Routing in Vehicular Ad hoc Networks (VANETs)

Simão Cunha[a93262], Gonçalo 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 âmbito da UC de Interligação de Redes IP, onde começaremos com uma introdução acerca do *routing* nas redes *ad hoc* veiculares assim como os principais objetivos inerentes. Também iremos apresentar algumas propostas no âmbito 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* móveis (`MANET's`), que consistem num conjunto de nós móveis conectados entre si numa rede sem fios. São responsáveis por dar conectividade em todo o lado aos utilizadores enquanto estão na estrada, em vez de acederem à internet através da rede de casa ou do local de trabalho e também são responsáveis por permitir comunicações eficientes entre veículos.

A sua principal aplicação é em ITS (*Intelligent Transportation Systems*), permitindo a monitorização do trânsito, *blind crossing* (veículos cruzam-se sem controlo de luzes), prevenção de colisões e de cálculo de rotas em tempo real ([1]).

Inicialmente, vários protocolos de *routing* foram desenvolvidos para as `MANET's` e podem ser aplicados diretamente em `VANET's`, mas, devido à alta velocidade dos veículos - nós da rede - e à troca dinâmica de informação, existe uma fraca *performance*, pelo que existe uma principal preocupação nos protocolos de *routing* em `VANET's`.

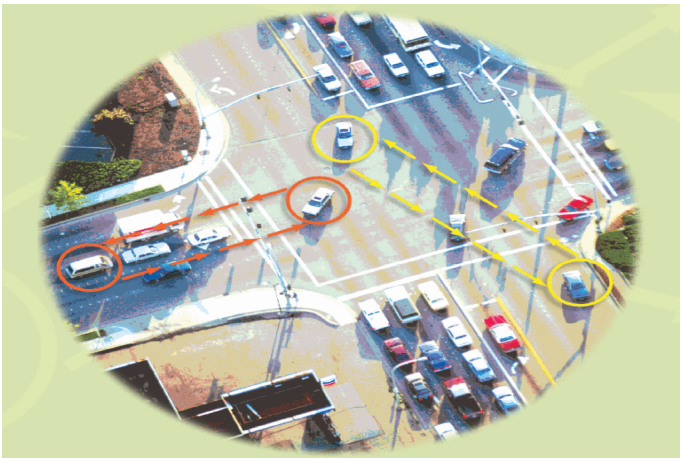

Figura 1: Ilustração de `VANET` (retirado de [1])

2 Principais objetivos

As aplicações podem ser as mais variadas mas focam-se essencialmente na monitorização e controlo de transito, tendo também um papel importante na prevenção de acidentes.

Esta tecnologia tem como objetivo oferecer mais segurança e conforto aos utilizadores num contexto rodoviário. As `VANET's`, através da conectividade dos veículos, serão capazes de detetar situações de congestionamento, condições da estrada, acidentes, emergências e, mais importante, serão capazes de difundir essa informação para todos os utilizadores. Além disso, serãp capazes de implementar *blind crossing* e prevenir colisões já que pode atuar em interseções e situações de ultrapassagem conhecendo exatamente o que rodeia um veiculo num dado momento. Por fim, consegue garantir que todos os veículos em circulação cumprem as regras de circulação da estrada.

Apesar de tudo, consideramos importante que numa primeira instância se olhe para este sistema como uma rede de sensores (veículos) que partilham e interligam informação do seu meio.

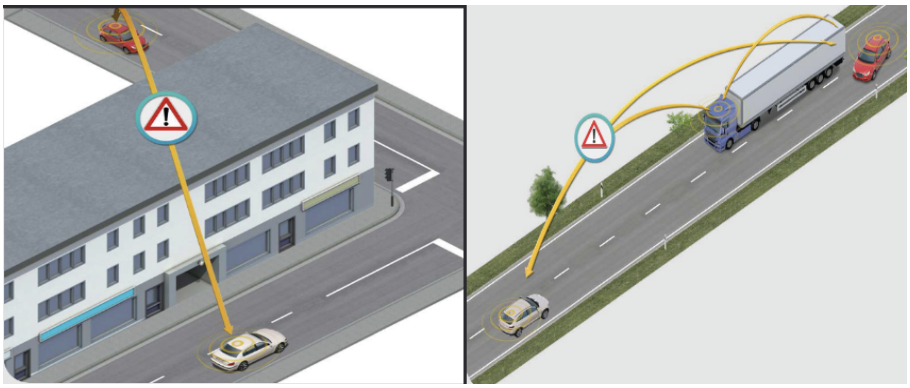

Figura 2: Exemplos de aplicações (retirado de [2])

3 Desafios

As `VANET's` são caracterizadas por uma extrema e rápida mobilidade dos nodos que as constitui que se traduz na constante e rápida mudança da topologia da mesma [3]. Por esse motivo, torna-se difícil manter rotas. A arquitetura destes sistemas caracterizam-se principalmente por dois cenários: alta densidade em pouca área ou baixa densidade numa área dispersa [4]. Além disso, sendo este um serviço em tempo real requer baixos valores de *delay* especialmente dado o risco que estas operações envolvem, em que um atraso de informação pode ter resultados catastróficos.

3.1 Routing

Pelos motivos já enunciados, é difícil manter rotas neste tipos de sistemas sendo uma grande preocupação desta área a procura de um protocolo de *routing* que consiga colmatar todas as fragilidades. Antes de discutir protocolos de *routing*, é importante perceber quais as comunicações que são possíveis numa topologia, assumindo um modelo híbrido que depende do uso de equipamentos externos. Neste caso, identificam-se 3 tipos de comunicações: veículo-veículo, infraestrutura-infraestrutura, veículo-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 convergência e baixo débito de comunicação [1]. Mais à 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 veiculo 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 [11]:

- **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, alguns dos principais ataques são:

- **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 pseudônimos e falsos nodos na rede, indicando aos outros veículos, por exemplo, um falso congestionamento;
- **Routing Attack** - Este ataque afeta o processo de *routing* da rede ou destrói os pacotes, através da exploração das vulnerabilidades dos protocolos de *routing* da camada de rede. Alguns destes ataques são, ataque de buraco negro, ataque de buraco quente e ataque de buraco cinza;
- **Timing Attack** - O ataque atrasa o envio de mensagens criticas para outros nodos da rede, aumentando assim o risco de acidentes.

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.

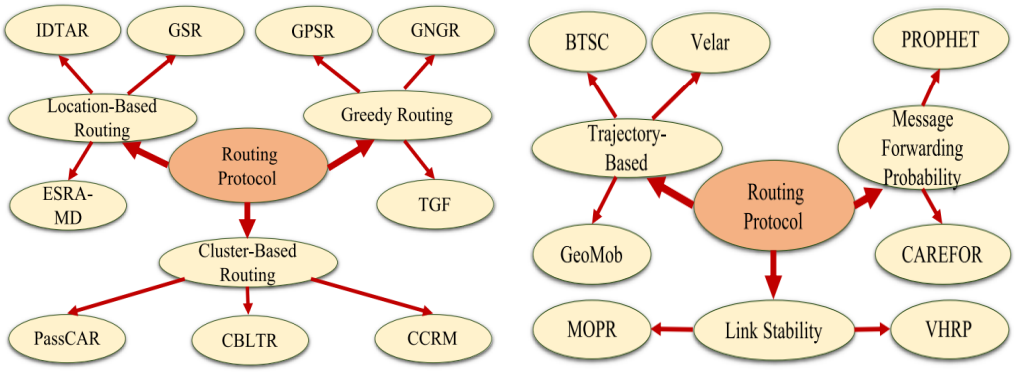

Figura 3: Tipos de protocolos de *routing* (retirado de [5])

4.1 Location-based protocols

Protocolos de *routing* baseados na posição geográfica dos nodos (veículos), obtida através de GPS, sendo esse o fator de decisão para o envio de dados. A posição geográfica é que determina que pacote de dados recebe cada nodo, diminuindo *delays* e aumentando a estabilidade.

Na imagem 4, podemos ver na prática como é que um protocolo deste tipo é executado. Permite que sejam aplicadas algumas medidas de segurança como um aviso pré-acidente, diagnóstico e manutenção do veículo, etc. Além disso, também permite ter algumas aplicações de entretenimento como jogar jogos, acesso a um *browser* de internet, etc.

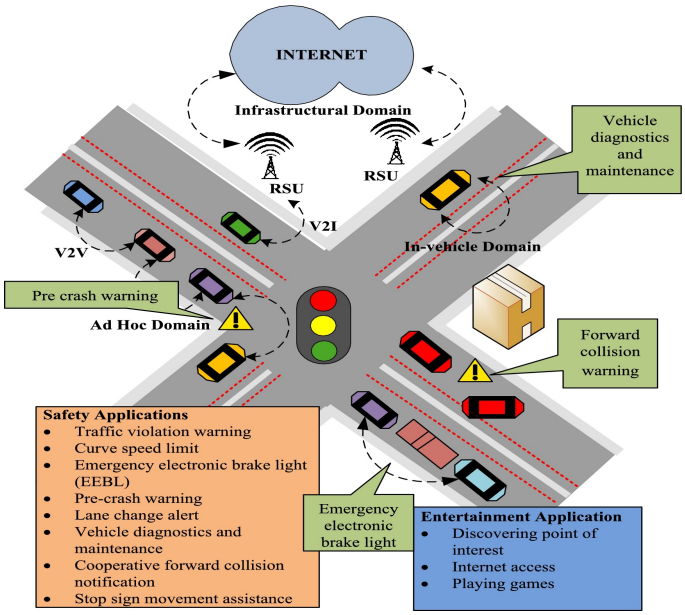

Figura 4: Exemplificação de um protocolo *location-based* (retirado de [6])

4.2 Cluster-based routing protocols

Protocolos de *routing* baseados em agrupar redes de nodos em *clusters* de acordo com determinadas características, como o grau de um nó (nº de arestas a incidir nesse nó ou número de arestas a sairem desse nó) ou a distância entre os nós. Posteriormente, tendo em conta a definição 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]

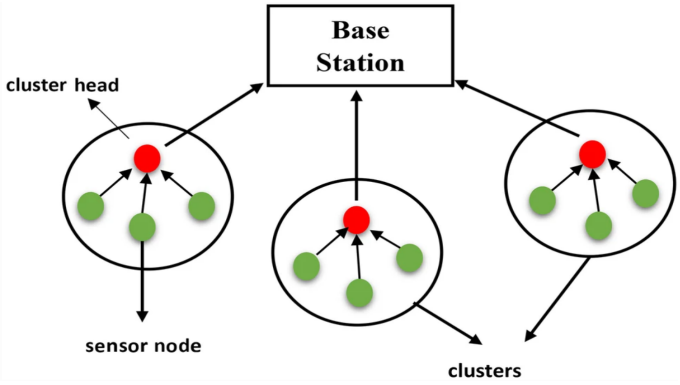

Figura 5: Estruturação de um protocolo *cluster-based* (retirado de [8])

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 Trajetory-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 dos 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 nenhumas proposta para minimização do risco mas abordamos alguns aspetos de segurança importantes a salvaguardar. Concessionárias de automóveis como a Audi, BMW, DaimlerChrysler, Fiat, Renault e Volkswagen uniram-se para a criação de uma associação sem fins lucrativos chamada *Car2Car Communication Consortium* (C2CCC), que se ocupa em estudar como aumentar a segurança do tráfego rodoviário através da interligação da informação dos veículos. [2].

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)