Mapeamento de aglomerados de pessoas em espaços livres no contexto de distanciamento social e de contágio de COVID-19

Pedro Valverde
Departamento de Investigação e Desenvolvimento
da Bright Science, Mora – Portugal

José Curva
Departamento de Investigação e Desenvolvimento
da Bright Science, Mora – Portugal

Resumo – Os espaços públicos ou privados excedem os limites de ocupação quando ultrapassam a caracterização própria definida nomeadamente pelas entidades de saúde para a concentração de pessoas. Contextos que impliquem alterações do número e geometria de lugares disponíveis, nomeadamente por imposição de regras de distanciamento social afetam a densidade e taxas de ocupação. A contagem de pessoas por áreas ou zonas geográficas, permite aferir e alertar os riscos de contágio pela verificação do cumprimento das regras de distanciamento. O sistema apresentado, deteta e contabiliza o número de telemóveis ou equiparáveis, com comunicações efetuadas via WiFi e Bluetooth. Analisando o sinal das transmissões de rádio, referencia-os no espaço geográfico e mapeia as aglomerações pelas suas densidades ocupacionais.

Palavras-chave - distanciamento social, concentração de pessoas, riscos de contágio, mapeamento ocupacional, verificação de cumprimento.

I – Introdução

No panorama atual de pandemia impõe-se o cumprimento das recomendações da Direção Geral de Saúde e das medidas de prevenção e combate à COVID-19, nomeadamente das medidas preventivas, pessoais e sociais de distanciamento social, minimizando a proximidade entre indivíduos, essenciais para minimizar o risco de contágio. Neste contexto de combate à COVID-19, inserem-se medidas de investigação e desenvolvimento de soluções tecnológicas que permitam manter de uma forma simplificada, passiva e não intrusiva, o distanciamento social e a não lotação de espaços, fechados ou abertos, com particular relevância este último, tendo em conta o aproximar do verão e a especial apetência das populações pelas praias e zonas de convívio social nesta altura do ano. Pretende-se, com este projeto, investigar e desenvolver uma solução diferenciadora e bastante económica, capaz de monitorizar de forma transparente e segura a lotação de pessoas, por zonas, num espaço, através da densidade de equipamentos pessoais, e assim medir o distanciamento social, com a capacidade de emitir alertas, assim que ultrapassado o número estimado de pessoas por local em blocos dinâmicos ou a proximidade entre indivíduos.

II – Trabalho relacionado

A solução foi desenhada com base num modelo multifuncional hierárquico de sistemas distribuídos considerando o diagrama de componentes apresentado na Figura 1:

- Dispositivo Sensor (*GSM* [1] e *LoRaWAN* [2]) – elemento com a capacidade de monitorizar ondas rádio na banda dos 2.4GHz, processar em tempo real a sua descodificação segundo as variantes do protocolo 802.11 [3], e caraterizar os tipos de dispositivos emissores da comunicação através dos cabeçalhos das tramas recebidas. A camada física de monitorização e descodificação de rádio é executada com recurso a um módulo OEM incorporado, com processamento dedicado e independente. A informação recolhida é submetida a três camadas funcionais: compressão, anonimização/encriptação e comunicação. O dispositivo incorpora 2 níveis de processamento de dados e gere as respetivas estruturas de suporte de informação e transporte de forma nativa. O controlo da camada de rede é gerido ao nível físico por modems especializados de *LoRaWAN* e *GSM* (embebidos como OEM no hardware) através de duas variantes distintas de placas de circuito impresso. O trabalho de I&D realizado no sensor, focou-se nas tarefas de construção, desde o hardware (considerando a sua escolha, montagem e incorporação dos módulos OEM indicados acima) até à investigação, desenvolvimento e teste dos métodos e algoritmos envolvidos no processamento presentes a dois níveis distintos neste dispositivo conforme descrito na alínea e);

- Serviço de Rede (GSM e LoRaWAN) – serviços de transmissão de dados móveis máquina-a-máquina, de baixa largura de banda, correspondentes às redes de operadores de comunicações no caso da tecnologia GSM e aos serviços de rede compostos por Base Stations e Network Server no caso da tecnologia LoRa;

- Serviço de Dados – em termos técnicos o ambiente é baseado em Linux, composto por máquinas virtuais instaladas com serviços de resposta *HTTP [4]* e *MQTT [5]* sobre *SSL [6]*, interpretadores de linguagens *script PHP [7]*, *Python [8]* e *NodeJS [9]*, base de dados *MariaDB* [10] e *PostgreSQL [11]*. Em termos funcionais os serviços são segmentados em gestão da rede dos sensores e interface de programação aplicacional de front-end com os utilizadores dos serviços.

- Aplicação de Utilizador – aplicação com processamento e interface final apresentada ao utilizador, através de componentes *HTML5 [12]*, *CSS [13]* e aplicações executadas do lado do cliente pelo *engine javascript* presente nos

Cofinanciado por:
COMPETE 2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

browsers modernos compatíveis com a sigla *HTML5* para modelos de navegação *responsive*.

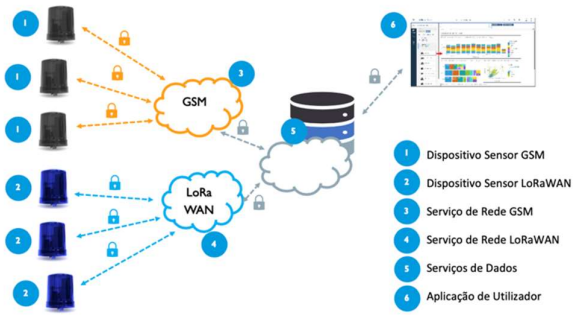

Figura 1 – Arquitetura e componentes do sistema.

a) Arquitetura macro do dispositivo sensor

O desafio proposto foi atingir uma elevada flexibilidade combinada pela relação entre o caso de utilização e a evolução dos desenvolvimentos com mais do que uma tecnologia comunicação de modo a endereçar futuras tecnologias. A modularidade na conceção da solução, permite-nos potenciar a reutilização de hardware como componentes constituintes, tanto nos processos de desenvolvimento, como nos diversos cenários de teste e produção, mantendo estruturas e hierarquias comuns.

Os módulos concebidos ao nível do hardware, conforme representados na figura 2, de baixo para cima são: medidor de energia, fonte de alimentação, unidade de processamento principal, unidade de comunicações IoT, unidade de processamento sensorial.

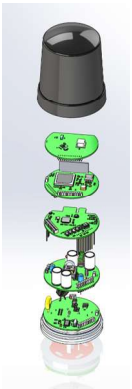

Figura 2 – Módulos de hardware.

b) Sensor de escuta por rádio

O endereçamento da camada física rádio a 2.4GHz foi efetuado através da inclusão de um módulo OEM, permitindo obter acelerações no hardware tais como na desmodulação e no controlo digital de sinal. A arquitetura do *firmware* desenvolvido, tira partido de bibliotecas genéricas do fabricante e do modo de operação promíscuo no qual o acesso às tramas de dados descodificados é absoluto (sem filtragem). Com este nível de abstração consegue-se o acesso direto ao nível da força do sinal (*RSSI)* das comunicações identificadas, à gama de canais de frequências utilizadas e ao conteúdo transportado no protocolo de rede com standard IEEE 802.11[3]. A gestão destes processos é denominada de nível 1 conforme descrito mais à frente na alínea e).

c) Comunicações IoT

Ao nível do dispositivo sensor, a arquitetura definida possibilita múltiplas opções de comunicações tendo sido implementados neste caso 2 tipos: *LoRaWAN* e *GSM/2G*. Foram desenvolvidas e implementadas duas placas de circuito impresso distintas, incorporando no primeiro caso um modem *LoRaWAN* e no segundo um modem *GSM/2G*.

A investigação centrou-se no caso mais exigente em termos de características e recursos – *LoRaWAN* – para que a abordagem pudesse ser replicada de forma adequada às restantes tecnologias. No caso da utilização da tecnologia *LoRaWAN*, as restrições são mais sensíveis a volumes de dados (na ordem das dezenas de bytes) e a uma maior latência. A estrutura da informação neste caso não é compatível com listas de dados extensas passando a solução encontrada por efetuar a contagem de equipamentos identificados, no dispositivo, por gamas de *RSSI*. No caso do *GSM/2G*, não se verificam estes graus de limitações, pelo que podem ser obtidas e transmitidas características adicionais. Ainda assim, de forma a reduzir o volume de dados transmitido e aumentar a eficiência da solução, a informação é comprimida conforme descrito na alínea d).

Ao nível da gestão destes processos, a denominação é de nível 2 conforme descrito mais à frente na alínea e).

d) Rede e Segurança

O trabalho realizado focou-se em duas vertentes principais:

- Minimizar o impacto na utilização da rede de comunicações;
- Garantir a consistência, autenticidade e anonimidade dos dados recolhidos.

Para o primeiro ponto foi deduzido um modelo de gestão com base em amostragens de tempo variáveis, adequadas à quantidade de dispositivos detetados versus a capacidade de memória do microprocessador do sensor e duas estruturas de informação alternativas, nas quais é possível agregar localmente a informação em contadores conforme descrito na alínea c), para o caso de redes mais exigentes como é o caso de *LoRaWAN* e transmitir características adicionais dos equipamentos identificados, para o caso de redes mais eficazes como são as *GSM/2G*. Em qualquer dos casos a informação é comprimida sempre que o método se torne eficiente (dependendo da quantidade e frequência dos valores a transmitir) conforme descrito no ponto III c).

No segundo ponto foram aplicadas técnicas de *hashing* e de verificação de redundância cíclica, combinadas para reduzir e derivar identificadores, tornando-os anónimos e garantindo ao mesmo tempo a integridade dos dados conforme apresentado em III d).

A gestão destes processos é denominada a nível partilhado entre 1 e 2 conforme descrito na próxima alínea e)

e) Definição dos níveis de processamento de informação

Nível 1 - correspondendo à camada mais física, controla e analisa o espectro dos canais rádio disponíveis. Captura e tipifica as comunicações dos equipamentos na rede sem fios, verifica a força de sinal (*RSSI)*, efetua a contagens das

comunicações, processa a compressão e a anonimização dos dados recolhidos no sensor.

Nível 2 – nível de controlo e transporte de dados que estabelece e lida com os protocolos de comunicação, assegura a encriptação e segurança dos dados, controla e gere os modems (*GSM* ou *LoRaWAN)* no sensor. É responsável pela entrega dos dados recolhidos no nível 1 ao sistema central de nível 3.

Nível 3 – corresponde ao sistema central, encarregue da gestão da rede de sensores. Assegura o envio/receção da informação do lado do servidor (para e dos sensores via *GSM* ou *LoRaWAN*), o tratamento e agregação dos dados recolhidos, as interfaces de programação (*APIs*) internas e externas (tais como o acesso e gestão de dados nas bases de dados a gestão de mensagens *MQTT* e a interação com aplicações distribuídas de utilizador) por acesso web.

III – Métodos propostos

a) Escuta e descodificação de emissões rádio

O método de captura das tramas envolve 2 processos distintos: *channel hopping* [14] e descodificação do cabeçalho da trama ao nível do MAC address em IEEE 802.11[3]
Ao nível do modelo OSI o método consiste na atuação ao nível das camadas 1 e 2 representados na tabela 1.

IEEE 802.11 Modelo OSI em WiFi

Contexto	Camada	Especialização
WiFi	1	Meio físico / Codificação / Deteção de Colisões
	2	Cabeçalho MAC
Rede	3	Cabeçalho IP
	4	Cabeçalho TCP
Aplicação	5 to 7	Aplicação / Codificação e Segurança / Gestão de Sessões

Tabela 1 –Modelo OSI em IEEE 802.11 aplicado a WiFi.

Ao nível da camada 1 do modelo OSI, o algoritmo processa o *channel hopping* varrendo os canais de 1 a 13 em modo de escuta, repetindo este processo em ciclo fechado para que seja possível detetar os dispositivos em toda a banda do *WiFi* a 2.4GHz. Para cada comunicação capturada, desmodula as tramas de dados e faz a medição do nível de sinal (*RSSI*).
Ao nível da camada 2 do modelo OSI, um segundo processo analisa o cabeçalho da trama, nomeadamente os dois octetos do *"Frame Control"* apresentado na tabela 2.

IEEE 802.11 WiFi Camada 2 - Formato da Trama (número de Octetos)

Frame Control	Duration	Address 1	Address 2	Address 3	Sequence	Address 4	QoS Control	HT Control	Payload	Checksum FCS	Total (Bytes)
2	2	6	6	6	2	6	0	0	0 - 2312	4	34 - 2346

Frame Control

Version	Type	Subtype	To DS	From DS	More Frag	Retry	Power Save	More	WEP	Order	Total (Bits)
2	2	4	1	1	1	1	1	1	1	1	16

Tabela 2 –Nível 2 da camada OSI WiFi.

A partir da informação dos dois octetos do *"Frame Control"* caraterizam-se o tipo de comunicação e os identificadores MAC (*"Media Access Control"*) de origem e destino referente aos dispositivos envolvidos na comunicação conforme a tabela 3.

Address Encoding

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	Destino	Origem	BSS ID	N/A
0	1	Destino	Envio AP	Origem	N/A
1	0	Receção AP	Origem	Destino	N/A
1	1	Receção AP	Envio AP	Destino	Origem

Tabela 3 –Nível 2 da camada OSI WiFi - address encoding

As colunas type e subtype na tabela 2 produzem a classificação de mensagens de acordo com os seguintes padrões:

- A mensagem provém de um Access Point ou de um dispositivo;
- A mensagem destina-se a um Access Point ou se é um Beacon / Probe Request [15].

A informação coletada é populada na memória do processamento de nível 1, na forma de um *array* associativo sobre o qual são aplicados os mecanismos de compressão, privacidade e segurança.

b) Cálculo da distância baseado no nível RSSI do sinal

Os modelos de propagação de ondas eletromagnéticas rádio, em espaço aberto, derivam da relação logarítmica inversa do sinal em função do dobro da distância, para aplicações sem obstáculos no caminho (*Free Space Path Loss*) [12].

$$FSPL = 20\log_{10}(d) + 20\log_{10}(f) + 20\log_{10}\left(\frac{4\pi}{c}\right) - G_{TX} - G_{RX} \quad (1)$$

Em (1), *d* corresponde à distância em metros, *f* a frequência em *Hertz*, *c* a velocidade de propagação no vácuo, *Gtx* e *Grx* o ganho em *dBi* das antenas relativamente ao ganho unitário para antenas não isotrópicas.

No caso de utilização de redes *WiFi*, é sabido que a potência de emissão não pode ultrapassar os 20 *dBm* em Portugal e na Europa (limite legal), e que a referida potência máxima se aplica ao ganho da antena do emissor, que tipicamente, em dispositivos móveis, não são antenas isotrópicas [16].

Sabendo que o ganho da antena do módulo de rádio sensor escolhido é de 3.7*dBi* e que as frequências de canais variam entre 2400 e 2483 (13 canais), é possível derivar as relações teóricas máximas entre sinal e distância representadas na figura 3, para potências de emissão efetivas, no meio ambiente, entre 0 *dBm* e 20 *dBm*.

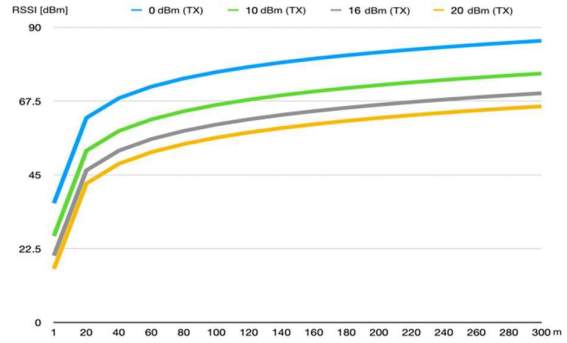

Fig. 3 – Relação entre distância e nível de sinal por cálculo em (1) para potências de emissão de 0, 10, 16 e 20 dBm.

Segundo a especificação do módulo utilizado, a antena recetora é do tipo F invertida impressa na placa de eletrónica (*PCB*), com um ganho máximo de 3.7*dBi* e introduz variância no plano X/Y não radialmente uniforme. O mesmo se passa ao nível dos equipamentos móveis emissores dos quais é desconhecido o diagrama de radiação.

Sabendo que os cálculos obtidos em (1) são teóricos e, portanto, apenas aplicáveis em condições ideais (sem obstáculos, sem interferências e quando não se conhece o ganho de sinal relativo aos ângulos em relação aos planos das antenas por desconhecer as posições dos emissores), é de esperar em ambiente real uma apreciável redução de sinal que será calibrada como coeficiente em função dos resultados obtidos por aprendizagem no terreno.

Com base em testes e medições no terreno foram aferidas 4 gamas de distância em função do sinal *RSSI,* classificado como bom, razoável, fraco e muito fraco correspondendo a:

- Bom – Maior que -65*dBm*: até 10 metros;
- Razoável – Entre -65 e -85*dBm*: de 10 a 50 metros;
- Fraco – Entre -85 e -90*dBm*: de 50 a 100 metros;
- Muito fraco – Menos de -90*dBm*: mais de 100 metros.

(2)

c) Compressão de dados coletados

Com base em [17], o procedimento de compressão-descompressão recorrendo a tabelas de *Huffman* é efetuado em 4 passos:

- Ler a informação a codificar, para determinar a frequência de cada caracter;
- Construir a tabela de *Huffman*, atribuindo códigos de comprimentos variáveis para cada caracter distinto (caracteres com maior frequência têm códigos menores);
- Ler novamente a informação a codificar, substituindo os caracteres pelo respetivo código;
- Descodificar a informação, recorrendo à tabela produzida.

Devido à variação de valores hexadecimais na informação a comprimir no caso de estudo, optou-se por uma solução baseada em tabelas dinâmicas e não em tabelas estáticas. Deste modo, é possível produzir uma tabela mais adequada à informação atual, pois ela vai ser composta pelos valores hexadecimais mais frequentes da mensagem à qual está acoplada. Por outro lado, o grau de compressão total é menos otimizado, devido ao envio de uma nova tabela aquando da transmissão de cada nova mensagem comprimida.

Para o caso em estudo, foi implementada uma adaptação da codificação de *Huffman*, na qual todos os códigos da tabela têm o mesmo comprimento, sempre de tamanho inferior ao dos caracteres hexadecimais. Deste modo, não é necessário especificar qual o código de *Huffman* associado a um dado valor hexadecimal, visto que este está subentendido na posição atribuída na tabela.

Sendo que as tramas a comprimir contêm valores hexadecimais de 8 bits, os códigos teriam de ser de tamanho inferior a 8 bits. Propôs-se neste caso que o tamanho da tabela seja estático, facilitando o processamento do programa, e recorrendo à fórmula:

$$\boldsymbol{S = 2^n - 1},$$

onde $\boldsymbol{S}$ é o tamanho da tabela de *Huffman* e $\boldsymbol{n}$ o número de bits por cada código da tabela. Deste modo, basta indicar quantos bits são usados para codificar a tabela para que o programa saiba qual o tamanho da mesma.

A informação comprimida é estruturada em 2 secções: um cabeçalho e um corpo. No cabeçalho da mensagem, é enviado o comprimento da trama original de informação, o número de bits usados para codificar e os caracteres hexadecimais a codificar. A ordem dos caracteres no cabeçalho indica o seu respetivo código. Se o 1º caracter apresentado for 0x00, o seu código será 0b00000, a 5 bits. Se o 12º caracter for 0xAB, o seu código será 0b01100, também a 5 bits. No corpo da mensagem, encontra-se toda a informação original comprimida, usando a tabela de *Huffman*. Dado que certos valores hexadecimais da mensagem podem não conter um código de *Huffman* associado, devido ao tamanho da tabela face ao número de valores hexadecimais distintos na mensagem original poder ser menor, é necessário indicar se os bits indicados representam um código ou o caracter de 8 bits original. Para tal, nos casos de utilização de um código da tabela, este é prefixado com um bit a 0 e nos casos de utilização de um caracter original de 8 bits, este é prefixado com um bit a 1.

d) Modelo de privacidade e segurança

Um endereço MAC é um conjunto de 6 valores hexadecimais de 8 bits cada (num total de 48 bits). Este endereço permite identificar univocamente um determinado equipamento numa rede de *Bluetooth* ou *WiFi*. Como tal, existe uma vertente de segurança que precisa ser endereçada, de modo a garantir a privacidade do utilizador do equipamento. Uma forma de endereçar este requisito é o recurso a algoritmos de *hashing*.

Um algoritmo de *hashing* toma um valor de entrada de tamanho variável, transformando-o num valor de saída de tamanho fixo, de modo a não ser possível associar o valor de saída ao valor de entrada. Alguns exemplos conhecidos são os MD5 de 128 bits e os SHA-256 de 256 bits. Estes algoritmos recorrem a rotações e deslocações de bits, operações lógicas, operações aritméticas e *padding* no processamento dos bits do valor de entrada original. No entanto, estes algoritmos não se verificaram adequados a este caso de estudo, devido ao grande incremento na dimensão do valor de entrada a anonimizar (endereço MAC de 48 bits para 128 ou 256 bits).

Alternativamente o *Cyclic Redundancy Check* (CRC), pode também ser utilizado como algoritmo de *hashing*. Através do CRC é gerado um valor de saída (*checksum*) de tamanho fixo, através de operações lógicas XOR e deslocações de bits, que sendo de menor dimensão que o valor de entrada, pode ser mais adequado para este caso [18].

Para este caso de estudo, foi investigada uma solução híbrida, com base nos algoritmos de *hashing* e no modo de funcionamento do CRC. Para tal, usa-se uma combinação de *checksums*, criando um endereço de 24 bytes, metade do tamanho original. Sendo este código diferente do original, aumenta-se assim o nível de segurança por um lado e reduz-se por outro o volume de informação a transmitir.

Para obter um *checksum*, é necessário definir um divisor representativo de um polinómio. No caso de um *checksum* de ***n*** bits, é assim necessário definir um polinómio de grau ***n***. Se usarmos como exemplo o polinómio:

$$x^8+x^2+x+1,$$

verificamos que a sua representação em divisor será um código de 8 bits, mais precisamente, o código **1000 0111**. Para obter o *checksum* de uma dada informação usando este valor, fazem-se operações lógicas XOR, da esquerda para a direita de forma cíclica, até que sobre apenas o resto da operação: o *checksum*.

Se aplicarmos o CRC com o polinómio supramencionado à trama "**02A0607C1094**", por exemplo, e calcularmos o respetivo *checksum,* o resultado será **0111 1110**, correspondente ao valor hexadecimal **7E**. Deste modo, é possível compreender que o código resultante desta combinação de operações é transformado em relação ao original de modo a garantir a anonimização da informação e a compressão da informação a transmitir.

IV – Resultados

A primeira aferição da performance e calibração do sistema foi realizada por meio da produção de 4 protótipos. Efetuaram-se ensaios aos sensores com telemóveis a circular no meio circundante a distâncias conhecidas, para dois tipos de ambientes distintos:

a) Em zona urbana, de cidade densamente povoada;
b) Em zona residencial, na periférica.

Os primeiros 3 sensores foram aplicados na zona a) e realizaram-se medições em modo de triangulação reduzida com poucos metros de interdistância entre cada sensor conforme a disposição na figura 5 e resultados na figura 6. As condições de instalação foram de tipo mural num edifício duma avenida de Lisboa, a cerca de 20 metros de altura relativamente ao solo. As distâncias do ensaio variaram entre 50 e 180 metros ao longo da avenida.

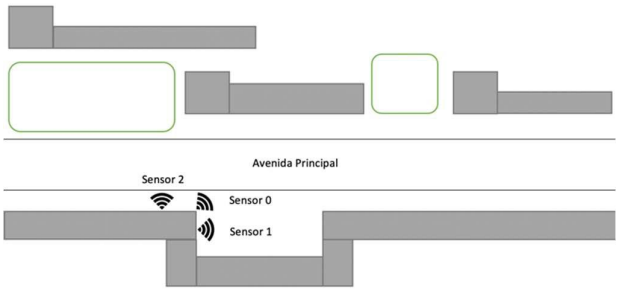

Fig. 5 – Diagrama de instalação de 3 sensores na zona a)

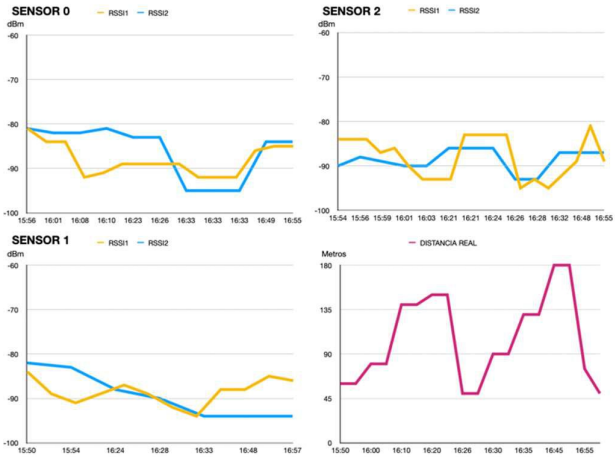

Fig. 6 – Relação entre distância real e medição de sinal captado nos sensores da zona a).

As medições foram efetuadas com mais de 200 pontos de acesso *WiFi* particulares existentes na zona de ensaio, tendo os sensores captado os telemóveis de teste até aos 180 metros e revelado aproximações aos cálculos teóricos.

O 4º sensor foi colocado em ambiente residencial, nos arredores de Lisboa a uma altura em relação ao solo de 1,5m tendo as medições sido efetuadas com telemóveis, circulando na zona circundante e tendo sido registadas as leituras indicadas na figura 7.

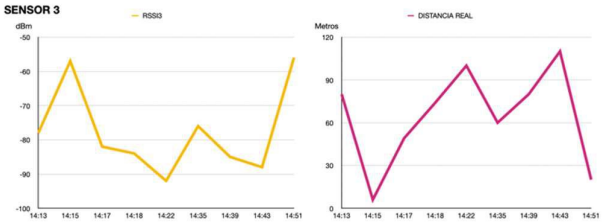

Fig. 7 – Relação entre distância real e medição de sinal captado no sensor da zona b)

V – Conclusões

A arquitetura implementada demonstrou uma modularidade que facilitou o desenvolvimento de cada uma das vertentes, nomeadamente pelo facto de, por exemplo, ter permitido trocar o módulo de comunicações *GSM* pelo módulo de *LoRaWAN* e vice-versa (com a simplicidade de trocar uma placa por outra), permitindo interligar da mesma forma os mesmos componentes alterando apenas o tipo das comunicações. Este tipo de operações de nível modular permitiu verificar e constatar as diferenças entre débitos e

latências, estabelecer análises comparativas com base nas performances obtidas, desenvolver, testar e consolidar software compatível para as diferentes combinações de hardware e sobretudo permitiu, desde a conceção, desenhar evoluir e otimizar as caraterísticas módulo a módulo, minimizando impactos com anomalias ou comportamentos não esperados, ajudando na resolução de processos de depuração, afinação e calibração dos sensores.

Ao nível do sensor rádio, com base nos ensaios efetuados, atendendo a que foram testados 3 sensores colocados na proximidade uns dos outros, não foi ainda possível constatar a eficiência da triangulação efetiva de telemóveis na área interior aferindo melhor a precisão com sinais abaixo dos -65*dBm* (i.e. mais de 10 metros). Os processos de *channel hopping*, leitura de nível de sinal e cálculo da distância pela fórmula *FSPL,* permitiram obter resultados coerentes, tendo-se atingido com sucesso o objetivo da caracterização do tipo de dispositivo. Testes efetuados com telemóveis identificados em rede *WiFi* foram identificados precisamente na categoria correta (como dispositivo registado) e ao ser feito o "esquecimento" da rede *WiFi* em que se encontravam, continuaram, na maior parte dos casos, a ser identificados, mas já como dispositivos nómadas, até intervalos da ordem dos 10 minutos após saírem da rede. Depois deste período de tempo os telemóveis utilizados "esconderam" o seu MAC real, tornando impossível a concretização das correspondências entre sinal e real identificação do telemóvel (pois em todos os casos ensaiados apareceram mais telemóveis desconhecidos na mesma zona).

Ao nível de testes de comunicação via GSM foi possível enviar conjuntos totais de dados respetivos a mais de uma centena de dispositivos detetados, i.e. dispositivos de todos os tipos: nómadas, registados, pontos de acesso e *Bluetooth*. Em comunicações *LoRaWAN*, não sendo possível o envio da mesma informação (por representar tramas com mais de 50 bytes de *payload* em *Spreading Factor* 12), foi em alternativa, possível segmentar a informação em vários pacotes de 50 bytes. Em *LoRaWAN* foi possível usar este método até algumas dezenas de dispositivos detetados. Acima desta ordem de grandeza (considerando a velocidade de transmissão mais baixa para modulação *LoRa*), deixam de ser cumpridos os limites legais europeus de *duty-cycle* de emissão por sensor. No caso das comunicações por *LoRa*, optou-se assim pelo envio das contagens totais nas gamas mencionadas no capítulo III b) ref. (2).

Em resumo, os dados comprovaram que existe uma correspondência direta entre o nível de sinal e distância entre os telemóveis e os sensores. Contudo fatores como obstáculos, reflexões e interferências causam desvios por vezes consideráveis que são atenuados com cálculos médios, especialmente se os telemóveis captados estiverem em movimento. Conclui-se que a aferição da distância relativamente ao sinal de rádio *RSSI* oscila consoante o ambiente circundante do sensor. Sempre que os erros provocados pelas reflexões de sinal, interferências ou obstáculos sejam representativos é necessária a aplicação de coeficientes de correção relativamente à fórmula *FSPL*.

Comprova-se igualmente que num ambiente com mais de 200 pontos de acesso disponíveis, usar a tecnologia *WiFi* com dispositivos conformes nas normas definidas na IEEE 802.11, cumprindo as respetivas regras (tais como o *Carrier Sense Media Access* entre outras), o sistema mantém a sua eficácia relativa.

VI – Trabalhos Futuros

Será determinante comprovar o sistema em condições distintas de triangulação, na ordem de equidistância de 100 metros, com 3 ou mais sensores, bem como a execução de simulacros com centenas de equipamentos.

A instalação de vários pilotos em espaços distintos durante um período experimental mais alargado, será um dos próximos passos que consideramos poder trazer maior valor acrescentado para a calibração e comprovação de toda a investigação, desenvolvimento e tecnologias aplicadas.

IV – Referências

[1] https://www.etsi.org/technologies/mobile/2g
[2] https://lora-alliance.org/about-lorawan/
[3] https://standards.ieee.org/standard/802_11-2020.html
[4] https://tools.ietf.org/html/rfc7230
[5] https://mqtt.org/mqtt-specification/
[6] https://tools.ietf.org/html/rfc8446
[7] https://www.php.net/
[8] https://www.python.org/
[9] https://nodejs.org/en/
[10] https://mariadb.org/
[11] https://www.postgresql.org/
[12] https://www.w3.org/TR/html51/
[13] https://tools.ietf.org/html/rfc7993
[14]https://frdgr.ch/wp-content/uploads/2015/06/Freudiger15.pdf
[15] http://sss-mag.com/pdf/802_11tut.pdf
[16]https://paginas.fe.up.pt/~amoura/APROWEB/AAM_Param_Fundamentais.pdf
[17] https://sci-hub.do/10.1145/3812.3815
[18] https://www.kernel.org/doc/Documentation/crc32.txt