Universidade do Minho
Escola de Engenharia

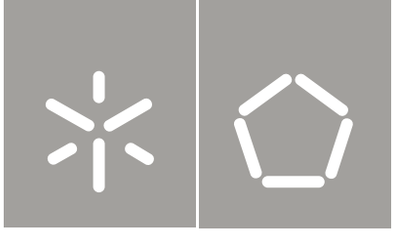
Henrique Joaquim Duarte da Silva

Uma Solução de *Handover* Seguro com QoS em Redes Veiculares

outubro de 2013

Henrique Joaquim Duarte da Silva Uma Solução de *Handover* Seguro com QoS em Redes Veiculares

UMinho | 2013



Universidade do Minho
Escola de Engenharia

Henrique Joaquim Duarte da Silva

Uma Solução de *Handover* Seguro com QoS em Redes Veiculares

Tese de Mestrado
Ciclo de Estudos Integrados Conducentes ao
Grau de Mestre em Engenharia de Comunicações

Trabalho efetuado sob a orientação do
Professor Doutor Nuno Vasco Lopes

e co-orientação do
Professor Doutor Alexandre Santos

outubro de 2013

DECLARAÇÃO

Henrique Joaquim Duarte da Silva

Endereço electrónico: a44040@alunos.uminho.pt Telefone: 911720027

Número do Bilhete de Identidade: 12928755

Título da Tese:

Uma Solução de *Handover* Seguro com QoS em Redes Veiculares

Orientador:
Professor Doutor Nuno Vasco Lopes
Co-orientador:
Professor Doutor Alexandre Santos
Ano de conclusão: 2013
Tese submetida na Universidade do Minho para a obtenção do grau de
Mestre em Engenharia de Comunicações

Universidade do Minho, ___/___/_____

Assinatura: _____

Agradecimentos

No decorrer do meu percurso académico pude sempre contar com o apoio de várias pessoas cruciais na minha vida e às quais não posso deixar de expressar os meus sinceros agradecimentos.

Agradeço aos meus orientadores neste projecto, Professor Doutor Nuno Vasco Lopes e Professor Doutor Alexandre Santos por todo o apoio prestado durante a elaboração da minha dissertação em que o conhecimento transmitido e os conselhos dados muito contribuíram para o meu enriquecimento a nível técnico e pessoal.

Aos meus amigos, Pedro Carvalho, Ricardo Rodrigues, Filipe Miranda, Manuel Pereira, Marcelo Silva, Diogo Sousa, Pedro Veloso, Alípio Duarte e Paulo Duarte pela camaradagem e paciência com que me apoiaram, muito obrigado!

Ao meu amigo Eng.º Fernando Veloso, pelo auxílio e pelo conhecimento transmitido, deixo um agradecimento especial.

À Carlota, por saber compreender os meus diferentes estados de espírito e pela motivação que sempre me tentou transmitir, muito obrigado!

Por último, mas não menos importante, agradeço a todos os elementos da minha família que sempre me apoiaram ao longo deste percurso e em especial àqueles que tudo fizeram para que eu chegasse até aqui e a quem dedico esta minha dissertação: Aos meus pais e irmão!

Resumo

As redes veiculares surgiram como um caso particular de redes *ad hoc* móveis denominadas por MANETS (*Mobile Ad-hoc Networks*), formando um campo específico de pesquisa na área de redes de computadores. As VANETs, (*Vehicular Ad-hoc Networks*) têm sido alvo de várias pesquisas científicas para o desenvolvimento do Sistema Inteligente de Transporte, sendo agora possível incluir nos automóveis software inteligente que melhorara a qualidade de vida dos condutores, através por exemplo de aplicações de entretenimento das quais se destaca a aplicação VoIP (*Voice Over Internet Protocol*).

Neste tipo de redes, devido à elevada mobilidade dos veículos ocorre a perda de conectividade entre dispositivos, essa perda de conectividade deve-se ao facto de um dispositivo móvel trocar de rede, a este processo dá-se o nome de *handover*. Constituindo o *handover* um grave problema nas redes veiculares, principalmente aquando da utilização de aplicações tempo-real como é o caso da aplicação VoIP, é relevante desenvolver mecanismos que melhore a gestão do *handover*.

Neste trabalho é apresentada uma solução que corresponde à execução de uma fase de pré-registo. Esta solução foi desenvolvida no sentido de se alcançar um *handover* seguro e com qualidade de serviço. Relativamente à segurança esta solução baseia-se no protocolo SIP (*Session Initiation Protocol*) e possibilita a utilização de um mecanismo de autenticação mútua através de troca de chaves. Quanto à qualidade de serviço a solução permite diminuir substancialmente o número de *handovers*, tendo a velocidade dos veículos e o número de RSUs (*Road Side Units*) espalhados pela estrada um papel preponderante na análise da mesma.

Pela simulação realizada, através dos resultados obtidos foi possível verificar a eficiência desta solução para a obtenção de um *handover* seguro e com qualidade de serviço.

Palavras-chaves – VANETs; VoIP; Mobilidade; *Handover;* Fase de pré-registo; Autenticação mútua.

Abstract

Vehicular networks have emerged as a particular case of mobile ad hoc networks called for MANETs (*Mobile Ad-hoc Networks*) forming a specific investigation field of computer networks. The VANETs (Vehicular Ad-hoc Networks) has been the subject of several scientific researches for the development of Intelligent Transportation Systems. Now its possible to include intelligent software in cars for improving the comfort of drivers, through entertainment applications, for instance, VoIP (Voice Over Internet Protocol) applications.

In this type of networks due to the high mobility of vehicles there are a lot of losses when a handovers occurs. The handover process is a serious problem in vehicular networks,especially when we are running real-time applications such as VoIP. Therefore, it is important to develop mechanisms to enhance the management of handover in vehicular networks.

The goal of this work is to propose a solution that underlying on a pre-registration phase that is used to exchange security and QoS parameters previously to the occurrence of one handover. This solution was developed in order to achieve a secure handover with quality of service. The results obtained show that the solution can substantially reduce the number of handovers, improving this way the quality of the service in a VoIP application.

Keywords – VANETs; VoIP; Mobility; Handover*;* pre-registration phase; Mutual authentication.

Índice

Lista de Figuras

Lista de Tabelas

Lista de Acrónimos

AAA Server	*Authorization and Accounting Server*
AKA	*Authentication and Key Agreement*
AP	*Access Point*
ARP	*Address Resolution Protocol*
BSP	*Basic Support Protocol*
BU	*Binding Update*
CK	*Canetti-Krawczk*
CN	*Correspondent Node*
CoA	*Care-of-Address*
DHCP	*Dynamic Host Configuration Protocol*
DoS	*Denial of Service*
ECDH	*Elliptic Curve Diffie-Hellman*
FMIPv6	*Fast Handovers for Mobile IPv6*
FN	*Foreign Network*
GPS	*Global Positioning System*
HA	*Home Agent*
HI	*Handover Initiate*
HN	*Home Network*
HR	*Home Redirect*
ICMP	*Internet Control Message Protocol*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
IPSec	*Internet Protocol Security*
LMA	*Local Mobility Anchor*
MAC	*Media Access Control*
MAG	*Mobile Access Gateway*
MANET	*Mobile Ad-hoc Network*
MD5	*Message Digest 5*
MIH	*Media Independent Handover*
MIPv4	*Mobile IPv4*
MIPv6	*Mobile IPv6*
MN	*Mobile Node*
MOS	*Mean Opinion Score*
NAKE	*New Authenticated Key Exchange*
NAR	*New Access Router*
NEMO	*Network Mobility*
NS2	*Network simulation 2*
OBU	*On-Board Unit*

OLSR	*Optimized Link State Routing Protocol*
P2P	*Peer to Peer*
PAR	*Previous Access Router*
PKIs	*Public Key-Infrastructures*
PMIPv6	*Proxy Mobile IPv6*
PrRtAdv	*Proxy Router Advertisement*
QoS	*Quality of service*
RA	*Router Advertisement*
RPTC	Rede Pública de Telefonia Comutada
RSS	*Received Signal Strengh*
RSU	Road Side Unit
RTP	*Real-time Transport Protocol*
RTT	*Round Trip Time*
RySolPR	*Router Solicitation for Proxy Advertisement*
S/MIME	*Secure/Multipurpose Internet Mail Extensions*
SCPKs	*Self-certified public keys on eliptic curves*
SCTP	*Stream Control Transmission Protocol*
SDP	*Session Description protocol*
SIP	*Session Initiation Protocol*
SPB	*Speed Probability-Based*
S-VHO	*speed-based, Qos-oriented Vertical Handover*
TA	*Trusted Authority*
TIGGER	*Topologically Integrated Geographic Encoding and Referencing*
TLS	*Transport Layer security*
UA	*User Agent*
UDP	*User datagram Protocol*
URI	*Uniform Resource Identifier*
URL	*Uniform Ressource Locator*
V2I	*Vehicle to Infrastructure*
V2V	*Vehicle to Vehicle*
VANET	*Vehicular ad-hoc Network*
VoIP	*Voice Over Internet Protocol*
VOVAN	*VoIP over VANETs*
VR	*Visited Redirect*

CAPÍTULO 1

Introdução

1.1. Enquadramento Geral e Motivações

Nos últimos anos tem-se verificado uma evolução dos dispositivos de comunicação sem fio (telemóveis, portáteis, etc.), causando um exponencial crescimento das redes que possuem como característica fundamental facultar a comunicação entre nós sem a necessidade de uma infra-estrutura, essas redes são denominadas por redes *ad-hoc*. Sendo que as principais capacidades que estas redes detêm é o facto de permitirem a livre movimentação dos nós, de serem facilmente acessíveis e de rápida instalação.

As redes veiculares, são consideradas como um subconjunto das redes *ad hoc*, denominadas por MANETs (*Mobile Ad-hoc Network*) e têm cada vez mais preponderância na vida quotidiana de um indivíduo. Estas redes têm como finalidade garantir a segurança no trânsito, oferecer comunicação aos motoristas e passageiros e oferecer vários tipos de aplicações tais como: aplicações de segurança e aplicações de conforto entre as quais se destacam as de entretenimento, tal como, a aplicação VoIP (*Voice Over Internet Protocol*) [5]. Contudo, este tipo de rede acarreta diversos desafios, proporcionando uma motivação extra aos investigadores a fim de encontrar uma solução adequada para os mesmos. Os desafios encontrados estão relacionados com a mobilidade e com a comunicação entre os nós, visto que a dificuldade no estabelecimento da conectividade entre dispositivos resulta das rápidas mudanças na topologia da rede como consequência da alta mobilidade dos veículos.

A mobilidade pode ser classificada em vários tipos, no entanto em redes veiculares a mobilidade é mais problemática ao nível do IP. Para combater a mobilidade IP surgem vários protocolos entre eles temos o MIPv4, o MIPv6, FMIPv6 e o PMIPv6. A gestão desta mobilidade pode ser melhorada através de uma melhor gestão da componente do *handover*.

Uma boa gestão do *handover* pode permitir que um dispositivo móvel troque de rede mantendo as suas conexões activas. O *handover* pode ser classificado em dois

tipos: vertical e horizontal. A execução do *handover* deve obedecer a políticas bem definidas tal como a largura de banda, custo, segurança, cobertura de rede e qualidade de serviço. A segurança e a qualidade de serviço serão o foco desta dissertação, uma vez que o desenvolvimento da mesma consiste na proposta de uma solução que permita executar um *handover* seguro baseado no protocolo SIP e que seja capaz de suportar aplicações *real-time* (VoIP), garantindo sempre níveis de qualidade de serviço adequados.

1.2. Objectivos

Esta dissertação tem como principal objectivo desenvolver uma solução que permita alcançar um *handover* seguro e com qualidade de serviço em aplicações de tempo-real, nas redes veiculares. No entanto, para que esse objectivo seja atingido é necessário desenvolver certas tarefas: como identificar problemas resultantes da mobilidade IP num contexto de rede veiculares, estudar a utilização de um protocolo como forma de garantir um processo de *handover* seguro e com elevada qualidade de serviço. Com base nestes propósitos fazer o levantamento de diversas soluções encontradas na literatura, para depois se proceder á comparação e análise das mesmas e elaborar o estado de arte.

Depois de elaborado o estado de arte com as diversas soluções encontradas é necessário escolher uma e com base nela propor uma solução de mobilidade IP segura e com qualidade de serviço para redes veiculares. Essa proposta terá de ser simulada verificando se os resultados obtidos terão vão de encontro aos resultados verificados na solução escolhida.

Por último é necessário retirar as devidas conclusões quanto ao trabalho realizado, fazendo a respectiva análise da proposta, comparando-a à solução escolhida e propor algumas tarefas que poderão ser realizadas num trabalho futuro.

1.3. Estrutura da Dissertação

Esta dissertação está organizada em cinco capítulos, sendo os três primeiros considerados capítulos introdutórios, o quarto aborda a solução proposta para esta dissertação e o quinto consiste numa conclusão do trabalho realizado.

O primeiro Capítulo diz respeito à “Introdução”, neste capítulo para além de ser destacada a importância das redes veiculares na vida quotidiana de um indivíduo, é identificado o problema referente à segurança e à qualidade de serviço para aplicações de tempo-real neste tipo de redes. Neste capítulo também serão identificados alguns objectivos que se pretende alcançar no desenvolvimento desta dissertação.

O segundo Capítulo é referente aos “Conceitos Relacionados”, neste capítulo serão apresentados alguns conceitos teóricos necessários para uma melhor percepção do problema abordado nesta dissertação. Serão expostos conceitos relacionados com as redes veiculares como as suas características e aplicações. Será explicada a aplicação de tempo-real, VoIP, como mais ênfase sobre a qualidade de serviço na mesma. Serão descritos conceitos, tais como conceito de mobilidade, onde se identifica alguns tipos de mobilidade existentes, conceito de *handover* identificando os diferentes tipos de *handover*, procedimentos e tarefas do mesmo e, por fim, conceito inerente ao protocolo SIP, onde se descreve a arquitectura do mesmo, a sua relação com a mobilidade e segurança.

O Capítulo três nomeado de “Estado de Arte” descreve alguns trabalhos relacionados resultantes da pesquisa de alguns artigos referentes à qualidade de serviço e segurança no *handover* para aplicações de tempo-real.

O Capítulo quatro denominado de “Proposta de *handover* seguro com QoS para aplicações de tempo-real em redes veiculares” diz respeito à apresentação da proposta de *handover*, com base nessa proposta serão efectuadas duas simulações para dois cenários distintos, o que permitirá obter determinados resultados para uma posterior análise e comparação.

O último capítulo, intitulado “Conclusões”, contém uma conclusão técnica de todo o trabalho desenvolvido bem como algumas sugestões que futuramente poderão ser desenvolvidas como forma de melhorar os resultados obtidos.

CAPÍTULO 2

Conceitos Relacionados

2.1. Redes Veiculares

A possibilidade de comunicação em ambientes móveis, sem recurso a qualquer tipo de infra-estrutura, tem motivado um elevado interesse na exploração das redes móveis designadas por MANETs [12]. A ampliação deste tipo de redes para um ambiente rodoviário deu origem a uma nova área de estudo designada por VANETs, as quais tem como finalidade o melhoramento das condições de circulação do tráfego rodoviário de forma segura e eficiente e proporcionando conforto aos utilizadores

As redes *Ad Hoc* Veiculares (VANETs) são consideradas uma subclasse das redes MANETs e têm como finalidade a comunicação entre veículos e/ou entre veículos e infra-estruturas localizadas na margem das ruas ou estradas, podendo essas infra-estruturas serem designadas por torres de comunicação móvel ou mesmo por um ponto de acesso externo para uma comunicação.

A VANET é uma abordagem que fornece novos serviços e aplicações e possui características diferentes de uma rede tradicional, como poderá ser verificado nas secções a seguir.

2.1.1. Características de uma rede veicular

Para o desenvolvimento de aplicações ou serviços para VANETs é necessário a utilização de novas técnicas em relação às redes sem fios convencionais, visto que as redes VANETs têm de lidar com elevadas mudanças nas suas conexões e com diferentes tipos de densidade da rede.

- **Arquitectura**

Uma arquitectura em rede veicular permite definir o modo como os nós se organizam e comunicam. De acordo com [13] nas redes veiculares podemos encontrar três tipos de arquitectura, os quais serão demonstrados na figura 2.1.

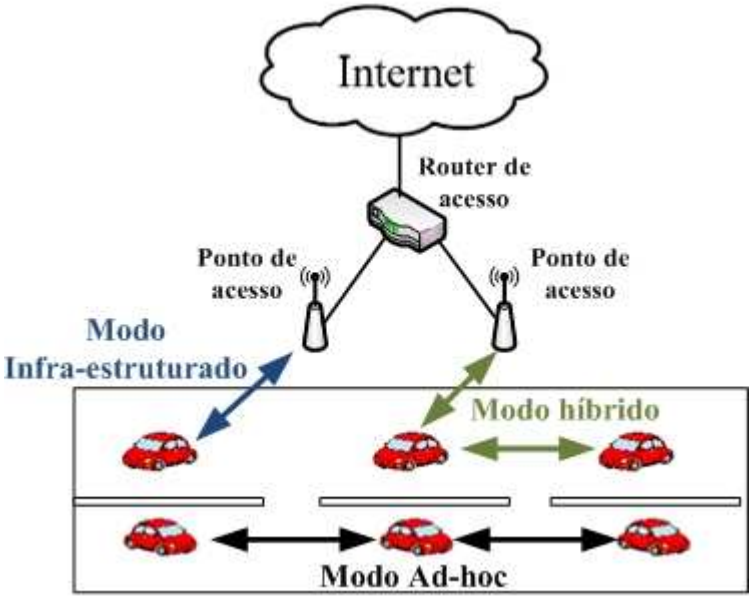


Figura 2.1 – Tipo de arquitectura em redes veiculares.

Os três tipos de arquitectura verificados na figura 2.1 são os seguintes:

- **Infra-estruturado:** Nesta arquitectura a comunicação estabelece-se entre um veículo e uma infra-estrutura (V2I – *Vehicle to Infrastructure*), sendo o acesso à internet e o encaminhamento de mensagens possíveis através do uso de pontos de acesso APs (Access Point). Os APs têm a funcionalidade de centralizar o tráfego da rede, servindo como nós intermediários das comunicações. Este tipo de arquitectura tem como vantagem o aumento da conectividade e a possibilidade de estabelecer a comunicação com outras redes, como é o caso da Internet e como desvantagem o facto que para garantir uma conectividade sempre activa é necessário um elevado número de APs, o que em termos práticos leva a um aumento considerável do valor da sua montagem.

- ***Ad hoc*:** Neste tipo de arquitectura todos os nós móveis comunicam entre si sem que exista um nó principal que funcione como encaminhador das comunicações. A comunicação estabelece-se de veículo para veículo (V2V - *Vehicle to Vehicle*), em que cada veículo desempenha o papel de *router* e encaminha o tráfego através de múltiplos saltos. Tem como principal desvantagem a conectividade depender da densidade e do padrão de mobilidade dos veículos. Apesar disso é uma das arquitecturas mais utilizadas em pesquisas [12], devido ao seu baixo custo e sua elevada flexibilidade de implantação.

- **Híbrida:** A arquitectura híbrida resulta da combinação das arquitecturas infra-estruturada e *ad hoc*, ou seja, é a combinação da comunicação V2I e V2V. Assim, se dois nós pretenderem estabelecer comunicação entre si, essa comunicação poderá ocorrer através de pontos de acesso, ou então, através de uma comunicação ad hoc.

- **Comparação entre redes veiculares e redes sem fio tradicional (ex: wifi…)**

Nesta secção serão apresentadas algumas características comparativas entre redes veiculares e redes sem fio tradicional [14].

- **Auto-configuráveis:** Tal como as redes sem fio tradicional, as redes veiculares possuem a capacidade de se auto-configurar, ou seja, automaticamente a rede é capaz de configurar vários parâmetros como: endereçamento, encaminhamento e controle da potência de transmissão e recepção do sinal.

- **Mobilidade:** Através da mobilidade podemos definir o padrão de movimentos dos nós móveis (ex: veículos). Uma vez que um automóvel pode atingir altas velocidades, a mobilidade dos nós nas redes veiculares é muito elevada. A circulação dos veículos é limitada a uma topologia fixa, isto é, a circulação dos veículos limita-se apenas a ruas e avenidas. Dos vários modelos, na literatura de redes veiculares destacam-se três, como se pode verificar na figura 2.2.

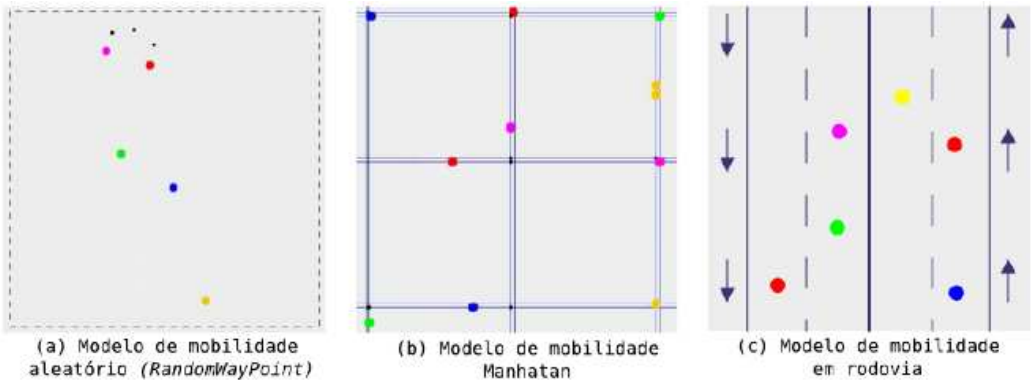


Figura 2.2 – Exemplos de modelos de mobilidade [1].

Na figura 2.2 (a) verifica-se os nós a movimentarem-se aleatoriamente, o que corresponde a um modelo de mobilidade típico das redes móveis *ad hoc*. A figura 2.2 (b) mostra o modelo de *mobilidade Manhattan* [15], que é um modelo

onde os nós param em cada cruzamento de estradas e escolhem a direcção que pretendem seguir. A figura 2.2 (c) apresenta um modelo de mobilidade em rodovia, onde se pode verificar diversas interacções entre os veículos que tanto circulam na mesma direcção como em direcções opostas.

Em suma, contrariamente às redes sem fios tradicionais, as redes veiculares possuem limitações geográficas e não podem ser levadas para qualquer lugar, isto é, há limitações nas trajectórias dos seus nós.

- **Velocidade de transmissão:** A velocidade de transmissão em redes veiculares contrariamente às redes sem fios tradicionais é considerada rápida. Pois para além de os veículos neste tipo de redes poderem atingir velocidades consideradas elevadas e instáveis, eles podem circular em direcções opostas o que leva a terem apenas alguns segundos para a transmissão de dados.

- **Topologia:** Em redes veiculares, tal como nas redes sem fio tradicionais a mudança na topologia é rápida, uma vez que os veículos na rede estão em constante movimento com velocidades elevadas.

- **Energia:** Na maior parte das redes sem fios, a energia nos nós é limitada, pois os dispositivos, caso não haja uma fonte de energia eléctrica, dependem do tempo de vida das suas baterias. Em redes veiculares, os veículos tanto podem ser equipados com ampla potência/energia como podem ser equipados com recursos computacionais significativos [16].

- **Largura de banda:** Tal como as redes sem fios tradicionais, as redes veiculares são dependentes da capacidade do hardware para realizar uma determinada comunicação.

- **Fragmentação da rede:** A fragmentação da rede poderá ocorrer devido ao alcance do raio de comunicação e pelo elevado dinamismo dos veículos. Normalmente as redes sem fios estão sujeitas a breves períodos de perda de conectividade, no entanto, em redes veiculares o período de perda de conectividade costuma ser maior especialmente em período de tráfego elevado.

Em resumo, na comparação entre redes veiculares e redes sem fios tradicionais verificou-se que existem diferenças significativas sendo que as principais são a velocidade dos nós na rede, o tempo de transmissão que os nós têm para transmitir dados e a fragmentação da rede.

Relativamente às redes celulares, as redes veiculares possuem duas vantagens significativas [17]:

- **Comunicação Directa:** Em comparação com as redes celulares, nas redes veiculares os veículos podem comunicar directamente entre si, sem o recurso a uma estação base, diminuindo assim o atraso da comunicação. Além disso, a comunicação entre veículos pode ser efectuada em áreas que as redes de telefonia móvel podem não conseguir operar, por exemplo em áreas rurais.

- **Ausência de Taxa de Serviço:** Contrariamente às redes celulares, as redes veiculares não necessitam de infra-estruturas de comunicação, nem de um fornecedor de serviço.

2.1.2. Aplicações das redes veiculares

Uma vez que os automóveis são cada vez mais preponderantes na vida das pessoas, as redes veiculares têm sofrido um enorme crescimento, sendo cada vez mais alvo de inúmeras pesquisas científicas nos últimos anos.

Embora o impulso inicial para VANET fosse a segurança no trânsito, rapidamente surgem outros tipos de preocupações. Actualmente os exemplos mais discutidos são dois tipos de aplicações [18], aplicações que dizem respeito à segurança e aplicações que dizem respeito ao conforto.

- **Aplicações de Segurança**

Nas redes veiculares estes tipos de aplicações visam à promoção da segurança dos condutores. Neste tipo de redes os veículos podem comunicar entre si, o que leva a que informações importantes possam ser partilhadas e utilizadas. Estas aplicações tanto podem utilizar comunicações V2V, como V2I ou então ambas. De acordo com [19] as aplicações de segurança podem ser classificadas em cinco categorias:

- **Sistema de anti-colisão em cruzamentos:** Os sistemas anti-colisão baseiam-se na comunicação V2I e/ou V2V. As infra-estruturas presentes nos cruzamentos recolhem as informações dos veículos que se encontram próximos, essas informações recolhidas por sensores são analisadas para determinar se existe alguma situação de risco que possa provocar um acidente. Caso exista, será enviada uma mensagem de alerta aos veículos que se encontram naquela área.

- **Segurança pública:** Este tipo de aplicações tem como objectivos minimizar o tempo de viagem das equipas de emergência e facilitar o pedido de assistência médica em caso de acidente, precavendo assim acidentes secundários.

- **Sinalização:** Utilizando a comunicação V2I, através de mensagens enviadas periodicamente, esta aplicação tem como motivação alertar os condutores sobre as diversas sinalizações presentes na via, evitando futuras distracções por parte dos mesmos.

- **Diagnóstico e manutenção dos veículos:** Têm como objectivo alertar os proprietários dos veículos sobre defeitos que podem comprometer a sua segurança e sobre programas de manutenção dos seus veículos.

- **Informações de outros veículos:** Esta aplicação utiliza a comunicação entre os veículos, obtendo informação diversificada relativamente aos mesmos. Alguns exemplos de aplicações desta categoria são: alerta de mudança de faixa, alerta sobre a condição da via e alerta de colisão.

- **Aplicações de Conforto**

Cada vez mais, as pessoas passam a maior parte do seu tempo conduzindo, logo um dos objectivos nas redes veiculares é melhorar a qualidade de vida desses condutores, fornecendo para isso aplicações de conforto. Podem ser implementadas aplicações comuns na internet, como correio electrónico, ou então, aplicações baseadas na interacção entre veículos tais como: jogos, aplicações de partilha de ficheiros entre utilizadores ou aplicações VoIP.

Muitas dessas aplicações utilizam sistemas par-a-par (P2P – *Peer to Peer*) em vez do modelo cliente-servidor, visto que nas redes veiculares muitas aplicações

utilizam uma arquitectura *ad hoc.* Sendo as aplicações P2P viáveis no contexto das redes veiculares, estas envolvem aplicações de diversos tipos, entre elas a aplicação VoIP.

De acordo com [20] , as aplicações P2P podem ser classificadas quanto ao papel do veículo na gestão de dados.

- **Fonte de dados:** Nesta categoria de aplicação os veículos recolhem e produzem dados, através de diversos sensores, como câmara de vídeo, detectores químicos ou sensores acústicos. Assim, um veículo pode, captar imagens das ruas, processando-as e encaminhando-as em forma de mensagem para outros veículos alertando-os sobre possíveis acidentes ou congestionamentos.

- **Consumidor de dados:** Neste tipo de categoria os veículos podem adquirir vários tipos de dados que vão desde arquivos de multimédia a dados sobre as condições da via. Por exemplo durante uma viagem, o condutor ou o passageiro pode utilizar aplicações do tipo multimédia, como *streaming* de filmes, musica e aplicações de localização que tanto pode servir para o auxílio de navegação como para entregar anúncios que possam interessar aos utilizadores.

- **Consumidor e produtor de dados:** Nesta categoria destacam-se aplicações interactivas, como o VoIP e/ou jogos *online* ou não. Sendo que estas aplicações solicitam comunicação em tempo real entre veículos.

- **Intermediário:** Nas categorias de aplicações descritas anteriormente é necessário confiar em veículos intermediários. Pois esses veículos podem fornecer armazenamento temporário para outros, assim como encaminhar dados ou consultas, melhorando a qualidade do desempenho da aplicação.

2.2. *Voice Over Internet Protocol*

Voz sobre IP (VoIP) pode ser definido como a forma de comunicação de voz sobre uma rede IP. Cada vez mais, VoIP tem ganho interesse e atenção por parte de investigadores e empresas. Existe duas razões essenciais para VoIP estar a substituir a Rede Pública de Telefonia Comutada (RPTC), a primeira, deve-se ao facto de VoIP

fornecer funcionalidades adicionais e flexíveis, por exemplo, VoIP pode ser integrada em outros serviços de internet como sistemas *groupware* (software que permite o auxilio a pessoas envolvidas em tarefas comuns e fornece uma interface para um ambiente partilhado, ex: chat e *wiki* e sistemas de gestão de relacionamento de clientes, a segunda, VoIP trouxe convergência de voz, vídeo e dados através da mesma infra-estrutura, reduzindo assim custos de instalação e manutenção [21].

Apesar das várias vantagens que esta tecnologia de comunicação possui, o sucesso da mesma, tem de ter em conta factores de qualidade de serviço e segurança.

2.2.1. Qualidade de serviço em VoIP

Para que as funcionalidades provenientes de uma arquitectura VoIP sejam executadas com sucesso é necessário uma qualidade de serviço aceitável [22]. A seguir serão identificados alguns factores que podem influenciar a qualidade de serviço em comunicações VoIP.

- **Atraso:** Podemos definir atraso como o tempo que o emissor demora a capturar a fala até a mensagem ser ouvida pelo receptor. A forma como poderá ocorrer um atraso pode ser dividido em dois tipos: atraso fixo e atraso variável. O primeiro diz respeito aos atrasos relacionados com o processamento de sinal, como é o caso o atraso relativo à fonte e o atraso relativo ao receptor. O segundo refere-se aos atrasos relacionados com a propagação do sinal na rede, denominado por atraso na rede.

  Em relação ao atraso na fonte podemos identificar os seguintes atrasos: o tempo que demora a criar blocos de amostra de sinal, o tempo que demora a comprimir as amostras baseado nas características humanas, tempo para preencher pacote com valores de amostra do sinal e tempo para transmitir os pacotes pela rede. No atraso relacionado com a rede é possível identificar-se o atraso provocado pelo tempo que demora a transmissão do pacote na rede e o atraso provocado pelo tempo nas filas de espera dos vários equipamentos de rede. Por fim o atraso correspondente ao receptor identifica-se o atraso relativo ao tempo que demora a armazenar pacotes num *buffer* de forma a serem exibidos na ordem e no tempo correcto e o tempo que demora a processar os pacotes de voz recebidos para serem exibidos.

- ***Jitter:*** Podemos definir *jitter* como atrasos variáveis que são criados ao longo da chamada, pois o caminho que cada pacote assume pode ser diferente, o que leva a uma variação estatística dos atrasos de entrega dos pacotes que ocorrem durante a recepção. Esta variação é um factor importante para a degradação da qualidade de serviço. Quando acentuados, os seus efeitos tornam a conversa imperceptível porque os atrasos variáveis da entrega que os pacotes sofrem irá quebrar a continuidade do tráfego em diferentes pontos de sessão.

  Para minimizar estes efeitos do *jitter* recorre-se ao *buffer jitter*, este permite armazenar os pacotes recebidos para posteriormente serem exibidos pela ordem temporal correcta, o que faz com que seja eliminada a supressão de espaços de silêncio entre palavras e a introdução de silêncio. O tamanho do pacote do *buffer* terá de ser aceitável, pois se este for reduzido os pacotes serão descartados e se for elevado levará um aumento do atraso.

- **Perda de pacotes:** Numa comunicação VoIP, a retransmissão de pacotes perdidos não é aconselhada, pois sendo este tipo de comunicação uma aplicação de tempo-real, um pacote retransmitido não chegaria a tempo de ser reaproveitado. No entanto, a perda de um pacote não é critico, pois como os pacotes de áudio são pequenos esta perda pode ser compensada através de *codecs*, capazes de fazer a correlação entre o pacote recebido e o pacote que irá receber depois de ter perdido um pacote, ou substituí-lo por um semelhante ao último recebido.

  Quando ocorrem perdas de pacotes, normalmente não é só um pacote que fica perdido mas vários, o que aumenta a degradação. Estas perdas poderão ocorrer em filas de espera nos equipamentos ou em *buffers*. Segundo os autores em [23] podemos qualificar um nível relacionado com essas perdas, sendo assim quando as perdas atingem valores inferiores a 1% podem tornar a chamada imperceptível, mas o *codec* pode ajudar a recuperar. Se as perdas alcançarem valores superiores a 5% é considerado um cenário catastrófico e nem os *codecs* podem ajudar a recuperar.

- **Largura de Banda:** Nos dias de hoje a largura de banda não é um factor crítico para VoIP, no entanto, apesar de a rede ter evoluído relativamente aos seus valores de capacidade, esta é partilhada por vários serviços com diferentes

necessidades, o que leva a que a largura de banda seja um factor limitativo do número de chamadas em simultâneo.

Um dos factores que mais contribui para o aumento da carga da largura de banda é a utilização de protocolos de segurança, torna-se essencial reavaliar o número de chamadas de acordo com o aumento de dados gerados pelos protocolos. Uma má avaliação pode levar a uma exaustão da largura de banda, podendo levar à indisponibilidade do serviço. Em caso de ataque a qualidade de serviço pode ficar comprometida, como é exemplo a ameaça DoS (*denial of service),* onde a largura de banda é consumida até à exaustão impedindo que utilizadores legítimos tenham acesso ao serviço [23].

2.2.2. E-Model

Como referenciado anteriormente são vários os factores que influenciam a qualidade das ligações na comunicação VoIP. Portanto tornou-se necessário avaliar o impacto que esses factores poderão ter nas comunicações entre utilizadores. Para isso, foi determinado pelos autores de [24] um método designado por MOS (*Mean Opinion Score*), cujo objectivo é avaliar o efeito dos sistemas e componentes nas transmissões, através da atribuição de uma pontuação com uma escala de 1 (má) a 5 (excelente).

No entanto como este método de acordo com [25] é de difícil reprodução e de complexa aplicabilidade em larga escala, foi elaborado um método alternativo designado por *E-Model* [10]. Este método fornece um modelo computacional útil para análises preditivas e mede directamente transmissões indicando o tipo de qualidade de voz que resulta das mesmas.

- **Visão geral sobre o E-Model**

O resultado de um cálculo com o E-Model é o factor de taxa de transmissão *R*, que combina todos os parâmetros relevantes considerados para uma conexão. Este é composto por [10]:

$$R = Ro - Is - Id - Ie + A \qquad \textbf{Eq.2.1}$$

Em que o factor *Ro* representa os efeitos da relação sinal-ruído, tal como ruído de ambiente e ruído do circuito; *Is* representa o factor degenerativo simultâneo e resulta das transmissões degenerativas causadas por uma distorção quantificada; *Id* representa o

factor degenerativo de atraso associado a atrasos na rede; *Ie* representa o factor degenerativo de equipamentos associado ao equipamento utilizado. *A* representa o factor de expectativa, considerado um factor de correcção que ajusta a qualidade percepcionada baseada na expectativa do utilizador. Desta equação resulta o valor escalar *R*, o qual varia na escala de 0 até 100. Como podemos verificar na Tabela 2.1 [9], este valor pode ser convertido à escala MOS (*Mean Opinion Score*), representando o nível de percepção dos utilizadores.

Tabela 2.1 - Avaliação da chamada VOIP [9].

Valor R	MOS	Avaliação dos Utilizadores
90	4.34	Muito Satisfatório
80	4.03	Satisfatório
70	3.6	Alguns utilizadores insatisfeitos
60	3.1	Muitos utilizadores insatisfeitos
50	2.58	Quase todos os utilizadores insatisfeitos

De seguida será apresentado o procedimento para a obtenção do valor dos diferentes factores que compõe a equação 2.1. Denotar que para resolver as diversas equações que nos permitem obter tais valores é necessário a utilização de uma tabela (Tabela 2.2) de valores padrão [10].

Tabela 2.2 - Valores padrão para o cálculo de *R* [10].

Parameter	Abbr.	Unit	Default value
Send loudness rating	SLR	dB	+8
Receive loudness rating	RLR	dB	+2
Sidetone masking rating	STMR	dB	15
Listener sidetone rating	LSTR	dB	18
D-Value of telephone, send side	DS	-	3
D-Value of telephone, receive side	DR	-	3
Talker echo path loss	TELR	dB	65
Weighted echo path loss	WEPL	dB	110
Mean one-way delay of the echo path	T	ms	0
Round-trip delay in a 4-wire loop	Tr	ms	0
Absolute delay in echo-free connections	Ta	ms	0

Number of quantization distortion units	qdu	-	1
Equipment impairment factor	Ie	-	0
Packet-loss robustness factor	Bpl	-	4.3
Random packet-loss probability	Ppl	%	0
Burst raio	BurstR	-	1
Circuit noise referred to 0 dBr-point	Nc	dBm0p	-70
Noise floor at the receive side	Nfor	dBmp	-64
Room noise at the send side	Ps	dB(A)	35
Room noise at the receive side	Pr	dB(A)	35
Advantage factor	A	-	0

- **Relação básica sinal-ruído, *Ro***

Como já foi referido anteriormente, *Ro* representa a relação básica sinal-ruído, incluindo ruídos no lado do emissor, no circuito de transmissão, no ambiente e na sensibilidade do sistema auditivo humano. A equação que permite obter o valor deste factor é a seguinte:

$$Ro = 15 - 1.5(SLR + No) \qquad \textbf{Eq. 2.2}$$

Em que *SLR* representa o nível de intensidade no emissor e o *No* é a adição de todas as fontes de ruído. Consoante as respectivas equações que resultam do cálculo de *Ro* [10] e utilizando os valores padrão da tabela 2.2 tem-se em *Ro* equivalente a 94,77.

- **Factor degenerativo simultâneo, *Is***

O factor *Is* é a soma de todas as degradações que ocorrem mais ou menos simultaneamente com a transmissão de voz, como podemos verificar na seguinte equação:

$$Is = Iolr + Ist + Iq \qquad \textbf{Eq. 2.3}$$

Em que, *Iolr* representa a degradação da qualidade causada pelo volume de áudio muito alto, *Ist* representa a interferência causada pela voz do locutor no seu

próprio auscultador de ouvido (*sidetone*) e *Iq* representa degradação dada pela quantização decorrente da digitalização do sinal de voz.

Utilizando os valores padrão da Tabela 2 definidos em [10], estima-se o valor do factor *Is* em 1,41.

- **Factor degenerativo de atraso, *Id***

As perdas causadas pelo atraso são calculadas pelo factor *Id*, o qual também é subdividido em três componentes como podemos ver na seguinte equação:

$$Id = Idte + Idle + Idd \qquad \textbf{Eq. 2.4}$$

Através dos factores *Idte* e *Idle* obtêm-se uma estimação do impacto com o eco no lado do emissor e receptor respectivamente. O factor *Idd* representa a deterioração causado por um atraso total.

Para o cálculo da componente *Idd* são considerados três parâmetros diferentes associados com o tempo de transmissão: O *Ta* representa o atraso total entre o emissor e receptor; o *T* consiste no atraso médio percorrido pelo eco; *Tr* representa o atraso de ida e volta (*Round-trip delay*) no circuito a quatro fios, isto é, circuito que contém uma separação física entre os dois sentidos de comunicação [10].

- **Factor degenerativo de equipamentos, *Ie***

O factor *Ie* resulta de transmissões degenerativas causadas por codificadores de taxa reduzida de bits e pela perda de frames no codificador [10] .

Os valores de *Ie* são constantemente actualizados e poderão ser observados na tabela seguinte.

Tabela 2.3 – Exemplos de valores provisórios do factor *Ie* para diferentes codecs [11].

Codec type	Reference	Operating rate [kbit/s]	*Ie* value
PCM	G.711	64	0
ADPCM	G.726, G727	40	2
	G.721, G.726, G.727	32	7
	G.726, G.727	24	25
	G.726, G.727	16	50
LD-CELP	G.728	16	7

		12.8	20
CS-ACELP	G.729	8	10
	G.729-A + VAD	8	11
VSELP	IS-54	8	20
ACELP	IS-641	7.4	10
QCELP	IS-96A	8	21
RCELP	IS-127	8	6
VSELP	Japanese PDC	6.7	24
RPE-LTP	GSM 06.10, full-rate	13	20
VSELP	GSM 06.20, half-rate	5.6	23
ACELP	GSM 06.20, enhanced full-rate	12.2	5
ACELP	G.723.1	5.3	19
MP-MLQ	G.723.1	6.3	15

- **Factor de Vantagem, *A***

Este factor permite compensar factores de perdas ou de deterioração, quando existe outras vantagens no uso. Assim sendo, um utilizador tem a capacidade de ser tolerante em relação à tecnologia e ao ambiente de uso, sendo essa capacidade considerada para a determinação final do cálculo de qualidade.

Um exemplo é quando um utilizador efectua uma conversação fixa ou móvel, nesta última os utilizadores aceitam uma deterioração maior que na primeira.

Para diferentes tipos de comunicação em [10] especificam valores provisórios do factor *A* como pode ser verificado na tabela 2.4.

Tabela 2.4 - Exemplos provisórios para o factor de vantagem, *A* [10].

Exemplo de sistema de comunicação	**Máximo valor para A**
Convencional (Telefonia fixa)	0
Comunicação móvel para redes celulares *in-door*	5
Comunicação móvel para redes geográficas ou redes Veiculares	10
Locais de difícil acesso (ex: redes com ligações a satélites)	20

2.2.3. Segurança na utilização do VoIP

A protecção do VoIP exige processos complexos, porque para executar a maioria dos ataques em VoIP não é necessário ter acesso físico aos recursos, basta conhecer minimamente a rede IP. Por isso, é importante identificar as ameaças a que uma comunicação VoIP está sujeita, para assim ser mais fácil definir as medidas de segurança que possam proteger o VoIP contra comportamentos hostis. Sendo então essencial qualificar as ameaças para se poder quantificar o seu risco, com base no documento [26] foram divididas nas seguintes categorias:

- **Ameaças sociais:** Nesta categoria os ataques têm em comum uma ligação próxima entre a vítima e o atacante, ou seja, para a concretização destes ataques é necessário uma interacção social entre o intruso e a vitima.

- **Intercepções:** Nesta categoria as ameaças têm com o objectivo monitorizar, capturar e reproduzir o fluxo da sessão recorrendo a processos ilegais. O VoIP encontra-se muito susceptível a esta ameaça, pois coloca em perigo a confidencialidade no sistema VoIP

- **Recolha e modificação:** Os ataques relacionados com recolha e modificação colocam em causa a integridade e confidencialidade das comunicações VoIP. Neste tipo de ataques o objectivo é recolher e/ou alterar a informação dos pacotes, podendo eliminar, introduzir ou substituir por outro conteúdo.

- **Negação de serviço:** Os ataques desta categoria colocam em causa a disponibilidade do serviço VoIP, levando à interrupção do serviço. O objectivo destes ataques é irritar a vítima de forma intencional, sem ter um interesse pessoal.

2.3. *Handover*

Se um dispositivo conectado a um *router* de acesso (AP) se afasta da área de cobertura, o nível do sinal do dispositivo vai enfraquecendo e ao se aproximar de outro *router* de acesso, com um nível de sinal mais forte, é necessário um mecanismo na rede

para que nessa transição, o estado da conexão se mantenha, transferindo a responsabilidade da comunicação ao novo *router* de acesso. Ao mecanismo que faz a transferência de conexão para um novo *router* de acesso denomina-se por *handover*.

2.3.1. Tipos e Procedimentos de *Handover*

De acordo com o tipo de tecnologia de redes sem fios o *handover* pode ser classificado em *handover* horizontal e *handover* vertical [27].

Handover horizontal ocorre entre pontos de acesso de mesma tecnologia em termos de: cobertura, velocidade de transmissão e mobilidade.

Handover vertical ocorre entre pontos de acesso com tecnologias diferentes, ou seja, é usado para redes heterogéneas que diferem em muitos aspectos tal como: largura de banda e frequência do sinal. Comparado com os *handovers* horizontais, estas características particulares dificultam a implementação dos *handovers* verticais, no entanto surgem padrões de forma a auxiliar na sua implementação, tal como o IEEE 802.21.

Relativamente ao procedimento de um *handover* [28] este pode ser dividido numa primeira fase em: detecção, atribuição e transferência. Nesta fase é executada tarefas de identificação de quando existe uma necessidade de iniciar um *handover*, a alocação e atribuição de um canal de comunicação, bem como a transferência do sinal da antiga para a nova estação. Esta fase é executada ao nível da camada física e depende da tecnologia sem fio adoptada.

Numa segunda fase em actualização. Esta fase tem como principal objectivo actualizar a informação relativa à localização do dispositivo móvel, para que os pacotes sejam direccionados sempre para a nova localização. Nesta fase pode-se utilizar várias técnicas para reduzir a latência e perda de pacotes. Aqui estão em foco os protocolos de mobilidade baseados em IP, que actuam na camada de rede.

2.3.2. Tarefas do *handover*

Na camada de rede, nos protocolos de mobilidade baseados em IP, tal como: MIP, a detecção do *handover*, é efectuada através de mensagens *Agent Advertisements* emitidas pela estação base. Um dispositivo móvel quando recebe uma mensagem deste tipo é capaz de identificar a ocorrência de uma transição e, a partir daí, iniciar um *handover*.

Para a execução de algumas tarefas, tem que se ter em conta as características da rede, dos protocolos de mobilidade utilizados e alguns requisitos das aplicações. No entanto, os protocolos de *handover*, utilizam diferentes técnicas para executar essas tarefas, tendo sempre como principal objectivo minimizar a latência e perdas durante o mesmo. Algumas tarefas que se podem efectuar na camada de rede são [28]:

- **Autenticação e permissão de acesso:** esta tarefa envolve alguns processos que permitem verificar se o dispositivo móvel está autorizado a autenticar-se a uma nova estação base. Essas funções são designadas por funções AAA – *Authentication, Authorization, Accouting.*

- **Reserva de recursos e atribuição de canais:** esta tarefa consiste na alocação de recursos em uma ou mais estações base candidatas. Por exemplo, reservar estruturas de buffer para um armazenamento temporário de pacotes nas estações base. Para que um *handover* seja considerado "suave", isto é, *soft handover*, é necessário uma pré-alocação de recursos no início do mesmo.

- **Actualização da rede:** esta tarefa consiste basicamente actualizar a informação da localização do dispositivo móvel, garantindo assim que os pacotes sejam encaminhados correctamente. Para a promoção de um *soft handover*, a tarefa de actualização deve ser executada antecipadamente, se houver uma identificação prévia de uma ou mais estações base candidatas.

- **Controle e optimização do fluxo de pacotes:** Nesta tarefa são utilizados vários mecanismos com o objectivo de reduzir atrasos, variações de atraso (*jitter*), minimizar a perda de pacotes e duplicações. Alguns mecanismos utilizados são: *buffering*, para o armazenamento de pacotes nas estações base; *forwarding points*, para o redireccionamento de pacotes para a nova estação base; replicação do fluxo de pacotes;

2.4. Mobilidade

O termo mobilidade no enquadramento de redes móveis é normalmente utilizado para classificar o movimento que uma entidade móvel produz, quando se desloca de um ponto de acesso para outro.

Na mobilidade as tecnologias de redes sem fios apresentam características diferentes que se adequam a cenários distintos, na Figura 2.3 podemos observar a relação da mobilidade com a taxa de transmissão (*throughput*) para as diferentes tecnologias [2].

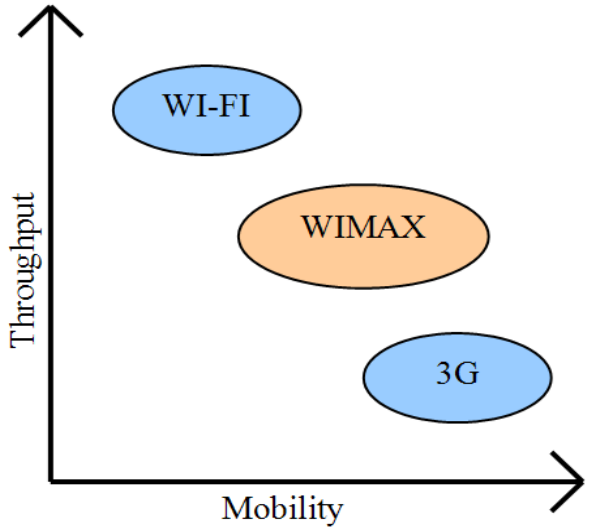


Figura 2.3 – Comparação entre várias tecnologias sem fios [2].

Através da Figura 2.3 podemos concluir que a tecnologia sem fios *Wi-Fi* não é adequada para grandes áreas, com grandes deslocações como por exemplo, deslocamento de veículo entre dois pontos a uma distância considerável. Esta tecnologia vai funcionando relativamente bem em espaços reduzidos como deslocações em centros comerciais, cafés e hospitais.

Pela mesma figura também se pode concluir que a tecnologia 3G é extremamente constante em relação à mobilidade, conseguem abranger uma grande área geográfica. No que diz respeito à taxa de transmissão é limitada, sendo mesmo inferior ás tecnologias *Wi-Fi* e *Wimax*.

Por fim, também pela análise da Figura podemos afirmar que a melhor relação existente entre taxa de transmissão e a mobilidade ocorre para a tecnologia *Wimax.*

O conceito de mobilidade é vasto e podemos classificar a mobilidade em vários tipos. Assim sendo temos a mobilidade Pessoal, considera as movimentações de um utilizador que está sempre em movimento entre diferentes terminais; a mobilidade de Sessão consiste no tratamento das transferências de sessões de aplicações em execução de um terminal para o outro; a mobilidade de rede que está relacionada com os deslocamentos de uma rede móvel; e por fim, a mobilidade IP que é o tipo de mobilidade frequentemente mencionada e a qual receberá uma explicação pormenorizada no capitulo seguinte.

2.4.1. Mobilidade IP

Este tipo de mobilidade permite que os terminais móveis mantenham o mesmo IP quando se deslocam entre diferentes redes e que possam encaminhar os pacotes, do terminal móvel ou para o terminal móvel, de uma forma transparente para as camadas superiores. Do ponto de vista da camada de rede trata-se de um mecanismo adequado tanto para redes homogéneas como para redes heterogéneas.

A mobilidade na rede IP pode ser dividida em Micro-Mobilidade e Macro-Mobilidade [29] um exemplo destes dois tipos de mobilidade IP pode ser observado na Figura 2.4.

A Micro-Mobilidade diz respeito à mobilidade dentro do mesmo domínio, não afectando assim a camada de rede IP. A solução para este tipo de mobilidade está relacionada com a utilização de protocolos entre pontos de acesso e tem como objectivo o melhoramento na qualidade do sinal.

A Macro-Mobilidade diz respeito à mobilidade entre diferentes domínios, o que afecta a camada de rede IP. A resolução dos problemas para este tipo de mobilidade, implica a utilização de alguns protocolos, como por exemplo o MIPv4 e o MIPv6.

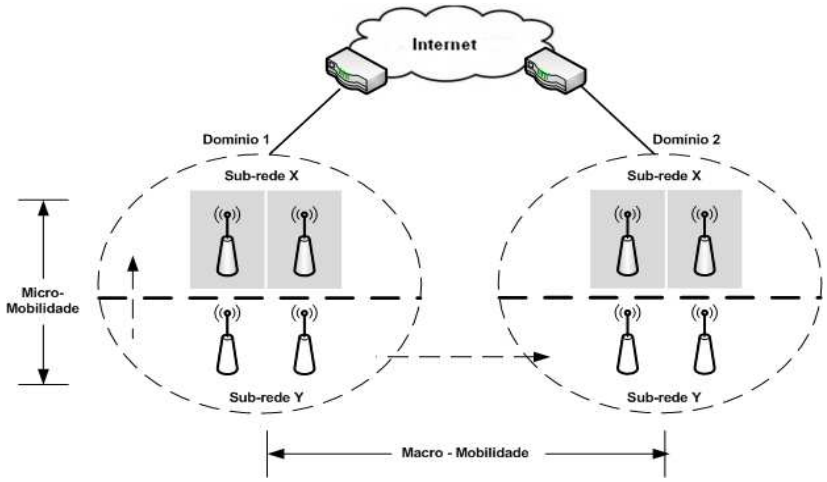


Figura 2.4 – Micro-Mobilidade e Macro-Mobilidade.

2.4.2. Protocolos de Mobilidade

Para uma melhor compreensão dos conceitos relacionados com protocolos de mobilidade é necessário um enquadramento com a terminologia. Sendo assim, o MN (*Mobile Node)* é um terminal móvel que se movimenta de uma rede para outra, mantendo a comunicação com um nó correspondente denominado por CN (*Correspondent Node)*. O MN está sempre acessível no seu *Home Address*, através do seu *Home Agent*, o que faz com que possa movimentar-se sem que as suas comunicações e ligação à rede sejam quebradas. O *Home Address* consiste num endereço IP especial que permanece inalterado, independentemente da posição do terminal móvel. Ou seja, quando o terminal móvel está na rede origem, é-lhe atribuído um *Home Address* mas, quando se movimentar é-lhe atribuído um endereço provisório, *Care-of-Address*.

A troca de uma rede HN (*Home Network)* para uma rede FN (*Foreign Network*) por parte de um MN, é controlada por um *router* denominado por HA (*Home Agent*), o qual tem a capacidade de receber e encaminhar todos os pacotes entre o MN e o CN. A comunicação entre o MN e o CN é implementada por túneis.

Denotar que o MN, o HA e o FA são três novas entidades implementadas para protocolos de mobilidade [30], a seguir podemos ver uma descrição mais pormenorizada das mesmas.

- ***Mobile Node* (MN)**: é considerado terminal móvel e pode movimentar-se de uma rede para outra mantendo o seu endereço IP constante, permitindo assim a continuidade de comunicação com outros nós.

- ***Home Agent* (HA):** é um *router* que se encontra presente na *Home Network* do MN e é responsável por registar a localização do MN permitindo que este esteja sempre detectável. Esta entidade tem a capacidade de enviar datagramas IP para o *Care-of Address* (CoA) actual da MN através da utilização de um túnel.

  O CoA é o ponto de terminação do túnel com o HA. Permite ao MN estar sempre detectável enquanto se encontra fora da sua HN. Existem dois tipos de CoA, o *foreign agent CoA*, diz respeito ao endereço do FA onde o MN se registou e o *co-located CoA*, que é um endereço local obtido externamente que o MN associa como uma das suas interfaces de rede, neste caso a utilização do FA deixa de ser necessária.

- ***Foreign Agent* (FA):** é um *router* que se encontra presente na *Foreign Network.* Enquanto o MN se encontrar na sua rede este fornece serviços de encaminhamento de forma a mantê-lo sempre acessível. Recebe os datagramas enviados pelo HA via túnel entregando-os ao MN.

A maioria dos trabalhos envolvendo Mobilidade IP tem como principal objectivo reduzir a latência gerada pela troca de mensagens de sinalização previstas na definição do protocolo. Podemos afirmar que inicialmente os protocolos de Mobilidade IP podem ser classificados relativamente à sua versão IP, MIPv4 e MIPv6. O MIPv6 suporta constantes evoluções, passando a existir algumas extensões do mesmo, tal como: FMIPv6 e PMIPv6.

- **MIPv4**

O Mobile IPv4 (MIPv4) trata-se de um protocolo que visa a permitir a mobilidade IP utilizando como protocolo de endereçamento o IPV4. Como já foi referido anteriormente o MIPv4 é um protocolo utilizado para resolver problemas de macro-mobilidade.

Para que a mobilidade no protocolo MIPv4 seja possível existem três tipos de mecanismos [30]: descoberta do CoA (*Care-of-Address*), registo do CoA e *Tunneling* para o CoA.

No primeiro para descoberta do CoA é necessário a utilização de mensagens ICMP *Router Advertisement* (RA). Estas mensagens são enviadas periodicamente e contêm informação relativa aos *default routers* de cada rede, são denominadas por *Agent Advertisement* e normalmente utilizadas pelos HAs. Tornam também possível a detecção de movimentação.

No segundo, depois do MN obter o CoA necessita de transmitir essa informação ao seu HA. Este processo pode ser feito entre o MN e o seu HA ou através do FN, através de mensagens *Registration request* e Registration Reply. O HA ao receber a informação do novo CoA utilizado pelo MN adiciona-o à sua tabela de encaminhamento para posteriormente efectuar o redireccionamento dos datagramas.

No terceiro, sempre que o MN não se encontra na sua HN para efectuar o processo de redireccionamento é utilizado o processo de *Tunneling* IP-em-IP.

Na Figura 2.5 para além de poder-se observar a arquitectura do protocolo MIPv4, também se pode observar o seu modo de operação:

1. Efectua-se uma comunicação normal entre o *Mobile Node* (MN) e o *Correspondent Node* (CN).
2. Ocorre uma movimentação do MN da *Home Network* para a *Foreign Network.*
3. O MN regista o seu *Care-of-Address* (CoA).
4. O MN envia pacotes para o CN directamente
5. O CN envia pacotes para *Home Address* do MN.
6. Os pacotes atravessam o túnel do HA para a *Foreign Network (FA)* do MN.
7. FA entrega os pacotes recebidos ao MN.

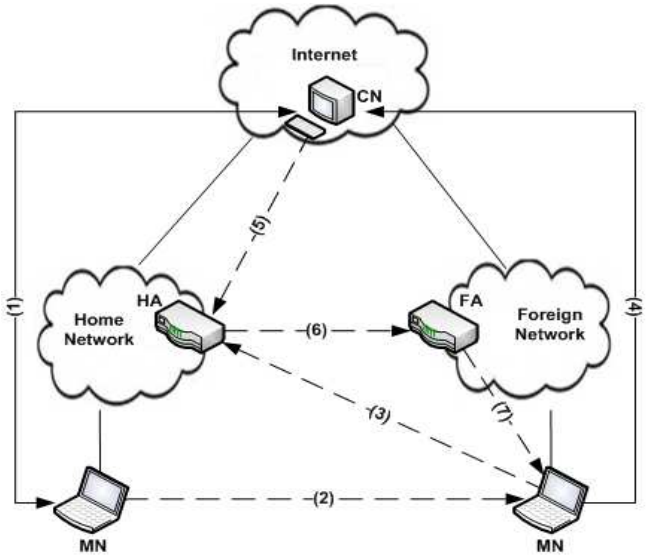


Figura 2.5 – MIPv4 arquitectura e modo de operação.

- **MIPv6**

Mobile IPv6 (MIPv6) é baseado no MIPv4, no entanto utiliza como protocolo de endereçamento o IPv6. Surge com o objectivo de resolver alguns problemas existentes no IPv4 e optimizar o processo de mobilidade.

De acordo com [31] existem algumas diferenças entre o MIPV4 e o MIPv6:

- O MN passar a obter os CoAs de forma automática através do DHCPv6 ou da auto-configuração, suportada pelo IPv6, deixando de haver a necessidade de utilização do FA.
- No MIPv6 o MN pode possuir vários CoAs.
- No MIPv4 quando se envia datagramas do MN para o CN, o endereço de origem será o HoA, no MIPv6 o endereço de origem é o CoA primário, sendo facultativo indicar o seu HoA.
- O MIPv6 utiliza o IPV6 *Neighbor Unreachability* para detectar se o MN se encontra acessível.

- No MIPv6 existe uma redução da sobrecarga relativamente ao MIPv4, pois a maioria dos pacotes enviados para o MN, quando se encontra longe da sua HN, são enviados usando o IPv6 *routing header* em vez do encapsulamento IP.
- O MIPv6 possui uma maior robustez pois é dissociado de qualquer camada de ligação, uma vez que utiliza IPV6 *Neighbor Discovery* em vez do *Address Resolution Protocol* (ARP).

Como este tipo de protocolo de mobilidade não necessita de qualquer *Foreign Agent*e numa *Foreign Network*, ao transitar para outra rede, o *Mobile Node* (MN) requisita um endereço IPv6 na nova rede e informa o seu *Home Agent* (HA) sobre a sua localização. A partir deste momento, é estabelecido um túnel IPv6 entre o *Mobile Node* (MN) e o seu *Home Agent* (HA). A comunicação entre o *Mobile Node* (MN) e o *Correspondent Node* (CN) procede por esse túnel.

Na Figura 2.6 podemos observar detalhadamente os passos do processo de troca de rede, designado por handover. Os passos são os seguintes:

1. O *Mobile Node* (MN) possui um endereço da sua *Home Network* (HN) e é estabelecida a comunicação com o *Correspondent Node* (CN).
2. O MN inicia o processo de troca de rede movendo-se para uma *Foreign Network* (FN). Neste momento irá receber um novo endereço IPv6 chamado *Care-of Address* (CoA).
3. Como o MN mantém o seu antigo endereço, deve enviar um pacote para o seu *Home Agent* pela *Foreign Network*, registando o novo endereço através de uma mensagem *Binding Update* (BU), onde o HA responde com *Binding Acknowledgement*.
4. O MN actualiza o seu endereço com o CN, que dependendo do suporte à mobilidade de CN a comunicação pode-se efectuar de duas formas, identificadas nos passos 5 e 6.
5. Estabelecimento da comunicação entre CN e HA através do túnel.
6. Estabelecimento da comunicação directa entre CN e MN.

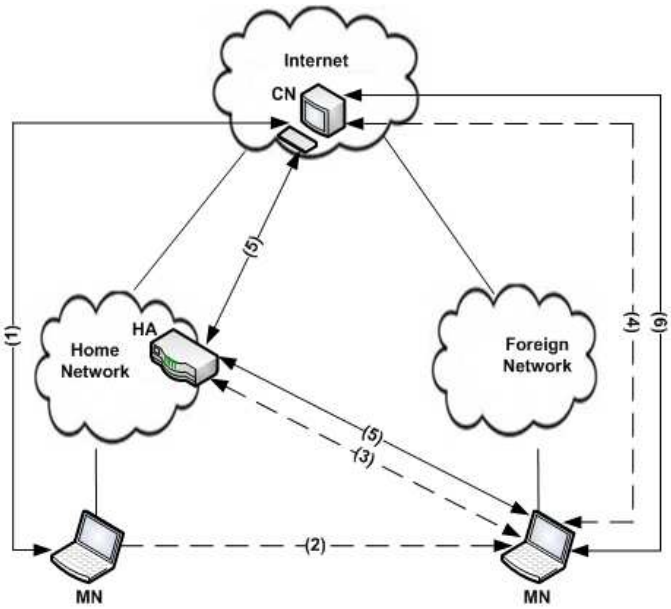


Figura 2.6 – MIPv6 arquitectura e modo de operação.

Como já foi referido anteriormente, existem protocolos considerados extensões do MIPv6, por exemplo FMIPv6 e o PMIPv6.

- **FMIPv6**

Fast Handover for Mobile IPv6 [32] tem como objectivo principal diminuir o tempo de interrupção do serviço quando um terminal móvel IPv6 se desloca para uma rede diferente à qual está conectado. Para isso a ideia do FMIPv6 é providenciar informação relativa à camada de ligação, com a finalidade de prever ou responder rapidamente a um evento de *handover*, sendo assim, prontamente estabelecida a conectividade IP a um ponto de acesso.

O facto de ser estabelecido um túnel entre o *router* actual e o novo *router* de acesso, torna possível a conectividade IP, mesmo antes de ser efectuado o registo do endereço no *Home Agent* ou no nó correspondente. O que permite que serviços em tempo real sejam restabelecidos antes do processo de registos de endereços estar concluído, pois este tipo de processo despende algum tempo.

Na Figura 2.7 pode-se verificar detalhadamente os passos para o processo de configuração da conexão no FMIPv6.

Os passos são os seguintes [33]:

1. Quando o MN realiza a negociação com o novo ponto de acesso, ele envia para o seu *Previous Access Router* (PAR) uma mensagem *Router Solicitation for Proxy Advertisement (RySolPr).*

2. Recebe em troca uma mensagem *Proxy Router Advertisement* (PrRtAdv) e inicia o processo de obtenção de um endereço *stateful* ou *stateless*. Endereço esse que será usado para definir um novo *Care-of Address* (CoA).
3. Na posse do seu endereço, mas ainda a comunicar através do seu PAR, MN envia um *Fast Binding Update* (FBU) para o PAR, requisitando o redireccionamento do tráfego através do *New Access Router* (NAR).
4. O PAR envia um *Handover Initiate* (HI) para o NAR, a informar quais os endereços *Previous Care-of Address* (PCoA) e *New Care-of Address* (NCOA), para que possam ser validados.
5. Em resposta o NAR envia ao PAR um *Handover Acknowledgement message* (HAck), a aceitar o endereço proposto, ou então a indicar o novo endereço válido.
6. Após essa negociação o PAR responde à mensagem FBU recebida anteriormente com um *Fast Binding Acknowledgement* (FBAck).
7. O MN envia *um Fast Neighboor Advertisement* (FNA) para o NAR, comunicando a sua presença na nova rede.
8. Neste ponto o tráfego transmitido pela rede antiga ao NAR é direccionado para o MN.
9. O MN informa ao CN o seu novo endereço para realizar uma possível optimização de rotas, o que permite a comunicação directa, sem necessidade de passar pelo PAR.

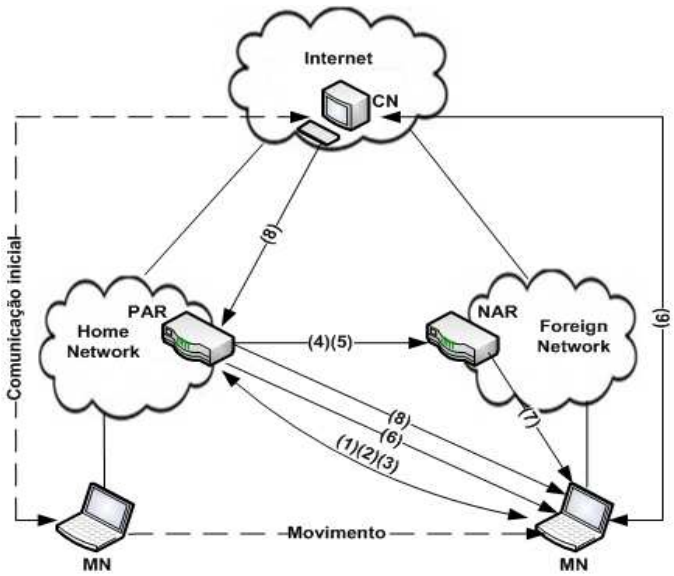


Figura 2.7 – Configuração da conexão no FMIPv6.

- **PMIPv6**

O protocolo Proxy Mobile IPv6 surge com um novo conceito, a mobilidade baseada na rede. Este conceito torna possível o suporte à mobilidade sem que seja necessária a interacção com o MN, isto é, o MN não precisa efectuar qualquer troca de mensagens na transição da sua rede local para uma rede estrangeira. Essa acção será feita por duas novas entidades: o *Mobile Access Gateway* (MAG), localizado na *Foreign Network*, e o *Local Mobility Anchor* (LMA), localizado na rede local [34]. Recorrendo à Figura 2.8 pode-se observar as mensagens trocadas nesta proposta.

Os passos que exemplificam a proposta são os seguintes [35]:

1. O MN para ter acesso a uma *Foreign Network* tem de realizar um processo de autenticação.
2. O MAG obtém o perfil do MN através de um *AAA Server (Authentication, Authorization and Accounting Server).*
3. O MAG envia um *proxy Binding Update* (PBU) para o LMA.
4. O LMA recebe a mensagem PBU e depois de verificar as políticas de segurança, aceita a mensagem PBU.
5. O LMA envia um *Proxy Binding Acknowledgment* (PBA) para o MAG, o prefixo da rede do MN e estabelece o ponto de extremidade do túnel com o MAG.
6. Após a realização da configuração do túnel, o MAG envia um Router Advertisement (RA) para o MN com as configurações da sua rede. A partir daqui, todas as mensagens enviadas e recebidas pelo MN serão estabelecidas através do MAG, utilizando o túnel até ao LMA.

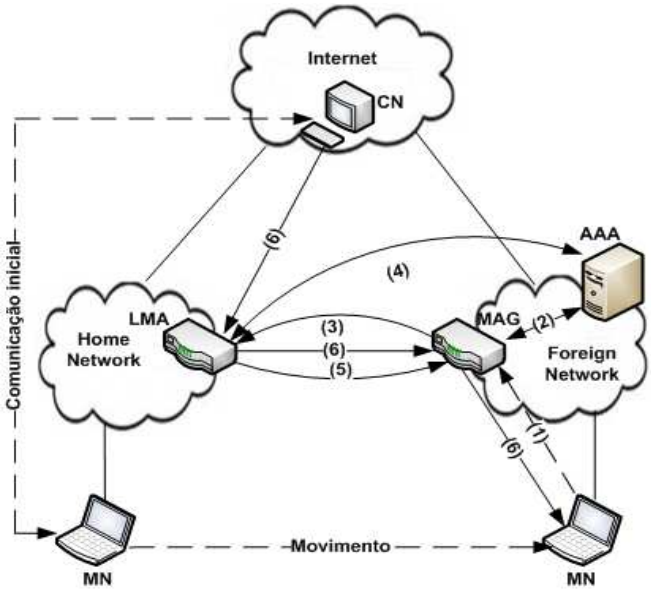


Figura 2.8 – Configuração da conexão no PMIPv6.

2.5. *Session Initiation Protocol*

O protocolo SIP (*Session Initiation Protocol*) é um protocolo de sinalização, localizado na camada de aplicação, especificado pela *Internet Engineering Task Force* (IETF) para o estabelecimento, manutenção e encerramento de sessões de comunicações em tempo real na rede IP. Concretamente em relação a VoIP um protocolo de sinalização tem como objectivo especificar a codificação da voz, a configuração das chamadas, transporte de dados, o modo de autenticação de segurança, métodos de comunicação, cabeçalho, endereçamento e sintaxe da mensagem. Tendo o IETF como filosofia a simplicidade, isto é, apenas específica o que é necessário e, como o SIP não se distancia dessa ideia, a sua simplicidade torna-o escalável e extensível, uma vez que se ajusta a diferentes arquitecturas e cenários de desenvolvimento. É um protocolo que se aproxima muito de protocolos de Internet como HTTP pois ambos são baseados no modelo pedido/resposta, com uma estrutura baseada em texto, codificam as suas mensagens de forma semelhante e o endereçamento é feito de forma idêntica à web e ao e-mail, onde o uso de *Uniform Ressource Locator* (URL) permite encaminhar as mensagens ao seu destino [36].

2.5.1. Arquitectura SIP

No SIP é possível a implementação de uma arquitectura de servidores definida para o apoio na localização, encaminhamento de mensagens e implementação de regras de comunicação. Visto serem componentes funcionais é possível numa mesma máquina ser implementados vários servidores. De seguida podemos ver a descrição dos componentes de uma arquitectura SIP [37].

- ***User Agent*** (UA): É uma entidade terminal com a capacidade de inicializar e terminar a conexão através de trocas e pedidos de respostas. Permite estabelecer comunicações Cliente-Servidor, pois têm a capacidade de fazer pedidos de início de sessão *User Agent Client* (UAC) e responder a requisições *User Agent Server* (UAS). Aqui, a comunicação pode ser estabelecida com outro Agente sem a necessidade de servidores SIP, bastando apenas ter o conhecimento da URI (*Uniform Resource Identifier*) e IP de cada dispositivo envolvido.

- ***Proxy Server:*** Encaminha mensagens de clientes que não podem fazer os pedidos directamente, actuando como um intermediário numa comunicação SIP. Este servidor pode ser utilizado nos domínios SIP com a finalidade de realizar autenticações e implementar regras de uso do sistema.

- ***Redirect Server:*** Tem como objectivo fornecer aos *User Agents* (UAs) informações sobre o endereço do servidor actual, para que possa contactar o endereço directamente.

A arquitectura pode ainda apresentar dois tipos de componentes:

- ***Register Server:*** A Finalidade deste servidor é suportar pedidos *Register*, para registar informações dos utilizadores em servidores de localização.

- ***Location Server:*** Os servidores de localização são considerados bancos de dados que armazenam informações relativas ao registo de utilizadores e suas localizações. Recebe os dados de entrada do servidor de registo e encaminha as informações para os servidores de redireccionamento e *proxy* para o correcto mapeamento de endereços lógicos e físicos dos utilizadores.

Para o estabelecimento de uma sessão SIP são usadas mensagens SIP, sendo que estas apenas podem ser de dois tipos: pedidos e respostas. Nas Tabelas 2.5 podemos verificar a lista de opções para pedidos SIP.

Tabela 2.5 – Mensagens de pedidos do SIP.

Método	Descrição
Register	Utilizado para o registo da localização do utilizador.
Invite	Pedido para estabelecimento de uma sessão multimédia. A mensagem pode conter uma descrição da sessão, através do protocolo SDP (*Session Description protocol*).
Ack	Confirma um pedido de tipo *Invite*.
Cancel	Cancela um pedido que ainda possa estar pendente.
Bye	Termina a sessão.
Options	Consulta de quais os métodos e extensões suportados pelos servidores e clientes.

Info	Permite a troca de informações durante uma sessão sem qualquer influência no estado da mesma.

Quanto às respostas no protocolo SIP, estas contêm códigos numéricos, baseados nos códigos HTTP. Existem seis classes que podem ser classificadas em dois tipos de respostas. As provisórias (classe 1xx), que apenas são utilizadas pelo servidor para informar o estado da sessão SIP, não procedendo depois ao término da mesma. E as finais (classe 2xx, 3xx, 4xx, 5xx e 6xx) estas são mensagens de resposta que encerram as sessões SIP. Em seguida na tabela 2.6 pode ser observado a especificação de todas as classes de resposta SIP.

Tabela 2.6 – Classes de respostas SIP.

Classe	Descrição
1xx	Classe informativa. Serve para indicar que o pedido foi recebido ou que ainda está a ser processado.
2xx	Indica que a acção foi completada com sucesso.
3xx	Quando há a necessidade de uma acção complementar para que o pedido possa ser efectuado.
4xx	Classe que aponta a um erro do cliente. Por ex: pedido com sintaxe inválida.
5xx	Classe que indica um erro no servidor.
6xx	Classe que informa que ocorreu uma falha global.

2.5.2. Protocolo SIP e a Mobilidade

A mobilidade é certamente um dos factores mais importantes no processo de difusão do protocolo SIP, pois a localização de um utilizador independentemente do dispositivo que esteja a utilizar (PC, notebook, telemóvel) não é fácil. Devido à possibilidade de ocorrência de *handover* é necessário que as infra-estruturas e algoritmos utilizados sejam capazes de prever o deslocamento do utilizador, com o objectivo de diminuir o impacto da sua chamada activa. Sendo assim, assume-se que o dispositivo móvel pertence a uma rede local, em que o *SIP Server* é responsável por fornecer a informação da localização do dispositivo. Um dos problemas gerais da

mobilidade, não apenas no protocolo SIP, é manter actualizada a informação da localização do dispositivo móvel, mesmo que ocorra uma mudança de rede.

De acordo com [3] a mobilidade no protocolo SIP pode ser descrita da seguinte forma. Quando um CN pretende iniciar a sessão com um MN, envia uma mensagem *Invite*. O servidor SIP localizado na *Home Network* do MN tem informação actual acerca da localização dos MNs e redirecciona a mensagem *Invite* para lá. Em seguida é realizado o procedimento normal para o estabelecimento da sessão SIP. Se o MN acede a uma nova rede, no decorrer da sessão obterá um novo endereço IP via DHCP e enviará uma mensagem *Re-Invite* com a descrição actualizada da sessão. Isto permite manter o mesmo *Call-ID* da sessão existente, mas substitui o *Contact field* do cabeçalho SIP e o campo *c* do cabeçalho SDP (*Session Description protocol*) pelo novo endereço IP. Na primeira substituição o CN é informado onde o MN pretende receber futuras mensagens SIP, na segunda indica a nova localização para onde os pacotes devem ser enviados. Após receber a mensagem *Re-Invite*, se o CN utilizar o protocolo UDP, enviará os pacotes directamente para o novo endereço IP, se utilizar o protocolo TCP, os pacotes serão enviados para o MN pela técnica de encapsulamento. Quando o MN recebe os pacotes encapsulados, o MN remove-os do encapsulamento IP. O MN também usa túneis para enviar os pacotes para o CN. Finalmente, o MN envia uma mensagem de registo para o *Home* SIP *Server* com o intuito de actualizar as informações de localização lá armazenadas, para que a nova chamada possa ser redireccionada correctamente. Na Figura 2.9 podemos ver um exemplo da Mobilidade no protocolo SIP e as suas operações.

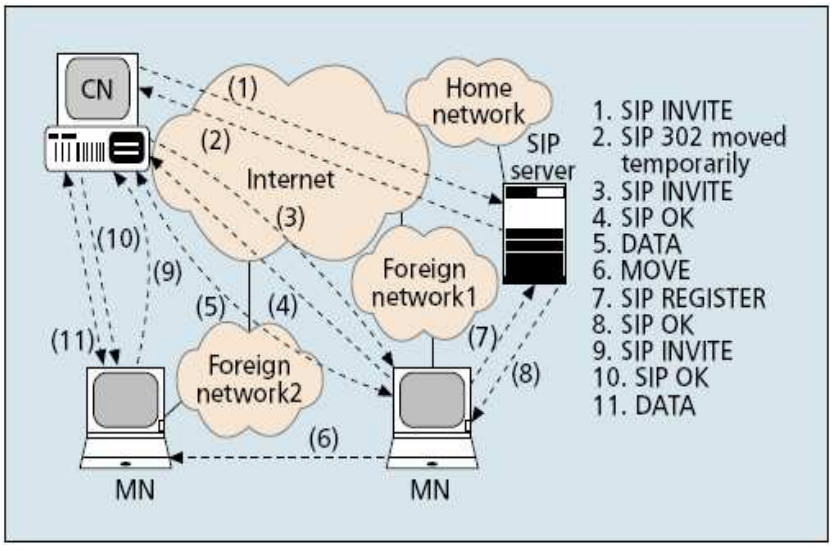


Figura 2.9 – Mobilidade SIP e suas operações [3].

2.5.3. Segurança em SIP

Ao nível da segurança o protocolo SIP deve cumprir diversos requisitos tais como: confidencialidade, onde apenas os utilizadores autorizados podem aceder à informação armazenada ou à que está a ser transmitida; autenticidade, aqui deve-se ter em conta a identificação da origem da mensagem, isto é, se ela foi mesmo enviada pelo emissor correspondente ou se é uma falsa mensagem enviada por um atacante; Integridade é necessário garantir que algo na mensagem não seja modificado ou apagado sem autorização; disponibilidade, somente os utilizadores autorizados tem acesso aos dados disponíveis; não repudio, tanto o emissor como o receptor não podem negar o envio e a recepção de mensagens; controle de acesso, o acesso a serviços, informações e recursos devem ser vigiados para os autorizados.

Concretamente numa rede VoIP os ataques são direccionados ao processo de sinalização entre os seus componentes. Quando bem sucedidos esses ataques violam os princípios de integridade e confidencialidade das informações. De seguida serão apresentados alguns mecanismos utilizados para fornecer segurança contra as ameaças e vulnerabilidades relacionadas com o processo de sinalização em redes de voz sobre IP.

- **Autenticação**

O *HTTP Digest Authentication* [37] é um mecanismo de segurança utilizado pelo *HTTP* e adoptado pelo SIP para proporcionar autenticação de mensagens e protecção contra ataques por replicação. No SIP a autenticação poderá ocorrer entre um *User Agent* (UA) e um servidor ou então entre dois *User Agents* (UAs). Na primeira um servidor poderá exigir uma autenticação de um UA antes de permitir que este utilize os seus serviços, na segunda os dois UAs necessitam de uma autenticação como forma de garantir com quem se está realmente a comunicar. A autenticação no SIP pode ser efectuada de uma forma simplificada baseada em *HTTP digest* ou então através de um esquema envolvendo criptografia e troca de certificados.

As credenciais de um utilizador no *HTTP digest* são o nome e a senha do mesmo, no entanto este método em si não garante a segurança, pois as credenciais não têm qualquer tipo de protecção, para tal é necessário o recurso a mecanismos de segurança associado ao *HTTP digest*, tal como o MD5, na Figura 2.10 podemos ver um procedimento de autenticação SIP [4]. Em todo o caso, sendo o *HTTP digest* um

mecanismo fraco de protecção é recomendado a utilização de criptografia para as mensagens de sinalização através de protocolos como TLS, IPSec e S/MIME.

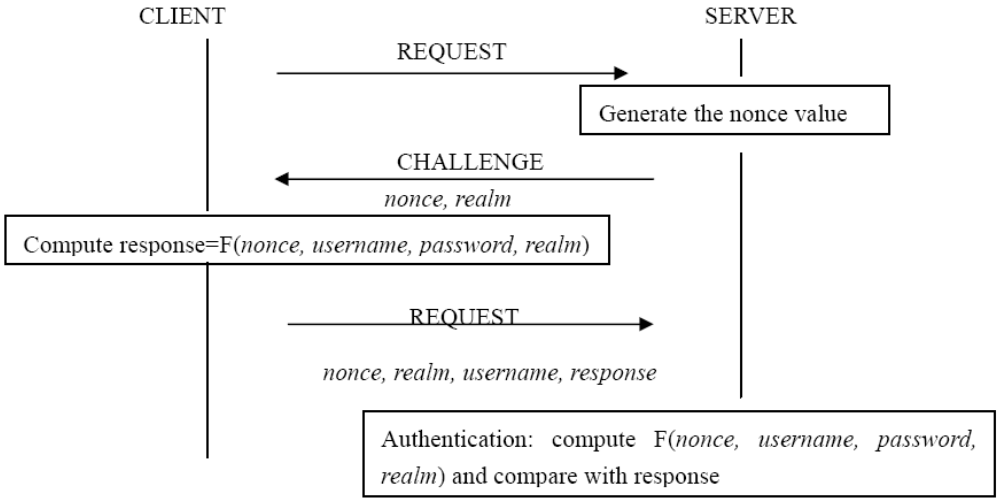


Figura 2.10 – Procedimento de autenticação *Digest* no SIP [4].

Antes de este esquema iniciar o cliente partilha a sua *password* com o servidor, em seguida este procedimento inicia-se com o cliente a enviar um *Request* ao servidor, o servidor gera um valor *nonce*, este valor *nonce* pode ser um MD5 *hash* único, resultante da conjugação que o SIP pode estabelecer entre o HTTP *Digest Authentication* e o *algoritmo Message Digest 5* (MD5). De seguida o servidor responde com uma mensagem que contem o campo *nonce* e *realm*. A resposta é uma mensagem de erro a solicitar ao utilizador uma autenticação. O campo *realm* é o algoritmo *digest* usado neste desafio. De seguida, o cliente calcula a resposta, através do cálculo do valor *nonce* recebido no desafio, do *username*, da *password* e do *realm*, enviando para o servidor a mensagem *Request* original, com o valor *nonce*, *username*, *realm* e o valor calculado de resposta. Por fim, de acordo com o *username*, o servidor tem acesso à *password* do cliente, e verifica se o campo *nonce* está correcto, se estiver, calcula o F (*nonce, username, password, realm*) e compara-a com a resposta do cliente, se forem iguais o servidor autentica o cliente.

CAPÍTULO 3

Estado de Arte

3.1. Introdução

Várias soluções são abordadas relativamente à qualidade de serviço e segurança para aplicações tempo-real (VoIP) em redes móveis. Contudo, normalmente estes dois aspectos na literatura têm sido abordados de uma forma independente.

Neste capítulo serão apresentados alguns trabalhos. Em primeiro serão apresentados trabalhos referentes à qualidade de serviço no *handover*, em segundo trabalhos referentes à segurança no *handover* e por último um trabalho que trata a qualidade de serviço e segurança no *handover* de uma forma conjunta. De notar que este último trabalho tem um grande contributo para o desenvolvimento desta dissertação.

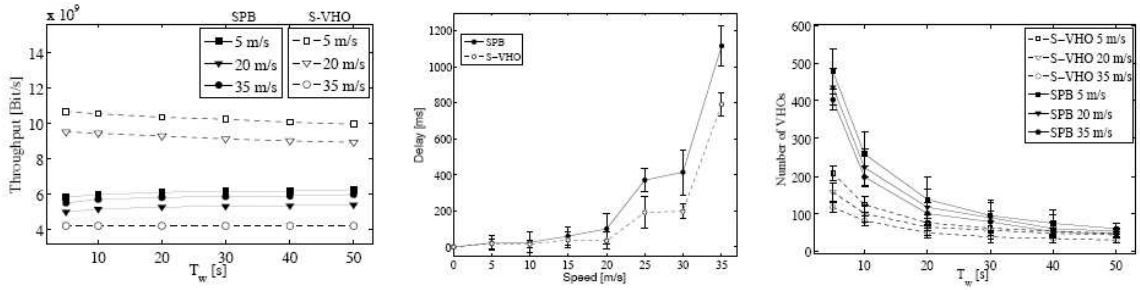
3.2. QoS em *handovers* para aplicações tempo-real (VoIP)

Em [5], os autores pretendem comprovar que os *handovers* verticais são os ideais para garantir uma conectividade sem interrupções e uma qualidade de serviço aceitável. Pretendem também comprovar que mesmo que uma rede candidata tenha uma largura de banda significativamente maior, poderá não ser benéfico o abandono da rede actual. Para tal, introduziram um modelo de análise para *handovers* verticais, um algoritmo baseado na velocidade do veículo, pois defendem a redução da velocidade do veículo como forma de garantir um QoS aceitável para aplicações de tempo-real. O algoritmo em causa denomina-se por *speed-based, Qos-oriented Vertical Handover* (S-VHO), a ideia de usar a velocidade do veículo como critério de *handovers* verticais não é nova, no entanto, os autores pretendem aplicá-la em aplicações de tempo real para VANETs. As suas simulações tiveram como base de comparação o trabalho desenvolvido por [38], que utiliza um algoritmo baseado na força do sinal recebido (RSS) e na velocidade de terminal móvel, através do S-VHO conseguiram obter melhores resultados em termos de *throughput*, *delay*, *jitter* e *overhead* (número de *handovers* verticais). O algoritmo S-VHO por eles desenvolvido é composto por três

entradas: a velocidade do veículo, o tempo de entrada do veículo numa rede *wireless* e a informação da localização do veículo através do sistema de localização GPS (*Global Positioning System*), posteriormente retornam uma variável de decisão do *handover* (0 ou 1). Este algoritmo decide se um *handover* é válido comparando o tempo de passagem numa célula, com o limite do tempo de passagem numa célula para *handovers* válidos.

Como já foi referido o S-VHO utilizará como base de comparação nas simulações efectuadas o algoritmo *Speed Probability-Based* VHO (SPB) proposto por [38], que tal como S-VHO utiliza a velocidade do veículo como critério de ponderação do *handover*. A técnica SPB baseia-se na avaliação da probabilidade do *handover*. Nesta técnica a decisão do *handover* efectua-se pela comparação da probabilidade do *handover* com um limite fixo da probabilidade que depende da velocidade do veículo e da latência do *handover*.

Com o objectivo de melhorar três métricas de QoS (*delay*, *jitter* e *throughput*) e manter um número reduzido de *handovers* verticais, os autores obtiveram determinados resultados através de um simulador denominado *network simulation 2* (NS2). Perante um determinado cenário proposto alcançaram os seguintes gráficos.



(*a*) (*b*) (*c*)

Figura 3.1 – *(a)* Em 100 simulações a média do *throughput* para S-VHO e SPB. *(b) Delay* dos pacotes com a velocidade do veículo é mais lenta em S-VHO do que em SPB. *(c)* Número de *handovers* verticais para os algoritmos S-VHO e SPB [5].

Na figura 3.1 podemos verificar o desempenho da rede relativamente aos parâmetros de *troughput*, *delay* e ocorrência de número de *handovers* verticais.

Na figura 3.1 (a), verifica-se o *throughput* que diz respeito aos bits recebidos durante uma conexão de *downlink* das técnicas S-VHO e SPB, versus o tempo de espera de uma comutação. Conclui-se que a eficácia do S-VHO é clara quando a velocidade do veículo é inferior ao limite de velocidade, neste caso verifica-se que esse limite é de 20m/s. Por outro lado podemos concluir que a técnica SPB não é sensível à velocidade e ao tempo de espera entre comutações, sendo o seu *throughput* limitado.

Na figura 3.1 (b), verifica-se que o *delay* para ambas as técnicas vai aumentando à medida que a velocidade também aumenta. Isto acontece porque não há tempo suficiente para fazer o *download* da próxima *frame*, antes do sinal ficar muito fraco. O S-VHO apresenta atrasos mais baixos comparado com o SPB, pois em média ele executa menos *handovers*.

Na figura 3.1 (c) observa-se o numero médio de *handovers* verticais para diferentes valores de tempo de espera de comutação esses valores vão de 0 a 50s. Como esperado o numero de *handovers* verticais diminui quando o sistema está inactivo por períodos longos, isto é quando o tempo de espera de comutação aumenta. Denotar que as simulações contém todos os *handovers* válidos e inválidos, sendo estes últimos representados pelo intervalo entre as curvas de S-VHO e SPB.

Relativamente ao desempenho do parâmetro *jitter* para as técnicas de S-VHO e SPB, podemos observar a comparação das mesmas nos seguintes gráficos.

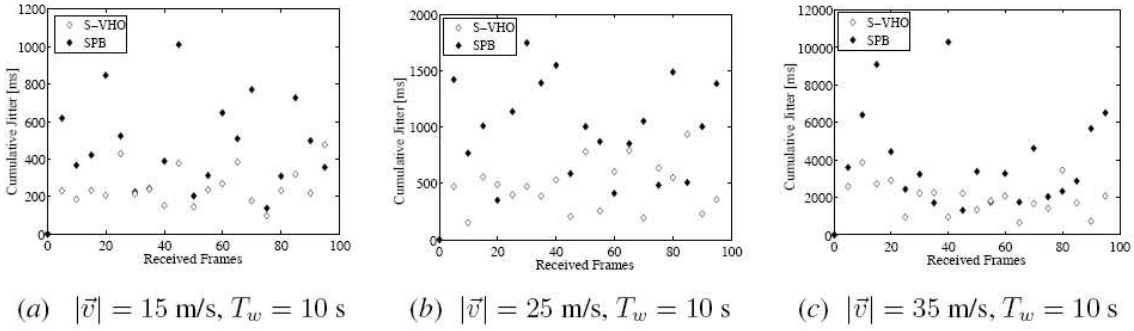


Figura 3.2 – Apresentação do parâmetro do *Jitter* para uma média de 100 simulações, para diferentes velocidades [5].

Na figura 3.2 (a), (b), (c) podemos observar as duas técnicas a serem comparadas ao nível do desempenho do *jitter*, para diferentes valores de velocidade e um tempo de espera de comutação constante. Cada ponto representa o *jitter* definido como a diferença entre o *delay* máximo e mínimo da frame para uma média de 100 simulações. A partir dos gráficos verifica-se que o *jitter* aumenta com a velocidade uma vez que duas frames chegam com maior frequência de diferentes redes sem fios e o tempo de passagem na célula diminui quando a velocidade aumenta.

Conclui-se que os objectivos propostos pelos autores de melhorar os parâmetros da rede, mantendo um número reduzido de *handovers* verticais foram alcançados com sucesso e comprovaram que quando um veículo encontra uma rede candidata, com uma taxa de dados maior, a conexão nessa rede não resultará necessariamente numa melhoria

do *throughput* uma vez que este não é apenas influenciado pela largura de banda, mas também, pelo tempo de passagem na célula e velocidade do veículo.

Em [6] foram propostas duas soluções para diferentes camadas com o objectivo de manter uma conectividade à internet contínua, sem qualquer interrupção.

A primeira foi uma solução baseada na mobilidade de rede (NEMO – *Network Mobility*) e num protocolo de suporte básico (BSP – *Basic Support Protocol*), o qual é uma extensão do MIPv6 na camada de rede. O MIPv6 baseado em NEMO BSP, designado por MIPv6-NEMO, utiliza um túnel bidireccional entre um agente *home* e o router móvel, onde todo o tráfego é obrigado a passar por esse mesmo túnel sem qualquer tipo de excepção. Verificaram que esta solução é incapaz de se livrar da limitação do túnel bidireccional, o qual pode introduzir várias vezes um processo de encapsulamento e desencapsulamento, e que o MIPv6 apenas analisa e define que a selecção do caminho é uma das questões do *multihoming* (quando um router móvel possui vários caminhos de acesso à internet) não identificando qualquer tipo de solução.

A segunda solução diz respeito ao protocolo de início de sessão (SIP) baseado na mobilidade da rede (NEMO), definido na camada de aplicação. Os autores integram a solução SIP-NEMO com o IEEE 802.21 *Media Independent Handover* (MIH) [6]. O serviço IEEE 802.21 permite a transferência e interoperabilidade entre tipos de redes heterogéneas, incluindo padrões de redes 802 e não 802. Sendo que o objectivo deste serviço é melhorar e facilitar o uso de nós móveis, proporcionando uma transmissão contínua em redes heterogéneas.

Esta integração tem como finalidade obter uma optimização de rotas independentemente do *multihomed* configurado, isto é, preservar a flexibilidade na troca de sinalização SIP, sempre que as configurações *multihoming* são diferentes. O servidor de mobilidade de rede SIP usa o serviço MIH a fim de decidir quais as interfaces de saída que devem ser usadas.

Os autores neste artigo realizaram duas experiencias, a primeira com o objectivo de medir a latência do *handover* (período de tempo sem recepção de pacotes enquanto ocorre o *handover*) e a segunda para medir o *throughput*. Para ambas as experiencias, o simulador utilizado foi o *network simulator 2* (NS2).

Por fim, para as soluções propostas por estes autores devemos ter em conta que eles não abordam aspectos importantes tais como: a influencia da velocidade do rede móvel no número de *handovers* realizados e o atraso induzido.

Especificamente para a aplicação de tempo real VoIP e para a avaliação da qualidade de serviço da mesma existe um método utilizado por diversos artigos denominado por E-Model.

Em [9] os autores utilizaram o E-Model para calcular a qualidade de voz durante o *handover*. A proposta deles consistiu num mecanismo de *handover* na camada de transporte utilizando o *Stream Control Transmission Protocol* (SCTP). O protocolo SCTP é um protocolo de transporte com características semelhantes ao TCP, sendo que a principal diferença entre eles diz respeito ao conceito de *multihoming* e a capacidade de transportar vários *streams* numa única conexão, a associação de uma *stream* com a conexão denomina-se por associação SCTP. O SCTP utiliza um mecanismo que permite detectar falhas na sessão, denominado por *hearbeat*, este mecanismo é usado essencialmente para monitorar a conectividade da sessão e permite saber quais os endereços definidos numa associação estão disponíveis.

Originalmente um *heartbeat* é enviado periodicamente a cada retransmissão Time-Out (RTO), este poderá ser um utilizador/aplicação de tempo definível. Quando um pacote *heartbeat* é recebido por um terminal é processado e é enviado um pacote *hearbeat ack*. Cada pacote *heartbeat* contém o tempo de quando foi enviado. Podendo assim aquando da recepção do *hearbeat ack* calcular o tempo que a informação demora a chegar ao destinatário e estimar o *Round Trip Time* (RTT). Os autores neste trabalho modificaram o mecanismo original com o objectivo de poderem enviar múltiplos pacotes heartbeat em um determinado espaçamento de tempo, podendo o número de pacotes e o espaçamento de tempo entre eles poder ser modificado. Para uma correcta estimativa do *Mean Opinion Score* (MOS) o mecanismo de *heartbeat* necessita de imitar o comportamento do *codec* VoIP a ser usado, sendo assim definiram um comprimento de 80 bytes para o pacote heartbeat e um espaço entre eles de 10ms.

Relativamente à decisão do handover eles baseiam-se no cálculo do ITU-T E-Model usando as medições dos parâmetros da rede, convertendo depois o valor resultante à escala MOS obtendo assim o nível de percepção do utilizador. Essas medições são calculadas usando os valores de RTT. É enviado em tempo determinado, consecutivos pacotes *heartbeat*, sendo nesse tempo calculado o valor de MOS de cada ligação de rede através do algoritmo E-Model, denotar que eles reduziram a equação de E-model, observada no capítulo 2 (eq. 2.1) apenas a duas variáveis *Id* e *Ie*. Posteriormente esse valor de MOS será utilizado no critério de decisão do *handover*, pois o mecanismo de *handover* seleccionará a ligação de rede que oferece melhor

qualidade de serviço. O *handover* utiliza alguns recursos do SCTP que permite que um endereço primário seja seleccionado de endereços alternativos, permitindo que o fluxo de dados possa ser modificado sem causar algum tipo de interrupção e atraso. Isto faz com que a execução do *handover* se realize de uma forma suave e transparente ao utilizador.

Em [7] a proposta dos autores é baseada numa investigação do desempenho VANET num contexto VoIP por meio de uma simulação de VoIP sobre VANETs (VOVAN – *VoIP over VANETs)*, para isso é necessário avaliar o desempenho de vários codecs de voz, uma vez que a principal função dos mesmos é realizar a conversão do sinal analógico/digital e analisar o impacto das métricas de qualidade de serviço relativamente à qualidade da voz durante uma comunicação. Os autores na realização desta investigação concentraram-se em quatro aspectos fundamentais: na geração realística de cenários urbanos em VANETs; na inclusão do padrão próprio para redes veiculares o IEEE 802.11 para alcançar simulações precisas; no estudo de diferentes métricas QoS para avaliação do desempenho dos codces; e testaram como o ambiente VANET pode influenciar a qualidade de percepção humana numa chamada de voz.

No primeiro, para simulação de tráfego utilizam o modelo GIPPs em conjunto com o NS2 e com mapas digitais de estradas do banco de dados TIGGER (*Topologically Integrated Geographic Encoding and Referencing*). O modelo GIPPs baseia-se no princípio *car-following*, isto é, na determinação de limites no desempenho do veículo e do motorista, utiliza esses limites para calcular a velocidade segura entre dois veículos, evitando assim a ocorrência de colisões. Consideram a cidade de Tanger em Marrocos para um cenário tipicamente urbano e que os veículos se deslocam a uma velocidade entre 0-50km/h durante 200s, num intervalo de 5 a 20m com incremento de 7m.

No segundo, especificaram as diferentes camadas utilizadas. Na camada física utilizaram o padrão IEEE 802.11p, na camada de rede para o cálculo do melhor caminho entre os nós VANETs utilizaram o protocolo de encaminhamento OLSR (*Optimized Link State Routing Protocol*), na camada de transporte utilizaram o protocolo RTP (*Real-time Transport Protocol*) habitual para aplicações de tempo-real e este por sua vez utiliza o protocolo de transporte UDP (*User datagram Protocol*) por fim, na camada de aplicação utilizaram uma aplicação que permite gerar tráfego de voz durante 60s.

No terceiro, identificam as três métricas que serão analisadas: o atraso, perda de pacotes e o MOS. O atraso será calculado pela média E2E (*End-to-End*), que é o tempo que um pacote demora desde que sai da fonte até ser entregue ao seu destino, sendo que para obter uma boa qualidade de transmissão o atraso não deve ultrapassar os 150ms, se for superior a 300ms a transmissão VoIP é considerada significativamente fraca. A perda de pacotes é medida pela percentagem de pacotes descartados no receptor. As aplicações VoIP toleram perdas de pacotes até 10%, sendo que uma perda de 5% já é perceptível ao utilizador. Por fim a última métrica analisada é o MOS, onde através do algoritmo E-Model será calculado o valor do factor de taxa de transmissão (R), para posteriormente ser convertido à escala *Mean Opinion Score* (MOS).

No quarto, foram analisadas graficamente as três métricas QoS, focando-se em dois cenários com o tamanho da área de simulação diferentes o segundo maior que o primeiro e em quatro diferentes *codecs* (G.711, G.723.1, G.729A e GSM.EFR). Na Figura 3.3 verifica-se que relativamente ao atraso o *codec* que apresenta melhor desempenho é o G.723.1. Isto deve-se ao facto de este tipo de *codec* ser um pacote de tamanho reduzido (20 bytes), pois quanto maior o pacote, mais tempo é necessário para o processar, como é o caso do *codec* G.711 em que o tamanho do pacote é o mais elevado (160 bytes) o que o leva a apresentar o pior desempenho. Também se verifica que o atraso relativamente aos cenários aumenta com o tamanho da área de simulação, à excepção do *codec* G.726A.

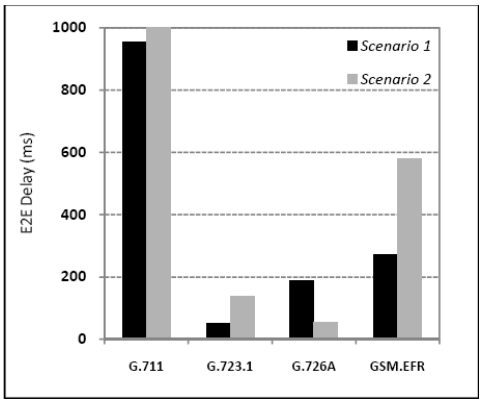


Figura 3.3 – Atraso (E2E) para diferentes codecs [7].

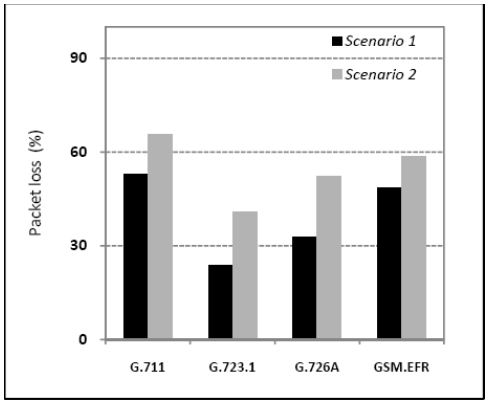


Figura 3.4– Perda de pacotes para diferentes codces [7].

Na Figura 3.4 observa-se o gráfico que diz respeito à perda de pacotes, aqui verifica-se que todos os *codecs* ultrapassam os 10% que é o limite para que uma

comunicação VoIP seja viável. Os autores concluíram que estas perdas resultam em primeiro do enorme tráfego introduzido pelos *codecs*, sendo que eles apenas são capazes de lidar com 50 pacotes por segundo na sua fila e em segundo do processo de descoberta do caminho em NS2, pois enquanto o nó procura o caminho para o destino, a fonte VoIP continua a produzir pacotes, acabando por encher a fila do *codec* e levar que os mesmos sejam descartados. Relativamente ao cenário, quanto maior este for, maior será a ocorrência de perdas, uma vez que o numero de conexões aumenta.

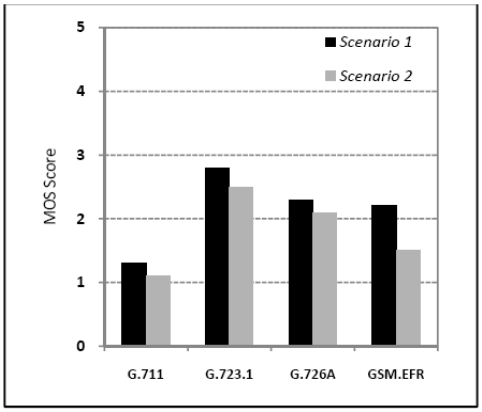


Figura 3.5 – Valor de MOS para diferentes codecs [7].

Por fim, relativamente à métrica de qualidade de serviço MOS que é amplamente afectada pela perda de pacotes e atraso, verifica-se na Figura 3.5 que o *codec* que apresenta o melhor valor MOS é o G.723.1. Relativamente ao outros *codecs* o MOS possui um valor fraco, isto deve-se ao facto da taxa de perda de pacotes ser elevada.

Com este trabalho realizado os autores concluíram que a qualidade de serviço com conexões VOVAN diminui com o tamanho do cenário.

3.3. Segurança no *Handover*

Os autores em [39] concentraram-se numa solução de segurança SIP baseada em *HTTP Digest*, o qual é utilizado para autenticação de clientes. A autenticação é um processo que permite verificar a autenticidade de uma identidade ao qual a rede SIP apenas verifica a legitimidade do *User Agent*. Existem outros mecanismos para autenticação como o TLS ou o S/MIME, mas estes são soluções mais difíceis de implementar. Por exemplo uma autenticação mútua entre o servidor e o cliente com o protocolo criptográfico TLS não é independente da camada de transporte, necessita do TCP e necessita ainda da implementação de PKIs (*Public Key-Infrastructures*).

Neste trabalho o mecanismo de autenticação mútua entre utilizadores e servidores de redes melhora a segurança sem alterar a sinalização SIP e sem aumentar o número de mensagens trocadas. Especificamente na proposta apresentada os autores estendem o cabeçalho de mensagens SIP a fim de incluir um valor "opaco", isto é, um valor aleatório. Sendo assim como forma de obter esse valor "opaco" o servidor proxy irá gerar um valor do campo "nonce" com uma chave pré-partilhada, a *password* e um elemento do cabeçalho SIP gerado pelo o utilizador. Quando o utilizador recebe esse valor "nonce", envia a resposta da autenticação SIP e ao mesmo tempo verifica o conteúdo do mesmo. O SIP *User Agent* compara esse valor com o valor "nonce" anteriormente calculado, se eles coincidirem o servidor proxy é considerado confiável. Este método é realizado com a utilização do MD5 que é um algoritmo de *hash* frequentemente utilizado pelo protocolo SIP.

Esta solução pode ser implementada sem interrupção de serviços, não alterando a capacidade de estabelecer uma sessão SIP. Assim, se um utilizador e um servidor proxy estão equipados com a solução proposta, obtêm uma autenticação mútua sem qualquer problema; se um servidor proxy está equipado com a solução proposta mas o utilizador não, o utilizador não tem acesso ao valor do campo "nonce", mas pode gerar um *REGISTER* com a resposta ao desafio, não usufruindo de qualquer serviço de segurança; se um utilizador é equipado com a solução proposta mas o servidor proxy não, o utilizador pode-se registar mas é informado que o servidor proxy não está autenticado.

Em suma, esta solução pode ser implementada de forma progressiva, podendo os servidores proxy e os telefones serem alterados numa infra-estrutura operacional sem a interrupção do serviço telefónico.

A utilização de curvas elípticas tem sido um mecanismo muito utilizado para garantir segurança no protocolo SIP. Em [4] os autores utilizam criptografia através de chaves públicas como uma solução para os problemas de autenticação e concordância de chaves existentes no protocolo SIP. Propõem um novo protocolo de troca de chaves autenticado NAKE (*New Authenticated Key Exchange*), que supera as fraquezas que mecanismos de autenticação mútua como por exemplo o esquema AKA (*Authentication and Key Agreement*) possa revelar. Este protocolo utiliza a implementação do protocolo ECDH (*Elliptic Curve Diffie-Hellman*) e fornece autenticação em ambas as partes nas trocas de mensagens. A segurança deste protocolo pode ser demonstrada através do modelo de segurança *Canetti-Krawczk* (CK), que é um modelo que permite modular e

analisar protocolos de troca de chave, simplificando o design e análise de protocolos de segurança. Os autores neste artigo analisaram a segurança do esquema proposto sendo que os resultados obtidos em relação a diversos factores revelaram-se satisfatórios. Pois verificaram que este esquema está imune a ataques por repetição, a ataques para adivinhação de senha e *spoofing* no servidor. Relativamente à autenticação mútua ambas as partes produzem um valor de *hash* com base na chave pré-compartilhada, cumprindo os objectivos de segurança para uma autenticação mútua.

Outro artigo que tem por base a utilização de chaves elípticas é o [40], neste artigo os autores apresentam um esquema de autenticação mútua baseado numa troca segura de chaves, chaves públicas auto-certificadas (SCPKs – *self-certified public keys on eliptic curves*) em curvas elípticas. Isto evita a necessidade de uma grande infra-estrutura de chave públicas e permite alcançar um melhor desempenho em contraste com outros sistemas que usam o mesmo tipo de chaves. As principais vantagens deste tipo de esquema são as seguintes: alcança uma autenticação mútua e um acordo de chaves de sessão; no servidor não mantém qualquer *password* ou tabela de verificação; previne possíveis ataques induzidos pela rede ou por mensagens SIP; pode ser aplicado para autenticar utilizadores com diferentes domínios SIP; fornece aos utilizadores uma actualização rápida e segura da *password*; e evita o problema *key escrow*. *key escrow* é quando as chaves necessárias para decifrar dados criptográficos são guardadas num local próprio e só uma terceira entidade devidamente autorizada é que poderá ter acesso a elas. Sendo assim torna-se essencial que essas chaves estejam devidamente protegidas para que a informação só seja fornecida ao destinatário pretendido.

O esquema na sua generalidade consiste essencialmente em quatro fases: Em primeiro a fase de instalação, os autores definem uma autoridade de confiança (TA - *Trusted Authority*) em cada domínio SIP, para emitir a longo prazo as chaves primárias para entidades pertencentes ao mesmo domínio; em segundo a fase de registo, antes de um utilizador se tornar membro do domínio SIP, realizará um determinado processo com implicação de TA; em terceiro a fase de autenticação mútua, quando um utilizador cliente pretende comunicar com um servidor; e por último a fase de mudança de senha que ocorre quando o utilizador cliente pretende actualizar a sua *password*, sendo que esta fase não implica qualquer interacção com TA.

Em comparação com o esquema *HTTP digest* para SIP, o esquema proposto não muda a estrutura da mensagem SIP, excepto para a adição de alguns parâmetros. Este só

por si não resolve todas as falhas de segurança de serviços baseados no SIP e tem uma capacidade de computação limitada para a autenticação de *User Agents*.

3.4. Segurança e Qualidade de Serviço no *handover*

Contrariamente à maior parte dos artigos na literatura, os autores deste artigo [8] tratam a segurança e a qualidade de serviço do *handover* em simultâneo.

Em [8], os autores com este trabalho pretendem propor uma solução segura e com qualidade de serviço para protecção de mensagens SIP na comunicação VoIP móvel. A solução é elaborada de acordo com algumas características provenientes de uma rede VANETs, mobilidade elevada nos veículos e arquitectura da rede. Pretendem com esta solução explorar uma sessão SIP segura, introduzindo como mecanismos de segurança uma autenticação mútua entre utilizadores e servidores de rede para evitar ataques de repetição e falsificação, para isso utilizam uma troca de novas chaves de sessão durante a fase de pré-registo, esta fase além de garantir segurança, irá ajudar o nó móvel a seleccionar a próxima unidade estacionária ao longo da estrada (RSU- *Road Side Unit*) a ser utilizada pelo *handover*, reduzirá atrasos e por fim através de um conjunto de parâmetros, preservará a qualidade da voz durante os *handovers*, reduzindo o número de recursos consumidos numa sessão SIP.

Antes de se focarem na solução do problema em questão, isto é, na segurança do *handover* e na qualidade de serviço do mesmo, os autores apresentaram uma proposta de arquitectura de rede. Em que começam por assegurar que a unidade de bordo (OBU- On-Board Unit) além de incluir o SIP *User Agent* é equipada por uma interface de rede e que o veículo é equipado com um sistema de localização para enviar periodicamente a sua posição aos RSU. A rede VANET é composta por várias zonas IP, sendo cada zona, um conjunto de servidores (Registo, Local, Proxy, Redireccionamento e DHCP), anexados a um conjunto de RSUs. Na movimentação de um veículo entre zonas não é apenas executado o *handover* na camada de ligação, mas também é executado na camada de aplicação. Os RSUs nesta arquitectura possuem as seguintes funcionalidades: encaminhar as mensagens SIP recebidas para o correspondente servidor; executar o *handover* na camada MAC para um veículo que se move na mesma zona; recolher periodicamente informação do veículo sobre a sua posição e velocidade, recolher informação dos RSU detectados e a força do sinal a eles relacionados; trocar

dados relativo às suas taxas de ocupação; aconselhar o veículo sobre qual o próximo RSU a que se deve anexar na ocorrência de um *handover*; e gerar e encaminhar dados criptográficos entre o veículo e o servidor SIP.

Como já foi referido, para alcançarem um handover seguro, os autores apresentaram um mecanismo de autenticação mútua por eles adaptado. O modo de funcionamento desse mecanismo é o seguinte: antes do processo de *handover* são enviados periodicamente *beacons* com o objectivo de informar o veículo da presença de um RSU. Caso o veículo se mova em diferentes zonas, irá adquirir um endereço IP através do servidor DHCP. A troca de mensagens SIP ocorre quando o veículo move-se de um RSU para outro. Antes da fase do *handover* é executado um pré-registo seguro, este consiste na troca segura de parâmetros QoS, que serão utilizados à posteriori num *handover*, caso este processo fosse repetido para cada *handover*, a qualidade da voz iria ser afectada. Se a autenticação fosse executada apenas no início da sessão, iria revelar alguns problemas relacionados com alguns tipos de ataques que podem ocorrer durante o *handover*. Sendo assim, um veículo será capaz de autenticar o próximo servidor SIP usando a troca de chaves durante a fase de pré-registo, pois assumem que todos os veículos são equipados com um certificado digital permitindo ser autenticado com o primeiro servidor SIP com que ele se comunica.

Em suma, pode-se afirmar que a fase de pré-registo tem como finalidade a execução de uma autenticação mútua entre duas entidades, a troca de parâmetros QoS recolhidos pelo veículo e redução na sobrecarga que os mecanismos de segurança podem causar durante o *handover*.

Para a proposta da qualidade de serviço no *handover* os autores tiveram em conta o principal problema relacionado com uma comunicação VoIP que é a garantia da qualidade da voz na mesma. Consideraram uma ferramenta computacional E-model, para estimar a qualidade da voz preservada pelo utilizador, onde o factor R e um conjunto de parâmetros relacionados para VANETs são usados no processo de decisão do handover. Este esquema tem como objectivo limitar o número de handovers e consequentemente reduzir os atrasos, pois sempre que um veículo se conecta a um novo RSU, deve enviar a sua posição a esse mesmo RSU, permitido ao RSU manter um histórico quanto à hora marcada da posição dos veículos e a prever qual o próximo RSU a que eles se vão conectar no mapa de estradas. É na fase de pré-registo que o veículo envia ao RSU conectado, a lista de RSUs detectados, a lista de valores R e a posição actual do veículo. Depois o RSU ao qual está conectado, perguntará ao próximo

potencial RSU se está disponível para receber o veículo, a resposta será efectuada através de uma taxa de ocupação de recursos (Or). Baseado nos parâmetros abaixo descritos é possível calcular o valor de selecção de um potencial RSU através da seguinte equação [8]:

$$Select = DsD.\left(\frac{Cr.D}{Or} + M_s + R\right) \qquad \textbf{Eq. 3.1}$$

Onde *DsD* representa uma variável *boolean* a indicar se o RSU se encontra na direcção do veículo, o *Cr*, o raio de cobertura do RSU, o *D*, a distância que um veículo percorrerá dentro da área de cobertura do próximo RSU ao qual se vai conectar, o *Or*, como já foi referido a taxa de ocupação de recursos do próximo RSU, o $M_{s,}$ a principal velocidade do veículo no período *camping*[1] e o *R*, o factor de taxa de transmissão.

Pela equação 3.1 pode-se verificar que quanto maior o factor R, maior será o valor do factor de selecção do RSU e consequentemente será este a ser seleccionado. Também se verifica que quanto maior a cobertura do raio do veículo (Cr), maior será a probabilidade da selecção desse RSU, com o propósito de diminuir o número de *handovers*.

Para a simulação de resultados, os autores apresentam duas propostas de simulação, na primeira pretendem mostrar a eficiência em termos de *handover* ocorridos por intervalo de tempo, na segunda estimar a média de número de *handovers* ocorridos em termos de velocidade média do veículo.

Notar que ambas as simulações são realizadas de acordo com dois cenários, no primeiro não é usado uma fase de pré-registo, no segundo têm em conta a fase de pré-registo.

Os resultados obtidos da primeira simulação podem ser verificados pela observação do gráfico da figura 3.6.

[1] O tempo que um veículo se encontra conectado a um RSU.

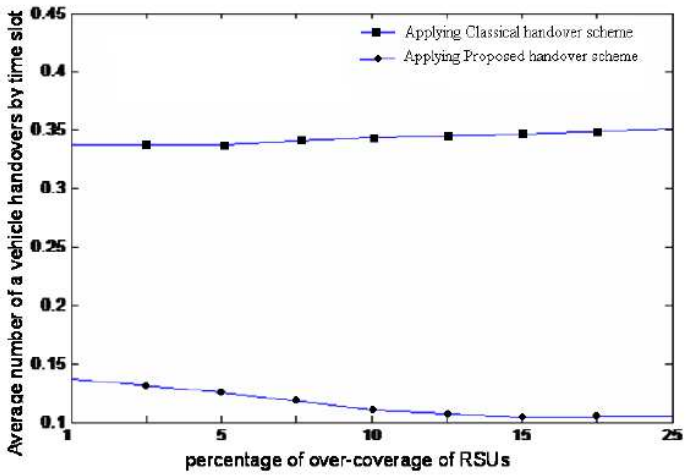


Figura 3.6 – Número médio de *handovers* por intervalo de tempo vs percentagem de *over coverage* de RSUs[8].

Perante este gráfico para o primeiro cenário podemos concluir que quanto maior a percentagem *over-coverage*[2], mais RSUs existem, logo maior será o número de *handovers*, pois sempre que um veículo detecta um novo RSU, que ofereça um elevado RSS, ele executa o *handover*. No segundo cenário verifica-se que quanto maior é a *over-coverage* menor será o número de *handovers*, pois os veículos tem a capacidade de seleccionar um RSU que garanta QoS e lhe permita permanecer com a mesma conexão o máximo de tempo possível, tendo em conta a direcção e velocidade do veículo. Portanto pode-se concluir que com a fase de pré-registo o problema do QoS relacionado com atrasos de *handovers* é significativamente melhorado com a redução do número de *handovers*.

Na segunda simulação, os resultados obtidos são apresentados no gráfico da Figura 3.7.

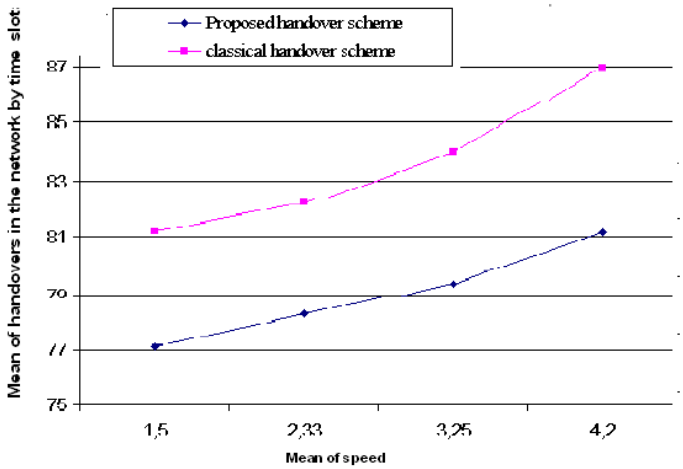


Figura 3.7 – Média do número total de *handovers* para todos os veículos vs Média da velocidade na rede[8].

[2] Quando a área de cobertura de diferentes RSUs se sobrepõem.

Perante o gráfico pode-se concluir que para ambos os cenários quanto maior a velocidade do veículo, maior o número de *handovers*, pois maior será a distância percorrida e consequentemente o veículo atravessará mais RSUs. Com o uso da fase de pré-registo, diminui a média do número de *handovers* pelo menos 5,5%. Isto reduz o atraso de *handovers* e o *overhead* referente à sinalização, preservando assim o desempenho VoIP com elevado QoS.

CAPÍTULO 4

Proposta de *handover* seguro com qualidade de serviço para aplicações de tempo real em redes veiculares

4.1. Introdução

Neste capítulo é apresentada uma proposta para *handovers* seguros e com qualidade de serviço para uma aplicação de tempo real, neste caso a aplicação VoIP. A proposta apresentada tem por base o trabalho [8], o qual já foi referido anteriormente como um artigo que aborda simultaneamente a segurança e a qualidade de serviço no *handover*.

Será proposto um esquema que no que diz respeito à qualidade de serviço terá de garantir qualidade da voz numa comunicação VoIP. Este tipo de comunicação poderá ser afectada por diversos factores, num contexto de redes veiculares o factor que mais contribui na interferência da qualidade de voz é o factor correspondente ao número de *handovers* ocorridos. Portanto para melhorar a qualidade deste tipo de serviço torna-se essencial reduzir o número de *handovers* ao máximo. No que diz respeito à segurança, este esquema terá de garantir que a troca de mensagens SIP cumpram diversos requisitos de segurança e que o número de mensagens seja reduzido.

Também neste capítulo serão demonstrados que os resultados atingidos são idênticos aos dos obtidos pelos autores no trabalho [8] que serviu de base a esta dissertação, apesar de se ter procedido a algumas modificações tanto ao nível da qualidade de serviço como ao nível da segurança.

4.2. Descrição da proposta

Para obtenção de uma solução segura e com qualidade de serviço para comunicações VoIP num contexto de redes veiculares é apresentada uma proposta que vai ao encontro da proposta elaborada pelos autores do trabalho em [8]. Isto é, será

executada uma fase de pré-registo que permitirá garantir segurança e reduzir atrasos através da limitação de número de *handovers*.

Nesta proposta foi considerado que um veículo é composto por um sistema de localização que permitirá enviar periodicamente a sua posição ao RSUs ao qual está conectado. A rede veicular será composta por zonas IP, em que um conjunto de servidores SIP estará anexado a um conjunto de RSUs.

Com a fase de pré-registo, em termos de qualidade de serviço, a decisão de execução de um *handover* será facilitada, pois através desta fase é possível escolher o melhor RSU ao qual o veículo se deve conectar. Em termos de segurança, nesta fase, será estabelecida uma troca segura de parâmetros QoS entre o veículo e os RSUs vizinhos antes da ocorrência de um *handover*.

De seguida será explicado e demonstrado com maior detalhe o esquema proposto para qualidade de serviço e segurança no *handover*.

4.3. Redução do número de *handovers*

Como já foi referido, numa comunicação VoIP é essencial garantir a qualidade da voz, para isso é importante ter em atenção parâmetros da rede como o atraso de pacotes, taxa de perdas de pacotes e força do sinal. Num contexto de redes veiculares o esquema aqui proposto, terá como base a diminuição da ocorrência de número de *handovers*, o qual será executado sempre que um veículo se mova de uma zona para outra.

A decisão de um *handover* será facilitada pela utilização de uma fase de pré-registo, pois é nesta fase que o veículo envia para o RSU ao qual está conectado, valores relacionados com três parâmetros: uma lista de todos os RSUs detectados na rede, uma lista de valores R e a posição actual do veículo. Com base nestes parâmetros o RSU tem a possibilidade de calcular o valor do factor de selecção para escolher qual o próximo RSU ao qual se deve conectar.

Sendo assim, a equação que permitirá calcular o factor de selecção é a seguinte:

$$Select = DsD.(Cr.D + M_S + R) \qquad \textbf{Eq. 4.1}$$

Em seguida será explicado em que consiste cada uma das variáveis que constituem a equação do factor de selecção:

DsD – representa uma variável booleana. É igual a zero se o RSU detectado não está na direcção do veículo e igual a 1 se está. Ou seja, o factor de selecção só poderá ser calculado quando o RSU se encontra na direcção do veículo.

Cr – Representa o raio de cobertura do RSU.

D – Representa a distância que um veículo percorrerá dentro da área de cobertura do próximo RSU ao qual está conectado.

M_S – No envio do parâmetro relativo à posição actual do veículo, o RSU prevê a direcção do veículo baseado nas duas ultimas posições recolhidas e calcula o período *camping* (tempo que um veículo encontra-se conectado a um RSU), M_S.

R – Representa o factor de taxa de transmissão. Este factor é calculado através da ferramenta computacional designada por E-Model que tem como principal utilidade estimar a qualidade de voz preservada pelo o utilizador. No processo de um *handover* VoIP normalmente é seleccionado o RSU que fornece o maior valor R, contudo este valor varia de RSU para RSU, mas como a nossa proposta será desenvolvida num cenário de simulação, não num cenário real, será atribuído um valor teórico igual para todos os RSUs.

Baseado na equação do factor de selecção podemos verificar que quanto maior a cobertura do raio do RSU, maior é a probabilidade desse RSU ser seleccionado, a fim de diminuir o número de *handovers* e aumentar o período *camping*.

4.3.1. Simulação da solução proposta

Com o objectivo de provar que com o esquema proposto os números de *handovers* poderão ser reduzidos realizaram-se duas simulações. A primeira com a finalidade de demonstrar a média do número de *handovers* ocorridos de acordo com a variação da percentagem *over-coverage* de RSUs. A segunda com o intuito de demonstrar a média do número de *handovers* ocorridos em termos de velocidade média do veículo.

Para cada uma das simulações foram considerados foram considerados dois cenários, o primeiro denominado de *handover* clássico, em que não é usado uma fase de

pré-registo, isto é, um *handover* ocorre sempre que um RSU ofereça uma elevada RSS (*Received Signal Strengh*). No segundo denominado de proposta de *handover*, é utilizada uma fase de pré-registo, ou seja, os RSUs cooperam juntos, de forma que o veículo possa seleccionar o RSU mais adequado.

Em termos analíticos, o cálculo do número de *handovers* para as duas simulações pode ser realizado através de duas equações para cada um dos cenários:

Assim, para o cenário denominado de *handover* clássico, o número de *handovers* ocorridos pode ser calculado pela seguinte equação:

$$N.^{o}\, handovers = (RSS / Dr) * over - \mathrm{cov}\, erage \qquad \textbf{Eq. 4.2}$$

Pela equação observamos que a força do sinal recebido (*RSS*), que consiste num valor fixo correspondente à potência do sinal emitido por um RSU, varia com a distância (*Dr*) do RSU em relação ao veículo, ou seja, quanto mais longe um RSU estiver do veículo menor vai ser a força do sinal. Quanto maior percentagem de *over-coverage*, mais RSUs serão detectados por um veículo.

Para o cenário correspondente à proposta de *handover*, tem-se em conta a fase de pré-registo, sendo que a equação para o cálculo do número de *handovers* estará relacionada com a equação relativa ao factor de selecção (eq. 4.1) do melhor RSU ao qual o veículo se deve conectar. Assim sendo, a equação que permite calcular o número de *handovers* para este cenário é a seguinte:

$$N.^{o}\, handovers = \frac{1}{(Cr * D + Ms) * over - \mathrm{cov}\, erage} \qquad \textbf{Eq. 4.3}$$

Sendo que o Ms é calculado pela distância percorrida pelo veículo na área de cobertura do RSU ao qual está conectado a dividir pela velocidade do veículo. A equação que traduz o cálculo do MS é a seguinte:

$$Ms = D / V \qquad \textbf{Eq. 4.4}$$

A equação 4.3 foi desenvolvida de acordo com os conceitos teóricos adquiridos. Uma vez que com a fase de pré-registo, será possível a escolha do melhor RSU ao qual o veículo se deve conectar, considerou-se que esta equação será inversamente proporcional à equação que permite o cálculo de números de *handovers* ocorridos para o cenário *handover* clássico.

Depois de explicado como se poderia calcular em termos analíticos o número de *handovers* para cada um dos cenários, será agora explicado como em termos práticos o mesmo objectivo foi cumprido.

Desenvolveu-se um programa em linguagem de programação *Java*, que fosse ao encontro das equações teóricas. O programa desenvolvido é adaptável a vários cenários de simulação, no entanto teve-se em conta algumas características pré-definidas para se efectuar as respectivas simulações. Sendo assim foi considerada uma área com 96 x 96, esta área é constituída por estradas que podem estar dispostas na horizontal ou na vertical. Cada estrada tem um comprimento de 16 metros, sendo que no final de cada estrada existe um cruzamento de estradas. Nas estradas serão colocados dois tipos de RSUs (RSU tipo I e RSU tipo II). Os primeiros tipos de RSU serão colocados em posições pré-definidas, isto é no meio e no cruzamento de estradas. Deste tipo serão distribuídos 169 RSUs os quais possuem um raio de cobertura de 8 metros. Os RSUs do segundo tipo possuirão um raio de cobertura de 18m e sofrerão uma variação de modo a ser possível obter um *over-coverage* de 1% para 25%, para alcançar um *over-coverage* de 25% são precisos 12 RSUs tipo II. A rota do veículo que se pretende estabelecer terá uma duração de 100s.

Este programa terá como finalidade calcular o número de *handovers* para respectivos cenários de cada uma das simulações. Sabendo que no caso do cenário correspondente ao *handover* clássico, um *handover* ocorrerá sempre que um veículo detecte a força do sinal de um novo RSU, seja para o RSU tipo I, seja para o RSU tipo II. E sabendo que no caso do cenário denominado por proposta de *handover*, um *handover* ocorre tal como no cenário anterior, quando um veículo detecta a força do sinal de um novo RSU, no entanto, se um veículo estiver conectado a um RSU do tipo II, mesmo que detecte um novo RSU, o *handover* só ocorrerá quando o raio de cobertura desse RSU tipo II for totalmente percorrido pelo veículo. Para uma melhor compreensão da forma como ocorrem os *handovers* foram elaboradas algumas figuras, denotar que para estas figuras apenas foi considerado uma área de 16X16, sendo que no programa desenvolvido, a área considerada é de 96X96. Na figura 4.1 para o cenário

handover clássico pode ser observado a ocorrência de *handovers* apenas com RSUs tipoI.

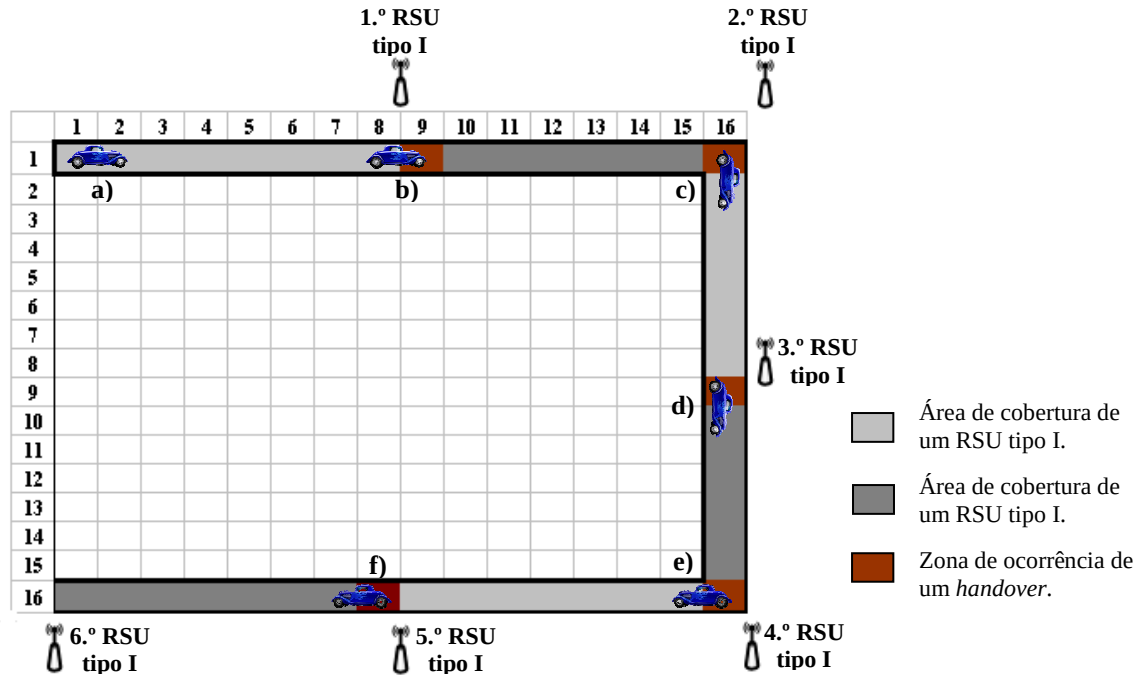


Figura 4.1 – Cenário *handover* clássico apenas com RSUs tipo I.

Neste cenário apenas são colocados RSUs tipo I com um raio de cobertura de 8m, estes tal como anunciado anteriormente são colocados em posições pré-definidas, isto é, no meio e no cruzamento de estradas. A rota estabelecida pelo veículo será estabelecida aleatoriamente, estando estes impedidos de inverter o sentido de marcha. Relativamente às várias posições em que o veículo se encontra podemos observar as situações em que ocorrerá um *handover*, isto é, quando um veículo conectado a um RSU detectará a força do sinal de um RSU diferente:

a) O veículo encontra-se na área de cobertura do 1.º RSU tipo I.

b) O veículo encontra-se na área de ocorrência de um *handover* entre o 1.º RSU tipo I e 2.º RSU tipo I.

c) O veículo encontra-se na área de ocorrência de um *handover* entre o 2.º RSU tipo I e 3.º RSU tipo I.

d) O veículo encontra-se na área de ocorrência de um *handover* entre o 3.º RSU tipo I e 4.º RSU tipo I.

e) O veículo encontra-se na área de ocorrência de um *handover* entre o 4.º RSU tipo I e 5.º RSU tipo I.

f) O veículo encontra-se na área de ocorrência de um *handover* entre o 5.º RSU tipo I e 6.º RSU tipo I.

Podemos então concluir que no trajecto efectuado pelo veículo, ocorreram cinco *handovers*. Na figura 4.2 podemos observar a adição de um RSU tipo II ao cenário anterior.

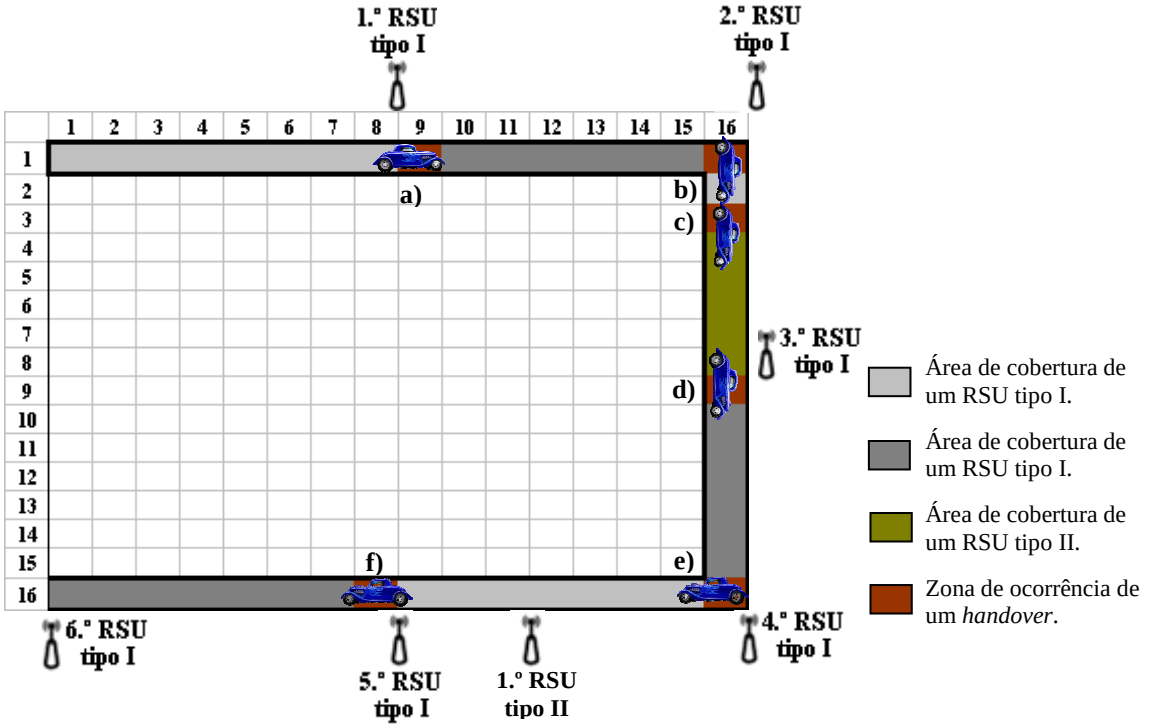


Figura 4.2 – Cenário *handover* clássico com RSUs tipo I e tipo II.

Partindo dos mesmos pressupostos do cenário da figura 4.2, este cenário difere do cenário anterior pela a adição de um RSU do tipo II. Estes tipos de RSUs têm a particularidade de possuírem um raio de cobertura de 18m e serem distribuídos ao longo da estrada de uma forma aleatória. As várias posições do veículo ao longo do circuito são identificadas a seguir:

a) O veículo encontra-se na área de ocorrência de um *handover* entre o 1.º RSU tipo I e 2.º RSU tipo I.

b) O veículo encontra-se na área de ocorrência de um *handover* entre o 2.º RSU tipo I e 3.º RSU tipo I.

c) O veículo encontra-se na área de ocorrência de um *handover* entre o 3.º RSU tipo I e 1.º RSU tipo II.

d) O veículo encontra-se na área de ocorrência de um *handover* entre o 1.º RSU tipo II e 4.º RSU tipo I.

e) O veículo encontra-se na área de ocorrência de um *handover* entre o 4.º RSU tipo II e 5.º RSU tipo I.

f) O veículo encontra-se na área de ocorrência de um *handover* entre o 5.º RSU tipo I e 6.º RSU tipo I.

Neste cenário foram contabilizados seis *handovers*, pois num cenário denominado de *handover* clássico, um *handover* ocorre sempre que um veículo detecta a força do sinal de um RSU diferente, não diferenciando RSUs do tipo I de RSUs do tipo II. Na figura 4.3 é apresentado o cenário denominado de proposta de *handover*.

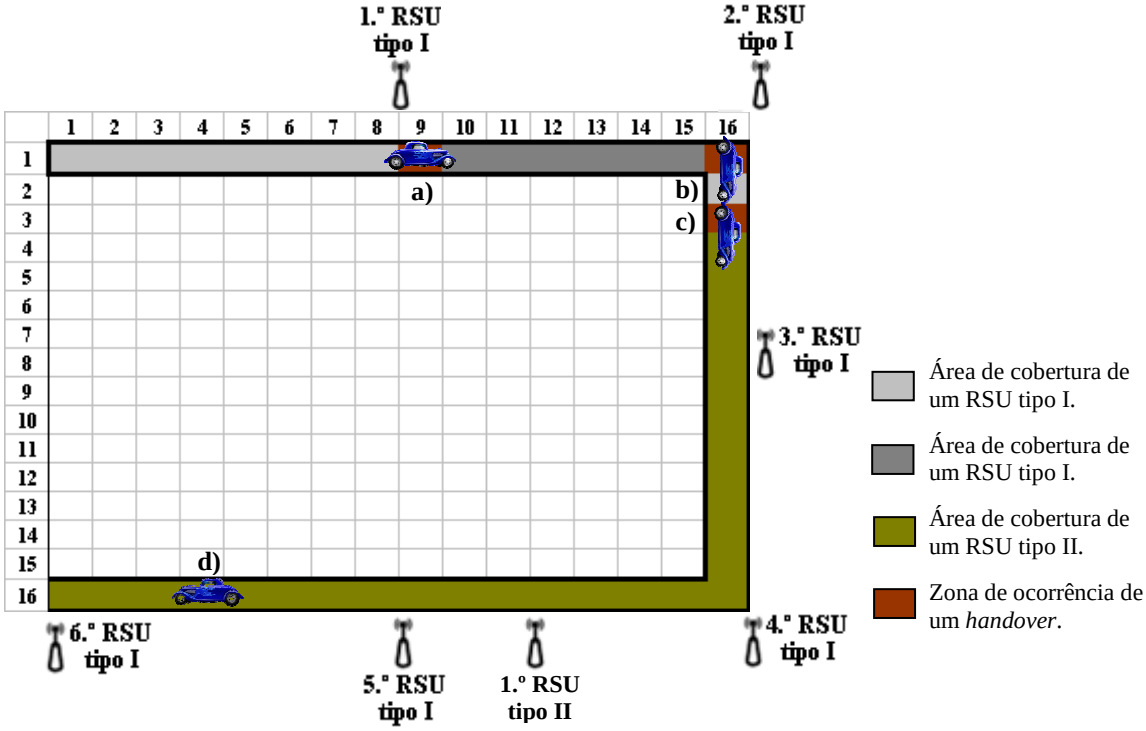


Figura 4.3 – Cenário proposta de *handover* com RSUs tipo I e tipo II.

Para este cenário proposta de *handover*, o que difere dos cenários anteriores é a forma como poderá ocorrer um *handover* com RSUs do tipo II. Isto é, caso um veículo esteja no raio de cobertura de um RSU tipo II e detecte a força do sinal de um novo RSU, o *handover* só ocorrerá quando o raio de cobertura desse RSU tipo II for totalmente percorrido. Para as diferentes posições do veículo podemos verificar que:

a) O veículo encontra-se na área de ocorrência de um *handover* entre o 1.º RSU tipo I e 2.º RSU tipo I.

b) O veículo encontra-se na área de ocorrência de um *handover* entre o 2.º RSU tipo I e 3.º RSU tipo I.

c) O veículo encontra-se na área de ocorrência de um *handover* entre o 3.º RSU tipo I e 1.º RSU tipo II.

d) O veículo encontra-se na área de cobertura do 1.º RSU tipo II.

Neste cenário pode-se verificar que apenas por três vezes ocorrem *handovers*. Pelo qual podemos concluir que com este cenário proposta de *handover* o número de *handovers* ocorridos diminuem consideravelmente.

Como forma de implementar estes cenários para posteriormente proceder-se a uma simulação foi elaborado um programa em linguagem java. Na figura 4.4 será apresentado um diagrama das classes que compõem o programa em questão.

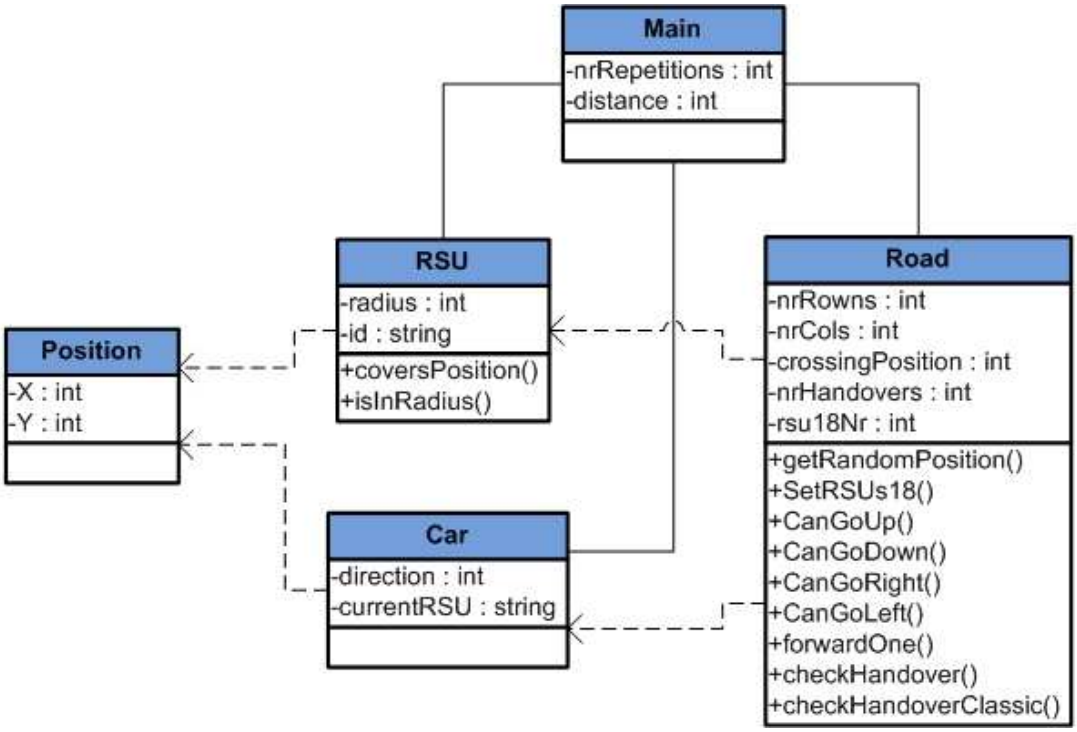


Figura 4.4 – Diagrama de classes.

Perante o diagrama de classes podemos observar que o programa desenvolvido é composto por cinco classes, onde é possível ver o nome das mesmas, os seus atributos e métodos. Observa-se também que a classe *RSU* e *Car* são dependentes da classe *Position*, uma vez que é através desta que tanto um veículo como um RSU obtém uma posição. Da mesma forma é possível observar que a classe *Road*, depende das classes *RSU* e *Car*, pois é esta a classe que possibilita a "criação" da estrada com os respectivos RSUs e veículo.

Em seguida será detalhada cada uma das classes, bem como cada um dos seus respectivos métodos.

Classe Position

Esta classe permite representar uma coordenada (X e Y). Esta coordenada será utilizada para representar uma posição dentro da matriz.

Classe Car

Nesta classe são declarados três parâmetros relativos ao veículo: a posição, a direcção e o RSU ao qual está conectado.

Classe RSU

Classe em que se declara os parâmetros relativos ao RSU: o raio, a posição e o identificador do RSU. Esta classe contém alguns métodos fundamentais relativos área de cobertura de um RSU, tais como:

- **coversPosition :** Este método recebe como argumento uma posição relativa à nova posição do veículo e verifica se a área de cobertura do RSU abrange essa posição. Primeiro é verificado no sentido X se o RSU cobre a posição recebida como argumento e só depois no sentido Y. Através da figura 4.5 temos uma melhor percepção do funcionamento deste método.

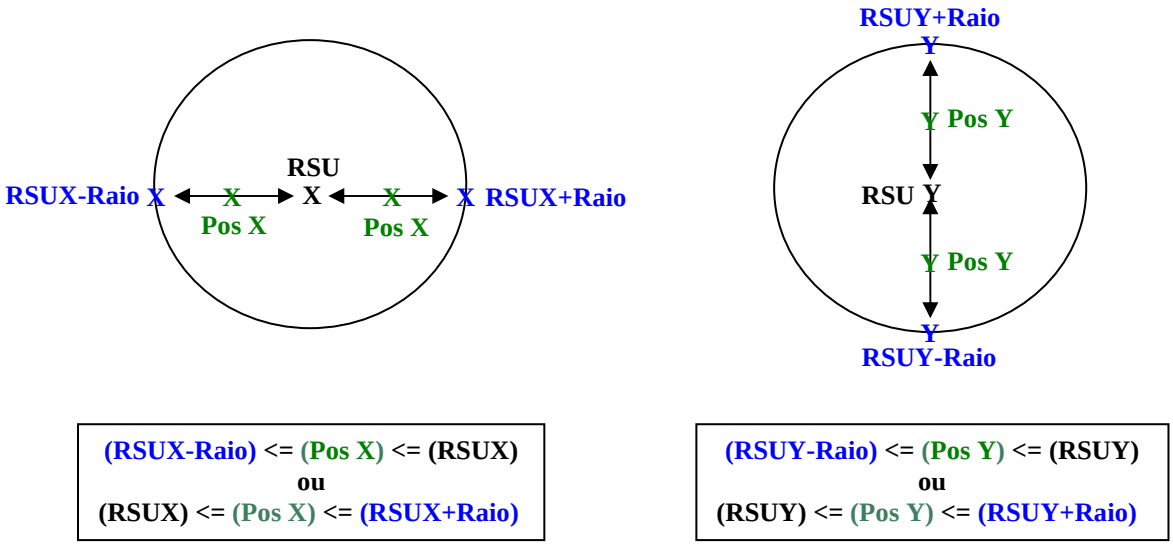


Figura 4.5 – Método *coversPosition*.

- **isInRadius:** Este método, tal como o anterior, recebe como argumento uma posição e permite verificar se essa posição está a intersectar o raio do RSU. Assim para

um sentido X temos: **(Pos X)==(RSU-Raio) ou (Pos X)==(RSU+raio).** E para um sentido Y: **(Pos Y)==(RSU-Raio) ou (Pos Y)==(RSU+raio).**

Classe Road

Esta classe para além de possibilitar a representação de uma estrada, permite registar o número de *handovers* ocorridos, quer para o cenário clássico *handover*, quer para o cenário proposta de *handover*. Os métodos que esta classe contém são os seguintes:

- getRandomPosition: gera uma posição válida para colocar os RSUs tipo II conforme os cruzamentos, calculando aleatoriamente a posição para um cruzamento no sentido de X ou para um cruzamento no sentido de Y da seguinte forma:

1. Calcula aleatoriamente qual dos eixos X ou Y será o primeiro a ser calculado.
2. Calcula um valor aleatório para o eixo calculado na alínea anterior.
3. Calcula um valor aleatório para o outro eixo.

- setRSUs18: Para um número de RSUs do tipo II calcula as respectivas posições baseadas no método anteriormente descrito (getRandomPosition).

- canGoUp: indica se o veículo tem a possibilidade de mudar a direcção para cima. Para tal, o veículo não se pode encontrar em Y=0, X tem de ser múltiplo de 16, isto é, quando existe um cruzamento e, a direcção actual do veículo não pode ser no sentido descendente uma vez que ele não pode inverter a direcção.

- canGoDown: indica se o veículo tem a possibilidade de mudar de direcção para baixo, para isso o veículo não se pode encontrar no fim de estrada (Y = nrRows), X tem de ser múltiplo de 16 e a direcção actual do veículo não pode ser ascendente.

- canGoRight: indica se o veículo tem possibilidade de mudar de direcção para a direita, para isso o veículo não se pode encontrar no fim da estrada (Y = nrRows), Y tem de ser múltiplo de 16 e a direcção actual do veículo não ser para a esquerda.

- canGoLeft: indica se o veículo pode mudar de direcção para a esquerda, para isso o veículo tem de se encontrar em X>1, Y tem de ser múltiplo de 16 e a direcção actual do veículo não pode ser para direita.

- forwardOne: este método faz com que o veículo se mova uma posição. Este método procede da seguinte forma:

1. Calcula as direcções válidas em que o veículo se pode mover (canGoUP, canGoDown, canGoRight e canGoLeft).
2. Consoante as direcções válidas escolhe uma delas aleatoriamente.
3. Calcula a nova posição baseada na direcção escolhida.
4. Verifica se ocorre *handover* (checkHandover, checkHandoverClassic).

- checkHandover: método para o cálculo do número de *handovers* ocorridos no cenário denominado de proposta de *handover*. Aqui é chamado o método checkRSU18 para identificar três casos que poderão ocorrer.

1.º caso: *Handover* de um RSU tipo I para um RSU tipo II

Se o veículo não estiver no raio de cobertura de um RSU do tipo II, percorre a lista de RSUs deste tipo e verifica se algum poderá estar a abranger a posição do veículo, se sim, regista o *handover*.

2.º caso: *Handover* de um RSU tipo II para um RSU tipo I e *handover* de um RSU tipo II para um RSU tipo II.

Quando está no raio de cobertura de um RSU do tipo II, calcula através do método (loseRSU18) se deixou de estar coberto por esse RSU, caso se confirme, passa a estar coberto por um do tipo I, uma vez que estes cobrem o mapa todo e regista o *handover*.

3.º caso: *Handover* de um RSU tipo I para outro RSU tipo I.

Se o veículo se mover no sentido de X verifica se a próxima posição entra no raio de um RSU1. Se for verdade Regista o *handover*.

Se o veículo se mover no sentido de Y verifica se a próxima posição entra no raio de um RSU1. Se for verdade Regista o *handover*.

- checkHandoverClassic: Método que permite calcular o número de *handovers* ocorridos no cenário *handover* clássico. Neste método um *handover* poderá ocorrer em quatros casos:

1.º caso: *Handover* de um RSU tipo I para um RSU tipo II.

Se o veículo não estiver no raio de cobertura de um RSU do tipo II, percorre a lista de RSUs deste tipo e verifica se algum poderá estar a abranger a posição do veículo, se sim, regista o *handover*.

2.º caso: *Handover* de um RSU tipo II para outro RSU tipo II.

Através do método (isInRadius), verifica se a próxima posição passa a estar coberta por um RSU do tipo II diferente, se sim, regista o *handover*.

3.º caso: *Handover* de um RSU tipo II para um RSU tipo I.

Quando está no raio de cobertura de um RSU do tipo II, calcula através do método (loseRSU18) se deixou de estar coberto por esse RSU, caso se confirme, passa a estar coberto por um do tipo I, uma vez que estes cobrem o mapa todo e regista o *handover*.

4.º caso: *Handover* de um RSU tipo I para um outro RSU tipo I.

Se o veículo se mover no sentido de X verifica se a próxima posição entra no raio de um RSU1. Se for verdade Regista o *handover*.

Se o veículo se mover no sentido de Y verifica se a próxima posição entra no raio de um RSU1. Se for verdade Regista o *handover*.

- classe Main: Esta classe instancia todas as outras classes e contém um método que permite executar o código.

4.3.2. Resultados

Nesta fase poderemos verificar os resultados derivados das duas simulações efectuadas, para a simulação da média de números de *handovers* ocorridos de acordo com a variação da percentagem *over-coverage* de RSUs e para a simulação da média do número de *handovers* ocorridos em termos de velocidade média do veículo.

Para ambas as simulações serão apresentadas para os respectivos cenários (*handover* clássico e proposta de *handover*) tabelas com os respectivos resultados e um gráfico com o objectivo de se obter uma melhor percepção dos mesmos.

- **Percentagem *over-coverage* de RSUs**

Para efectuar esta simulação para além de se considerar as características anteriormente enunciadas para a execução da mesma, foi considerado que o veículo se movia a uma velocidade constante na ordem dos 4m/s. Visto que a rota pretendida tem uma duração de 100s, com a velocidade constante de 4m/s o veículo terá de percorrer uma distância de 400m.

Sendo assim para a distância de 400m os resultados para os dois cenários podem ser verificados nas seguintes tabelas.

Tabela 4.1 – Resultados da 1.º simulação para o cenário *handover* clássico.

Cenário *handover* clássico		
Over-coverage (%)	**N.º RSUs Tipo II**	**Média de N.º handovers**
1%	1	0,58
5%	3	0,7
10%	5	0,76
15%	7	0,83
20%	11	0,91
25%	12	0,92

Tabela 4.2 – Resultados da 1.º simulação para o cenário proposta *handover*.

Cenário proposta de *handover*		
Over-coverage (%)	**N.º RSUs Tipo II**	**Média de N.º handovers**
1%	1	0,46
5%	3	0,4
10%	5	0,35
15%	7	0,31
20%	11	0,25
25%	12	0,24

Para a obtenção destes resultados em cada um dos cenários, efectuou-se para cada percentagem de *over-coverage*, em que cada uma corresponde a um determinado número de RSUs tipo II, 100 repetições. Sendo a média de *handovers*, o somatório do número de *handovers* para cada percentagem de *over-coverage* a dividir pelo número de repetições. Como o objectivo desta simulação para ambos os cenários é mostrar a eficiência em *handovers* ocorridos por intervalo de tempo é necessário dividir a média por 100s. Na figura 4.6 estes resultados poderão ser observados graficamente.

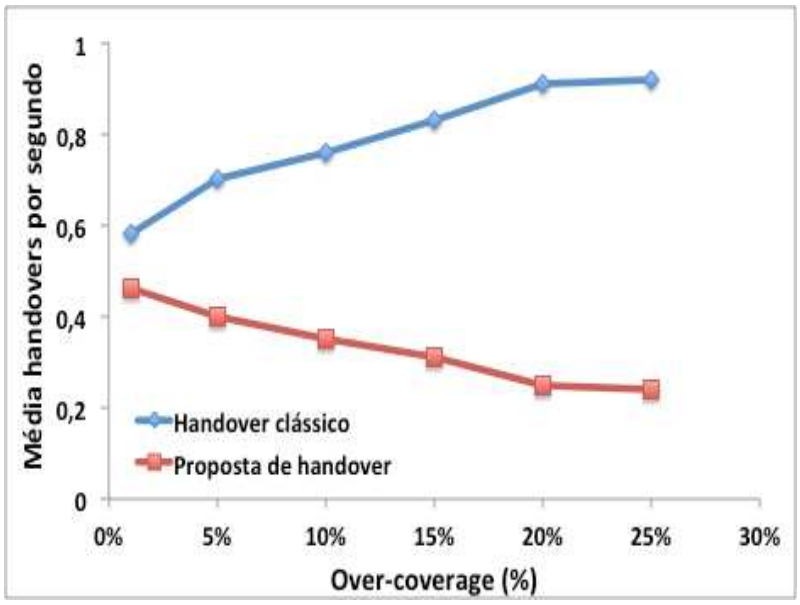


Figura 4.6 – Média do número de *handovers* ocorridos de acordo com a variação da percentagem *over-coverage* de RSUs.

Perante o gráfico da figura 4.6 podemos afirmar que para o cenário *handover* clássico, o número médio de *handovers* ocorridos aumenta com o aumento da percentagem *over-coverage* de RSUs tipo II. Isto deve-se ao facto de sempre que um veículo detectar a força do sinal de um novo RSU, ele executar um *handover*.

Para o cenário proposta *handover* verifica-se exactamente o contrário, a média de *handovers* diminui com o aumento da percentagem *over-coverage* de RSUs tipo II. Pois quanto maior o número de RSUs tipo II, maior é a probabilidade de estes serem detectados pelo veículo e como neste cenário só ocorrerá um *handover* quando o raio de cobertura desse RSU tipo II for totalmente percorrido pelo veículo mesmo que seja detectada a força do sinal de um novo RSU, o número de *handovers* ocorridos diminui.

- **Velocidade do veículo**

Nesta simulação, com o objectivo de estimar o número de *handovers* em termos de velocidade média do veículo definiu-se uma percentagem de *over-coverage* fixa em 15%, ou seja, serão distribuídos aleatoriamente 7 RSUs do tipo II ao longo da rota estabelecida pelo veículo. Os resultados obtidos para uma variação de velocidade por parte do veículo foram os seguintes:

Tabela 4.3 – Resultados da 2.º simulação para o cenário *handover* clássico.

Cenário handover clássico		
Velocidade (m/s)	**Distância (m)**	**Média de N.º handovers**
1,5	150	29
2,33	233	46
3,25	325	68
4,2	420	87

Tabela 4.4 – Resultados da 2.º simulação para o cenário proposta de *handover*.

Cenário proposta de handover		
Velocidade (m/s)	**Distância (m)**	**Média de N.º handovers**
1,5	150	12
2,33	233	18
3,25	325	25
4,2	420	31

Tal como na simulação anterior, para esta simulação efectuou-se 100 repetições, neste caso para cada uma das velocidades. Como a rota estabelecida por um veículo tem a duração de 100 segundos, para cada uma das velocidades o veículo percorre distâncias diferentes. A média de *handovers* foi então obtida, pela soma das repetições a dividir por 100.

Na figura 4.7 podemos observar um gráfico que nos permite ter uma melhor percepção dos resultados obtidos.

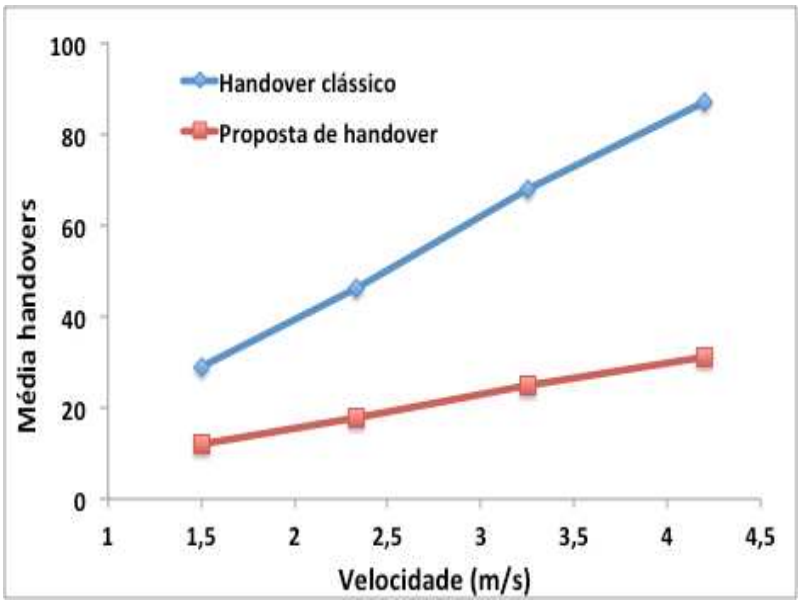


Figura 4.7 – média do número de *handovers* ocorridos em termos de velocidade média do veículo.

Perante o gráfico podemos afirmar que para ambos os cenários quanto maior a velocidade do veiculo, maior o número de *handovers*, pois com o aumento da velocidade a distância percorrida pelo veículo será maior e consequentemente detectará um maior número de RSUs. No entanto, também é visível no gráfico, que no cenário proposta de *handover* ocorrerão menos *handovers*.

4.4. *Handover* Seguro

Numa comunicação VoIP com a utilização de vários tipos de mensagens SIP é necessário proceder-se a três fases: o registo, Sessão *Invitation* e etapas de terminação da sessão.

Na primeira, um utilizador procede ao envio de mensagens de Registo, com o intuito de participar numa sessão SIP e registar-se no domínio do destinatário. Sempre que o utilizador é identificado no servidor de registo, de acordo com o seu perfil pessoal é reservado no servidor local uma localização IP e um número de porta.

Na segunda é necessário o envio de uma mensagem INVITE por parte do utilizador para o estabelecimento de uma sessão. Esta mensagem é enviada para um servidor proxy que enviará a mensagem para o nó correspondente, na recepção da mensagem INVITE o nó correspondente enviará como resposta um ACK.

Na terceira, caso uma chamada não seja estabelecida, o utilizador poderá terminar a sessão usando a mensagem CANCEL ou uma mensagem BYE.

Sendo assim, as trocas de mensagens SIP devem ser protegidas, de forma que a segurança e a privacidade na rede VoIP sejam garantidas sempre que ocorre um *handover*. Pois um atacante poderá encaminhar uma mensagem de RE-INVITE não autenticada para o servidor SIP com a finalidade de enganar o actual servidor para que um outro ponto de acesso seja excluído na comunicação, sendo este ataque considerado com um *denial of service* (DoS). Numa outra situação, um atacante poderia "sequestrar" uma sessão enviando uma mensagem BYE forjada e terminar a chamada original. Por isso um nó quando se move de uma zona para outra não deve considerar essa zona como uma rede confiável, e quando o servidor SIP recebe um pedido para um novo utilizador, deverá verificar se este corresponde a uma identidade de confiança.

4.4.1. Esquema para um *handover* seguro durante uma chamada

Relacionado com a mobilidade dos nós, é possível distinguir dois casos: quando ocorre mobilidade antes de uma chamada ou quando ocorre durante uma chamada.

Na primeira um *handover* ocorrerá quando é enviado um pedido de registo por parte do utilizador a um servidor *visited Redirect* (VR), o qual encaminhará o pedido ao servidor *home Redirect* (HR). De seguida um utilizador poderá iniciar uma sessão através do envio de uma mensagem SIP INVITE ao nó destinatário. Na segunda um *handover* ocorrerá depois do estabelecimento de uma sessão SIP, pois contrariamente à

mobilidade antes da chamada, aqui uma mensagem de estabelecimento de sessão é enviada antes da mensagem de Registo. O nó correspondente logo que receba a mensagem RE-INVITE envia os dados para a nova localização do utilizador, usando um identificador correspondente ao da configuração original.

Em seguida será proposto um esquema de segurança relativo à ocorrência de um *handover* durante uma chamada, este esquema foi desenvolvido para um cenário em que o veículo que pretende estabelecer uma chamada com um veículo correspondente, está a mover-se.

Numa primeira fase denominada por fase de pré-registo o veículo executa um pré-registo seguro com os RSUs vizinhos antes da ocorrência do *handover*, este pré-registo consiste numa troca segura de parâmetros QoS.

Como um veículo deve estar autenticado a um servidor de Registo SIP, deve-se evitar que a autenticação seja executada sempre no início da sessão, pois poderão ocorrer vários ataques SIP, para isso utiliza-se uma entidade de autenticação SIP com uma entidade de confiança entre o veículo e o próximo servidor SIP seleccionado durante o *handover*. Na autenticação entre o veículo e o servidor SIP será utilizado um mecanismo de autenticação mútua através de troca de chaves.

Em seguida inicia-se o processo de sinalização, no qual cada mensagem SIP é encriptada com um valor aleatório para evitar ataques por repetição, o receptor incrementa esse valor aleatório e envia de volta a mensagem de resposta SIP. Uma vez que os recursos num contexto de redes sem fios são mais escassos é importante evitar a sobrecarga da largura de banda com as mensagens de sinalização.

Depois de concluído o processo de sinalização, é executada a fase de Registo através de uma mensagem REGISTER. Esta mensagem será encriptada e enviada para o HR. Para encriptação da mensagem REGISTER será utilizado o mesmo procedimento da mensagem RE-INVITE.

Na figura 4.8 pode-se verificar um esquema que exemplifica com mais especificidade a troca de mensagens dos vários intervenientes. Neste esquema poderá ser observado a troca de mensagens na fase de pré-registo e no processo de sinalização.

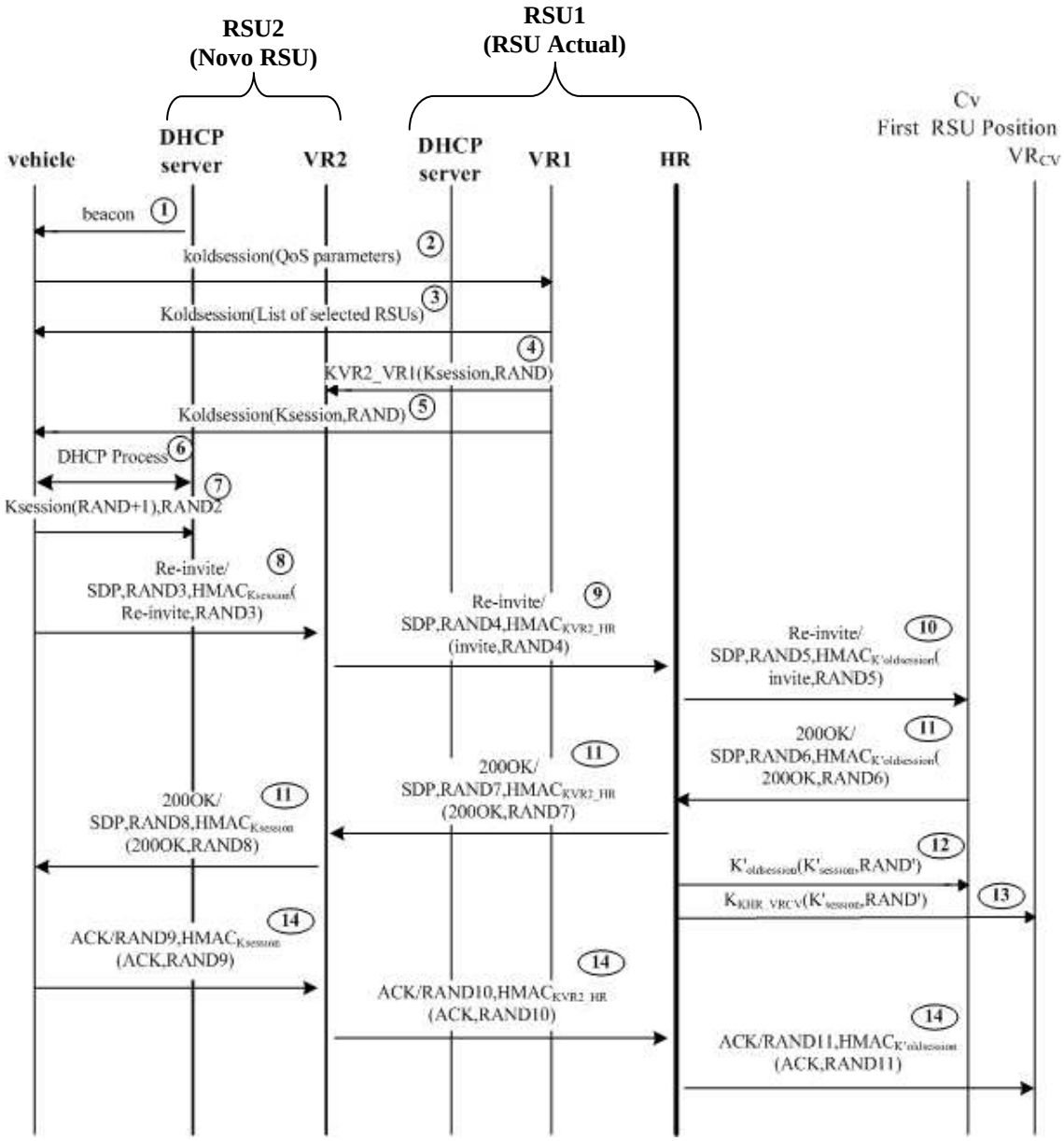


Figura 4.8 – Esquema exemplificativo da fase de Pré-Registo.

1. O veículo detecta a presença de um novo RSU através da recepção de um beacon.
2. O veículo envia um conjunto de parâmetros ao RSU1, que por sua vez os encaminhará para o *Visited Redirect Server* 1, VR1. Estes parâmetros são encriptados com a actual chave de sessão: $K_{oldsession}$.
3. O RSU1 enviará para o veículo a lista de RSUs seleccionados, encriptados com a $K_{oldsession}$.
4. O VR1 gera uma nova chave, a $K_{session}$, e envia para *Visited Redirect Server* 2, VR2. Essa chave é encriptada por outra chave simétrica, K_{VR2_VR1} a qual é

partilhada por VR2 e VR1. Adicionam um valor RAND, para evitar ataques por repetição.

5. O VR1 envia a chave $K_{session}$ para o veículo, essa chave é encriptada com o $K_{oldsession}$ e é adicionado um valor RAND para evitar ataques por repetição.
6. Tem início um *mid-call handover* com o RSU2 e o veículo a obterem um novo endereço IP.
7. O veículo envia ao VR2 o valor RAND incrementado, encriptado com a $K_{session}$ e um novo valor RAND2 para evitar ataques. O VR2 decifra o valor RAND+1 e verifica a sua exactidão. Se coincidirem o veículo fica autenticado e automaticamente o servidor também.
8. Inicia-se o processo de sinalização com o veículo a enviar a mensagem RE-INVITE protegida para *Visited Redirect Server* 2,VR2. Esta mensagem é protegida através de um *hash* baseado no código de autenticação da mensagem, encriptada com a chave de sessão $K_{session}$.
9. VR2 decifra a mensagem usando $K_{session}$, de seguida envia a mensagem encriptada com a mesma chave K_{VR2_HR} para o *Home Redirect Server*, HR.
10. O HR decifra a mensagem usando K_{VR2_HR} e encripta-a com a $K'_{oldsession}$ que representa a chave partilhada entre HR e o *Correspondent Vehicle*, CV.
11. O HR gera uma nova $K'_{session}$ e envia-a para o RSU ao qual o veículo correspondente está conectado. Esta chave é encriptada com o $K'_{oldsession}$ e é lhe adicionado um valor RAND para evitar ataques por repetição.
12. O HR envia a nova $K'_{session}$ e envia para o servidor do veículo correspondente, VR_{cv}. Esta chave é encriptada com o K_{HR_VRCV} e é lhe adicionado um valor RAND para evitar ataques por repetição
13. Recebendo a mensagem, o CV envia para o veículo um ACK200OK SIP, encriptado com o mesmo mecanismo usado para proteger a mensagem RE-INVITE.
14. O veículo envia de volta outra mensagem ACK protegida através das chaves $K_{session}$, K_{VR2_HR} e $K'_{oldsession}$. Os dados neste momento serão direccionados para o novo endereço IP.

CAPÍTULO 5

Conclusões

Num contexto de redes veiculares a tendência para melhorar a segurança e a qualidade de vida de um condutor é cada vez mais elevada. Por isso começam a surgir vários tipos de aplicações, entre as quais se destaca a aplicação tempo-real VoIP.

Para redes veiculares a mobilidade IP constitui um problema, pois uma elevada mobilidade faz com que sejam efectuadas por diversas vezes trocas de rede, ou seja, que o *handover* ocorra com maior frequência. Uma gestão ineficiente do *handover*, no caso de uma aplicação VoIP pode levar a perdas de conectividade, o que contribui para uma degradação da qualidade da voz numa comunicação.

Visto isto, este trabalho tinha como principal objectivo propor uma solução que alcançasse um *handover* seguro e simultaneamente com qualidade de serviço para aplicações de tempo-real em redes veiculares. Para tal, foram analisadas várias soluções, uma das quais foi escolhida para servir de referência à proposta apresentada.

A proposta apresentada neste trabalho resulta na execução de uma fase de pré-registo, tendo esta fase como objectivo garantir segurança na troca de mensagens e reduzir o número de *handovers*. Esta fase de pré-registo em relação à segurança permite antes da ocorrência de um *handover* efectuar uma troca segura de parâmetros QoS entre o veículo e RSUs vizinhos. Em relação à qualidade de serviço a fase de pré-registo possibilita a escolha do melhor RSU ao qual o veículo se deve conectar no momento em que é executado um *handover*.

5.1. Síntese do trabalho realizado

Para a proposta de um *handover* seguro e com qualidade de serviço para uma aplicação tempo-real em redes veiculares começou-se por construir uma solução que permitisse reduzir o número de *handovers*. Essa solução consistiu no cálculo de uma equação (eq. 4.1) relativa a um factor de selecção que permitisse seleccionar o melhor RSU ao qual o veículo se deve conectar. Essa equação tendo como base a equação (eq. 3.1) desenvolvida pelos autores no trabalho que serviu de referência sofreu algumas alterações. A primeira deve-se à disponibilidade do próximo RSU a ser conectado,

decidiu-se não utilizar a variável correspondente à ocupação de recursos, *Or*, uma vez que se considerou que estes estariam sempre disponíveis. A segunda deve-se ao facto de se ter considerado M_s não como a velocidade principal no período *camping*, mas como o tempo que um veículo está conectado a um RSU. Na terceira, decidiu-se atribuir para o factor de transmissão, *R*, um valor teórico igual para todos os RSUs, pois a solução foi desenvolvida num ambiente de simulação e não num ambiente real.

No fim concluiu-se pela equação (eq. 4.1) que quanto maior a cobertura do raio do RSU, maior é a probabilidade desse RSU ser seleccionado. Partindo deste pressuposto foram efectuadas duas simulações. A primeira teve como objectivo calcular a média de *handovers* ocorridos de acordo com uma percentagem *over-coverage*, a segunda de calcular o número de *handovers* ocorridos em termos de velocidade média. Ambas as simulações consideraram dois cenários, o primeiro onde não é usada a fase pré-registo, cenário *handover* clássico e o segundo onde é usada a fase de pré-registo, proposta de *handover*. Estes dois cenários foram desenvolvidos e analisados numa perspectiva mais teórica e numa perspectiva mais prática.

Em termos teóricos, para cada um dos cenários, foram desenvolvidas equações que permitem o cálculo do número de *handovers*. Para o cenário *handover* clássico teve-se essencialmente em conta a força do sinal recebido do RSU, para o cenário proposta de *handover* teve-se em conta a equação (eq. 4.1) que permite o cálculo do factor de selecção.

Em termos práticos, foi desenvolvido um programa em linguagem java que permitisse efectuar simulações para cada um dos cenários propostos. Cada cenário foi desenvolvido com diferentes pressupostos. No cenário *handover* clássico sempre que um veículo detectasse um RSU diferente ocorria um *handover*, no cenário proposta de *handover*, mesmo que veículo detectasse um RSU diferente, o *handover* só ocorria, quando o veículo acabasse de percorrer totalmente o raio de cobertura do RSU ao qual estava conectado.

Relativamente aos resultados obtidos, estes vão ao encontro do estudo efectuado analiticamente e aos resultados obtidos pelos autores no trabalho que serviu de referência à proposta aqui apresentada.

Depois de garantir qualidade de serviço através da redução do número de *handovers*, foi necessário garantir segurança no *handover*. Com base no trabalho que serviu de referência à proposta apresentada desenvolveu-se um esquema que possibilitasse obter um *handover* seguro durante uma chamada. No esquema elaborado

foi necessário garantir a segurança na fase de pré-registo, no processo de sinalização e na fase de registo.

Na fase de pré-registo, o veículo autentica-se a um servidor SIP por um mecanismo de segurança denominado por autenticação mútua que utiliza troca de chaves. Em contraste com a solução que serviu de base a este trabalho, depois de verificada a identidade de VR2, este será automaticamente autenticado pelo veículo, evitando assim mais uma troca de chaves na rede.

No processo de sinalização cada mensagem SIP é encriptada com um valor aleatório de, forma a, evitar ataques por repetição.

Para a fase de registo, a mensagem REGISTER foi encriptada da mesma forma que a mensagem RE-INVITE no processo de sinalização.

5.2. Trabalho futuro

Apesar do principal objectivo para o desenvolvimento deste trabalho ter sido cumprido é ainda possível melhorar esta solução ao nível da qualidade de serviço e segurança no *handover*, através das seguintes propostas:

1. Melhorar o modelo analítico, com a introdução de novos parâmetros responsáveis por verificar e melhorar o estado da rede na equação do factor de selecção. Tendo como objectivo reduzir o número de *handovers* e optimizar a utilização da largura de banda.

2. Verificar a consistência dos resultados obtidos, através da utilização de velocidades mais realísticas. Com velocidades mais elevadas a duração das simulações terão um aumento exponencial.

3. Em vez da proposta ser desenvolvida essencialmente na camada de aplicação, pode-se utilizar um modelo *cross-layer*. Este modelo permite a utilização de várias camadas e estabelecer uma comunicação directa entre os seus protocolos levando que a partilha de todo o tipo de informação seja feita com facilidade.

Referências

[1] B. G. Mateus, "Análise sobre o impacto da densidade veicular , da carga da rede e da mobilidade no desempenho de protocolos de roteamento para Redes Veiculares. Dissertação de Mestrado em Ciência da Computação, Universidade Federal do Ceará, Fortaleza, CE, Brasil," 2010.

[2] P. J. Fernandez Ruiz, C. A. Nieto Guerra, and A. F. G. Skarmeta, "Deployment of a Secure Wireless Infrastructure Oriented to Vehicular Networks," *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*. pp. 1108–1114, 2010.

[3] D. Le, X. Fu, and D. Hogrefe, "A review of mobility support paradigms for the internet," *Communications Surveys & Tutorials, IEEE*, vol. 8, no. 1. pp. 38–51, 2006.

[4] L. Wu, Y. Zhang, and F. Wang, "A new provably secure authentication and key agreement protocol for SIP using ECC," *Comput. Stand. Interfaces*, vol. 31, no. Elsevier Science Publishers B. V., pp. 286–291, 2009.

[5] F. Esposito, A. M. Vegni, I. Matta, and A. Neri, "On modeling speed-based vertical handovers in vehicular networks 'Dad, slow down, I am watching the movie'," *GLOBECOM Workshops (GC Wkshps), 2010 IEEE*. pp. 11–15, 2010.

[6] C.-M. Huang, C.-H. Lee, and P.-H. Tseng, "Multihomed SIP-Based Network Mobility Using IEEE 802.21 Media Independent Handover," *Communications, 2009. ICC '09. IEEE International Conference on*. pp. 1–5, 2009.

[7] S. El Brak, M. Bouhorma, and A. A. Boudhir, "VoIP over VANETs (VoVAN): A QoS Measurements Analysis of Inter-Vehicular Voice Communication in Urban Scenario," *New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on*. pp. 1–6, 2012.

[8] B. Triki, S. Rekhis, and N. Boudriga, "Secure and QoS-aware SIP handover for VoIP communication in vehicular adhoc networks," *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International*. pp. 695–700, 2011.

[9] J. Fitzpatrick, S. Murphy, and J. Murphy, "An approach to transport layer handover of VoIP over WLAN," *CCNC 2006. 2006 3rd IEEE Consumer Communications and Networking Conference, 2006.*, vol. 2, pp. 1093–1097.

[10] ITU-T, "Recommendation ITU-T G.107. The E-model: a computational model for use in transmission planning," 2011.

[11] ITU-T, "ITU-T Recommendation G.113. Transmission impairments due to speech processing," 2007.

[12] Z. Mo, H. Zhu, K. Makki, and N. Pissinou, "MURU: A Multi-Hop Routing Protocol for Urban Vehicular Ad Hoc Networks," *Mobile and Ubiquitous*

Systems: Networking & Services, 2006 Third Annual International Conference on, pp. 1–8, 2006.

[13] K. Zhu, D. Niyato, P. Wang, E. Hossain, and D. In Kim, "Mobility and handoff management in vehicular networks: a survey," *Wireless Communications and Mobile Computing*, vol. 11, no. 4, pp. 459–476, Apr. 2011.

[14] R. I. Meneguette, "Universidade Federal de São Carlos Rede Overlay de Suporte a Ambientes Virtuais Colaborativos em Redes Veiculares. Dissertação de Pós-Graduação em Ciência da Computação, Universidade Federal de São Carlos, SP, Brasil," 2009.

[15] S. Buruhanudeen, M. Othman, and B. M. Ali, "Mobility models, broadcasting methods and factors contributing towards the efficiency of the MANET routing protocols: Overview," *Telecommunications and Malaysia International Conference on Communications, 2007. ICT-MICC 2007. IEEE International Conference on*, pp. 226–230, 2007.

[16] A. Nandan, S. Das, G. Pau, M. Gerla, and M. Y. Sanadidi, "Co-operative downloading in vehicular ad-hoc wireless networks," *Wireless On-demand Network Systems and Services, 2005. WONS 2005. Second Annual Conference on*, pp. 32–41, 2005.

[17] L. Wischhof, S. Member, A. Ebner, H. Rohling, S. Member, and A. Intervehicle, "Information Dissemination in Self-Organizing Intervehicle Networks," vol. 6, no. 1, pp. 90–101, 2005.

[18] F. Li and Y. Wang, "Routing in vehicular ad hoc networks: A survey," *Vehicular Technology Magazine, IEEE*, vol. 2, no. 2, pp. 12–22, 2007.

[19] M. S. Almalag, "Vehicular Networks: From Theory to Practice, chapter Safety-Related Vehicular Applications. Chapman & Hall/CRC.," pp. 6[1–26], 2009.

[20] U. Lee, R. Cheung, and M. Gerla, "Vehicular Networks: From Theory to Practice, chapter Emerging Vehicular Applications. Chapman & Hall/CRC.," pp. 6[1–30], 2009.

[21] E. S. Boysen and L. Strand, "Security analysis of the SIP Handover Extension. University Graduate Center Kjeller (UNIK)," pp. 84–96, 2009.

[22] C. W. Hardy, *QoS Measurement and Evaluation of Telecommunications Quality of Service. New York, NY, USA, John Wiley & Sons*. 2001.

[23] T. J. Walsh and R. Kuhn, "Challenges in securing voice over IP," *Security & Privacy, IEEE*, vol. 3, no. 3. pp. 44–49, 2005.

[24] ITU-T, "Methods for objective and subjective assessment of quality," vol. P.800.1, 2006.

[25] L. Sun and E. C. Ifeachor, "Voice quality prediction models and their application in VoIP networks," *Multimedia, IEEE Transactions on*, vol. 8, no. 4. pp. 809–820, 2006.

[26] D. Endler, D. Ghosal, R. Jafari, A. Karlcut, M. Kolenko, N. Nguyen, W. Walkoe, and J. Zar, "VoIP Security and Privacy Threat Taxonomy, VoIPSA," p. 36, 2005.

[27] J. Manner and M. Kojo, "Mobility Related Terminology. IETF RFC 3753. June 2004," 2004.

[28] C. Perkins, "'IP mobility Support for IPv4', IETF RFC 3344, Agosto de 2002," 2002.

[29] D. Johnson and C. Perkins, "'Mobility Support in IPv6', IETF RFC 3775, Junho de 2004.," 2004.

[30] R. Koodli, "'Mobile IPv6 Fast Handovers'. IETF RFC 5568. July 2009," 2009.

[31] A. Viinikainen, J. Puttonen, M. Sulander, T. Hämäläinen, T. Ylönen, and H. Suutarinen, "Flow-based fast handover for mobile IPv6 environment – implementation and analysis," *Computer Communications*, vol. 29, no. 16, pp. 3051–3065, Oct. 2006.

[32] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "' Proxy Mobile IPv6'. IETFR FC 5213. August 2008," 2008.

[33] K.-S. Kong, W. Lee, Y.-H. Han, M.-K. Shin, and H. You, "Mobility management for all-IP mobile networks: mobile IPv6 vs. proxy mobile IPv6," *Wireless Communications, IEEE*, vol. 15, no. 2. pp. 36–45, 2008.

[34] S. Bhosale and R. D. Daruwala, "Experimental analysis of horizontal and vertical handovers in wireless access networks using NS2," *Information and Communication Technologies (WICT), 2011 World Congress on*. pp. 594–599, 2011.

[35] Yi-Bing Lin and I. Chlamtac, "*Wireless and Mobile Network Architectures*". *John Wiley & Sons, Inc, 2001*. 2001.

[36] G. Camarillo, *SIP Demystified*, McGraw-Hil. 2002, p. 320.

[37] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "'SIP: Session Initiation Protocol'. IETF RFC 3261. June 2002," 2002.

[38] Z. Yan, H. Zhou, H. Zhang, and S. Zhang, "Speed-Based Probability-Driven Seamless Handover Scheme between WLAN and UMTS," *Mobile Ad-hoc and Sensor Networks, 2008. MSN 2008. The 4th International Conference on*. pp. 110–115, 2008.

[39] T. Guillet, A. Serhrouchni, and M. Badra, "Mutual Authentication for SIP: A Semantic Meaning for the SIP Opaque Values," *New Technologies, Mobility and Security, 2008. NTMS '08.* pp. 1–6, 2008.

[40] Y.-P. Liao and S.-S. Wang, "A new secure password authenticated key agreement scheme for SIP using self-certified public keys on elliptic curves," *Computer Communications*, vol. 33, no. 3, pp. 372–380, Feb. 2010.