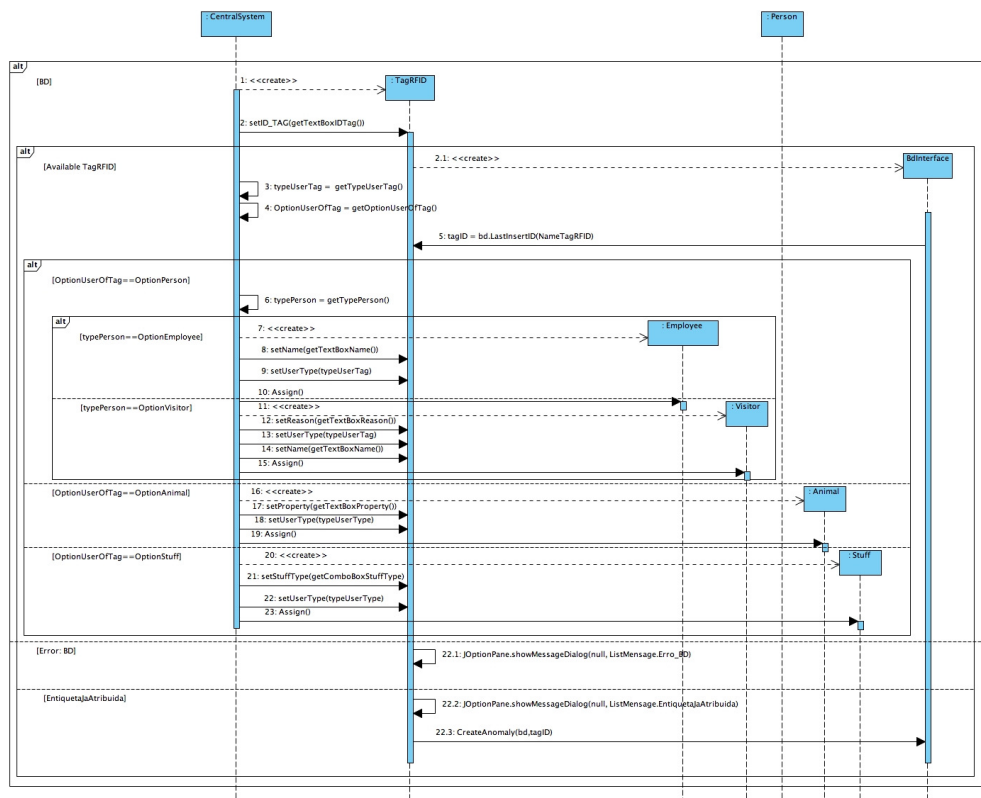


Figura 28 - Diagrama de sequência “Atribuir etiqueta RFID”.

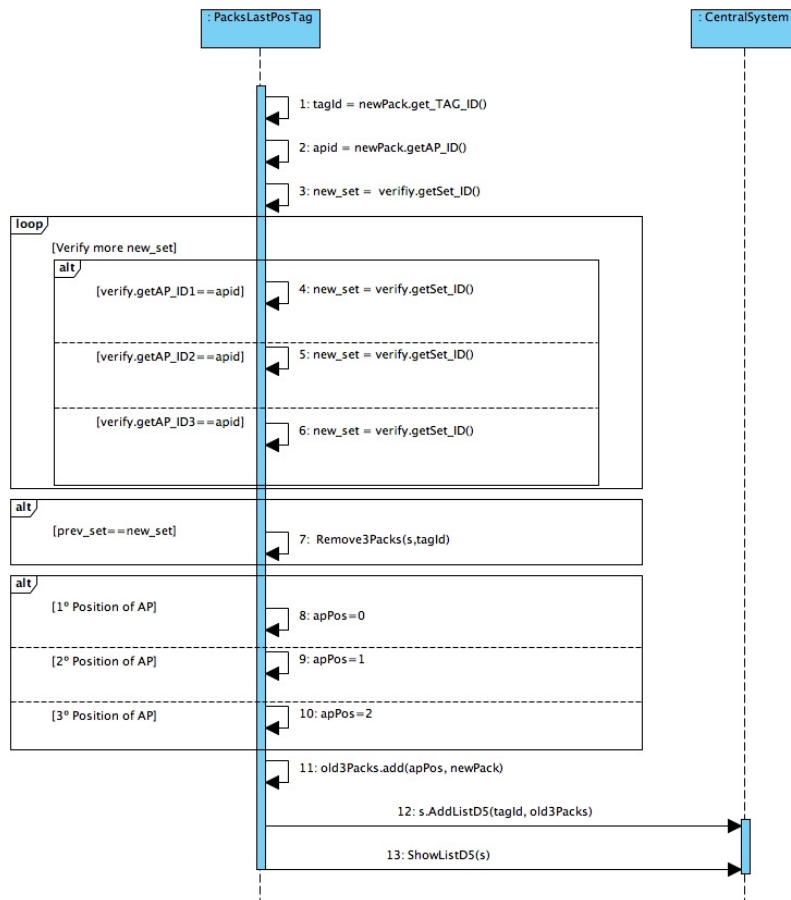


Figura 29 - Diagrama de sequência "Guardar pacote recebido dum AP".

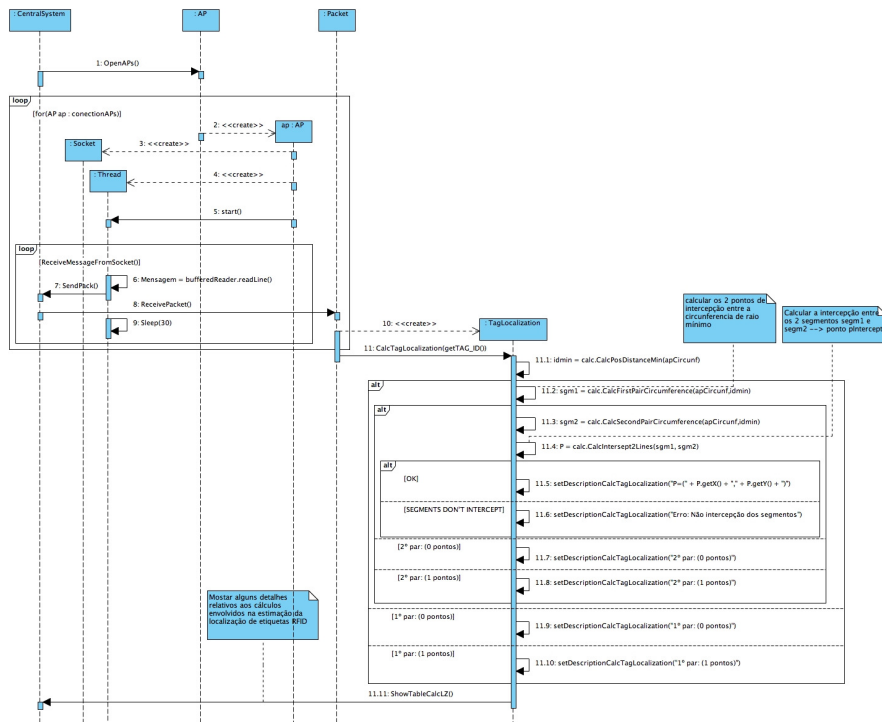


Figura 30 - Diagrama de sequência "Calcular localização duma TAG".

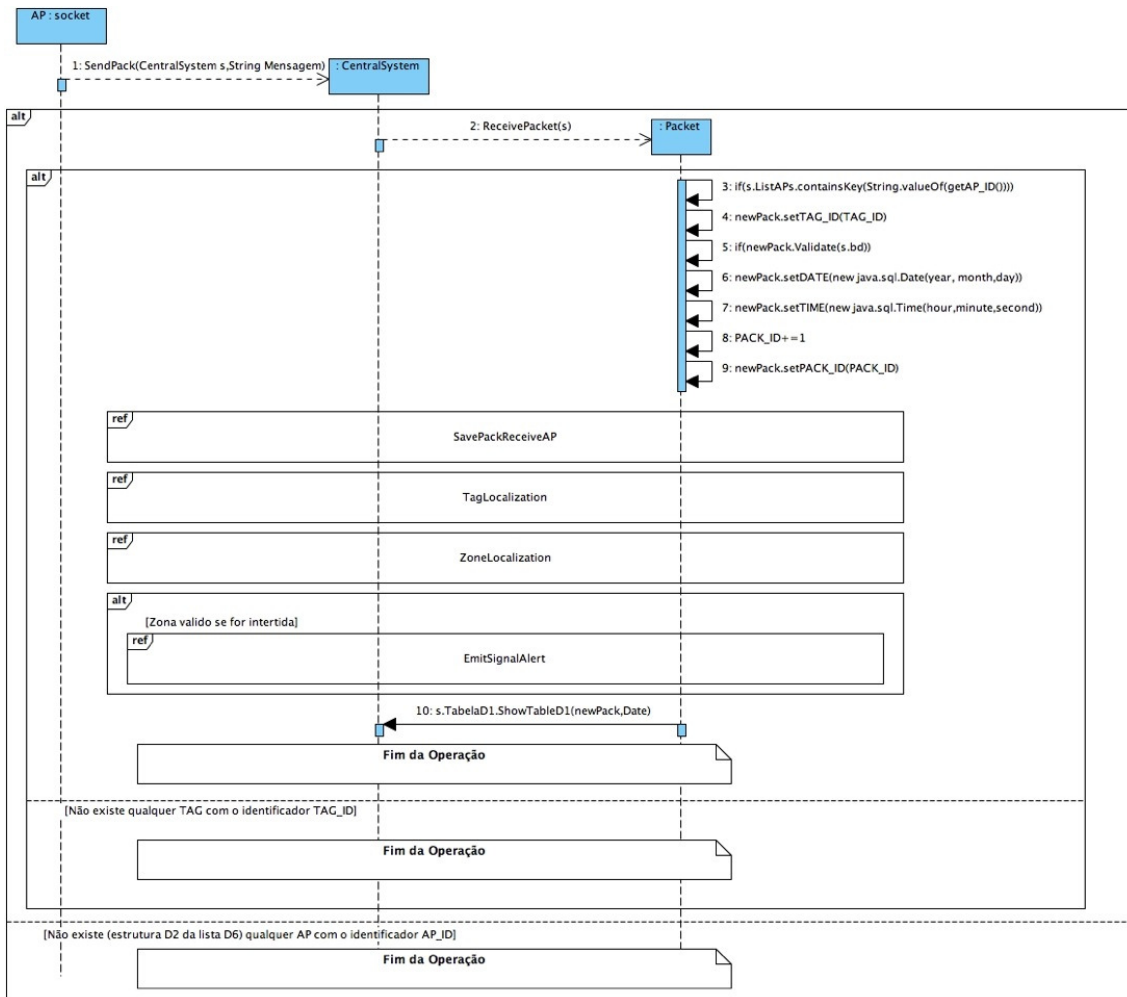


Figura 31 - Diagrama de seqüência "Receber pacote de AP por TCP/IP".

Capítulo 5 Implementação

Neste capítulo será descrita a implementação da solução concebida e que foi apresentada no capítulo anterior.

5.1. Tecnologias

As opções tecnológicas tomadas durante a implementação do protótipo foram as seguintes: (i) as classes concebidas durante a fase de modelação foram implementadas na linguagem JAVA, (ii) o modelo de dados persistentes foi implementado através duma base de dados relacional MySQL, e (iii) a interligação entre as classes JAVA e a base de dados MySQL foi feita com a API *Java Database Connectivity* (JDBC).

O protótipo do sistema central foi desenvolvido no ambiente integrado (IDE) **NetBeans**, dado facilitar a integração entre o código JAVA das classes do modelo UML, a interface com o utilizador implementada com a API **Swing** e o acesso à base de dados MySQL implementada com a API JDBC.

A tecnologia JDBC corresponde a uma API que permite o acesso a qualquer base de dados relacional a partir da plataforma JAVA, nomeadamente MySQL, como ilustra a Figura 32. Dado que o protótipo do sistema central foi desenvolvido em JAVA e a JDBC também, a escolha da JDBC em detrimento do *Microsoft Open Database Connectivity* (ODBC), dispensa mais justificações.

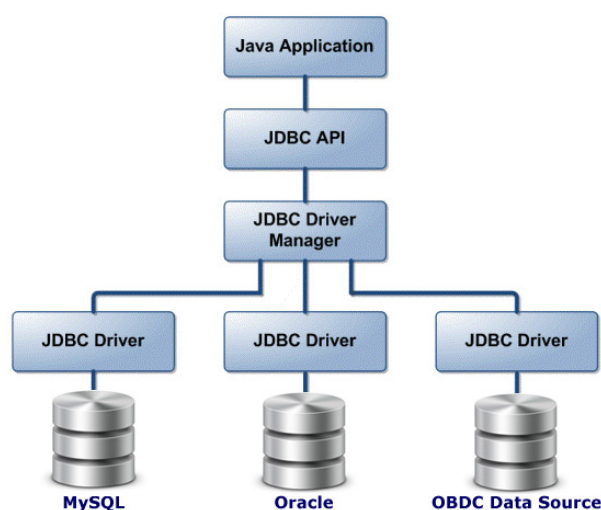


Figura 32 - Arquitetura da JDBC.

5.2. Integração entre o código da implementação e os modelos UML

A implementação do protótipo foi extensivamente apoiada na funcionalidade “*Java round-trip engineering*”² disponibilizada pelo *Visual Paradigm for UML*. Esta funcionalidade proporciona três vantagens: (i) ajuda na geração de código JAVA para as classes UML, (ii) gera/atualiza as classes UML a partir do código JAVA e (iii) ajuda a manter os modelos e a implementação sincronizados.

A funcionalidade “*Java round-trip engineering*” permite que sempre que se criam/alteram/apagam atributos ou métodos numa classe do diagrama de classes UML seja criado/alterado/apagado o código JAVA da implementação. Do mesmo modo, quando se criam/alteram/apagam atributos ou métodos numa classe da implementação JAVA são atualizados os atributos ou métodos da classe correspondente do diagrama de classes UML. Usando como exemplo a classe “*etiqueta_RFID*”, a Figura 33 ilustra a forma como se mantém o código JAVA e o diagrama de classes UML sincronizados.

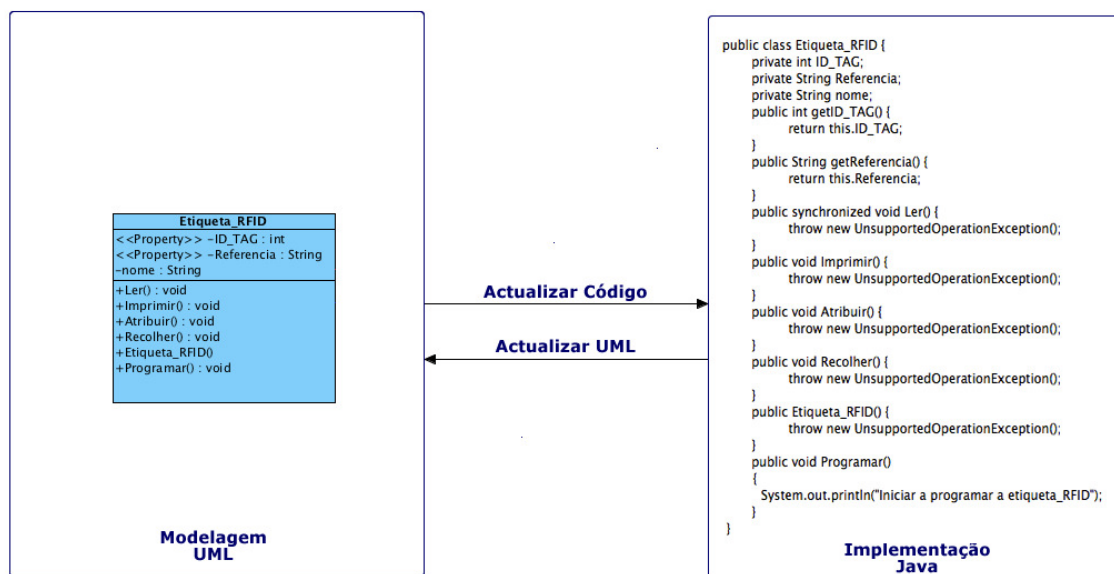


Figura 33 – Exemplo de integração entre o modelo UML e a implementação em Java para a classe “*etiqueta_RFID*”.

² http://media.visual-paradigm.com/media/documents/sde41javaug1/pdf/sdejava_user_guide_ch11.pdf

5.3. Algoritmos

5.3.1. Cálculo da menor distância dum ponto P a um segmento de reta

Nesta secção vamos apresentar as equações necessárias para que, dado um segmento de reta SI , definido pelos pontos $P_{1s} = (P_{1sx}, P_{1sy})$ e $P_{2s} = (P_{2sx}, P_{2sy})$, e um ponto $P = (P_x, P_y)$ externo a SI , se calcule a menor distância (d_{min}) de P a SI (ou à reta que inclui SI).

Considerando uma reta r , que forma um ângulo α com o eixo dos X, a inclinação desta reta é caracterizada pela tangente de α :

$$tg(\alpha) = \frac{\text{lado oposto}}{\text{lado adjacente}} \quad (\text{Equação 7})$$

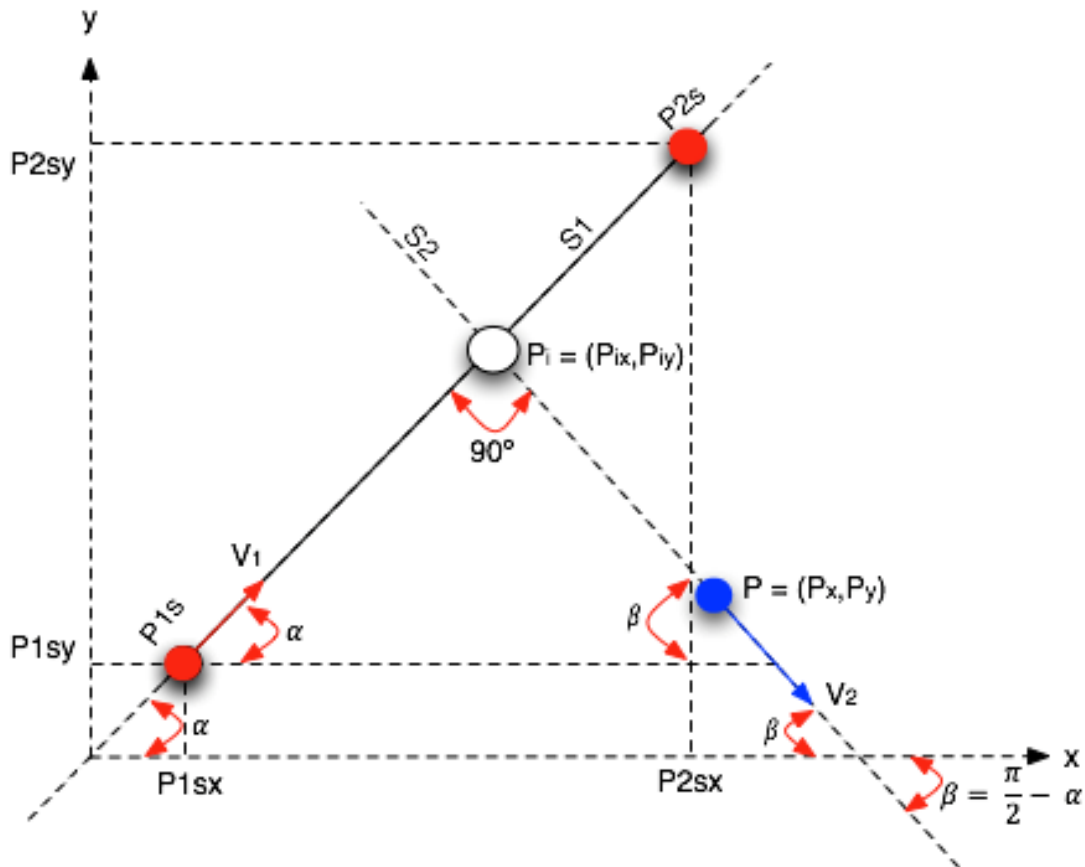


Figura 34 - Ilustração do cálculo da menor distância dum ponto a um segmento de reta (ou a uma reta).

A partir da Figura 34, a definição do segmento SI é:

$$P_i = P_{1s} + s * \bar{V}_1 \quad (\text{Equação 8})$$

ou seja

$$(P_{ix}, P_{iy}) = (P_{1sx}, P_{1sy}) + s * [(P_{2x} - P_{1x}) \cdot \hat{x}, (P_{2y} - P_{1y}) \cdot \hat{y}] \quad (\text{Equação 9})$$

em que s é um escalar e \bar{V}_1 é um vetor unitário com a direção de SI .

Do mesmo modo, a definição do segmento $S2$ é:

$$P_i = P + t * \bar{V}_2 \quad (\text{Equação 10})$$

ou seja

$$(P_{ix}, P_{iy}) = (P_x, P_y) + t * [(P_{2y} - P_{1y}) * \hat{x}, (P_{1x} - P_{2x}) * \hat{y}] \quad (\text{Equação 11})$$

em que t é um escalar e \bar{V}_2 é um vetor unitário com a direção de $S2$. Igualando as duas expressões de P_i (ponto de interseção) obtém-se:

$$s = \frac{P_x - P_{1sx}}{P_{2x} - P_{1x}} + t * \frac{P_{2y} - P_{1y}}{P_{2x} - P_{1x}} \quad (\text{Equação 12})$$

$$t = \frac{P_{1sy} - P_y}{P_{1x} - P_{2x}} + s * \frac{P_{2y} - P_{1y}}{P_{1x} - P_{2x}} \quad (\text{Equação 13})$$

Substituindo (Equação 13) em (Equação 12) obtém-se a equação para calcular s :

$$s = \frac{(P_{1sx} - P_x) * (P_{1x} - P_{2x}) - (P_{1sy} - P_y) * (P_{2y} - P_{1y})}{(P_{1x} - P_{2x}) * (P_{1x} - P_{2x}) - (P_{2y} - P_{1y}) * (P_{2y} - P_{1y})} \quad (\text{Equação 14})$$

A equação de t , que não é necessária, obtém-se da equação (Equação 13), substituindo s pela equação (Equação 14).

Para calcular o ponto de interseção P_i recorre-se à equação (Equação 9) e resulta:

$$\left\{ \begin{array}{l} P_{ix} = P_{1sx} + s * (P_{2sx} - P_{1x}) \end{array} \right. \quad (\text{Equação 15})$$

$$\left\{ \begin{array}{l} P_{iy} = P_{1sy} + s * (P_{2y} - P_{1y}) \end{array} \right. \quad (\text{Equação 16})$$

Finalmente, a menor distância de P a SI é dada por:

$$d_{min} = \sqrt{(P_{ix} - P_x)^2 + (P_{iy} - P_y)^2} \quad (\text{Equação 17})$$

5.3.2. Algoritmo para definir a zona em que se localiza um ponto P

Este algoritmo corresponde à implementação do caso de uso “Calcular zona da localização” e pretende-se com ele determinar a zona, dum edifício, em que se situa a posição estimada como sendo a localização dum etiqueta RFID em determinado momento. Uma zona corresponde a um espaço físico dum edifício e é representada por um conjunto de segmentos que delimitam esse espaço. Os segmentos formam um polígono com 3 ou mais segmentos. Por seu lado, um segmento é definido por dois pontos extremos, em que os pontos correspondem a esquinas no espaço físico do edifício. Por questões de simplificação, considera-se apenas o espaço em 2D, ou seja, não se considera a coordenada Z.

1. Procurar o segmento (S_{near}) que se encontra à menor distância do ponto $P=(P_x, P_y)$. Este ponto localiza-se na interceção entre este segmento e uma reta perpendicular a S_{near} e que passa por $P \rightarrow S_{near} = (P_{1near}, P_{2near})$.
2. $S_{atual} = S_{near}$
3. $zona(P) = \{ S_{atual} \}$
4. Escolher um dos pontos extremos de S_{atual} (P_1 ou P_2) $\rightarrow P_{atual}$
5. Ponto terminal da zona é $\rightarrow P_{final} =$ outro ponto de S_{atual} não utilizado.
6. Definir a vizinhança $S_{viz}(P_{atual})$ como sendo o conjunto de segmentos em que um dos extremos é P_{atual} .
7. Para cada segmento S do conjunto $S_{viz}(P_{atual}) - S_{atual}$ fazer:
 - (i) Calcular a direção (ângulo) $dir(S)$ do segmento S , considerando que o vetor direção tem origem em P_{atual} e aponta na direção do outro extremo de $S \rightarrow dir(S) = arctg((P_{2y}-P_{atual_y})/(P_{2x}-P_{atual_x}))$
 - (ii) Calcular:

$$maxDir(S) = máximo[dir(S_{atual}), dir(S)]$$

$$minDir(S) = mínimo[dir(S_{atual}), dir(S)]$$
8. Calcular o próximo segmento da $zona(P)$:
 - (i) $menorDeltaMin = 2*PI$
 - (ii) $menorDeltaMax = 2*PI$
 - (iii) Para cada segmento s do conjunto $S_{viz}(P_{atual}) - S_{atual}$ fazer:
 - se $(minDir(s) \leq dir(S_{p,patual}) \leq maxDir(S))$ então
 - se $(dir(S_{p,patual}) \leq dir(S_{atual}))$ então
 - $dm = dir(S_{p,patual}) - minDir(S)$
 - se $(dm \leq menorDeltaMin)$ então
 - $S_{next} = S$
 - $menorDeltaMin = dm$
 - fse
 - senão // $dir(S_{p,patual}) > dir(S_{atual})$
 - $dM = maxDir(s) - dir(S_{p,patual})$
 - se $(dM \leq menorDeltaMax)$ então

- $S_{next} = S$
 - $menorDeltaMax = dM$
 - fse
 - fse
 - fse
9. $S_{atual} = S_{next}$
 10. Adicionar o segmento S_{atual} à $zona(P) \rightarrow zona(P) = zona(P) \cup S_{atual}$
 11. De entre os 2 pontos extremos de S_{atual} , escolher aquele que não é P_{atual} , passando esse a ser o novo P_{atual}
 12. Voltar ao passo 6 enquanto $(P_{atual} \neq P_{final})$
 13. Determinar qual a identificação da zona do edifício que coincide com $zona(P)$:
 - (i) Z_{teste} = primeira zona da **lista de zonas** do edifício
 - (ii) $IDzona(P) = NULL$
 - (iii) Comparar $zona(P)$ com Z_{teste} :
 - se $(zona(P) = Z_{teste})$ então
 - $IDzona(P) =$ identificador da zona Z_{teste}
 - fse
 - (iv) Z_{teste} = próxima zona da lista **lista de zonas** do edifício
 - (v) Voltar ao passo (iii) enquanto $((Z_{testes} \neq NULL) \text{ E } (IDzona(P) = NULL))$
 14. Devolver $IDzona(P)$

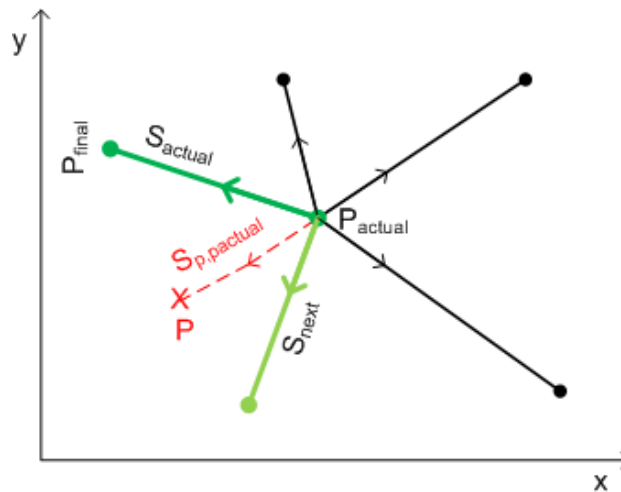


Figura 35 - Ilustração do funcionamento do algoritmo que calcula a zona numa localização P , em especial a definição da vizinhança $S_{viz}(P_{atual})$.

5.3.3. Algoritmo para calcular a localização duma etiqueta RFID

Apresenta-se nesta secção o algoritmo utilizado para calcular a localização de uma etiqueta RFID, com base nos valores estimados para a distância a que ela se

encontra de 3 APs, em que a localização desses APs é conhecida. O princípio em que se baseia o algoritmo é apresentado na Figura 37.

Algoritmo **CalcularLocalizacaoTag()** \equiv

Parâmetros de entrada:

- posição de 3 APs, dum mesmo conjunto de APs, que detetaram a etiqueta RFID (AP_i, AP_j, AP_k);
- valor do RSSI, em dBm, medido por cada um dos 3 APs que detetaram a etiqueta RFID (d_i, d_j, d_k);

Devolve:

- ponto **P**, calculado por trilateração, como sendo a localização da etiqueta RFID.
1. De entre os 3 APs que detetaram a etiqueta RFID, calcular o AP que se encontra mais próximo da etiqueta RFID $\Leftrightarrow d_{min} = \text{mínimo}(d_i, d_j, d_k)$
 2. Calcular os 2 pontos de interceção entre a circunferência de raio mínimo ($d_{min} = d_j$) e uma das outras duas circunferências ainda não usadas ($P1_{j,i}$ e $P2_{j,i}$). Estes 2 pontos definem o segmento de reta $S_{j,i}$.
 3. Calcular os 2 pontos de interceção entre a circunferência de raio mínimo (d_{min}) e a outras circunferência ainda não usada ($P1_{j,k}$ e $P2_{j,k}$). Estes 2 pontos definem o segmento de reta $S_{j,k}$.
 4. Aproximar a localização de etiqueta RFID pelo ponto de interceção entre os 2 segmentos de reta $S_{j,i}$ e $S_{j,k} \rightarrow$ ponto **P**.
 5. Devolver o ponto de interceção **P**.

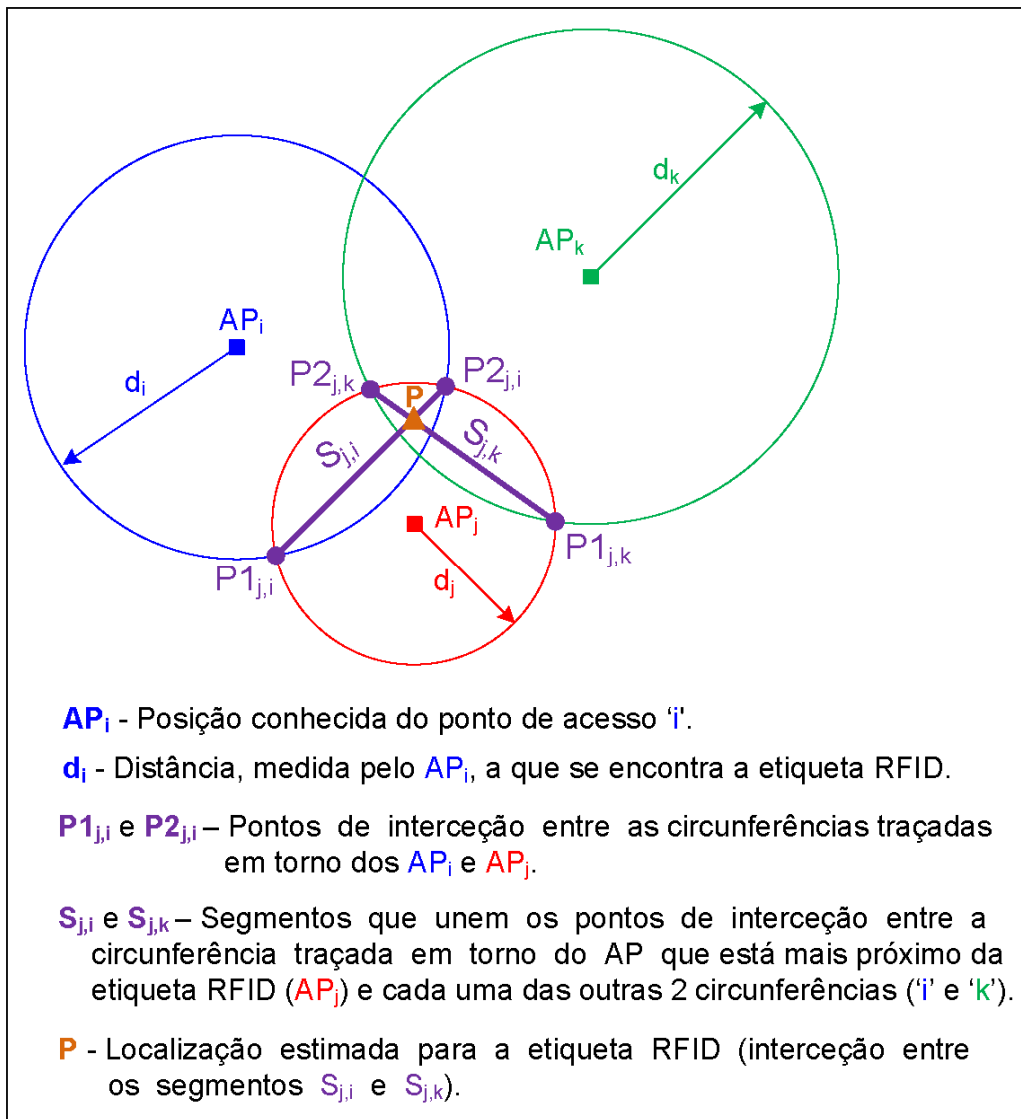


Figura 36 - Fundamento do algoritmo utilizado para calcular a localização duma etiqueta RFID

5.3.4. Algoritmo para calcular a interseção entre duas circunferências

Este algoritmo, utilizado no algoritmo de localização duma etiqueta RFID, permite calcular os pontos de interseção entre duas circunferências, com centros em $A \equiv (x_A, y_A)$ e $B \equiv (x_B, y_B)$ e raio r_A e r_B (ver Figura 37) [30]. O número de pontos de interseção pode ser 0, 1 ou 2. Definindo d como a distância entre os centros das 2 circunferências [30], o seu valor é:

$$d^2 = (x_B - x_A)^2 + (y_B - y_A)^2 \quad (\text{Equação 18})$$

Definido Ka como sendo a área do triângulo formado pelos centros das 2 circunferências e um dos pontos de interseção, o seu valor é dado por:

$$K_a = \frac{1}{4} * \sqrt{((rA + rB)^2 - d^2) * (d^2 - (rA - rB)^2)} \quad (\text{Equação 19})$$

Os pontos de interseção $E=(x1,y1)$ e $F=(x2,y2)$ são calculados de acordo com as seguintes expressões:

$$x1 = \frac{1}{2} * (xB + xA) + \frac{\frac{1}{2} * (xB - xA)(rA^2 - rB^2)}{d^2} + \frac{2 * (yB - yA) * K}{d^2} \quad (\text{Equação 20})$$

$$y1 = \frac{1}{2} * (yB + yA) + \frac{\frac{1}{2} * (yB - yA)(rA^2 - rB^2)}{d^2} - \frac{2 * (xB - xA) * K}{d^2} \quad (\text{Equação 21})$$

$$x2 = \frac{1}{2} * (xB + xA) + \frac{\frac{1}{2} * (xB - xA)(rA^2 - rB^2)}{d^2} - \frac{2 * (yB - yA) * K}{d^2} \quad (\text{Equação 22})$$

$$y2 = \frac{1}{2} * (yB + yA) + \frac{\frac{1}{2} * (yB - yA)(rA^2 - rB^2)}{d^2} + \frac{2 * (xB - xA) * K}{d^2} \quad (\text{Equação 23})$$

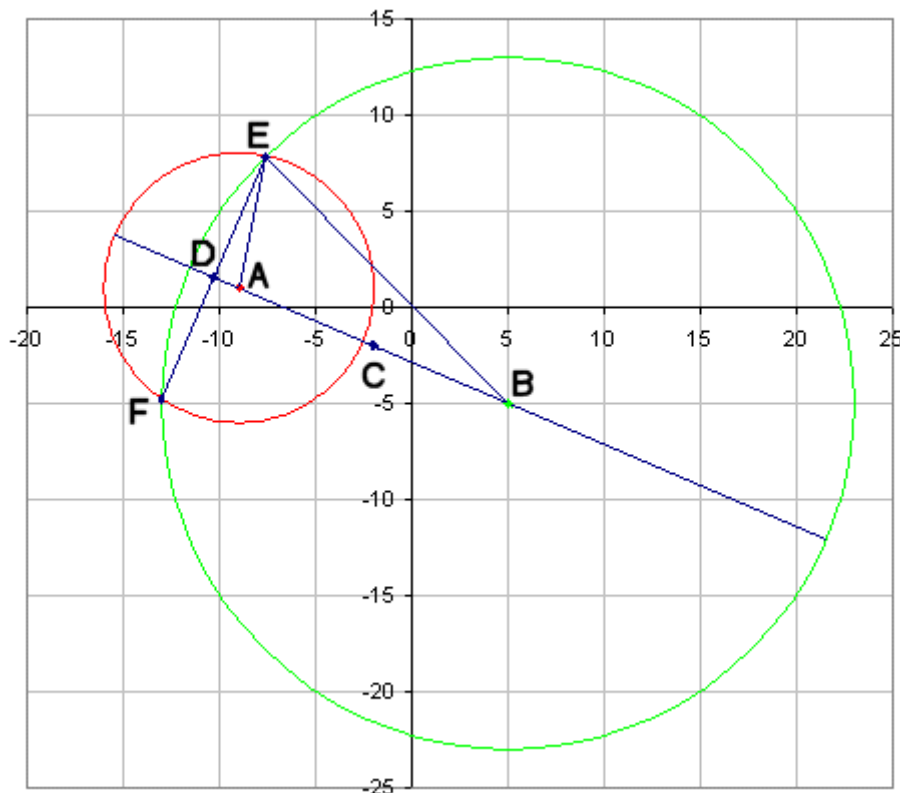


Figura 37 - Ilustração da metodologia utilizada para calcular os pontos de interseção (E e F) entre duas circunferências.

5.3.5. Algoritmo para calcular a interseção entre dois segmentos de reta

Este algoritmo, utilizado no algoritmo de localização duma etiqueta RFID, permite calcular o ponto de interseção $P=(x,y)$ entre dois segmentos de reta (ver a Figura 38) [31]. No caso de os segmentos não se intercetarem ou serem coincidentes, o valor devolvido é nulo. As equações que dão o ponto de interseção em cada um dos segmentos de reta são:

$$P_a = P1 + u_a (P2 - P1) \quad (\text{Equação 24})$$

$$P_b = P3 + u_b (P4 - P3) \quad (\text{Equação 25})$$

Igualando as duas expressões, ou seja $P_a = P_b$, obtêm-se duas equações a duas incógnitas (u_a e u_b):

$$x1 + u_a (x2 - x1) = x3 + u_b (x4 - x3) \quad (\text{Equação 26})$$

$$y1 + u_a (y2 - y1) = y3 + u_b (y4 - y3) \quad (\text{Equação 27})$$

Resolvendo as expressões em ordem a u_a e u_b obtém-se:

$$u_a = \frac{(x4 - x3)(y1 - y3) - (y4 - y3)(x1 - x3)}{(y4 - y3)(x2 - x1) - (x4 - x3)(y2 - y1)} \quad (\text{Equação 28})$$

$$u_b = \frac{(x2 - x1)(y1 - y3) - (y2 - y1)(x1 - x3)}{(y4 - y3)(x2 - x1) - (x4 - x3)(y2 - y1)} \quad (\text{Equação 29})$$

Substituindo as expressões de u_a e u_b na Equação 24 obtemos as coordenadas x e y do ponto de interseção:

$$x = x1 + u_a (x2 - x1) \quad (\text{Equação 30})$$

$$y = y1 + u_a (y2 - y1) \quad (\text{Equação 31})$$

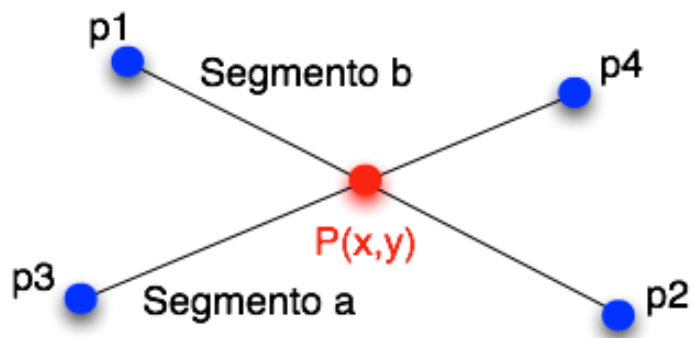


Figura 38 - Interseção entre dois segmentos de reta.

As coordenadas x e y do ponto de interseção P , ponto vermelho na Figura 38, serão calculadas pelo método *CalcIntersept2Lines* da classe *TagLocalization*. Este método devolve o ponto de interseção $P = (x,y)$, ou então devolve o valor *null* quando os segmentos não se intercetam.

5.4. Pontos de Acesso Utilizados

Dada a imensidão dos tipos de recetores (APs), passíveis de ser utilizadas com o sistema desenvolvido neste trabalho, optou-se por orientar a modelação das componentes do sistema que são mais dependentes dos APs, para um KIT RFID específico. Tendo consciência da perda de universalidade do sistema, esta decisão resulta em duas vantagens: contorna as dificuldades envolvidas na modelação de um sistema demasiado abstrato e permite validar o protótipo desenvolvido num cenário real.

O KIT RFID selecionado é fabricado pela SYRIS e o modelo em causa é o SYRD245-1N [25]. Este KIT opera na frequência de 2.45 GHz, possui um recetor (AP) que liga ao sistema central por TCPIP e uma ou várias etiquetas RFID. Um sistema completo poderá incluir vários APs e um número elevado de etiquetas (ver Figura 39).

Convém assim mencionar que a descrição textual de alguns casos de uso foi efetuada tendo em consideração as especificidades deste KIT, concretamente os casos de uso “Receber pacote de AP por TCP/IP”, “Configurar AP” e “Enviar Comando ao AP para Ler a Configuração”. A estes 3 casos de uso do sistema central, acresce a modelação do próprio AP, feita de forma simplista para validar o protótipo, e que como é normal depende do tipo de AP utilizado.

5.4.1. Comunicação entre pontos de acesso e sistema central por TCP/IP

A forma utilizada para comunicar entre os ponto de acesso e o sistema central obedece às regras estabelecidas no protocolo de comunicação designado por TCP/IP (*Transfer Control Protocol/Internet Protocol*). O princípio de funcionamento deste protocolo tem por base a transmissão de dados por pacotes. Deste modo, o TCP (*Transfer Control Protocol*) está encarregue de dividir os dados a transmitir por pacotes, associando-lhes as informações referentes à identidade do aparelho emissor e recetor, procedendo também à sua numeração, para que posteriormente na fase de chegada possam ser reordenados. Adicionalmente, o IP (*Internet Protocol*) é responsável pelo transporte dos pacotes entre a fonte e o destinatário. Entre os pontos de acesso e o sistema central poderão existir nós de interligação (*switches*) que encaminham os dados pelo itinerário mais adequado.

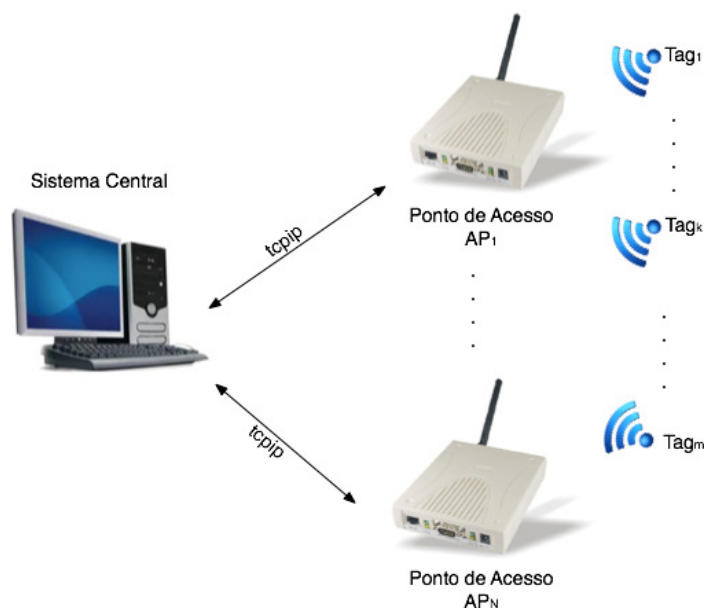


Figura 39 - Arquitetura do hardware utilizada na modelação e validação do sistema desenvolvido.

5.4.2. Comunicação entre etiquetas RFID e pontos de acesso

Iremos agora explicar como funciona a interação entre uma etiqueta RFID e um ponto de acesso. A etiqueta RFID emite periodicamente uma trama identificadora, sendo o intervalo entre tramas configurável pelo utilizador, mas terá um valor que é um

múltiplo do período base (ver Figura 40). O objetivo do envio das tramas é informar os APs da presença da etiqueta no seu raio de ação.

A etiqueta poderá receber informação do AP com o objetivo de a configurar, no entanto, só é permitido receber dados em determinados momentos. O período entre receções sucessivas obtém-se multiplicando o período de emissão pelo contador de receção (ver Figura 40). Geralmente configura-se este tempo com um valor da ordem de grandeza das dezenas de segundo, de forma a diminuir o consumo de bateria.

De salientar ainda que, cada vez que se prime o botão disponível nas etiquetas, estamos a forçar uma emissão. Se premirmos quatro vezes o botão estamos a forçar a ocorrência de uma receção, o que se revela apropriado para obrigar a que a etiqueta receba um comando.

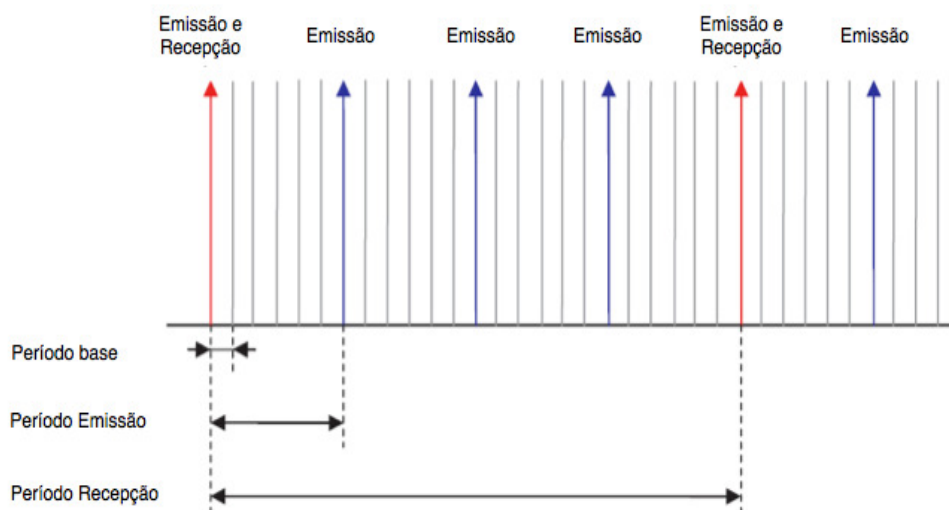


Figura 40 - Comunicação entre um ponto de acesso (recetor) e as etiquetas RFID.

O recetor recebe a informação da etiqueta via sinal RF modulado a 2.45 GHz, processa esta informação segundo a sua configuração, e envia-a para o hospedeiro via RS-232, RS-485 ou *Ethernet*. O hospedeiro ao receber a informação enviada pelo recetor, processa-a convenientemente para identificar o utilizador da etiqueta RFID associado à informação recebida.

5.4.3. Protocolo de comunicação entre ponto de acesso e sistema central

O sistema central recebe/envia pacotes por TCP/IP de/para o AP segundo um dos formatos definidos pelo fabricante. Cada formato de pacote é construído por vários campos, entre os quais se incluem o STX, INS, DATA, BCC, END) [26]. Um exemplo de comando enviado para o AP e da resposta desse AP é:

Comando: STX[01] + INS + { DATA } + BCC + END[0D]

Resposta: STX[02] + INS + { DATA } + BCC + END[0D]

Campo	Descrição
STX	01 (comando) <u>ou</u> 02 (resposta)
INS	Instrução que define a operação pretendida, codificada num único carácter (A, B, ...)
DATA	N bytes de dados <u>ou</u> nada
BCC	<i>Block Check Character (byte hexadecimal adicionado na transmissão para facilitar a deteção de erros na receção, calculado pelo XOR de todos os bytes):</i> STX xor INS xor (DATA1 xor ... xor DATAn)
END	Último campo, o qual termina o formato do pacote e deve assumir o valor hexadecimal 0D .

5.4.4. Protocolo utilizado no caso de uso “Receber pacote de AP por TCP/IP”

No caso de uso “Receber pacote de AP por TCP/IP” o sistema aguarda a receção de pacotes enviados por um ou vários APs ao mesmo tempo. Para isso, o sistema central deve suportar múltiplos fios de execução (*threads*). Neste caso cada *thread* é responsável por enviar comandos e receber pacotes dum dado AP, através dum *socket* específico.

Comando	
Descrição	Enviar um comando ao AP para obter dados de qualquer etiqueta RFID
Formato	STX + INS + BCC + END
Exemplo	[01] + “C” + “xx” + [0D]
Valores	
STX	[01]
INS	“C” (<i>leitura de dados de uma etiqueta</i>)
BCC	“xx” (<i>xx=STX xor INS, em hexadecimal</i>)
END	[0D]

Resposta	
Descrição	Ler o pacote do <i>socket</i> adequado (<u>primeiro passo</u> do caso de uso “Receber pacote de AP por TCP/IP”).
Formato	STX + INS + {Data} + BCC + END
Sucesso 1	[02] + “C” + “xx” + [0D] (<i>sem dados</i>)
Sucesso 2	[02] + “C” + “aaaaaaaaaaaaaaaa” + “bb” + “cc” + “dd” + “xx” + [0D] (<i>Etiqueta Tipo I</i>)
Sucesso 3	[02] + “C” + “aaaaaaaaaaaaaaaa” + “bb” + “cc” + “dd” + “eeee” + “xx” + [0D] (<i>Etiqueta Tipo II</i>)
Sucesso 4	[02] + “C” + “aaaaaaaaaaaaaaaa” + “bb” + “cc” + “dd” + “eeee” + “ffff” + “xx” + [0D] (<i>Etiqueta Tipo III</i>)
Modo de comando	[02] + “C” + “R” + “aaaaaaaaaaaaaaaa” + “g” + “hh” + “ii” + “xx” + [0D]

5.4.5. Protocolo utilizado no caso de uso “Configurar AP”

No caso de uso “Configurar AP” (ver Anexo V Descrição textual dos casos de uso do Sistema Central, secção 13) o sistema envia os dados para o AP com o objetivo de (i) configurar uma etiqueta RFID, (ii) definir o tipo de funcionamento do AP, (iii) definir o tipo de porta a utilizar na comunicação com o AP, (iv) definir o ID da rede em que se insere o AP, (v) definir o nível mínimo de potência do sinal RF (RSSI) para se considerar válida a receção de um pacote. Cada uma das tabelas seguintes está relacionada com a configuração de um destes aspetos.

Como exemplo, apresenta-se na tabela seguinte o formato do comando utilizado para definir o nível mínimo de potência do sinal RF para se considerar válida a receção de um pacote.

Comando para especificar o filtro do nível de RSSI	
Descrição	Definir o nível mínimo de potência do sinal RF (RSSI) para se considerar uma receção válida
Formato	STX + INS + {RSSI level} + BCC + END
Exemplo 1	[01] + “N” + “A0” + “xx” + [0D] (programar)
Exemplo 2	[01] + “N” + “xx” + [0D] (ler)
Valores	
STX	[01]
INS	“N”
RSSI Level	“A0” (<i>nível do sinal é 'A0', em hexadecimal</i>)
BCC	“xx” (<i>xx=01 xor INS xor A0, em hexadecimal</i>)
END	[0D]

5.4.6. Protocolo utilizado no caso de uso “Enviar Comando ao AP para Ler a Configuração”

No caso de uso “Enviar Comando ao AP para Ler a Configuração” o sistema envia um comando ao AP para ler os dados da sua configuração.

Como exemplo, apresenta-se a seguir o formato do comando que indica ao AP o tipo de dados da configuração que se pretende ler (ver Anexo V, com Descrição textual dos casos de uso do Sistema Central).

Comando para indicar ao AP o tipo de dados da configuração que se pretende ler (passo 4 do cenário principal do caso de uso “Enviar comando ao AP para ler configuração”)	
Formato 1	STX + INS + BCC + END
Formato 2	STX + INS + { ID } + BCC + END
Formato 3	STX + INS + { UAddr + UByte } + BCC + END
Formato 4	STX + INS + { UAddr + UByte + UData } + BCC + END
Exemplo 1	[01] + INS + “xx” + [0D] (ler)
Exemplo 2	[01] + “T” + “01” + “xx” + [0D] (“T” ≡ ler o ID da rede do AP)
Exemplo 3	[01] + “U” + “0000” + “04” + “xx” + [0D] (“U” – ler dados do utilizador)
Exemplo 4	[01] + “U” + “0000” + “04” + “12345678” + “xx” + [0D]
Valor do campo INS	
INS (<i>tData</i> no caso de uso)	“C” – Leitura de dados de uma etiqueta “D” – Leitura do S/N da etiqueta “S” – Leitura do S/N do AP “V” – Leitura da versão do <i>firmware</i> do AP “T” – Leitura do ID da rede do AP “U” – Leitura dos dados do utilizador
BCC	“xx” (em hexadecimal)

5.5. Protótipo do Sistema Desenvolvido

O protótipo do sistema desenvolvimento é composto por quatro pacotes, designadamente *AP*, *Start*, *Interface* e *SystemCentral*, os quais foram enquadrados no ambiente de programação NetBeans e no ambiente de modelação UML (ver a Figura 41).

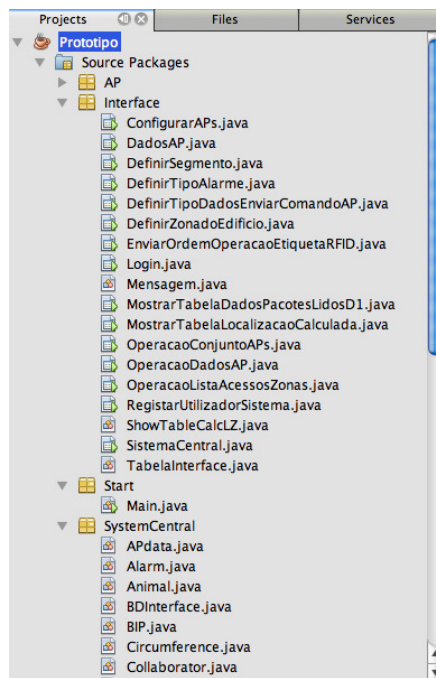


Figura 41 - Estrutura do protótipo do sistema.

Analisando mais especificamente a estrutura do Protótipo, constata-se que o pacote *Start* é utilizado durante a compilação e execução do sistema central. Quanto ao pacote *AP*, corresponde a uma interface que não foi implementada, tendo-se utilizado a API fornecida pelo fabricante do ponto de acesso. No que refere ao pacote *Interface*, cada formulário de dados foi desenhado através do(s) componente(s) *swing* mais indicado(s), de modo a possibilitar ao utilizador a execução de diversas tarefas, como por exemplo: introduzir dados, seleção de opções, clicar botão, entre outras. O pacote *SystemCentral* inclui todas as classes relevantes do modelo de classes, nomeadamente APs, conjuntos de APs, utilizadores de etiquetas RFID, funcionários da empresa, zonas do edifício e classes necessárias para a sua definição, etiquetas RFID, lista de zonas permitidas e interditas, classes para guardar os pacotes recebidos dos APs, e as classes de apoio ao cálculo da localização das etiquetas RFID.

Os pacotes *Start* e *Interface* referidos anteriormente, estão relacionados com o ambiente de programação. Enquanto os pacotes *AP* e *SystemCentral* resultam diretamente dos modelos desenvolvidos para o sistema.

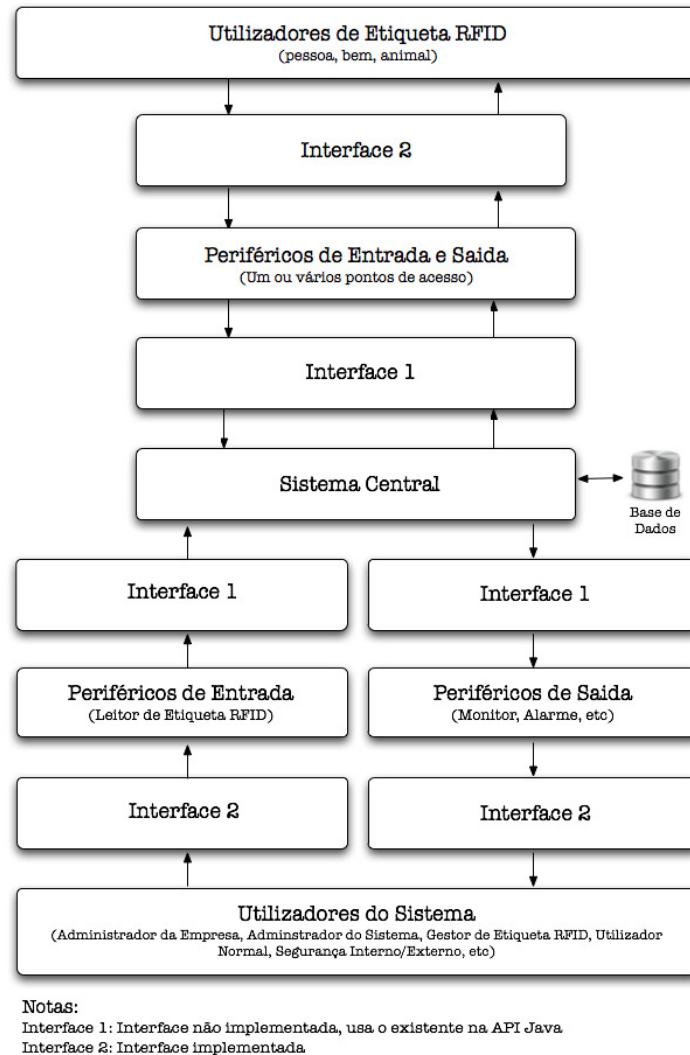


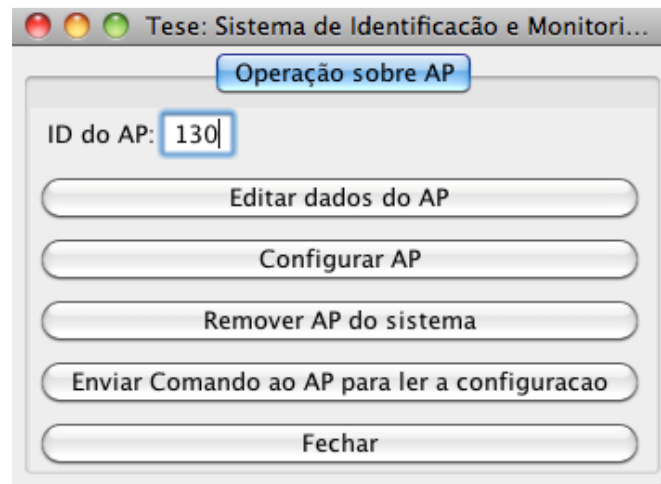
Figura 42 - Arquitetura do protótipo.

Na Figura 42, representa-se a arquitetura de protótipo, em conformidade com o levantamento de requisitos previamente efetuado e com o diagrama de contexto do sistema estruturado em 3 camadas, sendo as funcionalidades da interface devidamente explicadas nas próximas secções deste capítulo.

5.5.1. Operações sobre Pontos de Acesso (APs)

Este formulário de dados permite aceder às principais tarefas que poderão ser efetuadas sobre o(s) ponto(s) de acesso, designadamente, editar os dados do AP,

configurar o AP, remover o AP do sistema e enviar um comando ao AP para que este leia a configuração. No sentido de obter mais detalhes sobre a execução das tarefas associadas a este formulário, poder-se-á consultar o anexo V, mais especificamente as páginas 149, 152, 154, 156 e 164.



The image shows a graphical user interface window. The title bar at the top reads "Tese: Sistema de Identificação e Monitori...". Below the title bar, there is a blue button labeled "Operação sobre AP". Underneath this button is a text input field labeled "ID do AP:" containing the number "130". Below the input field, there are six buttons stacked vertically: "Editar dados do AP", "Configurar AP", "Remover AP do sistema", "Enviar Comando ao AP para ler a configuracao", and "Fechar".

Figura 43 - Formulário referente às operações sobre um AP.

5.5.1.1 Editar os dados dum AP

O formulário aqui apresentado tem por objetivo introduzir os dados relativos a um ponto de acesso, para que o sistema central possa iniciar a comunicação com esse AP. Geralmente, o administrador do sistema preenche os campos referentes às três coordenadas (X,Y,Z), as quais serão posteriormente validadas pelo sistema, o endereço do ponto de acesso, a descrição do AP e o conjunto a que pertence o AP. Seguidamente, será também submetido a validação o endereço do AP. O campo “conjunto do AP” (*apSet*) pode ser preenchido ou deixado vazio. Caso seja introduzido será necessário proceder à criação desse conjunto de APs, o qual possibilitará ficar associado no ID desse AP introduzido. Caso seja selecionado um ID de AP já existente, os dados do AP introduzidos previamente serão lidos para o formulário, de modo a permitir a sua alteração.

The image shows a software window titled "Tese: Sistema de Identificação e Monitorização de Etiquetas RFID". Inside the window, there is a sub-window titled "Editar dados do AP 1". The form contains the following fields and values:

- Coordenada X da localização do AP: 1
- Coordenada Y da localização do AP: 2
- Coordenada Z da localização do AP: 3
- Descrição: AP 1
- Conjunto do AP: (empty)
- Endereço TCP/IP: 192.168.1.101

There are two buttons on the right side of the form: "Fechar" and "Gravar".

Figura 44 – Formulário referente à operação de edição dos dados dum AP.

5.5.1.2 Configurar um AP

O objetivo subjacente a este formulário é proceder à configuração dum AP, através do preenchimento dos vários campos necessário. Os dados introduzidos serão posteriormente enviados para esse ponto de acesso de modo a configurá-lo. Uma vez concluída a transferência dos dados da configuração, o ponto de acesso será imediatamente reiniciado, para que a sua configuração seja concretizada e por questões de segurança. No caso de ocorrer uma falha de comunicação com o AP, e num intervalo máximo previamente definido, o sistema central informa o administrador de que o AP não respondeu ao pedido de configuração efetuado (para mais informações consultar o Anexo V, página 184). Geralmente, o administrador do sistema seleciona o tipo de funcionamento (normal, parar, retornar e *reset*) e o tipo de porta (tcpip, rs-232, rs-485). Seguidamente, será preenchido o campo “nível mínimo de potência do sinal RF”. Se tivermos selecionado o modo “TCP Client Mode”, será preciso introduzir 3 campos: o endereço IP do hospedeiro, a porta do hospedeiro e o valor de *time out*.

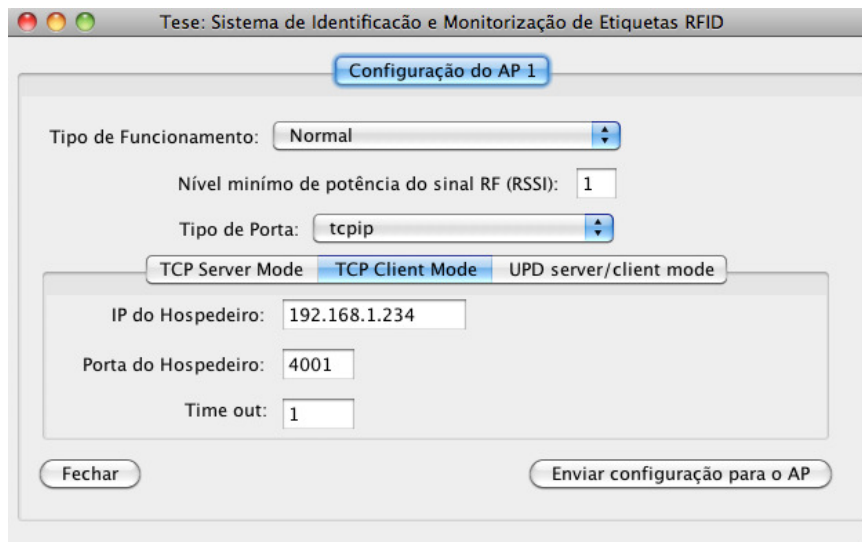


Figura 45 - Formulário referente à operação de configuração dum AP (no modo TCP Client).

5.5.1.3 Enviar um comando ao AP para ler a configuração

O formulário de dados que se apresenta a seguir permite seleccionar o tipo de dados que se pretende ler diretamente do AP, num determinado momento, e enviar o comando respetivo para o AP, no sentido de que este efetue a leitura da configuração. Depois de enviar o comando, o sistema central fica à espera da resposta desse ponto de acesso. Estas tarefas são descritas de um modo mais pormenorizado no anexo V, mais especificamente na página 164.

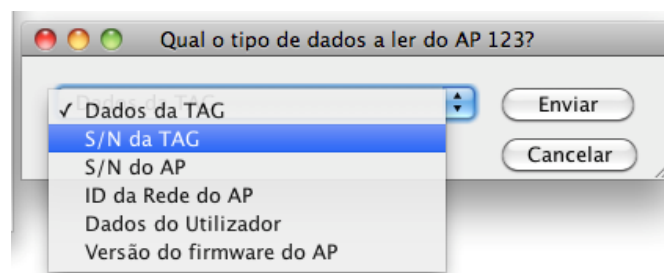


Figura 46 - Formulário relativo ao processo “Enviar um comando ao AP para ler a configuração”.

5.5.1.4 Remover um AP do sistema

Depois de ser seleccionada a tarefa “Remover um AP do sistema” aparece a caixa de diálogo apresentada na Figura 47, a qual tem por objetivo confirmar a eliminação da informação relativa a um AP do sistema (para mais informações consultar a página 156 do Anexo V).

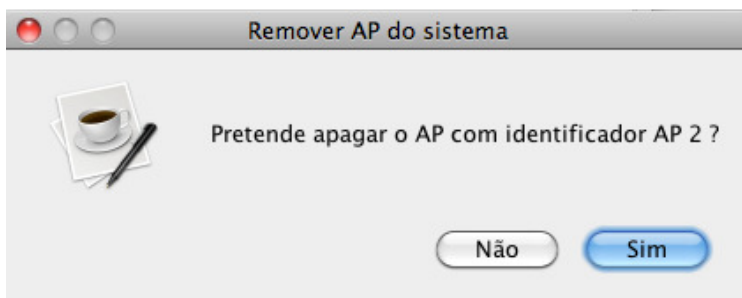


Figura 47 – Caixa de diálogo referente à operação de remover um AP do sistema.

5.5.2. Operações sobre conjuntos de pontos de acesso

O formulário agora apresentado dá acesso à execução das tarefas relacionadas com os conjuntos de pontos de acesso. Ou seja, a partir deste formulário é possível criar, eliminar e listar conjuntos de APS, e adicionar/remover APs a/de um conjunto. A composição de cada conjunto é guardada numa estrutura D7, que por sua vez é inserida na lista D3 (ver a Figura 48). Para obter mais detalhes sobre a execução das tarefas que estão associados a este formulário, deve consultar-se o anexo V, mais especificamente as páginas 160, 162 e 163.

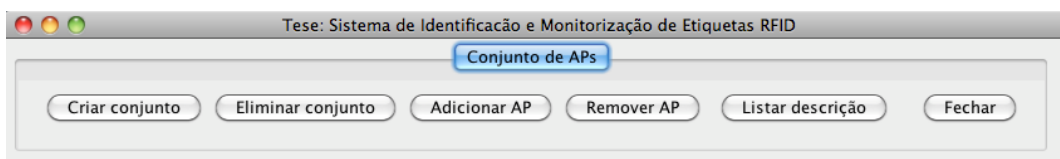


Figura 48 – Formulário utilizado para executar operações sobre conjuntos de APs.

1) Criar Conjunto de APs

Para criar um AP novo basta introduzir o número de identificação único na caixa de diálogo e posteriormente anexar-lhe até 3 APs, com identificadores diferentes, que irão fazer parte desse conjunto. A descrição textual da funcionalidade por trás deste formulário encontra-se no caso de uso “Adicionar AP a um conjunto de APs”, que pode

ser consultada na página 161. Os dados relativos à composição do AP serão guardados numa estrutura D7.

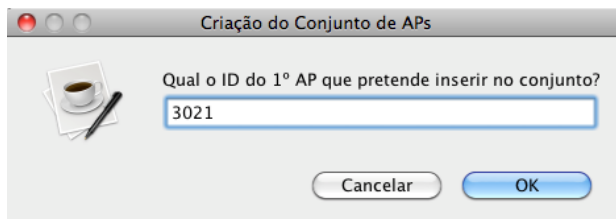


Figura 49 - Formulário de dados referente ao processo de "Adicionar AP a um conjunto de APs" que está a ser criado.

Em princípio, cada conjunto terá uma cardinalidade de três APs, de modo a permitir efetuar a localização de etiquetas RFID por um método de trilateração, conforme o que foi referido no passo 5 do cenário principal da descrição textual "Criar conjunto" e a descrição textual "Adicionar AP a um conjunto de AP's".

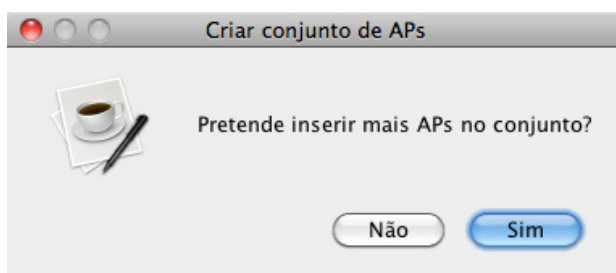


Figura 50 - Formulário de dados referente ao processo de inserção de mais APs no mesmo conjunto.

Após terminar a inserção da identificação dos vários AP do conjunto, o sistema pergunta ao administrador se deseja guardar a composição do conjunto (Ver a Figura 51). Em caso afirmativo, o sistema armazena os dados introduzidos em memória e base de dados.

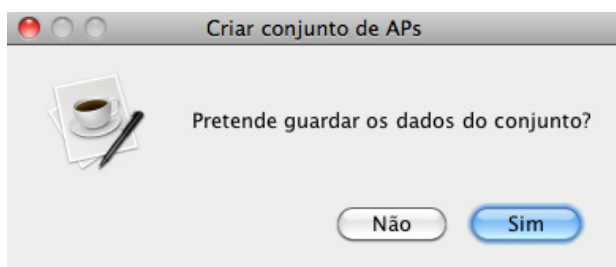


Figura 51 - Caixa de diálogo "Pretende guardar os dados do conjunto?".

2) Adicionar um AP a um dado conjunto de APs

Este formulário permite alterar a composição de um conjunto de APs, após a sua criação. Para o efeito é necessário apenas introduzir a identificação do novo AP que se pretende adicionar ao conjunto (Figura 52) e depois inserir a identificação do conjunto alvo. No entanto, esta operação só estará disponível caso o conjunto de APs tenha menos de 3 elementos.

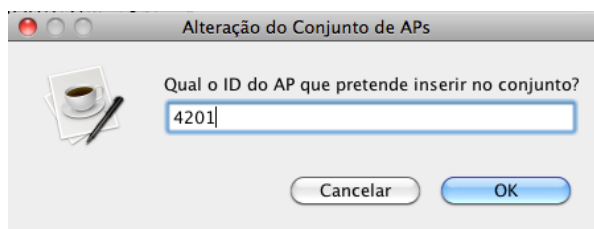


Figura 52 - Formulário de dados referente ao processo de alteração de um conjunto de APs previamente criado.

3) Listar descrição

Esta funcionalidade resume-se a mostrar a composição do conjunto de APs pretendido, ou seja, listar a identificação de cada um dos APs (0 a 3) já adicionados ao conjunto. Quando um lugar do conjunto estiver vazio, surge a indicação “---” em vez do identificador dum AP. Para mais detalhes, pode consultar-se a descrição textual do caso de uso “Listar descrição do Conjunto de APs”, na página 163.

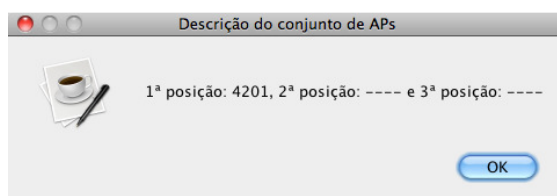


Figura 53 – Caixa de diálogo para mostrar a composição dum conjunto de APs.

5.5.3. Emissão de alertas quando um utilizador de etiqueta RFID entra numa zona interdita

Nesta caixa de diálogo é disponibilizada a lista de utilizadores de etiqueta RFID que tenham entrado numa zona interdita. Esta lista é atualizada sempre que se calcula a localização de um ou mais utilizadores. Na interface desenhada esta lista surge com designação “Emissão de alertas (utilizador de etiqueta RFID em zona interdita)” (ver a Figura 54).

Caso a localização do utilizador num dado momento corresponda a uma zona interdita, e o mesmo se encontre por isso em situação de violação, o sistema consulta a prioridade dos diferentes tipos de alarme associados a esse alerta (nomeadamente, sirene, BIP e telemóvel). Imediatamente a seguir, o sistema envia aos seguranças um alerta do tipo prioritário para essa situação específica.

DescrUtilizador	DescrZona	Alarma 1	Alarma 2	Alarma 3
Figo	Sala 1	Sinere 30s	Seg. Externa	Seg. Interno
Fatima	Sala 1	Sinere 30s	Seg. Externa	Seg. Interno
Fatima	Sala 1	Sinere 30s	Seg. Externa	Seg. Interno
Fatima	Sala 1	Sinere 30s	Seg. Externa	Seg. Interno
Fatima	Sala 1	Sinere 30s	Seg. Externa	Seg. Interno

Figura 54 - Seção da interface do protótipo relativa à emissão de alertas.

5.5.4. Criar e gerir utilizadores do sistema, incluindo administrador do sistema

O formulário apresentado nesta secção tem por finalidade introduzir os dados de autenticação dum novo utilizador, onde se inclui seleccionar o tipo/perfil de utilizador. As funcionalidades permitidas a cada utilizador dependem do seu perfil. No final do processo, ou seja, após o preenchimento dos campos necessários (os quais poderão ser visualizados na Figura 55), o administrador do sistema deverá premir “Registar” por forma a guardar a informação em base de dados.

Figura 55 - Formulário relativo ao registo dum utilizador do sistema.

5.5.5. Autenticação de um utilizador registado

O formulário ilustrado na Figura 56 permite a um utilizador registado autenticar-se perante o sistema. Com base nos dados introduzidos o sistema verifica as credenciais e ativa as funcionalidades correspondentes a esse tipo de utilizador. Um utilizador não registado não terá acesso a qualquer funcionalidade, para além de se tentar autenticar.

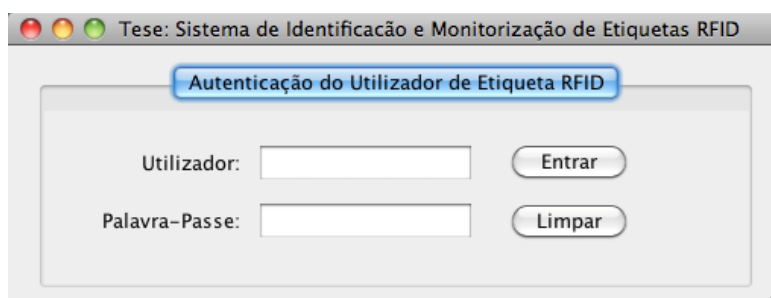
The image shows a software window titled "Tese: Sistema de Identificação e Monitorização de Etiquetas RFID". Inside the window, there is a sub-header "Autenticação do Utilizador de Etiqueta RFID". Below this, there are two input fields: "Utilizador:" and "Palavra-Passe:". To the right of the "Utilizador:" field is a button labeled "Entrar". To the right of the "Palavra-Passe:" field is a button labeled "Limpar".

Figura 56 - Formulário para um utilizador registado se autenticar perante o sistema.

5.5.6. Definir as zonas dum edifício

A interface apresentada nesta secção tem por objetivo ajudar a definir a geometria das zonas dum edifício. Para isso, começa-se por introduzir o número de identificação da zona a criar (ver a Figura 58), o qual será validado para garantir que não há várias zonas com o mesmo identificador. Posteriormente é necessário definir um conjunto de segmentos, em número de três ou mais, que delimitam a zona. Para mais detalhes deve consultar-se o caso de uso “Definir segmentos”, na página 47.

Um segmento é definido à custa de dois pontos, o ponto inicial e o ponto final. Na prática não há diferença substantiva entre os dois tipos de ponto, utilizando-se nomes diferentes apenas para os diferenciar no texto e para ajudar a definir as zonas fechadas (ver a Figura 57). Cada ponto é definido pelas coordenadas X, Y e Z. Como facilmente se constata, a Figura 57 ilustra uma zona retangular/quadrada definida à custa dos segmentos 1 a 4, que por sua vez são definidos com base nos 4 pontos P_a , P_b , P_c e P_d .

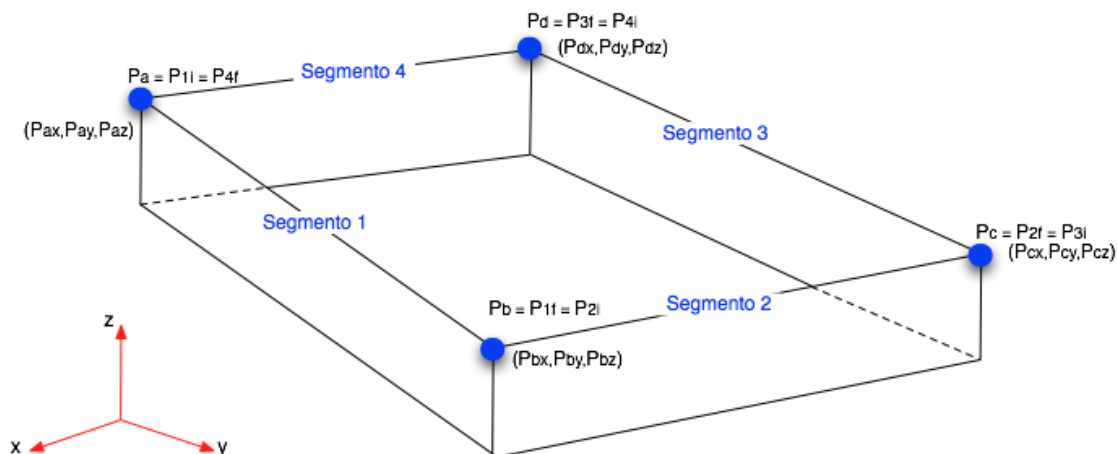


Figura 57 – Esquema ilustrativo da definição de uma zona dum edifício.

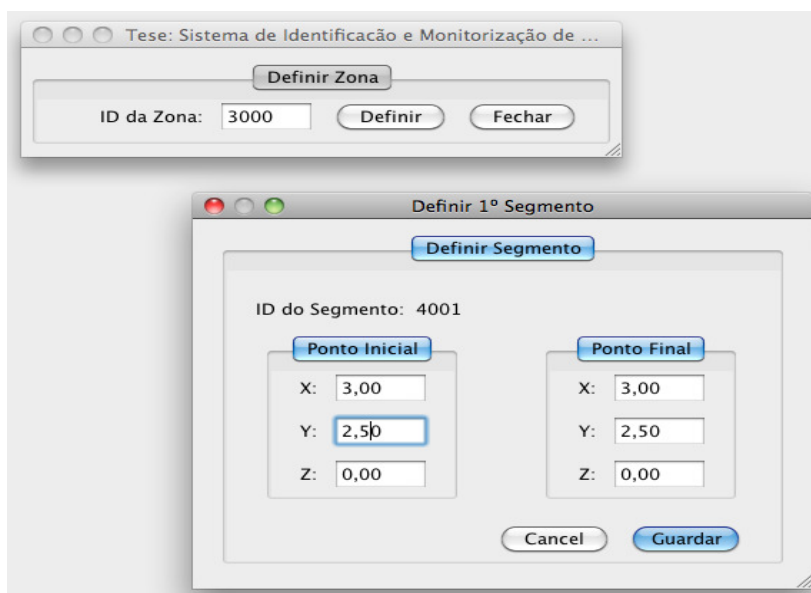


Figura 58 - Interface utilizada para definir uma zona dum edifício.

5.5.7. Criar e gerir as listas de zonas dum edifício permitidas e interditas a cada tipo de utilizador

A interface com o utilizador abordada nesta secção tem por objetivo, dado um tipo de utilizador (*tu*) selecionado, criar ou atualizar as listas de zonas permitidas e interditas a esse tipo de utilizador (ver Figura 59).

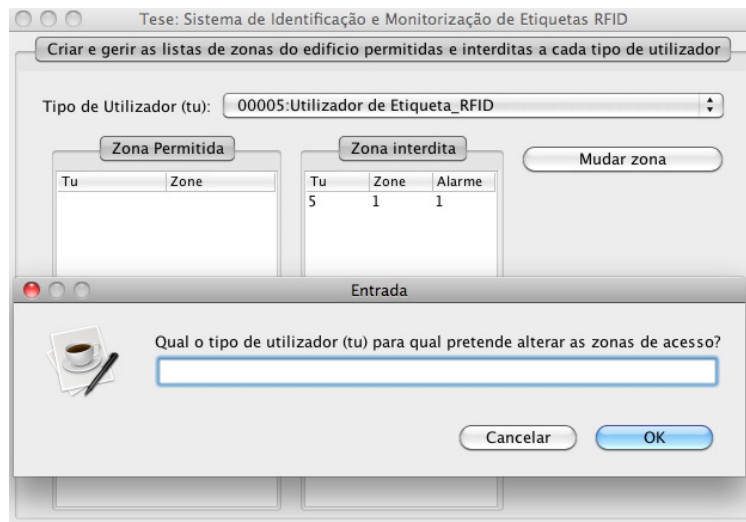


Figura 59 - Interface concebida para criar e alterar as listas de zonas permitidas e interditas do edifício.

A opção “Mudar zona”, disponível na caixa de diálogo, permite trocar uma zona entre a lista “permitida” e a lista “interdita”. Para isso, primeiro introduz-se a identificação do tipo de utilizador (*tu*) a que diz respeito a troca. Também se pode introduzir a identificação da zona a mudar de lista. Quando se especifica uma zona como sendo interdita, é preciso indicar até três tipos de alerta a emitir quando essa interdição for violada (ver Figura 60). Para mais detalhes ver a descrição textual dos casos de uso incluídos no anexo V, páginas **142 e 144**.

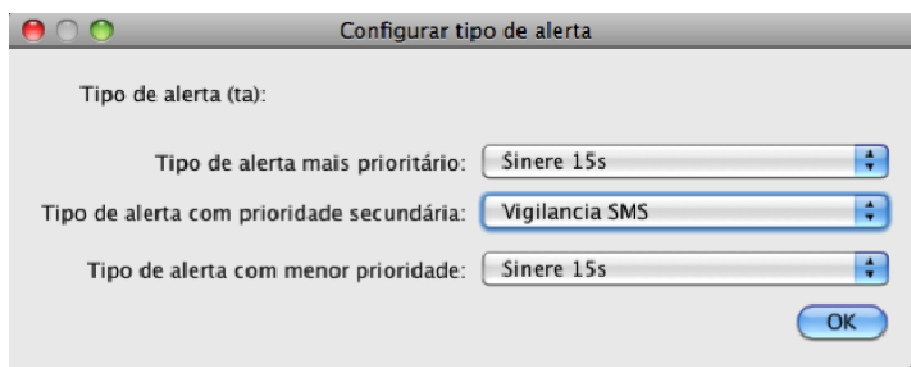


Figura 60 - Formulário referente ao processo “Configurar tipo de alerta”.

5.5.8. Operações sobre etiquetas RFID: atribuir, recolher e listar etiquetas atribuídas

A interface aqui apresentada permite efetuar as interações implícitas na descrição textual dos vários casos de uso contidos no diagrama de casos de uso “Enviar ordem para efetuar uma operação sobre a etiqueta” (Ver o Anexo V). As três operações que esta interface permite efetuar são: atribuir etiquetas, recolher etiquetas e listar as etiquetas atribuídas aos utilizadores. Para efetuar a atribuição é necessário seleccionar o tipo de utilizador – pessoa, animal, bem – e introduzir os seus dados. No campo “SN da TAG” introduz-se o número de série da etiqueta a atribuir, o qual funciona como identificação dessa etiqueta. Ao clicar-se no botão “Registrar atribuição da etiqueta RFID” é registada a associação (*etiqueta, utilizador, tipo de utilizador*) na base de dados.

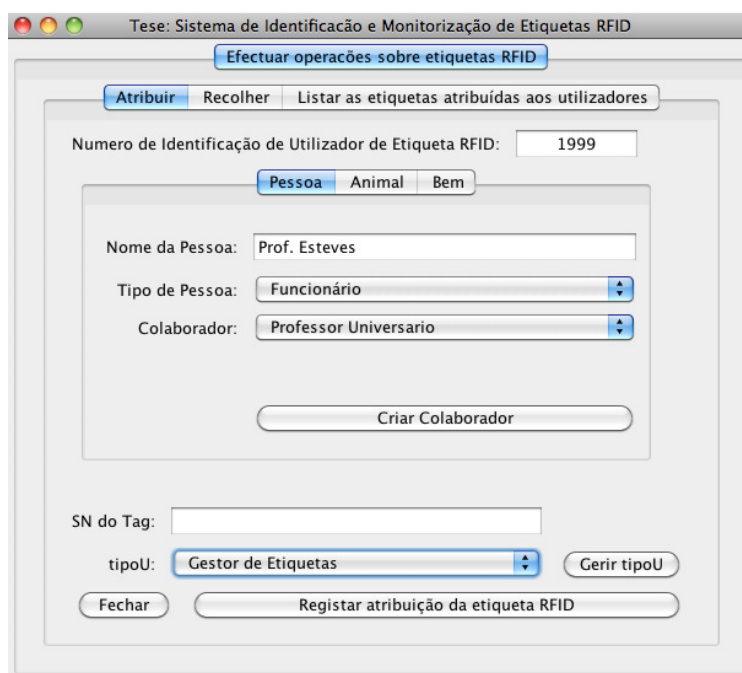


Figura 61 – Caixa de diálogo para registar a atribuição dum etiqueta RFID a um utilizador.

Quando se escolhe a operação de recolher uma etiqueta RFID o sistema mostra uma caixa de diálogo que permite introduzir o número de identificação do utilizador que pretende devolver uma etiqueta RFID previamente entregue (ver Figura 62). Nesta fase de desenvolvimento do protótipo, a recolha é manual mas poderá ser feita através de um leitor de etiquetas RFID. Depois de introduzir o número de identificação do utilizador, resta apenas clicar no botão “Remover atribuição da etiqueta RFID” para que o sistema

elimine a correspondente associação (etiqueta, utilizador, tipo de utilizador) da base de dados.

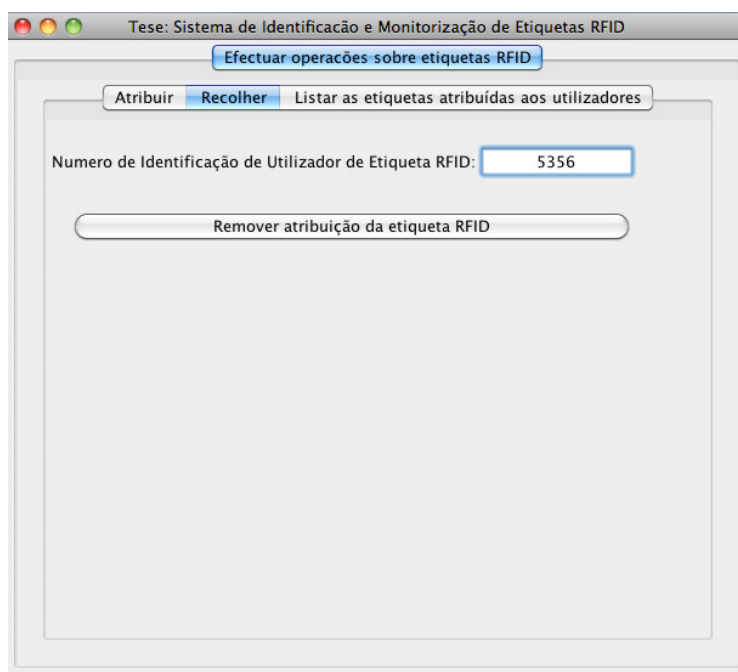


Figura 62 - Caixa de diálogo para registar a recolha dum etiqueta RFID entregue a um utilizador.

5.5.9. Localizar utilizadores de etiqueta RFID

Para calcular a localização dos utilizadores de etiqueta RFID é preciso implementar o caso de uso “Receber pacote de AP por TCP/IP”, que por sua vez precisa dos casos de uso “Guardar pacote recebido dum AP”, “Calcular localização dum Tag” e “Calcular zona de localização”, documentados no anexo V. Como foi descrito no resumo dos casos de uso, cada pacote recebido pelo sistema central a partir dum AP é colocado numa estrutura *packet* (D1). Posteriormente, este pacote é inserido na lista que contém os pacotes relativos à última posição de cada etiqueta RFID (*PacksLastPosTAG/D5*). Para cada etiqueta, identificada pelo valor de *TagID*, a interface desenvolvida mostra o identificador dos 3 últimos pacotes recebidos dessa etiqueta: colunas *Packet1*, *Packet2* e *Packet3* na Figura 63. Sempre que um AP recebe um pacote a lista D5 é atualizada.

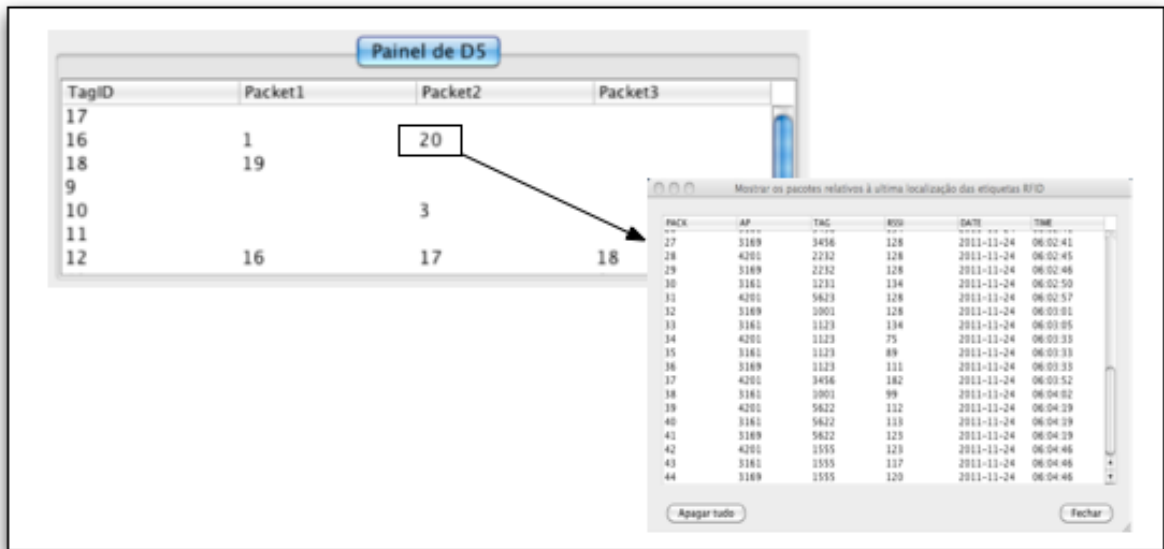


Figura 63 – Interface com o utilizador que mostra o conteúdo da lista PacksLastPosTAG (D5).

Na interface que mostra o conteúdo da lista D5 (Figura 63), quando se clica numa coluna abre uma nova janela que apresenta todos os pacotes recebidos em qualquer etiqueta RFID, como se pode ser na Figura 64.

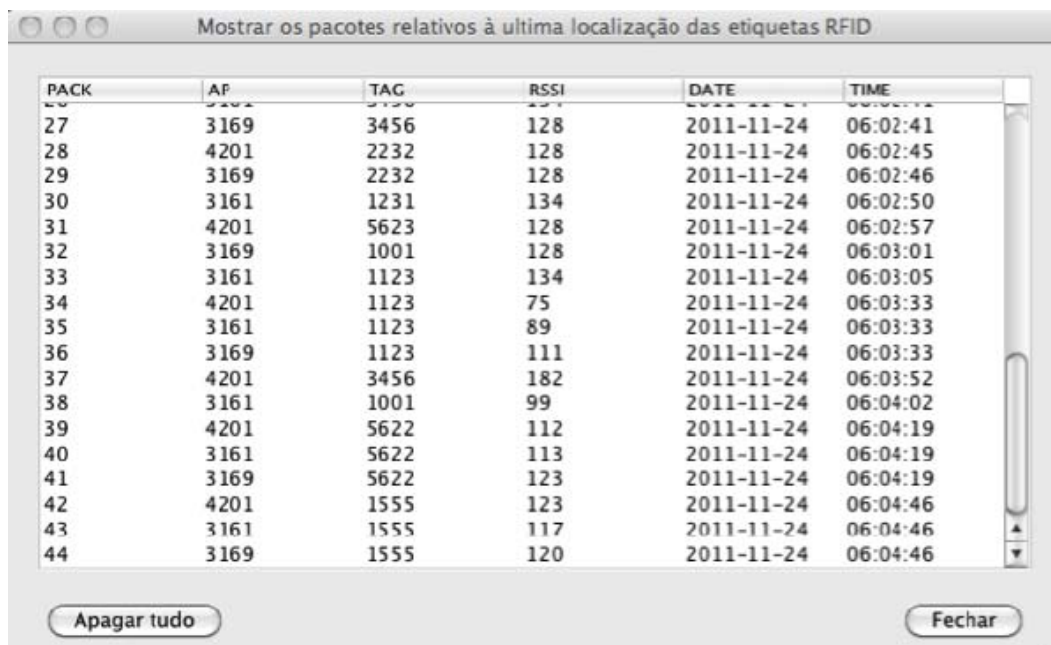


Figura 64 – Interface que mostra ao utilizador informação sobre os últimos pacotes recebidos.

Após calcular a localização de um utilizador de etiqueta RFID, tendo por base a trilateração de informação contida em 3 pacotes provenientes da mesma etiqueta e

detetados em 3 APs do mesmo conjunto, é calculada a zona do edifício a que corresponde essa localização. A informação gerada, e que é a mais relevante para o sucesso deste projeto, é mostrada ao utilizador através da interface apresentada na Figura 64. Como se pode observar nesta figura, para cada evento de localização é mostrada a identificação da etiqueta localizada e do seu portador, a descrição do utilizador, a localização (x,y,z) estimada para esse utilizador, a identificação e a descrição a zona do edifício em que se situa essa localização, a data e a hora em que ocorreu o evento. A lista de localizações é atualizada sempre que algum os APs detetem alterações na localização de um ou mais utilizadores.

The screenshot shows a window titled "Localização de Etiqueta RFID" containing a table with the following data:

Date	Time	TAG ID	User ID	UserDescription	X,Y,Z	Zone ID	ZoneDescri...
2011-11-21	12:47	5623	67	João Miguel Fernandes	(-0.0,6.0,0.0)	3001	Sala 1
2011-11-21	12:47	3456	69	Mauro Nuno Barbosa de Castro	(-0.0,6.0,0.0)	3001	Sala 1
2011-11-21	12:47	5622	68	Antonio Joaquim Esteves	(-0.0,6.0,0.0)	3001	Sala 1

Below the table, there is a button labeled "Mostrar alguns detalhes relativos aos cálculos envolvidos na estimação da localização de etiquetas RFID".

Figura 65 – Interface com o utilizador que mostra informação sobre a localização de utilizadores de etiqueta RFID.

5.5.10. Simular o envio de pacotes para se efetuar a trilateração entre medições de RSSI

O objetivo desta funcionalidade, incluída no protótipo desenvolvido, é simular (i) o envio de um pacote a partir duma etiqueta RFID, (ii) a correspondente deteção em 1 a 3 pontos de acesso virtuais: AP_X, AP_Y e AP_Z, (iii) a receção dos pacotes no Sistema Central. Esta funcionalidade justifica-se pelo facto de só estar disponível um ponto de acesso.

Tendo em vista obter mais detalhes relativos aos cálculos envolvidos na estimação da localização de etiquetas RFID, além da informação que interessa ao

utilizador final do sistema (Figura 65), implementou-se mais uma interface essencialmente vocacionada para quem desenvolveu o protótipo (ver Figura 67). Para cada evento de deteção presente na Figura 65, esta interface mostra a localização dos 3 APs que detetaram a etiqueta em causa, a potência do sinal recebido nesses APs (o valor entre [0:255] que vem nos pacotes e o valor em dBm), a distância estimada a que se encontra a etiqueta de cada um dos 3 APs, e finalmente a localização de etiqueta estimada por trilateração. Quando não é possível concluir com sucesso a trilateração, na coluna relativa à localização estimada indica-se o motivo da falha. As 3 situações em que o método de trilateração implementado falha são: (i) um ou os dois pares de circunferências intercetam-se em apenas um ponto; (ii) um ou os dois pares de circunferências não se intercetam; (iii) os segmentos de reta que resultaram dos pontos de interceção dos 2 pares de circunferências não se intercetam ou são coincidentes.

Simular o envio de pacotes para se efectuar a trilateração entre medições de RSSI

Definir TAG_ID igual para AP_X, AP_Y e AP_Z: 05622: Antonio Joaquim Este... ▾

Definir AP_ID para AP_X, AP_Y e AP_Z: 00001,X:4201,Y:3161 e Z:3169 ▾

Definir distância para AP_X, AP_Y e AP_Z: 5 m

AP_X

ID_AP: 4201 ▾ ID da Etiqueta RFID: 5622 ▾ RSSI: 128

Simular envio de pacote a partir duma Tag, via AP_X, para o Sistema Central

AP_Y

ID_AP: 3161 ▾ ID da Etiqueta RFID: 5622 ▾ RSSI: 134

Simular envio de pacote a partir duma Tag, via AP_Y, para o Sistema Central

AP_Z

ID_AP: 3169 ▾ ID da Etiqueta RFID: 5622 ▾ RSSI: 128

Simular envio de pacote a partir duma Tag, via AP_Z, para o Sistema Central

Simular envio de pacote duma Tag, via AP_X e AP_Y e AP_Z, para o Sistema Central

Figura 66 - Interface com o utilizador que permite simular o envio de pacotes para se efectuar a trilateração entre medições de RSSI.

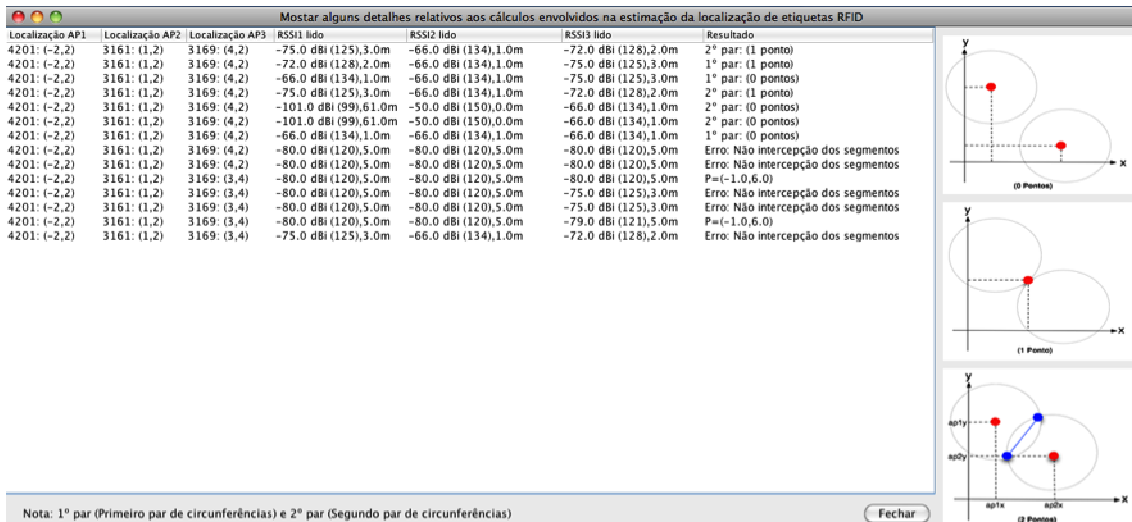


Figura 67 – Interface que mostra alguns detalhes relativos aos cálculos envolvidos na estimação da localização de etiquetas RFID.

A Figura 68 exemplifica os 3 cenários que podem ocorrer na interseção de cada um dos 2 pares de circunferências: (i) o par de circunferências não se interceta, (ii) o par de circunferências interceta-se em apenas 1 ponto e (iii) o par de circunferências interceta-se em 2 pontos. O cenário (iii) é o único que permite o algoritmo de localização implementado ter sucesso. Convém lembrar que cada circunferência está centrada num AP e tem um raio igual à distância a que se estima que a etiqueta RFID esteja desse AP.

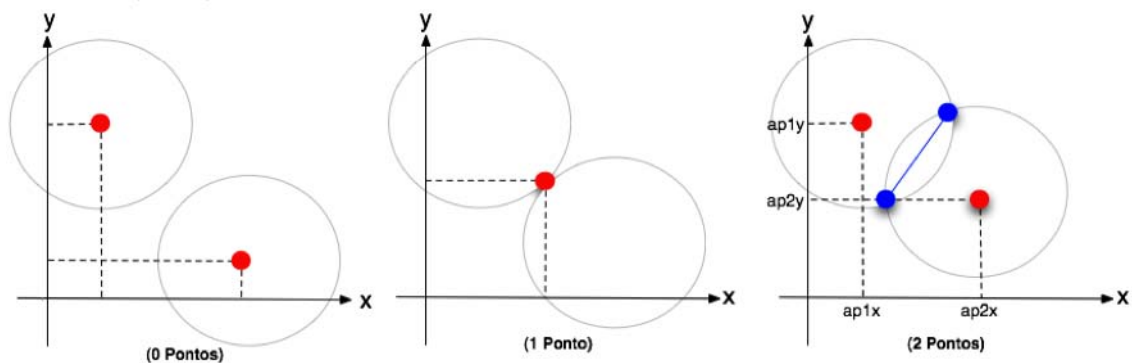


Figura 68 – Cenários que podem ocorrer no cálculo da localização duma etiqueta, no que diz respeito à interseção dum par de circunferências.

Capítulo 6 Testes Efetuados e Resultados

No presente capítulo serão detalhados os procedimentos seguidos nos testes do protótipo do sistema de localização de etiquetas RFID efetuados neste trabalho. Assim, vão ser apresentados: (i) o equipamento de *hardware* utilizado nos testes, (ii) o processo de calibração do equipamento, de modo a que ele possa ser utilizado no teste do protótipo com a maior correção possível, (iii) as decisões tomadas antes de execução dos testes, (iv) os resultados obtidos com a calibração do equipamento e (v) a funcionalidade do protótipo especialmente criada para facilitar os testes, ou seja, o simulador de envio de pacotes a partir de etiquetas RFID.

6.1. *Hardware* utilizado nos testes

As experimentações e testes realizados no âmbito desta dissertação foram todos realizados com um KIT RFID disponível e que inclui um recetor **Syris SYRD245-1N** uma etiqueta RFID ativa **SYTAG245-TM**. O recetor possui uma antena omnidirecional com um ganho de 1,8 dBi. Com este equipamento, os valores de RSSI que se podem obter no recetor estão na gama 0 a 255. Contudo em termos práticos, os valores que se consegue obter encontram-se na gama 80:200. O valor máximo de 200 foi usado no protótipo para converter os valores de RSSI na gama 0:255 para valores de RSSI em milidecibéis.

6.2. Calibração do *hardware* utilizado nos testes

A primeira fase dos testes teve como objetivo calibrar o sistema RF formado pelo conjunto emissor e recetor mencionado na seção anterior. Neste caso, a calibração consistiu em determinar o valor de K utilizado no modelo de propagação de rádio e que nos permite obter (i) o valor do RSSI em dBm em função da distância (Equação 2) ou (ii) o valor da distância em função do RSSI em dBm (Equação 3).

Numa fase inicial, efetuaram-se os testes de calibração numa sala do Departamento de Informática, na Universidade do Minho. Após realizar diversas medições, com várias distâncias e direções entre emissor (etiqueta RFID) e recetor (AP), constatou-se que para as mesmas condições experimentais as medições do RSSI apresentavam uma variação significativa. Tal facto deve-se essencialmente (i) à existência de vários equipamentos emissores de RF na zona (portáteis com Wi-Fi, telemóveis, etc.) e (ii) a ocorrerem reflexões em paredes e outros obstáculos. Olhando

em mais detalhe para os resultados obtidos neste cenário, verificou-se que para distâncias emissor-recetor inferiores a 1 metro, as medições de RSSI registadas para as mesmas posições do emissor e do recetor apresentavam pouca diferença entre si. No entanto, a partir de 1 metro de distância entre emissor e recetor, a variação das sucessivas medições do RSSI era considerável. Ou seja, para distâncias perto do nosso emissor, o seu sinal era predominante, mas para distâncias maiores os sinais emitidos por outras fontes causavam interferências relevantes.

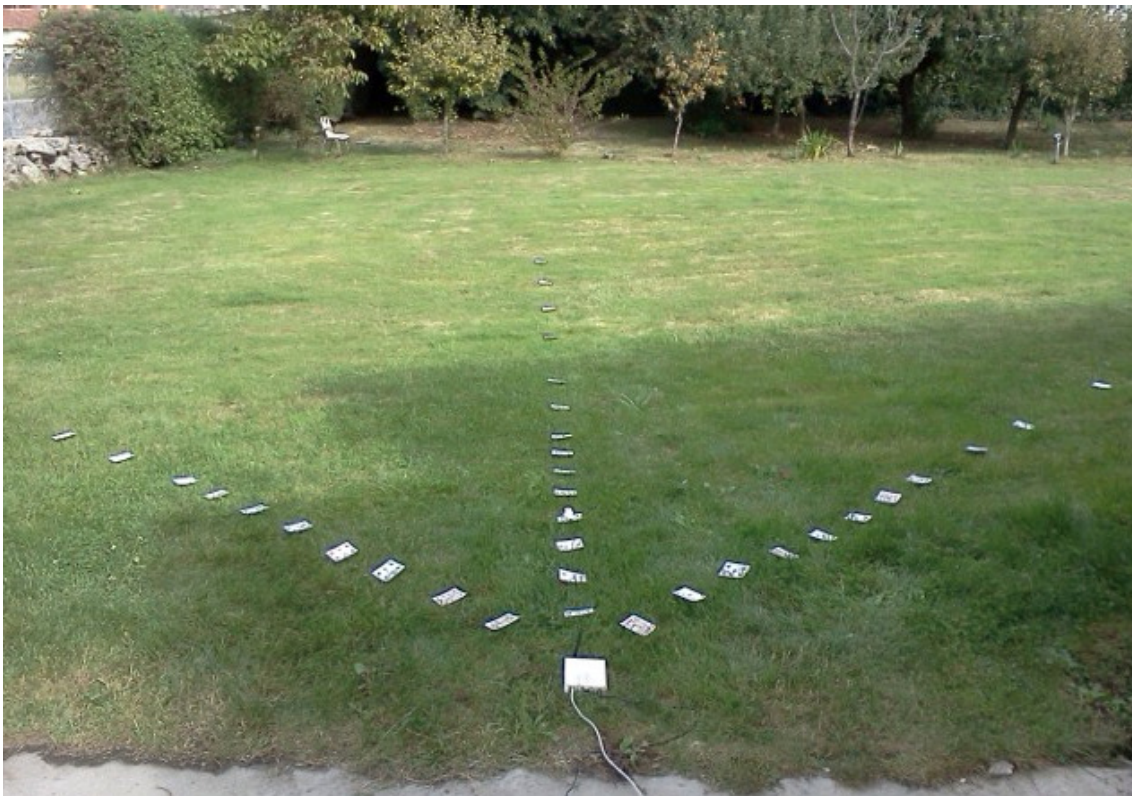


Figura 69 – Medição de RSSI no recetor, com a etiqueta RFID emissora colocada em diferentes distâncias e ângulos (posições assinaladas por uma carta na figura).

Em consequência dos resultados descritos atrás, decidiu-se prosseguir os testes de calibração num campo ao ar livre com a dimensão de pelo menos 10x10 metros quadrados (ver a Figura 69). Optou-se por um local como o referido, devido à sua dimensão e ao facto de ser uma zona sem obstáculos e onde existiriam poucas interferências de sinais RF. Deste modo, minimizou-se a sobreposição de sinais RF no recetor (AP), pelo facto de não existirem reflexões do sinal RF emitido pela etiqueta RFID e por não existir sinal RF proveniente de outros emissores. Para realizar os testes, foi usado o recetor **Syris SYRD245-1N** ligado por TPC/IP a um computador MacBook Pro. Foram feitas medições com a etiqueta RFID localizada a distâncias que variaram

entre 0,25 e 7 metros. De referir que entre os 0,25 e os 3 metros as medições foram efetuadas em intervalos de 0,25 metros. Enquanto entre os 3 e os 7 metros o intervalo entre as medições realizadas aumentou para 1 metro. Para além de se ter feito variar a distância, foram igualmente registadas medições para diferentes ângulos: 45°, 90° e 135°. Realizaram-se medições com 3 ângulos distintos para confirmar que a antena do recetor era mesmo omnidirecional. Os resultados obtidos serão apresentados na próxima secção.

6.3. Resultados da calibração do *hardware* usado nos testes

Tal como foi afirmado anteriormente, foram feitas medições de RSSI para distâncias recetor-emissor no intervalo 0,25 a 7 metros e para 3 direcções recetor-emissor: 45, 90 e 136 graus.

As medições de RSSI, na gama 0:255 e em dBm, podem ser consultadas na 2ª e 3ª colunas da Tabela 3 (45°), Tabela 4 (90°) e Tabela 5 (135°).

Com o objetivo de verificar se as medições de RSSI seguem o padrão definido pelo modelo de propagação teórico, que é habitualmente usado como referência e se traduz na Equação 3, foi traçado um gráfico do $RSSI_{dBm}$ medido em função da distância medida (Figura 70, Figura 72 e Figura 74). Embora os valores apresentem uma dispersão razoável é possível ver pelas linhas traçadas que os dados seguem uma tendência logarítmica como é definido pela Equação 3.

A coluna 4 e 5 de cada uma das 3 tabelas, cálculo de d^2 e $\log_{10}(d^2)$, são valores intermédios necessários para calcular o valor de K através da Equação 6. O valor de K obtido com a Equação 6, em cada uma das 3 direcções, foi:

- $K=6.9 \times 10^{-9}$ (para 45°)
- $K=3.0 \times 10^{-9}$ (para 90°)
- $K=1.5 \times 10^{-9}$ (para 135°).

Utilizando o valor de K agora calculado e as medições de $RSSI_{dBm}$, a Equação 3 permite estimar um valor para cada uma das distâncias. Os resultados desse cálculo são apresentados na 6ª coluna da Tabela 3, Tabela 4 e Tabela 5. A última coluna destas 3 tabelas mostra o erro relativo entre a distância medida (coluna 1) e a distância calculada (coluna 6). Como se pode verificar, os erros são bastante significativos:

Ângulo = 45 graus						
Distância medida (d)	RSSI Médio (0:255)	RSSI Médio (dBm)	Quadrado da distância (d ²)	log10(d ²)	Distância calculada (equação 3)	Erro na distância (%)
0,25	145	-55	0,06	-1,2041	0,05	81
0,5	117	-83	0,25	-0,6021	1,18	135
0,75	120	-80	0,56	-0,2499	0,83	11
1	130	-70	1,00	0,0000	0,26	74
1,25	117	-83	1,56	0,1938	1,18	6
1,5	127	-73	2,25	0,3522	0,37	75
1,75	98	-102	3,06	0,4861	10,49	499
2	116	-84	4,00	0,6021	1,32	34
2,5	125	-75	6,25	0,7959	0,47	81
3	108	-92	9,00	0,9542	3,32	11
4	100	-100	16,00	1,2041	8,33	108
5	99	-101	25,00	1,3979	9,35	87
6	94	-106	36,00	1,5563	16,62	177
7	90	-110	49,00	1,6902	26,34	276

Tabela 3 - Resultados da medição de RSSI para várias distâncias, com a etiqueta colocada numa direção de 45 graus.

- Para as direções de 45° e 90° há 3 casos em que o erro se desvia completamente do espectável e os restantes cálculos apresentam um erro próximo e abaixo de 100%.
- Para a direção de 135° há 3 casos em que o erro é próximo de 200% e os restantes cálculos apresentam um erro abaixo de 84%.

A Figura 71, a Figura 73 e a Figura 75 mostram a distribuição do erro relativo em função da distância.

Em consequência destes testes, há que referir dois valores que foram utilizados no protótipo do sistema de localização:

- O valor de K que resultou da média dos valores obtidos para cada uma das 3 direções analisadas, ou seja, $K=3.8 \times 10^{-9}$.
- O valor máximo de RSSI (na gama 0:255) igual a **200**.

Comparando o gráfico do $RSSI_{dBm}$ em função da distância, para as 3 direções analisadas (Figura 76), tanto em termos de medições como em termos de linha de tendência, mostram que embora haja uma dispersão de valores as linhas de tendência não são muito diferentes. A aproximação é mais notória para distâncias maiores. A conclusão é a de que a antena do recetor é razoavelmente omnidirecional, mas não perfeitamente.

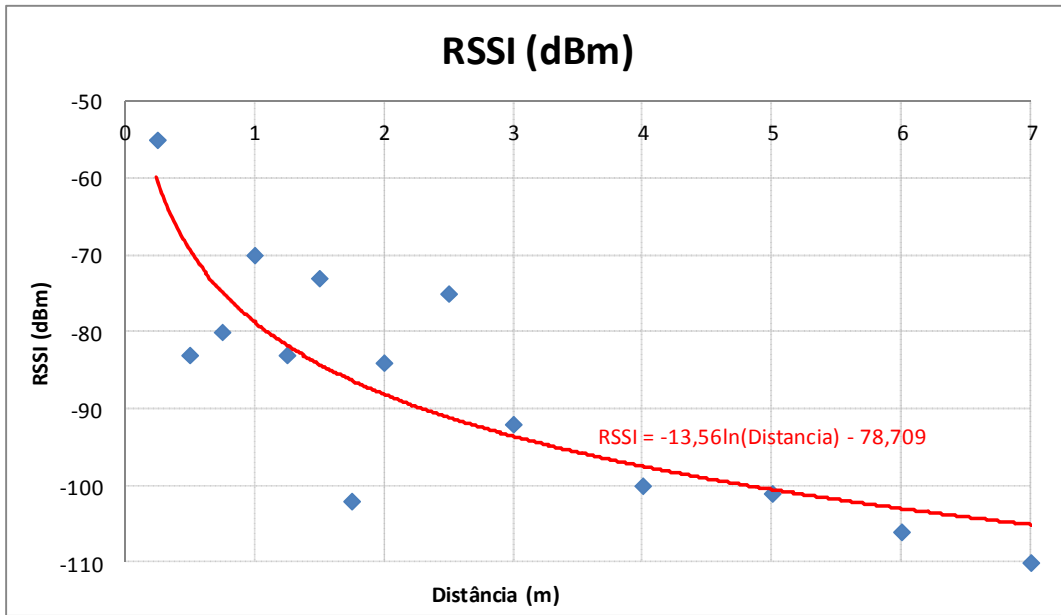


Figura 70 - Medição de RSSI em função da distância, com a etiqueta colocada numa direção de 45 graus.

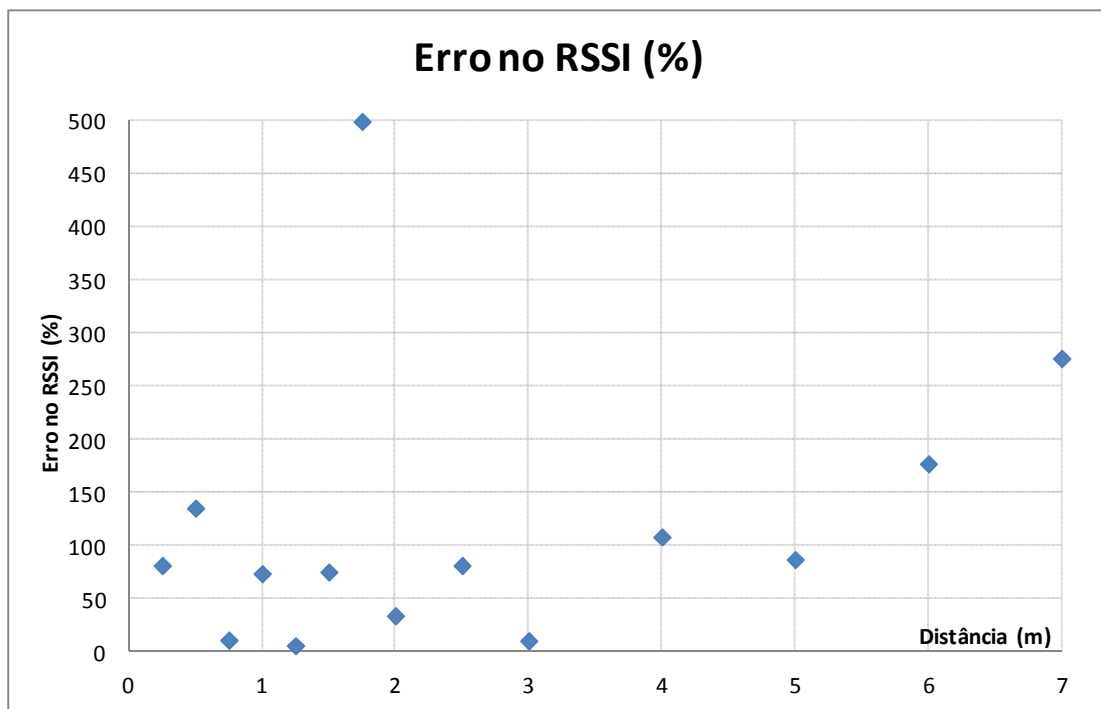


Figura 71 - Erro entre os valores de RSSI medidos e calculados com a equação 3, com a etiqueta colocada numa direção de 45 graus.

Ângulo = 90 graus						
Distância medida (d)	RSSI Médio (0:255)	RSSI Médio (dBm)	Quadrado da distância (d ²)	log10(d ²)	Distância calculada (equação 3)	Erro na distância (%)
0,25	139	-61	0,06	-1,2041	0,07	74
0,5	120	-80	0,25	-0,6021	0,58	16
0,75	117	-83	0,56	-0,2499	0,82	9
1	121	-79	1,00	0,0000	0,52	48
1,25	112	-88	1,56	0,1938	1,46	17
1,5	103	-97	2,25	0,3522	4,11	174
1,75	97	-103	3,06	0,4861	8,19	368
2	119	-81	4,00	0,6021	0,65	67
2,5	120	-80	6,25	0,7959	0,58	77
3	116	-84	9,00	0,9542	0,92	69
4	97	-103	16,00	1,2041	8,19	105
5	98	-102	25,00	1,3979	7,30	46
6	94	-106	36,00	1,5563	11,57	93
7	89	-111	49,00	1,6902	20,58	194

Tabela 4 - Resultados da medição de RSSI para várias distâncias, com a etiqueta colocada numa direção de 90 graus.

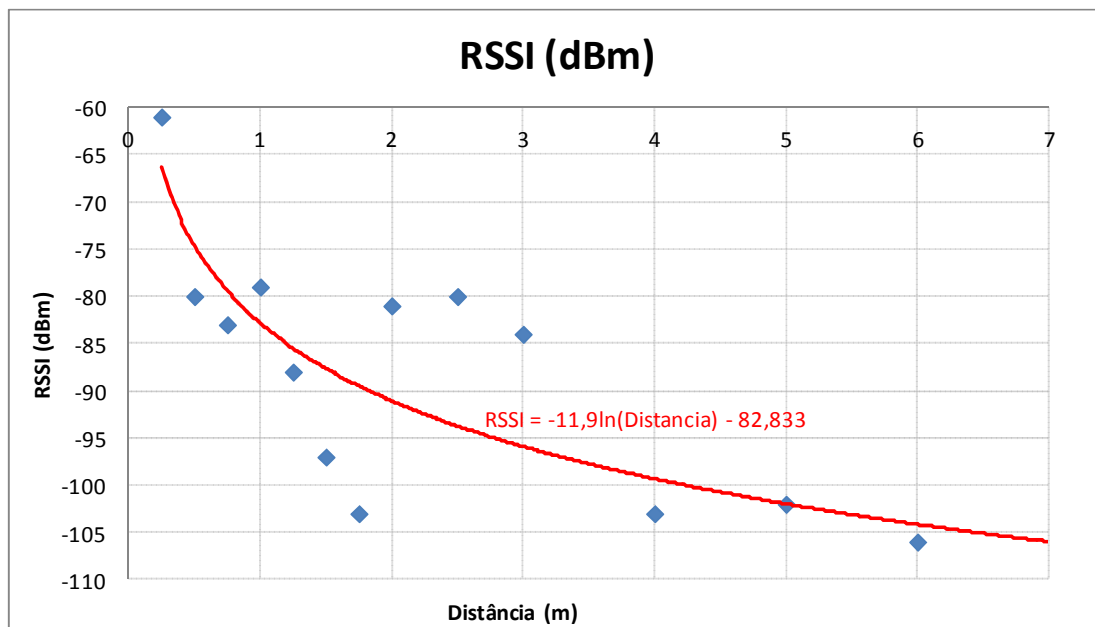


Figura 72 - Medição de RSSI em função da distância, com a etiqueta colocada numa direção de 90 graus.

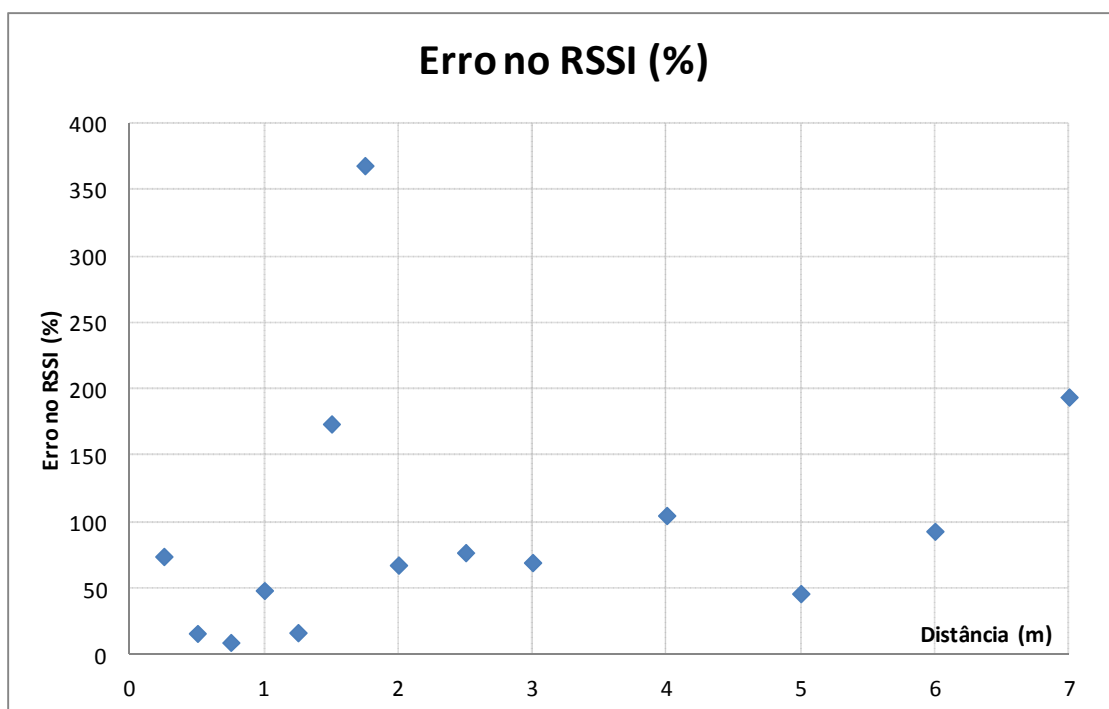


Figura 73 - Erro entre os valores de RSSI medidos e calculados com a equação 3, com a etiqueta colocada numa direção de 90 graus.

Ângulo = 135 graus						
Distância medida (d)	RSSI Médio (0:255)	RSSI Médio (dBm)	Quadrado da distância (d ²)	log ₁₀ (d ²)	Distância calculada (equação 3)	Erro na distância (%)
0,25	135	-65	0,06	-1,2041	0,07	72
0,5	108	-92	0,25	-0,6021	1,56	211
0,75	119	-81	0,56	-0,2499	0,44	42
1	102	-98	1,00	0,0000	3,10	210
1,25	109	-91	1,56	0,1938	1,39	11
1,5	103	-97	2,25	0,3522	2,77	84
1,75	99	-101	3,06	0,4861	4,39	151
2	112	-88	4,00	0,6021	0,98	51
2,5	118	-82	6,25	0,7959	0,49	80
3	110	-90	9,00	0,9542	1,24	59
4	96	-104	16,00	1,2041	6,19	55
5	98	-102	25,00	1,3979	4,92	2
6	95	-105	36,00	1,5563	6,95	16
7	90	-110	49,00	1,6902	12,36	77

Tabela 5 - Resultados da medição de RSSI para várias distâncias, com a etiqueta colocada numa direção de 135 graus.

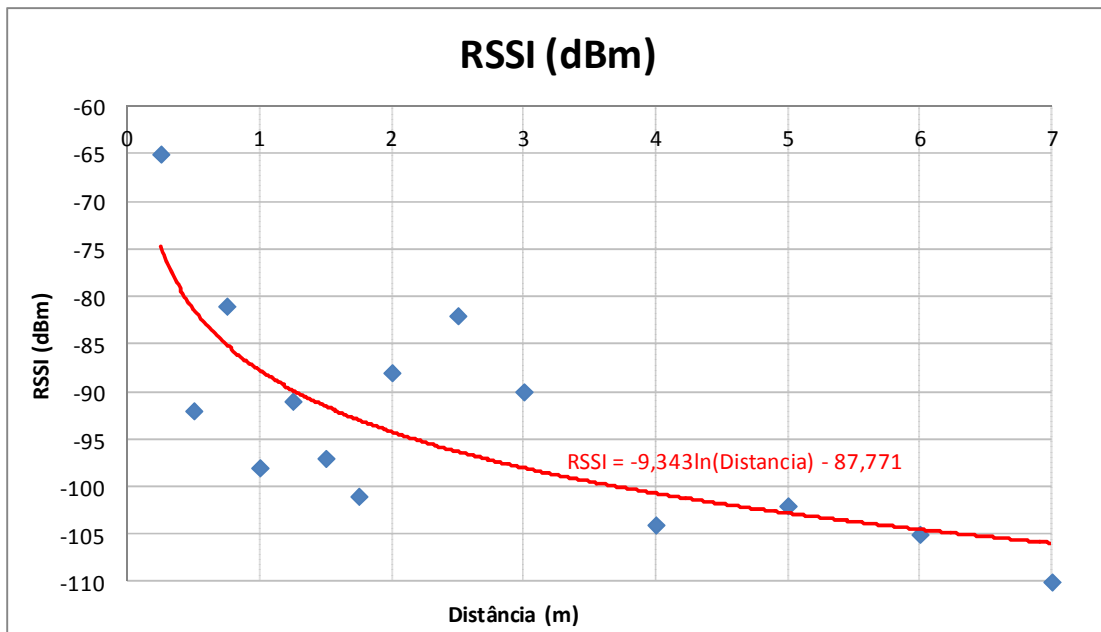


Figura 74 - Medição de RSSI em função da distância, com a etiqueta colocada numa direção de 135 graus.

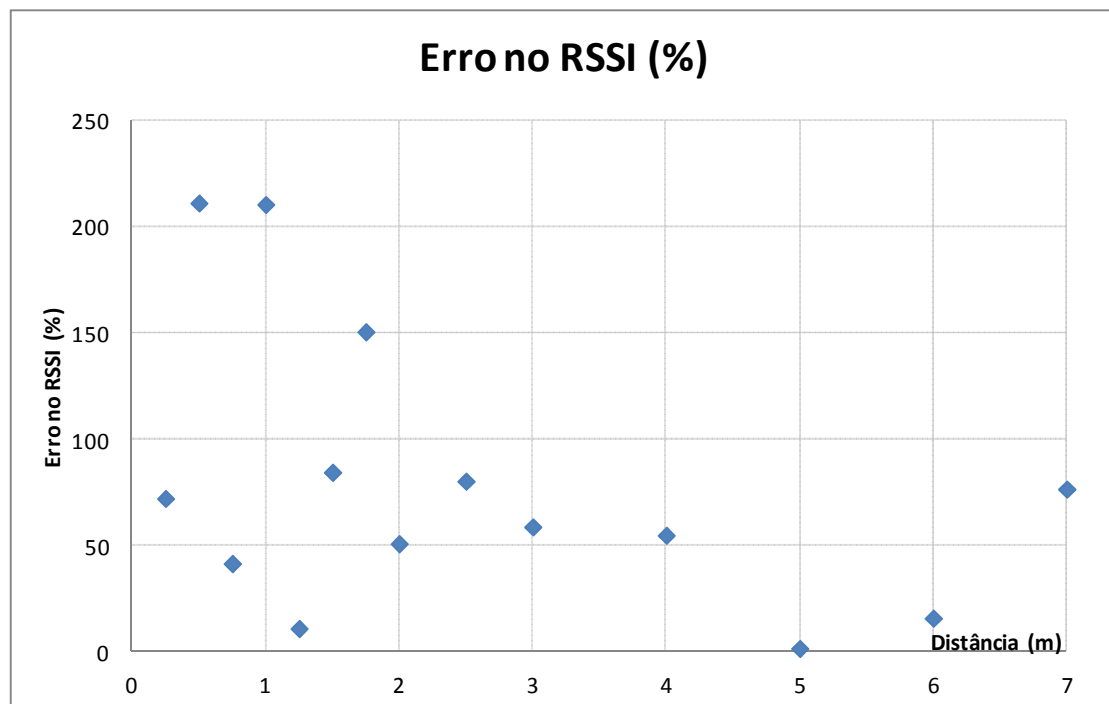


Figura 75 - Erro entre os valores de RSSI medidos e calculados com a equação 3, com a etiqueta colocada numa direção de 135 graus.

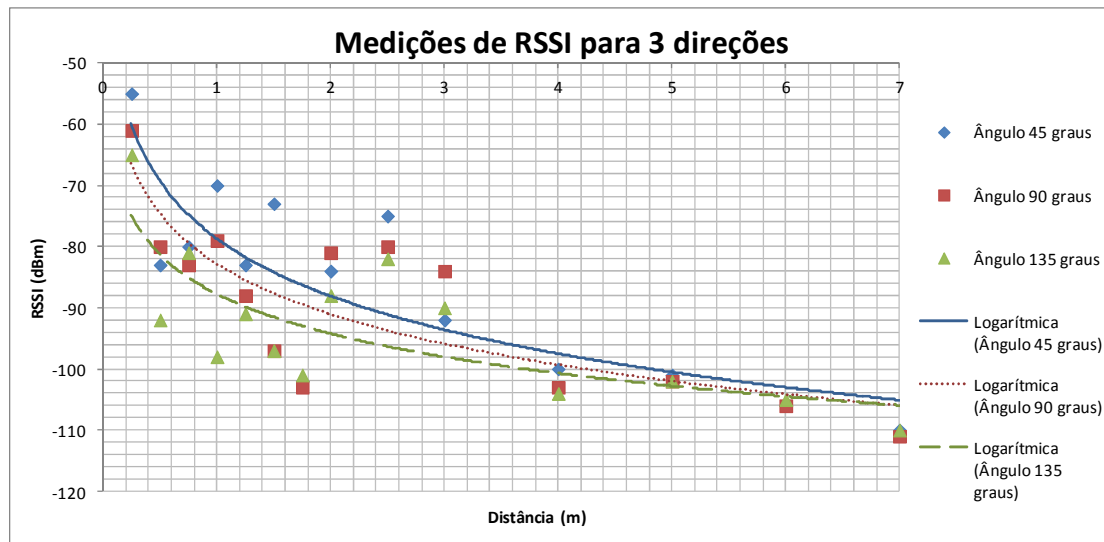


Figura 76 - Comparação das medições de RSSI, em função da distância, para 3 direções distintas (45, 90 e 135 graus).

6.4. Teste do protótipo desenvolvido

Para iniciar a utilização do protótipo, o utilizador tem que se autenticar. Após a autenticação o sistema pode começar a receber pacotes enviados por um ou vários APs em tempo real. No entanto, é necessário ter em atenção que os pacotes devem ser enviados a um cadência máxima que permita o protótipo processá-los e efetuar todos cálculos associados com a localização da origem desses pacotes.

Cada ponto de acesso emite um sinal RF que pode ser captado por qualquer etiqueta RFID de 2 em 2 segundos e envia o(s) pacote(s) recebido(s) das etiquetas via TCPIP para o protótipo (sistema central). Sempre que recebe um pacote, o sistema central atualiza automaticamente a sua lista dos últimos pacotes recebidos (Figura 64).

Como já foi referido na secção 5.5.10, o protótipo permite simular o envio de pacotes, a partir de etiquetas RFID, para facilitar o teste da trilateração entre medições de RSSI. Deste modo, foi possível testar a componente do protótipo mais diretamente relacionada com a localização nos variados cenários: (i) cenário em que o sistema central recebe 3 medições, originadas na mesma etiqueta, recebidas por 3 APs distintos e pertencentes ao mesmo conjunto, e próximas em termos de tempo de chegada. Este é o cenário base que possibilita a trilateração, (ii) cenários em que não estão reunidas todas as condições anteriores, (iii) cenários que reúnem as condições enumeradas em (i), mas em que falha a interseção de um ou dos dois pares de circunferências centradas nos pontos de acesso (que detetaram os pacotes) e com raio igual à distância estimada a

partir do RSSI (incluído nos pacotes detetados), (iv) cenários que reúnem as condições enumeradas em (i), mas em que falha a intersecção dos segmentos de reta definidos pela intersecção dos 2 pares de circunferências mencionados.

A Figura 77 mostra a interface com o utilizador que reúne o acesso às funcionalidades do protótipo mais diretamente ligadas com a localização de etiquetas RFID:

- A simulação do envio de pacotes a partir de uma etiqueta RFID para 1 ou 3 APs virtuais;
- A lista dos últimos pacotes provenientes das diversas etiquetas e detetados por cada conjunto de APs;
- O resultado dos cálculos da localização das etiquetas RFID, onde se inclui o momento da localização, a identificação da etiqueta, a identificação do seu utilizador, as coordenadas da localização estimada e a zona em que se insere essa localização;
- Os alertas emitidos quando os utilizadores entram em zonas interditas.

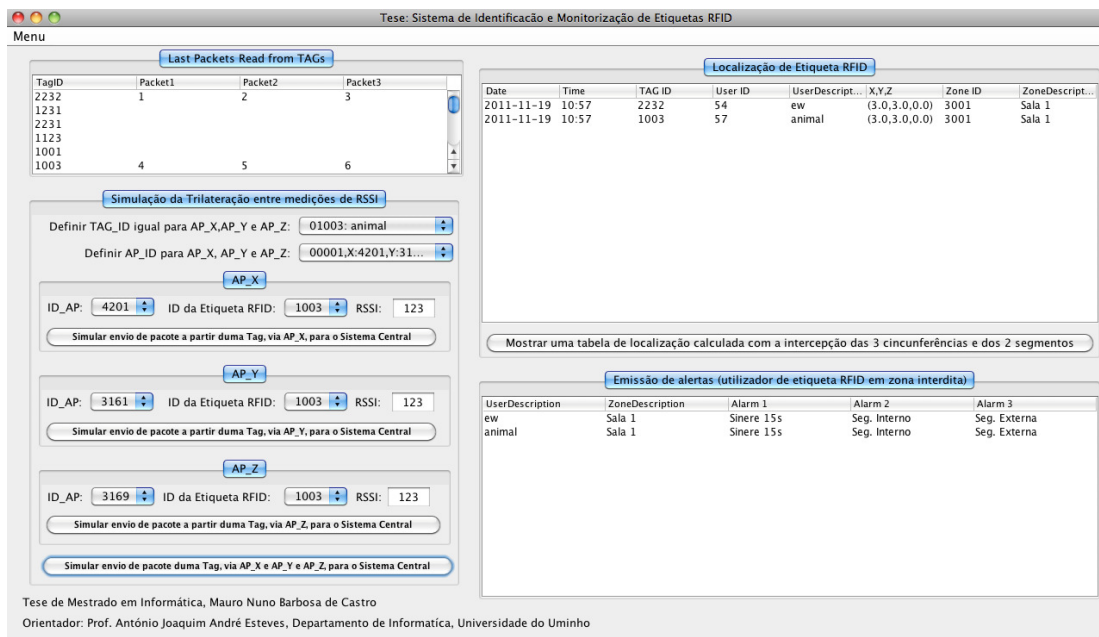


Figura 77 – Parte da interface com o utilizador que reúne o acesso às funcionalidades do protótipo mais diretamente ligadas com a localização de etiquetas RFID.

Capítulo 7 Conclusões e Trabalho Futuro

7.1. Conclusões

Neste capítulo serão apresentadas as principais conclusões retiradas do trabalho realizado, tendo por base os objetivos inicialmente traçados para o mesmo. Adicionalmente, serão descritas as limitações do estudo, apresentando-se também algumas ideias de trabalho futuro na continuidade do que foi realizado.

Começamos por salientar que este trabalho teve como objetivo principal a modelação e conceção de uma solução global de monitorização/localização baseada em RFID, para vários tipos de organismos ou empresa. Como tal, em todo este processo, pretendeu-se criar uma solução integrada de localização baseada na tecnologia RFID, mais do que apresentar ou implementar um conjunto de algoritmos de localização, os quais já foram por diversas vezes abordados na literatura desta área. Nesse sentido, o trabalho iniciou-se com o levantamento das necessidades, relativamente à utilização de tecnologia RFID, por parte de três organismos/empresas tipo. O levantamento foi concretizado através de inquéritos entregues a pessoas dessas empresas. Estes inquéritos revelaram-se importantes para ajudar na captura dos requisitos do sistema a desenvolver. A documentação dos requisitos foi feita através do modelo de Volere, que é um dos mais utilizados. Posteriormente, identificaram-se os utilizadores do sistema. A fase de conceção, aquela que demorou mais tempo, incluiu a elaboração do diagrama de casos de uso e da descrição textual detalhada de cada caso de uso, diagramas de sequência, modelo de dados persistentes e diagrama de classes. Durante a fase de implementação construiu-se um protótipo do sistema em linguagem Java, o qual foi depois submetido a alguns testes.

Cumprimento dos Requisitos Propostos

Uma das conclusões fundamentais a retirar após a conclusão do trabalho é indicar se os requisitos inicialmente identificados foram ou não implementados. Por isso dedica-se a seguir uma razoável atenção a cada um dos requisitos.

Requisito 1: gerir a comunicação entre os Pontos de Acesso e o sistema central.

O sistema consegue receber, processar e armazenar os pacotes enviados pelos APs através da classe *Packet* e dos respetivos métodos. O sistema consegue ainda enviar

comandos aos APs para os configurar ou ler a sua configuração. Esta funcionalidade foi concretizada através da classe *AP*, uma implementação simplificada de um ponto de acesso. Para permitir um funcionamento assíncrono entre o sistema central e os pontos de acesso, cada instância da classe *AP* corre numa *thread* separada.

Requisito 2: configurar pontos de acesso.

O sistema consegue criar, eliminar, alterar e listar corretamente os dados relativos a um ponto de acesso usando a classe *APdata*.

Requisito 3: formar e gerir conjuntos de pontos de acesso.

O sistema consegue criar, eliminar, alterar e descrever corretamente a composição dos conjuntos de pontos de acesso, usando as classes *SetAPs* e *ListSetAPs*.

Requisito 4: Localizar utilizadores de etiqueta RFID.

Utilizando a classe *TagLocalization* e o método *CalcDistanceTagLocalization* da classe *Packet*, o sistema consegue determinar em tempo real a zona do edifício em que cada utilizador de etiqueta RFID se localiza. Dadas as limitações dos métodos de localização baseados no RSSI e dada a pouca sofisticação do algoritmo de localização implementado, a precisão das estimativas é apenas sofrível.

Requisito 5: Emitir alertas nas situações em que um utilizador de etiqueta RFID entra numa zona que lhe é interdita.

Ao receber um pacote dum AP (método *ReceivePacket* da classe *Packet*), é calculada a distância entre a etiqueta que emitiu o sinal RF e o AP que reencaminhou o pacote respetivo para o sistema central (método *CalcDistanceTagLocalization* da classe *Packet*), este pacote será guardado na lista *PacksLastPosTag* (método *SavePackReceiveAP* desta classe). Se houver 3 pacotes originados nessa etiqueta e válidos para fazer a trilateração, calcula-se a posição da etiqueta (método *CalcTagLocalization* da classe *TagLocalization*) e finalmente a zona em que se insere a posição (método *CalcZoneLocalization* da classe *TagLocalization*). Caso a zona calculada seja interdita ao tipo de utilizador, o sistema envia alerta(s) para pessoal da segurança (método *EmitSignalAlert* da classe *Alarm*). Os alertas a emitir são configuráveis através da classe *ListForbidden*. Deste modo, o requisito é completamente cumprido.

Requisito 6: Criar e gerir utilizadores do sistema, incluindo o administrador do sistema.

O sistema permite criar, alterar e remover utilizadores registados, de um dado tipo, através das classes *SystemUser* e *TypeUser*. Um dos tipos possíveis é administrador do sistema.

Requisito 7: Permitir a um utilizador autenticar-se perante o sistema e encerrar uma sessão de trabalho.

O acesso e encerramento do acesso ao sistema faz-se através da classe *Login*, do package *Interface*, e do método *validate* da classe *SystemUser*, que valida as credenciais introduzidas pelo utilizador. As funcionalidades disponibilizadas, após efetuar a autenticação com sucesso, variam com o tipo de utilizador: administrador da empresa, administrador do sistema, gestor de etiquetas RFID e utilizador normal.

Requisito 8: Definir as zonas do edifício.

O sistema permite definir e validar a geometria dos vários espaços do edifício, usando para isso as classes *POINT*, *Segment* e *Zone*. Embora estas classes suportem coordenadas 3D, assume-se que a componente Z dos edifícios não é relevante para a geometria das zonas.

Requisito 9: Criar e gerir as listas de zonas do edifício permitidas e interditas a cada tipo de utilizador.

As classes *ListAllowed* e *ListForbidden* mantêm o registo das zonas permitidas e interditas, a cada tipo de utilizador. O método *initializeList*, de cada uma destas duas classes, define a composição inicial da lista em causa e se for o caso, especifica quais os alertas a emitir. Para mover um tipo de utilizador duma lista (de origem) para a outra, utiliza-se o método *MoveTypeUserToOtherList* da lista de origem. Quando a troca é da lista permitida para a lista interdita é preciso definir os alertas a emitir. Para isso recorre-se à classe *DefineTypeAlarm* do package *Interface*.

Requisito 10: Monitorizar a associação entre etiquetas RFID e utilizadores.

As tarefas relacionadas com a atribuição (recolha) de etiquetas RFID a (de) utilizadores e a listagem das etiquetas atribuídas em cada momento são suportadas pelas classes *TagRFID* e *UserTagRFID*.

Requisito 11: Efetuar operações sobre etiquetas RFID.

A programação e a impressão em papel dos dados numa etiqueta RFID não foram totalmente implementadas, embora a classe *UserTagRFID* disponha dos métodos *Program* e *Print* previstos para esse fim.

Em conclusão, com a exceção do requisito 11, de menor prioridade, todos os outros foram cumpridos.

Resultados Obtidos

Uma das maiores limitações do trabalho desenvolvido prende-se com o facto de o protótipo não ter sido testado com vários APs, nem com diferentes tipos de AP. Esta limitação deve-se essencialmente a restrições orçamentais. Esta limitação foi parcialmente ultrapassada com a utilização de um módulo desenvolvido para simular o envio de pacotes a partir de etiquetas para APs virtuais.

Os resultados da calibração do equipamento RFID utilizado mostraram que, apesar da dispersão dos valores, as medições de RSSI seguem o padrão logarítmico definido pelo modelo de propagação RF teórico.

Outro resultado obtido com a calibração do equipamento RFID traduziu-se na constatação de que a antena do recetor é omnidirecional. Este resultado é muito importante, porque sem ele o método de localização seria bem mais complexo, dado que nesse caso seria preciso estimar além da distância a direção da localização do emissor RF em relação ao recetor.

É um facto que os métodos de localização baseados na trilateração de medições de RSSI produzem resultados com erro apreciável. Isto resulta de os valores de RSSI serem pouco estáveis e pouco fiáveis para serem usados como medida da distância a que a fonte do sinal RF se encontra do receptor. A presente implementação não foge a esta tendência, como é comprovado pelos resultados apresentados no capítulo 6, onde o erro entre o valor de RSSI medido e estimado anda muitas vezes próximo dos 100%.

Funcionalidades do Protótipo

Um dos resultados relevantes desta dissertação é o protótipo desenvolvido em Java, válido para ser usado por diferentes tipos de organismos e empresas. Fazendo um resumo das funcionalidades do protótipo, pode dizer-se que permite (i) restringir o acesso ao sistema, (ii) gerir os seus utilizadores registados, (iii) fazer a gestão de etiquetas RFID, designadamente atribuir, recolher e listar, (iv) definir a

geometria de cada piso do edifício da empresa, (v) definir quais as zonas permitidas e interditas a cada tipo de utilizador. No caso de a zona ser interdita pode especificar-se até 3 tipos de alertas a emitir no caso de essa zona ser acedia por um utilizador do tipo em causa, (vi) gerir os pontos de acesso e os conjuntos de pontos de acesso utilizados na trilateração, (vii) e obviamente, estimar a localização de etiquetas RFID por trilateração. A localização estimada, além de ser disponibilizada em termos de coordenadas X, Y e Z, também é acessível em termos de zona do edifício. Outro aspeto que convém destacar resulta do facto de todas as funcionalidades modeladas e implementadas estarem acessíveis através duma interface gráfica. O protótipo inclui ainda uma facilidade que ajudou a realizar os testes do próprio protótipo: a simulação do envio de pacotes a partir de etiquetas RFID para pontos de acesso virtuais.

Como conclusão final, pode dizer-se que se concebeu um protótipo funcional que cumpre praticamente todos os requisitos propostos, possui uma interface fácil de utilizar e é suficientemente genérico para poder ser usado por empresas de tipos diferentes. Dado que o código e os modelos estão perfeitamente sincronizados, alterar ou adicionar funcionalidades ao sistema é relativamente seguro e com um custo moderado. Em termos da qualidade das estimativas da localização, os resultados não são positivos.

7.2. Trabalho Futuro

Para terminar, identificam-se algumas possibilidades de trabalho futuro na continuidade da dissertação realizada. A maioria das ideias propostas visa resolver limitações do trabalho desenvolvido.

- Efetuar mais testes ao protótipo, nomeadamente usando vários pontos de acesso e com pontos de acesso diferentes do que se utilizou durante a dissertação.
- Fazer testes de calibração mais exaustivos de modo a melhorar o cálculo da constante K usada na estimação das distâncias a partir do RSSI. Esta constante afeta de forma significativa o cálculo da posição dos emissores RF.
- Melhorar a estratégia de localização, nomeadamente para ter em conta a coordenada Z da localização das etiquetas. Não incluir a coordenada Z, terá um impacto bastante negativo nos casos em que a distância entre a etiqueta e o recetor apresente valores X e Y pequenos. A componente Z será sempre uma limitação, dado que não há certezas de qual a altura a que as etiquetas são transportadas e se ela se mantém constante.

- Implementar e agregar outras abordagens e algoritmos de estimativa da localização.
- Implementar o envio de alertas através de SMS, BIP ou e-mail para entidades de segurança.
- Disponibilizar a possibilidade gerar relatórios e gráficos com dados estatísticos da utilização do sistema.
- Implementar a programação de etiquetas RFID através do ponto de acesso.

Bibliografia

- [1] Goodman, P. S.; Sproull, L. S. (1990). *Technology and Organizations*. San Francisco: Jossey-Bass Publishers.
- [2] RFID Software. Compare Radio Frequency Identification Software. [Online]. Recuperado em Novembro de 2010 de: http://www2.technologyevaluation.com/ppc/request/rfid_eval_comp.asp?se=google&gclid=CJfeoJ7Ek6wCFcod4QodiiJgnw.
- [3] Roberti, M. (2002). The History of RFID Technology. In *RFID Journal*. [Online]. Recuperado em Junho de 2010 de: <http://www.rfidjournal.com/article/articleprint/1338/>.
- [4] Shepard, S. (2005). *RFID: Radio Frequency Identification*. New York: McGraw-Hill.
- [5] Gomes, H. M. (2007). Construção de um sistema RFID com fins de localização especiais. Dissertação de Mestrado. Universidade de Aveiro: Departamento de Electrónica e Telecomunicações.
- [6] Luís (2009). Funcionamento de um sistema RFID. [Online]. Recuperado em Novembro de 2010 de: <http://rfidtek.blogspot.com/2009/09/funcionamento-de-um-sistema-rfid.html>.
- [8] Ramos, L.; Grotti, R. Redes RFID. [Online]. Recuperado em Abril de 2010 de: www.getec.cfetmt.br/~ruy/2007/pos/wireless/trabalhos_alunos/RFID_apr.pdf.
- [9] Silva, A.; Ledur, H. (2006). Controle de Acesso e Agendamento Electrónico de Visitas ao Senado Federal [Distrito Federal]. Monografia de Especialização. Universidade de Brasília: Faculdade de Tecnologia. Departamento de Engenharia Electrónica.
- [10] SYBASE Portugal - RSC (RFID Solutions Center) (2006). Estado da Arte em RFID. Recuperado em Outubro de 2010 de: <http://www.cin.ufpe.br/~dfs3/rfid/EstadoDaArte.pdf>.
- [11] Couto, C. RFID (PDF). [Online]. Recuperado em Dezembro de 2010 de: http://www.dei.isep.ipp.pt/~qtdei/RFID_300403.pdf.
- [12] Radio-Frequency Identification. [Online]. Recuperado em Abril de 2010 de: <http://en.wikipedia.org/wiki/RFID>
- [13] Dias, J. F. (2008). Desenvolvimento de aplicações para sistemas RFID Comerciais. Dissertação de Mestrado. Universidade do Minho: Departamento de

Engenharia Electrotécnica Industrial e de Computadores.

- [14] Histórico RFID. [Online]. Recuperado em Abril de 2010 de: www.gta.ufrj.br/grad/09_1/versaofinal/rfid/historico.html.
- [15] Curso de RFID. Aplicações do RFID (Parte I). [Online]. Recuperado em Maio de 2010 de: <http://www.curso-rfid.com.br/artigos/aplicacoes-do-rfid-parte-i/>.
- [16] Nogueira, I. C. (2002). Gerenciando a Biblioteca do Amanhã: Tecnologias para otimização e agilização dos serviços de informação. Monografia. Universidade Federal de Minas Gerais: Escola de Ciência da Informação.
- [18] Finkelstein, A.; Galal, G.; Sharp, H. (1999). Stakeholder Identification in the Requirements Engineering Process. In *Proceedings of 10th International Workshop on Requirements Engineering Processes*. pp. 387-391
- [19] Fernandes, J. M. Unit 1 - Introduction to Requirements Engineering (PDF). Recuperado em Novembro de 2010 de: <http://www3.di.uminho.pt/~jmf/ACS/unit1-intro.pdf>.
- [20] Silva, A.; Videira, C. (2005). *UML - Metodologias e Ferramentas CASE*. Vol. 1. 2ª Edição. Vila Nova de Famalicão: Centro Atlântico Editora.
- [21] Fernandes, J. M.; Machado, R. J.; Seidman, S. B. (2009). A requirements engineering and management training course for software development professionals. In *22nd IEEE-CS Conference on Software Engineering Education and Training*. pp. 20-25. California: IEEE Computer Society Press.
- [22] Segurança em que pode confiar. [Online]. Recuperado em Maio de 2010 de: <http://www.netcaos.pt/docs/RFIDsolucao-global.pdf>.
- [23] Robertson, J.; Robertson, S. (2009). Volere Requirements Specification Template. [Online]. Recuperado em Janeiro de 2011 de: http://www.st.cs.unisaarland.de/edu/se/2009/slides/volere_specification_template_v6.pdf.
- [24] Ribeiro, A. N. (2008). Um processo de modelação de sistemas software com integração de especificações rigorosas. Tese de Doutoramento em Informática. Universidade do Minho: Departamento de Informática.
- [26] Arlow, J.; Neustadt, I. (2005). *UML 2 and the Unified Process: Practical Object-Oriented Analysis and Design*. 2nd. Edition. Addison-Wesley Professional.
- [28] Ladd, A.M.; Bekris, K.E.; Rudys, A.P.; Wallach, D.S.; Kaviraki, L.E. (2004). On the Feasibility of Using Wireless Ethernet for Indoor Localization. In *IEEE*

Transactions on Robotics and Automation. Vol. 20. pp. 555-559.

- [27] Ferris, B.; Lawrence, N.; Fox D. (2007). *WiFi-SLAM Using Gaussian Process Latent Variable Models*. In *Proceedings of 20th International Joint Conference on Artificial Intelligence (IJCAI)*. pp. 2480-2485.
- [29] Figueredo, L. F.; Couto, F. L.; Bauchspiess, A. (2009). *An Evaluation of RSSI Based Indoor Localization Systems in Wireless Sensor Networks*. Brazil: Robotics, Automation and Computer Vision Group (GRAV). University of Brasília: Department of Electrical Engineering.
- [30] McRae, G. Intersection of two circles - finding the coordinates of intersection given the equations of the two circles (using clever area-based method). [Online]. Recuperado em Fevereiro de 2011 de: <http://2000clicks.com/mathhelp/GeometryConicSectionCircleIntersection.aspx>.
- [31] Bourke, P. (1989). *Intersection point of two lines (2 dimensions)*. [Online]. Recuperado em Dezembro de 2010, de Intersection point of two lines: <http://paulbourke.net/geometry/lineline2d/>.
- [32] SYRD245-1N active RFID Network Reader User Manual. (2007). [Online]. Recuperado em Abril de 2011 de: http://www.inforidas.com/documents/AP/KIT_%20SYRD245-1N.pdf.
- [33] SYRIS. (2007). SYRD245 - Reader protocol Manual. [Online]. Recuperado em Abril de 2011 de: http://www.inforidas.com/documents/AP/reader_protocol_manual.pdf.
- [34] Robertson, J.; Robertson, S. (2006). Volere Requirements Specification Template. In *The Atlantic Systems Guild Limited*. pp. 3-4.

Anexos

Anexo I Inquérito para Armazéns

Este inquérito, desenvolvido por um aluno mestrado em Informática da Universidade do Minho, pretende recolher uma série de dados sobre a implementação de um sistema de monitorização de armazém, com vista à elaboração da sua dissertação no mestrado mencionado. O tratamento da informação pressupõe o anonimato do inquirido e a confidencialidade dos dados.

Introdução

RFID é um acrónimo do nome (*Radio-Frequency Identification*) em inglês que, em português, significa Identificação por Rádio Frequência. Trata-se de um método de identificação automática através de sinais de rádio, recuperando e armazenando dados remotamente através de dispositivos chamados de etiquetas RFID.

Uma etiqueta RFID é um emissor passivo, ou seja, um pequeno objeto que pode ser colocado num bem (equipamento, embalagem ou produto), e emitir um sinal RF com informação associada a esse bem.

A gestão de um armazém, ou do inventário de uma empresa, está diretamente relacionada com as vendas e, conseqüentemente, com os resultados. Na maioria das vezes, os erros associados a estas atividades resultam em prejuízos assinaláveis. O RFID pode ajudar a evitar falhas e a reduzir o tempo gasto com muitas das tarefas relacionadas com a gestão do armazém. Recorrendo à tecnologia RFID podemos saber, em tempo real, tudo o que entra e sai de um armazém sem ter que abrir caixas ou desmontar paletes para confirmar o que chega ou o que sai, automatizando assim todo este processo. Existe ainda a possibilidade de configurar os mais diversos alarmes automáticos. Os ganhos mais visíveis, relacionados com a utilização da tecnologia RFID, são a eliminação de perdas e de falhas humanas.

Caracterização geral do Inquirido

Idade Sexo Masculino Feminino

Profissão

1- Que tipos dos produtos existem no seu armazém?

Veículos Eletrodomésticos Produtos alimentares

Caixas Embalagens Vestuário

Outros. Quais _____

2- O Armazém já está equipado com um sistema de segurança semelhante ao referido?

Sim Não

3- Se respondeu sim, considera-o:

Insuficiente Tolerável ou eficaz

4- Se respondeu não:

4.1- Já sentiu necessidade de melhorar as operações do seu armazém?

Sim Não

5-De que forma? (assinale todos os que achar pertinentes)

Rastrear ativos, ou localizar equipamentos de alto valor;

Melhorar o prazo de entrega;

Reduzir gastos;

Determinar quais os ativos que serão etiquetados (itens individuais, caixas e/ou paletes);

Informação em tempo real do ponto de venda permitindo-lhe fazer reposições;

Soluções logísticas que lhe permitam acelerar o ritmo dos seus inventários e manter os produtos em constante movimento até eles chegarem às mãos dos consumidores.

6- Já ocorreu alguma situação que poderia ter sido evitada se existisse um sistema eficaz de segurança?

Sim Não

7- Neste momento já foram tomadas medidas para a implementação do referido sistema?

Sim Não

8- Em termos financeiros acha-o:

Pouco dispendioso Suportável Muito dispendioso

9- O que considera mais importante monitorizar/localizar?

Clientes Funcionários Bens

Outros. Quais? _____

10- Em caso de monitorização, se houver situação anómala qual o tipo de alerta desejado?

Tocar Sirene Registrar num LOG

Outros. Quais? _____

11- Que alternativas de forma de alerta dos funcionários existem ou gostava que existissem?

BIP Mensagem SMS para telemóvel Mensagem E-Mail

Aviso Visual no local do funcionário Aviso Sonoro no local do funcionário

Outras. Quais? _____

12- Que tipo de situações interessa monitorizar?

Movimento Entrada/Saída do Edifício

Outras. Quais? _____

13 - Em que unidades/departamentos considera esta monitorização mais relevante?

14 - Perguntas quantitativas:

a) Indique um valor aproximado para o número de médio (estimativa) de clientes por dia;

b) Indique um valor aproximado para o número aproximado de bens em armazém;

c) Indique um valor aproximado para o número de funcionários.

15 - Ocorre-lhe alguma sugestão de funcionalidade(s) do sistema de monitorização, que não esteja(m) implícita(s) neste inquérito? Quais?

Muito obrigado pela sua colaboração.

Anexo II Inquérito aos bibliotecários

Este inquérito, desenvolvido por um aluno do mestrado em Informática da Universidade do Minho, pretende recolher uma série de dados sobre a implementação de um sistema de monitorização dos livros, com vista à elaboração da sua dissertação no mestrado mencionado. O tratamento da informação pressupõe o anonimato do inquirido e a confidencialidade dos dados.

Introdução

As bibliotecas têm hoje de servir a nova geração de utilizadores que usam com facilidade as novas tecnologias. Em bibliotecas e centros de formação, a tecnologia RFID é utilizada para identificar o fundo documental, constituído por livros, CDs/DVDs, Revistas, etc, possibilitando a leitura e o rastreamento dos exemplares físicos dos documentos.

A Identificação dos documentos faz-se através de uma etiqueta de RFID (*tag*) neles fixada. Este tipo de etiqueta é plano (de 1 a 2 mm), adesivo, de dimensões reduzidas (50 x 50 mm em média), contém um *micro-chip* no seu centro e em redor deste uma antena metálica em espiral. Esta etiqueta e um ou mais sensores ativos RFID, que podem estar fixos ou ser moveis, possibilitam a codificação e leitura dos dados sobre o documento em causa, principalmente o seu código identificador (convencionalmente registado através dum códigos de barras).

É possível converter facilmente o código de barras, usado atualmente na identificação dos documentos, no identificador incluído nas etiquetas RFID, utilizando para isso um equipamento próprio para esta conversão.

Existem inúmeras potencialidades na aplicação da tecnologia RFID no processo de identificação usado em bibliotecas. Alguns exemplos de aplicação:

- Autoatendimento;
- Controlo de acessos de funcionários e alunos;
- Devolução;
- Empréstimo;
- Estatística de consulta local;

- Leitura de estante para inventário dos documentos;
- Localização de exemplares indevidamente ordenados no fundo documental;
- Localização de exemplares em outras bibliotecas da rede;
- Recatologação.

É ainda possível utilizar as etiquetas RFID para evitar o furto de documentos. Isto porque algumas etiquetas permitem gravar, num bit de segurança, a indicação sobre o facto de o documento se encontrar ou não emprestado. O sistema tradicional de segurança eletromagnético (vulgo EM) adotado em bibliotecas, que é facilmente anulado com recurso a um magneto, exige para a sua implementação uma dupla encriptação. Em contrapartida, um sistema de deteção de furto com recurso a etiquetas RFID apenas necessita de uma única encriptação (na sua configuração mais simples).

Caracterização geral do Inquirido

Idade Sexo Masculino Feminino

Profissão

1- Onde funciona a biblioteca em que exerce funções ?

1.1 Na universidade No Município outro

2- É muito frequentada?

3- Já foram registadas situações anómalas de grande importância?

- Furto Danificação Perda de Registo
- Etiqueta Desconhecida Falsificação Dois Registos Iguais
- Outras. Quais?

4- Que tipos de livros existem na biblioteca?

5- A Biblioteca já está equipada com um sistema de segurança semelhante ao referido?

Sim Não

6- Se respondeu sim, considera-o:

Insuficiente Tolerável ou eficaz

7- Se respondeu não:

7.1- Já ocorreu alguma situação que poderia ter sido evitada se existisse um sistema eficaz de segurança?

Sim Não

8- Acha pertinente a aquisição deste tipo de tecnologia?

Sim Não

9- Neste momento já foram tomadas medidas para a implementação do referido sistema?

Sim Não

10- Em termos financeiros acha-o:

Pouco dispendioso Suportável Muito dispendioso

11- De entre os tipos de documento do fundo documental, quais importa monitorizar/localizar?

Livros Revistas CD/DVD

Outros. Quais? _____

12- Em caso de monitorização, se houver uma situação anómala qual o tipo de alerta desejado?

Tocar Sirene Registrar num LOG

Outros. Quais? _____

13- Que alternativas de forma de alerta dos funcionários existem ou gostava que existissem?

BIP Mensagem SMS para telemóvel Mensagem E-Mail

Aviso Visual no local do funcionário Aviso Sonoro no local do funcionário

Outras. Quais? _____

13- Que tipo de situações interessa monitorizar?

Requisição Devolução Inventário Consulta Furto

Outras. Quais? _____

14 - Perguntas quantitativas:

a) Indique um valor aproximado para o número de utentes (por dia);

b) Indique um valor aproximado para o número de documentos;

c) Indique um valor aproximado para o número de funcionários;

15 - Ocorre-lhe alguma sugestão de funcionalidade(s) do sistema de monitorização, que não esteja(m) implícita(s) neste inquérito? Quais?

Muito obrigado pela sua colaboração.

Anexo III Inquérito aos profissionais de saúde

Este inquérito, desenvolvido por um aluno do mestrado em Informática da Universidade do Minho, pretende recolher uma série de dados sobre a implementação de um sistema de monitorização dos utentes numa unidade de saúde, com vista à elaboração da sua dissertação no mestrado mencionado. O tratamento da informação pressupõe o anonimato do inquirido e a confidencialidade dos dados.

Introdução

Para melhorar a segurança dos cuidados prestados aos utentes (doentes, visitantes, funcionários, etc.), vários hospitais adotaram no Bloco de Partos e no Serviço de Obstetrícia, um sistema de monitorização para os recém-nascidos.

Ainda em fase experimental, prevê-se que o sistema entre em pleno funcionamento em alguns hospitais até ao fim do mês de Outubro. É possível que este sistema, através de uma pulseira eletrónica no tornozelo do recém-nascido, detete de forma automática e sem fios todos os movimentos do bebé.

A vigilância é invisível, silenciosa e durante 24 horas por dia, garante assim proteção e tranquilidade ao bebé e à mãe. Se o bebé se aproximar de uma zona não autorizada, ou se ocorrer sabotagem da pulseira, maliciosa ou acidental, o sistema produz um alarme e procederá ao encerramento automático da porta de saída.

O sistema de segurança contra rapto de crianças é um dos mais utilizados em todo o mundo, devido à sua fiabilidade. É também “amigo do bebé” pois a pulseira é pequena, leve e ergonómica.

Caracterização geral do Inquirido

Idade Sexo Masculino Feminino

Profissão

1- A Instituição onde exerce funções é:

Hospital Maternidade Hospital com maternidade

Hospital pediátrico Centro de Saúde

2- Já está equipada com o referido sistema de segurança?

Sim Não

3- Se respondeu sim, considera-o:

Insuficiente Tolerável ou eficaz

4- Se respondeu não:

Já ocorreu alguma situação que poderia ter sido evitada se existisse um sistema eficaz de segurança?

Sim Não

5- Neste momento já foram tomadas medidas para a implementação do referido sistema?

Sim Não

6- Na sua opinião considera que a adoção do referido dispositivo é :

Pertinente Muito Pertinente

Adequado Muito adequado

7- Em termos financeiros acha-o:

Pouco dispendioso Suportável Muito dispendioso

8- Que tipos de utentes existem na unidade de saúde?

9- Desses tipos de utentes, quais importa monitorizar/localizar? Quais?

Doentes Funcionários Internos Trabalhadores Temporários

Visitantes auxiliares de saúde Segurança

Bombeiros Policias vendedores

Outros. Quais? _____

10- Em caso de monitorização, se houver uma situação anómala qual o tipo de alerta desejado?

Tocar Sirene

Registrar num LOG

Outros. Quais? _____

11- Que alternativas de forma de alerta dos funcionários existem ou gostava que existissem?

BIP

Mensagem SMS para telemóvel

Mensagem

E-Mail

Aviso Visual no local do funcionário

Aviso Sonoro no local do

funcionário

Outros, Quais? _____

12- Que tipo de situações interessa monitorizar?

Movimento

Entrada/Saída do Edifício

Outras. Quais? _____

13 - Em que unidades/departamentos considera esta monitorização mais relevante?

14 - Perguntas quantitativas:

a) Indique um valor aproximado para o número de doentes

b) Indique um valor aproximado para o número de visitantes (por dia)

c) Indique um valor aproximado para o número de funcionários internos

d) Indique um valor aproximado para o número de trabalhadores temporários

15 - Ocorre-lhe alguma sugestão de funcionalidade(s) do sistema de monitorização, que não esteja(m) implícita(s) neste inquérito? Quais?

Muito obrigado pela sua colaboração.

Anexo IV Implementação do Intervalo de Tolerância nas Medições (DELTAT) entre 0 e 2 Segundos

para cada uma das TAGS *tag*=(1 até tn) fazer

VALIDS = 0 // número de pacotes disponíveis para calcular localização da TAG *tag*

para cada uma das 3 posições *pos* da lista *LAST_TAG_POS[tag]* com *pos*=(1 até 3) fazer

se *time.LAST_TAG_POS[tag][pos]*!=NULL então // existe(m) pacote(s)

incrementar *VALIDS*

fse

fpara

// 1) há pacotes dos 3 APs do mesmo conjunto => pode-se tentar calcular localização da *tag*

se (*VALIDS* == 3) então

// 2) o pacote na posição 2 é antigo demais => é apagado

se ((*time.LAST_TAG_POS[tag][1]* - *time.LAST_TAG_POS[tag][2]*) > DELTAT) então

LAST_TAG_POS[tag][2] = NULL

decrementar *VALIDS*

fse

// 3) o pacote na posição 1 é antigo demais => é apagado

se ((*time.LAST_TAG_POS[tag][2]* - *time.LAST_TAG_POS[tag][1]*) > DELTAT) então

LAST_TAG_POS[tag][1] = NULL

decrementar *VALIDS*

fse

// 4)

se (*LAST_TAG_POS[tag][1]* != NULL) então

// 4.1) o pacote na posição 3 é antigo demais => é apagado

se ((*time.LAST_TAG_POS[tag][1]* - *time.LAST_TAG_POS[tag][3]*) > DELTAT) então

LAST_TAG_POS[tag][3] = NULL

decrementar *VALIDS*

fse

```

// 4.2) o pacote na posição 1 é antigo demais => é apagado
se ((time.LAST_TAG_POS[tag][3] - time.LAST_TAG_POS[tag][1]) > DELTAT) então
    LAST_TAG_POS[tag][1] = NULL
    decrementar VALIDS
fse
fse
// 5)
se ((LAST_TAG_POS[tag][2] != NULL) E ((LAST_TAG_POS[tag][3] != NULL)) então
    // 5.1) o pacote na posição 3 é antigo demais => é apagado
    se ((time.LAST_TAG_POS[tag][2] - time.LAST_TAG_POS[tag][3]) > DELTAT) então
        LAST_TAG_POS[tag][3] = NULL
        decrementar VALIDS
    fse
    // 5.2) o pacote na posição2 é antigo demais => é apagado
    se ((time.LAST_TAG_POS[tag][3] - time.LAST_TAG_POS[tag][2]) > DELTAT) então
        LAST_TAG_POS[tag][2] = NULL
        decrementar VALIDS
    fse
fse
// 6)
se (VALIDS == 3) então
    calcularLocalizacaoTag(tag)
    LAST_TAG_POS[tag][1]=NULL
    LAST_TAG_POS[tag][2]=NULL
    LAST_TAG_POS[tag][3]=NULL
fse
fse
fpara

```

Anexo V Descrição textual dos casos de uso do Sistema Central

1. Descrição Textual do caso de uso “Imprimir Etiqueta de Papel para Etiqueta_RFID”

Super Use Case		
Super Use Case	Enviar ordem para efetuar uma operação sobre etiqueta	
Author	mauro	
Date	11/Set/2010 12:04:19	
Brief Description	O gestor de etiquetas RFID pretende imprimir uma etiqueta de papel	
Preconditions		
Post-conditions	Sucesso: Etiqueta de papel imprimida corretamente. Insucesso: Operação cancelada.	
Cenário Principal	Actor Input	System Response
	1 O gestor de etiquetas envia ao sistema um pedido de impressão duma etiqueta de papel	
	2	O sistema envia dados da etiqueta de papel a imprimir para a impressora
	3 Impressora imprime a etiqueta de papel	
	4 A impressora envia ao sistema o resultado da impressão	
	5	O sistema envia uma mensagem (via DISPLAY) ao gestor de etiquetas RFID a indicar que pode recolher da impressora a etiqueta de papel
	6 O gestor de etiquetas recolhe da impressora a etiqueta de papel	
Cenário alternativo 3a	Actor Input	System Response
Erro de impressão	1 A impressora avisa o sistema que ocorreu um erro na impressão	
	2	O sistema envia uma mensagem (via DISPLAY) ao gestor de etiquetas a dizer que ocorreu erro na impressão

2. Descrição Textual do caso de uso “Atribuir etiqueta_RFID”

Main			
Super Use Case	Enviar ordem para efetuar uma operação sobre etiqueta		
Author	mauro		
Brief Description	Gerir a atribuição de uma etiqueta RFID a um utilizador e registo desse facto na base de dados		
Preconditions			
Post-conditions	Apenas confirmar ou recusar a atribuição de etiqueta RFID		
Date	10/Set/2010 15:27:08		
Cenário Principal		Actor Input	System Response
	1	O utilizador de etiquetas RFID faz um pedido de atribuição de uma etiqueta RFID ao sistema	
	2		O sistema encaminha pedido para o gestor de etiquetas
	3	O gestor de etiquetas RFID confirma a atribuição da etiqueta	
	4		O sistema regista a associação entre o ID da etiqueta (tagID) e os dados do utilizador (ID do utilizador, tipo de utilizador, descrição do utilizador) na lista UserOfTag (D10)
	5		O sistema avisa o gestor de etiquetas RFID que pode entregar a etiqueta ao utilizador
	6	O gestor de etiquetas RFID entrega a etiqueta ao utilizador	
Cenário alternativo 3a): Atribuição de etiqueta RFID rejeitada pelo Gestor de etiquetas RFID		Actor Input	System Response
	1	O gestor de etiquetas RFID recusa a atribuição da etiqueta	
	2	O gestor de etiquetas RFID avisa o utilizador da recusa	
	3		Voltar ao passo 1 do cenário principal
Cenário alternativo 4b): A ligação à base de dados falhou		Actor Input	System Response
	1		O sistema informa o gestor de etiquetas que não foi possível ligar-se à base de dados
	2		O sistema termina a operação de atribuição de etiqueta

Cenário alternativo 4c): A etiqueta RFID consta como atribuída		Actor Input	System Response
	1		O sistema indica que essa etiqueta RFID já está atribuída
	2	O gestor de etiquetas RFID recusa a atribuição da etiqueta RFID	
	3	O gestor de etiquetas RFID assinala a anomalia no sistema	
	4		O sistema regista a anomalia
5		Voltar ao passo 1 do cenário principal	

3. Descrição Textual do caso de uso “Programar etiqueta RFID”

Main			
Super Use Case	Enviar ordem para efetuar uma operação sobre etiqueta		
Date	11/Set/2010 12:25:38		
Brief Description	Gestor de etiquetas RFID pretende programar uma etiqueta RFID		
Author	mauro		
Preconditions			
Post-conditions	A etiqueta RFID é recolhida pelo gestor de etiquetas RFID após programação ou após recusa em reprogramá-la		
Cenário Principal		Actor Input	System Response
	1	O gestor de etiquetas RFID insere a etiqueta RFID no programador	
	2	O gestor de etiquetas RFID envia a ordem de programação da etiqueta RFID ao sistema	
	3		O sistema envia ordem de programação ao leitor/programador de etiquetas RFID
	4	O leitor/programador programa a etiqueta RFID	
	5	O leitor/programador envia ao sistema o resultado da programação	
	6		O sistema envia (via DISPLAY) uma mensagem ao gestor de etiquetas RFID com o resultado da programação da etiqueta (OK ou Erro)

	7	O gestor de etiquetas RFID remove a etiqueta do programador	
Cenário alternativo 3a): A etiqueta RFID já consta na base de dados		Actor Input	System Response
	1		O sistema notifica o gestor de etiquetas RFID de que não é possível programar uma etiqueta que já consta na base de dados.
	2		Voltar ao passo <u>1</u> do cenário principal.
Cenário alternativo 4b): Ocorreu um erro na ligação com o leitor/programador de etiquetas		Actor Input	System Response
	1		O sistema envia ao gestor de etiquetas RFID uma mensagem a indicar que ocorreu um erro na ligação com o leitor/programador
	2		O sistema envia ao gestor de etiquetas RFID uma mensagem a perguntar para este confirmar uma nova tentativa de programação da etiqueta
	3	O gestor de etiquetas RFID confirma a nova tentativa de programação da etiqueta	
	4		Voltar ao passo <u>3</u> do cenário principal
Alternativa ao passo 3 do cenário alternativo 4b): O gestor recusa a reprogramação da etiqueta		Actor Input	System Response
	1	O gestor de etiquetas RFID remove a etiqueta do programador	
	2		Voltar ao passo <u>1</u> do cenário principal

4. Descrição Textual do caso de uso “Recolher etiqueta_RFID”

Main			
Super Use Case	Enviar ordem para efetuar uma operação sobre etiqueta		
Author	mauro		
Date	11/Set/2010 14:48:26		
Brief Description	O gestor de etiquetas RFID recolhe uma etiqueta de um utilizador		
Preconditions			
Post-conditions			
Cenário Principal		Actor Input	System Response
	1	O utilizador indica ao gestor de etiquetas RFID que pretende entregar a etiqueta RFID que lhe foi entregue anteriormente	
	2	O gestor de etiquetas RFID envia ao sistema um pedido de registo da devolução por parte do utilizador	
	3		O sistema apaga a associação entre etiqueta (<i>tagID</i>) e os dados do utilizador (identificador do utilizador, tipo de utilizador, descrição do utilizador) da lista UserOfTag (D10)
	4		O sistema indica ao gestor de etiquetas RFID que efetuou a operação pedida e pode recolher o etiqueta do utilizador
	5	O gestor de etiquetas RFID recolhe a etiqueta do utilizador	
Cenário alternativo 3a): A ligação à base de dados falhou		Actor Input	System Response
	1		O sistema informa o gestor de etiquetas RFID que não foi possível ligar-se com a base de dados
	2		Voltar ao passo 2 do cenário principal

5. Descrição textual do caso de uso “Listar as etiquetas atribuídas aos utilizadores”

Main			
Super Use Case	Sistema Central		
Author	mauro		
Date			
Brief Description	O gestor de etiquetas RFID pretende consultar a lista com as etiquetas atribuídas aos utilizadores		
Preconditions	Existe uma lista com as etiquetas atribuídas aos utilizadores		
Post-conditions			
	Actor Input	System Response	
	1	O gestor de etiquetas RFID pretende consultar a lista com as etiquetas atribuídas aos utilizadores	
	2		O sistema seleciona uma nova entrada da lista UserOfTag (D10)
	4		Apresenta ao gestor o campo “UserID” dessa entrada
	5		Apresenta ao gestor o campo “TagID” dessa entrada
	6		Apresenta ao gestor o campo “UserType” dessa entrada
	7		Volta ao passo <u>2</u>
Cenário alternativo 7a) : Não há mais entradas na lista	Actor Input	System Response	
	1		Termina o caso de uso

6. Descrição Textual do caso de uso “Login”

Main			
Super Use Case	Sistema Central		
Author	mauro		
Date			
Brief Description	Faz a identificação de um utilizador do sistema		
Preconditions			
Post-conditions	<p>Sucesso: Utilizador corretamente identificado perante o sistema como sendo dum dado “tipoU”.</p> <p>Insucesso: Utilizador não possui credencias (<i>login,password</i>) válidas.</p>		
Flow of Events		Actor Input	System Response
	1	O utilizador pretende fazer login	
	2		Pede ao utilizador para se identificar. Pede <i>Login</i> e <i>Password</i>
	3	Introduz <i>login</i> e <i>password</i>	
	4		Consulta a base de dados dos (perfis de) utilizadores registados no sistema
	5		As credenciais (<i>login, password</i>) são válidas.
	6		Ativar as funcionalidades correspondentes ao tipo de utilizador (“tipoU”)
	7		Devolve o tipo do utilizador (“tipoU”)
Cenário alternativo 5b) Credencias inválidas		Actor Input	System Response
	1		Envia a mensagem de erro ao utilizador a indicar que o “ <i>login</i> ” e/ou “ <i>password</i> ” estão errados.
	2		Voltar ao passo <u>2</u> do cenário principal

7. Descrição Textual do caso de uso “Logout”

Main			
Super Use Case	Sistema Central		
Author	mauro		
Date			
Brief Description	Encerrar a sessão de trabalho de um utilizador do sistema		
Preconditions			
Post-conditions			
Flow of Events	Actor Input	System Response	
	1	O utilizador pretende fazer <i>logout</i>	
	2		O sistema envia a mensagem ao utilizador: “Pretende encerrar a sessão de trabalho?”
	3	Clica o botão “Sim”	
	4		Fecha todas as ligações a bases de dados
	5		O sistema desativa todas as funcionalidades exceto “Login”

8. Descrição Textual do caso de uso “Inicializar a lista de acessos às zonas do edifício”

Main			
Super Use Case	Sistema Central		
Author	mauro		
Date	5/Dez/2010 22:24:26		
Brief Description	Inicializar a lista que define para cada tipo de utilizador qual o tipo de acesso que tem a cada zona do edifício		
Preconditions			
Post-conditions	Cada linha da lista de acesso informa se uma zona é permitida ou interdita. Se for interdita, indica o tipo de alarme a emitir quando essa interdição for violada.		
Flow of Events	Actor Input	System Response	
	1	O administrador do sistema pretende inicializar a lista de acesso às zonas do edifício	
	2		<<Include>>: “Login”
	3		Selecionar o 1º tipo de utilizador (<i>tu</i>)
	4		Colocar a lista de zonas permitidas ao tipo de utilizador (<i>tu</i>) vazia

	5		Selecionar a primeira zona do edifício (Z) da lista <i>ListZones</i> (D9)
	6		Agregar o tipo de alerta definido por omissão (Ad) à zona Z do edifício e inserir o par (Z,Ad) na lista interdita do tipo de utilizador (tu)
	7		Avançar para a próxima zona (Z) da lista <i>ListZones</i> (D9)
	8		Voltar ao passo <u>6</u>
	9		Avançar para o próximo tipo de utilizador (tu)
	10		Voltar ao passo <u>1</u>
	11		<<Include>>: “Logout”
Cenário alternativo 3a): O perfil introduzido no login (<i>tipoU</i>) não é de “administrador do sistema”		Actor Input	System Response
	1		Enviar uma mensagem de erro a indicar que “Para inicializar a lista de acessos às zonas do edifício é preciso ter perfil de administrador do sistema”
	2		Voltar ao passo <u>1</u> do cenário principal
Cenário alternativo 4b): a lista de acessos já existe		Actor Input	System Response
	1		Enviar a mensagem “A lista de acessos às zonas do edifício já existe. Pretende apagá-la?”
	2	O administrador decide apagar a lista de acessos	
	3		Apagar a lista de acessos
	4		Voltar ao passo <u>4</u> do cenário principal
Alternativa 2a) do cenário alternativo 4b): o administrador decide não apagar a lista de acessos		Actor Input	System Response
	1	O administrador do sistema decide não inicializar de novo (apagar) a lista de acessos às zonas do edifício	
	2		Voltar ao passo <u>11</u> do cenário principal

9. Descrição Textual do caso de uso “Alterar a lista de acessos às zonas do edifício”

Main			
Super Use Case	Sistema Central		
Author	mauro		
Date	5/Dez/2010 22:24:26		
Brief Description	Alterar as zonas permitidas/interditas para um dado tipo de utilizador		
Preconditions			
Post-conditions	Mudou-se uma zona da lista permitida (interdita) para a zona interdita (permitida)		
		Actor Input	System Response
	1	O administrador do sistema pretende alterar as zonas permitidas/interditas	
	2		<<Include>>: “Login”
	3		Enviar a mensagem “Qual o tipo de utilizador (<u>tu</u>) para qual pretende alterar as zonas de acesso?”
	4	Introduz o tipo de utilizador (<u>tu</u>)	
	5		Pedir “Qual a zona a alterar?”
	6	Introduz a zona a alterar (<u>Z</u>)	
	7		Apagar a zona <u>Z</u> da lista “permitida” ao tipo de utilizador <u>tu</u>
	8		A zona <u>Z</u> é inserida na lista “interdita” ao tipo de utilizador <u>tu</u>
	9		Pede ao administrador qual o tipo de alerta a emitir quando o utilizador entrar nesta zona <u>Z</u> .
	10	Define tipo de alerta (<u>ta</u>)	
	11		O tipo de alerta (<u>ta</u>) é agregado à zona <u>Z</u> na lista de “zonas interditas” do tipo de utilizador em causa
	12		<<Include>>: “logout”
Cenário alternativo 3a): o perfil introduzido no login “Tipo U” não é de “administrador do sistema”		Actor Input	System Response
	1		Enviar mensagem de erro a indicar que “para alterar a lista de acessos às zonas do edifício é preciso perfil de administrador do sistema”
	2		Voltar ao passo <u>1</u> do cenário principal

Cenário alternativo 5b): tipo de utilizador (<i>tu</i>) inválido		Actor Input	System Response
	1		Enviar mensagem de erro a indicar que “o tipo de utilizador (<i>tu</i>) é inválido”
	2		Voltar ao passo <u>3</u> do cenário principal
Cenário alternativo 7c): mudar uma zona da lista interdita		Actor Input	System Response
	1		Apagar a zona <u>Z</u> da lista “interdita” ao tipo de utilizador em causa (<i>tu</i>)
	2		A zona <u>Z</u> é inserida na lista “permitida” ao tipo de utilizador <i>tu</i>

10. Descrição Textual do caso de uso “Registrar utilizador do sistema”

Main																																		
Super Use Case	Sistema Central																																	
Author	mauro																																	
Date	5/Dez/2010 22:24:26																																	
Brief Description	O administrador do sistema pretende registar um utilizador (do sistema) de modo a este ter acesso ao sistema																																	
Preconditions																																		
Post-conditions	Sucesso: utilizador criado com sucesso. Insucesso: operação cancelada.																																	
	<table border="1"> <thead> <tr> <th></th> <th>Actor Input</th> <th>System Response</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>O Administrador do sistema pretende criar um novo utilizador</td> <td></td> </tr> <tr> <td>2</td> <td></td> <td><<Include>>: Login</td> </tr> <tr> <td>3</td> <td></td> <td>Pede o “Login do utilizador a criar”</td> </tr> <tr> <td>4</td> <td>O administrador do sistema introduz o <i>login</i> do novo utilizador</td> <td></td> </tr> <tr> <td>5</td> <td></td> <td>O sistema verifica se o login do novo utilizador já existe</td> </tr> <tr> <td>6</td> <td></td> <td>O sistema pede a “<i>Password</i> do utilizador a criar”</td> </tr> <tr> <td>7</td> <td>O administrador insere a nova <i>password</i></td> <td></td> </tr> <tr> <td>8</td> <td></td> <td>O sistema pede para “Confirmar a password do utilizador a criar”</td> </tr> <tr> <td>9</td> <td>O administrador insere a <i>password</i> novamente</td> <td></td> </tr> <tr> <td>10</td> <td></td> <td>Pede para escolher o tipo de utilizador</td> </tr> </tbody> </table>		Actor Input	System Response	1	O Administrador do sistema pretende criar um novo utilizador		2		<<Include>>: Login	3		Pede o “Login do utilizador a criar”	4	O administrador do sistema introduz o <i>login</i> do novo utilizador		5		O sistema verifica se o login do novo utilizador já existe	6		O sistema pede a “ <i>Password</i> do utilizador a criar”	7	O administrador insere a nova <i>password</i>		8		O sistema pede para “Confirmar a password do utilizador a criar”	9	O administrador insere a <i>password</i> novamente		10		Pede para escolher o tipo de utilizador
	Actor Input	System Response																																
1	O Administrador do sistema pretende criar um novo utilizador																																	
2		<<Include>>: Login																																
3		Pede o “Login do utilizador a criar”																																
4	O administrador do sistema introduz o <i>login</i> do novo utilizador																																	
5		O sistema verifica se o login do novo utilizador já existe																																
6		O sistema pede a “ <i>Password</i> do utilizador a criar”																																
7	O administrador insere a nova <i>password</i>																																	
8		O sistema pede para “Confirmar a password do utilizador a criar”																																
9	O administrador insere a <i>password</i> novamente																																	
10		Pede para escolher o tipo de utilizador																																

	11	Seleciona o tipo de utilizador	
	12		O sistema armazena em BD os dados de identificação do utilizador criado
	13		<<Include>>: Logout
Cenário alternativo 3a): O utilizador não é “administrador do sistema”		Actor Input	System Response
	1		Enviar mensagem de erro a Indicar que “Não é administrador do sistema”
	2		Voltar ao passo 2 do cenário principal
Cenário alternativo 6b): utilizador existente		Actor Input	System Response
	1		Enviar mensagem de erro a indicar que “Não é possível criar um utilizador existente, tente inserir um utilizador diferente”
	2		Voltar ao passo 3 do cenário principal
Cenário alternativo 10c): as passwords não são iguais		Actor Input	System Response
	1		Enviar mensagem de erro a indicar que “As passwords não são iguais”
	2		Voltar ao passo 6 do cenário principal

11. Descrição Textual do caso de uso “Criar perfil de administrador do sistema”

Main			
Super Use Case	Sistema Central		
Author	mauro		
Date	5/Dez/2010 22:24:26		
Brief Description	O administrador da empresa pretende criar um perfil de administrador do sistema		
Preconditions			
Post-conditions	Sucesso: O perfil de administrador do sistema foi criado. Insucesso: A operação foi cancelada.		
		Actor Input	System Response
	1	O administrador do sistema pretende criar um <i>login</i> para administrador do sistema	
	2		<<include>>: Login
	3		Pede o “login do utilizador do sistema a criar”
	4	O administrador da empresa	

		introduz <i>login</i> do novo administrador do sistema	
	5		O sistema verifica se o <i>login</i> do novo utilizador já existe
	6		O sistema pede a “palavra-passe do utilizador a criar”
	7	O administrador da empresa insere a nova palavra-passe	
	8		O sistema pede para “confirmar a palavra-passe do utilizador a criar”
	9	O administrador da empresa insere a palavra-passe novamente	
	10		Definir o “ <i>tipoU</i> = admin do sistema”
	11		O sistema armazena em BD os dados de identificação do utilizador criado
Cenário alternativo 3a): O utilizador não é “administrador da empresa”		Actor Input	System Response
	1		Enviar mensagem de erro a indicar que “Não é administrador da empresa”
	2		Voltar ao passo <u>2</u> do cenário principal
Cenário alternativo 6b): Utilizador existente		Actor Input	System Response
	1		Enviar mensagem de erro a indicar que “Não é possível criar um utilizador existente, tente inserir um utilizador diferente”
	2		Voltar ao passo <u>3</u> do cenário principal
Cenário alternativo 10c): as palavras-passe não são iguais		Actor Input	System Response
	1		Enviar mensagem de erro a indicar que “As palavras-passe não são iguais”
	2		Voltar ao passo <u>6</u> do cenário principal

12. Descrição textual do caso de uso “Emitir sinal de alerta”

Main			
Super Use Case	Sistema Central		
Author	mauro		
Date	1/Dez/2010 19:47:00		
Brief Description	Numa situação de violação numa zona interdita, por parte de um utilizador, o sistema consulta a prioridade dos diferentes tipos de alarme associados a esse tipo de utilizador (sirene, BIP, telemóvel) e alerta os seguranças através desse tipo de alarme		
Preconditions			
Post-conditions			
Cenário Principal		Actor Input	System Response
	1		O sistema consulta os dados relativos a um dado utilizador de etiqueta RFID em base de dados
	2		O sistema notifica os seguranças através do tipo de alerta mais prioritário (sirene, BIP, ou telemóvel)
	3		O sistema notifica os seguranças através do tipo de alerta com prioridade secundária (sirene, BIP, ou telemóvel)
	4		O sistema notifica os seguranças através do tipo de alerta com menor prioridade (sirene, BIP, ou telemóvel)
Cenário alternativo 1a): A ligação à base de dados falhou		Actor Input	System Response
	1		O sistema informa o administrador do sistema de que não foi possível ligar-se à base de dados numa situação de alerta.
	2		Voltar ao passo 1 do cenário principal

13. Descrição textual do caso de uso “Configurar AP”

Main			
Super Case	Use	Sistema Central	
Author		mauro	
Date		12/Abr/2011 19:00:00	
Brief Description		O administrador do sistema pretende configurar um Ponto de Acesso (AP)	
Preconditions			
Post-conditions			
Cenário Principal		Actor Input	System Response
	1	O administrador do sistema pretende configurar um AP.	
	2		Pergunta ao administrador do sistema “quer usar uma configuração previamente guardada?”
	3	O administrador do sistema decide não usar uma configuração previamente guardada	
	4		O sistema pede ao administrador do sistema os vários campos passíveis de serem configurados
	5	Indica que quer configurar TAG(s), incluindo o modo como enviam dados para o AP	
	6	Define o tipo de funcionamento do AP (normal, parar, retornar e <i>reset</i>)	
	7	Define o tipo de porta que pretende usar para comunicar com o AP (tcpip, rs-232, rs-485,etc.)	
	8	Define o ID da rede em que se insere o AP	
	9	Define o nível mínimo de potência do sinal RF (RSSI) a considerar como receção válida	
	10	Especifica dados personalizados (<i>user data</i>) com a descrição do AP	
	11		O sistema envia a configuração para o AP
	12		O sistema espera a resposta com o resultado da configuração
	13		O sistema informa o administrador do sistema que a configuração foi efetuada com sucesso
14		O sistema pergunta ao administrador do sistema se “pretende guardar a configuração do AP?”	

	15	O administrador do sistema escolhe guardar a configuração do AP.	
	16		O sistema guarda a configuração do AP
	17		O sistema informa o administrador do sistema que a gravação da configuração foi efetuada com sucesso
	18		Termina a configuração do AP
Cenário alternativo 3a): o administrador do sistema decide usar uma configuração previamente guardada	1		Limpa a configuração atual do AP
	2		O sistema pergunta ao administrador do sistema "Qual a configuração guardada que pretende usar para reconfigurar o AP?"
	3	O administrador do sistema seleciona a configuração	
	4		O sistema lê essa configuração
	5		Salta para o passo <u>11</u> do cenário principal
Cenário alternativo 7b): o acesso ao AP faz-se por TCPIP ("TCP server mode")		Actor Input	System Response
	1	Escolhe a porta do protocolo	
	2	Define o delimitador dos pacotes de dados	
	3	Definir a porta TCP local (sistema central)	
	4	Definir o máximo de ligações	
	5	Definir os valores de "time out"	
6		Salta para o passo <u>11</u> do cenário principal	
Cenário alternativo 13c): ocorreu um erro na configuração do AP		Actor Input	System Response
	1		O sistema notifica o administrador do sistema que ocorreu um erro na configuração do AP
	2		O sistema pergunta ao administrador do sistema se quer tentar novamente o envio de configuração
	3	O administrador do sistema confirma o envio da configuração	
4		Salta para o passo <u>11</u> do cenário principal	
Exceção: o AP não respondeu ao pedido de configuração num tempo máximo definido		Actor Input	System Response
	1		O sistema notifica o administrador do sistema que o AP não respondeu ao pedido de configuração
	2		O sistema pergunta ao administrador do sistema se "quer tentar novamente o envio de configuração?"
3	O administrador do sistema confirma o reenvio da configuração		

	4		Salta para o passo <u>11</u> do cenário principal
Alternativa (3a) do cenário alternativo 7c): o método de acesso ao AP é "TCP client mode"		Actor Input	System Response
	1	Definir o IP do hospedeiro	
	2	Definir a porta do hospedeiro	
	3	Definir o valor de "time out"	
	4		Salta para o passo <u>11</u> do cenário principal
Alternativa (3b) do cenário alternativo 7c): o método de acesso ao AP é "UPD server/client mode"		Actor Input	System Response
	1	Escolher o modo de operação	
	2	Definir a porta local (do sistema central) a utilizar	
	3	Definir o IP inicial para cada gama de IPs a usar nos APs que vão ser auscultados	
	4	Definir o IP final para cada gama de IPs a usar nos APs que vão ser auscultados	
	5	Definir a porta do AP a utilizar em cada gama de IPs	
	6		Salta para o passo <u>11</u> do cenário principal
Cenário alternativo 16d): o administrador escolhe não guardar a configuração do AP		Actor Input	System Response
	1		Salta para o passo <u>18</u> do cenário principal
Cenário alternativo 17e): ocorreu um erro na gravação da configuração do AP		Actor Input	System Response
	1		Continua no passo <u>18</u> no cenário principal

14. Descrição textual do caso de uso “Criar dados do AP”

Main		
Super Case Use	Sistema Central	
Author	mauro	
Date		
Brief Description	O administrador da empresa pretende criar os dados que descrevem um AP	
Preconditions		
Post-conditions	Sucesso: Informação criada com sucesso Insucesso: Operação cancelada	
	Actor Input	System Response
1	O administrador do sistema pretende criar dados que descrevem o AP	
2		O sistema pede o <u>ID</u> do AP
3	Introduz o ID do AP → <u>apId</u>	
4		O sistema pede a coordenada <u>X</u> da localização do AP
5	Introduz a coordenada X	
6		O sistema pede a coordenada <u>Y</u> da localização do AP
7	Introduz a coordenada Y	
8		O sistema pede a coordenada <u>Z</u> da localização do AP
9	Introduz a coordenada Z	
10		Verifica se existe outro AP com X,Y,Z iguais
11		O sistema pede <u>descrição</u> do AP
12	Introduz a descrição do AP	
13		O sistema pede o <u>conjunto</u> do AP
14	Introduz o conjunto do AP → <u>apSet</u>	
15		O sistema pede o <u>endereço TCPIP</u> do AP
16	Introduz o endereço TCPIP	
17		O sistema pergunta ao utilizador se “Pretende guardar os dados do AP?”
18	Administrador do sistema opta por guardar os dados	

	19		O sistema guarda os dados AP (estrutura D2) na lista com dados dos APs (estrutura D6)
	20		Adicionar o AP " <i>apId</i> " ao conjunto " <i>apSet</i> " (estrutura D7 , que por sua vez é um elemento da lista D3)
	21		Voltar ao passo 1
Cenário alternativo 4a) : Já existe um AP com esse ID		Actor Input	System Response
	1		Avisa que já existe um AP com esse ID
	2		Voltar ao passo <u>2</u> no cenário principal
Cenário alternativo 11b) : Já existe outro AP com as mesmas coordenadas		Actor Input	System Response
	1		Voltar ao passo <u>4</u> do cenário principal
Cenário alternativo 15c) : Não existe nenhum conjunto com o identificador escolhido (<i>AP_SET</i>)		Actor Input	System Response
	1		Voltar ao passo <u>13</u> do cenário principal
Cenário alternativo 15d) : O conjunto não foi escolhido		Actor Input	System Response
	1		Coloca <i>apSet=NULL</i>
	2		Retomar o passo <u>15</u> do cenário principal
Cenário alternativo 15e) : O conjunto <i>AP_SET</i> já contém 3 APs		Actor Input	System Response
	1		Voltar ao passo <u>13</u> do cenário principal
Cenário alternativo 18f) : O administrador opta por não guardar os dados		Actor Input	System Response
	1	Escolheu não guardar os dados	
	2		Voltar ao passo <u>1</u> do cenário principal

Alternativa (4a) do cenário alternativo 5b): Já existe outro AP com as mesmas coordenadas		Actor Input	System Response
	1		Informa o administrador que já existe outro AP com X,Y e Z iguais.
	2		Voltar ao passo <u>4</u> no cenário principal
Cenário alternativo 5c): O administrador escolhe alterar a coordenada Z		Actor Input	System Response
	1		Pede ao administrador para introduzir o novo valor da coordenada Z
	2	Introduz coordenada Z	
	3		Verifica se existe outro AP com X,Y,Z iguais
	4		Guarda o novo valor da coordenada Z (em D2)
	5		Volta ao passo <u>1</u> do cenário principal
Alternativa (4a) do cenário alternativo 5c): Já existe outro AP com as mesmas coordenadas		Actor Input	System Response
	1		Informa o administrador que já existe outro AP com X,Y e Z iguais.
	2		Volta ao passo <u>4</u> no cenário principal
Cenário alternativo 5d): O administrador escolhe alterar a <u>descrição</u>		Actor Input	System Response
	1		Pede ao administrador para introduzir a nova descrição
	2	Introduz a descrição	
	3		Guarda a nova descrição (em D2)
	4		Volta ao passo <u>1</u> do cenário principal
Cenário alternativo 5e): O administrador escolhe alterar o conjunto do AP		Actor Input	System Response
	1		O sistema pede o novo conjunto do AP
	2	Introduz o conjunto do AP → <u>apSetNew</u>	
	3		Remove o o ID do AP (“apId”) do conjunto atual “ <u>apSet</u> ” (estrutura D7, que faz parte da lista D3)
	4		Guarda o novo valor do conjunto <u>apSetNew</u> (estrutura D2)
	5		Adiciona o AP “ <u>apId</u> ” ao novo conjunto “ <u>apSetNew</u> ” (estrutura D7)
Cenário alternativo 5f): O administrador escolhe alterar o endereço TCPIP		Actor Input	System Response
	1		Pede ao administrador para introduzir a novo endereço TCPIP
	2	Introduz o endereço TCPIP	
	3		Guarda o novo TCPIP (em D2)
	4		Volta ao passo <u>1</u> do cenário principal

Alternativa (3a) do cenário alternativo 5e): Não existe nenhum conjunto com esse "apSet"		Actor Input	System Response
	1		Volta ao passo <u>1</u> no cenário alternativo 5e)
Alternativa (3b) do cenário alternativo 5e): O conjunto "apSet" já contém 3 APs		Actor Input	System Response
	1		Volta ao passo <u>1</u> no cenário alternativo 5e)
Alternativa (3c) do cenário alternativo 5e): O AP não está inserido em qualquer conjunto ("apSet"=NULL)		Actor Input	System Response
	1		Avança para o passo <u>4</u> do cenário alternativo 5e)

16. Descrição textual do caso de uso "Remove AP do sistema"

Main																															
Super Use Case	Sistema Central																														
Author	mauro																														
Date																															
Brief Description	O administrador da empresa pretende remover um AP do sistema																														
Preconditions																															
Post-conditions	Sucesso: Eliminação efetuada com sucesso Insucesso: Eliminação cancelada																														
	<table border="1"> <thead> <tr> <th></th> <th>Actor Input</th> <th>System Response</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>O administrador do sistema pretende remover um AP</td> <td></td> </tr> <tr> <td>2</td> <td></td> <td>O sistema pede o <u>ID</u> do AP</td> </tr> <tr> <td>3</td> <td>Introduz o ID do AP → <u>apld</u></td> <td></td> </tr> <tr> <td>4</td> <td></td> <td>O sistema pergunta ao utilizador se "Pretende apagar o AP com identificador <u>apld</u>?"</td> </tr> <tr> <td>5</td> <td>O administrador decide que vai eliminar o AP</td> <td></td> </tr> <tr> <td>6</td> <td></td> <td><<include>> Remover o AP do conjunto de APs</td> </tr> <tr> <td>7</td> <td></td> <td>Remover a entrada desse AP (elemento D2) na lista de APs (tabela D6)</td> </tr> <tr> <td>8</td> <td></td> <td>Percorrer a lista <i>PacksLastPosTAG</i> (D5) e eliminar todos os pacotes provenientes desse AP</td> </tr> <tr> <td>9</td> <td></td> <td>Voltar ao passo <u>1</u></td> </tr> </tbody> </table>		Actor Input	System Response	1	O administrador do sistema pretende remover um AP		2		O sistema pede o <u>ID</u> do AP	3	Introduz o ID do AP → <u>apld</u>		4		O sistema pergunta ao utilizador se "Pretende apagar o AP com identificador <u>apld</u> ?"	5	O administrador decide que vai eliminar o AP		6		<<include>> Remover o AP do conjunto de APs	7		Remover a entrada desse AP (elemento D2) na lista de APs (tabela D6)	8		Percorrer a lista <i>PacksLastPosTAG</i> (D5) e eliminar todos os pacotes provenientes desse AP	9		Voltar ao passo <u>1</u>
	Actor Input	System Response																													
1	O administrador do sistema pretende remover um AP																														
2		O sistema pede o <u>ID</u> do AP																													
3	Introduz o ID do AP → <u>apld</u>																														
4		O sistema pergunta ao utilizador se "Pretende apagar o AP com identificador <u>apld</u> ?"																													
5	O administrador decide que vai eliminar o AP																														
6		<<include>> Remover o AP do conjunto de APs																													
7		Remover a entrada desse AP (elemento D2) na lista de APs (tabela D6)																													
8		Percorrer a lista <i>PacksLastPosTAG</i> (D5) e eliminar todos os pacotes provenientes desse AP																													
9		Voltar ao passo <u>1</u>																													

Cenário alternativo 3a): não existe nenhum AP com o ID especificado		Actor Input	System Response
	1		Avisa o administrador do sistema que não existe qualquer AP com esse ID
	2		Voltar ao passo <u>1</u> no cenário principal
Cenário alternativo 5b): O administrador do sistema decide cancelar a eliminação do AP		Actor Input	System Response
	1		Voltar ao passo <u>1</u> no cenário principal

17. Descrição textual do caso de uso “Receber pacote de AP por TCP/IP”

Main			
Super Use Case	Sistema Central		
Author	mauro		
Date	5/Fev/2011 09:02:35		
Brief Description	O sistema está à espera para receber pacotes enviados por um ou vários APs ao mesmo tempo		
Preconditions			
Post-conditions			
Flow of Events			
Cenário Principal		Actor Input	System Response
	1		Ler o pacote do <i>socket</i> adequado
	2		Consultar a tabela que associa os IPs dos APs aos <i>AP_IDs</i> e obter o <i>AP_ID</i> do AP que enviou o pacote. Guardar esse valor no campo <i>AP_ID</i> dum estrutura <i>Packet</i> (D1)
	3		Extrair o campo identificador da TAG do pacote recebido. Guardar esse valor no campo <i>TAG_ID</i> da estrutura <i>Packet</i> (D1)
	4		Extrair o campo <i>RSSI</i> do pacote recebido. Guardar esse valor no campo <i>RSSI_RX</i> da estrutura <i>Packet</i> (D1)
	5		Ler a data atual e guardar esse valor no campo <i>DATE</i> da estrutura <i>Packet</i> (D1)
	6		Ler a hora atual e guardar esse valor no campo <i>TIME</i> da estrutura <i>Packet</i> (D1)
	7		Gerar automaticamente um valor único para identificar o pacote e guardar esse valor no campo <i>PACK_ID</i> da estrutura <i>Packet</i> (D1)
8		<<include>> Guardar pacote recebido dum AP	

	9		<<include>> Calcular localização duma TAG
	10		<<include>> Calcular zona da localização
	11		Terminar caso de uso
Cenário alternativo 3a) : Não existe (estrutura D2 da lista D6) qualquer AP com o identificador <i>AP_ID</i>		Actor Input	System Response
	1		O sistema informa “não existe qualquer AP com o identificador <i>AP_ID</i> ” e rejeita o pacote.
	2		Voltar ao passo <u>1</u> do cenário principal
Cenário alternativo 4b) : Não existe qualquer TAG com o identificador <i>TAG_ID</i>		Actor Input	System Response
	1		O sistema informa que “não existe qualquer TAG com o identificador <i>TAG_ID</i> ” e rejeita o pacote.
	2		Voltar ao passo <u>1</u> do cenário principal
Cenário alternativo 11c): A zona de localização da etiqueta é interdita ao tipo de utilizador em causa.		Actor Input	System Response
	1		<<include>> Emitir sinal de alerta

18. Descrição textual do caso de uso “Guardar pacote recebido dum AP”

Main			
Super Use Case	Sistema Central		
Author	mauro		
Date	5/Fev/2011 09:02:35		
Brief Description	Guardar um pacote recebido dum AP		
Preconditions			
Post-conditions			
Flow of Events			
Cenário Principal		Actor Input	System Response
	1		Obter o identificador da TAG → <code>tagId = packet.get_TAG_ID()</code>
	2		Obter o anterior conjunto que detetou essa TAG → <code>prev_set</code>
	3		Obter o identificador do AP que enviou o pacote recebido, diretamente a partir desse pacote → <code>apid=packet.get_AP_ID()</code>
	4		Obter o valor do conjunto a que corresponde o AP que enviou o pacote recebido (<code>new_set</code>)
5		Comparar o valor de <code>prev_set</code> com o valor <code>new_set</code>	

	7		Apresenta o campo “Descrição”
	8		Apresenta o campo “AP_Set”
	9		Apresenta o campo “TCPIP”
Cenário alternativo 4a) : ID inexistente		Actor Input	System Response
	1		Avisa que “não existe qualquer AP com esse ID
	2		Volta ao passo <u>1</u> do cenário principal

20. Descrição textual do caso de uso “Criar conjunto de APs”

Main			
Super Use Case	Sistema Central		
Author	mauro		
Date			
Brief Description	O administrador da empresa pretende criar um conjunto de APs		
Preconditions			
Post-conditions	Sucesso: Conjunto criado com sucesso Insucesso: Operação cancelada		
		Actor Input	System Response
	1	O administrador do sistema pretende criar um conjunto de APs	
	2		O sistema pede para “introduzir o ID do conjunto”
	3	Introduz o ID do conjunto (<i>setId</i>)	
	4		<<include>> Adicionar AP a um conjunto de APs (<i>setId</i>)
	5		Pergunta se “pretende inserir mais APs no conjunto?”
	6	Decide não inserir mais APs	
	7		O sistema pergunta se “pretende guardar os dados do conjunto?”
	8	Confirma que pretende guardar os dados do conjunto	
	9		Guardar os dados do conjunto (estrutura D7 incluída na lista D3)
Cenário alternativo 4a) : Já existe um conjunto com o ID escolhido		Actor Input	System Response
	1		Avisa que “já existe um conjunto com o ID escolhido (<i>setId</i>)”
	2		Voltar ao passo <u>2</u> no cenário principal

Cenário alternativo 4b) : O conjunto já contém o máximo de APs permitido (três)		Actor Input	System Response
	1		Avisa que “o conjunto com o ID escolhido já contém o máximo de APs permitido”
	2		Avança para o passo <u>7</u> do cenário principal
Cenário alternativo 6c) : Decide inserir mais APs		Actor Input	System Response
	1		Voltar ao passo <u>4</u> no cenário principal

21. Descrição textual do caso de uso “Adicionar AP a um conjunto de APs”

Main			
Super Use Case	Sistema Central		
Author	mauro		
Date			
Brief Description	Adicionar um AP a um determinado conjunto de APs		
Preconditions	Foi especificado o ID de um conjunto de APs (<i>setId</i>)		
Post-conditions			
		Actor Input	System Response
	1		Pergunta “qual o ID do AP que pretende inserir no conjunto?”
	2	Introduz o ID do AP que pretende inserir no conjunto (<i>apId</i>)	
	3		O sistema adiciona o AP “apId” ao conjunto “setId” (estrutura D7 pertencente à lista D3)
	4		Altera o conjunto a que pertence o AP para “setId” (<i>campo AP_SET na estrutura D2</i>)
Cenário alternativo 1a) : O conjunto já contém o máximo de APs permitido (três)		Actor Input	System Response
	1		Avisa que “o conjunto <i>setId</i> já contém o máximo de APs permitido”
	2		Termina o caso de uso
Cenário alternativo 3b) : Não existe nenhum AP com esse ID		Actor Input	System Response
	1		Voltar ao passo <u>1</u> no cenário principal

22. Descrição textual do caso de uso “Remover AP do conjunto de APs”

Main		
Super Use Case	Sistema Central	
Author	mauro	
Date		
Brief Description	Remover um AP do conjunto em que está inserido	
Preconditions	Foi especificado o ID de um AP (<i>aplId</i>)	
Post-conditions		
	Actor Input	System Response
	1	Procurar qual o conjunto a que pertence o AP identificado como <i>aplId</i> (campo <i>AP_SET</i> da tabela D2) → <i>setAP</i>
	2	Eliminar o AP <i>aplId</i> do conjunto em causa (<i>setAP</i>) (tabela D7 , incluída na lista D3)
	3	Marcar o AP como não pertencente a nenhum conjunto (campo <i>AP_SET=NULL</i> na tabela D2)
Cenário alternativo 2a): O AP <i>aplId</i> não está inserido em qualquer conjunto (<i>AP_SET=NULL</i>)	Actor Input	System Response
	1	Terminar o caso de uso

23. Descrição textual do caso de uso “Eliminar conjunto de APs”

Main		
Super Use Case	Sistema Central	
Author	mauro	
Date		
Brief Description	Eliminar um conjunto de APs	
Preconditions		
Post-conditions		
	Actor Input	System Response
	1	O administrador do sistema pretende eliminar um conjunto de APs
	2	O sistema pede “Qual o ID do conjunto de APs a eliminar?”
	3	Introduz o ID do AP a eliminar (<i>APset</i>)

	6		Avança o apontador “pos” para a próxima posição da lista de APs do conjunto
	7		Voltar ao passo <u>5</u>
Cenário alternativo 4a): não existe nenhum conjunto com o ID escolhido		Actor Input	System Response
	1		Avisa que “não existe qualquer conjunto com esse ID (setId)”
	2		Voltar ao passo <u>1</u> no cenário principal
Cenário alternativo 6b): Não há mais APs no conjunto para mostrar		Actor Input	System Response
	1		Termina o caso de uso

25. Descrição textual do caso de uso “Enviar Comando ao AP para Ler a Configuração”

Main			
Super Use Case	Sistema Central		
Author	mauro		
Date			
Brief Description	Enviar um comando ao AP para ler dados da sua configuração		
Preconditions			
Post-conditions			
		Actor Input	System Response
	1	O administrador do sistema pretende enviar um comando ao AP para ler dados da sua configuração	
	2		Envia a mensagem “Qual o tipo de dados que pretende ler diretamente do AP (dados da TAG, S/N da Tag, S/N do AP, ID da rede do AP, dados do utilizador, versão do <i>firmware</i> do AP)?”
	3	Escolhe o tipo de dados a ler (<i>tData</i>)	
	4		O sistema envia o comando ao AP com o tipo de dados (<i>tData</i>) pedido
	5		Recebe a resposta do AP
	6		Apresenta os dados recebidos
Cenário alternativo 4a): O tipo de dados pedido é inválido		Actor Input	System Response
	1		Avisa que o tipo de dados pedido é inválido
	2		Voltar ao passo <u>2</u> no cenário principal

Exceção 6a): AP não respondeu dentro do tempo limite		Actor Input	System Response
	1		Avisa que “o AP não respondeu dentro do tempo limite”
	2		Voltar ao passo <u>1</u> no cenário principal

26. Descrição textual do caso de uso “Calcular localização duma TAG”

Main			
Super Use Case	Sistema Central		
Author	mauro		
Date	5/Fev/2011 09:02:35		
Brief Description	Calcular localização duma TAG (combinando a distância da TAG a vários APs cujas posições são conhecidas)		
Preconditions			
Post-conditions			
Flow of Events		Actor Input	System Response
Cenário Principal	1		Pegar na primeira TAG (<i>tagId</i>) da lista D4
	2		Verificar se há 3 pacotes disponíveis para essa 'tagId' na lista <i>PacksLastPosTAG[tagId]</i> (D5)
	3		Para cada par de pacotes dessa 'tagId' {(1,2), (1,3) e (2,3)}, verificar se os 2 pacotes do par são válidos (chegaram no intervalo[t-DELTAT, t+DELTAT], em que 't' é o tempo atual) para calcular a localização de 'tagId' (usar a lista <i>PacksLastPosTAG[tagId]</i> (D5))
	4		Com base nas 3 localizações/pacotes de 'tagId' calcular a sua localização P =(Px,Py,Pz), usando por exemplo o método de triangulação. Guardar a localização P calculada.
	5		Avançar para a próxima TAG da lista D4
	6		Voltar ao passo <u>2</u> do cenário principal
Cenário alternativo 3a): Não há 3 pacotes disponíveis		Actor Input	System Response
	1		Voltar ao passo <u>5</u> no cenário principal
Cenário alternativo 4b): Um dos pacotes do par, na posição 'x', é antigo demais em relação ao outro		Actor Input	System Response
	1		Apagar o pacote na posição 'x' (<i>PacksLastPosTAG[tag][x]</i> (D5))
	2		<<include>>: Mostrar a lista D5 ao utilizador
	3		Avançar para o passo <u>5</u> do cenário principal
Cenário alternativo 5c): Não há mais TAGs na lista		Actor Input	System Response
	1		Terminar o caso de uso

27. Descrição textual do caso de uso “Calcular zona de localização”

Main		
Super Use Case	Sistema Central	
Author	mauro	
Date	3/Julho/2011 09:35:00	
Brief Description	Calcular a zona de localização que corresponde à posição estimada (P) para uma etiqueta RFID	
Preconditions	Disponer de uma posição da etiqueta RFID (P) e da geometria das zonas do edifício	
Post-conditions	SUCESSO: devolve o identificador da zona que corresponde à posição P . INSUCESSO: devolve NULL.	
Flow of Events		
Cenário Principal	Actor Input	System Response
	1	Procurar o segmento do edifício (S_{near}) que se encontra à menor distância do ponto $P = (P_x, P_y)$
	2	Considerar $S_{atual} = S_{near}$ Inserir S_{atual} na lista de segmentos da zona(P)
	3	Escolher para P_{atual} um dos pontos extremos de S_{atual} (P1 ou P2)
	4	O ponto terminal da definição da zona (P_{final}) será o outro ponto de S_{atual} não utilizado
	5	Definir a vizinhança $S_{viz}(P_{atual})$ como sendo o conjunto de segmentos em que um dos extremos é P_{atual}
	6	Seleccionar um segmento S do conjunto $viz = S_{viz}(P_{atual}) - S_{atual}$ ainda não usado (<i>viz é do tipo listSegments / D8</i>)
	7	Calcular a direção $dir(S)$ do segmento S , considerando que o vetor direção tem origem em P_{atual} e aponta na direção do outro extremo de S
	8	Calcular o mínimo ($minDir(S)$) e o máximo ($maxDir(S)$) entre a direção de S e de S_{atual}
	9	Voltar ao passo <u>6</u>
	10	Calcular o próximo segmento S_{next} a incluir na zona(P) . Neste cálculo utilizam-se os valores de $minDir(S)$ e $maxDir(S)$ obtidos. O segmento a calcular será aquele que garante que o segmento $S_{p-P_{atual}}$ tem como segmentos vizinhos S_{atual} e S_{next}
	11	$S_{atual} = S_{next}$
	12	Adicionar o segmento S_{atual} à zona(P)
	13	De entre os 2 pontos extremos de S_{atual} , escolher aquele que não é P_{atual} , passando esse a ser o novo P_{atual}
	14	Voltar ao passo <u>5</u>
	15	Z_{teste} = primeira zona da lista listZones (D9) $IDzona(P) = NULL$
16	Comparar zona(P) com Z_{teste}	

	17		Z_{teste} passa a ser a próxima zona da lista <i>listZones</i>
	18		Voltar ao passo <u>16</u>
	19		Terminar o caso de uso
Cenário alternativo 9a) : Não há mais segmentos por utilizar		Actor Input	System Response
	1		Continuar no passo <u>10</u> do cenário principal
Cenário alternativo 14b) : $P_{atual} = P_{final}$		Actor Input	System Response
	1		Continuar no passo <u>15</u> do cenário principal
Cenário alternativo 17c) : $zona(P)$ é igual a Z_{teste}		Actor Input	System Response
	1		$ID_{zona}(P)$ = identificador ($ZONE_ID$) da zona Z_{teste}
	2		Continuar no passo <u>19</u> do cenário principal

28. Descrição textual do caso de uso “Definir Zonas”

Main			
Super Use Case	Sistema Central		
Author	mauro		
Date			
Brief Description	Definir a geometria (conjunto de segmentos) das zonas do edifício		
Preconditions	Existem segmentos para definir as zonas do edifício		
Post-conditions	Dados guardados na lista <i>listZones</i> (D9)		
		Actor Input	System Response
	1		Perguntar “Qual o identificador da zona cuja geometria pretende definir?”
	2	O administrador do sistema introduz o ID da zona a definir (Z_ID)	
	3		Perguntar “Qual o identificador do segmento que pretende adicionar à geometria da zona Z_ID ?”
	4	Introduz o identificador do segmento que pretende adicionar ao conjunto que define a zona Z_ID (S_ID). Este S_ID deve ser um identificador válido na estrutura <i>listSegments</i> (D8).	
	5		Adicionar o identificador de segmento S_ID à lista que define a geometria da zona Z_ID (estrutura D9).
	6		Perguntar “Pretende adicionar mais segmentos à geometria da zona Z_ID ?”

	7	Decide adicionar mais segmentos	
	8		Voltar ao passo 3
	9		Perguntar “Pretende definir a geometria de mais zonas do edifício?”
	10	Decide definir a geometria de mais zonas	
	11		Voltar ao passo 1
	12		Enviar uma mensagem a perguntar “Pretende guardar a geometria das zonas definidas em base de dados?”
	13	Decide guardar as zonas em base de dados	
	14		Guardar a geometria das zonas definidas em base de dados
	15		Terminar o caso de uso
Cenário alternativo 2a): Já existe uma zona com o identificador escolhido		Actor Input	System Response
	1		Enviar uma mensagem a dizer “Já existe uma zona com o identificador escolhido”
	2		Voltar ao passo 1 do cenário principal
Cenário alternativo 5b): Não existe segmento com o identificador escolhido		Actor Input	System Response
	1		Enviar uma mensagem a dizer “Não existe qualquer segmento com o identificador escolhido”
	2		Voltar ao passo 3 do cenário principal
Cenário alternativo 7c): O administrador do sistema não pretende adicionar mais segmentos à zona <i>Z_ID</i>		Actor Input	System Response
	1		Aceitar a zona como válida. A zona é considerada válida se a sua geometria (i) definir um único polígono (fechado), (ii) possuir um número de segmentos ≥ 3 , (iii) não possuir segmentos desligados num ou nos 2 extremos.
	2		Continuar no passo 9 do cenário principal
Alternativa 1a) do cenário alternativo 7c): A geometria da zona não é válida		Actor Input	Sytem Response
	1		Enviar uma mensagem a dizer “Deve reformular a geometria da zona <i>Z_ID</i> ”
	2		Enviar uma mensagem a dizer “Pretende remover um segmento adicionado?”
	3	Decide remover o segmento <i>S_ID_DEL</i>	

	7	Introduz o ponto final do segmento → Pf (Pfx,Pfy,Pfz)	
	8		O sistema calcula a direção do segmento com base em Pi e Pf → direcção
	9		Sistema pergunta ao utilizador do sistema “Pretende guardar os dados do segmento?”
	10	Utilizador do sistema decide guardar o segmento	
	11		Sistema guarda os dados do segmento <i>S_ID</i> (<i>Pi</i> , <i>Pf</i> , <i>direcção</i>) na lista <i>listSegments (D8)</i>
	12		Voltar ao passo 1
Cenário alternativo 4a) : Já existe um segmento com o ID escolhido		Actor Input	System Response
	1		Avisa que “Já existe um segmento com o ID escolhido”
	2		Voltar ao passo 2 no cenário principal
Cenário alternativo 10b) : Utilizador do sistema decide não guardar o segmento		Actor Input	System Response
	1		Continuar no passo 12 do cenário principal

Anexo VI Descrição textual dos casos de uso do Ponto de Acesso (AP)

1. Descrição textual do caso de uso “Receção de mensagem de etiqueta_RFID”

Main			
Super Use Case	AP		
Author	mauro		
Date	1/Dez/2010 23:15:54		
Brief Description	Receção de uma mensagem proveniente dum etiqueta RFID		
Preconditions	A etiqueta RFID emite o sinal RFID a cada 2 segundos		
Post-conditions			
Flow of Events		Actor Input	System Response
	1	A etiqueta RFID envia um sinal RFID com a sua identificação	
	2		O AP recebe da etiqueta RFID uma mensagem via sinal RFID
	3		<<include>>: Enviar pacote construído para o sistema central

2. Descrição textual do caso de uso “Enviar pacote construído para o sistema central”

Main			
Super Use Case	Sistema Central		
Author	mauro		
Date	1/Dez/2010 18:41:31		
Brief Description	Depois de receber uma mensagem dum etiqueta RFID, o sistema cria um pacote e envia-o para o sistema central		
Preconditions			
Post-conditions			
Flow of Events		Actor Input	System Response
	1		Juntar o ID da Tag
	2		Juntar o RSSI da Tag
	3		Juntar o <i>Link quality</i> da Tag
	4		Juntar o Estado da Tag
	5		Converter os campos para o pacote a enviar
	6		Enviar o pacote para o sistema central

3. Descrição textual do caso de uso “Responder a pedidos de leitura da configuração”

Main			
Super Use Case	AP		
Author	mauro		
Date	12/Abr/2011 20:00:00		
Brief Description	O AP responde a pedidos de leitura de dados da configuração feitos pelo sistema central		
Preconditions			
Post-conditions			
Cenário Principal		Actor Input	System Response
	1		Recebe um comando do sistema central para ler dados de configuração
	2		Descodifica qual o tipo de dados pretendido (dados duma TAG, S/N duma TAG, S/N do AP, ID da rede do AP, dados do utilizador, versão do <i>firmware</i> do AP)
	3		Envia ao sistema central um pacote contendo o tipo de dados do AP pedidos
Cenário alternativo 3a) : O tipo de dados pedidos tem a ver com uma etiqueta RFID (TAG)		Actor Input	System Response
	1		O AP envia o pedido de leitura à TAG pretendida.
	2		O AP espera uma mensagem dessa TAG via sinal RFID
	3		Envia para o sistema central um pacote contendo os dados recebidos dessa TAG
	4		Terminar o caso de uso

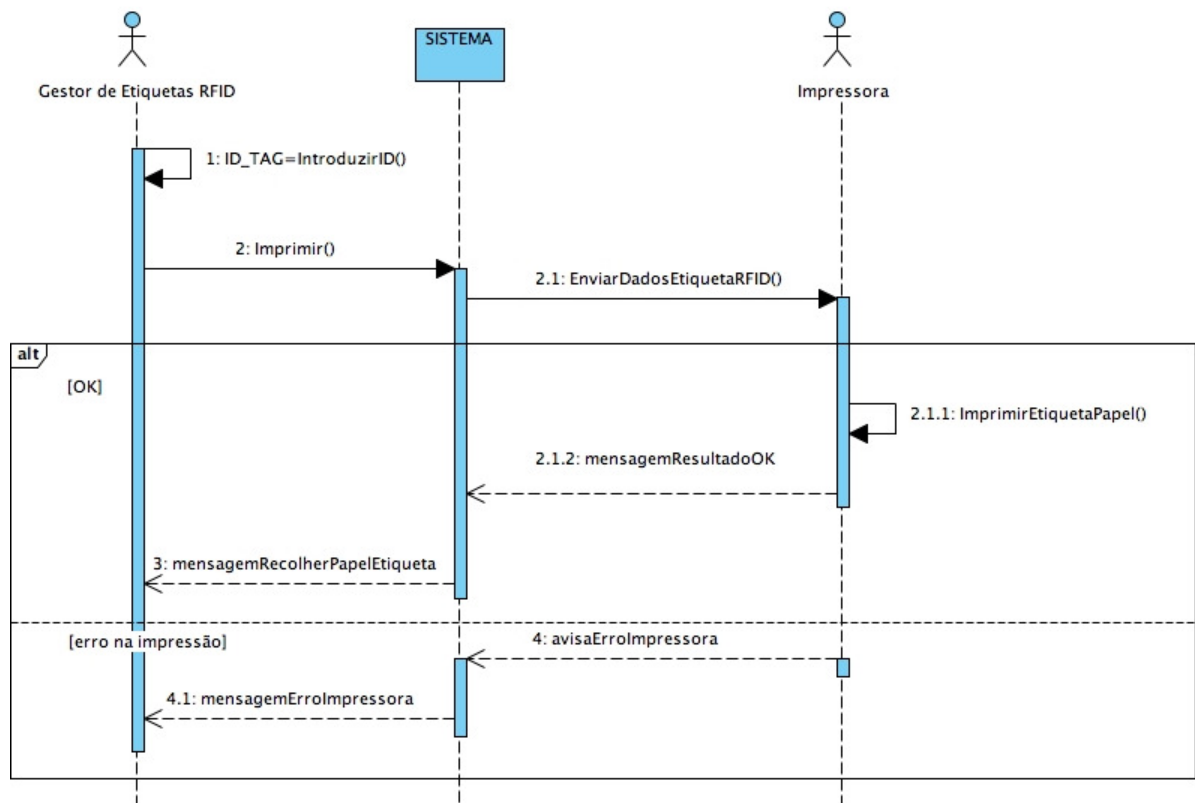
4. Descrição textual do caso de uso “Efetuar configuração do AP”

Main			
Super Use Case	AP		
Author	mauro		
Date	2/Abr/2011 18:00:00		
Brief Description	Efetuar a configuração do AP de acordo com os comandos recebidos do sistema central		
Preconditions			
Post-conditions			
Cenário principal	Actor Input	System Response	
	1	O sistema central pretende configurar um AP	
	2		O AP recebe do sistema central os comandos relativos à configuração das funcionalidades desse AP
	3		Efetua a configuração de cada uma das funcionalidades definidas pelos comandos recebidos do sistema central
	4		Envia ao sistema central uma resposta indicando sucesso na execução da configuração do AP
Cenário alternativo 1a) : O sistema central pretende programar uma etiqueta RFID através do AP e por RF.	Actor Input	System Response	
	1		O AP recebe do sistema central os dados para programar a Etiqueta RFID
	2		O AP envia os dados de programação para a etiqueta RFID
	3		Envia ao sistema central uma resposta indicando sucesso de programação da etiqueta RFID
Alternativa (2b) ao cenário alternativo 1a) : A TAG que se pretende programar não está acessível ou não suporta configuração via RF	Actor Input	System Response	
	1		Envia ao sistema central uma resposta indicando que não é possível configurar a TAG especificada
	2		Termina o caso de uso
Alternativa (3c) ao Cenário alternativo 1a) : Ocorreu um erro durante a programação da etiqueta RFID	Actor Input	System Response	
	1		Envia ao sistema central uma resposta indicando que ocorreu um erro durante a programação da etiqueta RFID

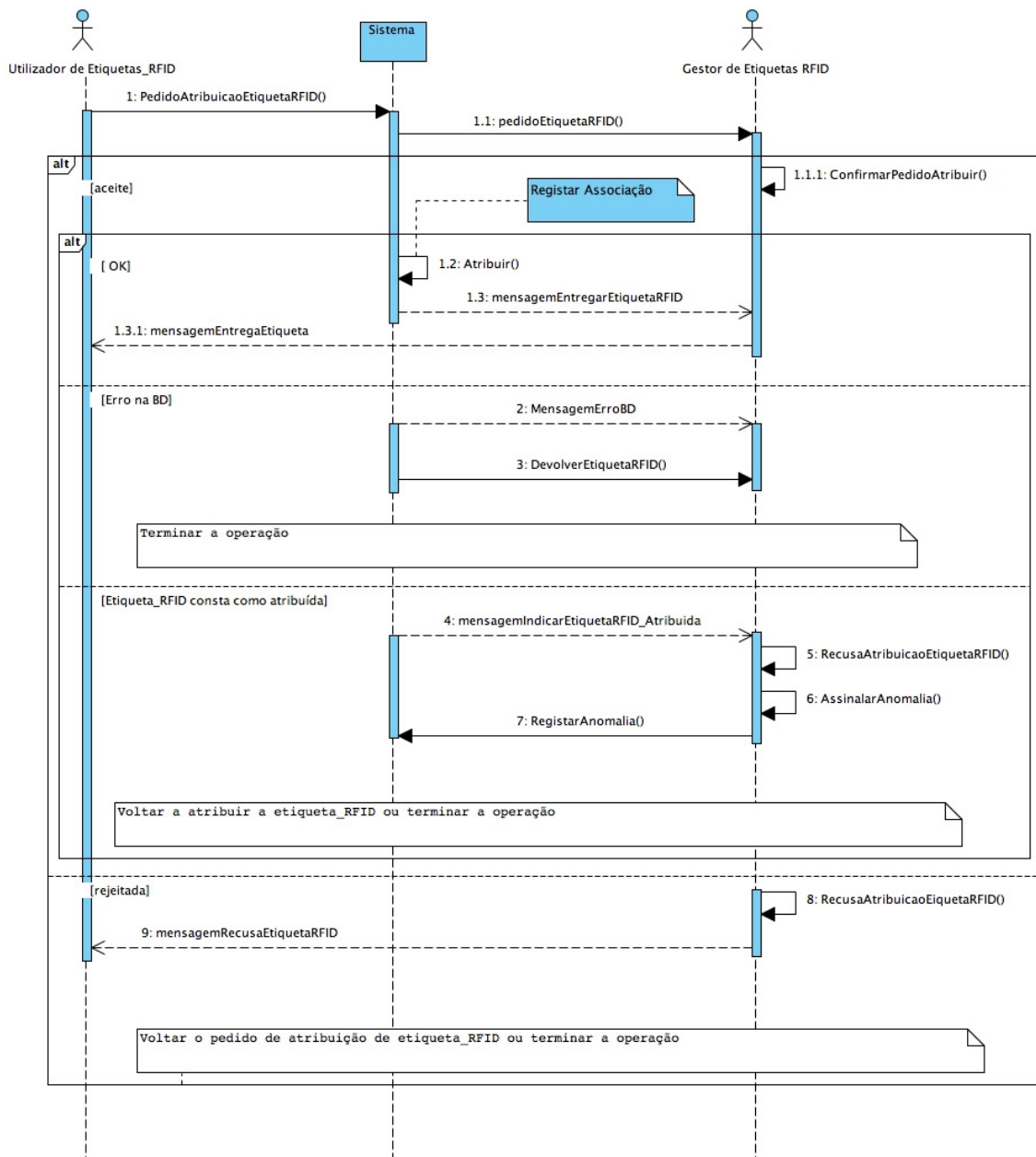
	2		Termina o caso de uso
Cenário alternativo 4d): Ocorreu um erro na execução da configuração		Actor Input	System Response
	1		Envia ao sistema central uma resposta indicando que ocorreu um erro durante a configuração do AP
	2		Termina o caso de uso

Anexo VII Diagramas de Sequência ao Nível do Sistema

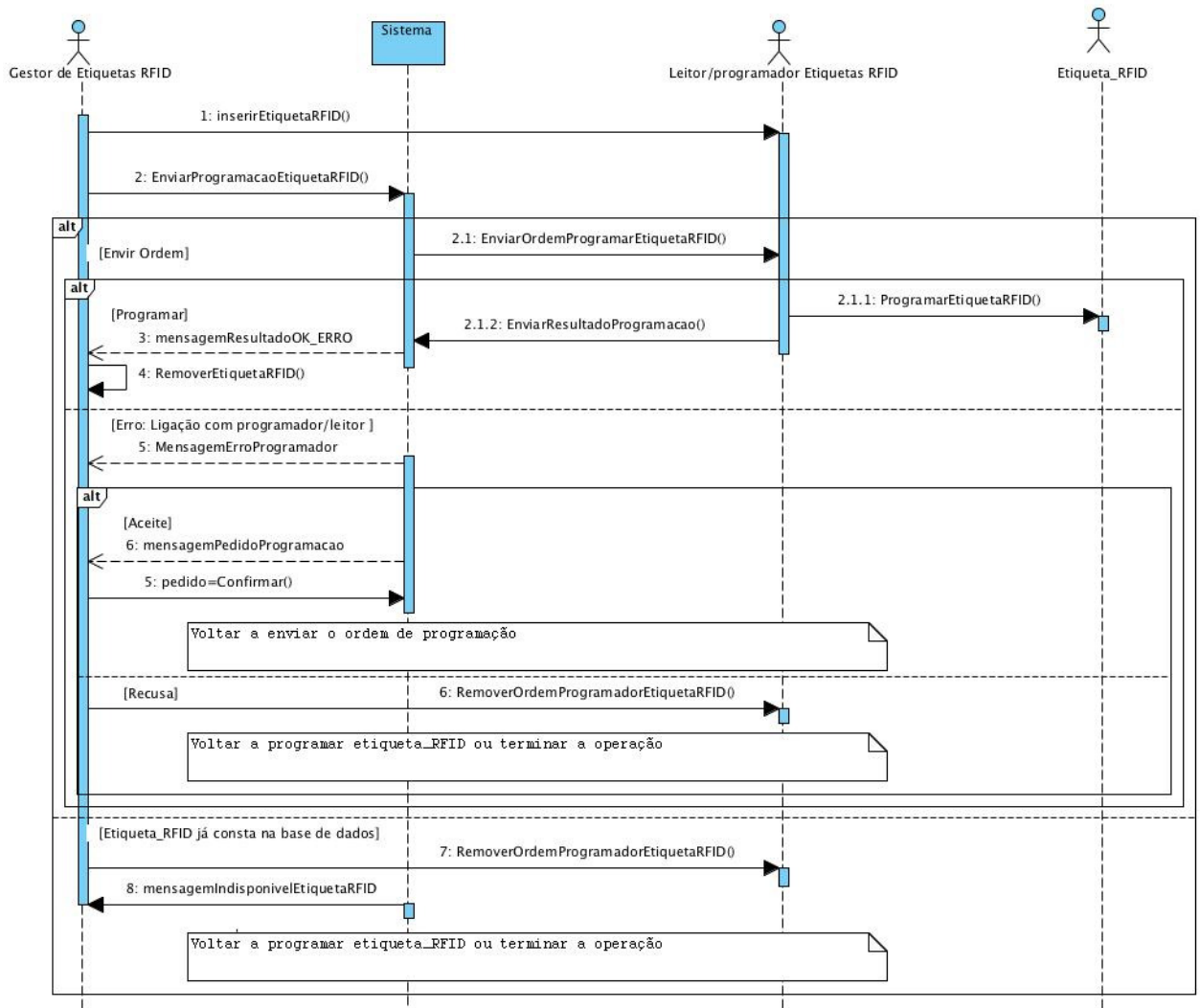
1. Diagrama de Sequência “Imprimir Etiqueta de Papel para Etiqueta_RFID”



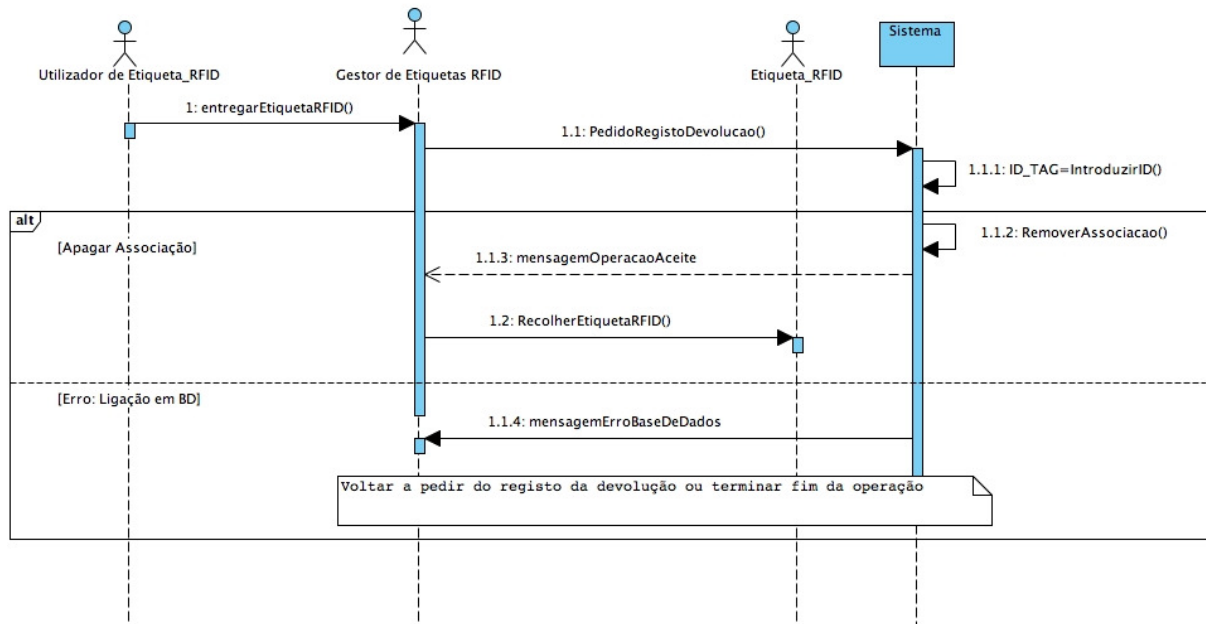
2. Diagrama de Sequência “Atribuir etiqueta_RFID”



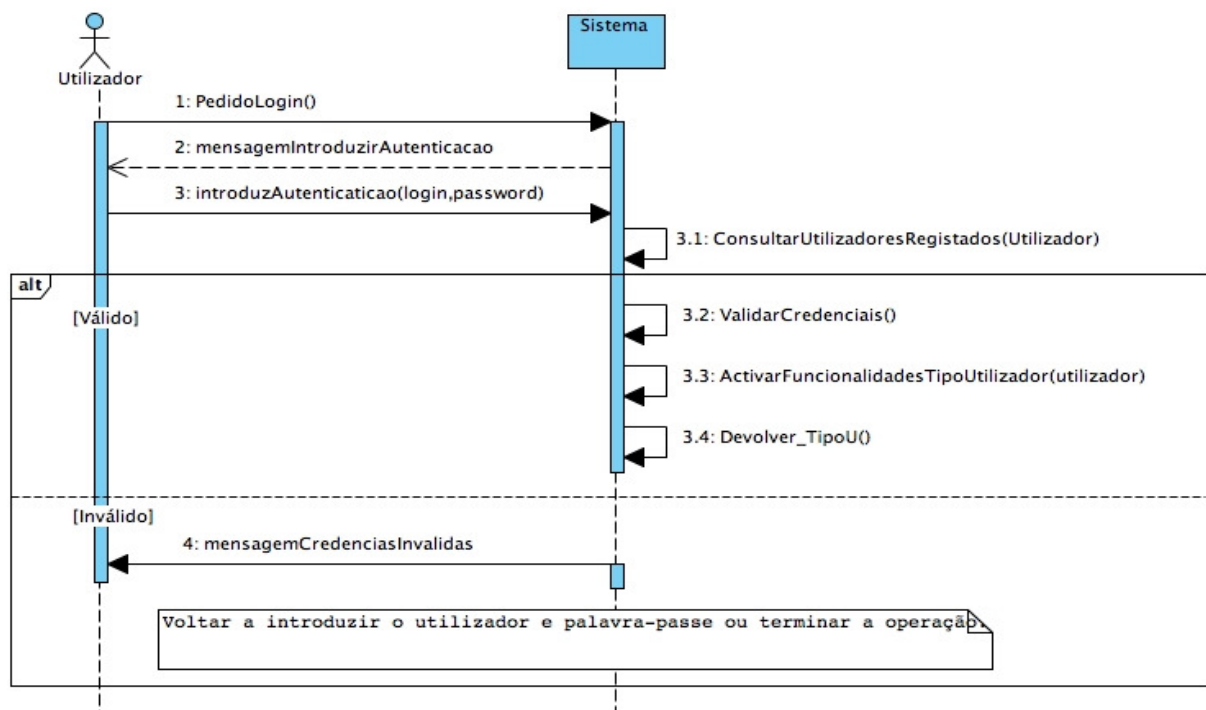
3. Diagrama de Sequência “Programar etiqueta_RFID”



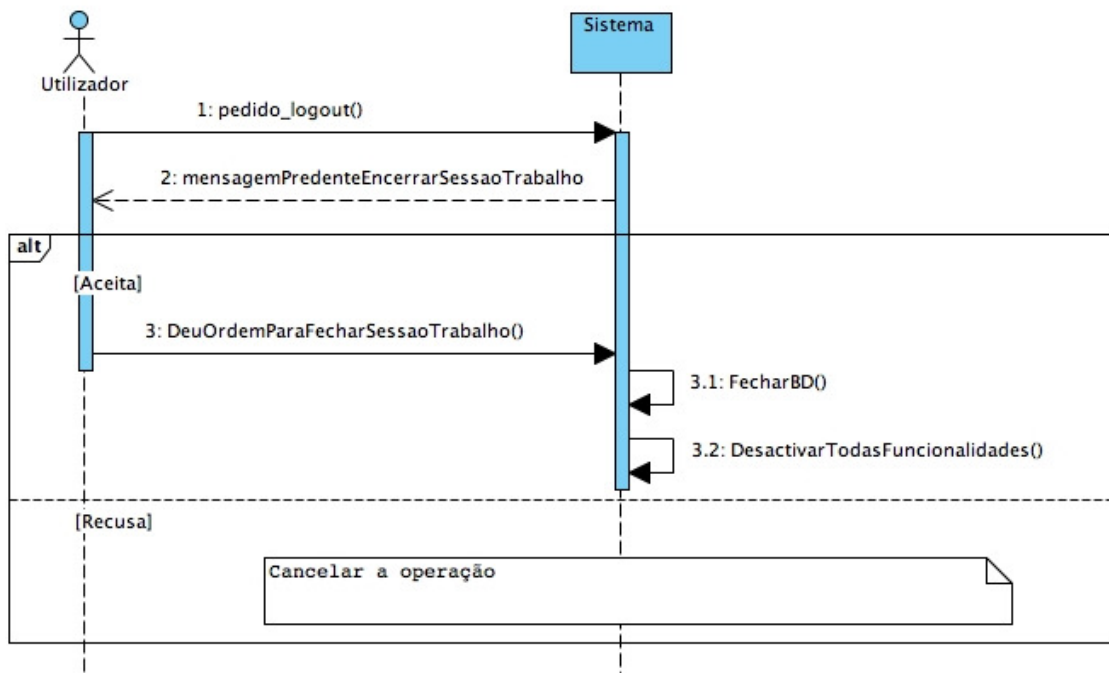
4. Diagrama de Sequência “Recolher etiqueta_RFID”



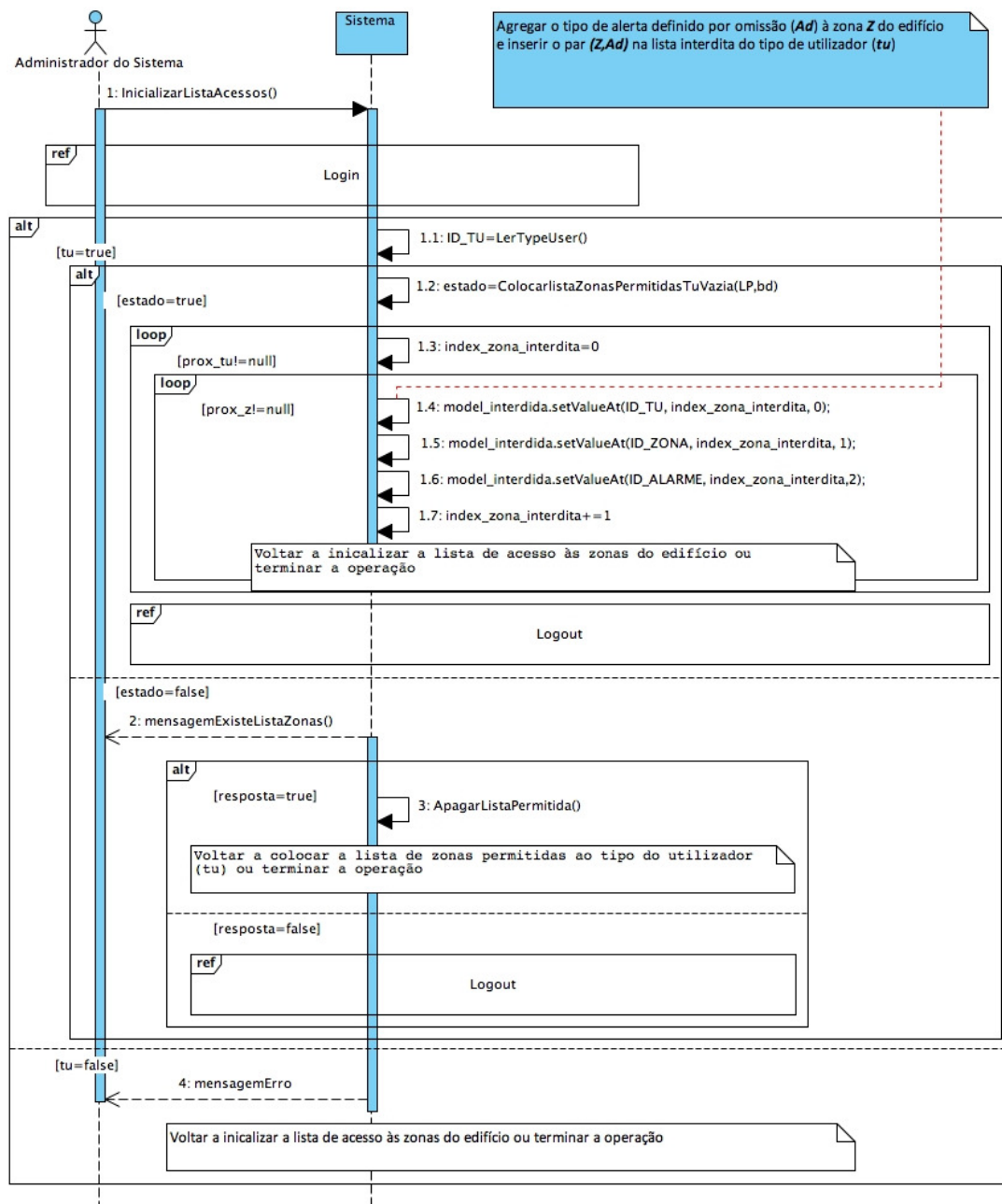
5. Diagrama de Sequência “Login”



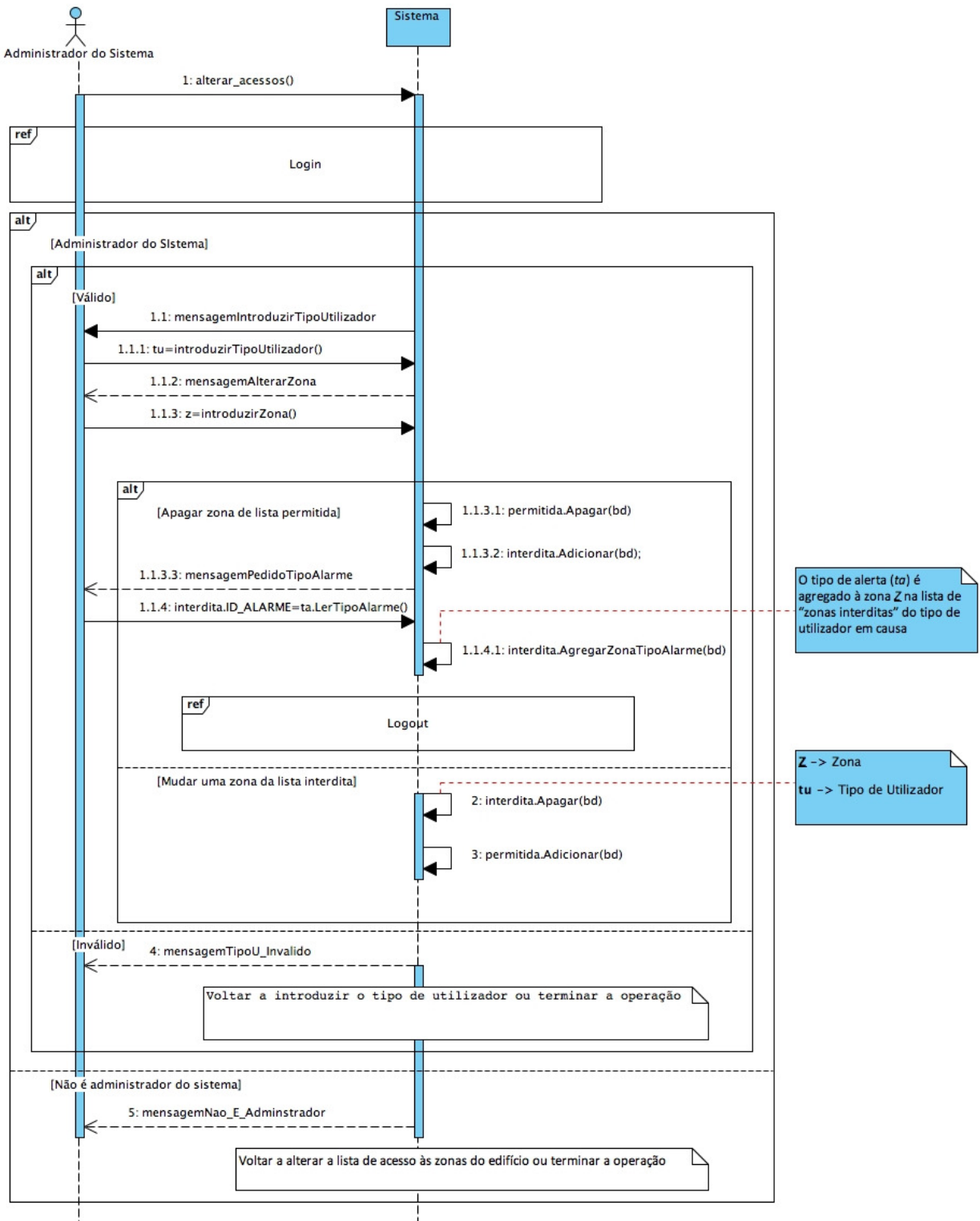
6. Diagrama de Sequência “Logout”



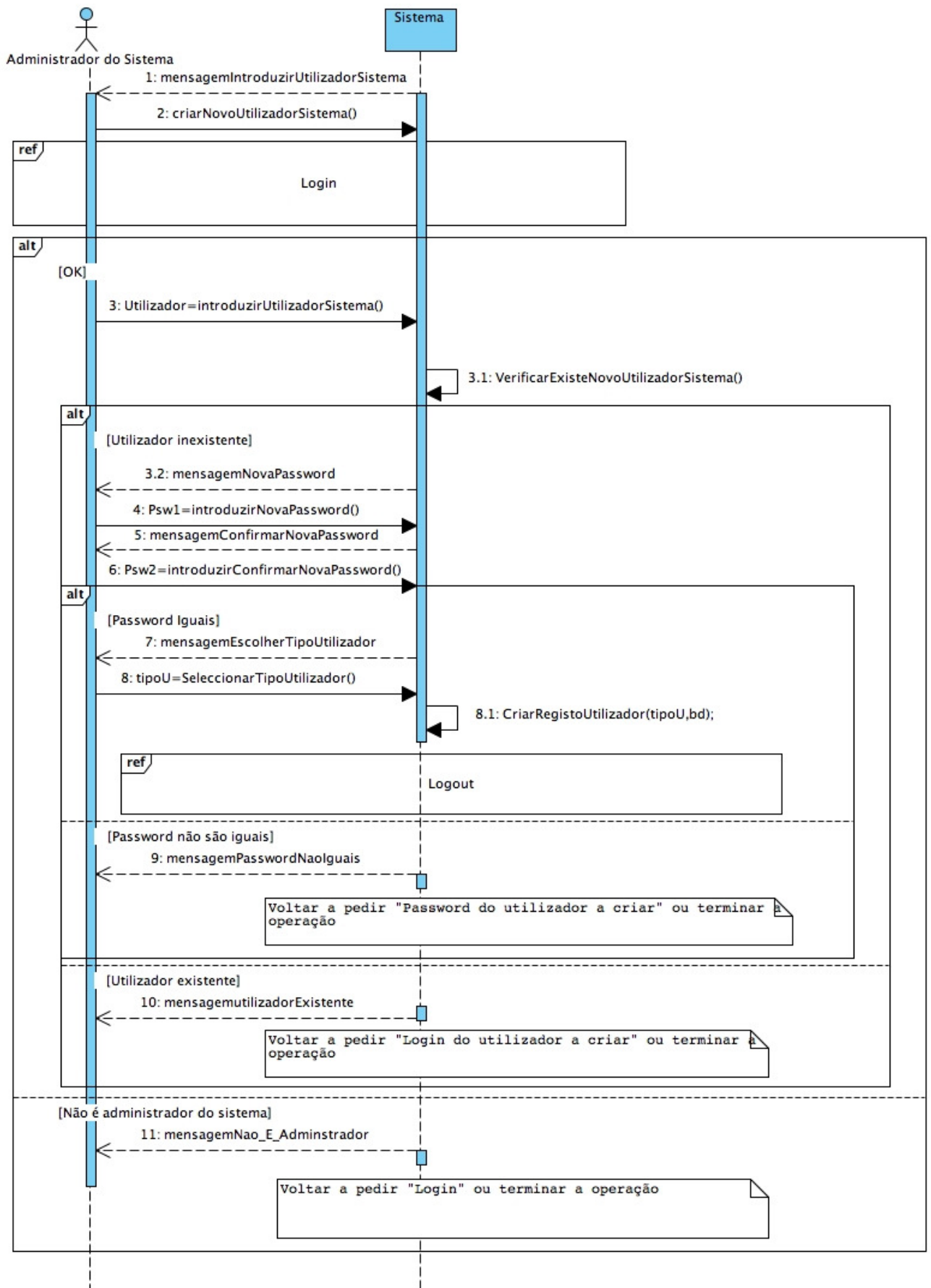
7. Diagrama de Sequência "Inicializar a lista de acessos às zonas do edifício"



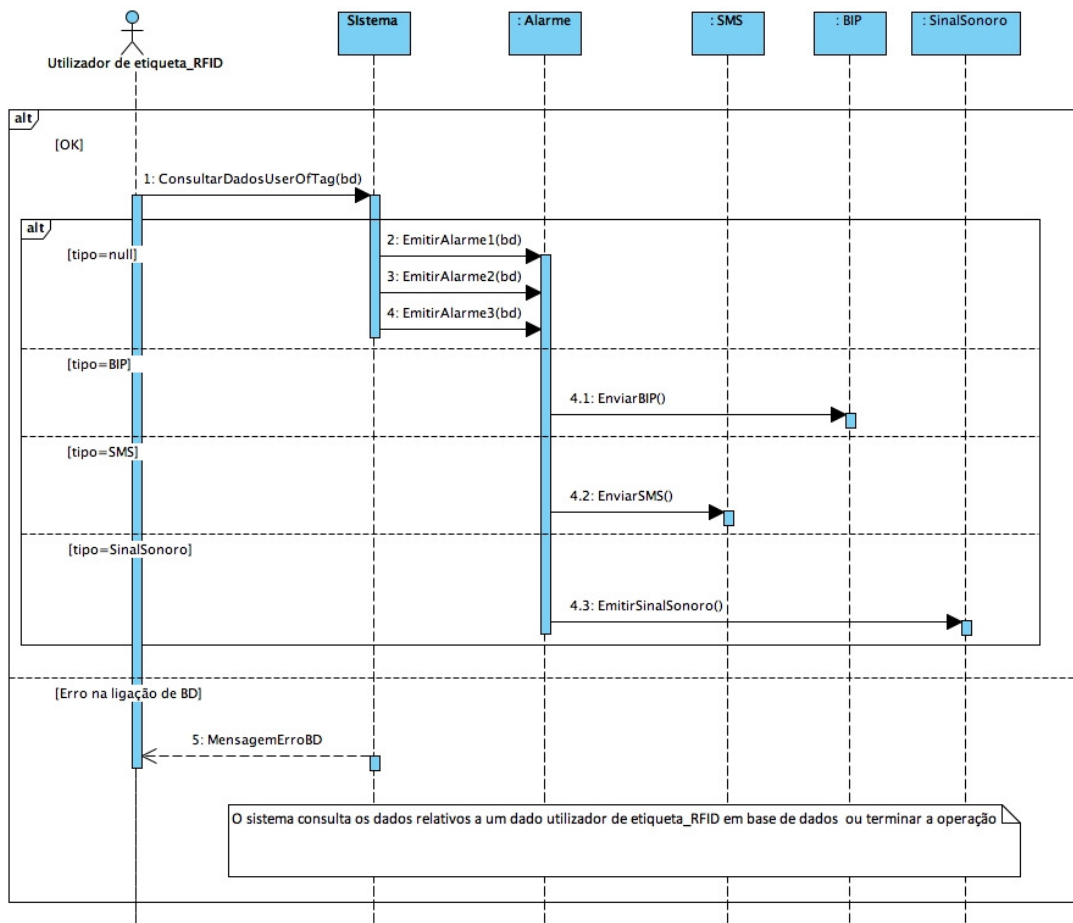
8. Diagrama de Sequência "Alterar a lista de acessos às zonas do edifício"



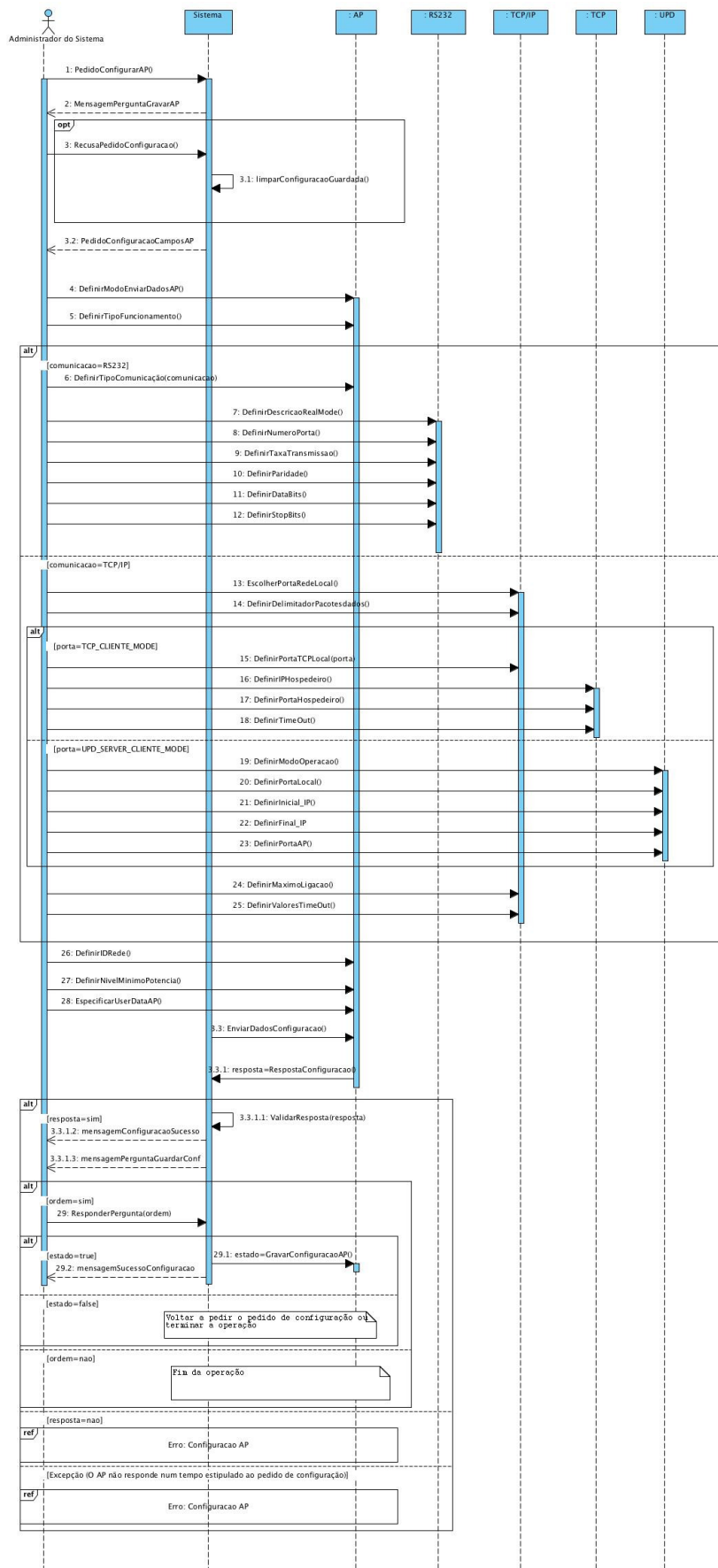
9. Diagrama de Sequência "Registrar utilizador do Sistema / Criar perfil de administrador do sistema"



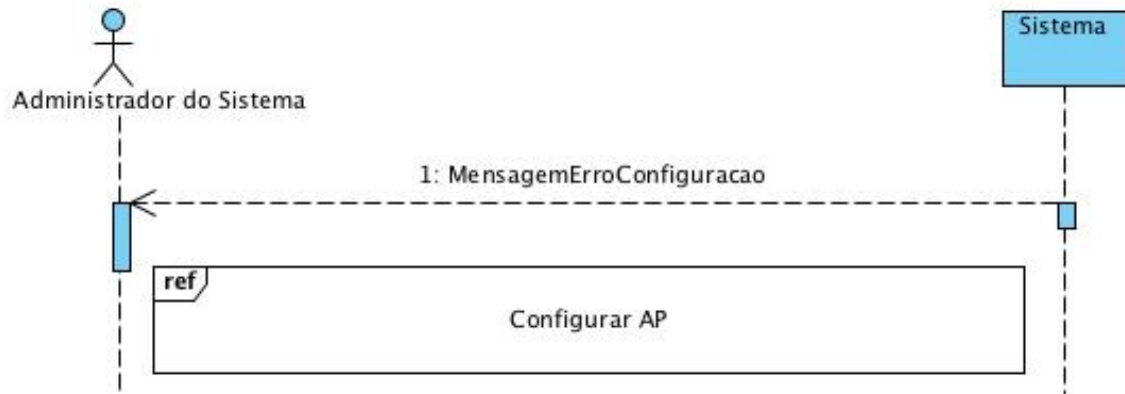
10. Diagrama de Sequência "Emitir sinal de alerta"



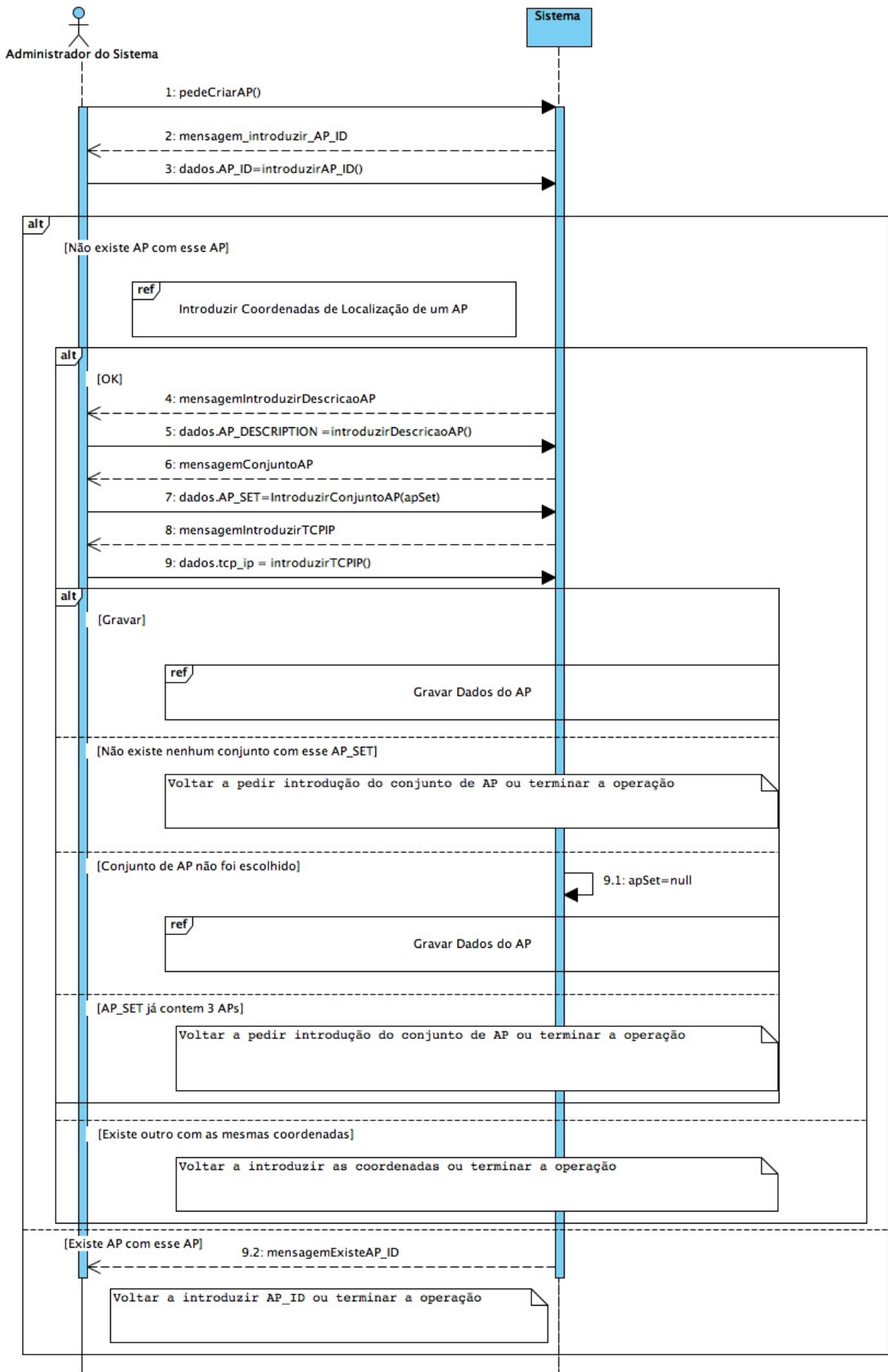
11. Diagrama de Sequência "Configurar AP"



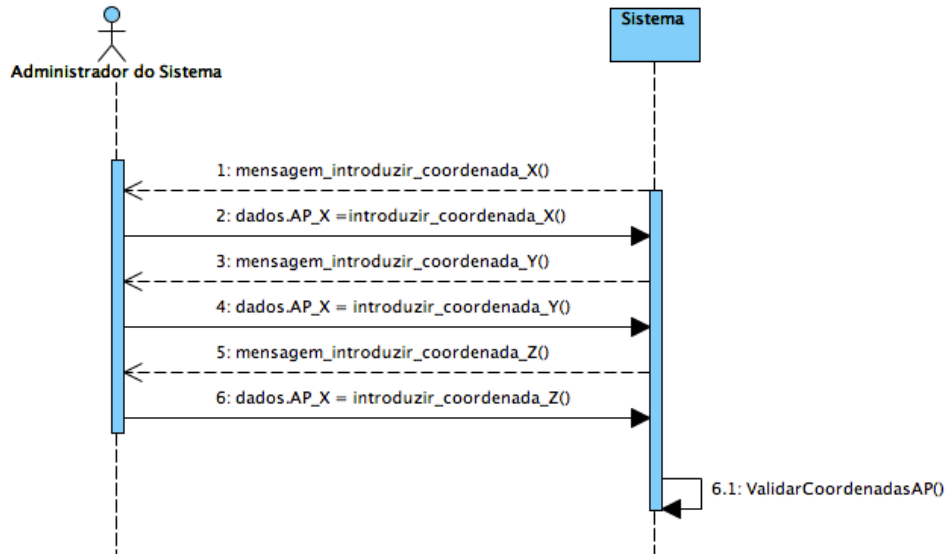
12. Diagrama de Sequência "Erro: Configurar AP"



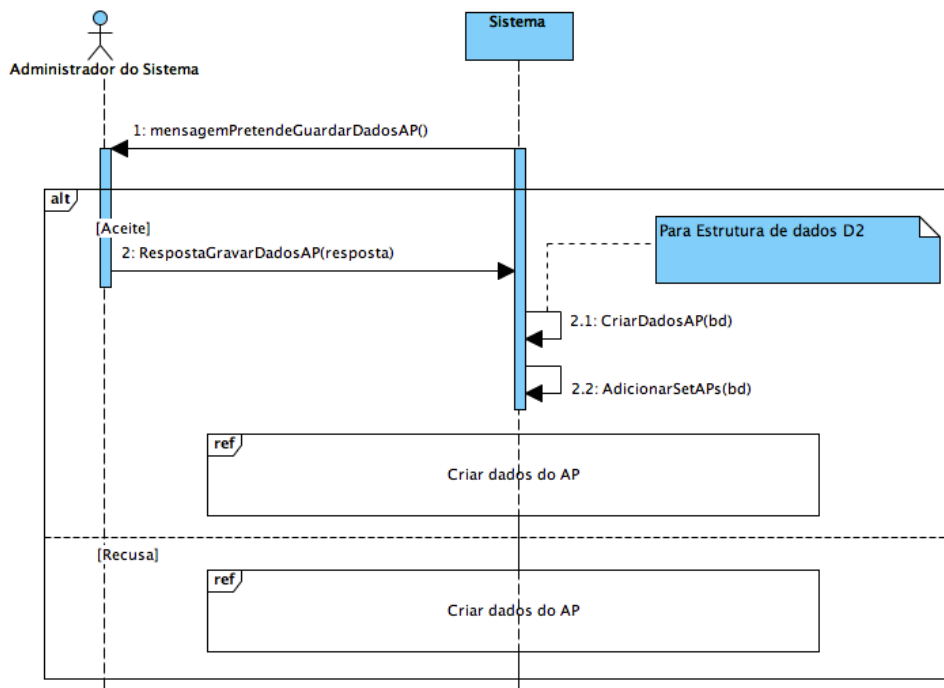
13. Diagrama de Sequência "Criar Dados de AP"



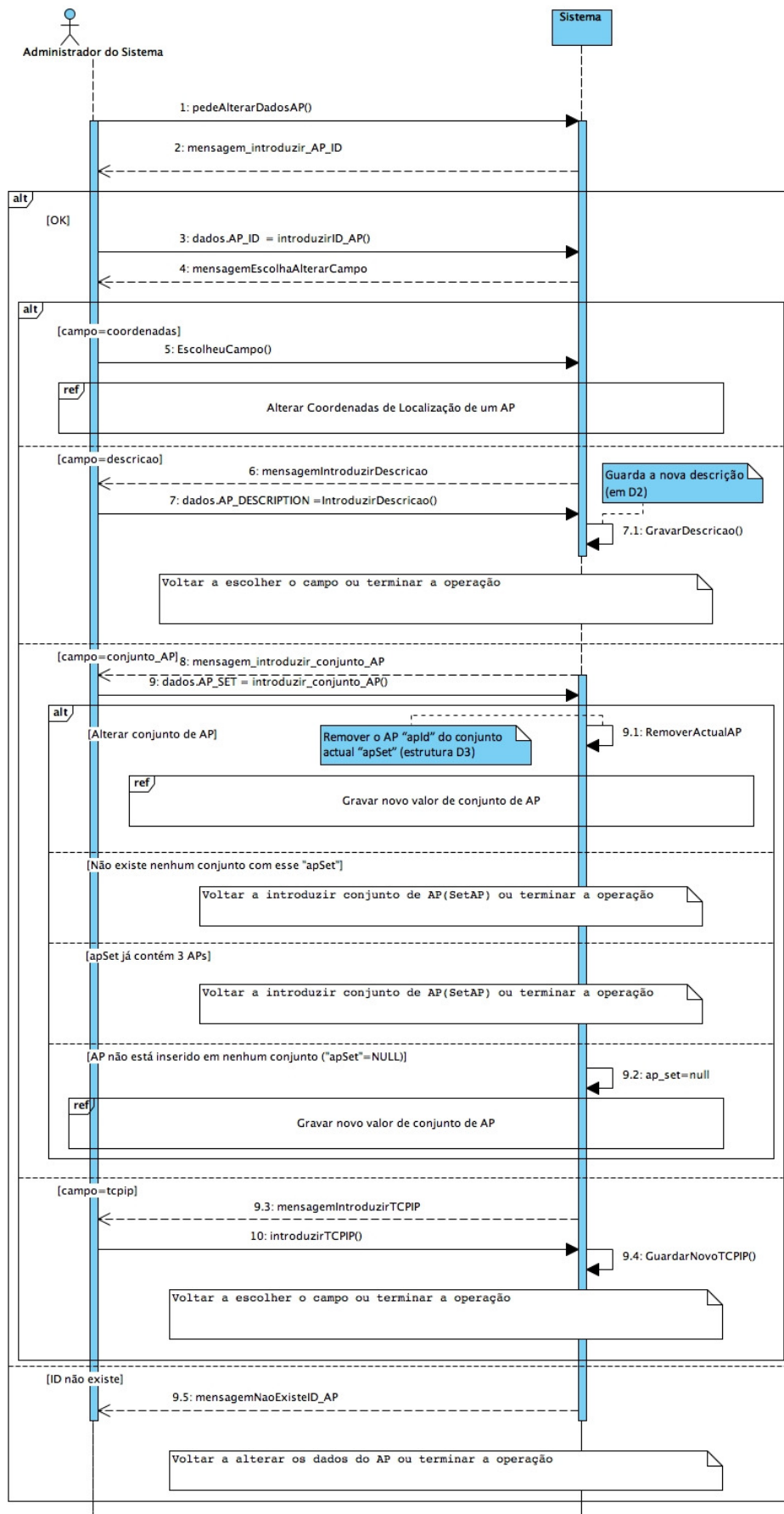
14. Diagrama de Sequência "Introduzir Coordenadas de Localização de um AP"



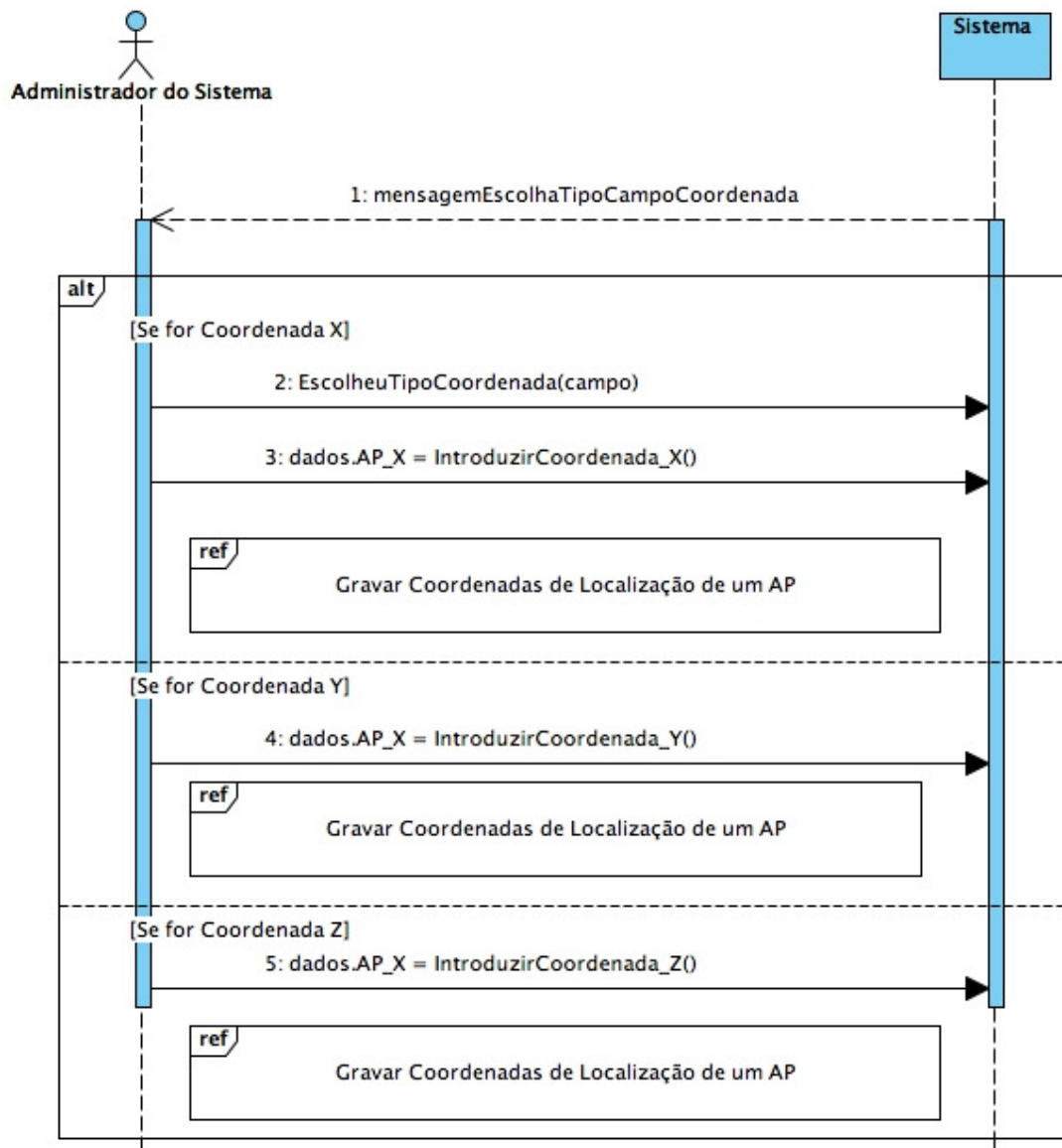
15. Diagrama de Sequência "Gravar Dados de AP"



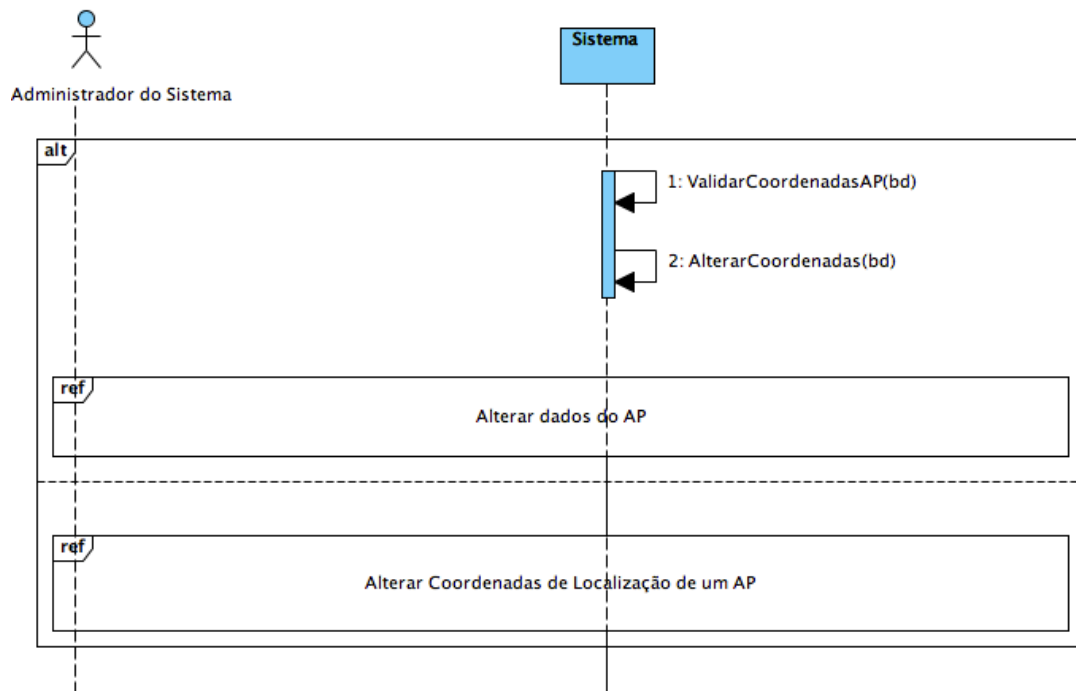
16. Diagrama de Sequência "Alterar Dados de AP"



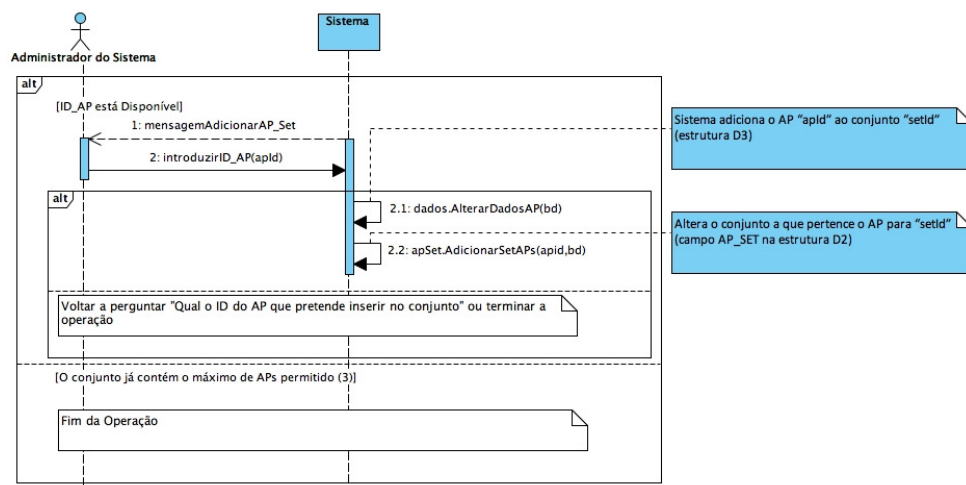
17. Diagrama de Sequência "Alterar Coordenadas de Localização de um AP"



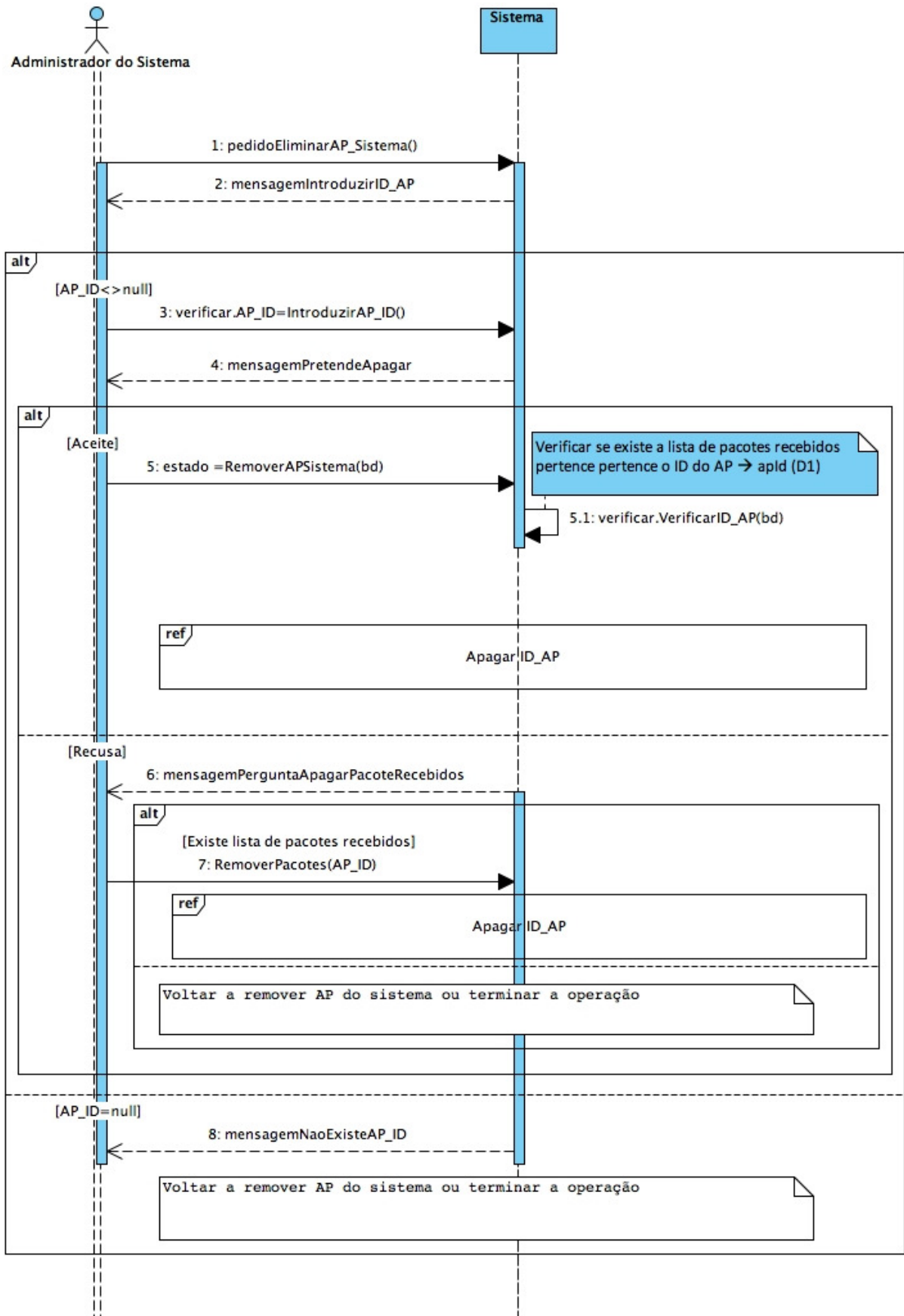
18. Diagrama de Sequência "Gravar Coordenadas de Localização de um AP"



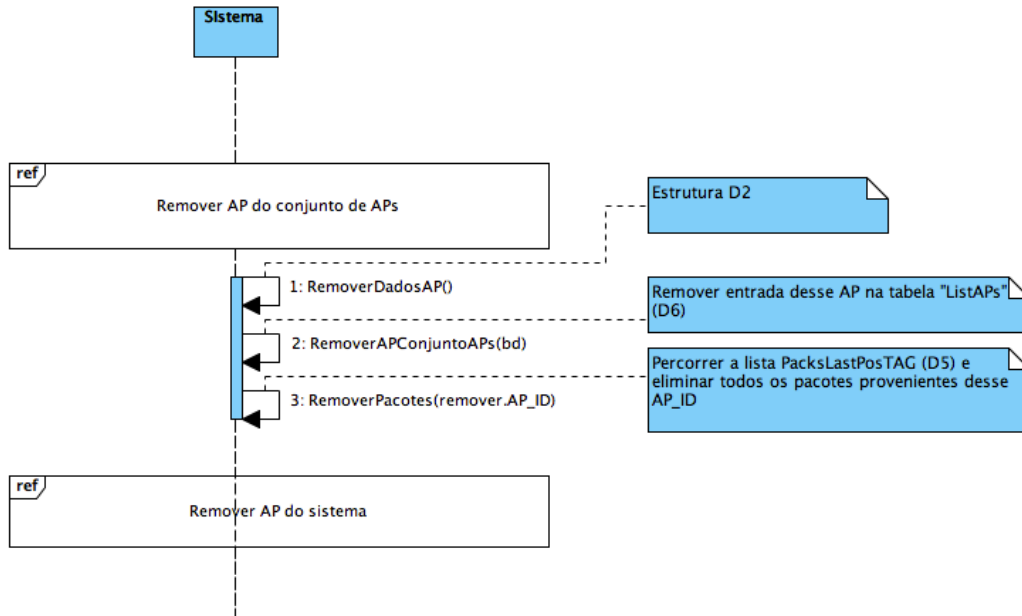
19. Diagrama de Sequência "Guardar novo valor de conjunto do AP"



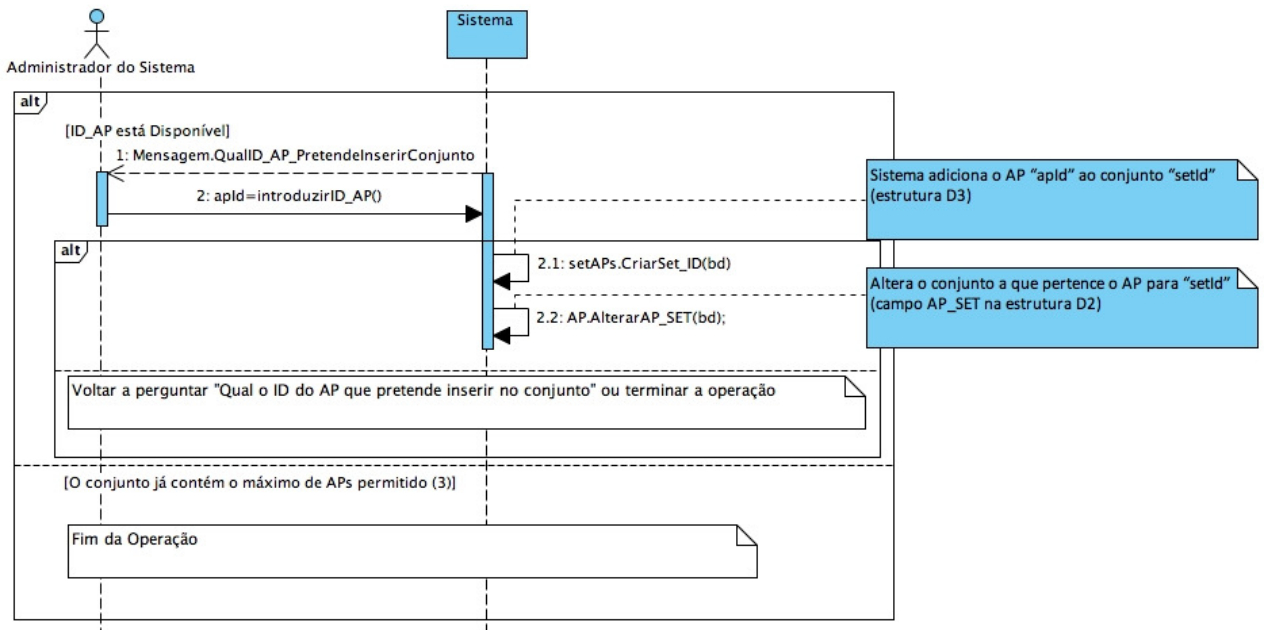
20. Diagrama de Sequência "Remover AP do sistema"



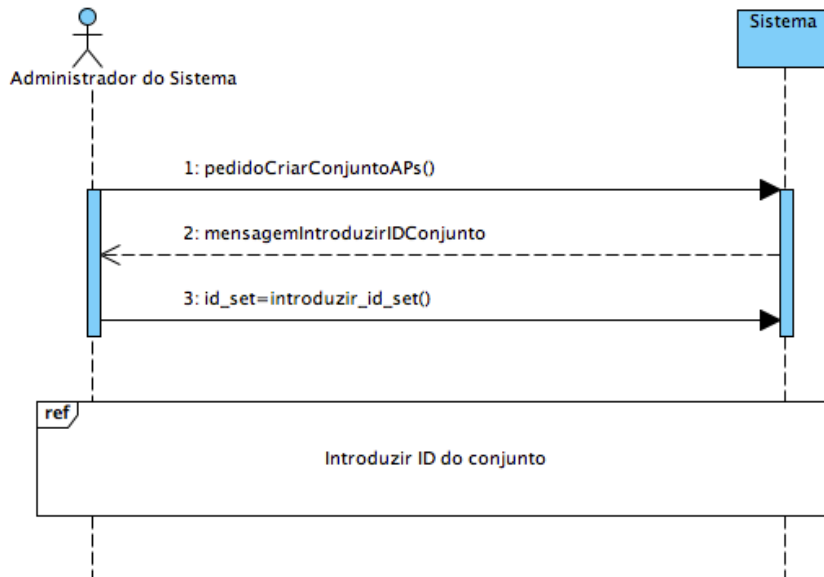
21. Diagrama de Sequência "Apagar ID_AP"



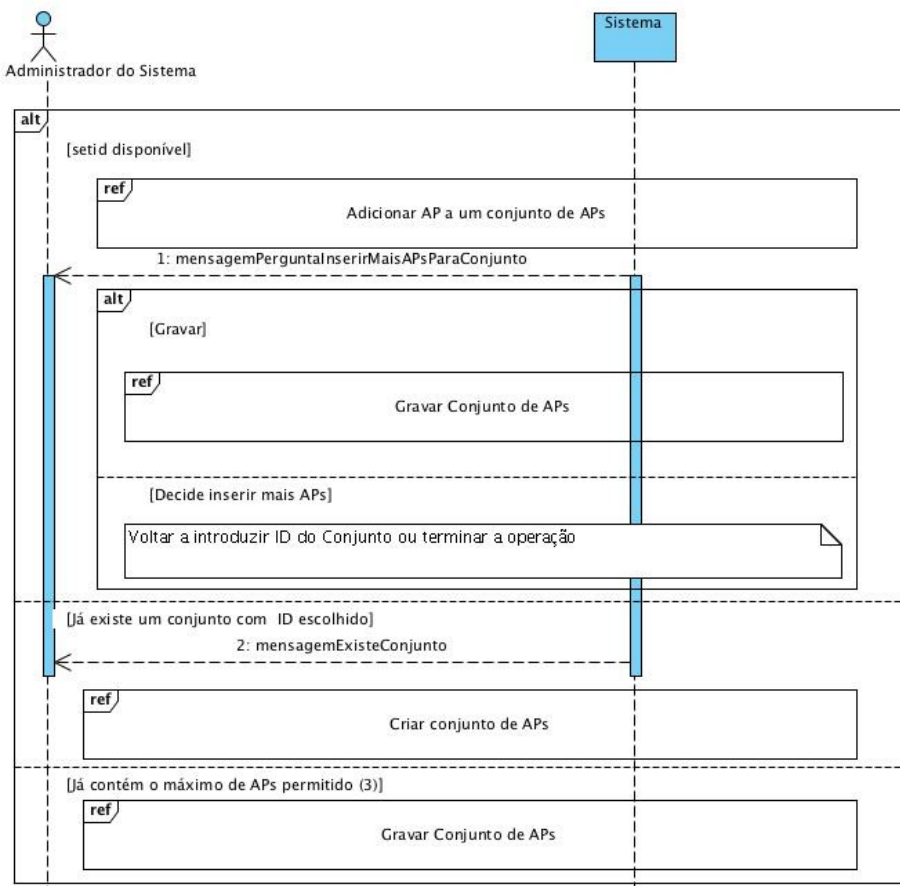
22. Diagrama de Sequência "Adicionar AP a um conjunto de APs"



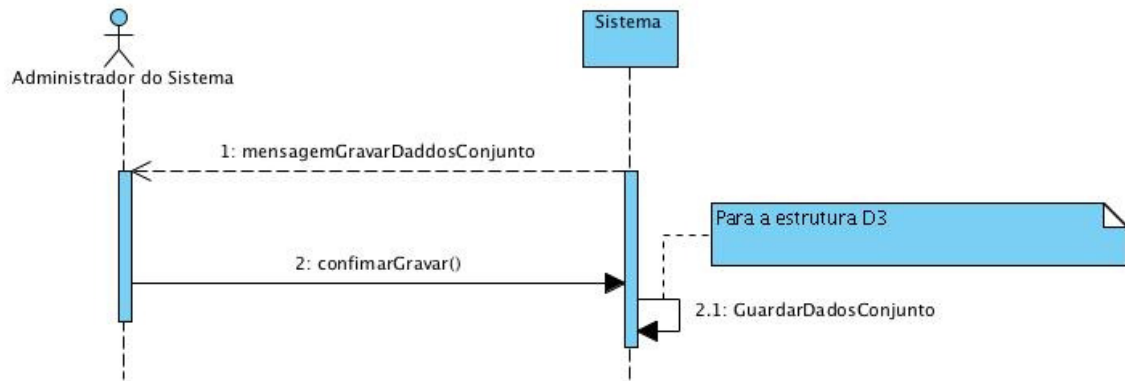
23. Diagrama de Sequência "Criar Conjunto de APs"



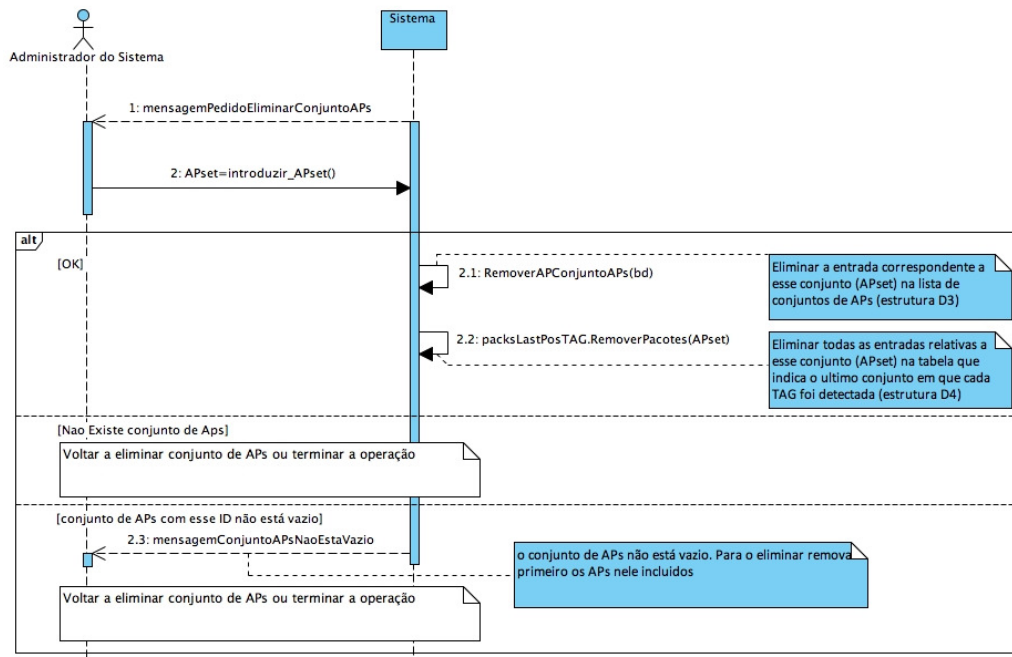
24. Diagrama de Sequência "Introduzir ID do conjunto"



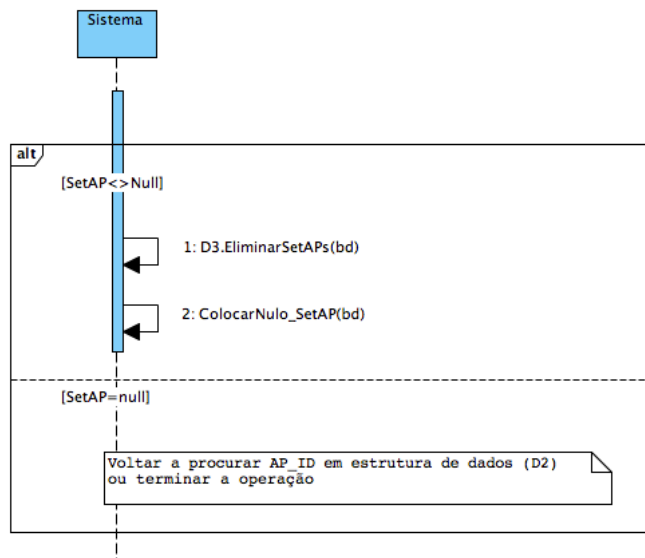
25. Diagrama de Sequência "Gravar Conjunto de APs"



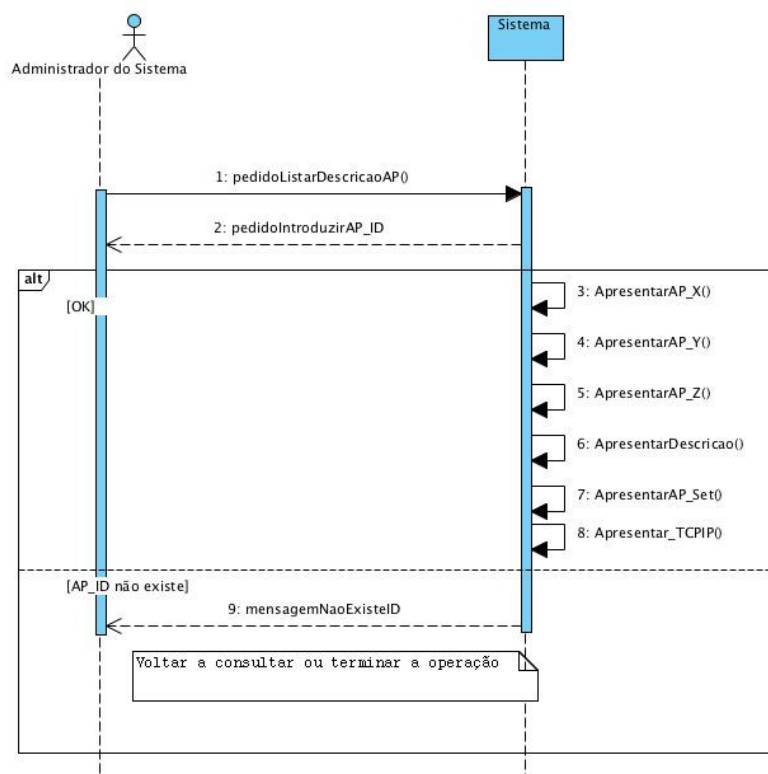
26. Diagrama de Sequência "Eliminar conjunto de APs"



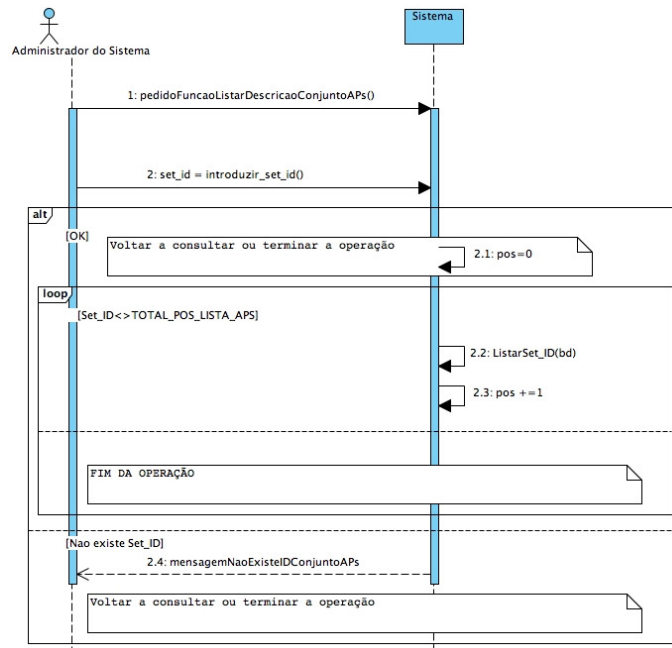
27. Diagrama de Sequência "Remove AP do conjunto de APs"



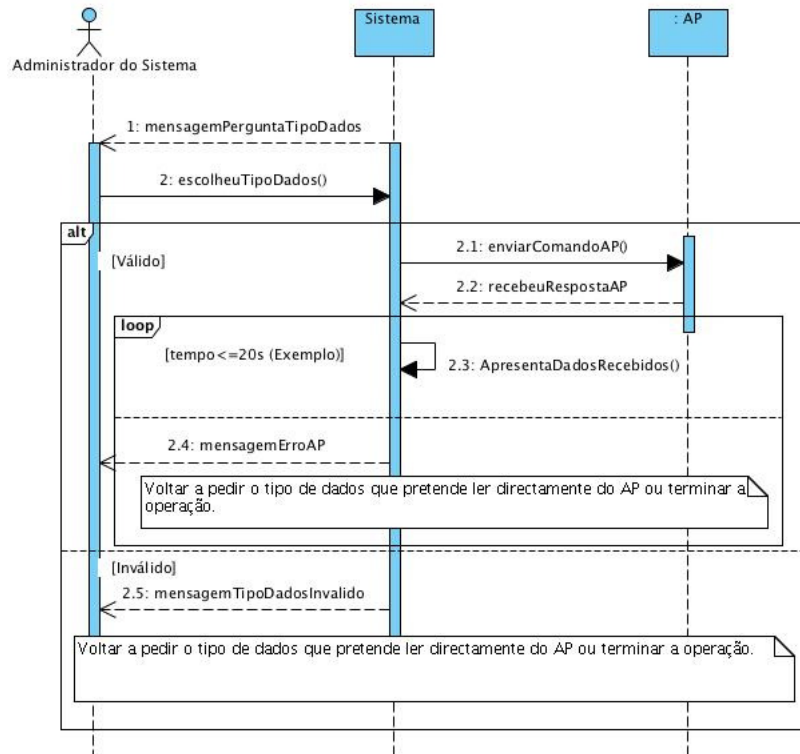
28. Diagrama de Sequência "Listar Descrição do AP"



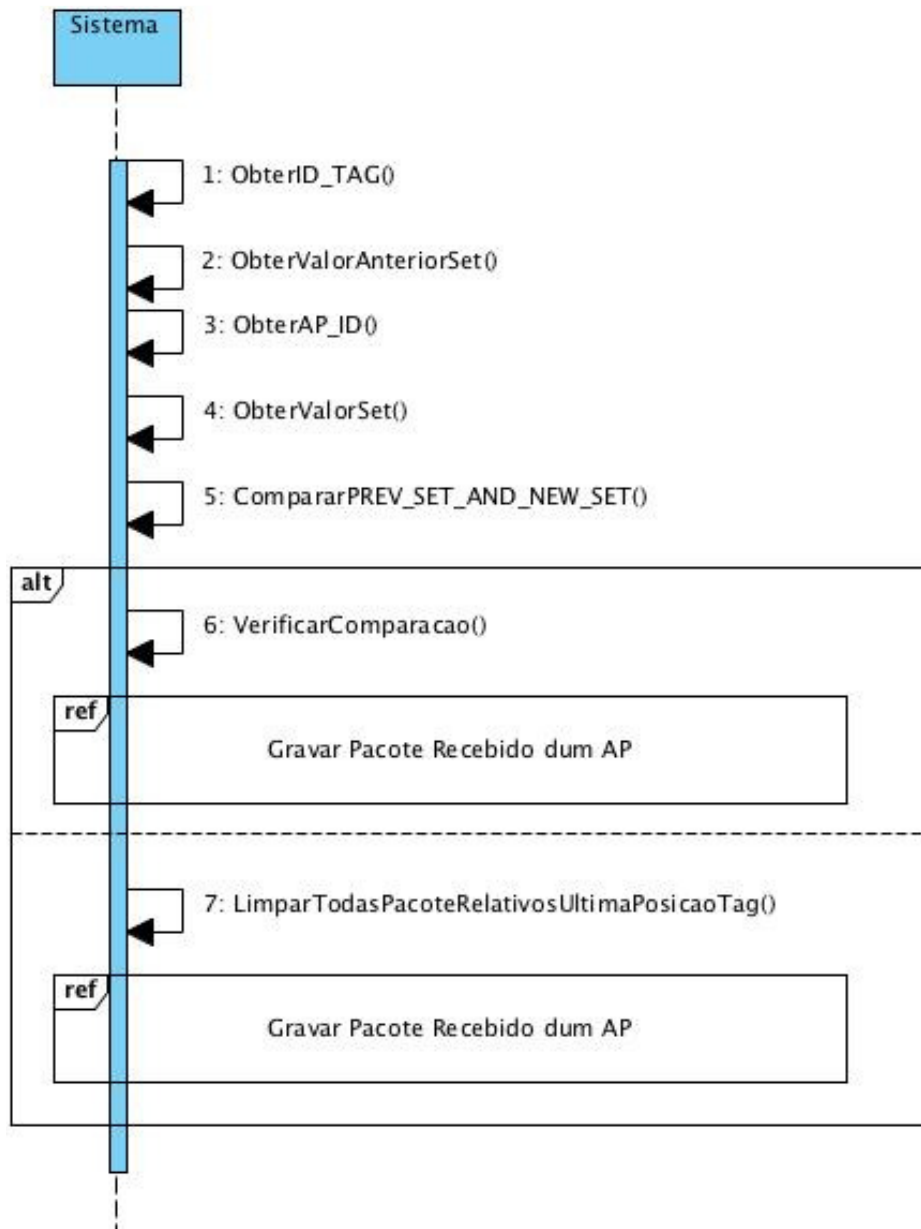
29. Diagrama de Sequência "Listar Descrição do Conjunto de APs"



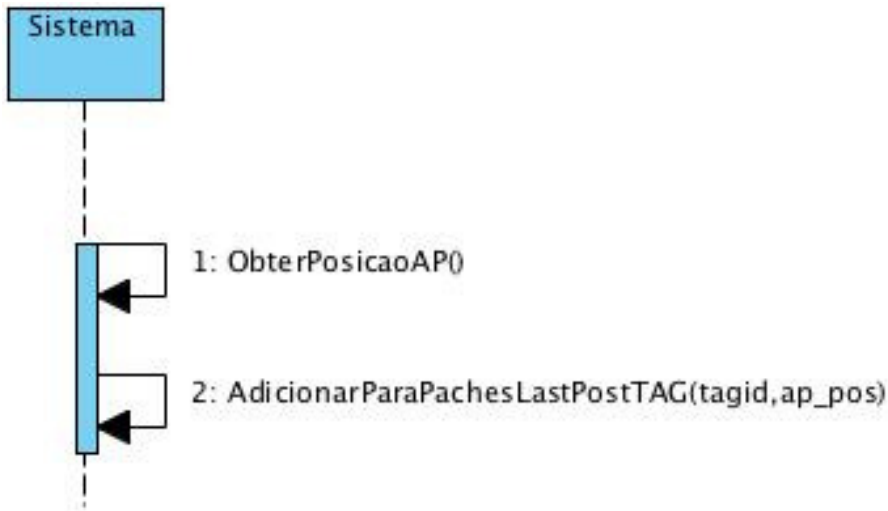
30. Diagrama de Sequência "Enviar Comando ao AP Ler a Configuração"



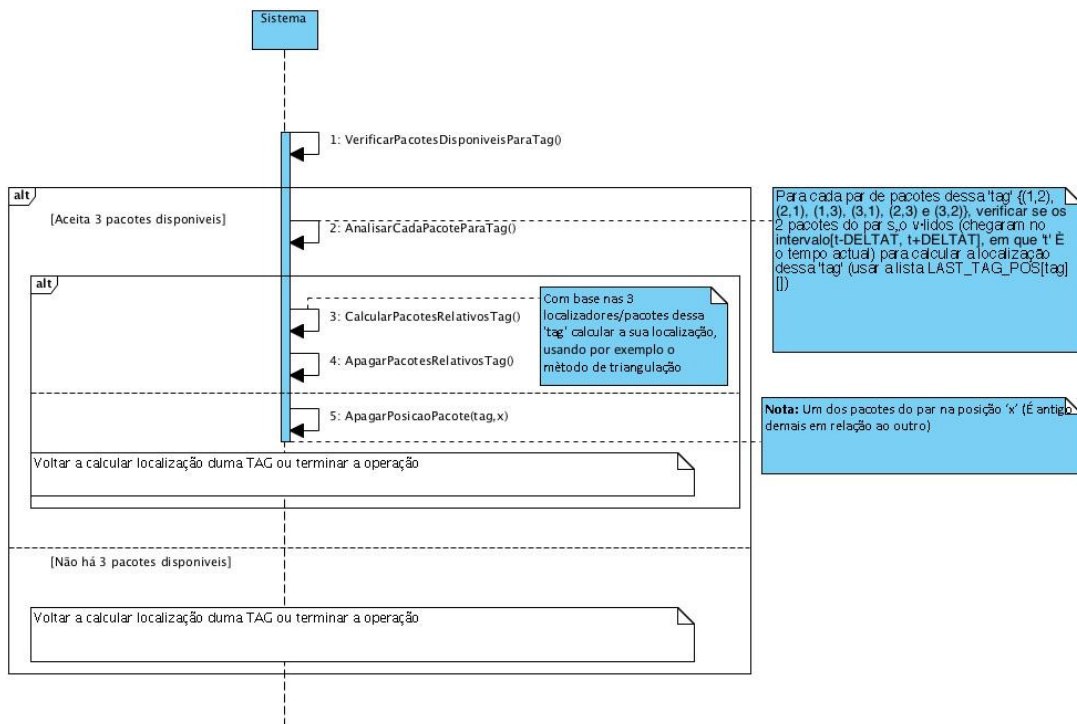
31. Diagrama de Sequência "Guardar pacote recebido dum AP"



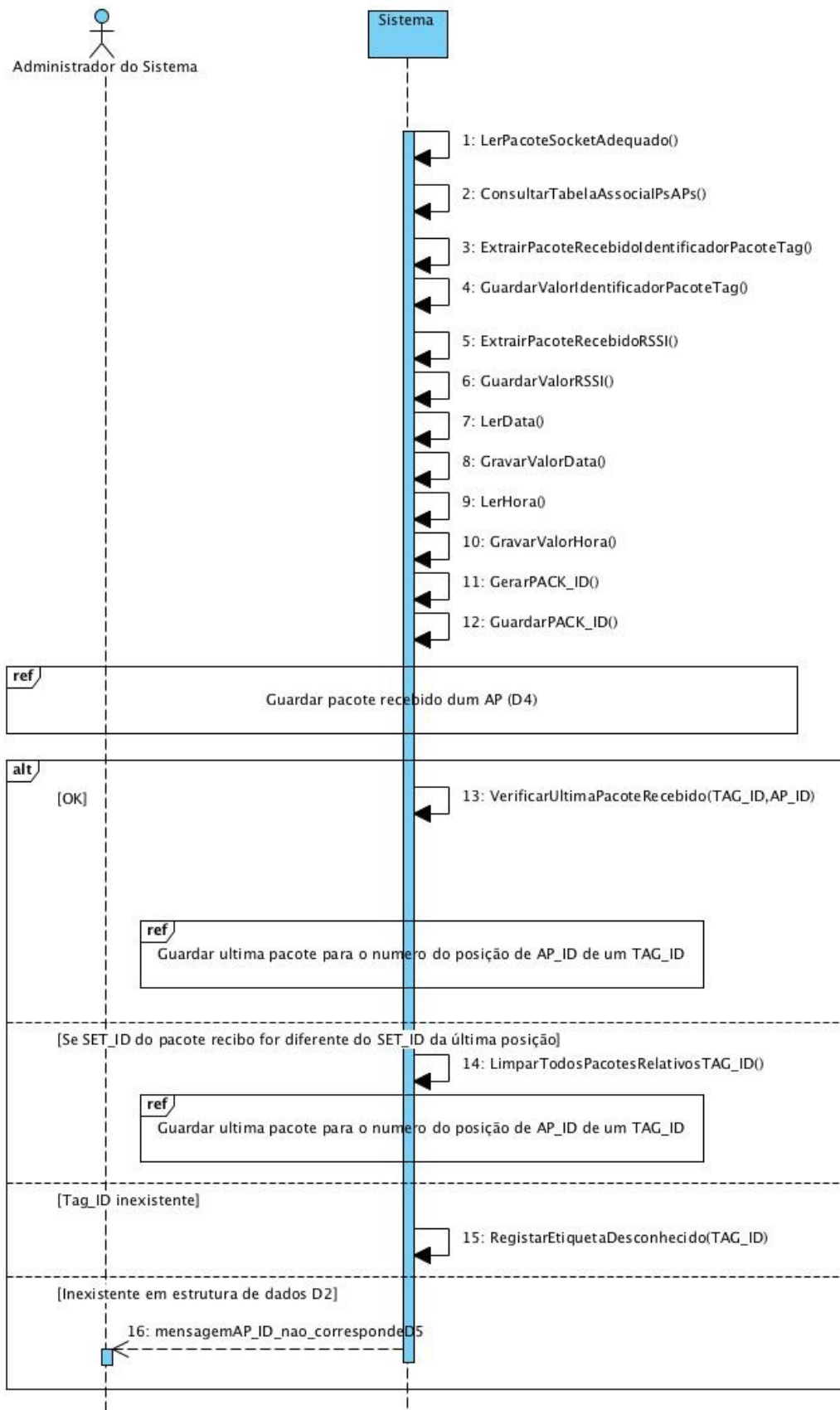
32. Diagrama de Sequência "Gravar pacote recebido dum AP"



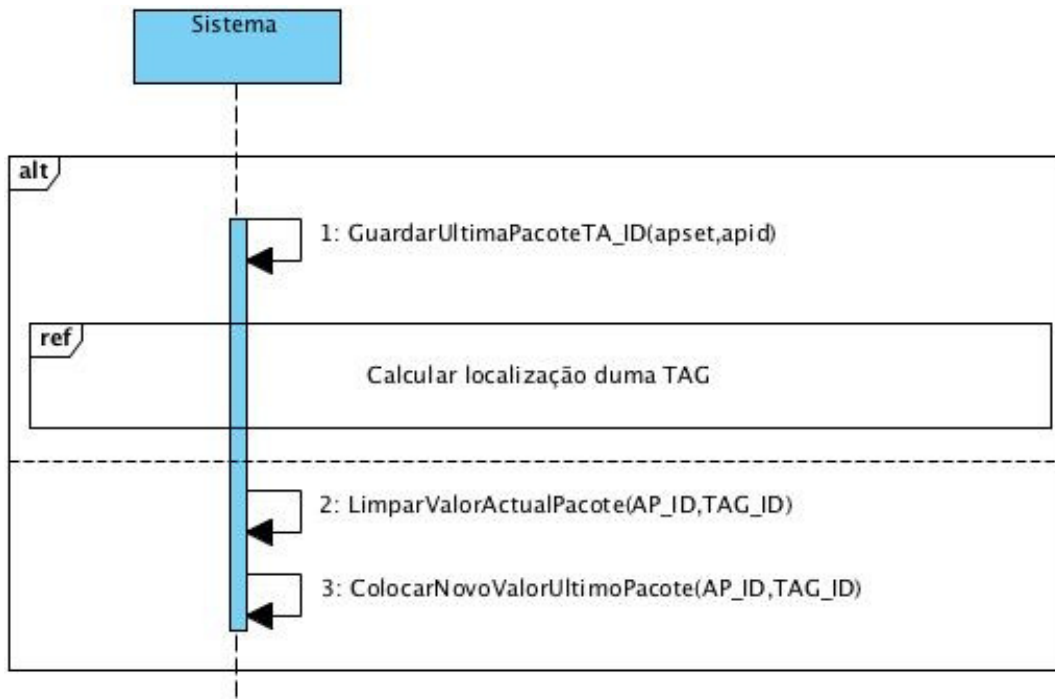
33. Diagrama de Sequência "Calcular localização duma TAG"



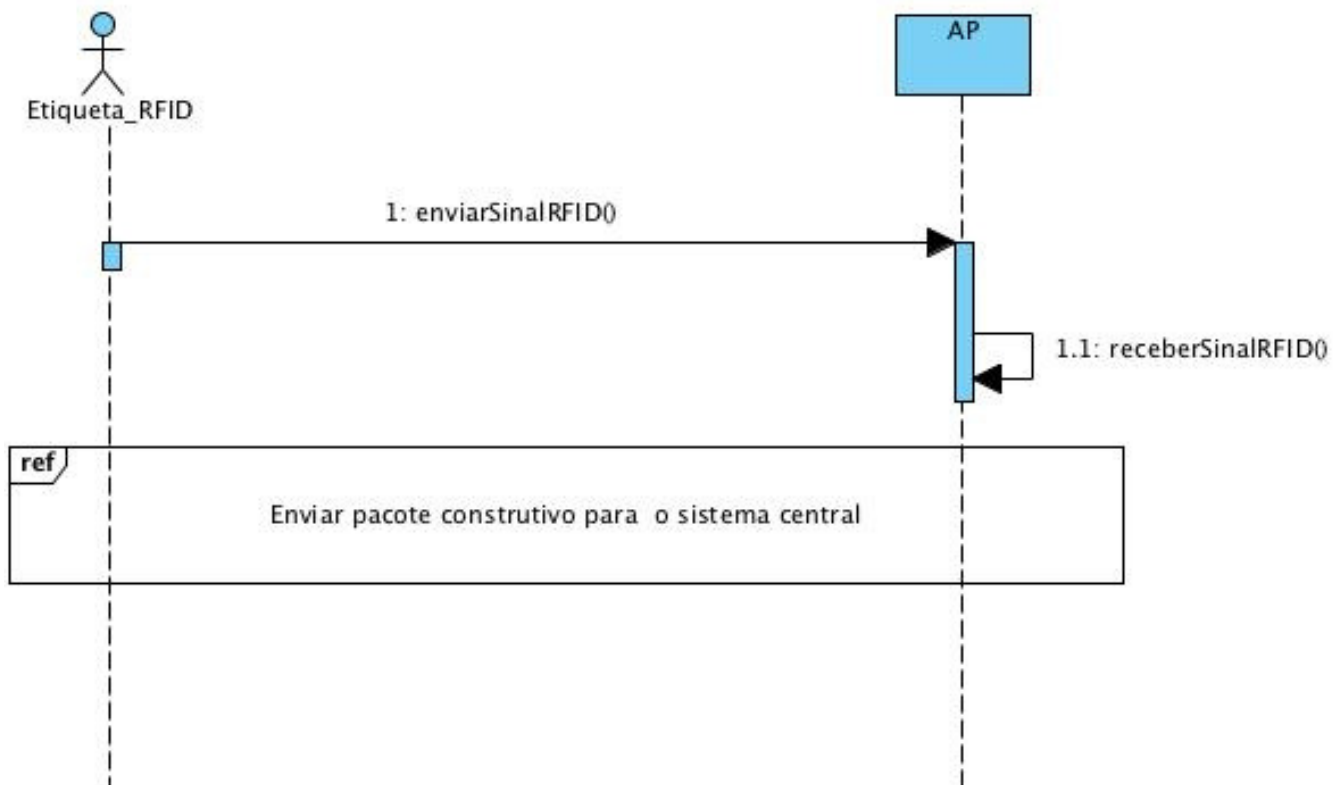
34. Diagrama de Sequência "Receber pacote de AP por TCP/IP"



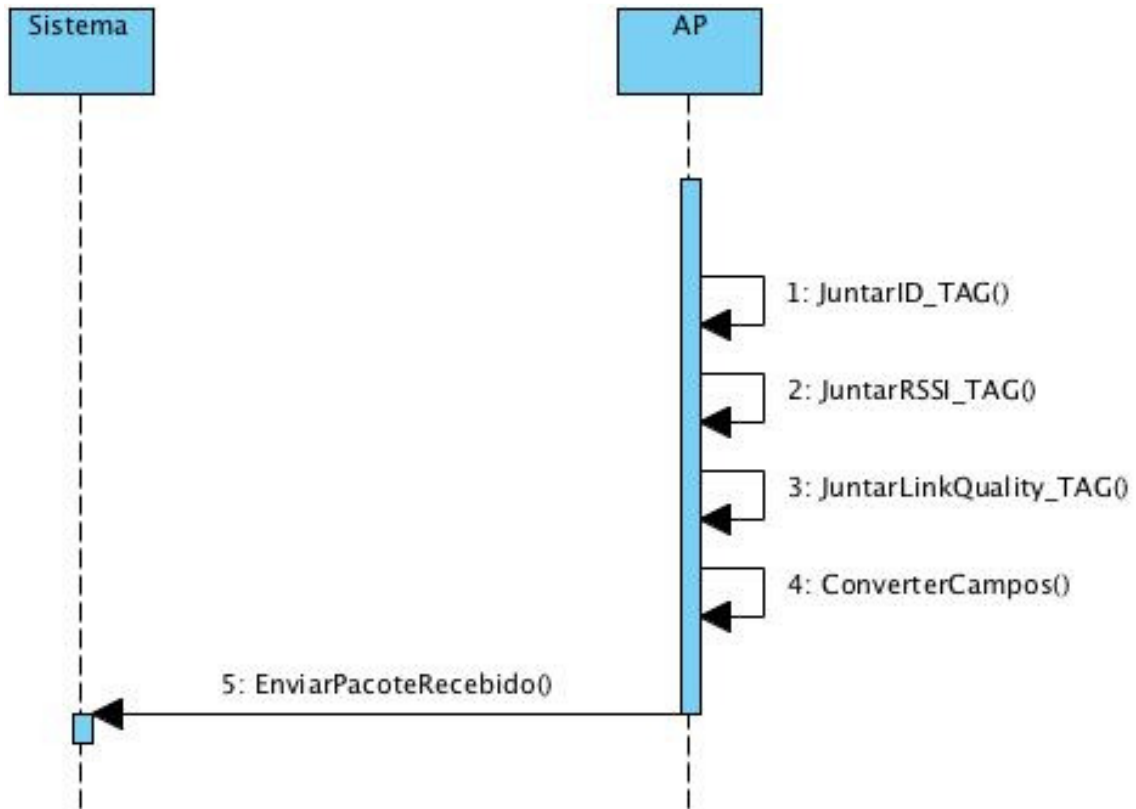
35. Diagrama de Sequência "Guardar ultima pacote para o numero do posição de AP_ID de um TAG_ID"



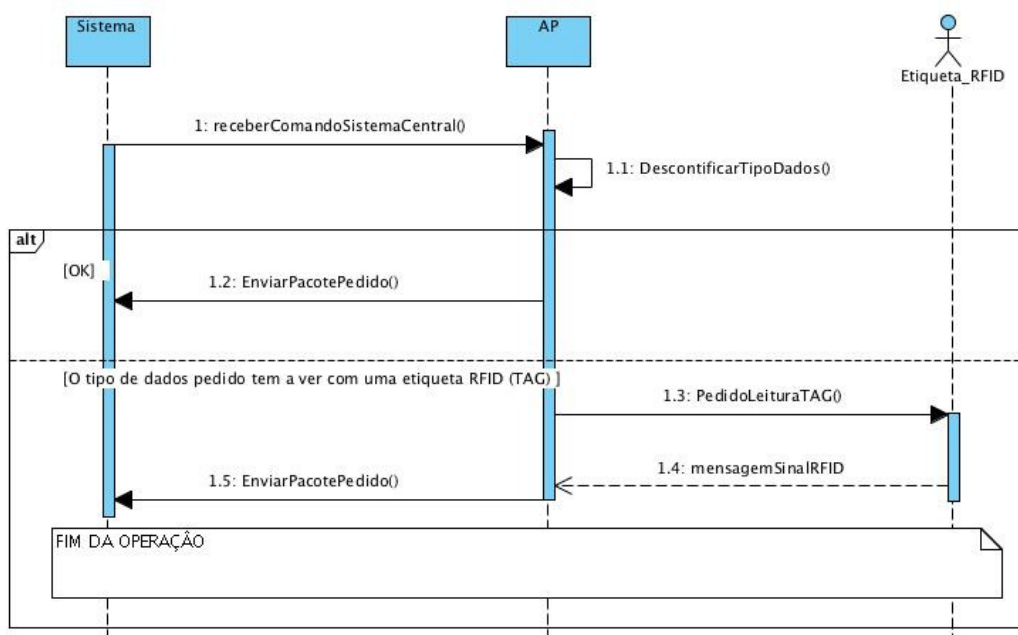
36. Diagrama de Sequência "Receção de mensagem de etiqueta_RFID"



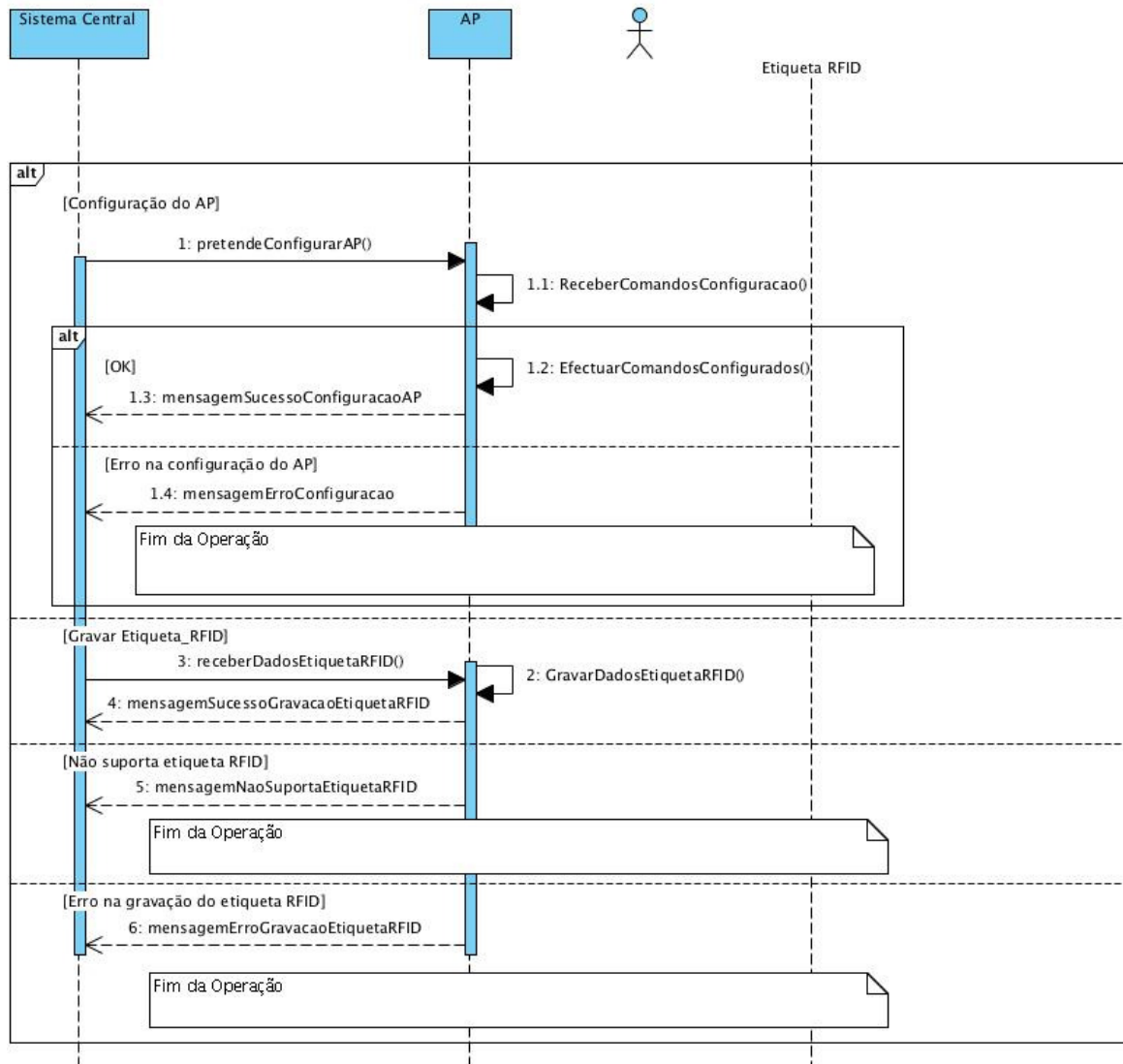
37. Diagrama de Sequência "Enviar pacote construído para o sistema central"



38. Diagrama de Sequência "Responder a pedidos de leitura de configuração"



39. Diagrama de Sequência "Efetuar Configuração do AP"



Anexo VIII Protocolo de Comunicação entre o(s) Ponto(s) de Acesso e o Sistema Central

1. Protocolo utilizado no caso de uso “Configurar AP”

(i) Comando para configurar uma etiqueta RFID	
Descrição	Configurar uma etiqueta
Formato	STX+INS+{SN+Comando+Tipo+Dados}+BCC+END
Exemplo 1	[01]+“E”+“SN”+“r”+“40”+“00”+“xx”+[0D]
Valor	
STX	[01]
INS	“E”
SN	“SN” Número de série da etiqueta (8 Bytes)
Comando	“r” Ler dados “w” Enviar dados “X” Fazer o <i>reset</i> da etiqueta “B” Fazer a etiqueta emitir um sinal sonoro (bip) “L” Fazer a etiqueta emitir um sinal no LED
Tipo + Dados	Ler / Escrever dados: Tipo=“40” TAG Active Time Mode Tipo=“41” TAG Active Time Count Tipo=“42” TAG Active Off Tipo=“43” TAG Receive Count Tipo=“46” LED Mode Todos os Dados=“00”~“FF” Fazer o <i>reset</i> da etiqueta: Tipo=“00”; Dados=“00” Fazer a etiqueta emitir um sinal sonoro: Tipo=“00”; Dados=“00”~“FF” (x 0.1 sec) Fazer a etiqueta emitir um sinal no LED: Tipo=“00”; Dados=“00”~“FF” (x 0.1 sec)
BCC	“xx” (Hex)
END	[0D]

(ii) Comando para configurar o tipo de funcionamento do AP	
Descrição	Definir o tipo de funcionamento do AP
Formato	STX + INS + {Action Type} + BCC + END
Exemplo 1	[01] + "B" + "1" + "xx" + [0D] (programar)
Exemplo 2	[01] + "B" + "0" + "xx" + [0D] (ler)
Valor	
STX	[01]
INS	"B"
Action Type	0 Normal A Parar B Retornar R Reset
BCC	"xx" (Hex)
END	[0D]

(iii) Comando para configurar a porta de comunicação	
Descrição	Definir o tipo de porta que pretende usar para comunicar com o AP (tcpip, rs-232, rs-485, etc.)
Formato	STX + INS + {Send Port} + BCC + END
Exemplo 1	[01] + "M" + "xx" + [0D] (programar)
Exemplo 2	[01] + "M" + "0" + "xx" + [0D] (ler)
Valor	
STX	[01]
INS	"M"
Send Mode	"0" Todas as portas (por omissão) "1" TCP/IP "2" Porta RS-232 "3" Porta RS-485
BCC	"xx" (Hex)
END	[0D]

(v) Comando para especificar o filtro do nível de RSSI	
Descrição	Definir o nível mínimo de potência do sinal RF (RSSI) para se considerar uma recepção válida
Formato	STX + INS + {RSSI level} + BCC + END
Exemplo 1	[01] + "N" + "A0" + "xx" + [0D] (programar)
Exemplo 2	[01] + "N" + "xx" + [0D] (ler)
Valor	
STX	[01]
INS	"N"
RSSI Level	"A0" (Hex)
BCC	"xx" (Hex)
END	[0D]

2. Protocolo utilizado no caso de uso “Enviar Comando ao AP para Ler a Configuração”

Comando	
Descrição	Enviar um comando ao AP para obter dados de qualquer etiqueta RFID
Formato	STX + INS + BCC + END
Exemplo	[01] + “C” + “xx” + [0D]
Valor	
STX	[01]
INS	“C”
BCC	“xx” (In Hex format)
END	[0D]

Resposta	
Descrição	Ler o pacote do <i>socket</i> adequado (<u>primeiro passo</u> do caso de uso “ Receber pacote de AP por TCP/IP ”).
Formato	STX + INS + {Data} + BCC + END
Sucesso 1	[02] + “C” + “xx” + [0D] (<i>sem dados</i>)
Sucesso 2	[02] + “C” + “aaaaaaaaaaaaaaaa” + “bb” + “cc” + “dd” + “xx” + [0D] (<i>Etiqueta Tipo I</i>)
Sucesso 3	[02] + “C” + “aaaaaaaaaaaaaaaa” + “bb” + “cc” + “dd” + “eeee” + “xx” + [0D] (<i>Etiqueta Tipo II</i>)
Sucesso 4	[02] + “C” + “aaaaaaaaaaaaaaaa” + “bb” + “cc” + “dd” + “eeee” + “ffff” + “xx” + [0D] (<i>Etiqueta Tipo III</i>)
Modo de comando	[02] + “C” + “R” + “aaaaaaaaaaaaaaaa” + “g” + “hh” + “ii” + “xx” + [0D]
Valor	
STX	[02]
INS	“C”
Data	“aaaaaaaaaaaaaaaa” → Número de série da etiqueta (8 Bytes) “bb” → RSSI (indicador da potência do sinal RF recebido no recetor) “cc” → LQI (indicador da qualidade do sinal RF) “dd” → Indicador de entradas digitais: bit0: indicação de que foi premida uma tecla na etiqueta bit1: indicação de que a pulseira foi retirada do pulso bit3: indicação de que a etiqueta está a ligar-se ao recetor bit4-7: indicador do nível da bateria da etiqueta “eeee” → Temperatura T1 “ffff” → Temperatura T2 (se a pulseira foi retirada T1 e T2 serão diferentes) “g” → Comando “hh” → Tipo de comando “ii” → Dados do commando
BCC	“xx” (<i>Hexadecimal</i>)
END	[0D]

Comando para indicar ao AP o tipo de dados da configuração que se pretende ler (<u>passo 4</u> do cenário principal do caso de uso)	
Formato 1	STX + INS + BCC + END
Formato 2	STX + INS + { ID } + BCC + END
Formato 3	STX + INS + {UAddr + UByte} + BCC + END
Formato 4	STX + INS + { UAddr + UByte + UData } + BCC + END
Exemplo 1	[01] + INS + “xx” + [0D] (ler)
Exemplo 2	[01] + “T” + “01” + “xx” + [0D]
Exemplo 3	[01] + “U” + “0000” + “04” + “xx” + [0D]
Exemplo 4	[01] + “U” + “0000” + “04” + “12345678” + “xx” + [0D]
Valor do Formato 1 – Qualquer tipo de configuração	
INS (<i>tData</i> no Caso de Uso)	“C” – Leitura de dados de uma etiqueta “D” – Leitura do S/N da etiqueta “S” – Leitura do S/N do AP “V” – Leitura da versão do <i>firmware</i> do AP “T” – Leitura do ID da rede do AP
BCC	“xx” (Hex)
Valor do Formato 2 – Leitura da rede do AP	
STX	[01]
INS	“T” – Leitura do ID da rede do AP
ID	“xx” (ID da rede) (Hex)
BCC	“xx” (Hex)
END	[0D]
Valor do Formato 3 – Leitura de dados do utilizador	
STX	[01]
INS	“U” – Leitura de dados do utilizador
UAddr	“xxxx” (“0000”-“00FF”) (Hex)
UByte	“xx” (“00”-“80”) (Hex)
UData	UByte bytes de dados (Hex)
BCC	“xx” (Hex)
END	[0D]

Resposta à leitura do pedido de dados da configuração (<u>passo 5</u> do cenário principal do caso de uso)		
Valor do Formato 1 – Resposta ao pedido de leitura de dados do utilizador		
Formato	STX + INS + {UData} + BCC + END	
Exemplo	[02] + “U” + “UData” + “xx” + [0D]	
Valor	STX	[02]
	INS	“U”
	UData	UByte bytes de Dados (Hex)
	BCC	“xx” (Hex)
	END	[0D]
Valor do Formato 2 – Resposta ao pedido de leitura do ID da rede do AP		
Formato	STX + INS + {ID} + BCC + END	
Exemplo	[02] + “T” + “ID” + “xx” + [0D]	
Valor	STX	[02]
	INS	“T”
	ID	“xx” 2 caracteres
	BCC	“xx” (Hex)
	END	[0D]

Valor do Formato 3 – Resposta ao pedido de leitura do S/N da etiqueta		
Formato	STX + INS + {SN} + BCC + END	
Exemplo	[02] + “S” + “SN” + “xx” + [0D]	
Valor	STX	[02]
	INS	“D”
	SN	“xxxxxxxxxxxxxx” 8 caracteres
	BCC	“xx” (Hex)
	END	[0D]
Valor do Formato 4 – Resposta ao pedido de leitura da versão do <i>firmware</i> do AP		
Formato	STX + INS + {Versao} + BCC + END	
Exemplo	[02] + “V” + “Versao” + “xx” + [0D]	
	STX	[02]
	INS	“V”
	Versao	“xxxxxxxxxxxxxxxxxxxxxx” 16 caracteres
	BCC	“xx” (Hex)
END	[0D]	
Valor do Formato 5 – Resposta ao pedido de leitura do S/N do AP		
Formato	STX + INS + {Estado + SN} + BCC + END	
Sucesso	[02] + “D” + “00” + “aaaaaaaaaaaaaa” + “xx” + [0D]	
Falha	[02] + “D” + “10” + “xx” + [0D]	
Valor	STX	[02]
	INS	“D”
	Estado	“00” → Sucesso “10” → Falha (Hex)
	SN	“aaaaaaaaaaaaaa” Número de série do AP (8 Bytes)
	BCC	“xx” (Hex)
	END	[0D]
Valor do Formato 6 – Resposta ao pedido de leitura de dados duma etiqueta		
Formato	STX + INS + {Dados} + BCC + END	
Sucesso 1	[02] + “C” + “xx” + [0D] (sem dados)	
Sucesso 2	[02] + “C” + “aaaaaaaaaaaaaa” + “bb” + ”cc” + ”dd” + “xx” + [0D] (Etiqueta Tipo I)	
Sucesso 3	[02] + “C” + “aaaaaaaaaaaaaa” + “bb” + ”cc” + ”dd” + ”eeee” + “xx” + [0D] (Etiqueta Tipo II)	
Sucesso 4	[02] + “C” + “aaaaaaaaaaaaaa” + “bb” + ”cc” + ”dd” + ”eeee” + ”ffff” + “xx” + [0D] (Etiqueta Tipo III)	
Modo de Comando	[02] + “C” + “R” + “aaaaaaaaaaaaaa” + “g” + ”hh” + ”ii” + “xx” + [0D]	
Valor	STX	[02]
	INS	“C”
	Dados	“aaaaaaaaaaaaaa” → Número de série da etiqueta (8 Bytes) “bb” → RSSI (indicador da potência do sinal RF recebido no recetor) “cc” → LQI (indicador da qualidade do sinal RF) “dd” → Indicador de entradas digitais: bit0: indicação de que foi premida uma tecla bit1: indicação de que a pulseira foi retirada do pulso bit3: indicação de que a etiqueta se está a ligar ao

		<p>recetor</p> <p>bit4-7: indicador do nível da bateria da etiqueta</p> <p>"eeee" → Temperatura T1</p> <p>"ffff" → Temperatura T2 (se a pulseira foi retirada T1 e T2 serão diferentes)</p> <p>"g" → Comando</p> <p>"hh" → Tipo de comando</p> <p>"ii" → Dados do comando</p>
	BCC	"xx" (Hex)
	END	[0D]

Valor do Formato 7 – Resposta ao pedido de leitura do S/N do AP		
Formato	STX + INS + {Estado} + BCC + END	
Sucesso	[02] + "E" + "00" + "aaaaaaaaaaaaa" + "xx" + [0D]	
Falha	[02] + "E" + "10" + "xx" + [0D]	
Valor	STX	[02]
	INS	"E"
	Estado	"00" → Suceso "10" → Falha (Hex)
	SN	"aaaaaaaaaaaaa" Número de Serie do AP (8 Bytes)
	BCC	"xx" (Hex)
	END	[0D]