

Routing in Vehicular Ad hoc Networks (VANETs)

Simão Cunha^[a93262], Gonalo Pereira^[a93168], and Rui Alves^[pg50745]

Universidade do Minho - Campus de Gualtar, R. da Universidade, 4710-057 Braga Portugal

Interligação de Redes IP (2022/2023) - Grupo 4

Resumo O presente relatório refere-se ao ensaio escrito no mbito da UC de Interligação de Redes IP, onde comearemos com uma introdução acerca do *routing* nas redes *ad hoc* veiculares assim como os principais objetivos inerentes. Também iremos apresentar algumas propostas no mbito das VANET's, tal como as suas aplicações no mundo real. Terminaremos com uma secção de conclusões a reter acerca deste tema.

Keywords: Routing, MANET, VANET, Protocolo, ITS

1 Introdução

As *Vehicular Ad Hoc Networks* (VANET's) são uma subclasse de redes *ad hoc* mveis (MANET's), que consistem num conjunto de ns mveis conectados entre si numa rede sem fios. So responsveis por dar conectividade em todo o lado aos utilizadores enquanto esto na estrada, em vez de acederem  internet atravs da rede de casa ou do local de trabalho e tmbm so responsveis por permitir comunicaes eficientes entre vculos.

A sua principal aplicao  em ITS (*Intelligent Transportation Systems*), permitindo a monitorizao do trnsito, *blind crossing* (vculos cruzam-se sem controlo de luzes), preveno de colises e de clculo de rotas em tempo real ([1]).

Inicialmente, vrios protocolos de *routing* foram desenvolvidos para as MANET's e podem ser aplicados diretamente em VANET's, mas, devido  alta velocidade dos vculos - ns da rede - e  troca dinmica de informao, existe uma fraca *performance*, pelo que existe uma principal preocupao nos protocolos de *routing* em VANET's.

A ttulo de curiosidade, as concessionrias automveis como a Audi, BMW, DaimlerChrysler, Fiat, Renault e Volkswagen uniram-se para a criao de uma associao sem fins lucrativos chamada *Car2Car Communication Consortium* (C2CCC), que se ocupa em estudar como aumentar a segurana do trfego rodovirio ao menor custo para o *end user* e para o ambiente [2].

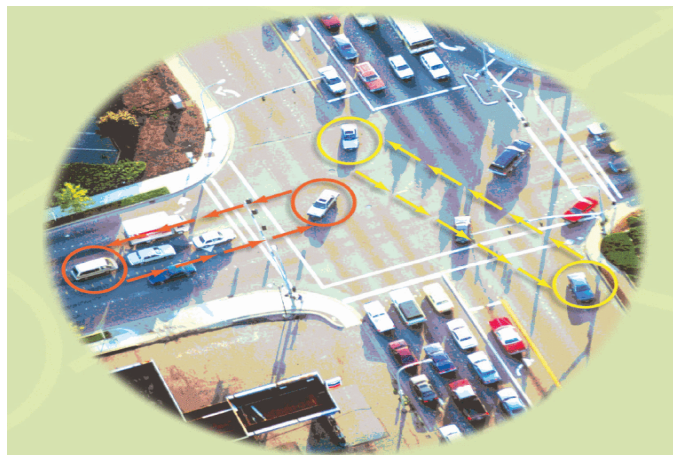


Figura 1: Ilustrao de VANET (retirado de [1])

2 Principais objetivos

As aplicaes podem ser as mais variadas mas focam-se essencialmente na monitorizao e controlo de transito, tendo tm um papel importante na preveno de acidentes.

Esta tecnologia tem como objetivo oferecer mais segurana e conforto aos utilizadores num contexto rodovirio. As VANET's, atravs da conectividade dos veculos, sero capazes de detetar situaes de congestionamento, condies da estrada, acidentes, emergncias e, mais importante, sero capazes de difundir essa informao para todos os utilizadores. Alm disso, sero capazes de implementar *blind crossing* e prevenir colises j que pode atuar em intersees e situaes de ultrapassagem conhecendo exatamente o que rodeia um veculo num dado momento. Por fim, consegue garantir que todos os veculos em circulao cumprem as regras de circulao da estrada.

Apesar de tudo, consideramos importante que numa primeira instncia se olhe para este sistema como uma rede de sensores (veculos) que partilham e interligam informao do seu meio.

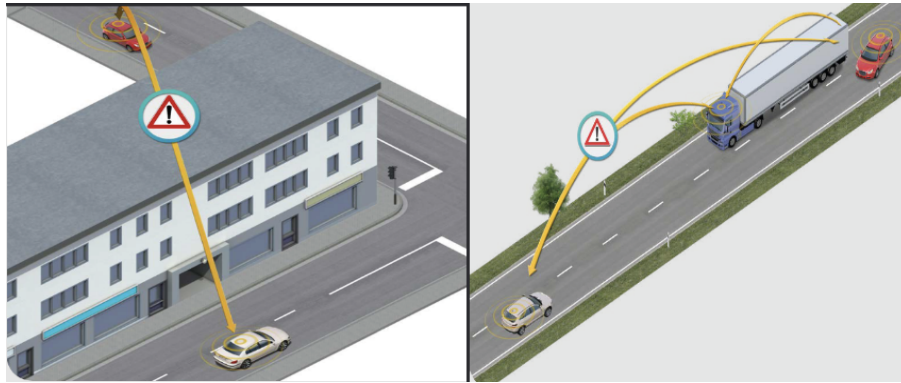


Figura 2: Exemplos de aplicaes (retirado de [2])

3 Desafios

As VANET's so caracterizadas por uma extrema e rpida mobilidade dos nodos que as constitui que se traduz na constante e rpida mudana da topologia da mesma [3]. Por esse motivo, torna-se difcil manter rotas. A arquitetura destes sistemas caracterizam-se principalmente por dois cenrios: alta densidade em pouca rea ou baixa densidade numa rea dispersa [4]. Alm disso, sendo este um servio em tempo real requer baixos valores de *delay* especialmente dado o risco que estas operaes envolvem, em que um atraso de informao pode ter resultados catastrficos.

3.1 Routing

Pelos motivos j enunciados,  difcil manter rotas neste tipos de sistemas sendo uma grande preocupao desta rea a procura de um protocolo de *routing* que consiga colmatar todas as fragilidades. Antes de discutir protocolos de *routing*,  importante perceber quais as comunicaes que so possveis numa topologia, assumindo um modelo hbrido que depende do uso de equipamentos externos.. Neste caso, identificam-se 3 tipos de comunicaes: veculo-veculo, infraestrutura-infraestrutura, veculo-infraestrutura.

Os protocolos de *routing* usualmente utilizados em MANET'S, como AODV (*Ad-hoc On-demand Distance Vector*) e DSR (*dynamic source routing*), demonstraram pouca convergncia e baixo dbito de comunicao [1]. Mais  frente iremos discutir em concreto algumas propostas de routing.

3.2 Segurança

O rápido crescimento das VANET's e as suas aplicações no mundo real levam à necessidade de manter estas redes seguras. Tal como em outras redes, também as VANET's necessitam de manter a integridade dos dados, manter confidencialidade, viabilidade, etc. As informações sobre o utilizador e sobre o seu veículo devem ser distribuídas adequadamente e de uma forma segura para outros utilizadores.

A segurança nas VANET's depende principalmente do meio de comunicação - os *delays* nestas transmissões, por exemplo, dão tempo para realizar possíveis ataques aos veículos.

Alguns dos requisitos de segurança nas VANET's são:

- **Autenticação e acessibilidade** - Os dados devem ser apenas acedidos e transmitidos pelo utilizador real. Sobre qualquer ataque, o sistema deve encerrar, não permitindo assim o acesso aos dados por entidades externas;
- **Confidencialidade** - A privacidade de todos os motoristas deve ser garantida. Este requisito de segurança é para garantir que os dados sejam lidos por utilizadores aprovados. O requisito de confidencialidade é necessário nas comunicações em grupo, onde apenas os membros do grupo têm permissão para ler esses dados;
- **Disponibilidade** - As redes VANET necessitam de agir em tempo real para muitos propósitos, pelo que devem estar acessíveis o tempo todo. Essas aplicações exigem uma reação rápida das redes de sensores ou da rede *Ad-hoc* - as mensagens que não cheguem ao destino em tempo útil podem ter resultados graves dependendo da circunstância;
- **Gravação de informação** - Qualquer informação e mensagens transmitidas são gravadas e guardadas, permitindo que, em caso de acidente, identificar a causa e corrigir eventuais erros ou *bugs*.

Caso a segurança destas redes não seja assegurada, podem ocorrer ataques como:

- **DoS Attack** (*Denial of Service* - o objetivo é tornar um serviço ou recurso indisponível para os utilizadores legítimos, ou seja, ganhar o controlo dos recursos do veículo. Isto é feito sobrecarregando o serviço ou recurso com um grande volume de tráfego ou de pedidos, de modo que ele não consiga responder a todas elas, ficando inoperável (não conseguirá receber informações críticas).
- **Sybil Attack** - Neste ataque, o invasor convence os veículos a seguirem um caminho alternativo, criando um grande número de pseudónimos e informando outros veículos sobre o congestionamento, reivindicando mais de cem veículos à frente

4 Propostas de routing

Na secção, iremos apenas abordar mais detalhadamente os vários tipos de protocolo de *routing* utilizados com VANET's.

Tal como mencionado, as topologias destas redes mudam muito rapidamente e várias vezes, pelo que as comunicações e a troca de dados são muito instáveis. De forma a combater esta problemática, foram criadas algumas estratégias de *routing* tal como observamos na figura 3.

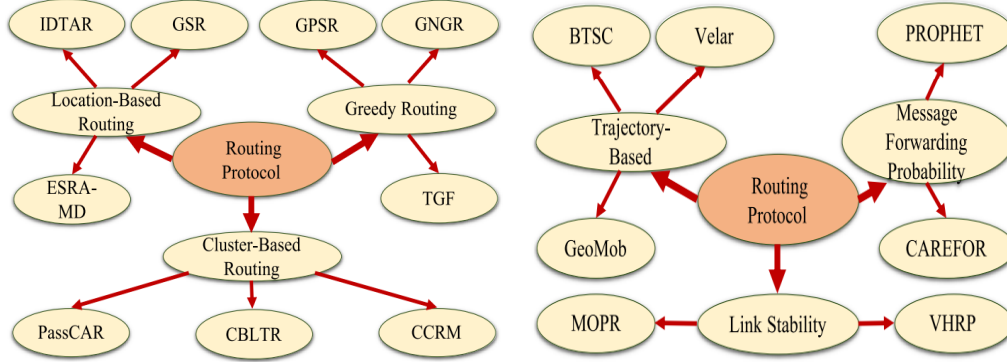


Figura 3: Tipos de protocolos de *routing* (retirado de [5])

4.1 Location-based protocols

Protocolos de *routing* baseados na posico geogrfica dos ndos (veculos), obtida atravs de GPS, sendo esse o fator de deciso para o envio de dados. A posico geogrfica  que determina que pacote de dados recebe cada ndo, diminuindo *delays* e aumentando a estabilidade.

Na imagem 4, podemos ver na prtica como  que um protocolo deste tipo  executado. Permite que sejam aplicadas algumas medidas de segurana como um aviso pr-acidente, diagnstico e manuteno do veculo, etc. Alm disso, tambm permite ter algumas aplicaes de entretenimento como jogar jogos, acesso a um *browser* de internet, etc.

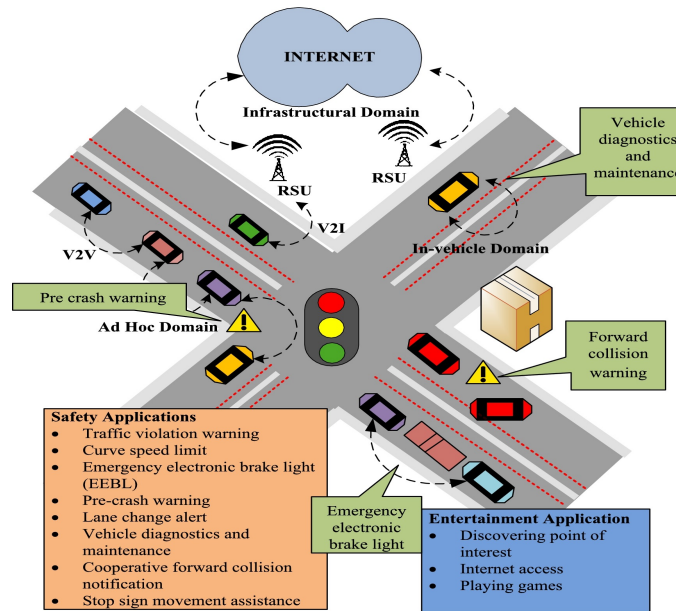


Figura 4: Exemplificao de um protocolo *location-based* (retirado de [6])

4.2 Cluster-based routing protocols

Protocolos de *routing* baseados em agrupar redes de ndos em *clusters* de acordo com determinadas caractersticas, como o grau de um ndo (n de arestas a incidir nesse ndo ou nmero de arestas a sairem desse ndo) ou a distncia entre os ndos. Posteriormente, tendo em conta a definio dos

clusters, procede-se ao envio dos pacotes de dados, o que provoca numa melhoria no débito e na estabilidade da rede.

Na imagem 4, podemos ver a estruturação de um protocolo deste tipo, onde existe uma *base station*, entidade que coordena as atividades da rede, *cluster head*, que é o centroide desse *cluster* e os *sensor nodes*, capazes de recolher informação de monitorização.

Estes protocolos têm várias aplicações como deteção de fogos artificiais, estacionamento de carros, monitorização de habitats, monitorização de saúde, manutenção de fábricas, automação industrial, etc. [7]

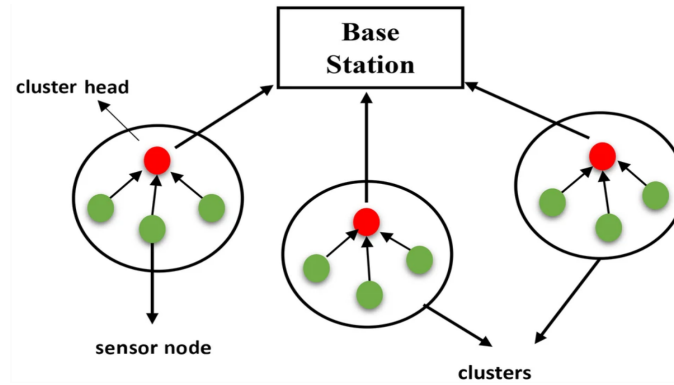


Figura 5: Estruturação de um protocolo *cluster-based* (retirado de [8])

4.3 Greedy protocols

Protocolos de *routing* baseados em construir o melhor caminho da origem até ao destino de acordo com a distância, *delay* e outras métricas.

4.4 Trajectory-Based protocols

Protocolos de *routing* baseados em trajetórias procuram estudar os dados de rotas previamente definidas de modo a conseguirem fazer previsões de padrões de trânsito.

Existem algumas variações deste tipo de protocolo, nomeadamente o protocolo baseado na rota de autocarros [9] e o protocolo baseado nas trajetórias extraídas da geolocalização dos veículos [10].

4.5 Message forwarding probability

Protocolos de *routing* baseados em probabilidade usam a informação de densidade de veículos, distância entre veículos, histórico de encontros com outros veículos para calcular a probabilidade que uma mensagem vai ser entregue.

4.6 Link Stability

Protocolos de *routing* que focam em manter as ligações estáveis, através do movimento do veículo. Estes protocolos tentam prever a duração de uma dada rota e tentam encontrar uma nova antes da ligação ser desfeita. Baseiam-se em manter tabelas de rotas e em ir prevendo a próxima rota.

5 Conclusões

Neste estudo caracterizamos VANET's, abordando os principais objetivos e apontando as duas maiores dificuldades que são o *routing* e a segurança.

Em termos de *routing* procura-se desenvolver um protocolo que consiga acompanhar todo o movimento dinâmicos deste tipo de redes mantendo os *delays* e o *packet loss* suficientemente baixos para que a informação chegue aos veículos em tempo útil. Consideramos que os protocolos de *routing* baseados na localização geográfica aparentam ser mais promissores para ultrapassar essas dificuldades, já que não guardam informação sobre o estado de ligação e nem tabelas de rotas [4]. O domínio da segurança é realmente preocupante nestas redes já que envolve um grande risco. Não apresentamos nenhuma proposta para minimização do risco mas abordamos alguns aspetos de segurança importantes a salvaguardar.

Por fim, VANET's mostram-se ser bastante únicas na sua organização e bastante promissoras para a interligação de sistemas e fluxo de informação num mundo cada vez mais interligado.

Referências

1. Fan Li *et al.*: Routing in vehicular ad hoc networks: A survey (2007)
2. Website Car2Car Consortium: <https://www.car-2-car.org/> (Consultado em fev. 2023)
3. Yingrui Jia *et al.*: Performance Analysis of VANET Routing Protocols and Implementation of a VANET Terminal (2017)
4. Hammouche Yassine *et al.* : VANET Cross-Layer Routing (2019)
5. Zhenchang Xia *et al.*: A Comprehensive Survey of the Key Technologies and Challenges Surrounding Vehicular Ad Hoc Networks (2021)
6. Ankita Srivastava *et al.*: Location based routing protocols in VANET: Issues and existing solutions (2020)
7. Asif Munir: Cluster based Routing Protocols: A Comparative study (2018)
8. Siddhant Bagga *et al.*: Clustering Based Routing Protocol for Wireless Sensor Networks Using the Concept of Zonal Division of Network Field (2022)
9. Gang Sun *et al.*: Bus-trajectory-based street-centric routing for message delivery in urban vehicular ad hoc networks (2018)
10. Fusang Zhang *et al.*: On geocasting over urban bus-based networks by mining trajectories (2016)
11. Kaur R. *et al.*: Security Issues in Vehicular Ad-Hoc Network(VANET) (2018)