Universidade Nova de Lisboa
Faculdade de Ciências e Tecnologia
Departamento de Informática

Dissertação de Mestrado

Mestrado em Engenharia Informática

Localização segura de objectos autenticados por RFID

Pedro Filipe Vicente Bernardo (aluno nº 26422)

2º Semestre de 2009/10

4 de Junho de 2010

Universidade Nova de Lisboa
Faculdade de Ciências e Tecnologia
Departamento de Informática

Dissertação de Mestrado

Localização segura de objectos autenticados por RFID

Pedro Filipe Vicente Bernardo (aluno nº 26422)

Orientador: Prof. Doutor Henrique João Lopes Domingos

Trabalho apresentado no âmbito do Mestrado em Engenharia Informática, como requisito parcial para obtenção do grau de Mestre em Engenharia Informática.

2º Semestre de 2009/10

4 de Junho de 2010

Para a minha namorada, os meus pais, tios, avós, primos, e ... para os meus amigos

Agradecimentos

Em primeiro lugar quero agradecer todo o suporte e apoio dados pelo meu orientador, o Prof. Doutor Henrique João Lopes Domingos. Ao longo desta dissertação, sempre procurou disponibilizar o máximo tempo possível para que pudessemos debater todos os temas envolvidos nesta dissertação. Sem qualquer dúvida, posso afirmar que foi uma ajuda preciosa em toda esta dissertação. Em todas as reuniões efectuadas sempre demonstrou grande interesse, pelo desenvolvimento efectuado pelo aluno e procurou sempre encaminhar o trabalho para que chegasse a bom porto.

Quero também agradecer ao departamento de informática por me ter concedido uma bolsa do Centro de Informática e Tecnologias da Informação (CITI), que sem dúvida nenhuma foi um importante suporte ao desenvolvimento desta tese.

Ao longo desta dissertação, tive o privilégio mais uma vez, de poder contar com a sempre preciosa ajuda da minha namorada, que me deu a força e a coragem necessárias, para enfrentar este trabalho.

Igualmente quero atribuir um agradecimento aos meus pais pela compreensão que sempre tiveram nas muitas ausências que aconteceram durante esta dissertação. Mais uma vez pude comprovar do seu amor e compreensão para comigo.

Aos meus amigos, deixo aqui um agradecimento especial pelo companheirismo e bom ambiente gerado durante esta dissertação. A vossa ajuda e cooperação foram determinantes para superar algumas das barreiras colocadas por esta dissertação. De entre este grupo destaco, o Danilo Manmohanlal, Nuno Luís, João Cartaxo, Amável Santo, Nuno Boavida, Bruno Félix, David Navalho, Emanuel Couto, pela sua disponibilidade durante este tempo.

Por último, quero agradecer a ajuda que o Prof. Doutor João Lourenço sempre procurou dar, nomeadamente no Latex, nas suas inúmeras visitas ao laboratório.

Resumo

Não obstante a utilização de tecnologia RFID estar hoje vulgarizada, a sua utilização em novas aplicações com requisitos de fiabilidade, ubiquidade, escala e segurança apresenta alguns problemas e limitações.

Na área da segurança de sistemas com tecnologia RFID, são importantes os aspectos associados à manutenção de propriedades de confidencialidade, autenticidade e privacidade dos alvos identificados, bem como garantias de operação confiável por parte de estações de leitura. São aspectos muito relevantes na monitorização ou localização de pessoas ou bens, em sistemas de monitorização remota, ubíqua e permeada em ambientes de larga escala, não supervisionados ou não coordenados por uma única entidade.

Por outro lado, a convergência entre a tecnologia RFID e as tecnologias da área das redes PAN sem fios (Wireless Personal Area Networks e redes 802.15.4), bem como com ambientes de redes de telefonia móvel, mostra-se uma direcção prometedora. Esta convergência apresenta desafios acrescidos à concretização de arquitecturas de segurança para monitorização e localização de alvos móveis identificados por RFID.

A presente dissertação visa propor, implementar e testar experimentalmente uma arquitectura de segurança para monitorização e localização remota de objectos autenticados por RFID. A arquitectura objectiva o suporte de ambientes de monitorização permeados e de grande escala, para localização ubíqua de alvos móveis. O sistema proposto conjuga protocolos de autenticação mútua entre dispositivos RFID, estações locais de monitorização e estações centrais de rastreio, salvaguardando condições de confidencialidade e de privacidade dos alvos.

A proposta considera ainda propriedades de fiabilidade e tolerância a intrusões como contramedidas complementares face a falhas de operação de estações locais de localização ou face a operação incorrecta das mesmas, resultantes de ataques por intrusão. Para o efeito usam-se mecanismos de processamento e agregação segura dos dados de localização, obtidos a partir de certificados de localização emitidos por estações independentes e enviados por múltiplas rotas de encaminhamento até às estações centrais de rastreio.

Palavras-chave: RFID, Segurança de sistemas RFID, Autenticação Mútua e Privacidade entre dispositivos RFID, Redes de Sensores sem Fios, Localização Segura de Objectos Móveis

Abstract

Nowadays RFID technology is very widespread in applications that have particular requirements of reliability, ubiquity, scale and security. These requirements present some problems and limitations.

In the computer security field, there are some important aspects in systems that use RFID technology such as, confidentiality properties, authentication, privacy, and guarantees that operations performed on reading stations are trustworthy. These aspects are relevant in monitoring or tracking people in remote monitoring systems, ubiquitous or large-scale, unsupervised or not coordinated by a single entity.

Nowadays RFID technology, wireless personal area networks, 802.15.4 networks, and mobile phone networks are converging and providing new challenges in developing secure architectures for monitoring and target location identification by RFID.

This thesis aims at implementing and evaluating an architecture for secure monitoring, and tracking of remote objects authenticated by RFID. The architecture supports large-scale monitoring environments, with possible tracking of ubiquitous targets.

Our proposed system combines protocols for mutual authentication between RFID tags, local monitoring stations and central stations. All of them ensure confidentiality and privacy of targets.

This thesis also provides reliability and intrusion tolerance properties as complementary countermeasure regarding failure of a local tracking station or against intrusion attacks. For this purpose, processing and secure data aggregation mechanism are used. The location data is previously obtained from independent stations that send information through several routing routes to central stations.

Keywords: RFID, Security of RFID Systems, Mutual Authentication and Privacy between RFID, Wireless Sensor Networks (WSN), Secure Tracking of Mobile Objects

Conteúdo

Lista de Figuras

Lista de Tabelas

1. Introdução

Actualmente, a utilização da tecnologia e dispositivos RFID [1] é vulgarmente utilizada em diferentes sistemas informáticos e em diversos domínios da aplicação, nomeadamente nos domínios da logística, na identificação, detecção ou localização de bens, mercadorias ou veículos; em sistemas de monitorização e inventariação de cadeias de distribuição e abastecimento de produtos; em sistemas de informação aeroportuários ou de portos marítimos; em sistemas de policiamento e controlo de circulação de veículos; em sistemas de identificação ou reconhecimento de pessoas; em sistemas de informação na área da saúde ou aplicações hospitalares; na área da indústria hoteleira; ou em inúmeras aplicações de gestão comercial e facturação.

A tecnologia de identificação de objectos com base em RFID (Radio-Frequency Identification), tem conhecido uma enorme evolução e interesse [71]. De acordo com dados publicados, a investigação e desenvolvimento da própria tecnologia deverá estar associada a investimentos directos que podem atingir entre 89 a 209 milhões de US dólares até 2012 [3], sendo uma das tecnologias de maior taxa de crescimento em vendas esperadas de novas tecnologias, com um mercado previsto de 11,1 biliões de US dólares, entre 2008 e 2012 [2].

De um modo geral, a tecnologia RFID permite a identificação, monitorização ou localização de objectos, de forma automática, sem utilização de comunicação com fios. A leitura de alvos RFID pode fazer-se a curtas distâncias, da ordem de alguns centímetros (no caso da utilização de leitores de RFID banais operando em baixa frequência na gama de 30 a 500 KHz e usando alvos de baixo custo baseados em dispositivos passivos), podendo ir até algumas dezenas de metros com possibilidade de detecção de alvos em movimento (no caso das soluções mais complexas e de elevado custo, envolvendo a instalação de antenas e receptores de alta frequência - nas gamas de 850 a 950 MHz e 2.4 a 2.5 GHz).

A banalização da tecnologia RFID tem permitido que o seu custo seja cada vez mais reduzido (nomeadamente ao nível das soluções de baixa frequência), e permite que as aplicações possam operar sobre alvos de monitorização, em melhores condições de fiabilidade, comodidade e cobertura, comparativamente a sistemas que usam formas de identificação por leitura óptica de códigos de barras ou de códigos de representação matricial (também conhecidos na terminologia de língua inglesa por *data-matrix codes*). A tecnologia RFID para alta frequência

[1] Ao longo da dissertação, RFID é usado como um acrónimo da designação em língua inglesa "Radio-Frequency-IDentification", que pode ser traduzida para língua portuguesa como "Identificação por Rádio-Frequência", referindo-se esta designação a uma tecnologia e um método de identificação automática de alvos através de sinais codificados e transmitidos por rádio frequência.

possui contudo limitações para utilização em sistemas ubíquos ou de monitorização permeada em ambientes de grande escala, devido aos constrangimentos provocados pela utilização do espectro de frequências livres e devido a exigir formas de operação geograficamente controladas, sob a coordenação de entidades particulares.

Não obstante a sua ampla utilização, a tecnologia RFID apresenta alguns problemas em aplicações recentes que possuem novos requisitos particulares, destacando-se aspectos de fiabilidade, ubiquidade, escalabilidade e segurança. Na área da segurança informática de sistemas que utilizam tecnologia RFID, são particularmente conhecidos os problemas associados a garantias de confidencialidade, autenticidade e privacidade em protocolos que utilizam identificação de sujeitos principais.

Os problemas anteriores são particularmente importantes em aplicações de monitorização que podem envolver pessoas ou bens confidenciais, ou em sistemas para monitorização permeada e não supervisionada, nomeadamente quando estes são utilizados em ambientes de acesso público ou de requisitos de cobertura de grande escala geográfica ou de grande número de objectos em movimento.

Para a resolução de alguns desses problemas, a convergência da tecnologia RFID e da tecnologia e normalização na área das redes PAN (Personal Area Networks) ou das redes de dispositivos de comunicação no espectro IEEE802.15.4 [1] ou tecnologia Zigbee [9], mostra-se como uma direcção bastante prometedora. No âmbito destas redes, a miniaturização de dispositivos computacionais que podem dispor de capacidades muito limitadas e específicas de processamento, memória, conversão analógico-digital e autonomia de energia, aliado ao abaixamento do seu custo, devido ao enorme leque de aplicações de redes de sensores e de actuadores para os mais diversos fins, permite que a anterior convergência seja uma hipótese cada vez mais justificada.

Por outro lado, a convergência tecnológica entre a normalização RFID, as redes 802.15.4, bem como outras normas de protocolos de comunicação já bem instituídos no domínio da computação e telefonia móvel (como por exemplo Bluetooth, 802.11 ou GPRS/UMTS), permite que dispositivos computacionais de grande proliferação, como por exemplo pequenos computadores portáteis, computadores de bolso ou PDAs (Personal Digital Assistants), bem como telefones móveis, possam operar como nós intermédios de monitorização ou de detecção de presença de alvos identificáveis por RFID, podendo assim actuar como estações de monitorização e localização desses alvos. Nesta visão, este tipo de equipamentos podem vir a ser usados como estações locais de monitorização, utilizadas de forma ubíqua, colaborativa ou oportunista, de

forma similar aos sistemas para sensoriamento participativo ou colaborativo.

1.1 Problemática

A utilização de tecnologia RFID e a sua convergência com outras tecnologias de redes sem fios, em novas aplicações que possuem requisitos particulares de segurança, escalabilidade, ubiquidade e fiabilidade, apresenta diversos problemas e coloca novos desafios. Na área da segurança informática destes sistemas, são particularmente importantes os aspectos associados à manutenção de propriedades de confidencialidade, autenticidade e privacidade.

Os problemas anteriores são particularmente importantes em aplicações de monitorização que podem envolver pessoas ou bens confidenciais, ou em sistemas para monitorização permeada e não supervisionada, nomeadamente quando estes são utilizados em ambientes de acesso público ou não supervisionados por uma mesma entidade. São igualmente importantes os problemas impostos por requisitos de cobertura e mobilidade de grande escala geográfica ou em cenários envolvendo um grande número de objectos em movimento.

Do ponto de vista das propriedades específicas de segurança, destacam-se particularmente os seguintes problemas:

- Necessidade de se garantir autenticação mútua entre os objectos-alvo e os sistemas de localização, nomeadamente através de estações locais de monitorização e estações ou sistemas centrais de rastreio.

- Necessidade de garantir a confidencialidade de dados trocados entre os alvos e os diversos subsistemas envolvidos numa arquitectura global de monitorização e localização.

- Necessidade de garantir condições de privacidade na utilização de objectos-alvo, nomeadamente quando estes são usados para identificar pessoas ou bens críticos.

- Necessidade de garantir condições de segurança extremo-a-extremo, entre alvos identificados e autenticados por RFID e estações centrais de rastreio que possam ser usadas como bases de computação confiáveis, independentemente do uso intermédio de estações locais ou estações de processamento intermédio de dados de monitorização ou localização.

- Necessidade de se tolerarem intrusões ou indução de informação falsa, em sistemas intermédios que actuem numa arquitectura global de monitorização, como estações locais de

monitorização ou de processamento intermédio de dados.

1.2 Objectivos da dissertação

A presente dissertação visa propor, implementar e avaliar experimentalmente uma arquitectura e um sistema de segurança para monitorização remota da localização de objectos móveis autenticados através de RFID. A arquitectura proposta tem como contexto motivacional o enquadramento anteriormente introduzido.

No sistema visado, os objectos associados aos alvos RFID podem estar em movimento e comunicam a sua identificação, de forma mutuamente autenticada, para estações locais de recepção e pré-processamento de identificadores RFID. Estas estações são dotadas de capacidades para detecção da sua própria localização geográfica (quando sejam estações móveis) ou possuem dados sobre a sua localização actual (quando sejam estações fixas).

As estações locais actuam como leitores locais de identificadores RFID e associam às identificações dos objectos detectados, a emissão de certificados autenticados que associam a sua própria localização a esses mesmos identificadores. Estes certificados são transmitidos para as estações centrais de rastreio remoto, constituindo estas, nós de computação confiáveis na arquitectura do sistema. As estações centrais procedem ao processamento e agregação final de informação recebida para gestão dinâmica da localização segura dos objectos-alvo identificados. As estações de rasteio podem também ser usadas como *gateways* para sistemas de informação finais mais complexos, associados a aplicações específicas.

A transmissão dos certificados de localização emitidos pelas estações locais para as estações de rastreio, pode ser efectuada através de diferentes mecanismos de comunicação segura que estão hoje bem estabelecidos, nomeadamente, redes locais, redes celulares ou através do encaminhamento de dados, como redes sobrepostas extremo-a-extremo, suportadas em ambiente *Internet*.

O sistema proposto na dissertação visa suportar ambientes de monitorização permeados e de grande escala, para localização ubíqua de alvos em movimento em ambientes não necessariamente supervisionados. O sistema proposto conjuga as propriedades de protocolos de autenticação mútua entre dispositivos RFID, estações de monitorização RFID e estações centrais de rastreio, assegurando ainda a confidencialidade de dados e a salvaguarda de condições de privacidade sobre os alvos monitorizados.

Simultaneamente, o sistema proposto apresenta mecanismos para tolerância a intrusões, de modo a prevenir potenciais ataques realizados contra as estações locais. Estes mecanismos introduzem condições de resiliência no processamento intermédio e agregação segura de dados das localizações, com base em certificados de localização emitidos por múltiplas estações e que podem ser enviados por múltiplas rotas de encaminhamento até às estações centrais de rastreio.

1.3 Principais contribuições

As principais contribuições da dissertação são resumidas da seguinte forma:

- Proposta de uma arquitectura de segurança para localização de objectos identificados com RFID, sendo essa localização monitorizada por estações locais de monitorização e transmitida para estações centrais de rastreio, com base em protocolos de autenticação mútua e preservando condições de confidencialidade e privacidade dos alvos de monitorização.
- Proposta de protocolos variantes para localização dos objectos-alvo identificados por RFID, por parte das estações locais de detecção de localização desses objectos, com diferentes opções e garantias de confidencialidade e privacidade dos dados associados aos identificadores monitorizados, bem como diferentes condições de mobilidade dos alvos. Estas variantes possibilitam ainda a materialização e adequação da arquitectura quando são utilizadas diferentes tecnologias, com características específicas.
- Proposta de mecanismos de tolerância a falhas ou operação incorrecta devido a intrusões ao nível de estações locais, considerando a sua operação remota, não supervisionada ou não coordenada por uma só entidade.
- Implementação e avaliação experimental da arquitectura e sistema propostos com base em protótipos, para estudo dos seguintes critérios de validação:
  - Condições de latência do protocolo de localização e obtenção de indicadores de suporte de mobilidade dos alvos.
  - Condições de precisão da localização obtida.
  - Condições de tolerância a falhas de operação, ao nível das estações locais de detecção e localização dos alvos, ou de resistência face a operação incorrecta que possa ser provocada por intrusões nessas mesmas estações.

  - Avaliação do impacto energético e de latência, quando utilizadas diferentes *suites* e métodos criptográficos.
  - As avaliações indicadas são realizadas numa base de simulação e num protótipo real de verificação e avaliação experimental de protocolos, a partir de uma implementação de alvos e estações locais de monitorização, com base em tecnologia e sensores Sun SPOT comunicando por IEEE 802.15.4, bem como de um ambiente com alvos RFID monitorizados e localizados por NFC, a partir de estações materializadas com base em dispositivos de leitura de RFID embebidos no telefone móvel.

1.4 Organização e estrutura do relatório de dissertação

O restante documento encontra-se organizado da seguinte forma:

- O capítulo 2 contêm uma apresentação inicial sobre a tecnologia RFID, uma visão complementar da convergência entre tecnologia RFID e a área das redes de sensores sem fios suportadas em comunicações IEEE 802.15.4 e revisita em detalhe os objectivos e contribuições da dissertação.
- O capítulo 3 apresenta sumariamente uma descrição sobre redes de área global, local e pessoal, relacionando o contexto de utilização dessas redes com o âmbito da dissertação. Este capítulo apresenta uma abordagem inicial a protocolos de autenticação e apresenta o trabalho relacionado com o contexto e âmbito específicos da dissertação.
- O capítulo 4 é dedicado à apresentação do modelo arquitectural e sua apresentação conceptual, definindo a arquitectura de segurança para localização segura de objectos RFID proposta pela dissertação.
- O capítulo 5 apresenta a implementação do modelo e arquitectura anteriormente descrita no capítulo 4, tendo por base um ambiente de simulação e um protótipo real para avaliação experimental.
- O capítulo 6 apresenta um conjunto de testes para avaliação do sistema proposto.
- Finalmente, o capítulo 7, resume as principais conclusões retiradas da realização da dissertação, discute alguns aspectos em aberto e apresenta direcções para trabalho futuro.

2. RFID e convergência entre RFID e redes 802.15.4

2.1 RFID

Como se introduziu no capítulo 1, RFID é um método usado para protocolos de identificação automática de bens, objectos ou pessoas, através de sinais de rádio. Os dados de identificação são obtidos ou emitidos de dispositivos (alvos RFID) também designados por *tags* ou, na tecnologia de RFID para baixa frequência e curto alcance, por etiquetas de RFID [84]. Neste caso, as etiquetas podem ser associadas a objectos-alvo de monitorização e funcionam como pequenos emissores de sinal rádio (ou RFID *transponders*), podendo estes emissores ser materializados em dispositivos de pequeníssimas dimensões (de cerca de $1mm^2$ a $1cm^2$ e espessura pouco maior do que uma folha de papel). Estes dispositivos podem assim ser colocados em pessoas [70], animais [83] ou bens (nomeadamente equipamentos, embalagens ou produtos).

Na tecnologia mais banalizada de RFID para detecção em baixa frequência (nas gamas de 30 a 500 KHz), as etiquetas RFID são materializadas num pequeno substrato contendo um *chip* de silício e uma antena de recepção ou emissão de rádio frequência, sendo capaz de comunicar com controladores ou leitores RFID (ou estações controladoras de RFID). Além de etiquetas passivas, que não possuem energia própria e que respondem a sinais enviados pelo controlador (com base numa excitação energética obtida da própria estação base), existem etiquetas designadas por etiquetas activas [72] (possuindo estas energia própria e podendo transmitir de forma autónoma o seu identificador) ou semi-passivas ou semi-activas (no caso de poderem operar com ou sem autonomia ou combinando os dois modos de operação).

Um controlador RFID é um dispositivo com interface de controlo para um sistema periférico de RFID (antena ou leitor e *transponders*), intermediando a comunicação entre as etiquetas e um sistema de informação de gestão (ou sistema final). Este sistema pode ser constituído num computador vulgar, ou pode ser implementado por um *gateway*, com base num suporte *middleware*, para inter-operação do ambiente de monitorização e sistemas e aplicações mais ou menos especializadas e de maior ou menor complexidade, dependendo da aplicação em vista.

2.2 *Middleware* para sistemas RFID

Os suportes *middleware* para integração de aplicações RFID são normalmente constituídos por *gateways* aplicacionais ou por bibliotecas e suportes *runtime*. Estes sistemas operam por subscrição de canais de eventos RFID (recebidos pelos leitores ou receptores RFID) e suportam APIs para interrogação periódica ou "a pedido" de objectos detectados, com consequente captura da informação recebida e enviada pelas etiquetas de RFID [84].

De um modo geral, os suportes *middleware* para sistemas RFID disponibilizam capacidades de pré-processamento de sinal recebido pelas antenas (depurando ruído, tratando anúncios sem garantia de integridade ou eliminando redundâncias ou duplicados de leituras em intervalos temporais). Com base nesse pré-processamento, fornecem as informações pré-processadas ao sistema que deve então processar a informação recebida, e que se pode integrar no âmbito de um sistema de gestão de informação particularmente associada aos objectos monitorizados que estão associados aos identificadores.

O desenvolvimento de suportes *middleware* para sistemas RFID pode ter que atender a propriedades e características mais ou menos especializadas, de acordo com o fim em vista. No entanto e de um modo geral, apenas a componente de recepção e tratamento dos identificadores é normalizada. Isto exige aos programadores um grau relativamente importante de conhecimento técnico de detalhe sobre a integração (a baixo nível de abstracção) e as tecnologias utilizadas, o que implica normalmente informação de detalhe sobre cada tecnologia específica, verificando-se algumas variações de acordo com o *hardware* de cada fabricante e suas características [85].

A não normalização generalizada de sistemas *middleware* para integração genérica de aplicações RFID, está associada à heterogeneidade de SDKs (*System Development Kits*), o que dificulta a programadores não especialistas o desenvolvimento e prototipagem rápida e simplificada de aplicações, sua adaptação ou portabilidade. Este aspecto é ainda hoje um obstáculo à divulgação e generalização do uso da tecnologia, a par das limitações na área da segurança, que assumem particular relevância em aplicações críticas deste ponto de vista [57].

Não obstante as dificuldades, o contínuo decréscimo do custo da tecnologia apresenta-se como um factor que motiva o interesse, cada vez mais crescente, na utilização e investigação da tecnologia e sistemas baseados em RFID, motivando a investigação de sistemas e arquitecturas *middleware* que possam constituir bases genéricas de integração de serviços para aplicações cada vez mais complexas e com maiores requisitos de escalabilidade, ubiquidade, heterogeneidade, fiabilidade e segurança.

2.3 Aplicações de sistemas RFID

O domínio de aplicações que estão a ensaiar as vantagens de utilização da tecnologia RFID (algumas de investigação recente ou de validação emergente), não pára de crescer [49].

Uma das motivações iniciais é a substituição de formas de identificação convencional de objectos (como por exemplo, identificação por códigos de barras ou outros códigos de representação com notação impressa, como são por exemplo os códigos matriciais). Mas outras motivações vão mais longe, na utilização da tecnologia em sistemas e aplicações emergentes e inovadoras, bem como da avaliação do impacto e desenvolvimento de tecnologias para RFID e direcções de investigação que têm sido endereçadas na bibliografia disponível [68], [37]. De entre estas aplicações e direcções de investigação destacam-se: aplicações e sistemas de logística de escala global [21]; sistemas de pagamento seguro [43]; aplicações na gestão de sistemas hospitalares [36]; controlo de implantes humanos [61], monitorização de doentes na área da saúde [46], [42] ou como controlo de acesso de pessoas a áreas reservadas; implantes para controlo de animais [83], sistemas para estudo de *habitats* de animais [52]; sistemas de identificação de telefones celulares ou sua utilização como meios de pagamento electrónico de conveniência [45], [23], [37]; sistemas de gestão de bibliotecas e aplicações de sistemas de monitorização e vigilância de veículos ou equipamentos em zonas de acesso controlado ou reservado [90], bem como a integração de muitas destas aplicações no âmbito de sistemas de informação e visualização com realidade aumentada [87].

2.4 Controladores de RFID e utilização em protocolos de comunicação

Tal como se introduziu, estão disponíveis controladores de RFID susceptíveis de serem integrados em protocolos de comunicação, distinguindo-se pela faixa de frequência em que operam [84].

Os sistemas de baixa frequência (operando na gama de 30 a 500 KHz) são usados em protocolos de curta distância de leitura e de baixo custo, sendo utilizados para sistemas de controlo de acesso ou monitorização de localização e identificação de objectos estáticos ou de muito pouca mobilidade, em áreas internas e vigiadas. O seu domínio de aplicação está limitado a sistemas de informação muito localizados e com elevado nível de supervisão e controlo humano de operação.

Os sistemas de Alta Frequência (operando nas gamas de 850 a 950 MHz e 2,4 a 2,5GHz [72]) possibilitam leitura em médias ou longas distâncias, podendo identificar alvos que se podem mover em alta velocidade (entre 80 a 120 Km/h). São estes controladores que são usados em portagens viárias com aplicações de leitura de *tags* em veículos que as atravessam. Um exemplo deste tipo de aplicação é, por exemplo, a Via Verde - Sistema de Pagamento Electrónico da BRISA, Auto-estradas de Portugal [14]. Estes sistemas permitem identificação de objectos em zonas específicas de monitorização. No entanto possuem limitações de custo e de abrangência para monitorização segura e com precisão de ambientes ubíquos ou para concepção de sistemas permeados, nos quais se pretenda monitorizar uma grande quantidade de objectos que se desloquem em ambientes geográficos não supervisionados e de grande escala.

Resumidamente, a tecnologia RFID possibilita hoje dar resposta ao mesmo tipo de requisitos de sistemas convencionais de monitorização ou controlo por códigos de barras, com a vantagem de não terem requisitos tão restritivos de utilização de controladores e etiquetas em linha de vista. Além disso é possível guardar e gerir informação adicional, para além dos identificadores, o que permite a sua utilização na gestão integrada de informação detalhada sobre objectos, sua localização, ao mesmo tempo que se tem maior protecção e controlo sob a contrafacção.

No entanto, a utilização de sistemas RFID, como hoje são usados, para os requisitos de ambientes computacionais como se perspectivam na presente dissertação, apresenta obstáculos relevantes em termos de cobertura escalável e ubíqua, bem como limitações importantes de normalização, interoperabilidade, fiabilidade e segurança. Os dispositivos RFID estão a tornar-se cada vez mais comuns, em grande parte devido à redução do preço das etiquetas e sistemas que operam na gama de 30 a 500 KHz. Esse facto torna a tecnologia interessante para localização de objectos. Todavia, os dispositivos RFID para esse espectro de operação dispõem de pouca energia e cobertura de comunicação muito limitada, o que leva à procura de novas soluções para melhorar as suas funcionalidades.

2.5 Integração e convergência entre RFID e redes de sensores sem fios

A integração e convergência entre RFID e as redes de sensores sem fios (WSN ou *Wireless Sensor Networks*) possibilitam abarcar novos cenários de aplicação. Um sistema de localização de objectos RFID em grande escala pode desta forma ser realizado de um modo mais escalável,

fiável e seguro, tirando partido das capacidades de processamento e autonomia dos dispositivos típicos usados nas redes de sensores sem fios e dotados de capacidade para transmissão de identificadores, de modo semelhante aos actuais sistemas RFID. A convergência dessas tecnologias, possibilita igualmente a utilização de identificação RFID em redes de sensores e por outro lado, proporciona a melhoria da inteligência e capacidade do processamento e comunicação dos actuais protocolos e das actuais condições de segurança nos sistemas RFID. Esta hipótese tem sido formulada e seguida na investigação recente [41], [60], [81].

Nos cenários onde um leitor RFID necessite de processar inúmeras *tags*, a utilização de rede de sensores, ao invés de um leitor RFID tradicional, permite melhorar a largura de banda da informação, mais concretamente através da utilização de inúmeros sensores organizados de forma ad-hoc.

Adicionalmente, a integração de sensores e RFID tem implicações económicas, pois o custo de um sensor é consideravelmente mais barato que um leitor RFID, tendo ainda a vantagem adicional de possuir um maior raio de alcance. Como estas tecnologias estão a tornar-se cada vez mais generalizadas, o preço mais baixo do estabelecimento da rede, torna estas tecnologias mais atractivas.

Em [41] pode-se analisar uma integração real de um leitor RFID num sensor Mica2 (da Crossbow), que constitui uma arquitectura de processamento típica de redes de sensores sem fios, que opera de acordo com a norma IEEE 802.15.4. Para demonstração da viabilidade desta integração foi criado um protótipo, onde os dois dispositivos foram ligados fisicamente, de modo que o processamento efectuado pelo sensor, possa ser utilizado para comunicar com outras *tags* RFID.

Em [60] criou-se um nó especial para uma rede de sensores (HSN - *Hybrid Smart Node*), que combina a função das redes de sensores com as de um dispositivo RFID. O sensor contido nesse nó tem a responsabilidade de recolher a informação do meio, enquanto a *tag* fica encarregue do armazenamento dos dados. Esta integração possibilita que um sensor não esteja periodicamente a pedir informação, podendo desta forma estar passivamente à espera de dados. Desta forma, reduz-se o gasto de energia na troca da informação entre os dispositivos.

As referências bibliográficas anteriormente apresentadas e os projectos e sistemas experimentais que lhes estão subjacentes, demonstram que as hipóteses de convergência entre as redes de sensores sem fios e a tecnologia RFID são hipóteses de trabalho válidas. Estes resultados da investigação recente mostram pois, que a formulação dessas hipóteses no contexto de uma proposta de uma arquitectura de monitorização e localização de objectos móveis, em condições

de ubiquidade e para contextos de grande escala, é uma aproximação realista e eventualmente realizável. É sobre esta hipótese que se concentram também os objectivos da presente dissertação.

Por outro lado, verifica-se também um interesse crescente, na abordagem da investigação recente, na convergência entre RFID e as tecnologias para NFC (*Near Field Communication*), alicerçada pelo suporte de dispositivos equipados com tecnologia NFC no âmbito de redes móveis de 3ª e 4ª gerações. A disponibilidade deste tipo de equipamentos cria oportunidades na exploração dessa convergência em diversos domínios de aplicação [28], [53], [29].

Esta direcção de trabalho, associada à disponibilidade recente dos primeiros telefones equipados com tecnologia de leitura RFID e equipados com sistemas de localização (GPS ou A-GPS), insere-se igualmente na motivação e exploração das hipóteses formuladas na presente dissertação. Nesta linha, é particularmente relevante endereçar arquitecturas de monitorização e localização de objectos RDID a partir de telefones ou PDAs que podem ser usados como estações de monitorização local, numa visão que aponta para uma arquitectura escalável de monitorização permeada em que este tipo de estações desempenham um papel de estações de monitorização ad-hoc (complementando eventualmente o uso de estações convencionais). Neste cenário, pode perspectivar-se um ambiente de localização participativo ou colaborativo, semelhante aos chamados ambientes da área dos sistemas para sensoriamento participativo ou colaborativo (ou *participatory sensing*) [32].

2.6 Segurança de protocolos com RFID e motivação da dissertação

Apesar da capacidade dos dispositivos RFID (nomeadamente os de baixa frequência) ser diminuta, ainda assim é possível aplicar técnicas que permitam aumentar a segurança na utilização dos mesmos em aplicações que tenham requisitos de segurança. Este é um problema actual na adopção de tecnologia actualmente disponível e na investigação do seu desenvolvimento.

Um dos problemas endereçados é a questão da privacidade [59], já que através do identificador incluído no RFID, é possível seguir o rasto do objecto ou obter informação adicional. Outro problema está associado às garantias de autenticidade dos objectos em ambientes menos vigiados ou em que possam verificar-se intrusões, com duplicação, roubo ou possibilidade de contrafacção de identificadores [55], bem como intrusões com captura e substituição de controladores.

Estas dificuldades são particularmente relevantes quando se tem em vista realizar monitorização remota (em média e grande escala) de objectos que se movimentam em áreas geográficas de grande dimensão. Nestes ambientes é necessário simultaneamente providenciar mecanismos necessários à gestão segura de localização de múltiplos destes dispositivos, o que se verifica em cenários como os perspectivados no âmbito da dissertação.

Num sistema de grande escala, os objectos a monitorizar podem estar em zonas fracamente vigiadas (ou não vigiadas de todo), podendo ser alvo de ataques que podem ter implicações graves na quebra das propriedades de segurança acima introduzidas. Mesmo em sistemas críticos de âmbito mais reduzido, as propriedades de segurança são absolutamente fundamentais para a adopção de uma solução baseada em tecnologia de RFID.

Por exemplo, os sistemas RFID possuem uma vasta utilização convencional na área dos sistemas de imobilização. No início dos anos 90 com o aumento do roubo de viaturas, o mercado de segurança para carros, alarmes e sistemas de imobilização tornou-se rapidamente num mercado de referência para utilização da tecnologia. Os alarmes usuais, com alcance de 5 a 20 metros são, na verdade, pequenos transmissores de RFID, que operam habitualmente na frequência de 433.92 MHz, tendo como objectivo accionar a mobilização/imobilização da viatura ou permitir que a ignição possa ser accionada. O problema é que, se o controle que desbloqueia a viatura for quebrado, por envio de um identificador não autenticado, o carro poderá facilmente ser objecto de intrusão por chaves falsas e processo mecânico. Na maior parte dos sistemas de alarme, não há depois forma de o sistema reconhecer se a chave inserida é genuína, permitindo que a utilização de chaves-mestras (ou processos por intrusão física à ignição) ou através do uso de duplicados de emissão do mesmo identificador possa facilmente desligar o alarme e abrir o veículo.

Uma tecnologia de *transponders* autenticados de RFID pode agir com maior eficácia se for utilizado um processo de autenticação mútua envolvendo a chave e um *transponder* (do lado da viatura). Assim, se uma chave não original do carro tentar liga-lo, o carro poderá ser imobilizado, mesmo que o alarme tenha sido desligado e as portas tiverem sido abertas por algum processo mecânico. Se o sistema de *transponders* do lado da viatura for replicado, as garantias de segurança aumentam significativamente, pois tornar-se-á muito difícil ao atacante proceder a algum tipo de operação por desconhecimento de todos os locais onde possam existir réplicas daqueles sensores.

"Mobilização Electrónica Segura" é a designação usual deste tipo de sistemas, nos quais

o sistema de ignição pode ser combinado com um ou mais *transponders*, incorporado directamente no topo de uma chave original do veículo, quando a mesma é inserida na ignição. Garante-se autenticação mútua entre a mesma e os dispositivos de leitura que podem ser vários e estarem instalados em diversos locais da viatura.

Esta tecnologia representa também a evolução de segurança das actuais soluções de detecção e prevenção de veículos, bem como de soluções comercialmente conhecidas por *anti-carjacking*, como são por exemplo as disponibilizadas actualmente por parte de operadores de redes móveis. [1]

2.7 RFID e redes de sensores sem fios como hipóteses para os objectivos da dissertação

Na presente dissertação o objectivo é propor uma arquitectura de segurança (inspirada na figura 2.1), para um sistema de monitorização e localização de objectos autenticados com base em RFID. A figura antecipa a hipótese de convergência de soluções híbridas que podem usar RFID e redes de sensores sem fios, para o fim em vista.

A arquitectura possui ainda pressupostos mais abrangentes de integração ao nível de uma base tecnológica heterogénea, pois pode ser perspectivada para implementação sobre diferentes tecnologias de meios de comunicação.

De acordo com a figura 2.1, os objectos-alvo de monitorização estarão associados a *tags* RFID, comunicando com garantias de autenticação mútua com estações locais de recepção de identificação RFID. Estas estações são responsáveis pela adição de informação geográfica, associada ao local da detecção, bem como pela emissão de certificados autenticados pelos intervenientes na identificação. A informação de localização será obtida com base em coordenadas GPS ou A-GPS, tendo em conta capacidades de processamento para o efeito que estarão instaladas nas estações locais.

[1] Um exemplo deste tipo de sistema operado em Portugal é designado por IMOB e é explorado pela Vodafone Portugal. Numa das opções deste sistema ([15]), uma rede de sensores ZibBee é instalada em várias partes do veículo, podendo ser integrada com actuadores sobre o sistema de ignição e diferentes micro-controladores de diferentes veículos (com adaptadores para diferentes marcas). Os sensores comunicam por rádio frequência com uma estação de sincronização (*sink node*) que opera um *gateway* para a rede GSM. Remotamente é possível ao utilizador enviar comandos (por SMS ou por voz) para obter informações sobre o veículo (posição, direcção de movimento, velocidade, detecção de abertura de portas, etc.), ou enviar comandos de actuação sobre o veículo (bloqueio na próxima paragem, corte de combustível, etc.).

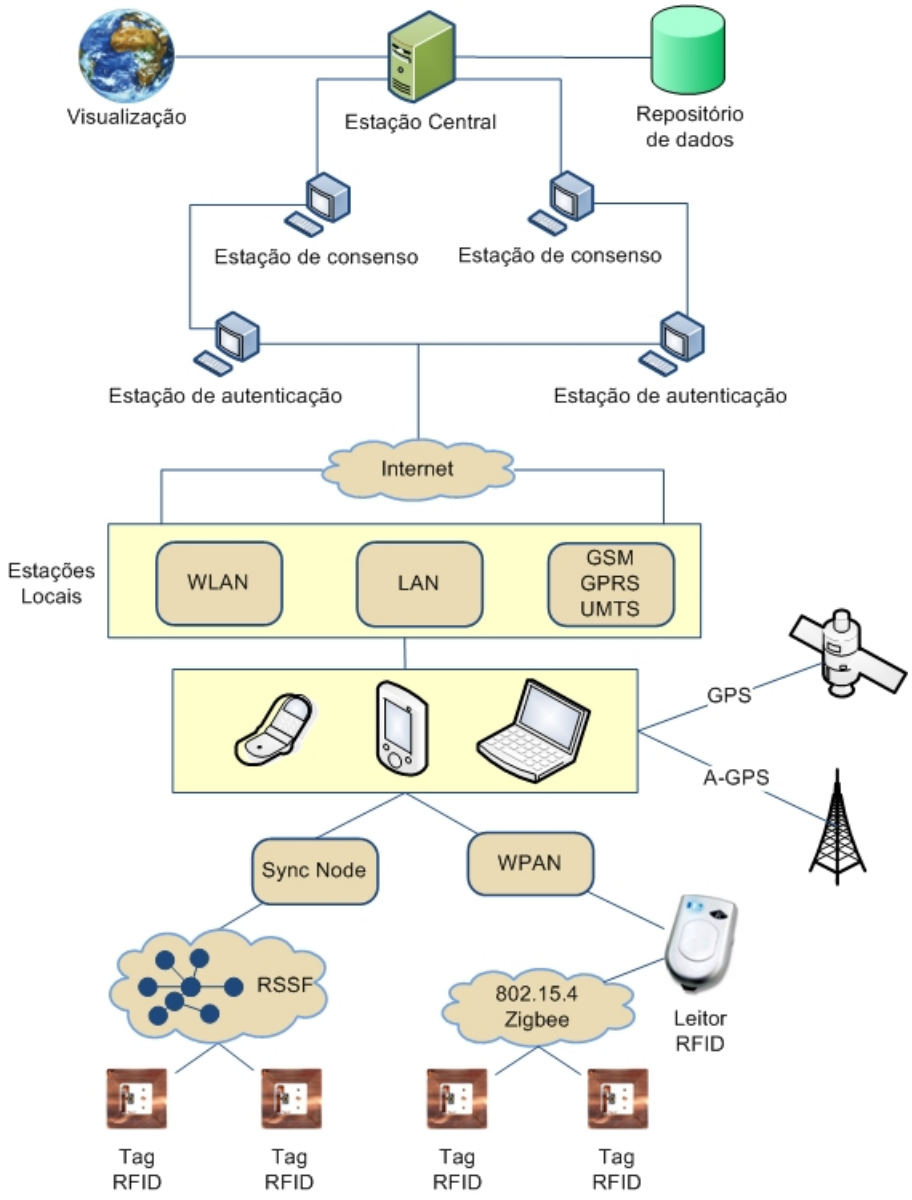

Figura 2.1 Diagrama inicial da arquitectura de referência

As estações locais transmitem os certificados de RFID a uma ou mais centrais intermédias de rastreio remoto, que podem estar agregadas num nível hierárquico de autenticação. A interligação entre as estações locais e intermédias podem incluir tecnologias de redes locais, redes GSM ou a própria rede *internet*. As estações intermédias procedem à autenticação dos alvos, agregação da informação e certificação da localização, emitidas pelas estações locais e

transmitem a informação de processamento para as estações centrais. Estas estações procederão ao processamento, agregação e gestão final dos certificados.

A transmissão remota dos certificados de localização, de objectos identificados e autenticados por RFID, será pois efectuada de forma segura, com base em normas de segurança associadas às tecnologias de rede utilizadas. Deve notar-se que o envio dos certificados poderá fazer-se de forma redundante, por mais do que uma estação local e com base na transmissão por mais do que uma tecnologia de rede de ligação, o que pode aumentar o nível de resiliência e tolerância a intrusões por parte do sistema. Por outro lado, pretendem-se garantir condições de segurança, numa perspectiva extremo-a-extremo, no que diz respeito a garantias associadas às propriedades de autenticação, confidencialidade, privacidade e integridade dos certificados de localização, transmitidos pelas estações locais.

A autenticação mútua entre *tags* RFID e as estações locais de monitorização será feita, com base em tecnologias baseadas em redes WPAN (*Wireless Personal-Area Networks*), podendo usar-se Bluetooth [4] operando em modo com segurança ou redes de sensores (com base nas normas IEEE802.15.4 [1] e/ou Zigbee [9]), operando como pequenas ilhas redundantes de detecção e localização de objectos RFID. A privacidade da informação contida ou transmitida pelas *tags* às estações centrais, encontra-se contemplada no processo de autenticação, efectuado pelas estações intermédias, que estão interligadas às estações locais.

No contexto da dissertação, os sensores poderão conter informação de localização autocontida (ou pré-configurada), pelo que se supõe a utilização de pequenas RSSF (redes de sensores sem fios) operando em modo de comunicação por difusão. Estas redes, sendo compostas por sensores (do tipo MicaMotes [6], TelosMotes [8], Sun SPOT [7]), que se integração na arquitectura através de nós especiais funcionando como *gateways* IEEE 802.15.4 ou ZigBee e WLAN, para pré-processamento e agregação local de informação (através de *sink nodes* com capacidades para agregação das localizações detectadas pelos sensores). Num contexto de mobilidade da rede de sensores, a informação de localização é fornecida aos sensores através da estação local.

O pré-processamento da localização de *tags* RFID e inserção da informação de localização e emissão de certificados, far-se-á com garantias de prevenção e resistência a intrusões, contra potenciais ataques aleatórios que possam realizar-se aos sistemas que implementam as estações locais. Estas defesas utilizarão replicação do processamento de detecção e localização

dos objectos a monitorizar, com base em mais do que uma estação local e através de mecanismos e protocolos de consenso probabilístico [27], [33]. As estações intermédias que realizam o consenso, encontram-se interligadas a estações de autenticação, recebendo certificados de localização autenticados por essas estações.

Para resistir a ataques de localização, a dissertação proporá mecanismos e protocolos adaptados a ambientes com diferentes recursos computacionais e capazes de resistirem a falhas assíncronas de estações locais ou operando incorrectamente como resultado de intrusões. Como se sabe, ataques arbitrários (de acordo com um modelo de adversário bizantino) podem ser realizados em F estações de controlo, desde que garantido o funcionamento correcto e o anúncio de localizações correctas por parte de 2F+1 dessas estações (pressupondo falhas arbitrárias sem ser por omissão, numa janela de sincronismo virtual temporizada e estabelecida centralmente pelo nó de rastreio). Para inclusão destas garantias, as estações deverão ser constituídas por dispositivos de baixo custo, de modo a poderem ser facilmente replicadas e combinadas em ilhas de estações locais de monitorização. A utilização de tecnologia de redes de sensores é particularmente interessante para criar este efeito.

As contribuições objectivadas pela dissertação e que foram introduzidas no capítulo 1, a partir da anterior arquitectura de referência, situam-se pois a diversos níveis, destacando-se as seguintes:

- Concepção, implementação e validação da arquitectura a partir da anterior arquitectura e cenário de referência, com base num protótipo de um sistema de monitorização de localização de objectos móveis, autenticados com base em RFID.

- Proposta de um protocolo de autenticação mútua com base em criptografia assimétrica leve (ECC), RSA ou apenas criptografia simétrica, entre dispositivos RFID e estações locais que emitem os respectivos certificados de localização, nomeadamente leitores e *tags* RFID. Apesar de existirem protocolos de autenticação que podem inspirar a contribuição [20], são trabalhos preliminares de investigação que não foram integrados e validados numa arquitectura e num sistema real, como o que foi realizado no âmbito da presente dissertação.

  A combinação do protocolo de autenticação mútua com o pré-processamento e emissão de certificados de localização ao nível das estações de monitorização, é um aspecto de concepção, desenvolvimento e aplicação com originalidade própria. Tanto quanto se julga saber, a aproximação que combina autenticação mútua de identidades e localizações com

RFID no âmbito de protocolos de consenso com características baseadas em aleatoriedade e mecanismos de resistência probabilística a intrusões ou falhas das estações de monitorização, apresenta um teor de inovação para aumentar o nível de resistência do sistema, face a ataques arbitrários de omissão ou anúncio de falsas localizações de objectos monitorizados.

- Combinação da contribuição anterior, numa arquitectura de *internetworking* (para interligação entre as estações locais de monitorização e estações de rastreio remoto de objectos RFID) assegurando propriedades de autenticação, confidencialidade, integridade, numa perspectiva extremo-a-extremo.

- Implementação e avaliação experimental da arquitectura proposta, que será integrada num sistema de gestão e monitorização remota de trajectórias de objectos autenticados com RFID, sendo este sistema demonstrado por uma aplicação de demonstração GIS com integração de suporte de visualização, com base no sistema Google Maps e coordenadas GPS obtidas de estações locais de monitorização.

3 . Trabalho relacionado

As secções do trabalho relacionado que serão apresentadas de seguida estão organizadas do seguinte modo: as secções 3.1 a 3.3 contêm uma descrição geral sobre tecnologias de redes de área global, redes locais e redes de área pessoal (ou PAN - *Personal Area Networks*), nomeadamente em relação às propriedades de segurança, tratando-se de tecnologias que podem ser usadas na arquitectura de referência apresentada no capítulo 2. No contexto da dissertação as secções 3.1 e 3.2 constituem apenas informação complementar associada à possibilidade de utilização dessas tecnologias na instanciação da arquitectura inicialmente apresentada como referência no capítulo 2 - secção 2.7.

Na secção 3.4 apresenta-se a problemática mais directamente associada ao contexto dos objectivos da dissertação, no que diz respeito à segurança em sistemas RFID. Destaca-se a problemática da privacidade e a proposta de protocolos de autenticação leves, representativos da investigação em segurança de sistemas RFID, que utilizam criptografia simétrica e criptografia assimétrica de curva elíptica. Na secção 3.5 apresentam-se duas arquitecturas para monitorização (ou *tracking*) de objectos, que inspiram a abordagem e objectivos previstos na dissertação. Estas arquitecturas são discutidas na secção 3.6, com base numa análise crítica e comparativa, em relação aos objectivos e contribuições previstas para a presente dissertação.

3.1 Segurança em redes de área global

3.1.1 Segurança em redes GSM, GPRS, 3G

3.1.1.1 Redes GSM e GPRS

As redes GSM [17] permitem hoje suportar um número muito elevado de utilizadores e apresentam boas condições de conectividade em muito grande escala. Estão preparadas para responder aos requisitos de mobilidade dos utilizadores, assegurando conectividade na maioria das situações de mobilidade.

Numa rede GSM operam entidades e dispositivos com funções variadas. Na terminologia normalizada de uma rede GSM os dispositivos móveis (MS - *Mobile Station*) comunicam com a rede, através de uma estação base (BS - *Base Station*). Um MS contêm um *smart card*, denominado por SIM (*Subscriber Identity Module*), que tem a função de não expor no MS a

informação e processamento criptográfico de segurança para comunicação de forma segura na rede. Este cartão, guarda uma chave de autenticação, apenas conhecida por um Centro de Autenticação (AuC ou *Authentication center*) [76] e um identificador internacional de identidade de subscritor (IMSI - *International Mobile Subscriber Identity*). Este identificador possui informação sobre o país e o operador da rede. O AuC tem a função de guardar as chaves secretas (K_i) partilhadas com os dispositivos MS e enviam desafios para autenticar os dispositivos MS, com base em processos criptográficos de informação que incluem protocolos de desafio/resposta, envolvendo números únicos gerados aleatoriamente pelo AuC (ou *NONCEs - Numbers Used Once*).

Os mecanismos de segurança utilizados asseguram autenticação unilateral do MS sendo esta efectuada entre o MS e o AuC. O BS actua como intermediário das mensagens. São utilizados algoritmos de cifra em cadeia (que têm sido normalizados pelo consórcio de normalização GSM). Nas redes actuais preponderam os algoritmos A3, A5, séries 1 ou 2 (hoje considerados potencialmente fracos, com base na literatura abundante sobre suas vulnerabilidades e ataques por criptanálise) e a variante 3 (que tem sido introduzida a partir das redes de 3ª geração ou 3G) bem como A8. O algoritmo A5/3 é uma variante de um algoritmo em cadeia obtido pela geração de uma cadeia pseudo-aleatória, com base num algoritmo de blocos denominado por KATSUMI, que usa uma chave de 128 bits e operando sobre blocos de 64 bits. O algoritmo A5/3 mais amplamente utilizado baseia-se na especificação definida pelo consórcio 3GPP [10]. O algoritmo A8 é um algoritmo de geração de chaves de sessão para A5, a partir de sementes iniciais (aleatórias e de uma chave inicial K_i de 128 bits, também conhecida por chave inicial de subscritor) usada como segredo de longa duração, partilhado entre o MS e o AuC.

Em traços gerais, a autenticação consiste na resposta a um desafio por parte do MS. O AuC envia um número aleatório como desafio e o MS deve cifrar esse número com dois diferentes algoritmos. Com base no desafio, o MS calcula uma resposta que é a cifra do desafio com A3 e a chave K_i e em paralelo calcula a cifra do número aleatório com o algoritmo A8. A primeira cifra é enviada ao AuC e a segunda é usada como chave de sessão para o algoritmo A5/3 garantindo confidencialidade na sessão.

Em relação aos mecanismos de utilização de cifra nas mensagens, é pois utilizado o algoritmo simétrico em cadeia A8 como gerador de chaves para produzir uma chave de sessão com 64 bits nos algoritmos A5 de variantes 2 e 3 ou de 128 bits na variante 3, tendo como pressuposto a existência da chave inicial K_i partilhada entre o MS e o AuC. Não obstante a utilização

de mecanismos de segurança, as redes GSM podem ser alvo de inúmeros ataques, estando alguns localizados ao nível da BS ou dos mecanismos de segurança (nomeadamente com alguns resultados de ataques com sucesso por criptanálise ao algoritmo A8 ou A5/3, e que apareceram descritos ultimamente na literatura da especialidade [40]).

Independentemente de condições de ataques de criptanálise, o processo de autenticação usado nas redes GSM apresenta ele próprio possíveis falhas relacionadas com o envio da resposta ao desafio pelo MS para a BS. Caso o atacante consiga recolher um elevado número de mensagens (da ordem de 160000 nos dados actualmente disponíveis), então consegue ter acesso à chave K_i e, neste momento, os mecanismos de segurança ficam comprometidos [76].

Para o processo de geração da chave de sessão K_c é utilizado o algoritmo A8, mas este na sua génese apresenta vulnerabilidades que podem comprometer a chave criada por ele. Este algoritmo baseia-se num algoritmo conhecido por COMP-128, gerando chaves de 64 ou 128 bits a partir de uma semente de até 128 bits. No caso das primeiras variantes usadas dos algoritmos A3 e A5, as chaves eram de 64 bits e em A5/3 podem ser usadas chaves de 64 bits por imposições legais na legislação vigente. A geração do algoritmo A8 fornece neste caso uma chave de sessão de 128 bits (sendo a geração processada no módulo SIM). Os 54 bits mais significativos desta chave são então extraídos, sendo adicionados 10 bits com valor "0", sendo este resultado usado como chave de sessão. Daqui resulta uma fragilidade iminente do processo, face ao número de bits da chave, se o atacante puder dispor de meios computacionais convenientes, comparativamente às capacidades computacionais dos dispositivos habitualmente usados como MS.

A comunicação com A5 pode também ser atacada se o atacante tiver ao seu dispor uma base de dados prévia com os estados do algoritmo e as *streams* correspondentes. Nessa situação é possível que este capture as mensagens enviadas por rádio e procure uma correspondência com a informação na base de dados. Caso esta propriedade se verifique, o estado do algoritmo é capturado e a partir desde momento o atacante consegue obter K_c [76].

Na normalização GSM as mensagens enviadas entre as partes não contemplam mecanismos de integridade, logo podem chegar danificadas ao destino sem que este tome conhecimento do sucedido, quer tenha ocorrido de forma acidental ou não. Esta rede pode por isso sofrer diversos ataques de DoS, por exemplo, a capacidade de desactivar uma célula GSM ou a alocação de

recursos sem ser necessária autenticação, por parte de um agente malicioso [25].

3.1.1.2 Redes 3G

As redes 3G [17] são uma evolução das redes 2G e propõem resolver as limitações do GSM, apesar da segurança se basear neste. Uma rede 3G contempla mecanismos de autenticação, confidencialidade e mecanismos de cifra. Foram propostas diversas alterações que se enquadram no reforço ou introdução de mecanismos de segurança. A autenticação passou a ser bidireccional entre a BS e o MS, de acordo com uma chave de cifra e de integridade que expiram após um tempo específico. A normalização 3G previu a introdução de mecanismos para controlo de integridade no terminal, mecanismo denominado por IMEI (*International Mobile Equipment Identity*) e a inclusão de números de sequência para impedir ataques de falsas BS. Assim, o MS e o AuC possuem dois números de sequência que são incrementados e sincronizados em cada autenticação. O MS inicia o processo de autenticação exigindo a autenticação do AuC e, como resultado do protocolo de autenticação mútua, o MS autentica-se igualmente perante o AuC.

Outra das alterações consiste no aumento do tamanho da chave utilizada, de modo a possibilitar a utilização futura de algoritmos criptográficos mais robustos. Por último, foram efectuadas modificações dentro da rede com a introdução de novos mecanismos de segurança e com a protecção das ligações entre a BS e o núcleo da rede.

3.1.2 Segurança na pilha TCP/IP

3.1.2.1 SSL

O SSL e TLS [79],[38] constituem o protocolo mais representativo e utilizado da pilha de segurança em TCP/IP. Foi concebido com o intuito de garantir segurança entre servidores e clientes *Web* através do estabelecimento de sessões seguras entre as partes e do estabelecimento de um canal de transporte seguro de mensagens para interacção cliente/servidor. Contudo, assegura serviços genéricos de autenticação de *endpoints* de comunicação (endereços IP ou DNS *Fully Qualified Names*, confidencialidade, integridade e controlo de sequenciamento de segmentos ou SSL *records*, na perspectiva de um transporte seguro baseado em *sockets* SSL/TCP/IP) e parâmetros autenticados que foram uma associação de segurança do nível sessão (e que estabelecem em SSL o contexto de nível de sessão segura). O SSL é de facto constituído por 4 sub-protocolos organizados em camadas que asseguram autenticação das entidades principais

de designação com base em certificados X509 [48], integridade, confidencialidade e autenticação dos fluxos de dados que decorrem nas sessões, tendo em vista a protecção do contexto de interacção cliente/servidor, de adversários que actuem na rede com base num modelo de adversário do tipo Dolev-Yao [39], ou que possa desencadear todas as tipologias de ataques caracterizados nas *frameworks* de segurança OSI X.800 [78] ou IETF RFC 2828 [75].

O SSL ou o TLS (que possuem entre si pequenas diferenças na sua normalização e de acordo com as suas variantes de versão) são amplamente conhecidos e estabelecidos no domínio da segurança na rede *Internet* e na pilha TCP/IP. Dada a enorme disponibilidade de bibliografia que cobre em maior ou menor detalhe a normalização e o funcionamento destes protocolos e dado que a sua utilização no âmbito da arquitectura anteriormente apresentada na secção 2.7 se faz de acordo com os moldes habituais, escusamo-nos de entrar em maior detalhe na descrição das propriedades, mecanismos e serviços de segurança associados à utilização de SSL ou TLS.

3.1.2.2 IPSec

O IPSec [80] situa-se ao nível da protecção da camada IP e pretende prevenir o acesso ao fluxo de datagramas encaminhados numa estrutura de *internetworking* com TCP/IP, por parte de um atacante que actua com acesso ao canal de dados (nível *data-link*). O IPSec, tal como o SSL, não é na verdade um único protocolo, mas sim uma pilha de sub-protocolos dentro da pilha TCP/IP. Pretende garantir autenticação de *endpoints* IP e assegura ainda confidencialidade, integridade de datagramas trocados entre *endpoints* IP. O IPSec possui ainda mecanismos para gestão e estabelecimento de chaves ponto-a-ponto, em diversas opções e variantes. A incidência das contra-medidas do protocolo IPSec actua sobre as hipóteses de adversários do tipo Dolev-Yao [39], de acordo com a tipologia de ataques às comunicações numa rede TCP/IP e conforme definidos nas *frameworks* OSI X.800 [78] ou IETF RFC 2828 [75].

A normalização e a bibliografia disponível que cobre em maior ou menor detalhe a normalização e o funcionamento da sub-pilha IPSec na pilha TCP/IP é extensa e bem conhecida. Dado que a possível adopção do suporte IPSec na arquitectura anteriormente apresentada na secção 2.7 se faz de acordo com os moldes habituais, escusamo-nos de entrar em maior detalhe na descrição das suas propriedades, sub-protocolos, mecanismos ou serviços opcionais de segurança.

3.1.3 Sumário

As redes GSM (nas suas diversas gerações) possibilitam um elevado nível de conectividade, pois estão presentes como uma infra-estrutura global de comunicações abrangente. Contudo, a sua utilização como infra-estrutura de suporte a necessidades de segurança extremo-a-extremo, por parte de aplicações, pode apresentar algumas fraquezas, sendo a principal, a autenticação unilateral por parte do dispositivo móvel, as vulnerabilidades induzidas por deficiência de autenticação de MS devido a limitações nos processos criptográficos existentes, sendo a confiança da utilização destas infra-estruturas fortemente dependente da base de confiança estabelecida pelo operador. A utilização de redes 3G atenua algumas das fraquezas do GSM (ao nível de propriedades de autenticação e integridade).

Relativamente à rede *internet*, o IPSec e o SSL constituem, do ponto de vista das comunicações, os protocolos de referência de segurança na pilha TCP/IP. A escolha de IPSec ou SSL para construção de uma arquitectura de comunicação segura, suportada em ambiente *internet* depende, sobretudo, da disponibilidade das duas pilhas nos equipamentos a utilizar, o que não constitui um problema para os computadores usuais, mas pode constituir um problema em dispositivos específicos (como por exemplo, telemóveis ou estações de monitorização com RFID). Depende ainda da disponibilidade ao nível da infra-estrutura de ligação. No caso da utilização de rede *internet* através de ISPs, só será possível a utilização generalizada de IPSec no modo túnel, podendo o core de uma solução de conectividade segura para a arquitectura de referência inicialmente apresentada no capítulo 1 ser constituída pelo estabelecimento de redes privadas virtuais seguras (ou *Secure* VPNs) entre as estações locais de monitorização e as estações centrais de rastreio.

No entanto, este tipo de implementação não está disponível ao nível de dispositivos vulgarmente usados para a construção de redes locais de monitorização. Neste contexto de utilização, a adesão da pilha SSL ou TLS pode apresentar diferentes vantagens sobre a solução IPSec, uma vez que podem ser mais facilmente usados como ambiente de segurança de maior disponibilidade ao nível transporte e sessão, para suporte de aplicações sobre a pilha TCP/IP.

Mais importante é referir que o modelo de adversário subjacente quer aos protocolos TLS ou SSL, quer à pilha IPSec não abrange contra-medidas face a ataques por intrusão ao nível

dos nós de processamento das redes. A simples utilização desses mesmos protocolos no âmbito de um sistema como o referenciado na arquitectura avançada na secção 2.7, mesmo nas suas configurações ou parametrizações mais robustas do ponto de vista de segurança, não protegem o sistema global de ataques que possam ser realizados aos nós de processamento da arquitectura, nomeadamente por intrusão às estações locais de localização ou estações intermédias onde possa haver processamento ou agregação de dados. Por outro lado, as soluções com SSL (ou TLS) bem como com IPSec, dependendo das opções de uso, podem revelar-se inadequadas pela exigência que colocam na gestão de infra-estruturas de certificação com chaves públicas (do tipo PKI - ou *Public Key Infrastructures*), o que não parece adequado para a utilização de dispositivos ad-hoc, que possam ser usados como estações de localização de alvos num ambiente pervasivo de localização com sensoriamento participativo ou colaborativo (ou *participatory-sensing environment*).

3.2 Segurança em redes de área local sem fios

As redes locais encontram-se em apartamentos, escritórios ou em espaços institucionais amplos, podendo ainda cobrir espaços públicos de maior ou menor dimensão. Têm um alcance de cerca de 100 metros por cada estação base e quando usadas em redes estruturadas, embora também possam ser usadas em topologias P2P (sem estrutura) ou em topologias mais extensas, através da hierarquização e interligação de estações de acesso (vulgarmente designados por *Access Points*). Existem protocolos que providenciam segurança nestas redes. Serão analisados os protocolos *Wireless Equivalent Privacy* (WEP), WPA e RSN, assim como a pilha 802.11i e o standard 802.1x.

3.2.1 WEP

O protocolo WEP [18] foi criado com o intuito de oferecer alguma segurança às redes locais sem fios, assim como, ser aplicável em dispositivos com pouco poder de processamento, oferecendo todavia o mesmo desempenho que a rede Ethernet usada sem qualquer protecção de dados. Este protocolo, na sua génese, apresenta diversas falhas que podem ser exploras por um atacante. Por este motivo, posteriormente foram introduzidos os protocolos WPA e mais tarde o RSN.

As características gerais do protocolo WEP são a razoável segurança apresentada (embora

sejam bem conhecidas e amplamente divulgadas diversas formas de quebrar a sua protecção), sincronização automática, pois as estações sem fios sincronizam-se com os pontos de acesso (AP ou *Access Points*) sem intervenção humana.

Para a utilização da cifra, é utilizado o protocolo RC4 com chaves de 40 bits, mais 24 bits para o vector de inicialização (IV). Contudo, alguns fabricantes utilizam chaves maiores, por exemplo 104, 232 bits. Existe um processo de autenticação na rede, porém, apenas válido para a estação móvel. O código de integridade utilizado é o CRC-32, um método reconhecidamente frágil do ponto de vista de ataques simples por colisões o que possibilita que um atacante modifique a mensagem e altere o correspondente código, de modo a que o receptor não se aperceba da alteração. Isto acontece, pois o CRC-32 não foi criado para propósitos de segurança, devendo para isso serem utilizadas funções de síntese segura de dados (ou *secure hashing*).

Uma versão mais robusta do protocolo WEP pode usar chaves de 128 bits, o que reduz significativamente as possibilidades de ataques por força bruta ou por análise de padrões texto conhecido-cifra. Deve notar-se que no âmbito da utilização do protocolo, muita da informação de texto (cabeçalhos das mensagens nas tramas que transportam os datagramas de dados) podem ser facilmente conhecidos pelo atacante ou podem ser por ele facilmente deduzidos.

O protocolo WEP não dispõe de refrescamento de chaves, pois a mesma chave é utilizada para cifrar e decifrar as mensagens, assim como durante a ligação da estação à rede. Está presente uma limitação de utilização de 4 chaves na rede portanto, podem existir estações móveis a utilizar a mesma chave no mesmo instante. Este aspecto facilita a obtenção da chave por parte de um atacante.

A utilização de um vector de inicialização com 24 bits também contribui para as fraquezas da utilização do algoritmo RC4 no contexto do protocolo WEP, já que não se encontra especificado como este deve ser actualizado. Regra geral, as implementações usuais incrementam o valor do vector de inicialização em cada pacote, mas como têm apenas 24 bits, num curto espaço de tempo dá-se a reutilização do valor do mesmo. De entre os valores possíveis para IVs, existem alguns que não são adequados, pois expõem bits do texto em claro ao atacante. Como este protocolo não apresenta mecanismos de detecção e prevenção de reprodução ilícita de mensagens (ou *anti-replaying*), o atacante pode personificar com maior ou menor facilidade a estação móvel, enviando os pacotes que capturou novamente para o AP. Caso as mensagens sejam importantes, esta falha pode ser preocupante.

3.2.2 WPA

Com o objectivo de colmatar as falhas do protocolo WEP foi proposto e normalizado o protocolo WPA [18], que está em concordância com uma parte da norma 802.11i. O WPA melhorou de forma significativa a segurança fornecida pela WEP e é compatível com o *hardware* existente, o que facilita a sua utilização de forma generalizada. As chaves utilizadas são de 128 bits e geradas de forma aleatória por um protocolo denominado por *Temporal Key Integrity Protocol* (TKIP) [64].

3.2.3 Pilha 802.11i

O grupo de trabalho 802.11i [18] foi criado para endereçar os problemas de segurança do protocolo WEP. Providencia duas camadas, uma para cifra e outra para controlo de acesso. A primeira camada suporta dois protocolos, TKIP para equipamento legado e CCMP para equipamento futuro. O protocolo TKIP garante protecção contra colisões, chaves fracas e ataques por reprodução ilícita de mensagens (ou *message replaying*). É constituído essencialmente por um protocolo de teste de integridade de mensagens (MIC ou *Message Integrity Test*), de sequência de vectores de inicialização, e uma nova construção de pacotes com inclusão do TKIP *Sequence Counter* (TSC) para protecção contra *replaying*.

O WPA, tal como foi referido, apresenta diversas melhorias, mas como à data não abrangia totalmente o futuro standard 802.11i, foi criado o protocolo RSN, vulgarmente denominado por WPA2 [30]. Este protocolo exibe semelhanças com o WPA, mas acrescenta algumas novidades como a negociação dinâmica de autenticação e algoritmos de cifra entre AP e dispositivos móveis, assim como autenticação baseada em 802.1x ou EAP [16]. A desvantagem da sua utilização é a necessidade, em alguns casos, de actualização no *hardware* dos clientes ou dos APs.

O standard 802.1x, para além da autenticação também garante um mecanismo de distribuição de chaves, estando desenhado para redes com e sem fios. Fornece uma *framework*, na qual podem ser utilizados diversos protocolos de autenticação. A comunicação neste standard é efectuada entre diferentes entidades principais: o *supplicant*, *authenticator* e o *authentication server* (AS). O *supplicant* é a entidade que executa o pedido de acesso ao *authenticator*. Este, actua como ponto de segurança do sistema encaminhando os pedidos de acesso do *supplicant* para o AS. Por fim, o AS decide com base nas credenciais apresentadas pelo *supplicant*, se este

pode ter acesso aos serviços fornecidos pelo *authenticator*.

Um conceito importante que se relaciona com estas entidades é a noção de porta, que consiste num meio de controlo de acesso, definido pelo *authenticator*. Inicialmente, quando o *supplicant* deseja comunicar com o *authenticator* a porta encontra-se no estado "não autorizado", podendo apenas comunicar com o AS. No momento em que as credenciais exibidas pelo *supplicant* são aceites, a porta passa ao estado "autorizado" e o *supplicant* passa a ter acesso aos serviços fornecidos pelo *authenticator*.

3.2.4 Sumário

Tal como apresentado na secção anterior, o protocolo WEP apresenta inúmeros problemas que o tornam bastante vulnerável face a um atacante. A introdução do WPA e mais recentemente do WPA2, vieram colmatar essas falhas. No contexto da arquitectura que se irá implementar, a utilização do WEP é desaconselhada (como já o é actualmente nas configurações mais robustas de segurança de redes 802.11), já que introduz inúmeros factores de risco no sistema e pode fazer com que toda a segurança aplicada se torne inútil, pois um atacante ao quebrar a protecção oferecida pela WEP, consegue o acesso aos dados que transitam na rede.

Para elevar o nível de confiança aconselha-se a utilização de WPA2 [30], ou no mínimo WPA, pois apesar de apresentar ainda possíveis vulnerabilidades que podem ser utilizadas por um atacante, apresentam um nível de confiança francamente superior ao WEP (mesmo quando este use chaves de 128 bits). Por outro lado, pelas suas características intrínsecas, todos os protocolos referidos apenas visam protecção das comunicações, pelo que se manterá a problemática de ataques complementares por intrusão ao nível dos equipamentos que utilizem estes protocolos.

3.3 Segurança em redes de área pessoal

3.3.1 Bluetooth

As redes Bluetooth [4] procuram oferecer conectividade via rádio a nós que se encontram relativamente próximos. É um protocolo standard para redes WPANs que contém na sua implementação mecanismos de segurança para garantir autenticação e confidencialidade. Na sua

implementação existem três classes (1,2,3) que suportam alcances de 100, 10 e 1 metro, respectivamente. Funciona na frequência de 2.4GHz e utiliza 79 canais entre o intervalo de frequências [2.402GHz, 2.480GHz], através de um algoritmo de varrimento do espectro que se designa por *fast-frequency-hopping*.

Esta rede apresenta nós com características distintas cujo funcionamento é importante realçar. De forma geral, os nós têm um comportamento de mestre (*master*) ou escravo (*slave*), podendo este último funcionar em diferentes modos. Cada nó é identificado pelo endereço do dispositivo, com 48 bits. Relativamente à rede, existe no Bluetooth dois conceitos de funcionamento, estabelecidos por configurações *piconet* ou *scatternet*. Numa rede *piconet* apenas existe um nó mestre, sendo os restantes nós escravos. É a menor colecção de nós ligados construída de forma dinâmica e suporta até 8 dispositivos. Caso o nó mestre da rede *piconet* tenha a função de escravo em outra rede *piconet*, então estamos da presença de uma rede *scatternet*.

Tal como se introduziu anteriormente, os nós da rede podem funcionar em diferentes modos: modo activo (ou *active mode*), modo de espera (ou modo *standby*), modo de bloqueio (ou modo *hold*), modo *park* e modo *sniff*. O nó mestre determina o salto de frequência (*frequency-hopping*) e pode retirar ou colocar nós no modo *park* ou *hold*.

Quanto à segurança, uma rede bluetooth apresenta vários modos opcionais de funcionamento. O primeiro modo é conhecido por modo inseguro (ou *Non-Secure*), não utilizando quaisquer mecanismos de segurança. O segundo modo, denominado por SLES (ou *Service-Level Enforced Security*) permite acesso a um serviço mediante um mecanismo de controlo de acessos estabelecido por uma lista de controlo de acessos que estabelece autorizações para tuplos (endereço do nó, chave, serviço). Por último, o modo LLES (ou *Link-Level Enforced Security*), requer autenticação e autorização. Este protocolo utiliza quatro chaves no seu funcionamento [19].

A primeira chave, denominada por chave de inicialização (ou *Initialization Key*) é gerada através de um PIN inserido (usado como semente de geração da chave) e é utilizada quando não existem outras chaves designadas por chaves de unidade (*Unit Key*) ou chaves de combinação (*Combination Key*). A chave de unidade, caso exista, está guardada em memória estável e regra geral é inalterável. A chave de combinação é gerada para cada par de dispositivos. Por fim, a chave mestra (ou *Master Key*) é uma chave temporária ou de curta duração. O processo de geração das chaves acima descritas, é realizada através de diversos algoritmos publicados e

normalizados, como o E21 ou E22.

Neste protocolo também está presente o processo de autenticação, realizado em traços gerais como resposta a um desafio lançado pelo dispositivo autenticador. Tal como referido atrás, a *Combination Key* utiliza PINs para geração da chave, mas como estes segredos são introduzidos pelo utilizador, abre um problema de usabilidade, visto que os PINs introduzidos são de pequena dimensão e geram assim chaves fracas. Este protocolo é maioritariamente utilizado por dispositivos em movimento, contudo as chaves utilizadas apenas se referem ao dispositivo em si, logo se o dispositivo for furtado o atacante consegue ter acesso aos recursos disponíveis ao dispositivo.

Como o processamento de muitos destes dispositivos é limitado, os algoritmos de cifra utilizados são poucos robustos.

3.3.2 802.15.4

As redes 802.15.4 [1], conhecidas por redes de área pessoal de baixa taxa de transferência (ou *Low-Rate* WPAN), têm como objectivo providenciar conexão entre dispositivos de baixo custo, comunicação sem fios e curto alcance de comunicação (entre 10 e 50 metros). A frequência de transmissão é de 2.4GHz (excepto na Europa e América do Norte), logo semelhante ao espectro de funcionamento das redes Bluetooth (ver secção 3.3.1) e 802.11 (ver secção 3.2, e como tal é necessário prever a existência de interferências quando estas redes coexistem.

As redes 802.15.4 são utilizadas em diversos sectores da indústria e conheceram uma enorme divulgação no âmbito da investigação e emergência das redes de sensores sem fios e suas aplicações. Este protocolo foi pensado para dispositivos de processamento que possam ser miniaturizados, de baixo custo e funcionando com autonomia energética, o que limita os recursos de processamento, de alcance e velocidade de comunicação, devendo ser concebidos para baixo consumo energético.

Em comparação com o protocolo Bluetooth, os dispositivos 802.15.4 apresentam assim um tamanho e custo muito inferior, apresentam consumos de energia e taxa de transferência de dados mais reduzidas. Ao contrário das redes Bluetooth, as redes 802.15.4 apresentam várias topologias, como estrela, malha ou anel e podem permitir a utilização de um grande número de dispositivos que podem formar redes auto-organizadas.

A normalização 802.15.4 implementa as duas primeiras camadas do protocolo: camada física (PHY) e camada de acesso ao meio para ligação de dados (MAC ou *Medium Access Control*), deixando o restante da implementação de uma pilha de comunicação, para protocolos orientados para aplicações específicas. Por isso se diz muitas vezes que as redes 802.15.4 são redes para aplicações específicas.

As tramas incluem um cabeçalho de sincronização (ou *Synchronization Header*) para sincronização do receptor com o transmissor, um cabeçalho de controlo e uma carga de dados (*payload*) que contém o pacote MAC.

A camada MAC [66] utiliza dois modos de acesso: *slotted* CSMA para redes estruturadas e coordenadas em estrela e *unslotted* CSMA/CA para redes P2P, formadas de forma auto-organizada e com coordenação probabilística e autónoma de acesso ao meio.

Apesar dos dispositivos a que se destina este protocolo, existem mecanismos de segurança contemplados na especificação do mesmo. Este protocolo permite garantir confidencialidade e autenticação. Para tal, disponibiliza *suites* de segurança que permitem a configuração das propriedades segurança desejadas. Como os dispositivos podem necessitar de comunicar com segurança para outros, torna-se necessário que as propriedades de segurança tenham em conta o destinatário das mensagens. Como implementação desta propriedade são utilizadas entradas para listas de controlo de acessos (ACL) [73] que contêm, de entre outras informações, a *suite* de segurança e a chave utilizada para um determinado dispositivo, possibilitando a troca confidencial de mensagens par-a-par, desde que se estabeleçam também chaves partilhadas par-a-par.

Numa rede 802.15.4 existem assim chaves partilhadas na rede, podendo estas serem partilhadas entre dois nós, por um conjunto de nós ou por todos os nós da rede, podendo também coexistir esquemas híbridos numa mesma rede.

Este protocolo apresenta alguns problemas de segurança, estando a maioria centrados em questões energéticas (por serem redes facilmente atacadas do ponto de vista de negação de serviço ao nível MAC) e problemática da distribuição e gestão de chaves. Relativamente à primeira questão é ainda necessário garantir que a ACL é mantida em caso de falha de energia, pois se isto não se verificar toda a informação de segurança nela contida perde-se.

Como vimos anteriormente, as entradas ACL não apresentam a flexibilidade das chaves utilizadas e isso coloca alguns problemas de segurança relacionados principalmente com a gestão de protocolos de desafio/resposta e utilização de *nonces*. No caso de utilização de chaves de

grupo é necessário colocar essa chave em todas as entradas para os destinatários do grupo, embora depois a gestão dos *nonces* se possa tornar complexa e ser ocupado imenso espaço a criar e guardar todas as entradas.

Caso o destinatário não esteja em nenhuma entrada ACL a chave de rede é utilizada por defeito, mas não oferece gestão contra *replaying*, pois não é possível convergir os *nonces* para todos os participantes na mesma.

3.3.3 Zigbee

O Zigbee é a especificação de um protocolo com várias camadas criado e mantido pela Zigbee Alliance [9]. Baseia-se no standard 802.15.4 para redes WPAN (aos níveis físico e ligação de dados) e a norma está vocacionada para redes malhadas (ou de estrutura em *mesh*). A última especificação data de 2007 e contêm dois perfis, *stack profile* 1 e *stack profile* 2, usualmente denominados por Zigbee e ZigBee Pro, respectivamente.

O primeiro, destina-se a uma utilização caseira e comercial. O segundo, acrescenta funcionalidades ao primeiro, tais como, comunicação multi-ponto, encaminhamento *many-to-one* e segurança, garantindo-se confidencialidade de dados e autenticação com MACs (*Message Authentication Codes*) ou CMACs (*Cryptography-based Message Authentication Codes*) usando-se criptografia simétrica e funções de síntese segura de mensagens com chaves criptográficas simétricas.

O protocolo é indicado para adopção em redes com grande número de dispositivos e em grande escala, pois tem associado um baixo custo de utilização, boa eficiência energética e a utilização de uma estrutura em rede *mesh* que providencia maior fiabilidade e mais longo alcance, através de estruturas de encaminhamento *multi-hop* de dados.

Existem inúmeras aplicações para este protocolo [86], nomeadamente para redes de monitorização industrial.

No funcionamento do Zigbee existem três funções distintas para os dispositivos:

- Zigbee Coordinator - Responsável pela criação da rede e, regra geral, é o dispositivo que apresenta maiores capacidades. Também tem a função de guardar a informação da organização da rede e funcionar como centro confiável e repositório confiável de chaves.

- Zigbee Router - Tem a função de transmitir dados para outros dispositivos.

- Zigbee End Devices - São dispositivos que estão nos extremos da rede *mesh* e apenas podem comunicar com nós com quem estejam emparelhados. Estes nós podem apresentar características de *hardware* mais simples e têm a possibilidade de funcionar em modos de poupança de energia durante mais tempo que os outros dispositivos com outras funções.

As redes Zigbee operam na frequência de 868 MHz na Europa, 915 MHz em outros países como EUA ou Austrália e 2.4GHz no resto do mundo.

3.3.4 Sumário

Nas secções anteriores foram apresentadas tecnologias de redes de área pessoal, que podem ser utilizadas na arquitectura de referência anteriormente introduzida. Estas redes, podem sofrer intrusões (incluindo intrusões físicas), que podem colocar em causa os serviços de segurança habitualmente suportados. Na utilização de tecnologias baseadas neste tipo de redes a segurança é uma das partes mais críticas, pois pode-se facilmente colocar em causa os pressupostos e garantias associadas às propriedades de segurança apresentadas.

A utilização de tecnologias WPAN no contexto da arquitectura de segurança a propor, deve ser acompanhada de mecanismos adicionais de detecção e prevenção de intrusões, ao nível de estações locais de monitorização que comunicam com as etiquetas RFID. Note-se que, as estações locais de monitorização podem ser materializadas com base em equipamento disponível, através da utilização de dispositivos de ampla utilização ou de baixo custo, como por exemplo: telemóveis e PDAs (com suporte RFID e conexão bluetooth), sensores (IEEE 802.15.4 ou ZigBee) ou estações controladoras de RFID, com interfaces bluetooth ou de redes de área local (IEEE 802.3 ou IEEE 802.11).

3.4 Segurança em RFID

Os RFID [84] são dispositivos que possuem memória e uma antena associada a um mecanismo de comunicação por rádio-frequência, cujas características podem ser diferentes de dispositivo para dispositivo. A memória pode ser só de leitura (ROM ou *Read Only Memory*) ou ser uma memória modificada de forma eléctrica (EEPROM). Neste ultimo caso, é necessário assegurar a protecção da informação, pois esta pode ser alterada.

Relativamente à modelação de sinal nos RFID [88], pode ser efectuada de diversas formas, tais como: *On-Off Keying* (OOK), *Bipolar Phase Shift Keying* (BPSK), *Amplitude Shift Keying* (ASK). Os RFIDs apresentam um modelo de comunicação (ver figura 3.1) que assenta em três camadas: camada aplicação, comunicação e física.

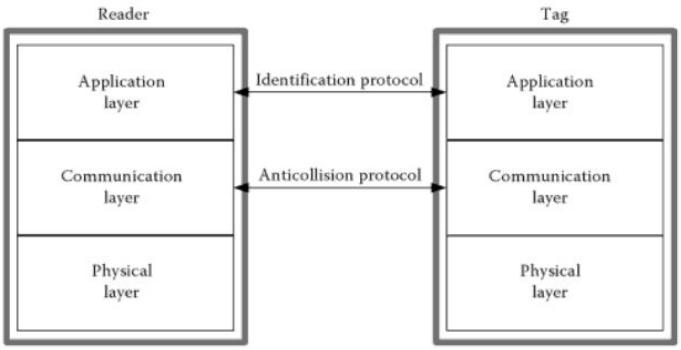

Figura 3.1 Modelo de comunicação do RFID

Na camada de aplicação, é processada a informação do utilizador, onde estão incluídos também os dados da *tag*. A segunda camada (comunicação), gere a forma como os leitores e as *tags* podem comunicar. Por isso, é neste local que estão incluídos os protocolos contra colisões. Por último, a camada física define, entre outros, a frequência, modelação, codificação de dados, transmissão, ou seja específica a interface física sem fios.

As *tags* também podem ser classificadas como básicas ou dotadas de criptografia (ou *crypto tags*) [89], de acordo com as capacidades criptográficas que apresentam. As *crypto tags* conseguem executar operações clássicas de criptografia, ao contrário das primeiras.

A utilização de criptografia nos dispositivos RFID tem como objectivo garantir protecção dos dados, privacidade, autenticação. Relativamente à protecção de dados, esta procura garantir protecção contra leitura de dados reservados e adulteração de dados de forma maliciosa. A privacidade é uma propriedade absolutamente essencial em sistemas que utilizam RFID, pois procura providenciar a não localização ou obtenção de informação adicional do objecto, apenas através do seu identificador. A garantia da propriedade de autenticação é também fulcral, pois visa garantir a originalidade de um objecto através de uma assinatura.

A utilização de protocolos criptográficos, de baixo custo computacional e que ofereçam garantias face a propriedades de autenticação mútua (*tag*-leitor), confidencialidade, integridade, condições de privacidade e protecção contra *replaying* é ainda um aspecto em aberto que tem

sido objecto de diversas contribuições da investigação.

De seguida, são apresentados diversos protocolos de autenticação que podem ser divididos de acordo com os algoritmos criptográficos utilizados. Os protocolos de autenticação leves, apenas utilizam operações simples, como XOR ou operações de autenticação de assinaturas rápidas ou de baixo custo computacional, inspiradas em códigos de autenticação de mensagens a partir de chaves partilhadas (do tipo MAC ou *Message Authentication Codes*). Para além destes, existem outros dois grupos de protocolos que utilizam criptografia simétrica ou assimétrica.

3.4.1 Privacidade

A privacidade [51] assume-se, tal como foi referido anteriormente, como uma propriedade fundamental dos sistemas RFID, já que ao contrário dos sensores comuns, apresentam um identificador que permite realizar associações directas sobre contextos que podem ter que ser mantidos privados. Um dos problemas que pode surgir, diz respeito à detecção não autorizada de movimento ou de uso de *tags* (designada genericamente por *tag tracking*). Como cada objecto-alvo apresenta um identificador único, caso seja detectado por algum leitor pertencente a um sistema RFID, é possível monitorizar os movimentos de um determinado objecto ou de uma pessoa que transporte uma *tag* e que assim pode ser facilmente relacionada com a mesma.

Como os RFID respondem a interrogações efectuadas pelos leitores, o registo de movimentos efectuados é possível. Actualmente, este problema ainda não assume uma preocupação extrema, pois os sistemas RFID são escassos, fragmentados e usados na maior parte dos casos em condições de supervisão humana. De todo o modo, à medida que o seu âmbito de funcionamento se alarga e o número de sistemas aumenta, a problemática da privacidade pode assumir preocupações importantes.

Os telemóveis são dispositivos que também apresentam problemas de privacidade. Contudo, como é possível desligar os mecanismos de comunicação como Bluetooth ou 802.11, esse problema não se torna tão importante, podendo ser conscientemente controlado pelos seus utilizadores. Para além disso, como são dispositivos com poder de computação bastante superior aos RFID, podem aplicar mecanismos de controlo de acesso mais sofisticados, de forma a mitigar esse problema.

3.4.2 Autenticação e privacidade

É necessário que a comunicação entre as *tags* RFID e os leitores seja autenticada, de modo a existir a garantia de que são dispositivos confiáveis e que fazem parte do sistema. Por esse motivo, o estabelecimento de protocolos de autenticação entre as duas partes torna-se uma boa solução. Nestes protocolos, para garantir a privacidade é necessário que a identificação do dispositivo não passe em claro no processo de comunicação e apenas seja conhecida por dispositivos confiáveis dentro da rede.

Como veremos de seguida, alguns protocolos utilizam técnicas distintas para proteger a captura do identificador do RFID. Alguns optam pela criação de pseudo-identificadores que são refrescados a cada comunicação com o leitor, enquanto outros, através da utilização de cifra nas mensagens, asseguram sempre a confidencialidade do identificador.

Fora do âmbito dos protocolos de autenticação, é possível implementar esquemas para assegurar a privacidade na utilização dos RFIDs. Uma solução apresentada consiste na reserva de um bit na memória do RFID para definir se pode ser interrogado pelos leitores. Uma das aplicações imediatas deste mecanismo situa-se num produto que é comercializado. No período anterior à sua venda, o bit de privacidade é colocado a 0, podendo ser interrogado pelos leitores RFID. No momento da compra, esse bit é colocado a 1, de modo a assegurar a privacidade do comprador do produto que contêm o RFID.

Com intuito de proteger a privacidade, as *tags* designadas por EPC [5], contêm um mecanismo de desactivação, através de um comando *kill* que utiliza um PIN de 32 bits para garantir que essa acção só é desencadeada por entidades autorizadas. Este esquema pretende atingir os mesmos objectivos da solução anterior, mas apresenta uma desvantagem. Enquanto o comando *kill* desactiva a *tag*, a solução anterior apenas define os parâmetros de privacidade, ou seja o RFID continua a ser utilizável.

3.4.3 Protocolos de autenticação leves

3.4.3.1 EMAP

Este protocolo [69] tem como objectivo garantir autenticação mútua entre um leitor e uma *tag* RFID. As entidades envolvidas são: servidor, leitor e *tag*. A comunicação entre leitor e servidor é considerada segura, ao invés da comunicação entre os leitores e as *tags* RFID. Este protocolo

utiliza pseudónimos com 96 bits para identificação da *tag* e uma chave dividida igualmente em fracções de 96 bits. A comunicação é iniciada pelos leitores devido ao tipo das *tags* em uso serem passivas.

O protocolo pode ser dividido em quatro fases: identificação da *tag*, autenticação mútua, actualização dos pseudónimos e actualização das chaves. Na primeira fase, o leitor envia uma mensagem de *hello* para *tag*, que responde com o seu pseudónimo. O leitor necessita de consultar o servidor, através do pseudónimo fornecido para lhe ser atribuída a chave da *tag*.

Na fase de autenticação mútua, o leitor gera dois números aleatórios, para construção de três sub-mensagens que compõem a mensagem e envia para a *tag*. Esta, verifica a autenticidade do leitor, pois nas mensagens estão incluídas partes da chave. De seguida, envia para o servidor uma mensagem composta por duas sub-mensagens com uma parte da chave, de modo a se autenticar perante o leitor. Após a fase de autenticação das partes, ambas actualizam pseudónimos através de uma parte da chave, apenas conhecida por ambos. A actualização das chaves é realizada em fases, após a autenticação com sucesso, sendo gerada essencialmente, através do identificador estático da *tag*, que não transita na rede e através da parte correspondente da chave anteriormente utilizada.

A componente da privacidade neste protocolo está assegurada, pois apenas um leitor reconhecido consegue comunicar de forma segura com o servidor e através do pseudónimo fornecido, obter informação sobre a *tag*. Os pseudónimos são actualizados a cada autenticação, por isso não é possível ao atacante monitorizar uma *tag* RFID.

Este protocolo não resiste a um ataque de negação de serviço (ou DoS - *Denial of Service*), pois se existir uma dessincronização entre o servidor e a *tag*, os segredos apenas são actualizados numa das partes, não havendo possibilidade de recuperação do estado de consistência no futuro, pois o servidor não irá reconhecer as chaves que a *tag* apresenta.

A propriedade de segurança futura (ou *forward security*) é igualmente assegurada, pois a actualização das chaves não permite que as mensagens anteriormente enviadas entre as partes possam ser decifradas.

3.4.3.2 RFID authentication protocol for low-cost tags

Neste protocolo [77] estão envolvidas três entidades: servidor, leitor e *tag*. O servidor guarda a informação relativa às *tags*. Para cada uma delas armazena informação pessoal, dois pares com o identificador corrente e antigo da *tag*, assim como as sínteses seguras (*secure hashings*) desses identificadores. A *tag*, por seu lado, apenas necessita de armazenar o *hashing* do seu identificador corrente, de forma a minimizar o processamento e a quantidade memória necessária.

Este protocolo contempla três fluxos de mensagens e utiliza desafios/respostas para garantir a integridade do fluxo e protecção contra *message replaying*. Em traços gerais, o primeiro fluxo consiste no desafio lançado pelo leitor à *tag*, sendo o segundo e o terceiro baseados nas mensagens enviadas entre a *tag* e o servidor, de modo a se autenticarem mutuamente. Inicialmente, o leitor envia um desafio à *tag* com um número aleatório. Esta, gera duas mensagens que contêm um número aleatório por ela criado e envia de volta para o leitor. Ao receber as mensagens reenvia-as para o servidor, acrescentando o número aleatório da mensagem inicial.

O servidor ao receber as mensagens, procura pelo *hashing* correcto da *tag*, tentando calcular uma mensagem igual à enviada pela *tag*. Caso isto se suceda, a *tag* passa a estar autenticada perante o servidor. Por forma ao servidor se autenticar perante a *tag*, envia uma mensagem que inclui o identificador e a informação da *tag* ao leitor, reenviando este a mensagem necessária à *tag*. Ao receber as mensagens, realiza um cálculo idêntico e uma comparação à mensagem recebida. Caso sejam iguais, o servidor passa a estar autenticado perante a *tag*. Como o servidor e o leitor comunicam através de um canal seguro, o leitor também passa a estar autenticado perante a *tag*.

Após o processo de autenticação, o servidor e a *tag* refrescam o identificador corrente, através do conhecimento que têm do identificador estático da *tag*. Este, em nenhum caso é transmitido durante a comunicação entre as partes.

Neste protocolo, a privacidade da informação é conseguida, pois através do identificador não é possível obter informação da base de dados, assim como a privacidade da localização, pois o identificador utilizado para indexar a base de dados é actualizado a cada autenticação e esse refrescamento não depende do identificador actual, de modo a não permitir que um atacante consiga reproduzi-lo com sucesso.

A propriedade *anti-replaying* é assegurada por este protocolo, na medida que as mensagens

enviadas pelas partes contêm *nonces* ou elementos que serão válidos apenas uma vez.

Outra das propriedades asseguradas por este protocolo é a protecção contra a personificação da *tag* RFID. Isto verifica-se, pois o atacante no momento do envio das mensagens pela *tag* não consegue ter conhecimento dos segredos partilhados entre ela e o servidor. No caso da personificação do servidor, a propriedade só é conseguida em parte, pois caso o atacante consiga ter acesso ao t_i e a todas as mensagens enviadas, então consegue calcular a chave utilizada na próxima sessão.

A segurança futura e passada também é alvo de análise por este protocolo, apesar de não ser conseguida uma protecção total nesse aspecto. Relativamente à segurança em interacções passadas, esta é assegurada por este protocolo, pois a *tag* apenas tem informação acerca do *hash* utilizado, logo não é possível descobrir os segredos utilizados anteriormente. Por outro lado, a segurança em futuras interacções só é conseguida, caso o atacante após conhecer o estado interno da *tag*, não consiga capturar uma das mensagens que contêm a informação necessária ao cálculo do novo identificador.

Se o atacante realizar um ataque de DoS à *tag*, pode resultar numa dessincronização dos segredos, na medida que serão actualizados no servidor e não na *tag*. Como resposta a este problema, o servidor mantêm a versão corrente e antiga dos segredos para a *tag* conseguir comunicar após o ataque com o servidor.

3.4.4 Protocolos de autenticação com criptografia simétrica

Na secção acima foram descritos alguns protocolos que não utilizam criptografia, mas sim operações mais simples e leves para implementar a propriedade de autenticação nos dispositivos RFID. Nesta secção serão expostos, dois protocolos que utilizam criptografia simétrica durante o seu funcionamento, mais concretamente recorrendo ao algoritmo AES. A escolha deste algoritmo deve-se ao seu relativo baixo custo e bom desempenho pelo que, em teoria, é implementável e utilizável numa *tag* RFID.

O primeiro protocolo, denominado por *Advanced Mutual-Authentication Algorithm Using AES* [82], tal como o nome indica, providencia autenticação mútua entre o leitor e a *tag* RFID. Para além destes elementos, existe um servidor central que serve como repositório de chaves. Em cada *tag* é colocada uma identificação única, assim como dois números aleatórios secretos

e uma chave de 128 bits. O servidor, para além desta informação também armazena o identificador estático da *tag*.

Tal como nos protocolos anteriormente apresentados, supõe-se que o canal de comunicação entre o servidor e o leitor seja seguro. É igualmente assumido que a *tag* possua *hardware* com capacidade para suportar o algoritmo AES, visto poder ser implementado com cerca de 4K *gates*.

Este protocolo consiste em três fases: desafio, autenticação do leitor, autenticação da *tag*. Antes do envio do desafio a uma *tag*, o leitor aplica um protocolo anti-colisão para escolher uma *tag* entre muitas que estão ao seu alcance. Após a escolha pede ao servidor os *nonces* cifrados e reenvia esse desafio para a *tag*, de modo a se autenticar perante ela.

Ao receber a mensagem, a *tag* verifica se o que recebeu são realmente os *nonces* que possui e caso isto se verifique autentica o leitor. Se o leitor não for autorizado a *tag* deixa de responder, o que impede um ataque de *man-in-the-middle*. Após a autenticação do leitor, a *tag* actualiza os *nonces* e envia uma mensagem cifrada contendo o seu identificador. O servidor, ao receber essa mensagem, compara com o identificador que está na base de dados e no caso de se verificar autentica a *tag* e actualiza os *nonces* de igual forma à efectuada pela *tag*. A actualização dos *nonces* previne ataques de *replaying*, pois são utilizados apenas uma vez numa sessão autenticada.

A problemática da privacidade está garantida neste protocolo, pois o identificador estático nunca é enviado nas mensagens e o identificador único colocado na *tag* e no servidor é enviado nas mensagens de forma cifrada, logo não é possível um leitor malicioso obter informação sobre a *tag* na base de dados nem seguir os movimentos da mesma.

Se um atacante conseguir obter os segredos internos de uma *tag*, como a chave nunca é refrescada, consegue descobrir o conteúdo das mensagens passadas, caso as tenha capturado.

O segundo protocolo, denominado por *Secure Symmetric Authentication for RFID tags* [20], utiliza criptográfica simétrica, nomeadamente o algoritmo AES, com o intuito de providenciar autenticação entre o leitor e a *tag* RFID. Na sua especificação existe a possibilidade da autenticação apenas se realizar de modo unilateral por parte do leitor ou da *tag*, mas para efeitos desta dissertação, apenas é interessante o estudo da vertente de autenticação mútua.

De modo igual aos protocolos apresentados anteriormente, existem três entidades no seu

funcionamento, um servidor, leitor e *tags* RFID. Os problemas principais focados por este protocolo são a falsificação, *tracking* não autorizado, e acesso não concedido à memória da *tag*.

A computação do algoritmo AES com chaves de 128 bits, apresenta um peso elevado em comparação com as outras operações efectuadas pela *tag*. Por esse motivo, foi obrigatório a realização de uma nova implementação do algoritmo, já que as disponíveis têm como objectivo principal elevadas taxas de transferência e não o consumo de energia. De acordo com os resultados obtidos, o consumo de energia cifrou-se na ordem de 4μA com uma área de 3500 *gates*. Como actualmente o consumo de energia numa *tag* não deve exceder os 10μA, o protocolo preenche os requisitos necessários para ser implementado.

É fundamental para o funcionamento do protocolo que o *output* do algoritmo AES esteja disponível dentro do tempo em que a *tag* possui energia. Devido a isso, a autenticação realiza-se em duas fases: *authentication request* (AR) e *response requests* (RR). Na primeira fase, o leitor contacta a *tag* enviando um desafio para ser respondido por ela. Na segunda fase, a cifra realizada é enviada para o leitor.

A fase de autenticação mútua, necessita do envio de desafios pelas partes, sendo a resposta da *tag* efectuada de forma faseada, como foi referido. O contacto inicial é efectuado pelo servidor, que posteriormente recebe um *nonce* enviado da parte da *tag*. De seguida, o leitor envia para a *tag* o resultado do desafio lançado por ela e um novo desafio para ser respondido pela *tag*. Após o leitor se autenticar perante a *tag*, esta responde ao desafio de forma cifrada, onde está incluído o seu identificador.

A privacidade da informação é garantida, pois o identificador da *tag* é enviado para o leitor de forma cifrada, logo apenas com conhecimento da chave é possível obtê-lo.

As características do protocolo também previnem contra um ataque de *replaying*, pois os *nonces* utilizados apenas são válidos por uma sessão, logo os duplicados das mensagens por parte de um atacante serão descartados. Contudo, este protocolo apresenta algumas desvantagens devido à não actualização das chaves que constituem os segredos. Caso um atacante consiga ter acesso ao estado interno da *tag* e tenha obtido mensagens anteriores, consegue decifrar as mensagens passadas, logo a propriedade *forward security* não é assegurada.

3.4.5 Protocolos de autenticação com criptografia de curva elíptica

O algoritmo apresentado nesta secção utiliza criptografia assimétrica com curva elíptica para garantir a propriedade de autenticação. Esta variante de criptografia assimétrica proporciona segurança equivalente a esquemas como o RSA, mas requer chaves de tamanho inferior. Também necessita de menor capacidade de processamento e memória, por isso dentro desta classe de criptografia são os mais indicados para serem implementados em RFID.

3.4.5.1 A secure elliptic curve-based RFID protocol

O protocolo proposto em [63] utiliza o protocolo de Schnorr's [74] para curva elíptica, com um mecanismo de actualização do segredo da *tag* RFID. Neste processo estão envolvidas três entidades: *tag*, leitor e base de dados.

Este protocolo processa-se em quatro fases: *setup*, autenticação do leitor, identificação e verificação da *tag*. Inicialmente, são inicializados os parâmetros da curva elíptica, incluindo a chave pública e o ponto secreto.

Na fase de autenticação, o leitor escolhe um número aleatório e realiza uma computação para enviar para a *tag*. Esta, envia um número aleatório para o servidor realizar outro cálculo e retorná-lo para a *tag*. Após receber a mensagem do servidor, compara o que recebeu com aquilo que calculou, para autenticar o leitor.

No caso da autenticação ter sido bem sucedida, o leitor pretende identificar a *tag* e proceder à leitura dos dados. Este processo, realiza-se a cada vez que o leitor pretender ler a informação de uma *tag*. Nesta altura, a *tag* calcula o seu pseudo-identificador e o seu novo ponto secreto.

Após estas operações, envia para o leitor o seu pseudo-identificador. Neste momento, a *tag* ainda não está autenticada perante o leitor. Por esse motivo, o leitor contacta a base de dados para verificar a identidade da *tag* e obter os seus dados. Caso o identificador esteja guardado na base de dados, procede-se à sua actualização do mesmo modo realizado na *tag*.

A viabilidade da implementação da curva elíptica em *tags* RFID foi comprovada em [22]. Tendo em conta que, actualmente, uma *tag* RFID suporta cerca de 15000 *gates* e a implementação realizada utiliza 10000 *gates* para 137 bits, logo considera-se exequível.

Um dos requisitos de performance para um sistema RFID, diz respeito à restrição de um segundo de duração para a comunicação. Sabendo-se que na implementação efectuada o tempo medido é cerca de 0.8 segundos, logo o requisito encontra-se cumprido.

	Protocolos de autenticação				
	EMAP[69]	Low-cost[77]	A. AES[82]	Secure S.[20]	Elliptic [63]
Privacidade da inform.	Sim	Sim	Sim	Sim	Sim
Privacidade da localiza.	Sim	Sim	Sim	Sim	Sim
Autenticação da *tag*	Sim	Sim	Sim	Sim	Sim
Autenticação do leitor	Sim	Sim	Sim	Sim	Sim
Forward Security	Sim	Sim	Sim	Não	Sim
DoS	Não	Sim	Não	Não	Parcial

Tabela 3.1 Protocolos de autenticação e propriedades de segurança garantidas

Relativamente às propriedades de segurança, mais concretamente à privacidade, pode-se afirmar que é satisfeita neste protocolo, pois apenas o pseudo-identificador pode ser relacionado com a *tag*, mas como este é alterado a cada autenticação, não é possível um atacante seguir os movimentos de uma *tag* nem aceder aos seus dados.

Um atacante através do pseudo-identificador da *tag*, não consegue ter acesso ao segredo, pois teria que executar o cálculo do logaritmo discreto, contudo não é computacional possível.

Na possibilidade do atacante conseguir o acesso à chave utilizada, continua a não ter meios para determinar as chaves anteriormente utilizadas, pois teria novamente que resolver o problema do logaritmo discreto. Por esta razão, a propriedade de *forward security* encontra-se satisfeita.

3.4.6 Sumário

Após análise dos protocolos de autenticação apresentados, verifica-se em termos gerais que todos têm as condições necessárias para serem implementados, apesar de na sua génese apresentarem diferentes mecanismos, de modo a garantir as propriedades de segurança apresentadas na tabela 3.1. Todos os protocolos apresentados suportam a privacidade da informação e localização da *tag* RFID, assim como autenticação mútua entre ela e o leitor.

Relativamente a outras propriedades de segurança não fundamentais, apresentam algumas diferenças. Uma propriedade que é interessante estar garantida é a propriedade de segurança futura e passada (*forward/backward security*), pois caso o estado interno da *tag* seja conhecido, é importante preservar a confidencialidade das comunicações anteriormente efectuadas ou garantir que a partir de um estado actual não seja possível colocar em causa a confidencialidade no

futuro. O único protocolo apresentado que não cumpre esta propriedade é o *Secure Symmetric Authentication for RFID Tags* [20], pois conhecida a chave utilizada, como esta não é refrescada, é possível decifrar as mensagens que transitaram na rede, caso tenham sido capturadas pelo atacante.

Um ataque de DoS também pode ser efectuado e nesse caso apenas o protocolo *RFID authentication protocol for low-cost tags* [77] consegue proteger dos seus efeitos, pois incluí mecanismos de recuperação da comunicação entre o leitor e a *tag*, em situação de dessincronização. Ainda em relação a esta propriedade, o protocolo *Secure elliptic Curve-based* [63] satisfaz parcialmente este requisito, enquanto os restantes não oferecem protecção.

Como estes protocolos utilizam chaves ou pseudo-identificadores, conhecidos pelos servidores e *tags*, com o intuito de preservar a confidencialidade das comunicações, é necessário existir um estabelecimento prévio dos segredos nas duas partes. Esta particularidade é evitada pela génese do protocolo que utiliza curva elíptica, pois como utiliza mecanismos de chave pública/privada não necessita de estabelecimento externo dos segredos no protocolo.

Esta particularidade em relação a todos os outros, assim como o cumprimento das propriedades de segurança que se consideram fundamentais, revela-se como um forte candidato a ser implementado na dissertação.

Tal como foi referido anteriormente, as *tags*, regra geral suportam cerca de 15000 *gates*. Analisando as dimensões necessárias para uma *tag* RFID, podemos verificar que a área necessária para ser implementado um protocolo de autenticação com criptografia simétrica é cerca de 20 vezes superior ao necessário para os protocolos leves, sendo o seu tamanho cerca de 0.25 mm^2, ou seja, sensivelmente a área de um grão de areia. Por sua vez, para implementação com curva elíptica, a área necessária é cerca de 2.5 vezes superior. Como a área necessária para o *chip* da *tag* RFID é bastante pequena e enquadra-se nas especificações actuais, então considera-se que seja aplicável no *hardware* disponível.

3.5 Arquitecturas comparativas

Nesta secção apresentam-se trabalhos relacionados com arquitecturas de localização e detecção de objectos, que permitem uma análise comparativa com o âmbito e os objectivos da dissertação.

3.5.1 Sistema para monitorização de localização geográfica de objectos

O sistema implementado em [54] pretende efectuar *tracking* de objectos RFID e oferecer uma interface gráfica, com o intuito de possibilitar a visualização do registo das leituras dos objectos. O objectivo desta implementação é similar ao pretendido por esta dissertação, mas a forma de o realizar e a complexidade do sistema apresentam diferenças significativas.

No sistema apresentado pelos autores, existem nós de referência que estão fixos e conhecem as coordenadas da sua localização, tendo como função, auxiliar os leitores RFID a obter localizações das leituras efectuadas. Este sistema apresenta um servidor com informação sobre o registo das leituras efectuadas, um computador que é utilizado para visualização dos eventos que ocorrem no sistema e um conjunto de nós Zigbee, cuja tecnologia foi apresentada na secção 3.3.3. Os nós Zigbee têm a função de registar as leituras dos RFID e transmitir essa informação pela rede, até alcançar um nó de acesso com ligação ao servidor.

O sistema que propomos implementar, ao contrário do proposto pelos autores, pretende fornecer esquemas de segurança, quer ao nível da comunicação entre os nós ou ao nível de intrusões a nós particulares, de modo a obter níveis de confiança para a informação obtida e mitigar potenciais ataques que possam surgir no sistema. Outra das diferenças que se verifica, diz respeito à forma de obtenção da localização, pois no sistema apresentado em [54] a localização é obtida por nós estáticos e não em movimento como o que propomos realizar. Como a mobilidade é uma propriedade importante nestes sistemas, o modo como se obtém a localização das leituras não deve ser estático, de forma a não limitar o funcionamento do sistema.

3.5.2 Arquitectura de monitorização de objectos num ambiente GIS e rede GSM

O sistema apresentado em [65] pretende efectuar *tracking* de objectos, utilizando um meio de comunicação por GSM (ver secção 3.1.1.1) para disseminar a informação. Como meio de visualização da informação recolhida pelos leitores utilizou-se o WebGIS, que é uma versão para *browser* do GIS.

Os leitores RFID ao recolherem a informação vinda das *tags*, transmitem-na através do módulo GSM que possuem. Nesta implementação são usadas SMS como meio de notificação de eventos que ocorrem no sistema. Devido ao seu baixo custo e facilidade de utilização, considerou-se uma boa forma de disseminação de notificações. Os dados são encaminhados para a base de dados para posteriormente serem visualizados no WebGIS.

Esta implementação, relativamente à solução que pretendemos realizar nesta dissertação, não utiliza mecanismos de segurança na transmissão da informação entre o RFID e o leitor, logo não consegue evitar que leitores ou dispositivos RFID maliciosos possam efectuar acções com sucesso no sistema. Apesar de procurar utilizar o GSM como meio de transmissão de informação, devido à ampla abrangência do mesmo, não apresenta meios alternativos de disseminação da informação.

Para a informação ser visualizada no mapa do WebGIS, é necessário que no intervalo de tempo entre a leitura do RFID e até que a informação alcance efectivamente a base de dados, a localização da leitura seja recolhida. Para este fim, foram utilizadas as coordenadas da *base station* (BS) que recebeu os dados do módulo GSM do leitor, mas resulta numa fraca precisão da informação, na medida que a BS pode estar consideravelmente longe do leitor.

Para a informação da localização apresentar valores mais correctos, seria necessário alternar ou combinar a localização por GSM, por exemplo com GPS. A disponibilidade do GPS em meios a céu aberto é boa, mas em meios *indoor* é baixa, logo nessas situações a localização com GSM seria importante para uma aquisição rápida de localização.

3.5.3 Sumário

As arquitecturas atrás descritas exibem semelhanças com o modelo que pretendemos implementar, pois utilizam RFIDs para realizar *tracking* de objectos, um servidor com uma base de dados de leituras e um mapa para visualização. Contudo, a forma como a arquitectura foi concebida tem algumas diferenças com a arquitectura proposta na dissertação e os seus requisitos inicialmente identificados.

Uma das diferenças prende-se com a não utilização de mecanismos de segurança para evitar intrusões ou ataques ao canal de comunicação, pois não foram criadas tendo em conta as propriedades de segurança fundamentais. Outra das diferenças está relacionada com os meios de comunicação utilizados. Isto verifica-se, pois no nosso modelo de implementação está previsto a utilização de diversas tecnologias, bem patente nas diferentes classes de redes apresentadas, pelo motivo de uma só tecnologia não estar contemplada na maioria dos dispositivos, por motivos de capacidade do *hardware* ou particularidades do meio de comunicação. Como a arquitectura que propormos implementar tem carácter genérico, é importante prever a utilização de

diferentes tecnologias para o mesmo fim, quando o meio onde é aplicado diverge significativamente.

3.6 Análise crítica

No capítulo 2 (secção 2.7) apresentou-se inicialmente um modelo genérico da arquitectura de referência que orienta a motivação e os objectivos da presente dissertação. Partindo dessa arquitectura, o capítulo 3 faz uma abordagem às tecnologias que podem ser consideradas para uma possível implementação dessa arquitectura. Apresentam-se assim diversas tecnologias de redes e discutem-se os seus principais mecanismos e serviços de segurança.

Relativamente às redes de área global, descritas na secção 3.1, a segurança fornecida pelo GSM é considerada inferior ao SSL ou IPSec, aspecto a ter em conta numa implementação da arquitectura de referência. Outro exemplo de diferenciamento de confiança nas soluções de segurança refere-se à eventual utilização de WEP em detrimento de WPA ou WPA2 no caso de se usar comunicação em redes 802.11.

Não estando nos objectivos da dissertação a correcção das vulnerabilidades ou fraquezas das soluções de segurança normalizadas nas tecnologias apresentadas, a observação principal a retirar é que essas vulnerabilidades justificam a inclusão de mecanismos complementares de segurança ao nível da arquitectura, para que essas fraquezas possam ser mitigadas.

Quanto à abordagem dos problemas de segurança em sistemas RFID destaca-se a problemática da implementação robusta de serviços de autenticação (nomeadamente a necessidade de mecanismos para autenticação mútua) e que assegurem condições de privacidade dos alvos. Os mecanismos para autenticação, confidencialidade e integridade para localização segura de alvos identificados por RFID, encontram desafios interessantes na concretização em dispositivos com capacidades muito limitadas, no que diz respeito à não possibilidade de adopção de métodos criptográficos computacionalmente e energeticamente muito exigentes.

Os protocolos apresentados e que são representativos da investigação recente, mostram ser possível suportar propriedades de segurança com métodos criptográficos simétricos e métodos de criptografia assimétrica de curva elíptica, compatibilizando-se os requisitos dos serviços de segurança, com a sua possível implementação prática em dispositivos de baixas capacidades em

recursos computacionais, bem como constrangimentos de disponibilidade e consumo de energia, como os que podem ser adoptados na área dos dispositivos para detecção e alvos RFID.

Das considerações anteriores resultam pois dois aspectos fundamentais. Por um lado, na arquitectura de segurança deve prever-se forma de "pesar" diferentes métricas ou condições de risco que possam estar associadas à utilização de diferentes tecnologias de redes de comunicação. Esta pesagem deve corresponder a diferentes condições e garantias de segurança usadas como bases de confiança do sistema. A pesagem e o seu processamento deve estar igualmente associada a informação de detecção de localização sobre os mesmos alvos, que chegue em diferentes condições espaço-temporais às estações centrais de rastreio, a partir de estações locais independentes que estejam interligadas na arquitectura. Essa pesagem pode ainda ser combinada com processamento de acordos de agregação segura de dados de localização provenientes das diferentes estações independentes, detectando e descartando dados incorrectos e relevando os dados considerados mais confiáveis. Para tal, devem poder obter-se leituras replicadas realizadas sobre o mesmo alvo, por parte de diferentes estações locais de monitorização, comunicando com diferentes opções de segurança com as estações centrais de rastreio.

Por outro lado, em nenhuma das soluções de segurança estudadas se contempla a possibilidade das estações locais de localização poderem operar com falhas ou operarem incorrectamente em decorrência de ataques por intrusão. É pois necessário incorporar na arquitectura de segurança os mecanismos anteriores e que possam funcionar como mecanismos adicionais de resistência face a essas intrusões. Finalmente são abordadas arquitecturas que exibem semelhanças com o modelo que pretendemos implementar, pois utilizam RFIDs para monitorização (ou *tracking*) de objectos, um servidor com uma base de dados de leituras e um mapa para visualização. Nota-se no entanto que a abordagem de segurança nestes sistemas não leva em linha de conta as propriedades de segurança que se pretendem objectivar na dissertação, nomeadamente (i) ao nível da resistência das estações face a falhas ou intrusões, (ii) cobertura e escala da solução, (iii) condições de ubiquidade, (iv) garantias de autenticação mútua e (v) avaliação do impacto energético desses protocolos e (vi) condições de latência dos protocolos e implicações na mobilidade dos alvos.

4. Arquitectura para localização segura de alvos RFID

Este capítulo apresenta a proposta de uma arquitectura para identificação e localização segura de objectos móveis identificados por rádio-frequência, aprofundando o modelo inicialmente apresentado no capítulo 2 (secção 2.7). A arquitectura é inicialmente formalizada e posteriormente detalhada ao longo do capítulo, de acordo com o seguinte enquadramento:

- A secção 4.1 formaliza os conceitos e componentes principais da arquitectura e seus níveis de estruturação, apresentando as entidades do modelo arquitectural e apresentando o processamento realizado por essas entidades, aos diferentes níveis.

- A secção 4.2 clarifica a arquitectura instanciando-a a partir de dispositivos e tecnologias de comunicação que podem ser utilizados na sua materialização.

- A secção 4.3 apresenta os serviços de segurança da arquitectura. Estes serviços envolvem as diversas entidades principais que inter-operam na arquitectura, nomeadamente: (i) o protocolo de autenticação entre alvos RFID, estações locais e estações centrais de rastreio; (ii) os mecanismos de garantia de privacidade dos alvos detectados pelas estações locais, (iii) a protecção das comunicações (que assegura autenticidade, confidencialidade e integridade dos fluxos de informação associados aos protocolos de detecção, identificação e localização de alvos, trocados entre os alvos, estações de localização e estações centrais de rastreio) e (iv) o estabelecimento de consensos de localização geográfica de alvos RFID detectados por diferentes estações locais, de modo a suportar falhas e tolerar ataques por intrusão nessas mesmas estações.

- A secção 4.4 apresenta em detalhe o protocolo de autenticação entre alvos e estações de monitorização, sendo apresentadas as variantes do protocolo e suas propriedades.

- A secção 4.5 é dedicada à discussão das condições de mobilidade de alvos, tendo em vista a avaliação dos protocolos de autenticação face a essa mobilidade.

- A secção 4.6 apresenta em detalhe os mecanismos utilizados para estabelecimento do modelo de consenso confiável de localização geográfica de alvos RFID.

4.1 Modelo Arquitectural

A figura 4.1 representa a organização global da arquitectura proposta. A arquitectura abarca as seguintes entidades principais: objectos-alvo, estações locais de monitorização e estação central de rastreio. Na arquitectura existem 2 níveis principais de estruturação: (i) o nível de detecção, identificação e localização de objectos-alvo e (ii) o nível de agregação, controlo e armazenamento persistente das localizações observadas.

4.1.1 Nível de detecção, identificação e localização

Este nível envolve os objectos que são alvo de monitorização e as estações locais que procedem a essa monitorização. Neste nível têm lugar as interacções entre os objectos-alvo (que se movimentam no espaço e no tempo) e as estações locais, que procedem à detecção dos objectos-alvo e registam a localização de observação dos alvos.

A identificação e a localização dos objectos pelas estações locais, suporta-se num protocolo de monitorização que garante a autenticação entre os identificadores dos objectos (RFID) e as próprias estações. A concretização deste nível da arquitectura pode fazer-se com base em tecnologia de comunicação de redes de sensores sem fios (com base nas normas IEEE 802.15.4 ou Zigbee ou soluções emergentes do tipo 6LoWPAN [67]) que pode ser usada para construção de *tags* ou para implementação de estações de localização. Este nível também pode ser concretizado por etiquetas passivas para RFID e dispositivos de leitura RFID de proximidade e de baixa frequência, em moldes usuais, sendo particularmente interessante nesta dissertação, a implementação das estações com base em telefones móveis equipados com sistemas de localização geográfica (através de GPS ou A-GPS).

Ao nível de identificação e localização dos objectos-alvo devem garantir-se as seguintes propriedades:

- Autenticação entre objectos-alvo e as estações locais, podendo esta ser autenticação unilateral ou autenticação mútua.
- Garantia de privacidade dos objectos-alvo durante o procedimento de autenticação entre estes e as diferentes estações locais de detecção.
- Garantia de propriedades de confidencialidade e integridade de dados nos fluxos de informação trocados entre os objectos-alvo e as estações locais, durante o processamento de

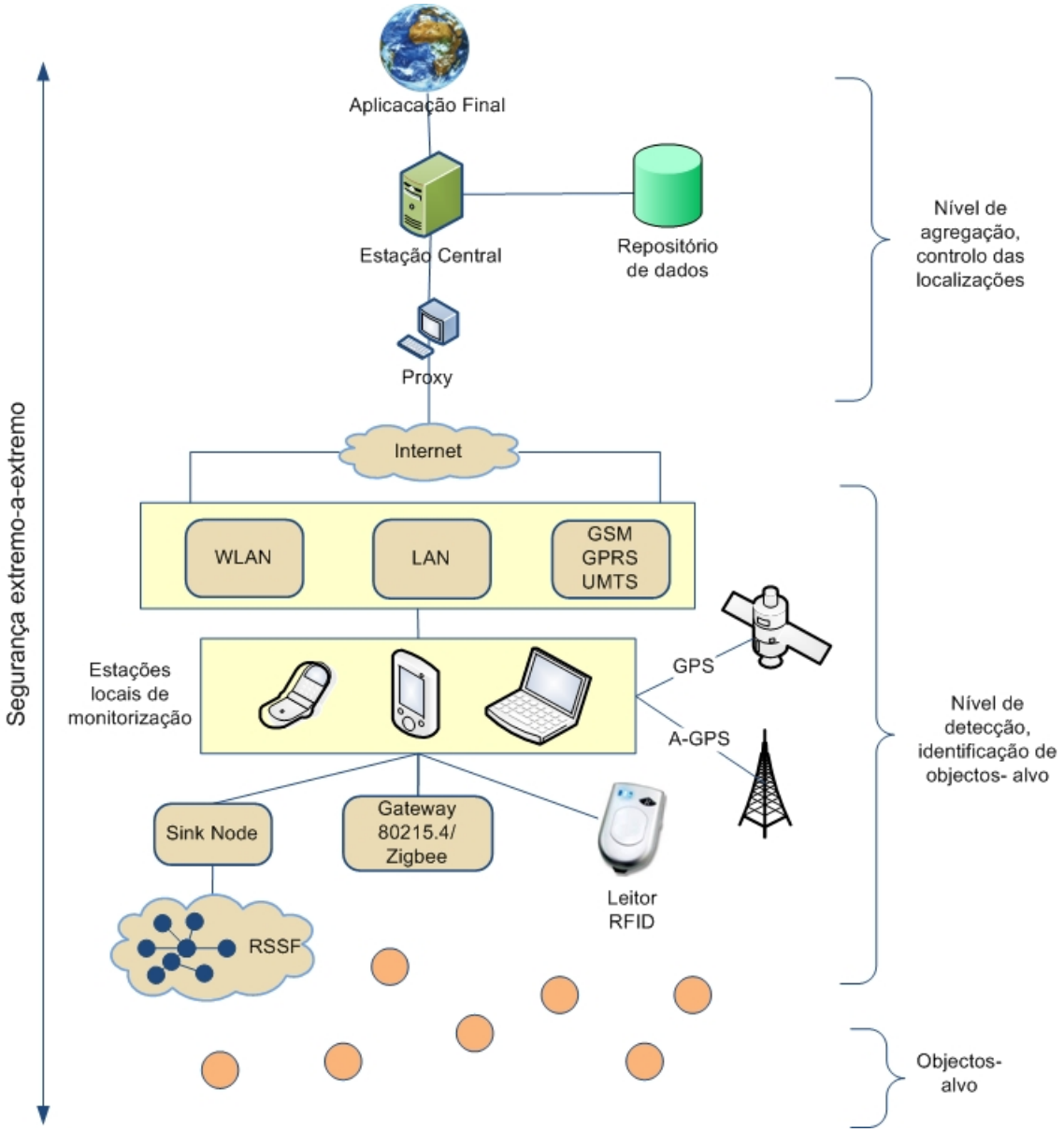

Figura 4.1 Diagrama conceptual da arquitectura

identificação e localização dos alvos e numa perspectiva extremo-a-extremo, isto é, entre os alvos e a estação central de rastreio.

De acordo com as propriedades anteriores, pretende-se preservar condições gerais de segurança face às tipologias de ataques, tal como definidas para adversários do tipo Dolev-Yao [39] e de acordo com as propriedades, mecanismos e serviços de segurança, tal como definido na

framework OSI X.800 [78].

4.1.2 Nível de agregação, controlo e armazenamento persistente de localizações

Conceptualmente, o nível de agregação, controlo e armazenamento persistente de localizações de alvos observados pelas estações locais, centraliza o processamento das localizações observadas por várias estações locais, agregando, verificando e processando a informação recebida a partir de diferentes estações locais interligadas a uma ou mais estações de rastreio. Este nível é suportado por um ambiente de comunicação segura de grande escala, podendo ser estabelecido através da rede *internet* ou combinando diferentes tecnologias de redes locais com ou sem fios, redes GSM ou redes PAN, numa estrutura de *internetworking* interligando esses ambientes e que ligam as estações locais de monitorização e as estações centrais de rastreio.

4.1.3 Processamento ao nível das estações locais

Como atrás se introduziu, o processamento ao nível das estações locais deve assegurar a detecção segura de objectos-alvo de monitorização. As estações locais devem poder desempenhar o protocolo de detecção e autenticação, que permite identificar e localizar os objectos-alvo com salvaguarda da sua privacidade, preservando ao mesmo tempo a confidencialidade e integridade dos dados trocados com os objectos-alvo.

Deve notar-se que na arquitectura global as estações locais podem ser fixas ou móveis. É importante referir que estas estações são dotadas de mecanismos de detecção de localização, como por exemplo GPS (quando se tratem de estações móveis). Sendo estações fixas, possuem conhecimento (por exemplo, por configuração) da sua localização geográfica.

Durante o processamento de protocolos de autenticação, as estações locais adicionam aos identificadores dos objectos móveis, a informação relativa à sua localização, que corresponde pois ao local de observação dos objectos. A conjugação da informação dos identificadores RFID observados, juntamente com a informação de localização das estações locais, dá origem à emissão de certificados de localização de identificadores observados, emitidos pelas estações locais. Estes certificados são enviados de forma autenticada pelas estações locais para as estações centrais de rastreio, no contexto do processamento dos protocolos de autenticação, associados à

detecção e localização dos objectos-alvo.

4.1.4 Processamento ao nível das estações centrais

Como inicialmente se referiu na apresentação preliminar da arquitectura no capítulo 2, admite-se que as estações locais possam operar (em maior ou menor número) de forma não supervisionada. As estações locais podem ser operadas de forma colaborativa com base num modelo participativo ou colaborativo de sensoriamento ou detecção (inspirado no modelo das plataformas designadas na investigação, por *participatory sensing platforms* [31]). Assim, as estações locais podem corresponder a diferentes dispositivos não controlados ou não supervisionados por uma mesma entidade. Admite-se igualmente que as estações locais, as estações de rastreio, os demais componentes da arquitectura de localização ou os recursos associados aos serviços de comunicação, possam globalmente ser geridos ou supervisionados por diferentes entidades organizacionais, constituindo assim um ambiente de gestão com supervisão descentralizada.

As estações de rastreio, que em última instância são utilizadas por entidades que necessitam de monitorizar conjuntos de alvos específicos, devem decidir sobre as localizações observadas através de mecanismos de processamento e agregação segura e confiável dos dados, podendo estes serem enviados com base em diferentes certificados de localização, por parte de diferentes estações locais que detectam os mesmos alvos. Como se pretende introduzir mecanismos de tolerância a falhas ou despistagem de operação incorrecta induzida por estações locais, que possam ter sido atacadas por intrusão, admite-se que as estações locais possam enviar informações incorrectas para as estações de rastreio. Na arquitectura proposta e modelo de adversário considerado, apenas se admite que as estações centrais de rastreio são confiáveis.

Os mecanismos anteriores devem assim permitir que o sistema resista a modelos de adversários bizantinos actuando ao nível das estações locais [58], [35]. Para este efeito, uma estação central de rastreio deve estar apta a detectar e descartar informação incorrecta, proveniente de estações locais que exibam comportamentos detectados como incorrectos, devendo o seu processamento permitir tomar as medidas necessárias para evitar a actuação de tais estações, como por exemplo reduzir gradualmente o peso dessas estações na informação que providenciam ou mesmo, revogar completamente essa informação e suprimir as referidas estações como estações a considerar.

O processamento de agregação segura de dados na estação de rastreio deve pois assegurar a detecção de desvios de informação de localização, através de análises envolvendo diferentes informações de localização, obtidas por diferentes estações independentes. Para este efeito, será necessário garantir que haja disponibilidade de informações obtidas a partir de um número de estações locais correctas, de modo a poder decidir-se sobre a correcção dos valores de localização enviados, num certo intervalo temporal sobre um mesmo alvo RFID. Este processamento recorre a uma amostra de várias localizações propostas por diferentes estações, o que permite às estações centrais de rastreio detectarem e descartarem informação considerada incorrecta ou falsa.

Garantindo-se as anteriores condições de resiliência, as estações de rastreio poderão então decidir sobre margens de segurança com que a informação de localização dos objectos-alvo pode ser armazenada e disponibilizada de forma confiável às aplicações finais, podendo mesmo aplicar diferentes heurísticas que podem ser mais ou menos especificamente definidas por parte de diferentes aplicações, de acordo com os seus requisitos. As margens de segurança são estabelecidas por métricas de intervalos de confiança (espaço-temporais), que não são mais do que parâmetros de QoT (*quality-of-trust*), fornecidos ao processamento das estações de rastreio, a partir de heurísticas definidas pelas aplicações finais. As métricas dos intervalos de confiança são baseadas por sua vez nos critérios e condições de confiança e por critérios e condições de mobilidade, tendo em conta a mobilidade máxima dos alvos.

4.1.5 Processamento de confiança e métricas de confiança das estações locais

Do ponto de vista do nível da estação de rastreio, as estações de localização devem ser inicialmente registadas. O registo das estações locais junto das estações de rastreio obriga à geração e distribuição de chaves criptográficas, usadas posteriormente pelas estações locais sempre que pretendam autenticar certificados de localização sobre objectos observados. Este processo depende das diversas tecnologias candidatas à interligação entre estações locais e estações centrais, podendo basear-se na emissão de certificados de chave pública para as estações locais ou na distribuição segura de chaves simétricas, com base num protocolo de autenticação e distribuição de chaves a partir de cada estação central de rastreio. De acordo com modelo arquitectural apresentado, esta interligação pode fazer-se com base em várias soluções e respectivas

normas de segurança, tal como foram apresentados no capítulo 3, nomeadamente:

- Redes celulares (com utilização dos mecanismos e serviços de segurança das redes GSM [17], comunicação GPRS [47] ou redes UMTS [56])

- Redes de área localizada ou pessoal sem fios (com base em comunicações seguras Bluetooth [4] ou com base nos serviços de segurança na normalização IEEE 802.15.4 [1] ou Zigbee [9])

- Redes locais sem fios (com base em suporte de comunicação IEEE802.11 e respectivas parametrizações de segurança)

- Suporte de comunicação *internet* com base nas parametrizações e configurações de segurança, de acordo com a normalização IPSec [80], bem como SSL [79] ou TLS [38]

Recorde-se que as estações locais podem estar equipadas com sensores de detecção e localização RFID (seja com base na tecnologia actual de RFID seja com base no suporte de identificação RFID suportado em dispositivos de redes de área pessoal, como são os casos de suporte sobre comunicação Bluetooth, IEEE 802.15.4 ou Zigbee). Admite-se que diferentes tecnologias envolvidas podem estar associadas a diferentes níveis ou condições de segurança e que tais condições estão na génese de diversas configurações ou parametrizações das soluções de interligação entre estações locais e estações de rastreio e que sejam utilizadas em cada caso.

A decisão final, por parte de uma estação de rastreio, sobre a localização de objectos-alvo identificados por estações locais na sua hierarquia, é assim baseada na combinação, durante o processo de agregação segura de dados provenientes de diferentes estações, entre (i) o grau de confiança de cada estação local no processo de localização e (ii) a tolerância espaço-temporal de informação de localização de um mesmo objecto-alvo durante o processamento do protocolo de agregação segura de dados, obtida a partir de um grupo de estações de localização consideradas e avaliadas como válidas, em função da amostra de dados de localização recolhidos.

Neste modelo nada obsta que a avaliação das condições associadas às métricas de confiança (quer em relação ao nível de confiança das estações locais, quer em relação ao número de amostras para um certo grau de confiança de localizações) possa ser feita com base em funções

de avaliação dinâmica do grau de confiança pretendido em função de parâmetros de disponibilidade e auditoria de operação do sistema [1].

4.2 Instanciação e concretização do modelo arquitectural proposto

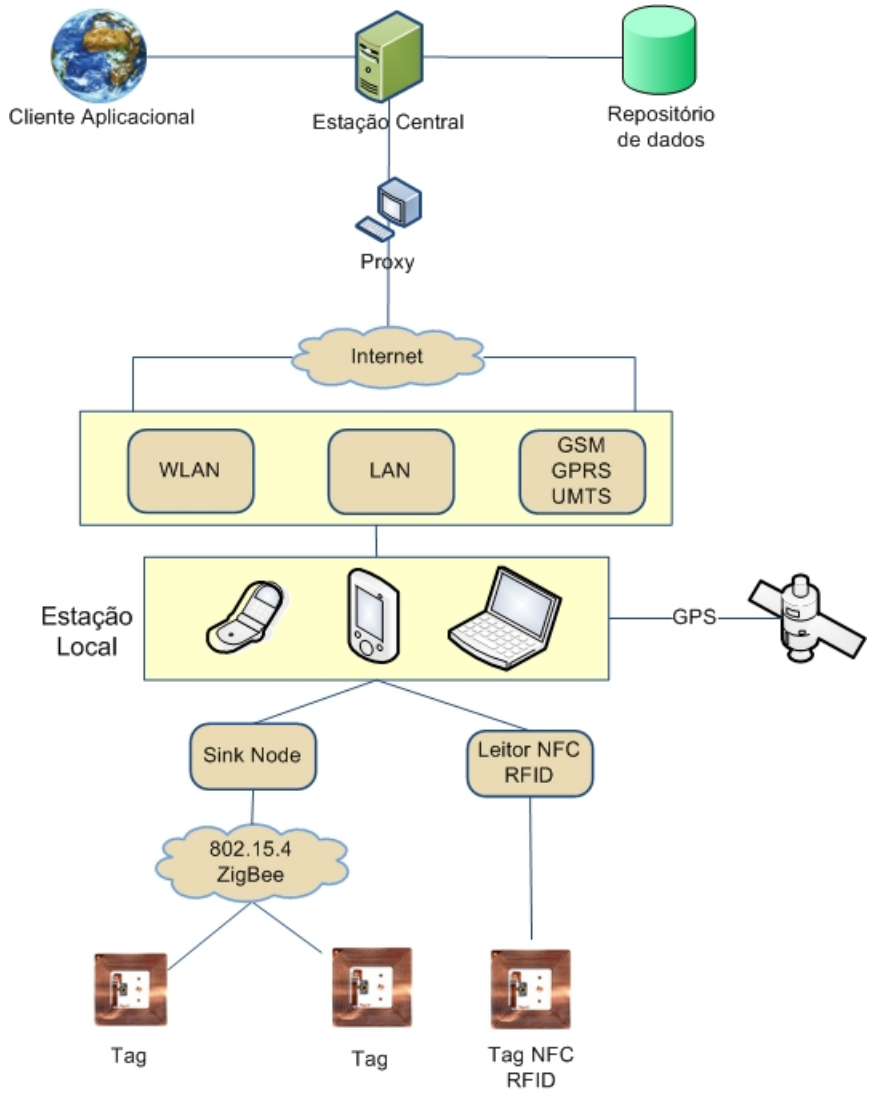

Figura 4.2 Diagrama instanciado da arquitectura

[1] Estes parâmetros devem ter em linha de conta o número e densidade de estações locais no espaço geográfico a monitorizar, bem como às condições de mobilidade que possam ser exigíveis.

Na figura 4.2 podemos observar a organização global da arquitectura, nas duas instâncias da visão apresentada. A arquitectura representada e descrita de seguida contém uma primeira instanciação da arquitectura na visão anteriormente descrita e que foi considerada como particularmente relevante para a concretização e avaliação da presente dissertação. Neste modelo da arquitectura os dispositivos RFID são modelados sob a forma de *tags* (ou etiquetas) materializadas por nós computacionais equipados para comunicação, com base na norma IEEE 802.15.4 (com a mesma tecnologia dos nós que actualmente se utilizam na área das redes de sensores sem fios).

Neste modelo, a localização de objectos-móveis faz-se então com base em comunicações por rádio frequência, que suportam o envio e recepção de identificadores RFID, segundo a normalização IEEE802.15.4 ou Zigbee. Os nós de detecção e captura da informação de identificação de *tags*, associadas aos objectos-alvo móveis, funcionam como *sink nodes* (SN), também eles concretizados por dispositivos IEEE 802.15.4 interligados com as estações locais (que podem assim ser materializadas por um vulgar computador portátil (do tipo *laptop*), um banal computador de mão (do tipo PDA) ou de um telefone móvel (*mobile phone* ou *smartphone*)), munidos de um sistema de localização por GPS. Estabelece-se assim uma concretização do nível conceptual de identificação e localização de objectos-alvo, tal como definido na arquitectura de referência indicada na anterior secção 4.1.

Interessa reter este modelo de concretização da arquitectura, já que o mesmo está na base de um cenário de aplicação de referência, bem como da concretização, implementação e avaliação experimental, tal como se discutirá mais à frente, no capítulo 5 da dissertação.

No modelo arquitectural anterior, as *tags* (ou etiquetas RFID) actuam como sensores que dispõem de capacidade autónoma para processarem identificadores, bem como para desempenharem protocolos, algoritmos e processos criptográficos. Estas *tags* são detectáveis por outros sensores, que actuam como dispositivos de captura dos identificadores que actuam como SN de redes de sensores, actuando como leitores associados às estações locais.

Cada dispositivo SN está pois interligado a uma estação local. Neste contexto, o leitor de *tags* RFID envia informação rádio para outros sensores que possam encontrar-se nas imediações e que actuam como *tags*, podendo autenticar-se perante os mesmos. As *tags*, por sua vez,

também podem anunciar a sua presença, logo que se movimentem dentro de um raio de alcance de dispositivos de localização estabelecidos pelos nós SN. Uma *tag*, que receba o pedido de leitura de um SN vai também poder responder a esse pedido, enviando informação de resposta, que poderá comprovar a sua identificação segura. Este modelo de concretização foi alvo de implementação e avaliação experimental com base em tecnologia de sensores Sun SPOT e comunicação 802.15.4, o que será apresentado mais à frente, no capítulo 5 da dissertação.

A arquitectura representada na figura 4.2 e descrita de seguida, contém uma segunda instanciação da visão apresentada, que foi igualmente considerada como importante para a concretização e avaliação da arquitectura.

Neste modelo os dispositivos RFID são modelados sobre a forma de *tags* RFID de baixo custo, com capacidades de *hardware*, em geral, bastante limitadas. A localização destes objectos faz-se então, com base em comunicação por rádio frequência de baixo alcance. Estabelece-se assim, de forma similar à instanciação anterior, o nível conceptual de identificação e localização de objectos-alvo.

Neste contexto, os nós de detecção RFID podem funcionar como dispositivos interligados a estações locais, munidas de sistemas de localização por GPS, ou serem eles próprios estações locais com capacidade de detecção e comunicação RFID, bem como de localização por GPS, podendo ser igualmente materializadas num vulgar computador ou em telefones móveis, nomeadamente em telefones com leitor NFC.

No âmbito desta instanciação, as *tags* são representadas pelas estações locais, na medida em que apenas possuem a capacidade de armazenar e transmitir identificadores. O processamento destes identificadores é realizado na própria estação local, que se encarrega de representar a *tag* perante as estações de rastreio, bem como de garantir as propriedades de segurança enunciadas na secção 4.1.1. Este modelo de concretização foi alvo de implementação e avaliação experimental, a partir de uma implementação da estação central com base num telemóvel equipado com NFC e leitura de etiquetas passivas RFID, o que será discutido mais à frente, no capítulo 5 da dissertação.

4.2.1 Preservação de condições de privacidade de objectos-alvo

De modo a salvaguardar a privacidade da informação de identificação de *tags*, a informação enviada para o leitor, apenas poderá ser lida por uma estação central de rastreio. A ideia de base, consiste no leitor poder detectar uma *tag*, mas não conseguir retirar informação do seu identificador, de modo a impossibilitar a realização de *tracking* não autorizado a objectos que detecta na sua vizinhança. Note-se que apenas ao nível da estação de rastreio se consegue ter acesso à informação de identificação persistente de *tags*.

Assim, cada *tag* possui um identificador persistente que apenas é do conhecimento da estação de rastreio, que actua na arquitectura como base de computação de confiança, contudo, durante a sua movimentação exibirá múltiplos identificadores contextuais e únicos (não reutilizáveis em mais do que uma identificação e localização) e que são os identificadores processados ao nível da identificação e localização de objectos-alvo e respectivas *tags*, por parte de estações locais.

Estes identificadores são dinamicamente gerados no processamento de autenticação extremo-a-extremo, entre as *tags* e a estação central de rastreio, embora sob intermediação das estações locais. Cada *tag* será assim identificada continuamente, ao longo do tempo, por uma cadeia de identificadores voláteis e únicos, autenticáveis, mas sem qualquer mapeamento conhecido, ao nível das estações locais, com o identificador persistente da *tag*, registado na estação central de rastreio.

4.3 Resumo dos serviços de segurança da arquitectura

Na secção 4.1, efectuou-se uma descrição de forma conceptual, da estrutura e organização da arquitectura, nomeadamente dos níveis de identificação e localização dos objectos-alvo, bem como do nível de agregação, controlo e armazenamento persistente de localizações. Para garantia das condições de segurança referidas para cada nível da arquitectura existem serviços de segurança, que lhe estão associados e que se passam a introduzir.

Relativamente, ao nível de identificação e localização, foram enunciadas as propriedades de segurança que se pretendem garantir e que são concretizadas através da realização de um

protocolo de autenticação, com duas variantes e uma extensão, que pretende adaptar-se à heterogeneidade dos diversos dispositivos que podem ser envolvidos na arquitectura.

Uma das propriedades fundamentais referidas, consiste na privacidade dos objectos-alvo que interagem na arquitectura, sendo necessário preservar o anonimato destes dispositivos. Para garantia destas premissas, um atacante através do identificador da *tag* não dispõe de meios da obtenção da sua informação pessoal, e acima de tudo não consegue efectuar *tracking* ao objecto, pois esse identificador tem um carácter contextual e não vinculativo aquele dispositivo. A geração dinâmica dos identificadores voláteis ou contextuais autenticáveis é realizada com a manutenção de propriedades de segurança passada e futura perfeitas, sendo essa geração realizada de forma independente e sem ter por base nenhum segredo partilhado entre a *tag* e qualquer estação local que proceda à sua localização. Este esquema visa garantir a privacidade do identificador persistente de cada objecto-alvo, identificado por qualquer *tag* e em qualquer instante.

Outra das propriedades mencionadas, consiste na autenticação dos objectos-alvo e estações locais, que se pode efectuar de forma mútua ou unilateral. No cenário de autenticação mútua é necessário que a *tag* possua a capacidade de realização de operações criptográficas, de modo que apresente a sua assinatura digital à entidade autenticadora. Neste contexto, foram introduzidas duas variantes do protocolo de autenticação, que garantem a autenticação mútua dos intervenientes e se adaptam às condições de mobilidade e segurança pretendidas. Estas variantes, bem como a extensão do protocolo, serão descritas em maior detalhe na secção 4.4.

Por outro lado, na presença de *tags* de baixo custo, a autenticação pode efectuar-se de forma unilateral, pois tal como apresentado anteriormente, as *tags*, regra geral, não dispõem de capacidades criptografias. Neste contexto, recorre-se à extensão do protocolo de autenticação, onde as *tags* são representadas pelas estações locais, que efectuam a sua autenticação perante a entidade autenticadora. Esta entidade no contexto do protocolo de autenticação é representada pelo *proxy*. As restantes propriedades de segurança mencionadas, nomeadamente confidencialidade e integridade dos dados, são asseguradas pela protecção criptográfica dos fluxos de mensagens nas diversas rondas do protocolo de autenticação.

Relativamente ao nível de agregação, controlo e armazenamento persistente de localizações, pretende-se a manutenção da garantia das propriedades mencionadas, numa perspectiva

extremo-a-extremo e a resistência face a informação incorrecta, introduzida por estações locais. Para tal, introduziu-se um serviço de segurança que pretende efectuar o processamento e validação da informação de localização introduzida pelas estações locais. A validação é efectuada através do cruzamento da informação dos certificados de localização emitidos por estações locais, relativamente a uma *tag* em concreto. Este processo será descrito em maior detalhe na secção 4.6. A validação é particularmente importante, na situação em que se recorre à extensão do protocolo, pois como a *tag* depende da estação local para se autenticar, a estação central não consegue obter uma garantia elevada, na real leitura daquela *tag*. Desta forma, a verificação da posição introduzida por aquelas estações, consiste num mecanismo adicional ao protocolo de autenticação, para certificação da autenticidade de leitura da *tag*.

4.4 Protocolo de autenticação

O protocolo de autenticação, proposto nesta arquitectura, visa, tal como o nome indica, garantir autenticação entre um leitor e uma *tag*. Possui duas variantes, uma completa e outra optimizada, que asseguram autenticação mútua, bem como níveis de privacidade distintos, consoante as condições de mobilidade pretendidas. Destinam-se a *tags*, cuja capacidade de processamento e armazenamento permite o envio de mensagens dinâmicas e autenticadas pelo próprio.

Adicionalmente, criou-se uma extensão ao protocolo, que visa interagir e autenticar *tags* (de forma unilateral) que não disponham da capacidade de envio de mensagens dinâmicas e cujo armazenamento é bastante limitado. Esta extensão do protocolo reduz a complexidade das mensagens, na medida que a interacção entre os intervenientes efectua-se de forma mais limitada.

Note-se que a informação relativa ao protocolo que esteja dependente de escolhas de implementação, nomeadamente o estabelecimento das chaves e identificadores, será descrita no capítulo 5, que apresenta a implementação do protocolo nas suas variantes.

De seguida, descreve-se o protocolo e o fluxo de execução do mesmo, na sua variante completa.

4.4.1 Propriedades de segurança da variante completa

Este protocolo garante as seguintes propriedades de segurança:

- Autenticação do leitor
- Autenticação da *tag*
- Privacidade da informação
- Privacidade da localização
- Forward Security (Segurança em interacções passadas)
- Backward Security (Segurança em interacções futuras)

4.4.2 Intervenientes no protocolo

Este protocolo realiza-se entre três entidades, *tag*, leitor e um *proxy*. A *tag*, responde a pedidos de identificação e recebe informação do *proxy* acerca do seu novo identificador volátil. O leitor actua como estação local, efectuando pedidos de autenticação e actua como intermediário entre a *tag* e o *proxy*, fornecendo as coordenadas de localização de leitura da *tag*. Por fim, o *proxy* actua como entidade que autentica a *tag* e o leitor, ficando ligado à estação central de rastreio. É igualmente responsável pela geração do novo identificador volátil a usar pela *tag*, no contexto de cada execução do protocolo de autenticação.

4.4.3 Mensagens do protocolo

De seguida procede-se a uma descrição inicial das mensagens do protocolo e seus objectivos, que está presente na tabela 4.1.

4.4.4 Notação na representação do protocolo de autenticação

A tabela 4.2 apresenta a notação usada na representação do protocolo de autenticação e formatação das mensagens.

4.4.5 Formato das mensagens

As mensagens trocadas entre os participantes, no contexto da variante completa do protocolo de autenticação, apresentam o formato indicado no seguinte quadro:

Mensagem	Descrição
M1	Mensagem enviada pelo leitor à *tag* (actuando como estação local) com a sua identificação, de modo a desencadear o protocolo de autenticação.
M2	Mensagem de resposta da *tag* ao leitor na sequência de M1. Contém informação de autenticação a apresentar ao *proxy*, bem como dados para geração de uma chave simétrica entre ambos.
M3	Mensagem enviada pelo leitor, que contém informação gerada por si e pela *tag*. A mensagem M3, inclui dados de autenticação do leitor perante o *proxy*, assim como informação acerca das coordenadas de leitura da *tag* RFID.
M4	Mensagem enviada pelo *proxy* em resposta à mensagem M3. A mensagem está dividida em duas partes, a primeira destina-se ao leitor e a segunda à *tag*. A parte da mensagem referente ao leitor contém informação sobre um desafio/resposta ao *proxy*. O leitor ao receber esta mensagem verifica que efectivamente se autenticou.
M5	Mensagem original criada pelo *proxy* e reenviada pelo leitor para a *tag*. Contém informação para criação da mesma chave de sessão gerada pelo *proxy*. Com esta chave, a *tag* consegue decifrar parte da mensagem, vinda do *proxy* e dessa forma, obter o seu novo identificador volátil. Quando a *tag* recebe a mensagem M5, certifica-se que foi autenticada perante o *proxy*.

Tabela 4.1 Descrição de cada mensagem do protocolo

Símbolo	Descrição
$\|\|$	Concatenação
$\{M\}Sig_{tag}$	Mensagem M assinada pela *tag*
$\{M\}Sig_{reader}$	Mensagem M assinada pelo leitor
$\{M\}Sig_{server}$	Mensagem M assinada pelo *proxy*
MD(M)	*Message Digest* da mensagem M
$K_{t,s}$	Chave de sessão simétrica utilizada entre *tag-proxy*
$E(K_{t,s}, [M])$	Mensagem M cifrada com a chave $K_{t,s}$
Time	*Timestamp*
id_T	Identificador volátil corrente da *tag*
$id_{T'}$	Novo identificador volátil da *tag*
subID_Static	Parte do identificador estático da *tag*
id_R	Identificador do leitor
$subKey_T$	Parte da chave utilizada pela *tag*
$subKey_R$	Parte da chave utilizada pelo leitor
N_1	*Nonce* criado pelo leitor com destino à *tag*
N_2	*Nonce* criado pela *tag* com destino ao *proxy*
N_3	*Nonce* criado pelo leitor com destino ao *proxy*
idType	Bit para escolha do tipo de verificação do identificador
Lat	Valor da Latitude
Lng	Valor da Longitude
$seed_T$	Semente criada pela *tag* para geração da chave de sessão
$seed_S$	Semente criada pelo *proxy* para geração da chave de sessão

Tabela 4.2 Legenda do protocolo de autenticação

4.4.6 Fluxo das mensagens

A relação temporal das mensagens trocadas entre os participantes nesta variante do protocolo de autenticação está presente na figura 4.3 e demonstra a divisão do protocolo de autenticação em três fases lógicas: identificação; autenticação; resposta à autenticação.

Na fase de identificação, o leitor procura por *tags* RFID que estejam no seu raio de alcance, através do envio de uma mensagem de iniciação do protocolo, que terá de ser respondida pela *tag*. Na segunda fase (autenticação), os intervenientes que procuram autenticar-se enviam

Mensagem	Formato
M1	$id_R \| N_1$
M2	$M2_{tag} \| MD(M2_{tag} \| N_1 + 1)$ $M2_{tag}$ = { idType $\|$ subKey$_T$ $\|$ seed$_T$ $\|$ Time $\|$ $id_R \| N_2 \| MD(id_T)$ }Sig_{tag}
M3	$M2_{tag} \| M3_{reader}$ $M3_{reader}$ = { $id_R \|$ subKey$_R \|$ Lat $\|$ Lng $\| N_3$ } Sig_{reader}
M4	$M4_{reader} \| MD(M4_{reader} \| N_3 + 1) \| M4_{tag} \| MD\ (M4_{tag} \| N_2 + 1)$ $M4_{reader}$ = { $N_3 + 1$ } Sig_{server} $M4_{tag}$ = { $id_R \| seed_S \| N_2 + 1 \| E(K_{t,s}, [id_{T'}])$ }Sig_{server}
M5	$M4_{tag} \| MD\ (M4_{tag} \| N_2 + 1)$

Tabela 4.3 Formato de cada mensagem do protocolo

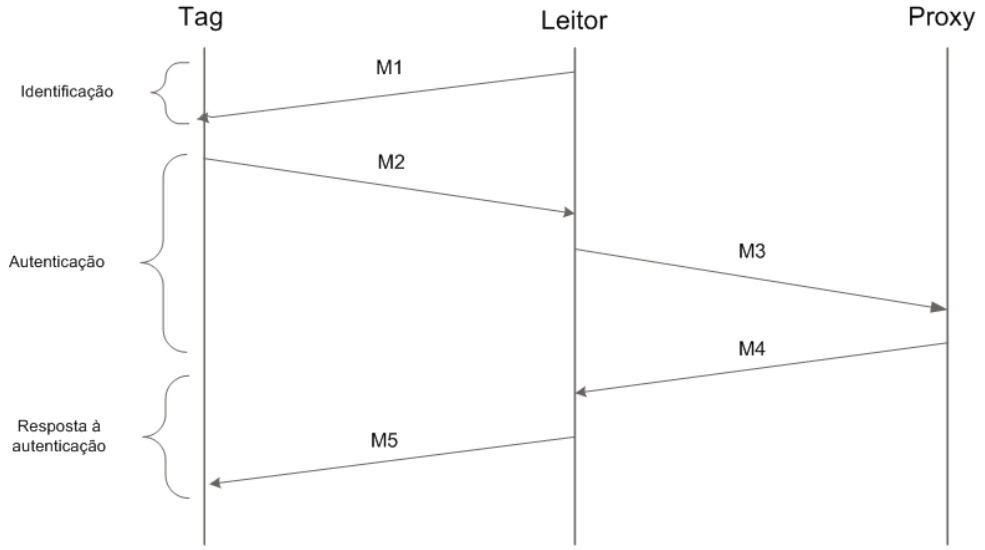

Figura 4.3 Fluxo temporal da variante completa do protocolo de autenticação

mensagens assinadas, de modo a serem validadas pelo *proxy*. Por último, na situação de autenticação com sucesso, o *proxy* envia mensagens de resposta para os restantes intervenientes do protocolo.

4.4.7 Descrição do protocolo

Nesta secção será aprofundada a apresentação do protocolo na secção 4.4.3, descrevendo-se agora em detalhe a finalidade dos parâmetros trocados em cada mensagem, bem como as verificações efectuadas e propriedades de segurança garantidas no protocolo. É de notar que a descrição efectuada, tal como a génese do protocolo apresenta um carácter genérico e refere-se

à variante completa do mesmo, cujos aspectos dependentes da sua concretização serão enunciados no capítulo de implementação. De seguida, descreve-se detalhadamente o fluxo de execução do protocolo de autenticação:

1. O leitor envia uma mensagem M1 por *broadcast*, para iniciação do protocolo de autenticação que contém o seu identificador e um *nonce*.

2. Uma *tag*, ao receber a mensagem anterior, responde com uma mensagem (M2), que será posteriormente encaminhada para o *proxy* aplicacional, de forma a se conseguir autenticar. Esta mensagem contém o tipo, valor do índice, semente para geração da chave de sessão, *timestamp*, identificador do leitor que iniciou o protocolo, um *nonce* e informação sobre o identificador da *tag*.

   A *timestamp* é utilizada para descartar mensagens recebidas, que se encontrem fora de um intervalo de tempo definido no sistema. O subKey_T pertence à mensagem, pois permite que através de parte da chave utilizada, seja possível alcançar com algumas tentativas a informação da *tag*, onde está incluída a informação sobre a sua chave.

   O identificador do leitor, também pertence à mensagem, com o intuito de garantir que a *tag* está a responder ao protocolo de autenticação iniciado por aquele leitor. Esta confirmação é essencial, pois é possível que existam inúmeros leitores, a procurar realizar o protocolo de autenticação, com as mesmas *tags*. A mensagem inclui ainda um *nonce*, de modo a prevenir ataques de *replaying* e informação que permite ao *proxy*, verificar qual o identificador volátil utilizado pela *tag*.

   Como os identificadores são refrescados, pode haver dessincronização, portanto a *tag* precisa de fornecer informação acerca do identificador volátil que utiliza, sem o expôr de forma clara na rede.

   As duas abordagens possíveis são: realizar um *digest* do identificador, de modo a não o expôr e criar dispersão nas mensagens ou em alternativa, utilizar filtros de bloom [24].

3. No momento em que o leitor recebe M2, cria uma mensagem para enviar ao *proxy* (M3) e concatena-a à mensagem recebida. A mensagem M3 é constituída pelas coordenadas geográficas de leitura da *tag* e informação para autenticação do leitor, perante o *proxy* e por fim, um *nonce*.

4. O proxy ao receber M3, extrai a parte da mensagem vinda da *tag*. Inicialmente, verifica se a *timestamp* encontra-se dentro do intervalo temporal até à data corrente, continuando o protocolo, caso a mensagem seja válida temporalmente. De seguida, no caso de sucesso da operação anterior, certifica-se de qual o tipo de verificação do identificador volátil que será efectuada.

   Com o conhecimento de parte da chave da *tag*, procura pela totalidade da informação das chaves, que corresponda ao índice dado. Caso a operação tenha sucesso, o *proxy* vai verificar a assinatura que está presente na mensagem. Se a assinatura for verdadeira, a *tag* pertence ao sistema e foi ele que assinou a mensagem. Caso contrário, a *tag* não se autenticou e o processamento do resto da mensagem termina.

   Como existe a possibilidade de dessincronização do identificador volátil, o *proxy* verifica qual deles está a ser usado. Para que a sua informação fique em concordância com a *tag*, actualiza se necessário, o histórico recente de identificadores voláteis utilizados.

   Após o processamento de parte da mensagem M3, vinda da *tag*, o *proxy* vai tratar dos dados produzidos pelo leitor. Esta mensagem contém o identificador que vai ser utilizado para indexar o dispositivo, no conjunto de leitores conhecidos pelo *proxy*. Como cada um, em teoria, pode possuir inúmeros pares de chaves, então é também fornecido uma parte da chave que utilizou, de modo que o *proxy* consiga indexar a chave correcta.

   Quando a chave é encontrada, o *proxy* certifica-se de que o leitor com esta informação pertence ao sistema e, em caso afirmativo, verifica a assinatura produzida por ele. Caso tenha sucesso, o leitor está autenticado perante o sistema. Após a autenticação, o *proxy* lê as coordenadas de leitura da *tag*.

   No caso do leitor e a *tag* estarem autenticados perante o *proxy*, este vai produzir uma mensagem resposta com destino final a ambos, como forma de se certificarem que foram realmente autenticados. O *proxy* para evitar a reutilização do identificador volátil da *tag*, actualiza-o para ser utilizado num posterior protocolo de autenticação. Igualmente, cria uma semente para geração da chave de sessão entre ele e a *tag*.

5. O *proxy*, tal como enunciado, gera uma mensagem M4 tendo como destinatário inicial o leitor, sendo dividida no conteúdo a ser lido pelo leitor e *tag*. A primeira parte da mensagem M4 ($M4_{reader}$), dirige-se ao leitor e contém o *nonce* enviado pelo ele, embora de forma incrementada, como resposta a M3.

A segunda parte da mensagem, dirigida à *tag* ($M4_{tag}$) é constituída pelo identificador do leitor, semente para geração da chave de sessão, a resposta ao *nonce* criado pela *tag* e um elemento cifrado. O identificador do leitor está incluído na mensagem, para que a *tag* tenha conhecimento de qual leitor obteve resposta do *proxy*, pois na *tag* pode existir mais do que um protocolo de autenticação pendente.

O elemento que transita cifrado na rede é o novo identificador volátil da *tag*, de modo que o leitor ou outros dispositivos não consigam efectuar *tracking* da *tag*.

A parte da mensagem M4 com destino à *tag* e leitor é assinada pelo *proxy*. Igualmente é efectuado um *digest* de cada parte da mensagem, como forma de verificação rápida da integridade da mensagem, por parte dos destinatários finais.

6. O leitor ao receber M4, apenas processa a parte da mensagem que lhe diz respeito. Verifica a sua integridade e em caso de sucesso, a assinatura efectuada pelo *proxy*. O leitor igualmente certifica-se de que o *nonce* enviado na mensagem M3, foi alterado de forma correcta. Caso todas as verificações ocorram com sucesso, reencaminha para a *tag* a parte da mensagem que lhe diz respeito.

7. A *tag* ao receber a mensagem M5, verifica a integridade da mesma e em caso de sucesso, a assinatura efectuada pelo *proxy*.

   Caso a verificação da assinatura ocorra com sucesso, conclui-se que ambos foram autenticados com sucesso pelo *proxy*. Através do processamento dos dados da mensagem, conhece o *nonce* que enviou (de forma incrementada) e a semente que será utilizada, para criar a chave de sessão, que lhe permite ler o restante conteúdo cifrado da mensagem.

   Após a geração da chave secreta, decifra o restante da mensagem e lê o novo identificador volátil que será utilizado, posteriormente, num novo protocolo de autenticação. Após a execução do protocolo, a *tag* actualiza o seu novo identificador, de acordo com o recebido pelo *proxy*.

   A privacidade da localização encontra-se garantida no protocolo, pois os identificadores voláteis utilizados são refrescados a cada autenticação e não transitam em claro na rede. A privacidade da informação também é garantida, na medida que através do conhecimento do identificador volátil não é possível obter informação adicional acerca da *tag*.

   Os identificadores voláteis utilizados pela *tag* nos sucessivos protocolos de autenticação não apresentam relação alguma entre si, assegurando-se dessa forma a segurança futura

perfeita ao nível dos identificadores, já que através de um deles, não é possível prever os anteriores ou posteriores identificadores utilizados. Note-se que o *proxy* apesar de estar encarregue de gerar os novos identificadores voláteis, também não tem conhecimento *a priori* dos futuros identificadores daquela *tag*, pois são gerados no momento e de forma totalmente aleatória.

As propriedades de segurança futura e passada asseguradas pelo protocolo que estão dependentes das parametrizações utilizadas, serão descritas na concretização do mesmo, no capítulo de implementação.

4.4.8 Variante optimizada do protocolo

O protocolo genérico apresentado possui propriedades de segurança futura perfeita, respeitante à distribuição e refrescamento de identificadores voláteis, pois não existe qualquer relação entre a cadeia de identificadores. Contudo, o fluxo de mensagens contempla uma resposta por parte do *proxy*, o que resulta num aumento da latência. Esta necessidade de resposta por parte do *proxy*, advém do facto de ser este componente o responsável pela geração e distribuição dos identificadores para as *tags* envolvidas nos sucessivos protocolos.

Desta forma criou-se uma variante optimizada do protocolo, que visa reduzir significativamente a latência do mesmo, o que por sua vez tem implicações na mobilidade das *tags*, através da geração dos identificadores voláteis de forma coordenada entre a *tag* e o *proxy*. Nesta variante deixa de ser necessário o envio do identificador por parte do *proxy*, eliminando-se as mensagens de resposta enviadas para o leitor e *tag*. A aproximação reduz a segurança futura perfeita ao nível dos identificadores, pois os próximos identificadores, apesar de não transitarem em claro na rede, são gerados em cadeia a partir dos anteriores.

De modo a combinar as duas variantes do protocolo e melhorar a relação latência/segurança futura perfeita, é possível utilizar um híbrido das duas aproximações. Esta variante híbrida ou mista, permite que a relação entre a cadeia de identificadores da variante optimizada seja desfeita, com a execução, em intervalos temporais da variante completa e mais segura do protocolo de autenticação. A cadeia de identificadores na variante optimizada é calculada através da utilização de um esquema de *one-time pad* (OTP), cuja chave é o identificador volátil e o elemento periódico é uma *timestamp*, que pressupõe uma sincronização de relógios entre os participantes,

podendo no entanto esta sincronização ser "*soft*", uma vez que é possível a re-sincronização dos identificadores, face a desvios pré-definidos.

Com esta aproximação híbrida, garante-se uma maior segurança, pois a relação entre os identificadores voláteis é agora temporária, embora à custa de um aumento da latência, no momento da utilização da variante completa. Desta forma, estabelece-se uma gestão de balanço entre desempenho do protocolo e as propriedades de segurança, de forma a obter o maior ganho possível nas duas variáveis. Esta abordagem pouco altera o formato e os campos da mensagens das duas variantes (completa e optimizada) do protocolo, sendo necessário parametrizar na *tag*, quanto à periodicidade de utilização da variante completa.

4.4.8.1 Fluxo das mensagens

Tal como enunciado na secção anterior, o *proxy* aplicacional não necessita de enviar uma mensagem de resposta ao leitor e *tag*. Desta forma, o formato das mensagens M1 e M2 permanece inalterado e as mensagens M4, M5 deixam de constar na variante optimizada do protocolo. Relativamente à mensagem M3, deixa de ser necessário a presença do campo seed_T, pois como a *tag* gera o identificador volátil, não necessita de criar uma chave de sessão para decifrar o identificador recebido do *proxy*, como acontece na variante completa.

De qualquer modo, apesar da *tag* não receber mensagem da parte do *proxy*, para que tenha uma confirmação da recepção da mensagem enviada para o leitor, este responde-lhe com uma mensagem M6, que apresenta o seguinte formato:

- $\text{M6} = \text{id}_R \parallel \text{N}_1 + 2$

Desta forma, altera-se o fluxo das mensagens em relação à variante optimizada, podendo ser visualizado na figura 4.4.

4.4.8.2 Descrição da variante do protocolo

Anteriormente foi referido que o formato da mensagem M1 permanece inalterado. Contudo, no campo *idType* existe uma *flag* que indica qual a variante do protocolo a utilizar.

O fluxo das mensagens na versão optimizada inicia-se, tal como descrito anteriormente com o envio da mensagem M1 por parte do leitor e a consequente resposta com a mensagem M2, por parte da *tag*. No momento em que o leitor recebe esta mensagem, cria a mensagem M6 a

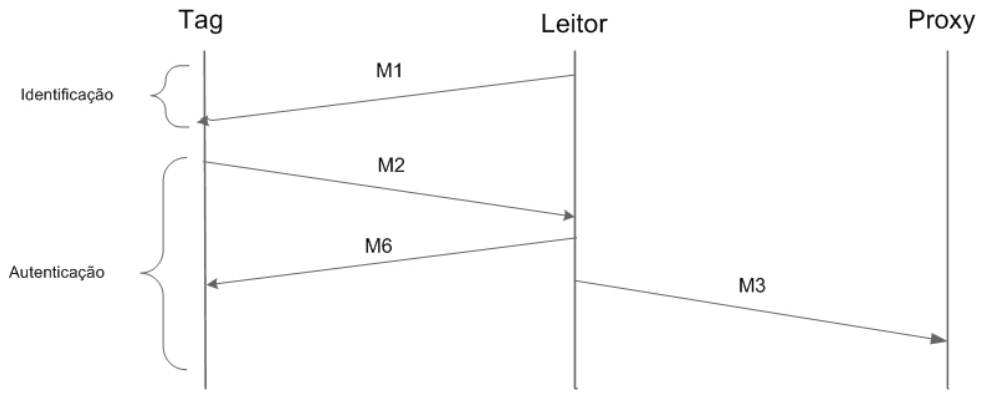

Figura 4.4 Fluxo temporal da variante optimizada do protocolo de autenticação

ser enviada para *tag*, que contêm o seu identificador, de modo que a *tag* tenha conhecimento de qual leitor está a receber a resposta à identificação, bem como uma nova resposta ao desafio anteriormente processado pela *tag*. O leitor ao enviar a mensagem M6, cria a mensagem M3 e envia para o *proxy*, de forma equivalente ao descrito anteriormente.

O *proxy* ao receber a mensagem verifica através da leitura do *idType*, que está ser utilizada a versão optimizada do protocolo e desse modo prepara-se convenientemente para analisar o restante conteúdo da mensagem. Como o *proxy* consegue aceder à informação da *tag*, tem acesso ao identificador corrente, que é utilizado como chave no esquema de OTP e dessa forma dispõe de todos os dados necessários para actualizar o identificador utilizado pela *tag*.

Numa situação de dessincronização do identificador da *tag*, o *proxy* efectua um determinado número de tentativas com os identificadores voláteis que conhece para aquela *tag*, para sincronização do identificador utilizado. Caso o identificador recebido não esteja na lista de identificadores voláteis conhecidos e que ainda não foram utilizados pela *tag*, realiza um determinado número de tentativas com identificadores futuros que a *tag* irá gerar. Se ainda assim o *proxy* não conseguir encontrar o identificador da *tag*, pode efectuar tentativas com *timestamps* anteriores ou posteriores à utilizada correntemente. Caso este mecanismo tenha sucesso, indica que o relógio do *proxy* e *tag* encontram-se dessincronizados e nessa altura, o *proxy* para aquela *tag*, passa a utilizar a *timestamp* adequada, face ao desvio temporal.

O processamento restante de todo o conteúdo da mensagem M3 é idêntico ao enunciado anteriormente. Após o processamento com sucesso, o *proxy* não envia mensagem de resposta

ao leitor, pois na versão optimizada do protocolo, a *tag* gerou de forma coordenada o novo identificador volátil, a ser utilizado no próximo protocolo de autenticação em que intervenha aquela *tag*.

4.4.9 Extensão ao protocolo para opção de autenticação unilateral de *tags*

O protocolo de autenticação contempla uma extensão que visa permitir a autenticação unilateral de *tags*, quando estas não dispõem da capacidade de enviar mensagens dinâmicas. Estes dispositivos no contexto do protocolo, unicamente respondem a *queries* efectuadas pelos leitores, através do envio do identificador volátil. De forma a refrescar esse mesmo identificador, o leitor procede igualmente a uma substituição do mesmo na *tag*. O refrescamento do identificador é realizado pelo leitor e *proxy*, com base no esquema de geração de senhas OTP dinâmicas, cuja chave é o identificador volátil da *tag* e o elemento periódico é uma *timestamp*.

4.4.9.1 Formato da mensagem

A mensagem gerada pelo leitor, que contém a informação do identificador volátil da *tag* e dados geográficos da leitura, apresenta o seguinte formato:

- M = { id_R || subKey_R || Lat || Lng || N_3 || subID_Static || $\mathrm{MD}(\mathrm{id}_T)$ || Time} $\mathrm{Sig}_{\mathrm{reader}}$

4.4.9.2 Descrição do protocolo

A extensão do protocolo de autenticação contempla a leitura e escrita de identificadores de *tags* RFID, que apenas armazenam informação de identificação, processando-se da seguinte forma:

1. O leitor pesquisa por *tags* RFID que estejam ao seu alcance. Ao detectar algum dispositivo, lê a informação do identificador volátil presente na *tag*.

2. O leitor gera um novo identificador volátil e substitui na *tag* o identificador corrente.

3. O leitor cria uma mensagem para enviar ao *proxy* que contém todos os dados presentes na mensagem M3, descrita anteriormente. Adicionalmente, contém informação sobre uma parte do identificador estático da *tag*, que será utilizado como indexação da informação da *tag*. A mensagem contém ainda um *digest* do identificador volátil e uma *timestamp*. Esta informação no protocolo anteriormente descrito, era gerada e transmitida pela *tag*,

contudo, nesta situação as *tags* não dispõem da capacidade de responder dinamicamente a pedidos do leitor e por essa razão não conseguem gerar mensagens com a informação a ser lida. Desta forma, o leitor inclui na mensagem a enviar para o *proxy*, a informação de identificação do dispositivo RFID.

4. O *proxy* ao receber a mensagem verifica se é válida temporalmente e em caso afirmativo, continua o processamento da mesma. De seguida indexa a informação relativa à *tag*, através de parte do identificador estático fornecido. Em caso de sucesso, verifica o identificador volátil utilizado pela *tag*, sendo que, em caso de dessincronização é necessário a realização de um determinado número de tentativas, de modo a determinar qual o identificador volátil utilizado pela *tag*. O restante processamento da mensagem efectuado pelo *proxy* é idêntico à referida mensagem M3.

4.4.10 Comparação com outros protocolos

	Protocolos de autenticação					
	[69]	[77]	[82]	[20]	[63]	Protocolo Proposto
Privacidade da informação	Sim	Sim	Sim	Sim	Sim	Sim
Privacidade da localização	Sim	Sim	Sim	Sim	Sim	Sim
Autenticação da *tag*	Sim	Sim	Sim	Sim	Sim	Sim
Autenticação do leitor	Sim	Sim	Sim	Sim	Sim	Sim
Forward Security	Sim	Sim	Sim	Não	Sim	Sim

Tabela 4.4 Comparação das propriedades de segurança garantidas entre o protocolo de autenticação proposto e os apresentados no trabalho relacionado

A tabela 4.4 expõe uma comparação das propriedades de segurança, a diversos níveis, do protocolo apresentado em relação aos protocolos expostos no trabalho relacionado. Através da sua observação é possível concluir que o protocolo implementado cumpre os requisitos de segurança dos protocolos estudados.

Contrariamente aos restantes protocolos estudados, apresenta uma flexibilidade de utilização, pois é possível adaptar a versão do protocolo a utilizar, tendo em conta as capacidades de autonomia energética, capacidade da computação e latência da comunicação. Esta característica será demonstrada, quando forem descritas as diferentes versões do protocolo de cariz genérico, apresentado atrás. Igualmente, a componente de testes no capítulo 6 demonstrará que os requisitos de computação de cada versão são bastante distintos entre elas.

Note-se que a propriedade de *Backward security* não consta na tabela, por falta de dados para comparação com os protocolos do trabalho relacionado.

4.5 Condições de mobilidade dos alvos

O protocolo de autenticação apresentado na secção anterior impõe uma restrição na mobilidade da *tag*, pois a mobilidade depende da latência do completamento do protocolo. A figura 4.5 demonstra as condições de mobilidade previstas para a interacção entre uma *tag* e leitor. Na secção de testes, referente a este tema (6.2.1.3), as condições serão concretizadas para as diversas implementações do protocolo de autenticação.

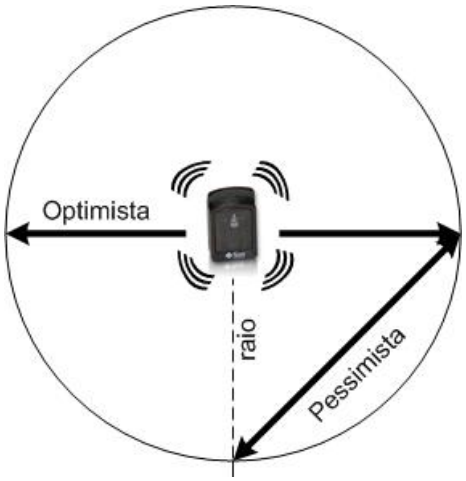

Figura 4.5 Condições de mobilidade

No modelo previsto, existe a possibilidade de uma *tag* encontrar-se em movimento na altura do protocolo de autenticação e nesse cenário, a *tag* e o leitor têm que estar ao alcance um do outro via-rádio, até que o protocolo termine. Esse alcance é representado pelo circulo traçado à volta do leitor.

De qualquer forma, não se prevê *a priori* qual a distância que a *tag* irá percorrer, estando ao alcance do leitor. Desta forma é possível adaptar uma abordagem optimista ou pessimista, conforme se considere que a distância percorrida pela *tag* é máxima ou mínima (segundo as condições de mobilidade), respectivamente.

No caso optimista, a *tag* atravessa o raio de alcance do leitor exactamente no seu centro, ou

seja a *tag* percorre todo o diâmetro do círculo. Na situação pessimista, a *tag* atravessa o círculo por uma das suas cordas. Essa corda, definiu-se como a hipotenusa (h) do triângulo formado pelos catetos, que correspondem ao raio do circulo. Nestas duas situações a distância que a *tag* percorre, dentro do raio de alcance do leitor é distinto. Se o diâmetro do circulo corresponder a um valor d, a distância da corda é:

$$h = \sqrt{\left(\frac{d}{2}\right)^2 + \left(\frac{d}{2}\right)^2} \tag{4.1}$$

Para cada uma destas situações, existe um valor médio de velocidade que a *tag* pode apresentar no momento da autenticação, sendo esse cálculo efectuado da seguinte forma:

$$Velocidade = \frac{\text{Distância}}{\text{Tempo}} \tag{4.2}$$

4.6 Processamento com agregação e consenso de localização geográfica de objectos

Nas secções seguintes conclui-se a apresentação dos serviços de segurança na arquitectura proposta com o mecanismo de processamento com agregação e consenso de localização geográfica. Como inicialmente se apresentou, este mecanismo visa dotar a arquitectura de tolerância a falhas ao nível das estações locais (ou leitores RFID) ou melhoria de resistência da arquitectura, face a operação incorrecta das estações locais e leitores RFID devida a ataques por intrusão. Passa-se a descrever a preparação inicial dos dados que são considerados elegíveis como correctos pelo consenso da localização geográfica, assim como uma descrição do funcionamento do consenso, na fase de escolha dos leitores e definição da localização final ao nível da estação central de rastreio.

4.6.1 Resistência do sistema face a estações locais incorrectas

Na situação em que um atacante forje um leitor e interaja com a *tag*, ao enviar a informação para o sistema, vai ser detectado que o leitor não é válido (por não estar registado) e nesse caso a informação enviada será descartada. O atacante pode também decidir forjar uma *tag* RFID. Nesse caso, quando essa *tag* for lida por um leitor válido, a informação vai ser enviada para

o sistema, contudo não será validada, pois a autenticação por parte da *tag* não poderá ser feita com êxito. Similarmente, o protocolo de autenticação detecta a situação em que tanto o leitor como a *tag* são forjados por um atacante e não possam ser autenticados no sistema.

Ainda assim, um leitor previamente registado e devidamente autenticado no sistema pode efectuar um ataque ao nível da localização, com anúncio de localizações falsas ou incorrectas sobre a posição de um objecto. De modo a resistir a esse ataque, efectua-se uma validação das coordenadas de localização enviadas pelos leitores. A ideia subjacente a este processo consiste em validar a informação recebida por um leitor autenticado, através do conhecimento que o sistema tem sobre a localização desse objecto, recebida por outros leitores, de acordo com uma avaliação espaço-temporal que permita detectar informação incorrecta.

Assim, no momento em que o sistema apresente registos de localização respeitantes à mesma *tag*, procede-se ao cruzamento de dados para verificar possíveis discrepâncias ao nível da informação. Este processo de validação das localizações é descrito à frente, no ponto 4.6.4.

Devido a poderem surgir falsos positivos na detecção de um impostor, é estabelecido um número de tentativas por estação ou leitor para inserção de informação falsa. À medida que a estação de rastreio contabilize um comportamento acumulado de anúncio de falsas localizações ou que possa inferir sobre a falsidade da informação introduzida por um leitor, através de um número máximo de detecções de informação incorrecta ou através da detecção de uma localização correcta por parte de uma estação considerada confiável, condiciona a colocação de informação no sistema, quer através do protocolo de autenticação, quer através da invalidação das posições geográficas.

4.6.2 Preparação dos dados para estabelecimento do consenso

A preparação dos dados elegíveis para o consenso ocorre após o término do protocolo de autenticação com sucesso.

Para se iniciar o consenso e dependendo do nível de resiliência, é necessário garantir a existência de vários dispositivos que sejam capazes de efectuar a detecção de uma *tag* RFID, dentro de um intervalo espaço-temporal, calculado e parametrizado na aplicação em função das condições de mobilidade dos alvos (tal como anteriormente se representa na figura 4.5). O critério de elegibilidade dos dados recebidos baseia-se na reserva de um afastamento temporal, que seja bastante superior ao tempo necessário para efectuar o protocolo de autenticação, de

modo a poder agrupar diferentes registos da mesma *tag*, efectuados por diferentes leitores (actuando ao nível de estações locais).

De forma similar, calcula-se um espaço geográfico no qual, tendo em conta um registo conhecido, as localizações dos restantes registos tenham que se encontrar no interior desse espaço, para que sejam consideradas como verdadeiras. A selecção de uma posição, como informação para o cálculo de posição final, depende da percentagem de votos positivos, recebidos pelos restantes registos envolvidos no consenso, obtidos a partir das diferentes estações e leitores.

O intervalo geográfico tem em conta o valor estipulado para o raio de alcance dos dispositivos, assim como o erro da informação de localização que é obtida pelos leitores. Adicionalmente, o intervalo é influenciado pelo deslocamento possível, efectuado pela *tag*, durante o intervalo para se poder realizar o consenso. Este deslocamento é condicionado pela velocidade máxima de acordo com o modelo admissível de mobilidade, pois é assim garantido que se detecte a *tag* e se conclua o protocolo de autenticação.

No essencial, o mecanismo consiste num descarte primário das localizações que são efectivamente falsas. Simultaneamente, pretende-se não condicionar em demasia o intervalo geográfico a verificar, de modo a obter um número mínimo de falsos positivos. Um elevado número de falsos positivos, respeitante a um determinado registo de um leitor, pode condicionar a adição temporária de novos registos que venha a efectuar.

À medida que os registos produzidos pelos leitores chegam à estação central, vão ser tratados tendo em conta a informação dos consensos que estão pendentes, existindo vários tratamentos a efectuar na preparação e agregação dos dados. A primeira situação surge quando não existe nenhum consenso pendente para aquela *tag*. Neste caso, cria-se um novo consenso, sendo esta informação, inicialmente, o único registo. Outra situação ocorre quando já existe um consenso para aquela *tag*, embora o intervalo temporal, tendo em conta o primeiro registo desse consenso, já não permita que estes dados sejam manipulados por esse consenso, que ainda se encontra pendente. Nesta situação, é criado um novo consenso para essa *tag*, que irá ser executado após o consenso anterior. Esta situação pode ocorrer, pois caso a estação central esteja com alguma sobrecarga podem existir consensos cuja informação de *input* já se encontra num estado final, embora ainda não tenham sido processados pela estação.

Adicionalmente, podem ainda ocorrer duas situações para novos registos quando já existe

um consenso, cujos dados ainda não se encontram no seu estado definitivo, ou seja, ainda podem ser incluídos novos registos a esse consenso. A primeira dessas hipóteses ocorre quando se detecta a existência de leituras para a mesma *tag*. Nessa situação é adicionado um registo dessa *tag*, realizada por um leitor diferente dos registos anteriores.

Outro cenário, verifica-se quando um leitor efectua sucessivos protocolos de autenticação sobre a mesma *tag*. Nesse caso, os dados de localização que obteve vão ser pré-agregados, de modo que apenas um registo daquela *tag*, efectuado por aquele leitor, seja manipulado no consenso. Esta opção foi tomada pois não se perspectiva interesse para uma aplicação final, a existência de inúmeros registos, dentro de um espaço geográfico e temporal diminuto, efectuados por um mesmo leitor. No momento em que a estação central detecta que a informação mais antiga presente num consenso já igualou um espaço temporal definido na aplicação, procede-se, assim que seja possível pela estação, à execução do consenso.

4.6.3 Aspectos de parametrização do consenso geográfico

O consenso inclui algumas parametrizações que importa referir, pela sua importância na decisão de validação do mesmo. A primeira parametrização relaciona-se com a validade do registo de uma posição, efectuada por um leitor. Para que seja considerada válida, necessita de obter o rótulo de verdadeira por uma percentagem de leitores (parametrizada na aplicação) presentes neste consenso.

Da mesma forma, um consenso também necessita de ser tornado válido, portanto, para as suas decisões se repercutirem no repositório de dados, exige-se que a percentagem de leitores considerados verdadeiros seja no mínimo equivalente a um valor considerado como válido no sistema. Esta restrição é importante, pois se os leitores considerados como verdadeiros existem em número bastante diminuto, então a informação de localização a ser processada pelo consenso teve que ser muito díspar entre eles. Nessa situação, existem poucos leitores cujos dados de localização encontram-se na mesma vizinhança geográfica. Perante este cenário, como o sistema não consegue ter confiança nos resultados obtidos, tomou-se a opção de retirar todas essas leituras duvidosas da informação do sistema.

Como existe a possibilidade de enfrentar leitores maliciosos, ou que não se apresentem nas melhores condições e possam prejudicar o sistema, contabiliza-se o número de registos

que não foram considerados como verdadeiros no protocolo de autenticação, pelos respectivos leitores. No momento em que o número de incorrecções de localização inseridos no sistema pelos leitores superar o patamar definido pelo mesmo, ficam impedidos (ou apenas condicionados) de injectar dados, pois já não considerados como dispositivos de confiança.

Por último, após o cálculo da posição final, com base nos registos recebidos dos leitores, pode efectuar-se uma validação dessa posição com a informação presente no repositório, que apenas pode ser efectuada de acordo com um intervalo temporal definido na aplicação. Desta forma, torna-se necessário definir esse limite temporal para validação da posição final, com o último registo armazenado, pois ultrapassado esse limite, não é expectável prever em que espaço temporal a *tag* teria que estar no momento do registo.

A validação da informação recebida, com a do repositório, efectua-se através de uma verificação com a última informação de consenso, conhecida acerca da respectiva *tag*. Este registo de consenso, por seu turno, já foi comparado com o último registo existente na data da sua inserção.

Note-se que para aplicar uma validação adicional com a informação presente no repositório e que diga respeito aquela *tag* é necessário conhecer o trajecto efectuado ou os trajectos possíveis que a *tag* pode efectuar. Apenas dessa forma é possível prever um espaço geográfico onde a *tag* deveria estar, com grande probabilidade.

4.6.4 Descrição e definição do consenso

A descrição do funcionamento do consenso geográfico, processa-se após a preparação e pré-agregação das localizações registadas pelos leitores e divide-se em duas fases: (i) selecção dos leitores considerados como verdadeiros e (ii) escolha da localização final.

Na primeira fase, são seleccionados todos os leitores cujos registos de localização são considerados verdadeiros. Um leitor é colocado nesse estado, caso a distância geográfica compreendida entre o seu e os restantes registos de localização se situar no interior do espaço geográfico admitido pelo sistema. É exigido igualmente que a comprovação da veracidade seja obtida por uma percentagem de leitores superior à mínima admitida pelo sistema.

A selecção dos leitores, cuja informação de localização será processada no consenso, procura

garantir que apenas sejam manipulados e agregados os dados cujas coordenadas geográficas estiverem dentro do padrão das restantes localizações.

Após a selecção dos leitores considerados como verdadeiros, avalia-se as coordenadas de localização resultantes, de modo a definir uma posição geográfica final, a registar como definitiva no sistema. Para tal, procede-se a uma avaliação da confiança de cada leitor, cujas métricas foram descritas na secção 4.1.5.

Na tomada de decisão da posição final, são consideradas todas as posições registadas pelos leitores considerados como verdadeiros. Os que apresentem confiança superior, terão um maior peso na localização, de modo que todos os leitores possam contribuir. Em suma, o objectivo pretendido consiste na combinação mais justa dos dados registados pelos leitores considerados como verdadeiros.

Após a recolha da informação de localização introduzida pelos leitores considerados como verdadeiros, procede-se à fase da decisão da posição final de leitura da *tag*. Esta posição é calculada através da utilização da fórmula do centro de massa para polígonos [13]. De todo o modo, a sua aplicação, tal como é conhecida, não contempla o cálculo ponderado através dos valores de confiança conhecidos, dos pontos considerados como verdadeiros. Desse modo, procedeu-se a uma separação dos pontos em categorias, de acordo com a confiança, para que seja possível aplicar a fórmula do centro de massa, a cada grupo formado por nível de confiança.

O processo da escolha da localização inicia-se com o ponto cuja confiança é a mais baixa e posteriormente, com os restantes pontos elegíveis para a construção do polígono. Os pontos elegíveis para cada etapa do consenso são aqueles cuja confiança é igual ao ponto seleccionado. Caso não existam pontos com igual confiança, seleccionam-se todos cuja confiança esteja num patamar acima da confiança do ponto inicial seleccionado.

A construção do polígono é efectuada através de uma parte do método Graham Scan [44] para cálculo do *convex hull* de um polígono simples. Essencialmente, este método, de acordo com um conjunto de pontos, constrói um polígono, efectuando uma escolha do ponto inicial. Seguidamente, seleccionam-se de forma ordenada os pontos seguintes, através um varrimento radial efectuado pelo ponto inicial.

Após a construção do polígono pelo referido método, efectua-se o cálculo do seu centro de

massa como localização escolhida para aquele conjunto de pontos. O ponto resultante substitui, no cálculo da posição final do consenso, os pontos utilizados para a construção do polígono. Deste modo, procede-se a um refinamento sucessivo da posição final, através dos pontos processados até ao momento.

O processamento do consenso termina, após a não existência de pontos adicionais a serem utilizados no cálculo do consenso. Os pontos com menor confiança são os primeiros a serem utilizados no cálculo da posição, para que a sua influência seja menor do que aqueles que possuem um maior crédito de confiança perante o sistema. O objectivo do cálculo da posição baseia-se na consideração de todos os pontos verdadeiros, privilegiando no entanto a informação de localização obtida através de dispositivos cuja confiança seja superior.

5 . Implementação da arquitectura

Neste capítulo aborda-se a implementação prática da arquitectura e os desenvolvimentos práticos associados. Apresenta-se o *hardware* e o ambiente de desenvolvimento de *software*, bem como as tecnologias que foram utilizadas na implementação da arquitectura. Adicionalmente, são descritos os módulos da arquitectura, bem como informação sobre detalhes de implementação do protocolo de autenticação e suas variantes, bem como do mecanismo de consenso geográfico para tolerância a falhas e resistência a intrusões, ao nível de estações locais e leitores RFID.

5.1 Concretização da arquitectura e protótipos para sua instanciação

A arquitectura implementada refere-se directamente às duas instanciações do modelo conceptual, enunciadas na secção 4.2.

Relativamente à primeira instanciação da arquitectura, os dispositivos RFID que funcionam como *tags*, são materializadas por sensores e micro-controladores com capacidades de comunicação por rádio frequência, segundo a norma IEEE 802.15.4. Por outro lado, os nós associados às estações de localização são materializados por sensores IEEE 802.15.4, ligados a um computador portátil. Na concretização prática do protótipo de implementação, os dispositivos RFID correspondem a dispositivos Sun SPOT, e os nós de detecção por *sink nodes* Sun SPOT, com ligação USB a um computador portátil.

Em relação à segunda instanciação da arquitectura, implementou-se um protótipo em que as *tags* correspondem a *tags* RFID de baixo custo (ou etiquetas passivas) e os nós de detecção por telefones móveis Nokia 6212 NFC equipados com leitura de etiquetas passivas RFID. Note-se que na arquitectura implementada, este tipo de dispositivo encontra-se interligado à estação local, materializada por um computador portátil através de bluetooth, embora o próprio telefone pudesse ser utilizado como estação local autónoma.

Como se referiu, de forma transversal às duas concretizações práticas da arquitectura, a estação local, *proxy* e estação central foram implementadas com recurso a um computador portátil. Como se poderá ver no capítulo de testes, para a realização de testes experimentais à latência do protocolo, a estação local, o *proxy* e a estação central foram implementados com recurso a

máquinas distintas.

Como o computador tipo que implementa a estação local não dispõe de localização por GPS, utilizou-se um telemóvel Nokia 5800 que fornece as coordenadas geográficas à referida estação, através de comunicação por Bluetooth. À frente serão apresentadas as características e dados completos sobre o *hardware* e *software* utilizados nos protótipos experimentais que foram implementados e avaliados.

5.2 Fluxos de informação na arquitectura

No primeiro cenário de implementação, envolvendo os sensores Sun SPOT, o leitor que tem o papel de *sink node* (SN), encontra-se periodicamente à procura de sensores que representam *tags* RFID (*tags* 802.15.4) que estejam "visíveis" nas áreas circundantes, através do envio de mensagens de iniciação do protocolo de autenticação. Uma *tag* ou sensor 802.15.4 que receba essa mensagem, inicia então o protocolo de autenticação, podendo fazê-lo, segundo a sua parametrização, com recurso à variante completa ou optimizada do protocolo, ambas implementadas neste protótipo. Após o sensor responder ao pedido do leitor e dar inicio ao protocolo, este processa-se entre a *tag*, leitor e a estação local, de acordo com a variante do protocolo em cada caso.

Tal como referido na descrição do protocolo de autenticação, na secção 4.4, o leitor necessita de introduzir as coordenadas de localização de leitura da *tag*. Nessa situação, como o leitor não dispõe de capacidades de GPS, efectua um pedido de localização à estação central, que ou dispõe de localização geográfica pré-configurada (quando simula uma estação fixa), ou conhece dispositivos que lhe possam fornecer essa informação dinâmica (quando simula uma estação móvel). No cenário colocado em prática, devido a restrições de *hardware*, a estação local não dispõe de GPS. Como tal, na modelação de uma estação móvel envia um pedido de localização a um telefone móvel, que dispõe dessa capacidade e que no protótipo implementado é um telefone Nokia modelo 5800.

No cenário concretizado, a rede de sensores (constituída como base de suporte entre as tags e as estações locais de localização) funciona como uma rede *broadcast* (*one hop only*). Uma

tipologia de redes de sensores mais densas, com topologia em malha (*mesh*) ou com características por difusão *multi-hop*, não foram cobertas na fase de implementação da dissertação. De qualquer modo, existem algumas abordagens de localização que poderiam fornecer maior precisão à localização nessas tipologias de rede. Na primeira abordagem possível, poderiam existir nós de localização espalhados numa rede de sensores que actua como ambiente de monitorização e que possuem informação de localização [34]. Estes nós são designados por nós de verificação de posição (ou *verifiers*). Os restantes nós de uma rede de sensores, para determinarem a sua posição, efectuam pedidos de localização aos nós *verifier*. Cada sensor que actue como leitor calcula a sua posição final, através de um método denominado por multilateração.

Por outro lado também é possível obter dados de localização, através da informação recebida de sensores circundantes que actuam como *beacon nodes* [62]. O sensor que pretende saber a sua posição, espera durante um determinado intervalo de tempo, de modo a obter assinaturas que contêm a intensidade de sinal do emissor. A posição final é calculada com base na avaliação da distância de Manhattan das assinaturas recebidas.

As anteriores abordagens de obtenção da localização são suportadas quando um leitor faz parte de uma infraestrutura de rede de sensores circundantes, que pode ser desenvolvida (ou *deployed*) de forma aleatória e auto-organizada, de acordo com os processos usuais em redes de sensores não supervisionadas para monitorização de eventos. Estas posições podem depois ser convertidas em localizações GPS, ao nível da estação local que está ligada a um nó de captura de informação (ou *sink node*). Uma tal topologia de redes de sensores, a ser utilizada, deverá cobrir toda a área previsível de mobilidade de *tags*.

Note-se que a tipologia de sensores sem fios com comunicação baseada nas normas IEEE 802.15.4 ou Zigbee, actualmente disponíveis (e nomeadamente as utilizadas na dissertação), não dispõem habitualmente de suporte GPS ou A-GPS. Desta forma necessitam que a informação de localização lhes seja fornecida por um elemento circundante, com quem consigam comunicar, de modo a obter coordenadas de posição associadas a coordenadas geográficas ou que possam ser mapeadas em coordenadas GPS ou A-GPS ao nível da estação local.

No segundo cenário de implementação, que envolve dispositivos com tecnologia NFC, a interacção entre *tag* e leitor apenas pode ser efectuada a poucos centímetros de distância. Desta forma, dá-se inicio ao protocolo de autenticação, no momento em que uma *tag* passiva NFC

está próximo do leitor NFC implementado por um telefone móvel Nokia 6212 NFC. Tal como na situação dos sensores, o protocolo de autenticação processa-se entre *tag*, leitor e *proxy*. Contudo, nesta situação em particular, recorre-se à extensão do protocolo de autenticação, tal como descrito na secção 4.4.9. A informação de localização requerida pelo protocolo efectua-se de forma similar aos sensores, com o pedido do leitor à estação local materializada num computador portátil, que por sua vez, recorre a um telefone Nokia 5800 através de comunicação por Bluetooth para obtenção de coordenadas de localização. O conjunto do leitor NFC baseado num telefone Nokia 6212, o computador portátil e o telefone Nokia 5800, simulam assim uma estação móvel para localização de etiquetas RFID.

Em ambos os cenários de implementação, após o término com sucesso do protocolo de autenticação, o *proxy* envia para a estação central, informação de identificação persistente da *tag* e leitor, que foram alvo do protocolo, bem como as coordenadas de localização introduzidas durante o processamento do mesmo.

A estação central, encontra-se continuamente à espera de novos certificados de leitura autenticados e enviados pelo *proxy*. No entanto, apenas inicia o consenso geográfico, quando estiverem reunidas as condições para tal, de acordo o descrito no capítulo 4, nomeadamente na secção 4.6.2.

Após a realização do consenso, a estação central armazena a informação resultante da sua execução no repositório de dados. Esta informação fica disponível para visualização, através de um mapa, ao utilizador da aplicação final, actuando esta aplicação como um demonstrador de prova de conceito, sendo uma aplicação do tipo GIS. Esta aplicação é descrita em maior detalhe na secção 5.5, ponto 5.5.10.

5.3 Hardware utilizado

Descrevem-se de seguida as características do *hardware* utilizado nos protótipos de implementação da arquitectura.

Sun SPOT

Este dispositivo é constituído por três componentes principais: (i) bateria, (ii) *board* principal com processador, memória , rádio e interface USB e (iii) *board* de sensores.

A *board* principal é constituída essencialmente por:

- 180 MHz 32 bit ARM920T core
- 512K RAM/4M Flash
- 802.15.4 radio
- Interface USB
- Bateria ião-lítio de 3.7V e capacidade de 720mAh

A *board* de substrato que integra os sensores incluí os seguintes sensores:

- Acelerómetro de 3 eixos
- Sensor de luz
- Sensor de temperatura

Figura 5.1 Sun SPOT e seus componentes

O rádio incluído nos Sun SPOTs implementa a norma IEEE 802.15.4, que opera na gama dos 2.4 GHz e têm um menor custo, tendo porém potência inferior aos *standards* Bluetooth ou Wi-Fi. De momento não existem implementações de dispositivos Sun SPOT para comunicação segundo a normalização Zigbee. O suporte de comunicação destes sensores apresenta as seguintes características:

- *Frames* 802.15.14 com 128 bytes
- Alcance de cobertura de rádio em linha de vista de cerca de 70m
- Velocidade de transmissão de 250 Kbps
- Transmissão na banda de frequência de 2.4GHz

O sensor utilizado como *sink node* nesta dissertação, apenas inclui a *board* com processador rádio. Não necessita de bateria, pois é ligado ao computador através de uma porta USB e recebe por este meio a energia necessária.

Telemóvel: Um dos telemóveis utilizados nesta dissertação é um dispositivo Nokia 5800, cujo processador é um ARM 11 a 434MHz e tem como sistema operativo o Symbian OS v9.4, Series 60. Este dispositivo contém um receptor GPS e apresenta diversas formas de conectividade. Possui Wi-Fi 802.11 b/g, bluetooth v2.0 e 3G a 3,6Mbps.

Computador: O computador utilizado nesta dissertação é um computador usual e tem como sistema operativo o Windows 7 de 32 bits. Utiliza um processador com dois núcleos e contém 3GB de memória e 320GB de disco rígido.

Telemóvel com leitor NFC: O telemóvel utilizado na extensão do protocolo de autenticação é um Nokia 6212 NFC. Tem a capacidade de ler e escrever informação em vários tipos de *tags* NFC, e possui uma bateria de 1000 mAh. Utiliza o sistema operativo Symbian Series 40 e dispõe de bluetooth e GPRS. A informação sobre a especificidade do processador utilizado pelo dispositivo não é disponibilizada pela Nokia.

Figura 5.2 Nokia 6212 NFC

5.4 Software e tecnologias utilizadas

5.4.1 JAX-WS

JAX-WS [12] é uma API Java para WebServices em XML para criação de web services que está presente na plataforma Java EE. A implementação principal da tecnologia está disponível

em *open source*.

5.4.2 Mysql

MySQL é uma base de dados em *open source*, com suporte a multi-utilizadores. Proporciona o acesso a várias bases de dados por um utilizador e possui, entre outras características, a capacidade de efectuar *commit* em grupo e suporte a múltiplas transacções, por parte de vários utilizadores.

5.4.3 PHP

Hypertext Preprocessor, vulgarmente denominado por PHP, consiste numa linguagem de *script* desenvolvida para a produção de páginas dinâmicas e desenvolvimento *web*.

5.4.4 Apache

Apache é um servidor HTTP que suporta o conteúdo de páginas estáticas e dinâmicas. De modo a garantir segurança em transacções HTTP, dispõe de um módulo que permite suportar o protocolo HTTPS.

5.4.5 Google Maps

O Google Maps consiste num serviço de pesquisa e visualização de mapas. Incluí igualmente imagens de satélite e rotas para diversos países. Possibilita através do acesso por uma conta à criação de rotas, pontos, áreas, etc. Com o recurso a um arquivo KML é possível integrar as funcionalidades do Google Maps no Google Earth. Este suporte foi integrado no demonstrador de uma aplicação GIS que foi desenvolvido no âmbito da implementação e validação dos protótipos.

5.4.6 J2ME

A plataforma J2ME consiste numa versão reduzida da máquina virtual J2SE, aplicada a dispositivos com capacidade limitada. A decisão da escolha desta tecnologia nos dispositivos móveis,

utilizados nesta dissertação, foi influenciada pela forte integração e heterogeneidade de comunicação suportada pelos dispositivos utilizados. Esta tecnologia possibilitou a implementação dos módulos aplicados, nos telemóveis e nos sensores Sun SPOT. Estes em particular incluem uma máquina virtual J2ME reduzida, denominada por Squawk, que executa directamente no processador, sem a necessidade de um sistema de operação.

A plataforma J2ME possibilitou igualmente a implementação da extensão do protocolo de autenticação, realizado no telemóvel Nokia 6212 NFC, pois recorrendo ao JSR 257 é possível interagir com *tags* NFC.

5.5 Módulos da arquitectura

Nesta secção efectua-se uma descrição dos módulos criados no contexto da arquitectura, enunciando alguns detalhes concretos de implementação.

5.5.1 Estação central

A estação central tem a missão de gerir o conteúdo do repositório, utilizando o conector JDBC para consultar e manipular a informação da base de dados. A estação suporta igualmente as *queries* efectuadas pelo cliente da aplicação final e processa o consenso, através da informação recebida pelo *proxy*. Este transmite a informação para a estação central, por um WebService disponibilizado, nomeadamente através da invocação do método *insertRegistryRFID*. Utiliza Apache e PHP para disponibilizar o ambiente Web e possibilitar a realização de *queries* à base de dados MySQL por parte do cliente da aplicação.

À medida que a estação recebe conteúdo vindo do *proxy*, prepara a informação recebida para ser processada pelo consenso. Simultaneamente, insere os registos na base dados, invocando o método *insertRegRFID*.

Na fase de inicialização descrita em 5.6.1, a estação central regista a informação das novas *tags* e dos leitores, através da invocação dos métodos *insertTag* e *insertReader*.

5.5.2 Segurança

Este módulo suporta as operações de segurança utilizadas pela implementação do protocolo de autenticação, apresentado em 4.4. As operações fornecidas podem ser decompostas essencialmente, em sínteses de mensagens (com *secure hashing*), assinaturas de mensagens (com base em operações criptográficas do tipo MAC - *Message Authentication Codes* que podem usar sínteses seguras (HMAC) ou algoritmos criptográficos simétricos (ou CMACs), bem como operações de cifra/decifra de mensagens. Este suporte utiliza ainda implementações de acordos de distribuição de chaves com base em algoritmos assimétricos (RSA ou ECC), bem como assinaturas RSA ou ECDSA, bem como geração de chaves de sessão temporárias com implementação de acordos de Diffie Hellman baseado em ECC (ECC-DHE). Estas operações são utilizadas por diversos elementos da arquitectura, nomeadamente pelos componentes *proxy*, leitor e *tag*.

Para a assinatura/verificação de mensagens no protocolo recorre-se à classe genérica *Signature*. Relativamente a operações de *hashing* de mensagens, utiliza-se a classe *MessageDigest*, nomeadamente através das parametrizações SHA-1 ou MD5. Para cifra e decifra dos elementos utilizados, para geração da chave de sessão ou protecção do envio do identificador volátil, utiliza-se a classe *Cipher*.

Como explicado acima, utilizou-se criptografia simétrica e/ou assimétrica em diversas operações do protocolo (podendo as *ciphersuites* ser configuradas para os protocolos implementados, usando-se diferentes dimensões de chaves ou blocos). Para operações com criptografia simétrica utiliza-se a classe *Key*, contudo, para operações com criptografia assimétrica, existem especificações diferenciadas para RSA ou curva elíptica (ECC). No caso de RSA, as chaves públicas e privadas são implementadas com recurso às classes *RSAPublicKey* e *RSAPrivateKey*, respectivamente. Por ultimo, para operações com chaves de curva elíptica, utiliza-se as classes *ECPublicKeyImpl* e *ECPrivateKeyImpl*, respectivamente.

Este módulo suporta as operações de segurança utilizadas pela implementação do protocolo de autenticação, apresentado em 4.4. As operações fornecidas podem ser decompostas essencialmente, em *hashing*, assinatura ou cifra/decifra de mensagens. Estas operações são utilizadas por diversos elementos da arquitectura, nomeadamente pelo *proxy*, leitor e *tag*.

Para assinatura/verificação de mensagens no protocolo recorre-se à classe genérica *Signature*. Relativamente a operações de *hashing* de mensagens, utiliza-se a classe *MessageDigest*,

nomeadamente através das parametrizações SHA-1 ou MD5. Para cifra e decifra dos elementos utilizados, para geração da chave de sessão ou protecção do envio do identificador volátil, utiliza-se a classe *Cipher*.

5.5.3 Proxy

O *proxy* é o componente que efectua a ligação entre a estação local e a estação central. Comunica com base em SOAP, com o servidor implementado na estação central como um serviço WEB (ou WebService). O protocolo ao nível do *proxy* executa-se enviando os dados de autenticação invocando o método *insertRegistryRFID*. De forma similar, o *proxy* fornece um WebService à estação local, para que tenha a capacidade de receber a informação gerada pelo leitor e pela *tag*. A estação local transmite os dados de autenticação, para o *proxy*, invocando o método denominado por *authInfo*.

Durante o processo de autenticação, o *proxy* manipula os dados vindos da *tag* e do leitor, utilizando os métodos *authenticateTag* e *authenticateReader*, respectivamente. No caso de autenticação com sucesso, gera a mensagem de resposta pelo método *authenticateResponse*. Os dados são devolvidos à estação local, através do retorno do método *authInfo*.

5.5.4 Bluetooth

Este módulo efectua uma pesquisa de dispositivos que disponham de comunicação por bluetooth activa. A procura é efectuada por um *array* de atributos definidos e por um identificador do serviço UUID.

5.5.5 Localização

O módulo de localização encontra-se instalado no dispositivo móvel com capacidades GPS e bluetooth, mais concretamente num telefone Nokia 5800. Inicialmente, efectua-se uma procura por dispositivos vizinhos, nas condições apresentadas na secção anterior. Após a ligação ao dispositivo móvel por bluetooth é possível interagir com o módulo de localização. Este módulo, captura as coordenadas de localização por GPS, definindo a precisão pretendida e o *timeout* da recepção das coordenadas.

Os dispositivos que pretendam preparar-se para receber informação GPS por este módulo, necessitam de efectuar a ligação, através do método *requestChannel*. Nos instantes em que

necessitem de um refrescamento das coordenadas geográficas, invocam o método *requestLocation*, sendo essa informação enviada por bluetooth.

5.5.6 Estacao local

Este elemento da arquitectura funciona como intermediário entre o leitor e o *proxy*. Se o leitor estiver mapeado num *sink node* Sun SPOT, a ligação entre os dois faz-se por USB. Por outro lado, para o leitor concretizado no telefone móvel Nokia 6212 NFC, a ligação entre os dois faz-se por bluetooth. A estação local tem também a missão de capturar informação de localização, a fornecer ao leitor e pode opcionalmente apresentar capacidades de aquisição de localização. Nessa situação não necessita de utilizar o módulo bluetooth, mas apenas de utilizar o módulo de localização. No caso de não possuir essa capacidade, utiliza o módulo de pesquisa por bluetooth, para encontrar dispositivos na vizinhança que lhe possam fornecer o serviço de localização.

A estação local encontra-se ligada ao leitor, logo, este componente tem a responsabilidade de colocar na arquitectura a informação gerada e capturada pelo leitor. Como a estação local comunica directamente via *proxy*, nomeadamente através do WebService disponibilizado, reencaminha a informação resultante do protocolo de autenticação para o leitor. Se este e/ou a *tag* não se autenticarem perante o *proxy*, a estação local reencaminha uma mensagem de erro, para que nenhum desses dispositivos fique à espera da informação de autenticação.

5.5.7 Leitor Sun SPOT

Este módulo da aplicação, utiliza as operações de segurança no protocolo de autenticação, descritas na secção 5.5.2. De forma equivalente ao módulo da *tag*, tem a particularidade de utilizar o protocolo 802.15.4, descrito no capítulo 3 (secção 3.3.2), para envio de mensagens rádio. Este leitor como tem o objectivo de desencadear um protocolo de autenticação, inicia a descoberta de *tags* que estejam no seu raio de alcance, enviando mensagens *broadcast*. Para tal, recorre ao seguinte código:

Listing 5.1 Envio de pacotes pelo leitor

```
1
2 RadiogramConnection sendCon = (RadiogramConnection) Connector.open("
     radiogram://broadcast:" + control.getHOST_PORT());
3 Datagram dg = sendCon.newDatagram(control.getDatagramSize());
```

```
4 sendCon.send(dg);
```

Para recepção das mensagens de resposta vindas da *tag*, utiliza o seguinte código:

Listing 5.2 Recepção de pacotes pelo leitor

```
1
2 RadiogramConnection radioConn = (RadiogramConnection) Connector.open("
    radiogram://:" + control.getHOST_PORT());
3 Datagram recDg = radioConn.newDatagram(radioConn.getMaximumLength());
4 radioConn.receive(recDg);
```

5.5.8 Tag Sun SPOT

Este módulo encontra-se implementado no sensor Sun SPOT, que tem a função de *tag* na arquitectura. Tal como o módulo anterior, recorre às operações do módulo de segurança (ver secção 5.5.2), de modo a assegurar as propriedades do protocolo de autenticação enunciadas no capítulo 4 (secção 4.4.1).

A *tag* recebe pacotes vindos do leitor, no momento da iniciação do protocolo de autenticação e quando o leitor termina de processar/autenticar a mensagem vinda do *proxy*. Para receber o conteúdo desses pacotes, a *tag* utiliza o seguinte excerto de código:

Listing 5.3 Recepção de pacotes pela tag

```
1
2 RadiogramConnection rCon = (RadiogramConnection) Connector.open("radiogram
    ://:" + HOST_PORT);
3 Datagram dg = rCon.newDatagram(rCon.getMaximumLength());
4 rCon.receive(dg);
```

No momento em que a *tag* recebe pacotes vindos de um leitor, gera a mensagem de autenticação (M2) e envia para o leitor. O processo de envio da mensagem resposta ao leitor, via rádio é efectuado da seguinte forma:

Listing 5.4 Envio de pacotes pela tag

```
1 Datagram dgreply = rCon.newDatagram(rCon.getMaximumLength());
2 rCon.send(dgreply);
```

5.5.9 Leitor NFC

Este módulo da arquitectura encontra-se implementado num telefone Nokia 6212 NFC, interagindo com a *tag* NFC. Relembra-se que esta *tag* não consegue gerar mensagens dinâmicas, respondendo apenas com informação por ela armazenada. Desta forma, o leitor NFC gera mensagens autenticadas por si, com informação de leitura da *tag*. Tal como o Sun SPOT utilizado como leitor, recorre ao modulo de segurança, por forma a assinar digitalmente as mensagens e interage com *tags* NFC, nomeadamente através da leitura do identificador e escrita do novo identificador volátil gerado por ele próprio.

A leitura do identificador volátil da *tag*, processa-se da seguinte forma:

Listing 5.5 Leitura do identificador volátil

```
protected String readNDEFPayload(TargetProperties[] detectedTarget){
    NDEFTagConnection conn = null;
    for (int i = 0; i < detectedTarget.length; i++) {
        if (detectedTarget[i].hasTargetType(TargetType.NDEF_TAG)) {
            try {
                String url = detectedTarget[i].getUrl(Class.forName("javax.
                   microedition.contactless.ndef.NDEFTagConnection"));
                conn = (NDEFTagConnection) Connector.open(url);
                NDEFMessage message = conn.readNDEF();
                NDEFRecord record = message.getRecord(id_Record.getBytes())
                   ;
                if(record == null){
                    new NFCUtil().showAlert("Error", "record é nulo !",
                       display, 2000, form);}
                conn.close();
                return new String(record.getPayload());
                ...
```

A escrita do novo identificador é realizada da seguinte forma:

Listing 5.6 Escrita do identificador volátil

```

private void WriteNdefWithConn(String url, String payload) {
        NDEFTagConnection conn = null;
        try {
            conn = (NDEFTagConnection) Connector.open(url);
        } catch (IOException e1) {
```

```
7               new NFCUtil().showAlert("ERROR", "Cannot create
                    NDEFTagConnection", mDisplay, 2000, form);
8               e1.printStackTrace();}
9           if(conn!=null){
10              try {
11                  NDEFRecordType myType2 = new NDEFRecordType(NDEFRecordType.
                        NFC_FORUM_RTD,
12                          "urn:nfc:wkt:T");
13                  NDEFRecord myRec2 = new NDEFRecord(myType2, EchoConstants.
                        ID_RECORD.getBytes(), payload.getBytes());
14                  NDEFRecord[] myRecArray = new NDEFRecord[] { /*myRec, */
                        myRec2 };
15                  NDEFMessage myMessage = new NDEFMessage(myRecArray);
16                  conn.writeNDEF(myMessage);
17                  conn.close();
18                  new NFCUtil().showAlert("Info", "New ID Written !",
                        mDisplay, 2000, form);
19                  ...
20      }
```

5.5.10 Aplicação

Foi implementada uma aplicação na qual o utilizador tem ao seu dispor um conjunto de mecanismos que permitem filtrar a informação a ser exibida num mapa, de acordo com os dados disponíveis no repositório. Estes mecanismos tornam possível a visualização de registos de uma ou várias *tags* RFID, dentro de um espaço temporal e /ou espacial.

Cada posição é colocada no mapa, através de um *placemark* colorido, em que as cores correspondem a graus de confiança que a estação central tem em cada posição representada.

A aplicação permite efectuar interrogações à base de dados (através do conector para mysql, disponível para PHP), que são traduzidas numa tabela de registos referente à pesquisa efectuada e principalmente em *placemarks* com informação do consenso de localização processado. As interrogações que se podem realizar à base de dados podem conter filtros de *tags*, *timestamps* ou intervalos geográficos. Para efectuar a ligação à referida base de dados recorre-se ao seguinte código:

Listing 5.7 Ligação à base de dados

```
$connection=mysql_connect ('localhost', $username, $password);
```

O cliente aplicacional realiza inúmeras *queries* que são aplicadas na base de dados por este método:

Listing 5.8 *Queries* à base de dados

```
          $result = mysql_query($query);
```

Uma das acções mais relevantes do cliente aplicacional consiste na colocação de *placemarks* no google maps. Contudo, a informação da base de dados necessita de ser convertida para XML, para depois ser possível colocar no referido visualizador geográfico.

Para criar as *tags* XML com a informação vinda da base de dados, o cliente recorre ao seguinte código:

Listing 5.9 Informação do *placemark* vindo da base de dados

```
while ($row = @mysql_fetch_assoc($result)){
                    echo '<marker ';
  echo 'lat="' . $row['avg_latitute'] . '" ';
  echo 'lng="' . $row['avg_longitute'] . '" ';
  echo 'id_tag="' . $row['id_tag'] . '" ';
  echo 'date_read="' . $row['first_date_read'] . '" ';
  echo 'id_reader="' . $row['id_reader'] . '" ';
  echo '/>';
}
echo '</markers>';
```

Os dados XML acima gerados são colocados no mapa através do seguinte excerto de código:

Listing 5.10 Inserção de dados no mapa

```
var xml = GXml.parse(data);
var markers = xml.documentElement.getElementsByTagName("marker");

for (var i = 0; i < markers.length; i++) {
  var id_reader = markers[i].getAttribute("id_reader");
    var name = "name";
    var address = "addr";
    var type = "type";
  var id_tag = markers[i].getAttribute("id_tag");
  var date_read = markers[i].getAttribute("date_read");
```

```
11      insRow(markers[i].getAttribute("lat"), markers[i].getAttribute("lng"),
            id_tag, date_read, id_reader);
12    var point = new GLatLng(parseFloat(markers[i].getAttribute("lat")),
13                            parseFloat(markers[i].getAttribute("lng")));
14    var marker = createMarker(point, name, address, type);
15    map.addOverlay(marker);
16  }
```

5.6 Protocolo de autenticação

O protocolo de autenticação descrito na secção 4.4 abarca as variantes optimizada e completa que são utilizadas pelos sensores Sun SPOT, bem como uma extensão do protocolo, que é utilizada pelo telefone móvel Nokia 6212 NFC. Nas secções seguintes são descritos aspectos de inicialização do protocolo de autenticação, assim como detalhes de implementação do mesmo.

5.6.1 Inicialização e aspectos de parametrização

A arquitectura implementada tal como concebida, prevê a introdução de novos leitores e *tags* numa fase inicial de desenvolvimento e operacionalização da mesma ou dinamicamente durante o tempo de funcionamento do sistema. Por esse motivo, especifica-se a fase de *setup* ou inicialização de cada um dos dispositivos, que se encontra intrinsecamente ligado ao processo de autenticação e do mecanismo de processamento de consensos de localização, bem como às condições globais de segurança a considerar.

O protocolo de autenticação possui um carácter genérico, e está concebido para ser concretizado em várias configurações. As diferenças de configuração residem essencialmente no tipo de criptografia a utilizar. Por configuração, na implementação actual pode usar-se criptografia assimétrica (RSA ou curva elíptica), bem como criptografia simétrica, podendo usar-se cifra em cadeia com RC4 ou cifra em bloco com AES.

No cenário em que se recorre a criptografia assimétrica é criado um par de chaves RSA ou de curva elíptica para o dispositivo, quer seja uma *tag* ou leitor. Dessa forma, as *tags* ficam com conhecimento do seu par de chaves, ao invés do componente que actua como estação central,

que apenas regista e conhece as chaves públicas correspondentes dos leitores e *tags*. De forma similar, os dispositivos que operem como leitores ou *tags* (à excepção da *tag* NFC), ficam com conhecimento de uma das chaves públicas da estação central, caso esta disponha de vários pares de chaves válidas.

Relativamente à utilização de criptografia simétrica, é partilhada uma chave simétrica ao nível da estação central e da *tag*, bem como ao nível da estação central e do leitor. Estas chaves são utilizadas durante o processo de assinatura e geração de uma chave de sessão, no contexto protocolo de autenticação. É de realçar que a *tag* NFC não possui capacidades criptográficas e como tal, não se procede à geração de chaves para a mesma, não desempenhando qualquer processamento criptográfico.

Independentemente da variante ou extensão do protocolo, se estivermos a realizar a inicialização de uma nova *tag*, gera-se um identificador volátil e coloca-se no dispositivo. A estação central fica com conhecimento do identificador estático (que actuará como identificador único e persistente da *tag*) e do pseudo-identificador da *tag* (que actuará como identificador volátil único em cada processo de autenticação e localização da *tag*).

5.6.2 Desenvolvimento e concretização do protocolo

O protocolo de autenticação, tal como referido, é constituído por uma variante completa e optimizada, bem como uma extensão do protocolo, que diferem no conteúdo e fluxo das mensagens trocadas entre os participantes.

Relativamente à variante completa, na abordagem com curva elíptica, utiliza-se o par de chaves criado para assinar a mensagem e enviar para o *proxy*. Esta mensagem contém o elemento semente para geração da chave de sessão, que consiste na utilização do método de distribuição de chaves de Diffie-Hellman (DH) para curva elíptica. Desta forma, o sensor gera um par de chaves de curva elíptica e envia na mensagem assinada por ele o valor público de DH, armazenando o valor secreto de DH.

O *proxy* ao receber a mensagem da *tag* utiliza a chave pública de curva elíptica da *tag*, para verificação da sua autenticidade. No caso de verificação com sucesso, gera de forma similar à *tag*, um par de chaves de curva elíptica, utilizada na geração da chave de sessão. Esta chave é gerada pelo *proxy*, utilizando o valor público DH enviado pela *tag* e o valor privado de DH gerado por si. Este processo é igualmente efectuado pela *tag*, utilizando o seu valor público

de DH e o valor privado de DH recebido na mensagem enviada pelo *proxy*. Esta mensagem é assinada pelo *proxy* e verificada pela *tag*, utilizando a chave pública colocada na *tag*, na fase de inicialização que foi descrita na secção anterior.

A utilização do método de DH para geração da chave de sessão, fornece uma garantia de segurança futura perfeita, pois as diversas chaves de sessão geradas pelo mesmo par <*tag*,*proxy*> não apresentam relação entre si. Desta forma, caso um atacante consiga descobrir a chave de sessão utilizada, não consegue prever a nova chave de sessão a utilizar ou as chaves de sessão anteriormente geradas, logo, não consegue decifrar o novo identificador volátil da *tag*.

A abordagem com chaves RSA, ainda relativamente à variante completa, assemelha-se à utilização de curva elíptica à excepção dos elementos semente a utilizar, para geração da chave de sessão. Desta forma, o processo de assinatura e verificação da mensagem apenas varia no tipo de chaves a utilizar, que neste caso são de RSA. O processo de geração da chave com RSA inclui a criação de um *pre-master-secret* (PMS), cifrado com a chave pública do *proxy*. Este ao receber o PMS, utiliza-o para geração do *master-secret* (MS), que será a última semente a utilizar para geração da chave. O MS transita na rede cifrado com a chave pública da *tag*, de modo que apenas o destinatário consiga decifrar o MS. De forma análoga, o *proxy* e a *tag* utilizam o MS para geração da chave de sessão.

Por último, foi utilizada uma abordagem que não utiliza criptografia assimétrica e recorre aos algoritmos AES e RC4. As mensagens que transitam na rede são assinadas pelo emissor e verificadas no destinatário, através da geração de um CMAC, cuja chave utilizada corresponde à chave simétrica corrente, partilhada entre os participantes. O refrescamento da chave é efectuado de forma similar ao método com RSA, utilizando PMS e MS. Contudo, a cifra desses elementos é efectuada pela chave de sessão corrente e não pela chave pública do destinatário, como no método com RSA.

Esta abordagem do protocolo não apresenta garantia de segurança perfeita, pois caso um atacante obtenha acesso à chave de sessão, consegue decifrar os segredos PMS, MS e dessa forma gerar ele próprio a nova chave de sessão. De qualquer forma, o atacante não consegue reproduzir as chaves de sessão utilizadas em sessões passadas do protocolo de autenticação. Com a obtenção da chave de sessão, um atacante pode igualmente assinar e verificar a assinatura de mensagens, pois o CMAC utilizado necessita da chave de sessão corrente.

A variante optimizada, por seu turno, elimina algumas das operações de segurança efectuadas pela variante completa, nomeadamente a geração da chave de sessão, verificação da assinatura do *proxy* e decifra do novo identificador volátil.

A extensão do protocolo de autenticação utiliza as mesmas operações de segurança que recorre a variante optimizada. De todo o modo, neste contexto a *tag* não gera mensagens, ou seja, as operações de segurança são aplicadas apenas pelo leitor NFC.

5.7 Consenso geográfico e visualização dos dados

A arquitectura de localização segura de *tags* RFID efectua a autenticação de dispositivos RFID e consenso geográfico, com o intuito de registar os movimentos de *tags* pertencentes à arquitectura, cujos registos de leitura são considerados como verdadeiros perante a estação central. Os registos de leitura e informação resultante do consenso geográfico são armazenados pela arquitectura no seu repositório de dados, que se encontra implementado em Mysql. A informação geográfica armazenada pela base de dados, pretende-se que seja apresentada no mapa, perante clientes aplicacionais que necessitem de monitorizar objectos RFID.

De todo o modo, a aproximação utilizada no armazenamento dos dados do consenso no repositório depende da politica seguida pela arquitectura. Desta forma são aplicados dois modos de funcionamento no armazenamento dos dados, podendo seguir uma base optimista ou pessimista.

No funcionamento optimista, assim que os dados chegam à estação central são colocados no mapa, realizando-se uma aproximação primária à localização final, através de uma média ponderada dos valores obtidos. O intuito desta aproximação, consiste em fornecer informação de localização ao cliente da aplicação final, que esteja próxima daquela que será obtida posteriormente, pelo consenso geográfico. De qualquer modo, assim que seja possível pela aplicação e mediante os intervalos temporais utilizados para aguardar novos registos, o consenso é efectuado e os dados são colocados à disposição de forma definitiva no mapa.

Por outro lado, na situação pessimista, os dados apenas são colocados à disposição do cliente aplicacional, quando o sistema tiver a garantia de que não existirá nenhuma alteração aos mesmos, ou seja a informação colocada no repositório de dados consiste na informação resultante do consenso. Nesta situação, não se pretende responder a requisitos de tempo real, mas sim na

disponibilização da informação do modo mais fiável possível.

Ainda assim, toda a informação que é colocada à disposição, seja ela temporária ou definitiva, é marcada tendo em conta a confiança da posição que se conhece naquele instante. À medida que o cliente interage com a informação presente no repositório, os dados a fornecer são actualizados consoante a informação que é possível dispor no momento.

Para implementação do consenso geográfico criou-se um módulo que gera a informação resultante do consenso, para ser colocada no repositório. Para tal, utiliza o método *chooseGoodReaders*, para selecção dos leitores considerados verdadeiros. Através da informação fornecida por estes leitores, é invocado o método *coordConsensus*, de modo a se proceder ao cálculo da posição, resultante da localização. Para tal, são seleccionados conjuntos de pontos, mediante a confiança deles para construção do polígono. A confiança acerca de cada leitor é obtida, através do método *getReaderTrust*. A classe *OrderPoints*, efectua a ordenação dos pontos para criação do polígono, seguindo-se o cálculo do centro de massa desse polígono, recorrendo ao método *centroid*. Por fim, verifica-se a validação do consenso pela execução do método *validateConsensus*.

Na gestão da base de dados, perante o consenso optou-se por utilizar a base optimista logo, os dados após o consenso necessitam de ser actualizados na base de dados, para afectação das novas coordenadas geográficas e confiança obtida nessa informação. Na situação do consenso validado, a informação da base de dados é actualizada através do método *updateRegistryConsensus*. De forma similar, a gestão dos leitores incorrectos e a sua futura acção no sistema é efectuada pelo método *updateReaderWrongLocation*.

6 . Avaliação experimental e análise de resultados

Este capítulo apresenta a avaliação das principais contribuições da dissertação. A avaliação é suportada nos resultados obtidos de diversos testes experimentais, utilizando os protótipos de implementação desenvolvidos.

A secção 6.1 apresenta os testes experimentais realizados, as condições de realização dos mesmos e aspectos de terminologia e parametrização comuns aos diversos testes. A secção 6.2 apresenta a avaliação das variantes do protocolo de autenticação. A secção 6.3 é particularmente focada na avaliação do suporte de processamento para consenso geográfico obtido na estação central de rastreio a partir da informação de localização enviada pelas estações locais. A secção 6.4 apresenta, em síntese, uma discussão sobre os resultados obtidos e a análise crítica desses resultados face aos objectivos da dissertação.

6.1 Estrutura dos testes realizados e condições de avaliação

6.1.1 Protótipos e cobertura dos testes realizados

Os testes que se apresentam nas secções seguintes cobrem as duas dimensões principais associadas às contribuições da dissertação, nomeadamente:

- Verificação e avaliação experimental do protocolo de autenticação, nas variantes propostas e para os protótipos desenvolvidos.
- Verificação do protocolo e mecanismos de processamento para estabelecimento do consenso geográfico, em condições de simulação de estações locais de localização operando em falha ou actuando com processamento incorrecto (eventualmente provocado por intrusões provocando propagação de informação falsa).

6.1.1.1 Protocolo de autenticação e protótipos de avaliação

Os protótipos utilizados, cuja concretização foi descrita no capítulo 5, secção 5.1, como instâncias de realização das arquitecturas apresentadas no capítulo 4, secção 4.2 envolvem a implementação e avaliação das duas variantes e de uma extensão do protocolo de autenticação, tal como a seguir se descreve:

Protótipo de implementação da estação e *tag* com base em dispositivos Sun SPOT

Trata-se do protótipo de implementação de alvos materializados com sensores Sun SPOT, comunicando com base na norma IEEE 802.15.4 e operação com bateria autónoma, funcionando como *tags* activas para identificação por rádio-frequência, na banda dos 2.4 GHz. Este protótipo, corresponde à implementação de uma estação local com base num sensor Sun SPOT ligado por USB a um computador portátil que usa um dispositivo móvel externo (baseado num telemóvel Nokia 5800) como leitor de coordenadas de localização por A-GPS. O conjunto implementa assim a noção de estação de localização fixa ou móvel, assim utilize ou não o subsistema de localização por A-GPS.

Neste protótipo foram avaliadas as seguintes variantes do protocolo de autenticação:

- **Variante completa:** trata-se da variante inicialmente proposta, descrita no capítulo 4, secção 4.4. Esta variante inclui o suporte para autenticação mútua e protecção de privacidade de *tags*, com utilização de identificadores voláteis, não reutilizáveis e assegurando propriedades de confidencialidade, integridade e autenticidade de fluxos de dados trocados entre as *tags*, estação local de localização e estação central de rastreio.

- **Variante optimizada:** trata-se da variante do protocolo de autenticação que está descrita na secção 4.4.8 e que visa optimizar a latência associada ao completamento do protocolo e assim, permitir suportar uma maior mobilidade das *tags*.

Os testes sobre as anteriores variantes do protocolo de autenticação incidiram na avaliação dos seguintes indicadores:

- Avaliação de desempenho do protocolo.

- Avaliação de condições de latência, quando utilizadas diversas configurações de segurança (nomeadamente configurações de suites criptográficas e tamanhos de chaves) e seu impacto na execução do protocolo.

- Avaliação de condições de mobilidade dos alvos RFID, face à cobertura de sinal rádio e às repercussões da latência associada ao completamento do protocolo.

- Avaliação da eficiência energética do protocolo de autenticação para aferição das condições de processamento por parte de alvos móveis ou estações locais de localização que operam com bateria autónoma e, portanto, com limitações energéticas.

Protótipo de implementação da estação com dispositivo móvel com NFC e *tags* baseadas em etiquetas passivas com RFIDs

Trata-se do protótipo de implementação de alvos RFID materializados com etiquetas passivas (para leitura RFID na frequência de 13.56 MHz) e sobre o qual foi implementada a variante de extensão do protocolo de autenticação descrita no capítulo 4, secção 4.4.9. Este protótipo corresponde à implementação de uma estação local, com base num dispositivo móvel com suporte para NFC e leitura RFID (telefone móvel Nokia 6212 NFC), com ambiente Symbian Series 40 e suporte para aplicações JAVA MIDP 2.0. Por restrições de comunicação na rede *internet* e de forma a facilitar a comunicação e a obtenção dos dados de teste, o telefone móvel comunica com o *proxy* (ao nível da estação de localização), por intermédio de um componente local, que se encarrega de gerir os resultados dos testes efectuados e que são recebidos no telefone.

Os testes sobre o protocolo de autenticação na extensão implementada para este protótipo incidiram na avaliação dos seguintes indicadores:

- Avaliação de desempenho geral do completamento do protocolo.
- Avaliação de alguns indicadores energéticos.

6.1.1.2 Avaliação do suporte de processamento de consenso de localização geográfica

Esta avaliação foi realizada num ambiente de simulação, sendo a natureza dos testes centrada na avaliação do mecanismo de processamento e decisão do consenso com recurso ao simulador Freemote [11], vulgarmente utilizado como simulador para redes de sensores, tendo suporte para simular redes com sensores Sun SPOT. A figura 6.1 mostra a interface do simulador. Para efeitos da sua utilização no contexto da dissertação fizeram-se algumas alterações ao simulador e que se passam a explicar.

Como referido na descrição do protocolo de autenticação (apresentado no capítulo 4, secção 4.4) as *tags* não transmitem sempre ou de forma espontânea os seus identificadores. Apenas o fazem como resultado de interrogações iniciadas pelos leitores ao nível das estações de localização. Deste modo, procedeu-se a uma alteração no funcionamento dos nós do simulador, pois neste, cada nó que representa um sensor possui um ciclo de funcionamento em que envia eventos de acordo com o escalonamento CSMA/CA subjacente ao funcionamento do protocolo IEEE 802.15.4. Por outro lado, os nós que simulam os leitores (nível das estações locais)

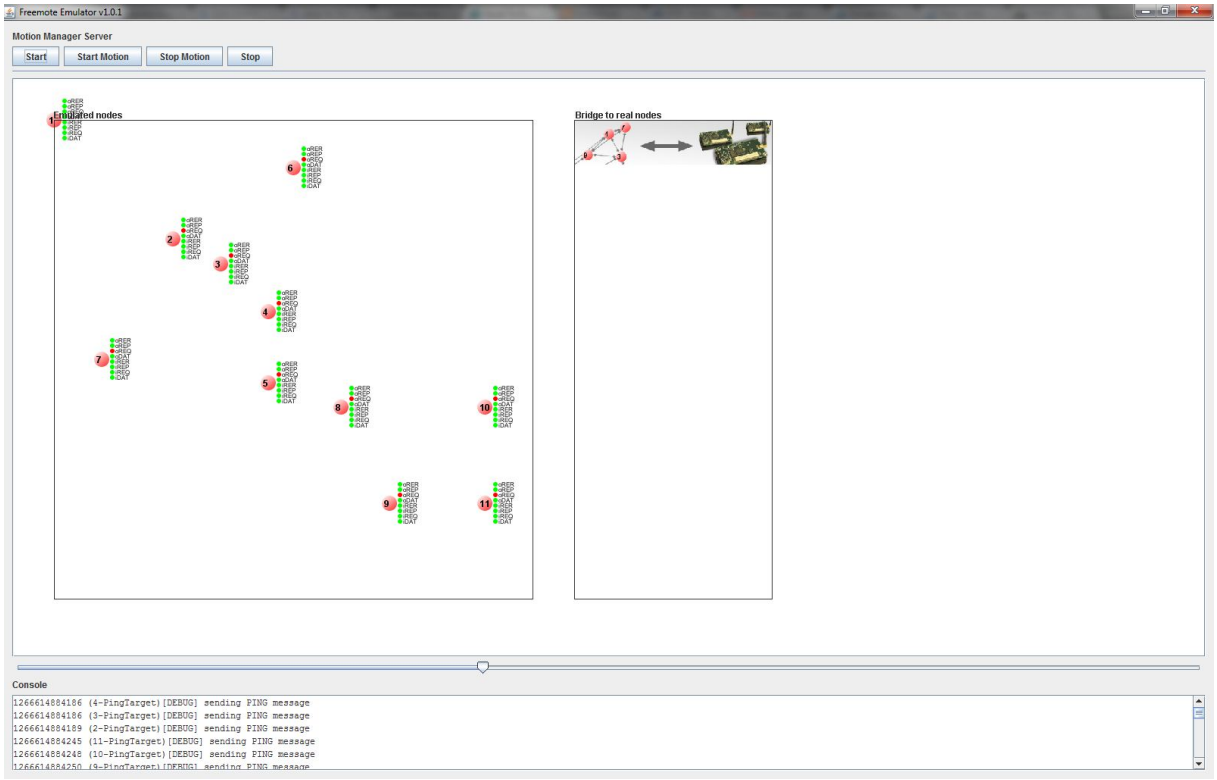

Figura 6.1 Imagem da interface do simulador

enviam interrogações para as *tags*, contudo, não respondem a pedidos efectuados por outros leitores ou *tags*.

6.1.2 Condições gerais dos testes e aspectos terminologia

Protocolo de autenticação

As avaliações envolveram o estudo e análise experimental do impacto de diversas configurações de segurança e dessa forma foram configuradas nos dispositivos e demais componentes, chaves de diferentes tipos e tamanhos, consoante as configurações apresentadas na tabela 6.1 e 6.2.

Tal como descrito na secção 5.6.1, antes da execução do protocolo é necessário inicializar os dispositivos e componentes que vão interagir no mesmo, nomeadamente a *tag*, leitor (nível

	Assinatura			Chave de Sessão*		
Configuração	**Algoritmo**	**Dimensão**	**Síntese**	**Semente**	**Algoritmo**	**Dimensão**
ECC 160	ECDSA	160	SHA-1	Diffie-Hellman	AES	128
AES 128	CMAC	128	SHA-1	PMS/MS	AES	128
AES 256	CMAC	256	SHA-1	PMS/MS	AES	128
RSA 512	RSA	512	SHA-1	PMS/MS	AES	128
RSA 1024	RSA	1024	SHA-1	PMS/MS	AES	128
RSA 2048	RSA	2048	SHA-1	PMS/MS	AES	128
* - Apenas utilizado na variante completa						

Tabela 6.1 A parametrização das diferentes configurações de segurança para o protocolo de autenticação

ECC 160	Utilização do algoritmo de curva elíptica, com chaves (privada e pública) de 160 bits, para assinaturas ECDSA [50]
AES 128	Utilização do algoritmo simétrico AES, chave de 128 bits (blocos de 128 bits), para assinaturas CMAC, com operação em modo CBC.
AES 256	Utilização do algoritmo simétrico AES, chave de 256 bits (blocos de 128 bits)para assinaturas CMAC com operação em modo CBC.
RSA 512	Utilização do algoritmo RSA, com chaves (privada e pública) de 512 bits, para assinaturas RSA, com síntese SHA-1 e *padding* PKCS1
RSA 1024	Utilização do algoritmo RSA, com chaves (privada e pública) de 1024 bits, para assinaturas RSA, com síntese SHA-1 e *padding* PKCS1
RSA 2048	Utilização do algoritmo RSA, com chaves (privada e pública) de 2048 bits, para assinaturas RSA, com síntese SHA-1 e *padding* PKCS1
ECDSA	Operação de assinatura de chave pública com base no standard DSA, usando uma chave privada ECC de 160 bits (ou, na verificação, usando a chave pública respectiva ao par, com dimensão de 160 bits). No método DSA, usam-se sínteses de 160 bits, subjacentes às assinaturas)
SHA-1	Operação de síntese segura de mensagens (segundo a norma FIPS SHA-1 *Secure Hashing*), com sínteses de 160 bits
Diffie-Hellman	Método de geração de chaves com base no algoritmo de Diffie-Hellman, a partir de uma semente (número privado e número público) de 160 bits, para geração de uma chave de 128 bits utilizada como chave de sessão para algoritmo AES
PMS-MS	Método de geração de chave de sessão envolvendo encadeamento de sínteses a partir de semente pseudo-aleatória para cálculo encadeado do PMS e MS como valores de entrada para o cálculo da chave de sessão. O encadeamento é: PMS = Random ‖ idType ; MS = H(Random ‖ PMS) + H (PMS)

Tabela 6.2 Configurações possíveis e significado das operações criptográficas

estação local) e *proxy* (nível estação local-estação central de rastreio). Esta inicialização envolve a geração e colocação de um identificador volátil na *tag* e de um identificador estático no leitor. São igualmente geradas as chaves criptográficas associadas às diferentes configurações do protocolo nos respectivos dispositivos e componentes da arquitectura.

Relembra-se que na variante optimizada e para a variante de extensão do protocolo, a *tag* não recebe o novo identificador volátil durante a execução do protocolo e dessa forma não é necessário gerar a chave de sessão.

Em alguns testes relativos à variante completa, procede-se à alteração do algoritmo e dimensão da chave de sessão gerada. Nestas variações recorre-se aos algoritmos AES ou RC4 (ARCFOUR) e dimensões de chave de 128, 192 e 256 bits. É de notar que a implementação

de RC4 utilizada nos Sun SPOT e posteriormente no telefone NFC, não contempla a criação de uma *keystream*, a partir da chave inicial, recorrendo directamente à chave utilizada e sua reutilização subsequente para cifrar directamente o texto. Por essa razão, é possível utilizar até 256 bits como dimensão para a chave de entrada do algoritmo.

No cenário idealizado para a realização de testes de avaliação do processamento associado à obtenção do consenso geográfico, os nós encontram-se dispersos no painel do simulador com a função de verificar, periodicamente, se existe alguma *tag* em movimento ou não nas suas redondezas (no respectivo raio de alcance rádio). Ao invés dos SN reais, que utilizam GPS para obtenção das coordenadas de localização, estes leitores do simulador recorrem às coordenadas de posições que estão representadas no mapa. Os nós maliciosos ou incorrectos são simulados pelo envio de informação incorrecta para a estação, que não corresponde à sua posição correcta no simulador.

De modo a agregar a funcionalidade dos nós *tag* e leitor, efectuou-se uma alteração no simulador que permite parametrizar de forma mais acessível as condições dos testes realizados. A interface de configuração dos testes encontra-se na figura 6.2. Esta interface gera um cenário de configuração para RFID, que consiste na colocação de uma *tag* em movimento, cujo trajecto encontra-se no raio de 10 leitores durante um determinado intervalo de tempo. Esse intervalo depende da distância que o dispositivo percorreu ao alcance do leitor.

A figura 6.3 demonstra a disposição dos leitores e da *tag* no painel do simulador, relativos ao cenário utilizado nos testes de localização. Como se pode observar, a *tag* encontra-se no canto superior esquerdo da figura e percorre o trajecto no sentido e direcção indicados pela seta, que cobre toda a área de simulação.

6.2 Avaliação do protocolo de autenticação

6.2.1 Protótipo com Sun SPOT

Para a realização dos testes experimentais neste protótipo, a *tag* encontra-se à espera de mensagens enviadas por difusão pelos leitores ao nível da estação de localização. Estas mensagens são enviadas pelo leitor a cada 5 segundos, para iniciação do protocolo de autenticação.

Após a conclusão com sucesso do protocolo, a *tag* envia a informação estatística para o leitor, e este por sua vez entrega à estação local, que é responsável pelo armazenamento de

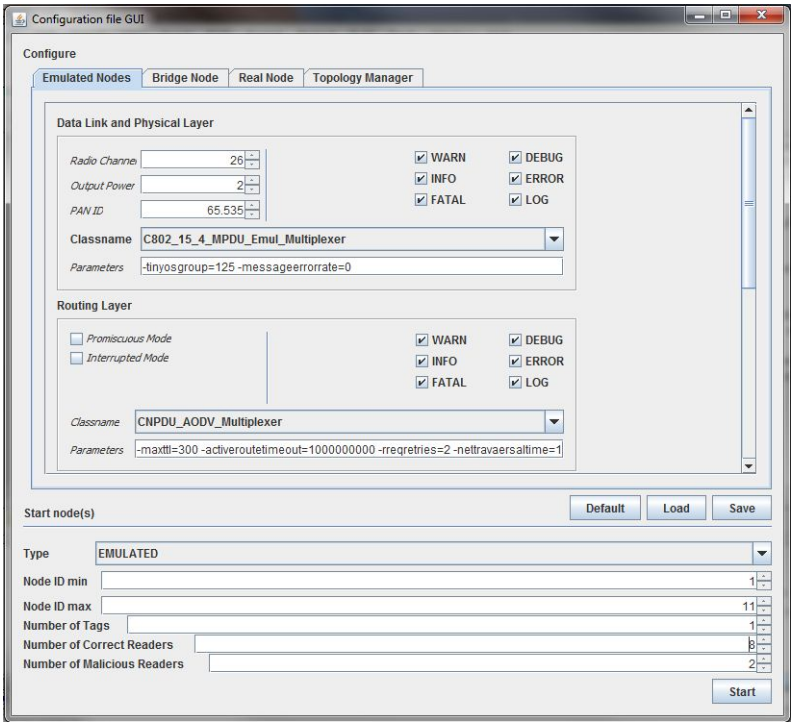

Figura 6.2 Imagem da configuração do simulador para nós RFID

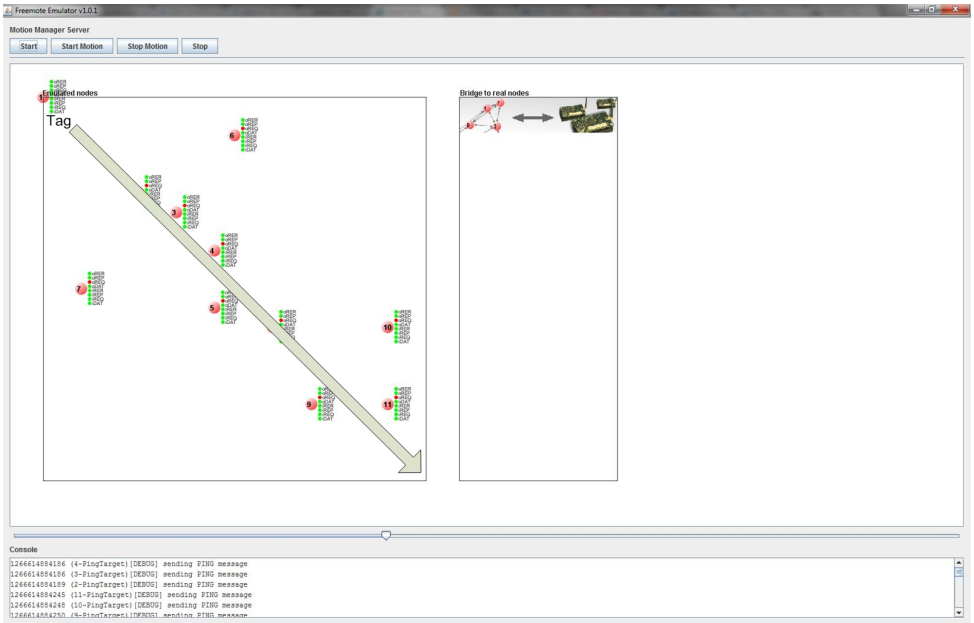

Figura 6.3 Cenário de validação da localização

todos os dados obtidos dos testes experimentais. Cada teste realizado, à excepção daqueles que pressupunham a descarga da bateria, foi sujeito no mínimo a 10 repetições, sempre nas mesmas condições. Após a recolha dos dados, efectuou-se a média dos valores obtidos.

6.2.1.1 Desempenho

Nesta secção avaliam-se parâmetros de desempenho no processamento do protocolo de autenticação, obtido de forma experimental, face a diversas configurações de segurança. Estes parâmetros abarcam todo o processamento efectuado pela *tag*, que inclui o processamento da mensagem (M1) gerada e enviada desta para o leitor e da mensagem recebida pela *tag*, por parte do leitor (M5 na variante completa e M6 na variante optimizada). Relembra-se que o fluxo das mensagens na variante completa e optimizada estão descritos no capítulo 4, nas secções 4.4.6 e 4.4.8.1, respectivamente.

De modo a medir o processamento da mensagem M1, procede-se à medição temporal entre o momento em que a *tag* recebe a mensagem de início do protocolo e a geração da mensagem M1, por parte da *tag*. Relativamente à mensagem recebida pela *tag*, inicia-se a medição temporal entre o momento em que esta recebe a resposta da parte do leitor e o momento em que finaliza o processamento da mensagem. Para cada uma das operações criptográficas incluídas nestas mensagens, procede-se à medição do tempo despendido para a sua realização.

Impacto das configurações de segurança no protocolo de autenticação

	Geração da semente da chave	**Assinatura**	**Síntese**	**Geração da chave**	**Verificação assinatura**	**Decifra do ID**	***Overhead***
ECC 160	0,5517	0,5919	0,0510	0,0588	0,7744	0,0217	0,1911
AES 128	0,0488	0,0107	0,0570	0,1531	0,0230	0,0210	0,1764
AES 256	0,0495	0,0096	0,0578	0,1607	0,0227	0,0261	0,1761
RSA 512	0,1503	2,6678	0,0552	0,1493	0,1124	0,0207	0,1760
RSA 1024	0,3835	18,9226	0,0571	0,1515	0,3355	0,0209	0,6189
RSA 2048	1,2720	142,9788	0,0573	0,1536	1,2054	0,0210	0,1967

Tabela 6.3 Tempo de processamento (s) nas diversas operações dos protocolos, face a diversas configurações do protocolo

Este teste, cujos resultados são representados na tabela 6.3, permitem avaliar o impacto das operações de segurança efectuadas, para cada configuração de segurança, na variante completa do protocolo.

As operações apresentadas na tabela podem ser separadas em duas fases do protocolo de autenticação. A primeira fase corresponde às operações efectuadas pela *tag*, a incluir na mensagem a enviar ao *proxy*. Estas operações são: geração da semente para criação da chave de sessão (geração do PMS ou parâmetros de Diffie-Hellman para curvas elípticas), assinatura e síntese da mensagem. As operações da segunda fase são executadas, após a recepção da mensagem vinda do *proxy* e incluem: geração da chave de sessão, verificação da assinatura do *proxy* e decifra do identificador volátil.

De um modo geral, através da observação da tabela, verifica-se que as configurações AES 128 e AES 256 são significativamente mais rápidas que as restantes. Por outro lado, analisando as configurações que recorrem a chaves assimétricas, constata-se que a configuração ECC 160 é significativamente mais rápida que as restantes configurações de RSA.

A análise de cada operação criptográfica, no contexto interno de uma configuração de segurança é efectuada entre as figuras 6.4 e 6.10.

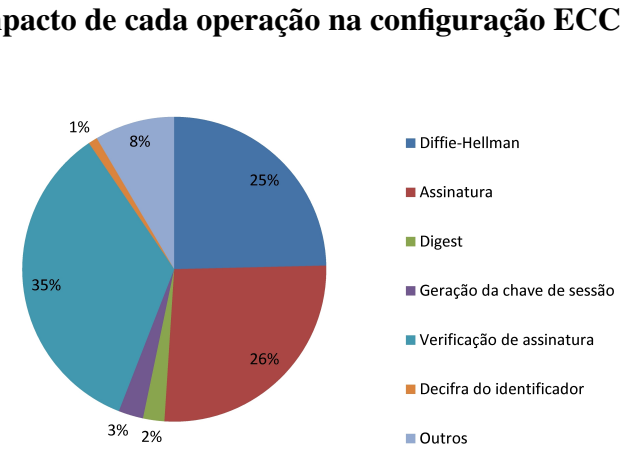

Figura 6.4 Percentagem de tempo de processamento (%) nas diversas operações do protocolo com a configuração ECC 160

Para este teste, apresentam-se na figura 6.4 os pesos de processamento das diversas operações criptográficas, bem como do *overhead* obtido, quando se recorre à configuração ECC 160 na variante completa do protocolo. Através da sua observação, verifica-se que o processo de geração dos parâmetros de Diffie-Hellman ocupa 25% do tempo de processamento total do protocolo, ou seja apenas para a produção da semente a utilizar na geração da chave de sessão já se consumiu 25% do tempo do protocolo. Este valor constitui um peso elevado no protocolo, pois

efectivamente ainda não se utilizou nenhum mecanismo para garantia de alguma propriedade de segurança.

De todo o modo, o elevado peso computacional desta operação garante um nível elevado na segurança futura das chaves utilizadas, pois um atacante apenas com os dados que transitam na rede não consegue reproduzir, nem verificar, alguma relação entre os elementos trocados entre os participantes.

Verifica-se também que as operações de assinatura/verificação ocupam cerca de 60% do tempo de processamento do protocolo. As restantes operações e overhead do protocolo representam cerca de 15% do total, não tendo por isso um impacto considerável no mesmo.

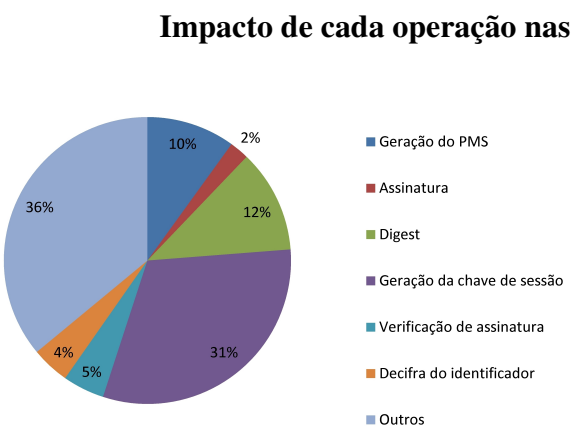

Figura 6.5 Percentagem de tempo de processamento (%) nas diversas operações do protocolo na configuração AES 128

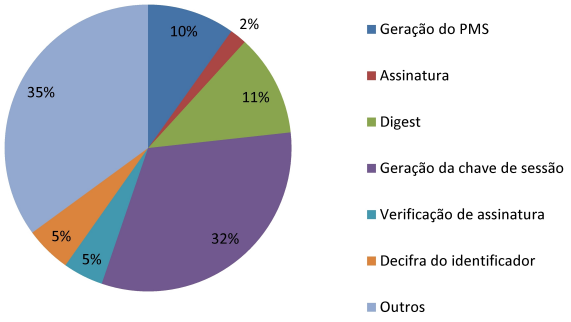

Figura 6.6 Percentagem de tempo de processamento (%) nas diversas operações do protocolo na configuração AES 256

As figuras 6.5 e 6.6, ilustram o peso das operações criptográficas, bem como do *overhead* obtido na variante completa do protocolo, para as configurações AES 128 e AES 256.

Através da observação dos gráficos, verifica-se, em termos gerais, que o *overhead* do protocolo representa cerca de 1/3 da computação efectuada pela *tag*. Nas restantes configurações do protocolo (ECC e RSA) este valor não tem um peso considerável (8% e $\approx$ 0%), pois o tempo requerido para as operações de segurança é menor e o peso do funcionamento do protocolo *per si* diluí-se no tempo total de processamento.

Este *overhead* do protocolo incluí a sequência das operações a efectuar, verificações de integridade das mensagens recebidas, *nonces* gerados, etc. De um modo geral, representa todo o

peso de funcionamento, exceptuando as operações criptográficas referidas nas figuras.

Outra operação com grande relevância no processamento efectuado pela *tag* consiste na geração da chave de sessão, que representa cerca de 1/3 do peso do protocolo. Esta chave no contexto da configuração ECC 160 necessita de ser utilizada cerca de 8 vezes para que o *overhead* da sua geração seja equivalente ao tempo despendido na decifra do conteúdo enviado pelo *proxy*.

Comparando as figuras de forma transversal, verifica-se que à medida que a dimensão da chave aumenta, o peso da sua geração e decifra da informação igualmente aumenta, como seria expectável. Contudo, o seu impacto é pouco relevante no contexto global do protocolo.

Impacto de cada operação nas configurações RSA 512, RSA 1024, RSA 2048

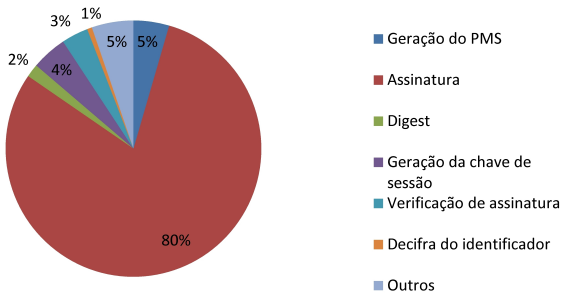

Figura 6.7 Percentagem de tempo de processamento (%) nas operações do protocolo com a configuração RSA 512

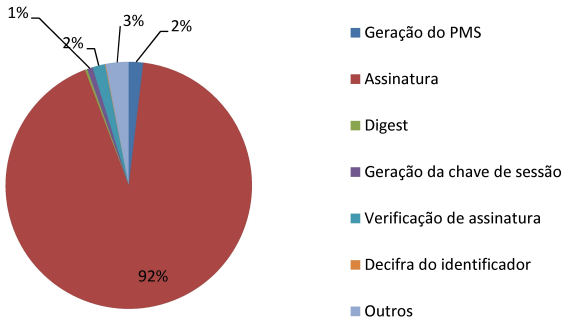

Figura 6.8 Percentagem de tempo de processamento (%) nas operações do protocolo com a configuração RSA 1024

Tal como ilustrado nas figuras 6.7, 6.8 e 6.9, estão representados os pesos das operações criptográficas, bem como do *overhead* na variante completa do protocolo de autenticação, quando se recorre às configurações RSA 512, 1024 e 2048, respectivamente.

De um modo geral, a operação de assinatura representa no mínimo 80% do peso da computação efectuada pela *tag*, o que a torna bastante representativa da sua influência no desenvolvimento do protocolo.

Tal como seria esperado, o peso da operação de assinatura aumenta consideravelmente, à medida que eleva o número de bits utilizados na chave RSA. Este valor é tão elevado no contexto total do protocolo, pois com as chaves de 1024 e 2048 bits, o seu peso no protocolo é de

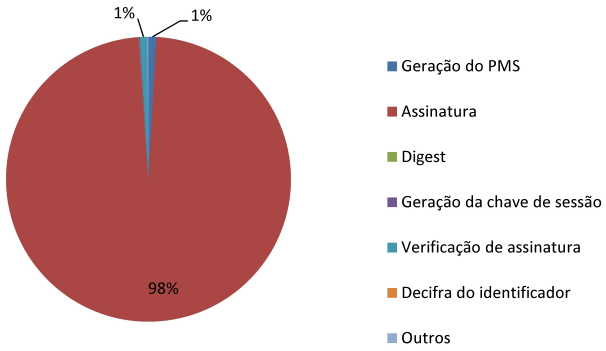

Figura 6.9 Percentagem de tempo de processamento (%) nas operações do protocolo com a configuração RSA 2048

92% e 98%, respectivamente. Neste último caso, considera-se que todas as restantes operações do protocolo são desprezáveis, pois são irrelevantes na influência do seu desempenho.

Visão comparativa do tempo de cada operação em diferentes configurações de segurança

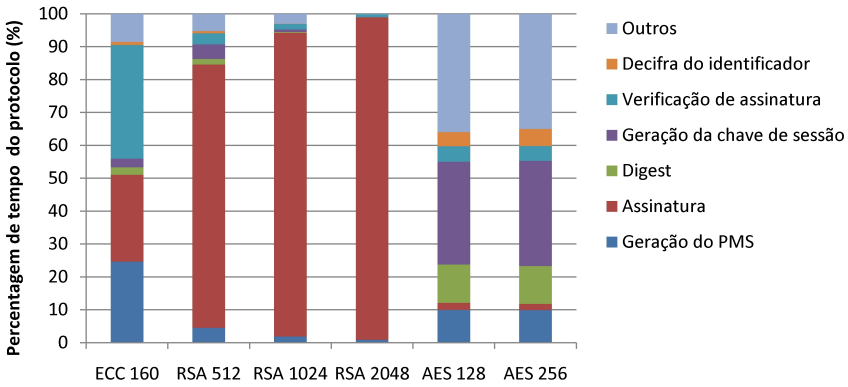

Figura 6.10 Visão comparativa da percentagem (%) de cada operação, em relação ao tempo total, nas diferentes configurações do protocolo

Neste teste, com recurso à figura 6.10, apresenta-se uma visão geral da percentagem de tempo que cada operação criptográfica necessita, na variante completa e para diferentes configurações do protocolo de autenticação.

Através da análise da figura verifica-se que nos tempos obtidos, o *overhead* apenas toma um valor considerável nas configurações AES 128 e AES 256, sendo mesmo irrelevante nas de RSA.

Conclui-se ainda que a operação de assinatura com ECC 160 apresenta um menor custo do que a verificação da mesma, ao contrário das configurações com RSA. De todo o modo, nestas configurações a diferença de valores é bastante superior, em relação a ECC 160 e, por isso, esta torna-se bastante mais interessante e aplicável nos sensores utilizados.

Pode-se concluir igualmente que a utilização de RSA só seria favorável a curva elíptica, caso a *tag* tivesse apenas que efectuar verificação de assinaturas. De qualquer forma, este cenário hipotético não se pode aplicar na arquitectura, pois o *proxy* para aceitar registos de localização necessita, entre outras coisas, de autenticar a *tag* e nessa situação teria que realizar operações de autenticação.

Visão comparativa do tempo de processamento nas variantes completa e optimizada

	Completa	**Optimizada**
ECC 160	2,24	0,78
AES 128	0,49	0,19
AES 256	0,50	0,19
RSA 512	3,33	2,85
RSA 1024	20,49	19,25
RSA 2048	145,88	142,55

Tabela 6.4 Tempo de processamento (s) na variante optimizada e completa do protocolo face a diversas configurações do protocolo

Neste teste, a tabela 6.4 apresenta uma visão comparativa dos tempos totais de processamento do protocolo de autenticação, nas variantes completa e optimizada. Relativamente à variante completa, os valores de tempo de processamento total reflectem a soma do tempo das operações criptográficas e *overhead* do protocolo, apresentadas na tabela 6.3.

Uma visão geral sobre os dados da tabelas permite concluir que os tempos obtidos na variante optimizada são em todas as configurações inferiores à variante completa. Nomeadamente, os ganhos em tempo de processamento obtidos com a configuração ECC 160 ou simplesmente AES 128 ou AES 256 são superiores a 60%.

Analisando em pormenor a configuração ECC 160, verifica-se que os ganhos obtidos devem-se essencialmente à eliminação da geração dos parâmetros de Diffie-Hellman (DH), utilizados para geração da chave de sessão e à anulação da mensagem de resposta, por parte do *proxy*, o que permite poupar no tempo de verificação da assinatura que o *proxy* efectuou. Por outro lado,

as configurações com AES (128 ou 256) obtém os ganhos em processamento essencialmente devido à eliminação da geração da chave de sessão, PMS/MS e uma diminuição do *overhead* de processamento, resultante do processamento mais simples da mensagem de resposta recebida pela *tag*, por parte do leitor.

As configurações com RSA apresentam igualmente um ligeiro ganho em tempo de processamento, que se diluí à medida que se aumenta a dimensão da chave, pois a eliminação dos parâmetros necessários à geração da chave de sessão ou verificação da assinatura do *proxy*, apresentam um peso reduzido, relativamente ao tempo utilizado pela *tag* para assinar a mensagem.

Impacto no processamento face a variações da configuração ECC 160

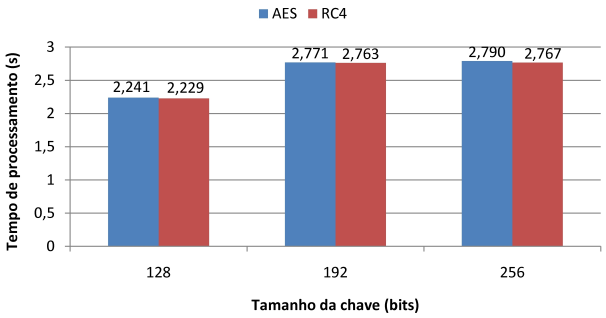

Figura 6.11 Tempo de processamento(s) face a diversas dimensões de chave no algoritmo AES e RC4 no protocolo de autenticação com a configuração ECC 160

Neste teste apresentam-se os resultados relativos ao impacto da variação do algoritmo e da dimensão da chave de sessão na configuração ECC 160, para a variante completa do protocolo de autenticação. As variações aplicadas nesta configuração consistem na alteração da dimensão da chave simétrica (128, 192 ou 256 bits), do algoritmo utilizado (AES ou RC4(ARCFOUR)) e podem ser visualizados na figura 6.11. Estas variações resultam numa alteração do tempo necessário para criação da chave de sessão e decifra do identificador.

Em termos gerais, verifica-se, como seria expectável, que o aumento da dimensão da chave resulta num incremento do tempo de processamento do protocolo de autenticação. É de notar que o aumento da chave, de 128 para 192 bits, conduz a um aumento de cerca de 20% no tempo total de processamento do protocolo. Contudo, a alteração de 192 para 256 bits resulta num aumento desprezável, no contexto geral do protocolo.

O aumento do tempo de processamento deve-se quase exclusivamente ao aumento do tempo despendido para geração da chave de sessão. Note-se que na configuração ECC 160, a geração da chave de sessão realiza-se com base nos parâmetros de Diffie-Hellman, gerados pela *tag* e *proxy*, respectivamente.

Verifica-se igualmente, para todas as dimensões de chave utilizadas, um ligeiro ganho em termos de desempenho com a utilização de RC4, ao invés de AES. Esta vantagem evidente do RC4 face a AES, embora noutras proporções, foi igualmente obtida em [26].

Tempo de decifra do identificador face a variações na configuração ECC 160

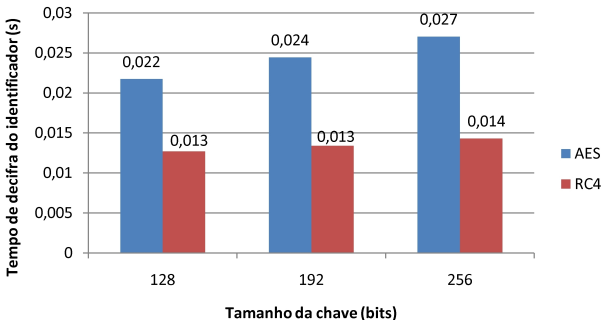

Figura 6.12 Tempo de decifra no identificador (s) face a diversas dimensões de chave no algoritmo AES e RC4 no protocolo de autenticação com a configuração ECC 160

Neste teste analisa-se o impacto da variação do algoritmo (AES e RC4) e dimensão (128, 192, 256) da chave de sessão na decifra do identificador volátil. As variações foram aplicadas na configuração ECC 160 para a variante completa do protocolo e podem ser visualizados na figura 6.12.

Através da sua observação, verifica-se que o algoritmo RC4 é mais rápido a decifrar o identificador volátil de 64 bits e também o que menos agrava o desempenho, quando se aumenta a dimensão da chave a utilizar. Com a análise desta figura e da anterior, conclui-se que a diminuição do tempo de processamento do protocolo quando se utiliza RC4 em relação ao AES deve-se quase exclusivamente aos ganhos de desempenho na decifra do identificador. De todo o modo, o processamento necessário para decifrar o identificador não é muito influente no contexto geral do protocolo.

6.2.1.2 Latência

Nesta secção, avalia-se a latência obtida de forma experimental, quando a comunicação entre o leitor e o *proxy* faz-se através da rede local (LAN) ou *internet*, para as variantes completa e optimizada do protocolo de autenticação. Para ambas as variantes, armazena-se o valor temporal corrente no momento em que a *tag* termina o processamento da mensagem (M1) a enviar para o leitor, bem como no momento em que esta recebe a mensagem de resposta por parte do leitor. O tempo despendido entre os dois valores temporais registados, corresponde à latência real do protocolo.

	Completa				**Optimizada**			
	LAN		**Internet**		**LAN**		**Internet**	
	Latência	**Tempo**	**Latência**	**Tempo**	**Latência**	**Tempo**	**Latência**	**Tempo**
ECC 160	0,78	2,97	2,03	4,22	0,12	0,90	0,12	0,90
AES 128	0,75	1,25	2,00	2,50	0,11	0,30	0,11	0,30
AES 256	0,81	1,32	2,06	2,57	0,12	0,30	0,12	0,31
RSA 512	0,85	4,19	2,47	5,80	0,13	2,98	0,12	2,98
RSA 1024	1,03	21,21	2,77	22,81	0,19	19,44	0,20	19,29
RSA 2048	1,32	146,84	3,72	148,54	0,49	143,23	0,48	142,77

Tabela 6.5 Valores de latência (s) e tempo total (s) do protocolo, em rede local (LAN) ou *internet*, face a duas variantes do protocolo de autenticação

Os testes efectuados com o intuito de medir a latência do protocolo obrigam a uma alteração do procedimento utilizado para a sua realização, pois é imperativo que o *proxy* esteja dissociado da máquina utilizada para recolher os dados do SN, de modo a obter-se valores de latência nas configurações de rede local (LAN) e *internet*. A máquina utilizada para suportar o processamento do *proxy* é um PC portátil, com processador de 1.6 GHz e 1.5 GB de memória.

Nos testes em rede local, o *proxy* está ligado na mesma rede wireless (WLAN) que a estação local e em ambiente *internet* os dois componentes estão ligados a ISP's portugueses distintos. O RTT obtido para a rede local é aproximadamente 1 ms, enquanto que em ambiente internet é cerca de 590 ms.

A análise da tabela anterior permite verificar a diminuição do tempo de processamento na variante optimizada do protocolo, em relação à completa. Da mesma forma, verifica-se igualmente uma diminuição na latência apresentada por esta variante nas duas configurações de rede. A tabela 6.5 apresenta essa variação da latência quando a comunicação entre a estação local e *proxy* é efectuada pela rede local ou *internet*.

Analisando a tabela na sua globalidade é possível verificar que a latência apresentada pela

variante optimizada é similar em todas as configurações de rede, e sempre inferior à variante completa do protocolo. A manutenção dos valores de latência deve-se ao facto do protocolo decorrer de forma assíncrona, ou seja a *tag* termina o processamento do protocolo de forma independente do *proxy*. A latência obtida na variante optimizada deve-se essencialmente ao tempo de trânsito das mensagens trocadas entre a *tag*, leitor, ao processamento e envio da mensagem por parte do leitor, bem como ao envio da informação da *tag* para o leitor.

A latência da variante completa inclui adicionalmente o tempo de trânsito das mensagens entre a estação e *proxy*, assim como o tempo de processamento, por parte do *proxy*, do conteúdo gerado pelo leitor e *tag*, que é influenciado maioritariamente pela verificação das assinaturas.

As diferenças de latência para as duas variantes podem na prática apresentar valores superiores. Para tal, apenas é necessário que a latência da comunicação aumente, o que afectará a variante completa, e que a autenticação se processe de forma hierárquica, tal como apresentado no modelo arquitectural. Nesta situação, os dados de autenticação transitariam entre diversas *proxy's*, o que resultaria numa superior latência de comunicação e processamento das mensagens.

Verifica-se igualmente na variante optimizada que o tempo de processamento é dominante em relação à latência, pois a latência é estável e no máximo apresenta um peso de cerca de 40% do tempo total. Por outro lado, na variante completa, a latência à medida que aumenta pode tornar-se dominante, pois no limite, se apresentar valores muito elevados, o protocolo fica totalmente dependente desse factor, o que influenciará grandemente a mobilidade que a *tag* poderá apresentar, de modo que o protocolo termine com sucesso.

Tal como demonstrado, a latência é uma variável influente no desempenho do protocolo, apesar de existirem outros factores que podem contribuir para a sua degradação. Um desses factores verifica-se na variante optimizada e corresponde à situação de dessincronização dos identificadores voláteis. Relembra-se que nesta variante, os identificadores são gerados periodicamente pelo *proxy* e *tag*, através de um esquema de geração de senhas OTP dinâmicas, cuja chave é o identificador volátil da *tag* e o elemento periódico é a *timestamp*.

Na situação de dessincronização, o *proxy* necessita de verificar se o identificador recebido é equivalente a um dos identificadores passados que ainda não foram utilizados pela *tag* ou se é um dos identificadores futuros. De qualquer modo, ainda é possível que o elemento periódico

seja distinto do utilizado pelo *proxy* e, nessa situação, é necessário efectuar um número de tentativas ao nível desse elemento.

No teste efectuado a lista de identificadores passados tinha dimensão 10 e o número de tentativas com identificadores futuros era igualmente de 10. A periodicidade de geração de novos identificadores é de 30 segundos. Ao nível das *timestamps*, procurou-se testar duas anteriores e posteriores, ou seja 30 e 60 segundos antes e depois, respectivamente, da *timestamp* corrente.

Na situação limite, em que não é encontrado o identificador por nenhum dos meios, foram realizadas no total 100 tentativas para o encontrar. Estas tentativas referem-se às 5 *timestamps* utilizadas e para cada uma delas às 20 tentativas efectuadas, que correspondem a identificadores passados ou futuros. Este teste demorou cerca de 26 ms a efectuar, o que significa que, comparando com o menor tempo total do protocolo, obtido nos testes de latência (0,30 segundos na configuração AES 128), não chega a 10% do tempo, ou seja, não apresenta um grande impacto na degradação do protocolo.

6.2.1.3 Condições de mobilidade

Condições teóricas de mobilidade nos cenários optimista e pessimista

	Optimista				**Pessimista**			
	Completa		**Optimizada**		**Completa**		**Optimizada**	
	LAN	**Internet**	**LAN**	**Internet**	**LAN**	**Internet**	**LAN**	**Internet**
ECC 160	72,70	51,20	239,94	239,45	51,41	36,20	169,59	169,32
AES 128	172,91	86,45	716,02	713,58	122,27	61,13	506,30	504,58
AES 256	164,15	84,20	709,75	707,95	116,07	59,54	501,87	500,60
RSA 512	51,53	37,23	72,44	72,53	36,44	26,32	51,22	51,29
RSA 1024	10,18	9,47	11,11	11,20	7,20	6,70	7,86	7,92
RSA 2048	1,47	1,45	1,51	1,51	1,04	1,03	1,07	1,07

Tabela 6.6 Valores de velocidade máxima do protocolo (km/h), em rede local (LAN) ou *internet*, face a duas variantes do protocolo de autenticação e a cenários optimista e pessimista

As condições de mobilidade apresentadas na secção 4.5 possuem um cariz genérico, cujas condições dependem da variante e da configuração de segurança do protocolo de autenticação, ao qual estão aplicados.

Com base nos resultados de latência e tempo de execução do protocolo, efectuados na secção anterior, torna-se possível extrair valores teóricos de mobilidade para a *tag*.

Na tabela 6.6 estão representados esses valores para a situação optimista e pessimista. Por sua vez, para cada um destes casos, foram obtidos valores para cada variante do protocolo e em condições distintas de conectividade (LAN e *internet*). Estes valores de mobilidade correspondem à velocidade média teórica que a *tag* pode apresentar, de modo a completar o protocolo de autenticação nas suas diversas configurações. Note-se que os dados apresentados na tabela não correspondem a valores obtidos experimentalmente, mas sim a cálculos teóricos, de acordo com as condições de latência observadas. É igualmente importante frisar que se pressupõe a presença de um leitor fisicamente estático e continuamente a enviar pedidos de autenticação para *tags*. Este pormenor e o seu impacto nas condições de mobilidade é avaliado com maior detalhe nas tabelas 6.7 e 6.8.

Os sensores Sun SPOT utilizados nesta dissertação dispõem de um raio de alcance teórico na ordem de 70 metros. De qualquer forma, como este valor depende essencialmente da direcção da antena e das condições do meio, optou-se por definir um valor realista de 30 metros como raio de alcance. Desta forma, segundo as condições de mobilidade apresentadas em 4.5, na situação optimista a *tag* percorre 60 metros dentro do raio de alcance do leitor, ou seja todo o seu diâmetro, e na situação pessimista percorre cerca de 42 metros.

Analisando a tabela na sua globalidade, verifica-se rapidamente que, tal como esperado, para cada variante e condições de conectividade correspondentes, a velocidade máxima obtida no caso pessimista é inferior à situação optimista. No fundo, a tabela apresenta um intervalo de mobilidade, cujo valor mais restritivo corresponde à situação pessimista. É possível observar igualmente que os valores de mobilidade obtidos pela variante optimizada em relação à completa e entre a rede local e *internet* são superiores, tal como seria de prever através da descrição efectuada dos testes.

Nas configurações do protocolo em que se recorre apenas a criptografia simétrica (AES 128 ou AES 256), ocorrem os melhores valores de desempenho, resultando em superiores velocidades máximas suportadas para cada coluna da tabela apresentada, exceptuando a situação em que se utiliza criptografia de curva elíptica (ECC 160) na variante optimista.

Por outro lado, como esperado, as implementações de RSA apresentam o pior desempenho, em particular quando se recorre às configurações RSA 1024 e RSA 2048. Nestas situações os valores de mobilidade são muito reduzidos, permitindo uma liberdade bastante diminuta às *tags* para que o protocolo de autenticação ocorra com sucesso. Na situação em que se utiliza

a configuração RSA 512, os valores de mobilidade apresentados permitem movimentos relativamente rápidos à *tag*. Contudo, a segurança que proporciona é significativamente inferior às restantes configurações de RSA.

A configuração de segurança que apresenta a melhor relação de segurança/mobilidade é a ECC 160, pois proporciona uma autenticação forte entre participantes, permitindo simultaneamente uma boa liberdade de movimentos para a *tag*. Com a utilização desta configuração reside uma das maiores vantagens da adopção da variante optimizada em relação à completa, pois o caso em que a velocidade é máxima, permite que decorra com sucesso o protocolo de autenticação, quando a *tag* transita em praticamente todos os meios de transporte terrestres.

Esta tabela demonstra que através das configurações de segurança é possível afinar a execução do protocolo, de modo a que se obtenha a melhor relação entre a segurança pretendida e a mobilidade esperada.

Condições de iniciação do protocolo para diferentes períodos de descoberta de *tags*

	Optimista					**Pessimista**				
	1	**2**	**3**	**4**	**5**	**1**	**2**	**3**	**4**	**5**
10	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
20	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
50	Sim	Sim	Sim	Sim	Não	Sim	Sim	Sim	Não	Não
100	Sim	Sim	Não	Não	Não	Sim	Não	Não	Não	Não
200	Sim	Sim	Não	Não	Não	Não	Não	Não	Não	Não
500	Não	Não	Não	Não	Não	Não	Não	Não	Não	Não

Tabela 6.7 Verificação da recepção da mensagem por parte da *tag*, face a períodos de descoberta de *tags* (1-5 segundos) e diversas velocidades (10 - 500 km/h)

Tal como referido anteriormente, a tabela 6.6 representa uma situação teórica que pode ser refinada, de modo a reflectir melhor as condições reais de utilização. Deste modo, apresenta-se com recurso à tabela 6.7, diferentes períodos de envio de mensagens de descoberta (1 a 5 segundos), para iniciação do protocolo e diversas velocidades (10-500 km/h) que a *tag* poderá apresentar. Para cada combinação destas variáveis, cada elemento da tabela representa a certeza de que a *tag* consegue receber o pedido de autenticação ou a possibilidade de não o receber, enquanto se encontra no raio de alcance do leitor.

De alguma forma como esperado, quando a *tag* move-se a 10 km/h, para quaisquer dos períodos de descoberta, efectuados pelo leitor e respectivos cenários das condições de mobilidade (optimista e pessimista), verifica-se que teoricamente a *tag* consegue receber todos os pedidos de autenticação enquanto está no leitor. Esta avaliação teórica é importante, pois na prática o leitor não se encontra continuamente a enviar pedidos de autenticação.

Deste modo, os dados da tabela auxiliam a afinação dos tempos de descoberta, face à velocidade apresentada pela *tag*. Note-se que esta tabela não se refere a nenhuma configuração de segurança, pois apenas apresenta as condições de recepção da mensagem de iniciação do protocolo.

No caso extremo apresentado, quando a *tag* transita à velocidade constante de 500 km/h, poderá não conseguir receber nenhum pedido de autenticação, pois o tempo de deslocamento no interior do raio de alcance é inferior ao tempo de descoberta.

Nas restantes velocidades apresentadas, a *tag* poderá ou não receber os pedidos de autenticação. De qualquer forma, para cada par (velocidade, período de envio), apesar de se poder garantir teoricamente que a *tag* recebe os pedidos, a posição no interior do raio de alcance poderá variar, consoante o período de envio de mensagens, ou seja quando é muito longo (por exemplo, 5 segundos) a *tag* poderá receber o pedido, quando já percorreu uma distância considerável no raio de alcance. Nestas condições, a velocidade que a *tag* poderá apresentar será menor, pois dispõe de uma menor distância a percorrer, até sair definitivamente do raio de alcance. É igualmente dependente da configuração de segurança a utilizar, pois como descrito, configurações diferentes permitem velocidades máximas distintas.

Velocidade máxima teórica para diferentes períodos de descoberta

	0	**1**	**2**	**3**	**4**	**5**
ECC 160	51,20	41,39	34,73	29,92	26,48	23,43
AES 128	86,45	61,74	48,02	39,28	33,24	28,81
AES 256	84,20	60,58	47,31	38,81	32,90	28,55
RSA 512	37,23	31,76	27,69	24,54	22,04	20,00
RSA 1024	9,47	9,07	8,71	8,37	8,06	7,77
RSA 2048	1,45	1,44	1,43	1,43	1,42	1,41

Tabela 6.8 Valores teóricos de velocidade máxima do protocolo (km/h), face a diversos períodos de descoberta de *tags* (0-5) e diferentes configurações de segurança

A referida relação do período de envio de mensagens, por parte do leitor, para cada configuração de segurança e velocidade máxima teórica possível é apresentada na tabela 6.8. Analisando a sua informação, verifica-se, tal como expectável, que à medida que o período de envio de mensagens de descoberta aumenta, a velocidade máxima teórica possível diminui. Verifica-se igualmente que a diminuição das velocidades é proporcionalmente maior nas configurações do protocolo com ECC 160, AES 128 e AES 256, pois tal como descrito na tabela 6.5, são nesses casos onde o protocolo é mais rápido. Esta situação acontece, porque o aumento do período de envio possui um maior peso nessas configurações, logo o desempenho do protocolo degrada-se numa maior proporção.

6.2.1.4 Energia

Nesta secção avalia-se a energia despendida no protocolo de autenticação. O procedimento para a obtenção dos valores de energia é semelhante ao realizado nos testes de desempenho. A única diferença relaciona-se com a medição da capacidade disponível da bateria a cada momento, ao invés do valor temporal.

Energia de processamento das variantes do protocolo

	Completa	**Optimizada**
ECC 160	0,931	0,317
AES 128	0,190	0,069
AES 256	0,198	0,071
RSA 512	1,375	1,189
RSA 1024	8,712	8,089
RSA 2048	67,278	60,438

Tabela 6.9 Energia de processamento (J) na variante optimizada e completa do protocolo

Neste teste analisa-se as diferenças de consumo de energia no processamento do protocolo, nas variantes optimizada e completa, que podem ser observadas na tabela 6.9. Tal como seria esperado, verifica-se que a diminuição da energia na variante optimizada para cada configuração segue a tendência de diminuição do tempo de processamento, verificado na tabela 6.4.

É de realçar os baixos consumos de energia e principalmente os elevados ganhos energéticos quando se recorre à variante optimizada, que são apresentados pelas configurações ECC 160, AES 128, AES 256, resultantes da maior optimização do tempo de processamento entre as duas variantes do protocolo.

Por outro lado, comparando a variante completa com a optimizada, para as configurações RSA 512, RSA 1024, RSA 2048 verifica-se que ocorreu apenas uma ligeira diminuição da energia despendida, o que está em concordância com os ganhos ténues em desempenho apresentados na tabela 6.4.

Energia de processamento face a variações na configuração ECC 160

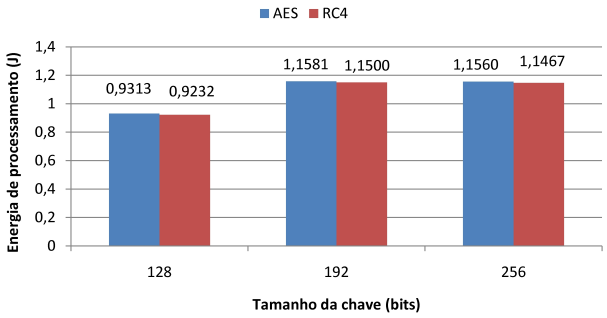

Figura 6.13 Energia de processamento (J) no protocolo com a configuração ECC 160 face a diversas dimensões de chaves nos algoritmos AES e RC4

Neste teste analisa-se as diferenças de energia de processamento, na variante completa do protocolo para a configuração ECC 160, através da variação da dimensão da chave simétrica e do algoritmo utilizado. Estas variações de energia podem ser visualizadas na figura 6.13. Através de uma análise da figura, verifica-se que estas variações seguem a tendência da alteração do tempo de processamento observado na figura 6.11, sensivelmente na mesma proporção. De todo o modo, a energia despendida que se observou apresenta valores reduzidos, o que indica que as variações impostas na configuração ECC 160 podem ser aplicadas na prática, resultando apenas uma ligeira alteração energética.

Energia do protocolo em rede local ou *internet*

Neste teste analisa-se a energia total despendida pelas duas variantes do protocolo, em rede local ou *internet*, que são apresentadas na tabela 6.10. Verifica-se, tal como esperado, a manutenção da energia gasta no protocolo, na variante optimizada, o que reflecte os tempos obtidos na tabela 6.5.

	Completa		Optimizada	
	LAN	**Internet**	**LAN**	**Internet**
ECC 160	1,145	1,437	0,364	0,365
AES 128	0,403	0,723	0,104	0,107
AES 256	0,426	0,740	0,108	0,108
RSA 512	1,650	2,027	1,245	1,253
RSA 1024	8,865	9,122	8,237	8,246
RSA 2048	62,112	62,392	60,371	61,673

Tabela 6.10 Energia (J) total do protocolo, em rede local (LAN) ou *internet*, face a duas variantes do protocolo de autenticação

Por outro lado, tal como seria expectável, ocorreu um aumento do gasto energético na variante completa do protocolo, quando o protocolo decorre na *internet*. Estes gastos energéticos por sua vez são superiores aos apresentados pela variante optimizada em qualquer meio de comunicação.

Analisando, em particular a configuração ECC 160 e a configuração correspondente em nível de segurança do algoritmo RSA (RSA 1024), verifica-se que ocorre um gasto de energia cerca de 8 vezes superior quando se recorre à variante optimizada e cerca de 24 vezes superior, relativamente à variante optimizada, ou seja, a diferença de consumo energético entre os dois algoritmos triplica quando se transita da variante optimizada para a variante completa.

Número de autenticações e tempo de funcionamento nas duas variantes do protocolo

	Completa		Optimizada	
	Tempo	**Autenticações**	**Tempo**	**Autenticações**
ECC 160	6,67	4781	8,8	5680
AES 128	8,09	5813	9,48	6126
AES 256	8,13	5817	8,59	6077
RSA 512	7,01	2449	6,86	4501
RSA 1024	5,69	816	5,30	944
RSA 2048	5,19	126	5,26	130

Tabela 6.11 Número máximo de autenticações e tempo de funcionamento no protocolo (horas), face a duas variantes do protocolo de autenticação

Neste teste apresenta-se uma visão comparativa do número máximo de autenticações realizadas e do tempo de funcionamento correspondente, para as duas variantes do protocolo de autenticação, que pode ser observada na tabela 6.11.

Estabelecendo uma comparação entre a variante optimizada e completa verifica-se, tal como expectável, que o número máximo de autenticações na primeira variante é sempre superior

para todas as configurações e o tempo de funcionamento apenas não é superior na variante optimizada, para as configurações RSA 1024 ou RSA 512. Esta superioridade geral da variante optimizada é expectável, na medida em que o tempo e energia total requeridos nesta variante é inferior, logo à *priori* teria que apresentar melhor resultados nestes parâmetros.

Os ganhos em tempo de funcionamento e autenticações conseguidas é particularmente relevante nas configurações de ECC 160, AES 128 e AES 256, na medida em que residiram aí as melhorias mais significativas, na comparação entre as duas variantes. De todo o modo, seria expectável uma melhoria mais significativa, que pode ser explicada pelo número superior de mensagens trocadas entre os participantes e pelo superior tempo de espera entre autenticações (leitor envia pedidos de autenticação a cada 5 segundos), por parte da *tag*, o que eleva o consumo energético fora do âmbito da monitorização do protocolo.

Nas configurações de RSA (RSA 1024 e 512), o tempo de funcionamento até a bateria descarregar na variante optimizada é realmente menor, em comparação com a variante completa. Contudo, o número de autenticações por unidade de tempo, para as referidas configurações é 87% e 24% superior, o que na prática se traduz num aumento substancial da eficiência de funcionamento. De todo o modo, não era expectável uma subida tão elevada do número de autenticações da configuração RSA 1024 na variante optimizada, que se verificou após a repetição do teste.

Energia despendida em diversos níveis de bateria na variante completa do protocolo

	ECC 160	**AES 128**	**AES 256**	**RSA 512**	**RSA 1024**	**RSA 2048**
90%	1,1122	0,3719	0,3499	1,6382	8,6707	62,7446
80%	1,1395	0,3759	0,3483	1,6435	8,8217	63,6471
70%	1,1556	0,3840	0,3543	1,6668	8,9268	64,4827
60%	1,1771	0,4010	0,3582	1,6875	9,0377	65,4504
50%	1,1851	0,4020	0,3619	1,6970	9,1550	65,9810
40%	1,1794	0,3926	0,3661	1,7077	9,2419	66,3420
30%	1,1837	0,3915	0,3677	1,7186	9,3123	66,6956
20%	1,1901	0,3914	0,3706	1,7226	9,3601	67,0246
10%	1,1964	0,3956	0,3712	1,7411	9,4005	67,6484
5%	1,1998	0,3989	0,3721	1,7557	9,4783	68,0870
Fim	1,2036	0,4012	0,3743	1,7586	9,5544	68,4201

Tabela 6.12 Energia despendida (J) em diversos níveis de bateria (%) para cada configuração do protocolo

Os sensores Sun SPOT, tal como referido anteriormente, recorrem a uma bateria para fornecer a energia que necessitam. Deste modo, procurou avaliar-se qual o comportamento da descarga

da bateria (em diversos níveis) para as diferentes configurações na variante completa do protocolo de autenticação. A tabela 6.12 indica para determinado nível da bateria, em percentagem, qual a energia gasta no cumprimento do protocolo. Através da sua observação, conclui-se como seria expectável, que ocorre um aumento da energia despendida (em média) à medida que a energia disponível no sensor diminui. Note-se que a partir de 16mAh (cerca de 2% da capacidade), o sensor deixa de executar correctamente. Contudo, continua a emitir dados via rádio. Este valor é o ponto de paragem na execução do protocolo de autenticação.

6.2.2 Protótipo com dispositivos NFC

A extensão do protocolo de autenticação, apresentada na secção 4.4.9, foi igualmente alvo de avaliação experimental, nomeadamente em relação ao tempo total de execução e à extracção de alguns indicadores energéticos.

O tempo total de execução do protocolo consiste no tempo que decorreu desde a leitura da *tag* NFC, até à escrita do novo identificador volátil na *tag*. Em cada um destes momentos, o leitor NFC armazena o valor temporal corrente e no fim do protocolo envia para a estação local a diferença temporal dos valores obtidos, que corresponde ao tempo total do protocolo.

Em relação à energia despendida na execução do protocolo de autenticação, apenas foi possível reunir alguns indicadores energéticos, pois o telefone móvel Nokia 6212 NFC, nomeadamente o seu sistema operativo, apresenta uma série de restrições de implementação, sendo uma delas a extracção de valores energéticos. Como tal, procurou-se obter alguns indicadores, através da descarga completa da bateria e posterior observação do número de protocolos de autenticação efectuados. Como a estação local está encarregue de gerir todos os resultados dos testes, o telefone móvel envia mensagens para a estação a cada 100 autenticações com sucesso.

Desempenho

Neste teste apresenta-se na tabela 6.13, o tempo de cada assinatura e o tempo total do protocolo, para as diferentes configurações utilizadas. Observando os dados fornecidos pela tabela e comparando com os testes descritos dos sensores, é possível verificar que se mantém a hierarquia quanto ao tempo utilizado por cada configuração do protocolo. As configurações AES 128 e AES 256 mantêm-se as mais rápidas, seguidas da ECC 160 e por último as de RSA.

	Assinatura	Tempo Total
ECC 160	0,0067	0,0111
AES 128	0,0016	0,0055
RSA 512	0,0102	0,0143
RSA 1024	0,0338	0,0379
RSA 2048	0,1237	0,1282

Tabela 6.13 Tempo total e de assinatura (s) em cada protocolo de autenticação

De todo o modo, efectuando uma comparação transversal com os testes realizados nos sensores, em particular na variante optimizada em rede local, verifica-se que os tempos obtidos com as configurações RSA estão significativamente mais próximos dos resultados obtidos com as configurações ECC 160 ou AES 128 e AES 256.

É de realçar que, independentemente dos maiores tempos obtidos pelas configurações RSA, todos os resultados demonstram que qualquer configuração do protocolo pode ser utilizada na prática, sem que seja perceptível ao utilizador algum atraso nas operações. Esta facilidade de execução das operações de segurança, em comparação com os sensores, deve-se ao superior poder de processamento do dispositivo móvel, que contém o leitor NFC.

Ao nível dos sensores, os tempos mais elevados (obtidos com a configuração RSA) restringem a mobilidade das *tags* RFID, ao ponto de quase não se tolerar movimentos, e tornam a interacção entre *tags* e leitores bastante morosa.

A extensão do protocolo de autenticação, se for utilizada em particular por dispositivos com tecnologia NFC, não coloca os problemas de mobilidade ao nível do protocolo, pois a própria interacção entre *tags* e leitores restringe a distância entre os intervenientes. Por esse motivo, estes testes não foram enquadrados nas condições de mobilidade.

Indicadores energéticos

	Tempo	Autenticações
ECC 160	10,608	3226600
AES 128	10,327	3163300
RSA 512	10,154	2270800
RSA 1024	10,404	874300
RSA 2048	11,373	276700

Tabela 6.14 Número máximo de autenticações e tempo de funcionamento (horas) na extensão do protocolo de autenticação

Anteriormente referiu-se que, devido ao sistema operativo utilizado pelo telefone móvel, não foi possível retirar indicadores de energia. Apesar desta contrariedade efectuaram-se testes ao tempo de funcionamento e ao número de autenticações que a *tag* consegue realizar de forma consecutiva. Os resultados obtidos são apresentados na tabela 6.14.

Para todas as configurações de segurança testadas com o telefone, o tempo máximo de funcionamento foi sempre superior a 10 horas e atingiu o valor máximo com RSA 2048. É de realçar que no teste efectuado, ao contrário do teste apresentado pela tabela 6.11, as autenticações são realizadas de forma consecutiva, ou seja não existem os tempos de espera para recepção de mensagens de início de autenticação.

Relativamente ao número de autenticações, os resultados obtidos estão de acordo com as ordens de grandeza do tempo de cada autenticação, à excepção da configuração AES 128, pois esperava-se que pudesse apresentar o maior número de autenticações, contudo, a falta de informação energética não permite realizar observações mais conclusivas acerca deste valor elevado, que se repetiu após inúmeras repetições do teste.

Apesar dos tempos máximos de funcionamento muito similares, verifica-se que as configurações ECC 160 e AES 128 conseguem realizar cerca de 300000 autenticações por hora. Por outro lado, as configurações com RSA 512, 1024 e 2048, tal como expectável, apresentam piores resultados, conseguindo cerca de 220000, 84000 e 24000 autenticações por hora.

6.3 Avaliação do suporte para estabelecimento do consenso geográfico

Esta secção contém os testes efectuados no simulador freemote [11], ao nível do consenso geográfico. Os testes consistem na colocação de um cenário experimental, em que se procede à variação do comportamento dos leitores nele presentes. Inicialmente, todos os leitores possuem um comportamento correcto, ou seja fornecem à estação central as coordenadas de localização que efectivamente foram obtidas no momento da leitura da *tag*. São igualmente colocados leitores incorrectos no simulador, para que injectem uma falsa localização de leitura da *tag*. Esses leitores procuram provocar uma incorrecção nos dados de consenso, obtidos pela estação central. O impacto dessas incorrecções é avaliado para diferentes parametrizações do número de leitores incorrectos no sistema. Como tal, é necessário que se apresente um método de visualização geográfico, que permita demonstrar a incorrecção de localização introduzida pelos

leitores. Por esse motivo colocou-se os registos de localização obtidos no Google Maps. Finalmente, efectua-se um teste onde todos os leitores apresentam um comportamento incorrecto.

É expectável que nos testes realizados, cujos leitores são todos correctos ou incorrectos, os resultados obtidos pelo consenso sejam todos verdadeiros ou falsos, respectivamente. Relativamente aos testes, onde existe um misto de leitores correctos e incorrectos, os resultados obtidos dependem da percentagem de leitores incorrectos e da percentagem desses leitores, que efectivamente conseguiram contactar a *tag* com sucesso. O que se espera é que à medida que se incrementa o número de leitores, a percentagem de resultados incorrectos também apresente uma tendência crescente.

Para cada variação do número de leitores incorrectos no simulador são apresentadas duas figuras. A primeira figura, inclui todos os registos recebidos por parte dos leitores, que corresponde ao comportamento do sistema caso nada fosse efectuado para refinar as coordenadas geográficas dos registos recebidos. Por outro lado, a segunda figura corresponde ao resultado do consenso efectuado pela estação central, durante o trajecto da *tag*. O resultado obtido consiste nas posições geográficas resultantes da execução do mesmo, bem como do trajecto, desenhado com cor azul clara, obtido pela estação central, que está de acordo com o valor temporal dos registos do consenso.

As duas figuras incluem dois pontos geográficos, de cor azul, que correspondem às extremidades do trajecto em linha recta de cor vermelha percorrido pela *tag*. Nas situações onde a segunda imagem não consegue demonstrar correctamente o resultado do consenso, face ao trajecto da *tag*, é colocada uma figura sobreposta a esta, com *zoom* superior para fornecer maior detalhe na visualização dos trajectos.

É de realçar que o trajecto efectuado pela *tag* é igual para todos os testes relativos ao consenso. É igualmente importante frisar que nos testes efectuados com o mesmo cenário experimental, os registos recebidos não são idênticos, pois dependem da ordem de chegada dos pedidos de registo à *tag*. Em alguns casos, significa que a estação central não chega a receber registos de todos os leitores, pois no momento em que a *tag* tratou do pedido do leitor, este já não se encontrava no seu raio de alcance.

Tal como foi referido anteriormente, o primeiro teste de localização consiste na colocação de 10 leitores com comportamento correcto no sistema. A figura 6.14 mostra os registos de

Figura 6.14 Registos de 10 leitores correctos

Figura 6.15 Consenso de 10 leitores correctos

localização geográfica efectuados pelos leitores bem comportados. O teste efectuado com esta parametrização demonstra, através da análise da figura 6.15, que o resultado do consenso está contido na zona geográfica dos registos recebidos, ou seja, efectivamente ocorreu uma agregação e refinamento das coordenadas de localização obtidas. Verifica-se igualmente que o trajecto do consenso, obtido através dos pontos resultantes, encontra-se geograficamente próximo do trajecto efectuado pela *tag*.

O teste seguinte foi efectuado de forma similar ao anterior, contudo nesta situação existem leitores com comportamento incorrecto. Estes ainda são em menor número que os correctos, logo é expectável que se obtenham posições mais próximas dos registos recebidos pelos correctos. Na configuração deste teste estão presentes 20% de leitores incorrectos para um total de 10 leitores. Tal como se pode observar, a figura 6.16 contém os registos de localização da *tag*, efectuadas por todos os leitores. Estabelecendo uma comparação desta figura com a figura 6.14, verifica-se que a grande maioria dos leitores colocaram as posições geográficas no mesmo sítio e que os leitores incorrectos injectaram no sistema localizações relativamente distantes das verdadeiras.

Como resultado deste teste, a figura 6.17 demonstra que a colocação de alguns leitores incorrectos não teve impacto nas localizações resultantes do consenso, pois as coordenadas de localização resultantes encontram-se na mesma área geográfica do trajecto da *tag*. Com esta configuração, os leitores maliciosos procuram colocar posições de localização incorrectas. No entanto, como os leitores incorrectos são em número diminuto, são descartados na selecção dos

Figura 6.16 Registos de 8 leitores correctos

Figura 6.17 Consenso de 8 leitores correctos

leitores verdadeiros. Nesta situação as posições colocadas pelos leitores maliciosos não serão alvo de tratamento na definição da posição final do consenso, pois foram descartados numa verificação preliminar do mesmo.

Figura 6.18 Registos de 6 leitores correctos

Figura 6.19 Consenso de 6 leitores correctos

No teste seguinte foram colocados 40% de leitores incorrectos, igualmente num total de 10

leitores. Os registos obtidos por todos os leitores estão representados na figura 6.18. É expectável que os resultados validados pelo consenso nesta configuração apresentem uma tendência "verdadeira", pois os leitores correctos ainda são em maior número. Com esta configuração, existem consensos que não são validados pois existem dois grupos, cujos registos dentro do grupo estão na vizinhança geográfica, mas distantes das localizações do outro grupo. Nesta situação, o sistema não consegue determinar quais são os leitores que estão a falar verdade, procedendo a um descarte dessas localizações. Por outro lado, o processamento dos registos apenas resultou num consenso validado, como se pode visualizar na figura 6.19, ou seja o número de leitores considerados como verdadeiros, numa ronda do consenso, superou os 50%.

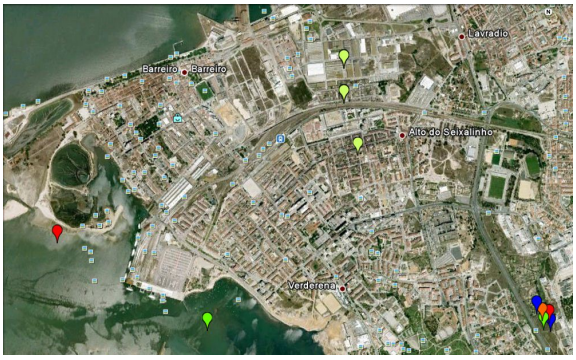

Figura 6.20 Registos de 4 leitores correctos

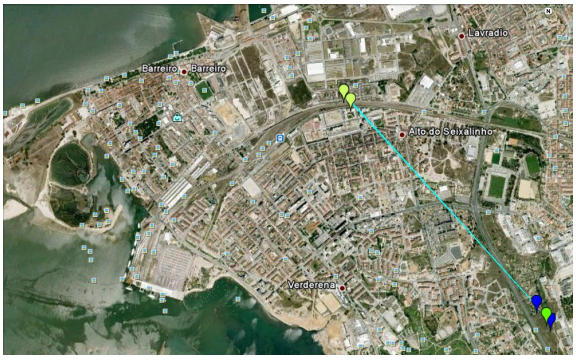

Figura 6.21 Consenso de 4 leitores correctos

Em outro teste efectuado, os leitores incorrectos pela primeira vez encontram-se em maior número (60%), logo é expectável que existam leituras correctas e incorrectas, mas tendencialmente incorrectas. Os registos obtidos nesta configuração encontram-se na figura 6.20 e o resultado do consenso está demonstrado na figura 6.21. Como se pode observar, algumas posições obtidas pelo consenso afastaram-se maioritariamente das posições originais. Tal como no teste anterior, ocorreram situações onde a estação central não conseguiu validar o consenso.

Nos restantes testes efectuados, a percentagem de leitores incorrectos é de 80% ou 100%, ou seja é expectável que a grande maioria e a totalidade dos resultados do consenso, respectivamente, seja maioritariamente incorrecto e totalmente incorrecta.

No caso onde apenas existam leitores incorrectos é previsível que as localizações finais sejam posições incorrectas, contudo, na situação onde existem 80% de leitores incorrectos é possível que resultem posições correctas. De qualquer forma, não se obtiveram essas posições, pois os leitores correctos encontraram-se sempre em número consideravelmente inferior, o que

levou a estação central a concluir, que o leitor que colocou a posição distinta dos restantes é incorrecto. O resultado deste teste demonstra que a aplicação consegue, regra geral, refinar de forma correcta as posições obtidas. Todavia, no caso de existir um aglomerado de leitores incorrectos em espaços temporais consecutivos, leva a que o sistema considere como errados os leitores correctos. Desta forma e como é expectável que os leitores correctos no sistema sejam, regra geral, em maior número que os incorrectos, estes continuam a ser penalizados pela informação incorrecta que introduzem.

6.4 Análise crítica dos resultados obtidos

Nesta secção apresenta-se as conclusões gerais dos testes efectuados ao nível do protocolo de autenticação (variantes e extensão) e consenso geográfico.

Relativamente às variantes do protocolo de autenticação, verifica-se em termos gerais, que nos parâmetros de desempenho e energia, as configurações mais eficazes são AES 128 e AES 256, seguidas da ECC 160, e por fim, as que se baseiam em RSA. Das configurações apresentadas, as que se baseiam em RSA, penalizam em demasia o tempo de processamento e latência do protocolo, o que leva a que não sejam adequados a dispositivos que exijam algumas condições de mobilidade e que necessitem de funcionar durante maiores períodos de tempo. Por outro lado, a configuração ECC 160 torna-se adequada quando se requer segurança elevada e alguma mobilidade da *tag*. Nesta configuração é de salientar a segurança futura perfeita ao nível dos identificadores, com recurso a parâmetros autenticados de Diffie-Hellman e a autenticação forte proporcionada pela assinatura ECDSA. Na situação da *tag* apresentar uma mobilidade elevada, as configurações AES 128 e AES 256 são as mais adequadas, devido à elevada *performance* e baixo custo energético.

As duas variantes apresentadas podem ser aplicadas na prática, contudo é necessário avaliar as condições do meio e o nível de segurança que se pretende na privacidade das *tags*. Através dos testes apresentados, verifica-se que a variante optimizada tem melhor desempenho e apresenta uma latência constante, ao contrário da variante completa. Por outro lado, esta variante garante uma maior segurança na cadeia de identificadores gerados, pois não apresentam relação entre si.

Analisando as variantes do protocolo, face ao que foi proposto realizar nos objectivos da

dissertação, conclui-se que a implementação e avaliação foi plenamente conseguida, na medida que foi criado um protótipo com sensores Sun SPOT, o que possibilitou a avaliação de forma experimental dos parâmetros de desempenho, latência e energia, bem como a obtenção de condições de mobilidade teóricas, face ao tempo total do protocolo, quando é executado em rede local ou *internet*.

Em relação à extensão do protocolo de autenticação, é possível concluir que o processamento do telefone móvel diluí as diferenças de desempenho que seriam expectáveis entre configurações, pois todas elas apresentam resultados bons, susceptíveis de serem aplicados na prática. Em termos energéticos, os testes possíveis de realizar não permitem retirar dados precisos, todavia, pode-se verificar que o telefone móvel, em relação aos Sun SPOT, consegue realizar um número bastante superior de autenticações, o que indicia um menor gasto energético de cada execução do protocolo, em relação à capacidade da sua bateria.

Os objectivos que foram propostos para a extensão do protocolo, foram maioritariamente cumpridos, na medida que foram retirados indicadores energéticos através da descarga completa da bateria e foi possível avaliar o desempenho do protocolo de forma experimental, através da realização de um protótipo com dispositivos NFC. De todo o modo, devido a restrições no sistema operativo do telefone móvel, apenas não foi possível retirar directamente dados energéticos.

Por último, os testes efectuados no consenso geográfico permitem verificar, em termos gerais, que a estação local consegue refinar as posições de leitura finais, bem como resistir na maioria das situações à introdução de localizações incorrectas. De todo o modo, espera-se que a percentagem de dispositivos maliciosos seja bastante inferior aos dispositivos correctos. Nessa situação o sistema consegue descartar as posições incorrectas e penalizar esses dispositivos, para que fiquem condicionados na inserção de certificados de localização na arquitectura.

Os objectivos propostos para o mecanismo de estabelecimento do consenso geográfico, como mecanismo que actua como medida de tolerância a falhas e controlo para tolerância a intrusões ao nível das estações locais, foram cumpridos. É possível analisar o comportamento de tolerância do sistema perante um determinado volume de dispositivos maliciosos, bem como a determinação de uma rota "correcta", obtida através dos pontos resultantes do consenso, permitindo melhorar a precisão das localizações calculadas pelo sistema, face ao trajecto efectuado pela *tag*, mesmo quando existem estações e leitores com comportamento incorrecto ou malicioso.

7 . Conclusões e trabalho futuro

Neste último capítulo apresenta-se um resumo com conclusões relativas à dissertação, descrevem-se alguns aspectos em aberto e apresentam-se algumas direcções para trabalho futuro.

7.1 Conclusões

A utilização de tecnologia RFID e a sua convergência com outras tecnologias de redes sem fios pode permitir a abordagem de novas aplicações que possuem requisitos particulares nas dimensões da segurança, escalabilidade, ubiquidade e fiabilidade, características que limitam a utilização de tecnologia RFID mais vulgarmente disponível. Aquela convergência é pois uma direcção de investigação interessante e promissora, que permite ultrapassar as limitações da tecnologia para sistemas RFID, tal como está hoje disponível. Esta linha de investigação apresenta porém diversos desafios e problemas, cujas soluções estão em aberto.

Na área da segurança informática são particularmente importantes e conhecidos os aspectos associados à segurança de sistemas de monitorização e gestão de alvos com identificadores de rádio-frequência, quando é necessário garantir propriedades de confidencialidade, integridade, autenticidade e protecção da privacidade dos alvos, bem como tolerar falhas de operação ou intrusões ao nível dos equipamentos que operam como leitores ou estações de detecção ou monitorização de identificadores.

Os problemas acima referidos são particularmente importantes em aplicações que envolvem detecção, monitorização ou localização de pessoas e bens. Os aspectos de segurança referenciados são particularmente relevantes em ambientes de monitorização permeada e não supervisionada, nomeadamente quando os sistemas operam em ambientes de acesso público, em ambientes não supervisionados ou ainda em situações cujo âmbito de monitorização não pode ser coordenado centralmente por uma única entidade.

São igualmente importantes os problemas impostos por requisitos de cobertura e mobilidade em grande escala ou em ambientes de localização ou detecção de um grande número de objectos em movimento.

A anterior linha de convergência entre a tecnologia RFID, as redes de sensores sem fios baseadas na normalização IEEE 802.15.4, as redes sem fios de área pessoal e a tecnologia de

telefonia móvel com suporte para NFC e leitura de objectos por RFID, é uma direcção de inspiração para os objectivos e contribuições da presente dissertação. De acordo com a anterior direcção, a dissertação propõe uma arquitectura de segurança para localização de objectos identificados por RFID para um ambiente de grande escala. A localização é baseada em protocolos de autenticação, com diversas variantes para autenticação mútua ou autenticação unilateral entre alvos, estações locais de localização e estações centrais de rastreio.

Os protocolos de autenticação propostos na dissertação, nas suas diferentes variantes, preservam condições de confidencialidade, integridade e autenticidade de todos os fluxos de informação de identificação e localização entre alvos, estações locais de detecção ou leitura desses alvos e estações centrais de rastreio, ao nível das quais se podem desenvolver aplicações específicas.

Os protocolos propostos e sua utilização na arquitectura apresentada têm em conta a preservação de condições de privacidade dos alvos de monitorização, e a incorporação de flexibilidade no balanço entre garantias de segurança e condições de mobilidade, sendo estes aspectos pedras de toque das contribuições da dissertação.

Uma segunda dimensão das contribuições da dissertação está associada à possibilidade de utilização e integração, na arquitectura proposta, de diferentes tecnologias de redes de comunicação. Esta dimensão está associada à necessidade de se suportarem diferentes cenários de aplicações de localização, vocacionadas para operarem em diferentes ambientes de *internetworking* para operação em grande escala.

Uma terceira dimensão das contribuições da dissertação está associada à característica da arquitectura para poder operar com base em cenários de localização com detecção participativa e colaborativa de alvos, de uma forma semelhante às plataformas colaborativas para sensoriamento participativo (que têm vindo a ser designadas por plataformas para *participatory sensing*). Neste sentido, a arquitectura proposta pode utilizar estações de monitorização ad-hoc, fixas ou móveis, que podem ser pertença de entidades distintas e operadas de forma autónoma, podendo ser implementadas e disponibilizadas em equipamento de uso massificado, como sejam telemóveis com suporte para NFC ou computadores com sensores de detecção de RFIDs com suporte de comunicação para IEEE 802.15.4.

Finalmente, de modo a dotar a arquitectura de critérios de resiliência face a falhas de operação de estações de localização, bem como de tolerância face a operação incorrecta provocada

por intrusões ao nível dessas estações, incorpora-se um mecanismo de processamento intermédio para agregação e estabelecimento de consensos de confiança sobre a localização de alvos. Este processamento é realizado num componente ao nível das estações centrais de rastreio, que actua a partir da informação de localização sobre os mesmos alvos obtida a partir de estações de localização independentes. Neste âmbito, diferentes estações podem enviar informação de localização sobre os mesmos alvos, de forma independente e por diferentes meios e tecnologias de comunicação, com diferentes condicionalismos e garantias de segurança ou de supervisão de operação. A informação recebida é filtrada, agregada e processada com base em mecanismos de ponderação associados à confiança na informação de localização recebida, de acordo com critérios espaciais e temporais associados às condições de observação da localização dos alvos, condições de mobilidade dos mesmos e métricas de confiança calculadas e estabelecidas para as diferentes estações.

A arquitectura, os protocolos e os mecanismos de segurança associados, foram objecto de implementação e avaliação experimental, com base num ambiente de simulação e na construção de dois protótipos de implementação:

- Um protótipo de implementação de *tags* activas materializadas em plataformas de sensores Sun SPOT e comunicação 802.15.4, sendo as estações de localização materializadas com base em sensores Sun SPOT 802.15.4, actuando como leitores de identificação interligados a um computador portátil, que está interligado por Bluetooth com um sistema de localização A-GPS, concretizado com base num telefone móvel equipado com A-GPS e comunicações Bluetooth.

- Um protótipo de implementação de *tags* passivas com base em etiquetas RFID convencionais, de leitura a curta distância e baixa frequência, e estação de localização implementada a partir de um telefone com suporte para NFC e leitura de etiquetas RFID, sendo o telefone interligado por Bluetooth com um computador portátil, materializando o processamento da estação local de localização.

A avaliação destes protótipos permitiu realizar diversos testes de viabilidade, validação experimental e comprovação das soluções propostas. Nesta validação foram avaliadas condições de latência, completamento e correcção do funcionamento dos diversos mecanismos propostos, condições de mobilidade de alvos, condições de consumo energético e avaliação do impacto

face à configuração de diferentes suites criptográficas e face a utilização de vários métodos e algoritmos criptográficos.

As observações e resultados experimentais obtidos permitem verificar a viabilidade das hipóteses e soluções propostas, tendo por base a utilização da tecnologia hoje disponível e que foi utilizada nos protótipos de avaliação.

7.2 Aspectos em aberto e trabalho futuro

Os resultados obtidos na dissertação revelam vários aspectos em aberto e direcções interessantes para trabalho futuro.

Uma possível direcção de trabalho passa por conceber e implementar redes de sensores sem fios, de densidade e cobertura adequada, que possam funcionar como redes de topologia *mesh* e estrutura de encaminhamento *multi-hop*, como ilhas de detecção de localização de alvos em movimento, preservando as mesmas garantias de segurança que foram tidas em conta na arquitectura actualmente definida. Estas redes, poderiam funcionar como redes permeadas de localização primária de objectos móveis, identificados por RFID sobre comunicação IEEE 802.15.4 ou Zigbee, podendo realizar-se aí formas de processamento intermédio para obtenção de localização confiável, com base em modelos bizantinos tolerantes a falhas ou tolerantes a intrusões ao nível dos diversos sensores de detecção de localização. Estas estruturas podem funcionar como ilhas de localização que permitiriam injectar informação confiável de localização de alvos, através de *sink nodes*, que actuariam como *gateways* para as estações locais e primária de autenticação, tal como definidas na actual arquitectura.

Outra possibilidade de trabalho poderá passar por estender a arquitectura com um nível de diversas estações intermédias, que podem ser organizadas segundo uma rede ad-hoc, de modo a poder melhorar-se as condições de escalabilidade da solução e a sua redundância.

A estrutura anterior possibilitaria formas de agregação e consenso distribuído, com maiores garantias de tolerância a intrusões em diferentes componentes e níveis da arquitectura. Uma solução como a anterior, poderia minimizar o custo computacional e a introdução de pontos centrais de falha ao nível de estações centrais de rastreio, permitindo a utilização de replicação a este nível e permitindo o estabelecimento de critérios de distribuição de carga ao nível

das estações intermédias. Estas poderiam então encarregar-se de proceder a processamento distribuído de consensos, associados à observação de localização de objectos por múltiplas estações locais e poderiam então disseminar desde logo, para níveis hierárquicos superiores, certificados de informação de localização que já agregavam consensos resultantes de processamentos intermédios envolvendo diferentes estações.

Por outro lado, revela-se necessário proceder a testes mais extensos e de maior cobertura e escala, para se aferir do comportamento da arquitectura e dos protocolos, quando suportados pelas soluções tecnológicas endereçadas na dissertação e face a um incremento da quantidade de alvos detectados que se movimentem na área de cobertura de estações de monitorização. Estes testes deverão permitir obter primariamente informação real, do tipo da informação observada pelos testes experimentais iniciais realizados na presente dissertação e que pode depois ser usada como informação de entrada e de calibração para novas avaliações de escalabilidade e carga de processamento, só possíveis de realizar num ambiente de simulação que deverá ter que ser criado para o efeito.

Bibliografia

[1] Wireless medium access control and physical layer specifications for low-rate wireless personal area networks, IEEE Standard, 802.15.4, 2006.

[2] Market study covers the future of rfid. *Gartners RFID Market Trends*, Jan 2008.

[3] Rfid technology: An update vision. *ISRC Technology Briefing Series*, 2008.

[4] Bluetooth, June 2009. `http://www.bluetooth.com/bluetooth/technology/`.

[5] EPCglobal, June 2009. `http://www.epcglobalinc.org`.

[6] MICA2, July 2009. `http://www.xbow.com/products/Product_pdf_files/Wireless_pdf/MICA2_Datasheet.pdf`.

[7] Sun SPOT, November 2009. `https://www.sunspotworld.com`.

[8] TELOSB, July 2009. `http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/TelosB_Datasheet.pdf`.

[9] ZigBee Alliance, June 2009. `http://www.zigbee.org/`.

[10] 3GPP TS 35.202: Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi specification". 3GPP. 2009., May 2010. `http://www.3gpp.org/ftp/Specs/html-info/35202.htm`.

[11] Freemote, January 2010. `http://www.assembla.com/wiki/show/freemote`.

[12] JAX-WS, January 2010. `https://jax-ws.dev.java.net/`.

[13] Polygon Area and Centroid, January 2010. `http://local.wasp.uwa.edu.au/~pbourke/geometry/polyarea`.

[14] Via Verde, January 2010. `http://www.viaverde.pt/ViaVerde/vPT/`.

[15] Wireless Safe Car, February 2010. `http://www.imob-iberia.com`.

[16] B. Aboba. Extensible authentication protocol (eap). RFC3748, United States, June 2004.

[17] Frank Adelstein, Sandeep KS Gupta, Golden Richard Iii, and Loren Schwiebert. *Fundamentals of Mobile and Pervasive Computing*, chapter Security in Wide Area Networks, pages 357–367. McGraw-Hill Professional, 2005.

[18] Frank Adelstein, Sandeep KS Gupta, Golden Richard Iii, and Loren Schwiebert. *Fundamentals of Mobile and Pervasive Computing*, chapter Security in Wireless Local Area Networks, pages 329–346. McGraw-Hill Professional, 2005.

[19] Frank Adelstein, Sandeep KS Gupta, Golden Richard Iii, and Loren Schwiebert. *Fundamentals of Mobile and Pervasive Computing*, chapter Security in Wireless Personal Area Networks, pages 317–328. McGraw-Hill Professional, 2005.

[20] Manfred Aigner and Martin Feldhofer. Secure symmetric authentication for rfid tags. *Telecommunication and Mobile Computing*, 2005.

[21] Henning Baars, Hans-Georg Kemper, Heiner Lasi, and Marc Siegel. Combining rfid technology and business intelligence for supply chain optimization scenarios for retail logistics. In *HICSS '08: Proceedings of the Proceedings of the 41st Annual Hawaii International Conference on System Sciences*, page 73, Washington, DC, USA, 2008. IEEE Computer Society.

[22] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede. An elliptic curve processor suitable for rfid-tags. Cryptology ePrint Archive, Report, 2006/227.

[23] Erik-Oliver Blass, Anil Kurmus, Refik Molva, and Thorsten Strufe. Psp: private and secure payment with rfid. In *WPES '09: Proceedings of the 8th ACM workshop on Privacy in the electronic society*, pages 51–60, New York, NY, USA, 2009. ACM.

[24] Burton H. Bloom. Space/time trade-offs in hash coding with allowable errors. *Commun. ACM*, 13(7):422–426, 1970.

[25] V. Bocan and V. Cretu. Mitigating denial of service threats in gsm networks. page 6, April 2006.

[26] David E. Boyle and Thomas Newe. On the implementation and evaluation of an elliptic curve based cryptosystem for java enabled wireless sensor networks. *Sensors and Actuators A: Physical*, October 2009.

[27] Gabriel Bracha. An asynchronous [(n - 1)/3]-resilient consensus protocol. In *PODC '84: Proceedings of the third annual ACM symposium on Principles of distributed computing*, pages 154–162, New York, NY, USA, 1984. ACM.

[28] José Bravo, Ramon Hervas, Gabriel Chavira, and Salvador Nava. Adapting technologies to model contexts: Two approaches through rfid and nfc. In *ICDIM*, pages 683–688. IEEE, 2007.

[29] Gregor Broll, Susanne Keck, Paul Holleis, and Andreas Butz. Improving the accessibility of nfc/rfid-based mobile interaction through learnability and guidance. In *MobileHCI '09: Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services*, pages 1–10, New York, NY, USA, 2009. ACM.

[30] Halil Ibrahim Bulbul, Ihsan Batmaz, and Mesut Ozel. Wireless network security: comparison of wep (wired equivalent privacy) mechanism, wpa (wi-fi protected access) and rsn (robust security network) security protocols. In *e-Forensics '08: Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop*, pages 1–6, ICST, Brussels, Belgium, Belgium, 2008. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[31] J. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, and M. B. Srivastava. Participatory sensing. In *Workshop on World-Sensor-Web (WSW'06): Mobile Device Centric Sensor Networks and Applications*, pages 117–134, 2006.

[32] J. Burke and D. et al. Estrin. Participatory sensing. In *Proc. of the 1st Workshop on World - Sensor Web - Mobile Device Centric Sensor Networks and Applications - co-locates with the 4th ACM Conference on Embedded Networked Sensor Systems*, 2006.

[33] Christian Cachin, Klaus Kursawe, and Victor Shoup. Random oracles in constantipole: practical asynchronous byzantine agreement using cryptography (extended abstract). In *PODC '00: Proceedings of the nineteenth annual ACM symposium on Principles of distributed computing*, pages 123–132, New York, NY, USA, 2000. ACM.

[34] Srdjan Capkun and Jean pierre Hubaux. Secure positioning of wireless devices with application to sensor networks. In *IEEE Infocom*, 2005.

[35] Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance. In *OSDI '99: Proceedings of the third symposium on Operating systems design and implementation*, pages 173–186, Berkeley, CA, USA, 1999. USENIX Association.

[36] Khosla R. Chowdhury, B. Rfid-based hospital real-time patient management system. pages 363 –368, July 2007.

[37] P. Coulton, O. Rashid, and R. Edwards. *RFID Handbook: Applications, Technology, Security and Privacy*, chapter RFID and NFC Phones, pages 375–390. CRC Press, 2008.

[38] T. Dierks. The transport layer security (tls) protocol. RFC5746, United States, August 2008.

[39] Danny Dolev and Andrew C. Yao. On the security of public key protocols. Technical report, Stanford, CA, USA, 1981.

[40] Orr Dunkelman, Nathan Keller, and Adi Shamir. A practical-time attack on the a5/3 cryptosystem used in third generation gsm telephony. Cryptology ePrint Archive, Report 2010/013, 2010. `http://eprint.iacr.org/`.

[41] A. Mason et al. Rfid and wireless sensor network integration for intelligent asset tracking systems. 2005.

[42] Emory A Fry and Leslie A Lenert. Mascal: Rfid tracking of patients, staff and equipment to enhance hospital response to mass casualty events. *AMIA Annu Symp Proc*, pages 261–5, 2005.

[43] Yuli Fu and Qi Fu. Scheme and secure protocol of mobile payment based on rfid. In *ASID'09: Proceedings of the 3rd international conference on Anti-Counterfeiting, security, and identification in communication*, pages 631–634, Piscataway, NJ, USA, 2009. IEEE Press.

[44] R.L. Graham. An efficient algorith for determining the convex hull of a finite planar set. In *Information Processing Letters*, pages 132–133, 1972.

[45] Amir Herzberg. Payments and banking with mobile personal devices. *Commun. ACM*, 46(5):53–58, 2003.

[46] Loc Ho, Melody Moh, Zachary Walker, Takeo Hamada, and Ching-Fong Su. A prototype on rfid and sensor networks for elder healthcare: progress report. In *E-WIND '05: Proceedings of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis*, pages 70–75, New York, NY, USA, 2005. ACM.

[47] Simon Hoff, Michael Meyer, and Joachim Sachs. Analysis of the general packet radio service (gprs) of gsm as access to the internet, 1998.

[48] ITU-T. Recommendation x.509. Technical report, August 2005.

[49] Bong-Keun Jeong and Ying Lu. The impact of radio frequency identification (rfid) investment announcements on the market value of the firm. *J. Theor. Appl. Electron. Commer. Res.*, 3(1):41–54, 2008.

[50] Don Johnson, Alfred Menezes, and Scott Vanstone. The elliptic curve digital signature algorithm (ecdsa. Technical report, 1999.

[51] A. Juels. Rfid security and privacy: a research survey. *Selected Areas in Communications, IEEE Journal on*, 24(2):381–394, Feb. 2006.

[52] T. Laughlin Kevin Hamed, D. Ledford. Monitoring non-breeding habitat activity by subterranean detection of ambystomatid salamanders with implanted passive integrated transponder (pit) tags and a radio frequency identification (rfid) antenna system. *Herpetological Review - Society for the Study of Amphibians and Reptiles*, 39(3):303–306, 2008.

[53] Vivek Khandelwal. Envisioning a world with nfc-enabled phones. *RFID Journal*, May 2010.

[54] Sungjun Kim, Doohyun Ko, and Sunshin An. Geographical location based rfid tracking system. In *WOWMOM '08: Proceedings of the 2008 International Symposium on a World of Wireless, Mobile and Multimedia Networks*, pages 1–3, Washington, DC, USA, 2008. IEEE Computer Society.

[55] Karl Koscher, Ari Juels, Vjekoslav Brajkovic, and Tadayoshi Kohno. Epc rfid tag security weaknesses and defenses: passport cards, enhanced drivers licenses, and beyond. In *CCS '09: Proceedings of the 16th ACM conference on Computer and communications security*, pages 33–42, New York, NY, USA, 2009. ACM.

[56] Mr Ralf Kreher and Torsten Ruedebusch. *UMTS Signaling: UMTS Interfaces, Protocols, Message Flows and Procedures Analyzed and Explained*. Wiley, 2007.

[57] Ching-Huan Kuo and Houn-Gee Chen. The critical issues about deploying rfid in healthcare industry by service perspective. In *HICSS '08: Proceedings of the Proceedings of the 41st Annual Hawaii International Conference on System Sciences*, page 111, Washington, DC, USA, 2008. IEEE Computer Society.

[58] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. *ACM Trans. Program. Lang. Syst.*, 4(3):382–401, 1982.

[59] Marc Langheinrich. A survey of rfid privacy approaches. *Personal Ubiquitous Comput.*, 13(6):413–421, 2009.

[60] Ze Li, Haiying Shen, and Baha Alsaify. Integrating rfid with wireless sensor networks for inhabitant, environment and health monitoring. In *ICPADS '08: Proceedings of the 2008 14th IEEE International Conference on Parallel and Distributed Systems*, pages 639–646, Washington, DC, USA, 2008. IEEE Computer Society.

[61] Vance Lockton and Richard Rosenberg. Rfid: The next serious threat to privacy. *Ethics and Information Technology*, 7(4):221–231, December 2005.

[62] Konrad Lorincz and Matt Welsh. Motetrack: a robust, decentralized approach to rf-based location tracking. *Personal Ubiquitous Comput.*, 11(6):489–503, 2007.

[63] Santi Martínez, Magda Valls, Concepció Roig, Josep M. Miret, and Francesc Giné. A secure elliptic curve-based rfid protocol. *Journal of Computed Science and Technology*, vol. 24(2):pages 309–318, March 2009.

[64] Moffat Mathews and Ray Hunt. Evolution of wireless lan security architecture to ieee 802.11i (wpa2). In *AsiaCSN '07: Proceedings of the Fourth IASTED Asian Conference on Communication Systems and Networks*, pages 292–297, Anaheim, CA, USA, 2007. ACTA Press.

[65] Shengguang Meng, Wei Chen, Gang Liu, Shitong Wang, and Liu Wenyin. An asset management system based on rfid, webgis and sms. In *ICUIMC '08: Proceedings of the 2nd international conference on Ubiquitous information management and communication*, pages 82–86, New York, NY, USA, 2008. ACM.

[66] Jelena Misic and Vojislav B. Misic. *Wireless Personal Area Networks: Performance, Interconnections and Security with IEEE 802.15.4*, chapter Operation of the IEEE 802.15.4 Network, pages 17–38. Wiley, 2008.

[67] Geoff Mulligan. The 6lowpan architecture. In *EmNets '07: Proceedings of the 4th workshop on Embedded networked sensors*, pages 78–82, New York, NY, USA, 2007. ACM.

[68] E. Ngai, K. Moon, F. Riggins, and C. Yi. Rfid research: An academic literature review (1995-2005) and future research directions. *International Journal of Production Economics*, 112(2):510–520, April 2008.

[69] Pedro Peris-lopez, Julio Cesar Hern, Juan M. Estevez-tapiador, and Arturo Ribagorda. Emap: An efficient mutual authentication protocol for low-cost rfid tags. In *In: OTM Federated Conferences and Workshop: IS Workshop*, pages 352–361. Springer-Verlag, 2006.

[70] Lenin Ravindranath, Venkata N. Padmanabhan, and Piyush Agrawal. Sixthsense: Rfid-based enterprise intelligence. In *MobiSys '08: Proceeding of the 6th international conference on Mobile systems, applications, and services*, pages 253–266, New York, NY, USA, 2008. ACM.

[71] Amit Rawal. Rfid: The next generation auto-id technology. Vol. 52(No. 3), Mar 2009.

[72] C.M. Roberts. Radio frequency identification (rfid). *Computers and Security*, 25(1):18 – 26, 2006.

[73] Naveen Sastry and David Wagner. Security considerations for ieee 802.15.4 networks. In *WiSe '04: Proceedings of the 3rd ACM workshop on Wireless security*, pages 32–42, New York, NY, USA, 2004. ACM.

[74] Claus-Peter Schnorr. Efficient signature generation by smart cards. *J. Cryptology*, 4(3):161–174, 1991.

[75] R. Shirey. Internet security glossary. RFC2828, United States, May 2000.

[76] S.M. Siddique and M. Amir. Gsm security issues and challenges. pages 413–418, June 2006.

[77] Boyeon Song and Chris J. Mitchell. Rfid authentication protocol for low-cost tags. In *WiSec '08: Proceedings of the first ACM conference on Wireless network security*, pages 140–147, New York, NY, USA, 2008. ACM.

[78] W. Stallings. *Cryptography and Network Security, 4 ed.* Prentice Hall, 2006.

[79] William Stallings. *Cryptography and Network Security Principles and Practices*, pages 531–544. Prentice Hall, 2005.

[80] William Stallings and Lawrie Brown. *Computer Security Principles and Practice*, pages 656–662. Prentice Hall, 2008.

[81] Bo Sun, Yang Xiao, Chung Chih Li, Hsiao-Hwa Chen, and T. Andrew Yang. Security co-existence of wireless sensor networks and rfid for pervasive computing. *Comput. Commun.*, 31(18):4294–4303, 2008.

[82] Batbold Toiruul and KyungOh Lee. An advanced mutual-authentication algorithm using aes for rfid systems. *Journal of Computer Science and Network Security*, vol. 6:pages 156–162, 2006.

[83] Athanasios S. Voulodimos, Charalampos Z. Patrikakis, Alexander B. Sideridis, Vasileios A. Ntafis, and Eftychia M. Xylouri. A complete farm management system based on animal identification using rfid technology. *Computers and Electronics in Agriculture*, 70(2):380 – 388, 2010. Special issue on Information and Communication Technologies in Bio and Earth Sciences.

[84] Roy Want. An introduction to rfid technology. *IEEE Pervasive Computing*, 5(1):pages 25, 2006.

[85] Ron Weinstein. Rfid: A technical overview and its application to the enterprise. *IT Professional*, 7:27–33, 2005.

[86] A. Wheeler. Commercial applications of wireless sensor networks using zigbee. *Communications Magazine, IEEE*, 45(4):pages 70–77, April 2007.

[87] Tan-Hsu Tan Yu Liu and Yu-Ling Chu. Outdoor natural science learning with an rfid-supported immersive ubiquitous learning environment. *Journal of Educational Technology and Society*, 12(4):161–175, 2009.

[88] Yan Zhang and Paris Kitso. *Security in RFID and Sensor Networks*, chapter Analysis, Modeling, and Implementation, pages 56–59. CRC Press, 2009.

[89] Yan Zhang and Paris Kitso. *Security in RFID and Sensor Networks*, chapter Public Key in RFIDs: Appeal for Asymmetry, pages 195–216. CRC Press, 2009.

[90] Hongzi Zhu, Minglu Li, Yanmin Zhu, and Lionel M. Ni. Hero: Online real-time vehicle tracking. *IEEE Trans. Parallel Distrib. Syst.*, 20(5):740–752, 2009.