Resumo

As redes veiculares são, hoje em dia, um alvo forte de investigação, que têm como principal objetivo aumentar a segurança nas vias de trânsito.

O objetivo deste trabalho é dar a conhecer a arquitetura das redes veiculares, os protocolos de comunicação e onde podem ser aplicadas estas redes. Sem deixar esquecido um pormenor bastante importante, a segurança e a proteção dos utilizadores.

Por fim, pretende-se dar a conhecer um projeto já concretizado na cidade do Porto, o *Drive-IN*.

Introdução

Verifica-se que nos últimos anos houve um aumento do interesse e das pesquisas em relação às comunicações entre veículos. Estes sistemas de comunicação entre veículos formam as chamadas redes veiculares.

Hoje em dia, as viaturas têm incorporado diferentes avanços tecnológicos que melhoram a experiência do condutor e dos passageiros. Exemplos disso são a utilização de sistemas mais eficazes de travagem, sensores capazes de detectar e advertir o condutor da proximidade de obstáculos e alarmes de velocidade acima do permitido.

Em geral, esses sistemas são baseados em sensores e atuadores cada vez mais sofisticados, que fazem com que o veículo possa detectar sinais no ambiente e informar o condutor.

A necessidade da existência de uma variedade de aplicativos que viabilizem a comunicação entre veículos e infra-estruturas, torna cada vez mais relevante o estudo sobre as redes veiculares, de modo que estas tenham a capacidade de comunicarem através de algum dispositivo sem fio.

Este trabalho abordará as redes veiculares, percebendo a importância de estabelecer comunicação rápida e eficiente nos mais variados seguimentos da sociedade.

Arquitetura

As redes veiculares podem ser consideradas um caso especial das redes móveis ad-hoc (MANETs), que utilizam o padrão de comunicações sem fio IEEE 802.11. A comunicação entre veículos pode ser efetuada da seguinte maneira:

- Comunicação veículo a infraestrutura (V2I)

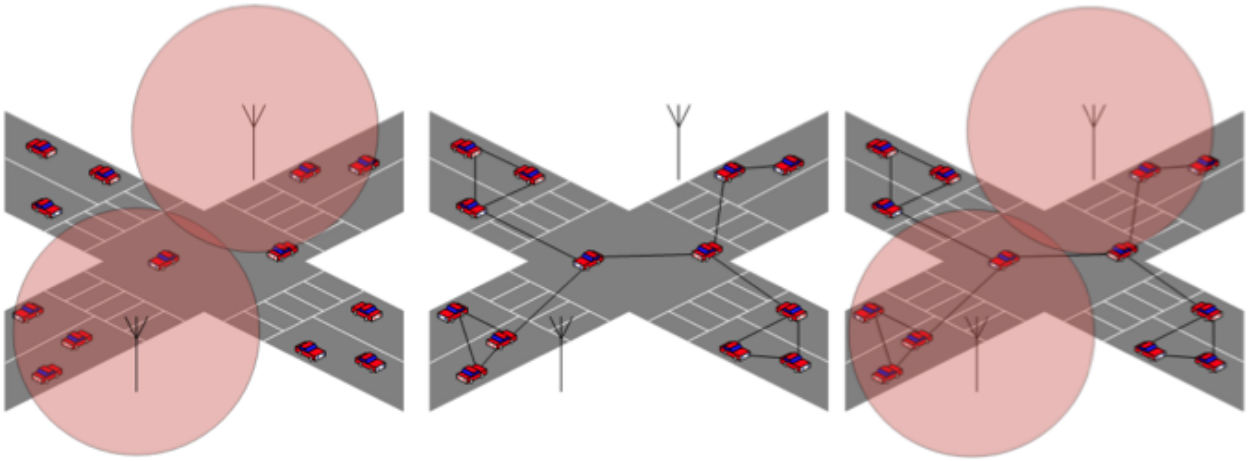
Antenas fixas colocadas ao longo da estrada, funcionam como pontos de acesso fornecendo acesso à internet. Neste cenário não existe qualquer ligação entre veículos. Neste modelo, a implementação de pontos de acesso numa auto-estrada torna-se bastante dispendiosa para se obter uma cobertura total.

- Comunicação veículo a veículo (V2V)

Tal como o nome indica, redes formadas por vários veículos equipados com dispositivos de comunicação sem fios de curto alcance que podem comunicar entre si. Veículos equipados com estes dispositivos formam um tipo especial de rede Ad-hoc móvel, denominada "*Vehicular Ad-hoc Network"* (VANET).

- Hibrida

É simultaneamente composta pelas duas arquiteturas anteriores, V2I e V2V, para colmatar as falhas existentes.

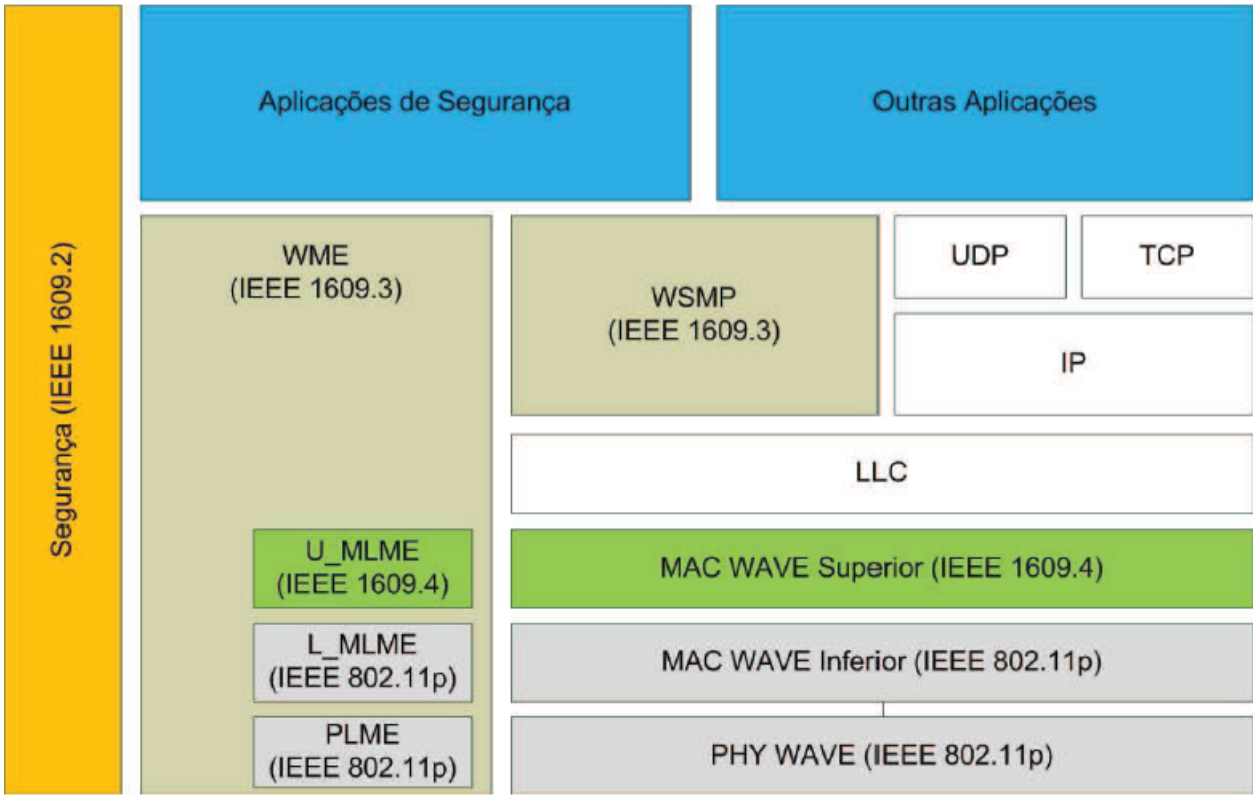


Protocolos de comunicação

A arquitectura WAVE

Wireless Access in Vehicular Environments (WAVE), também conhecido por 802.11p, é um protocolo MAC ainda em desenvolvimento pelo grupo de trabalho IEEE 802.11, baseado no padrão IEEE 802.11, de modo a fornecer um sub-nível MAC e físico fiável (oferecendo uma latência baixa entre os 100 microssegundos e os 50 milissegundos, um alcance rádio até os 1000 metros e um bom funcionamento do protocolo em veículos com velocidades máximas ate 200 km/h) em cenários de redes veiculares.

Além disso, a arquitetura WAVE designa uma família de padrões que não se restringe às camadas MAC e física. Os padrões da família IEEE 1609 definem outras camadas da pilha de protocolos, incluindo uma camada de rede alternativa à camada IP, caraterísticas de segurança para aplicações DSRC e operação em múltiplos canais de comunicação.



O objectivo principal do IEEE 1609 é prover um conjunto padronizado de interfaces para que diferentes fabricantes de automóveis possam prover comunicações entre veículos (V2V) ou entre veículos e a infra-estrutura de comunicação (V2I). Esse passo é importante para que haja interoperabilidade entre todos os dispositivos fabricados. Além da padronização das interfaces, o padrão deve considerar que os veículos estão em altas velocidades e, portanto, as comunicações devem ser completadas em intervalos curtos de tempo para que os requisitos dos Sistemas Inteligentes de Transporte sejam atendidos.

O padrão IEEE P1609.1 especifica serviços e interfaces da aplicação de Gerenciamento de Recursos da arquitetura WAVE. O IEEE P1609.2 define formatos e processamento seguros de mensagens. O IEEE P1609.3 especifica os serviços das camadas de rede e de transporte, incluindo o endereçamento e o roteamento. Além disso, o padrão 1609.3 define a MIB (*Management Information Base*) para a pilha WAVE. O padrão IEEE P1609.4 define modificações no padrão IEEE 802.11, para a operação em múltiplos canais. Finalmente, o acréscimo IEEE 802.11p define as diferenças específicas do controle de acesso ao meio em ambientes de comunicação WAVE com relação ao IEEE 802.11 tradicional.

Segurança/Problemas relevantes (privacidade ...) [Pag. 238-084.PDF]

Quer a segurança, quer o fornecimento de serviços confiáveis e autênticos, são sempre uma questão chave em Redes de Computadores. Não é diferente em Redes Veiculares. As VANETs visam possibilitar segurança nas estradas, planejamento de rotas rodoviárias e comércio eletronico. Para estas aplicações em particular, segurança de redes é ainda mais fundamental. Com isto, torna-se necessário garantir a confiança neste tipo de redes através de protocolos específicos para o efeito.

O padrão IEEE P1609.2 [IEEE Std 1609.2 2006] define formatos e processamento de mensagens seguros. Esse mesmo padrão é também utilizado para definir as circunstâncias em que devem ser usadas e processadas as mensagens seguras, de acordo com a definição do sistema DSRC/WAVE. O padrão abrange métodos para garantir a segurança da gestão das mensagens WAVE e as mensagens de aplicativos, com a excepção de mensagens de segurança originadas pelo veículo. Também descreve as funções administrativas necessárias para apoiar as ferramentas essenciais/tradicionais de segurança, (a Infraestrutura de Chaves Públicas (PKI) e certificação). Por exemplo, define como a chave pública de um utilizador é usada para criptografar uma mensagem ou como é realizada a autenticação do usuário, sem anonimato.

Outro tipo de segurança que se tem de ter em conta, é a prevenção a eventuais ataques de “hackers”. Há diversas naturezas de dados maliciosos nas VANETs. Um atacante pode enviar informações falsas sobre excertos da VANET ou sobre si próprio (localização errada, por exemplo). Como um nodo usa toda a informação disponível na VANET para verificar a validade de uma nova informação, a densidade da rede e os sensores disponíveis podem acabar por tornar os ataques imprevisíveis.

Há a possibilidade de que existam atacantes capazes de se comunicarem a longas distâncias. Tais atacantes têm flexibilidade na localização dos nós que tentam convencer da veracidade de dados falsos. Pode-se dividir os alvos entre locais (fisicamente próximos do atacante) e remotos.

Contra alvos locais, o atacante tende a ter maior sucesso, posto que a probabilidade de dados conflituosos vindos dos nós vizinhos é menor. Assim, a proximidade necessária para um ataque local é de difícil manutenção (afinal, trata-se de redes veiculares, móveis), e a potencialidade de ataques locais é menos preocupante. Além disso, alvos remotos são naturalmente mais numerosos.Quando um atacante tenta convencer nós alvos de que dados incorretos são válidos, três desdobramentos são possíveis:

- O ataque pode não ser detectado pelos nós alvos – portanto, um sucesso completo. Ocorre em geral quando os alvos estão isolados ou completamente cercados por dados maliciosos. Neste caso, o nó acaba por aceitar todas as informações maliciosas.
- Pode ser detectado por um ou mais alvos, mas ainda deixar incertezas sobre a veracidade dos dados; E, no mais otimista dos cenários,
- Pode ser detectado e corrigido – ou seja, não sobrando incerteza sobre a validade dos dados.

Quando os nós alvos têm acesso a nós honestos podem ser capazes de detectar que um

ataque está ocorrendo através de inconsistências nos dados coletados de diversas fontes, mas ao mesmo tempo eles podem se recusar a corrigir o ataque devido a informações insuficientes. Caso contrário, poderiam estar se arriscando a fazer um diagnóstico incorreto, caso no qual os dados maliciosos permaneceriam ilesos. Com acesso a um número suficientemente grande de nós sabidamente honestos, os alvos são capazes de identificar corretamente os dados falsos e corrigir – cessar o ataque.

Âmbito de aplicação [Pag 210 - 084.pdf]

- Segurança no transito;

Um dos principais incentivos ao desenvolvimento das redes veiculares é o aumento da segurança rodoviária. Através da troca de informação entre veículos pode ser possível reduzir o número e a fatalidade de acidentes. Este tipo de informação pode ser apresentado ao condutor ou accionar um mecanismo ativo de segurança.

Uma maneira de evitar acidentes de trânsito é através do uso de mensagens periódicas que indiquem a velocidade, a posição e direção dos veículos. Outra perspetiva é através de mensagens somente em casos de emergência.

A *Cooperative Collision Avoidance (CCA)* é uma aplicação exemplo nesta categoria que tem por objetivo evitar colisões. Esta aplicação avisa o condutor de uma situação de emergência através do envio de mensagens. Este tipo de ação pode também ser usada em situações em que não haja muita visibilidade na via.

Em casos em que uma colisão não possa ser evitada, a utilização de mensagens serve para avisar os veículos que se aproximam do acidente e assim evitar que este se torne mais grave. Além disso, o envio de mensagens pode acelerar o envio dos serviços de emergência sem necessidade de mediação do ser humano...

- Entretenimento*;*

A grande maioria de aplicações propostas para as redes veiculares está ligada à ubiquidade de acesso à Internet. Cada vez mais os utilizadores se tornam dependentes da rede e desejam poder aceder a esta a qualquer instante em qualquer lugar. É necessário então adaptar as aplicações mais usadas às redes veiculares.

Muitas das aplicações para redes veiculares defendem o uso da arquitetura ad hoc por possibilitar a comunicação entre veículos sem necessidade dos pontos de acesso. O problema que existe é que algumas destas aplicações necessitam frequentemente de acesso à internet, que só é possível através das chamadas *gateway's* (pontos fixos de conexão).

- Assistência ao Motorista

A finalidade principal das aplicações para assistência ao motorista é auxiliar a condução do veículo a partir da disponibilização de informação útil sobre avisos de estacionamento, informação das vias de trânsito, controlo de tráfego (Radares), auxílio em cruzamentos, condução conjunta em veículos, localização em mapas, aumento da visibilidade e veículos sem condutores humanos. Ests informações obtém-se a partir de serviços e/ou podem ser consultadas através de procedimento de busca.

Dentro das aplicações desta classe, a que tem recebido mais atenção é sobre os avisos de estacionamento.

Principais desafios associados

Uma das etapas mais importantes no desenvolvimento de um protocolo, com vista a ser utilizado em redes veiculares ou em qualquer outro tipo de redes, é o seu teste/validação. Em redes veiculares, para que o desempenho real de um protocolo seja satisfatório, é necessário que o modelo de mobilidade utilizado no cenário de teste reproduza de forma mais realista possível o meio onde este vai ser utilizado. O cálculo de rotas em redes veiculares é uma tarefa desafiadora devido à alta mobilidade dos nós da rede e à instabilidade dos enlaces sem-fio.

Para definir a mobilidade veicular num cenário real, utiliza-se o tráfego de vias urbanas e baseia-se no espaço percorrido em relação ao tempo gasto, para uma distinção mais apurada do movimento veicular e dos componentes do movimento, sendo: velocidade e aceleração/desaceleração, e a medida do tempo de pausa que devem ser avaliadas.

Utiliza-se assim, o cálculo da velocidade média veicular. Esta relaciona o espaço percorrido e o tempo levado para percorrer tal espaço. Ao dividir o espaço pelo tempo obtém-se a velocidade média do veículo.

Formula da velocidade media: bla bla

Projeto

Em 2011, o projeto drive-in, envolvendo investigadores da Universidade de Aveiro (UA), implementou uma rede que ligou cerca de 500 táxis na cidade do Porto e assim permitiu a troca automática de dados entre veículos para facilitar a circulação. Trânsito, acidentes e problemas são automaticamente comunicados sem intervenção do condutor.

Permite também enviar informações sobre qualquer problema mecânico, quer para os carros em redor quer para uma oficina e serviços de reboque. Simultaneamente, em caso de acidente, o próprio carro, alerta os serviços de emergência, indicando o local onde se encontra o condutor em apuros, enquanto avisa os veículos que circulam nas proximidades.

Esta rede possui ainda outras caracteristicas. De copiloto, isto é, auxilia na ultrapassagem de grandes veículos e videoconferências entre veículos. Nos passageiros, assegura e disponibiliza acesso à internet assim como informações sobre locais de interesse na região onde está o taxi.

A tecnologia de comunicações veiculares foi desenvolvida de raiz na Universidade de Aveiro, conta também com a colaboração da Universidade do Porto e de Carnegie Mellon (EUA), o Instituto de Telecomunicações e as empresas N-DRIVE e GeoLink.

Conclusão

O objetivo principal deste trabalho era apresentar e explicar alguns conceitos das redes veiculares, tais como a sua arquitetura, rede protocolar, aplicações principais e projetos.

As redes veiculares são um avanço tecnológico que torna a experiência de conduzir mais segura. O recurso a aplicações que evitam colisões, reduzem o tempo de viagem, evitam congestionamentos, entre outras coisas, transformam a condução numa agradável sensação. Ainda a possibilidade dos passageiros terem à disposição aplicações de entretenimento torna as viagens menos aborrecidas e dinâmicas.

Claro está, as caracteristicas deste tipo de redes são um desafio ao seu desenvolvimento. É, então, necessário melhorar e criar novos protocolos e mecanismos de ligação de rede para se ter um desempenho superior.

Apesar dos claros benefícios, as ameaças de segurança à informação e a questão da privacidade representam um enorme desafio para a expansão e uso das VANETs.