Vehicular Ad Hoc Networks

João Nunes, Luís Braga, and Luís Martins

University of Minho, Department of Informatics, 4710-057 Braga, Portugal
e-mail: {a82300,a82088,a82298}@alunos.uminho.pt

Resumo Vehicular ad hoc networks (VANET) é uma área que nos ultimos tempos tem tido cada vez mais popularidade e financiamento e como tal, de modo a apresentar este assunto irá ser feita uma abordagem do que está por detrás da VANET ou seja as ad hoc networks, bem como abordar a VANET em si. Explicar o seu funcionamento, as aplicações propostas e os problemas de privacidade que esta rede trás.

1 Introdução

Vehicular Ad Hoc Networks (VANET) permite que os veículos troquem informação entre si e com infraestrutura [4] de modo a melhorar significativamente a segurança na estrada. Para conseguir efetuar esta comunicação, é utilizado o conceito de wireless ad hoc networks.

Contudo, é de referir que existem vários problemas associados a esta rede, problemas essas que podem ser tanto sociais, económicos bem como tecnológicos uma vez que esta rede requer uma larga escala e elevada mobilidade [1], sendo que são vários os entraves que fazem com que esta área não esteja ainda mais desenvolvida, embora largos progressos têm sido feitos nos últimos anos.

O artigo está organizado por secções, que irão descrever como irá ser abordada a arquitetura da VANET que inclui os seus componentes, tipo de comunicação, e o funcionamento em geral desta mesma, na secção 2, quais são os principais problemas de privacidade associado a esta rede, bem como alguns modelos propostos de modo a melhorar a privacidade na terceira secção, irá ser ainda apresentado um caso de estudo da VANET na secção 4, e, por fim, a secção 5 está reservada para a conclusão deste artigo.

2 Vehicular Network

2.1 Arquitetura do Ad Hoc Vehicular Network

A VANET tem por base uma rede wireless chamada ad hoc network, ou seja, é um caso particular do ad hoc network que trabalha sobre o domínio veicular [3], numa maneira muito geral, a rede consiste em nodos móveis (carros), infraestrutura fixa e conecção wireless entre estes que permite a comunicação constante que, por sua vez, facilita a troca de informação.

O desenvolvimento desta rede serve o propósito de melhorar a segurança na estrada, uma vez que os carros, ao partilhar informação sobre o piso rodoviário ou sobre o estado de trânsito tudo isto sem interrupção da conetividade e em tempo real [5], faz com que a quantidade de informação ao dispor dos condutores facilite a sua tarefa de condução, ao ajudar na tomada de decisão.

Para ser desenvolvida esta rede, é necessária uma arquitetura que é duplamente robusta e eficiente, para tal foram estabelecidos os seguintes componentes da arquitetura VANET:

1. **AD Hoc Enviroment**: consiste em nodos (veículos) inteligentes que comunicam entre si e possui dois componentes:
   (a) On Board Unit: componente que tem a capacidade de comunicação;
   (b) Application Unit: trabalha por detrás da OBU e possui os programas de segurança e prevenção do carro [5].

2. **Infrastructure Enviroment**: consiste nas Road Side Units (RSUs) que são infraestruturas auxiliares colocadas ao lado das estradas e Access Network com dois tipos de comunicação:
   (a) V2V (Vehicle to Vehicle): comunicação veículo para veículo;
   (b) V2I (Vehicle to Infrastructure): entre os nodos móveis e a infraestrutura (RSU).

A comunicação nesta network é portanto baseada num abordagem de cooperação com cada nodo e RSU a compartilhar informação entre si. Desta forma os veículos conseguem antecipar, evitar e prevenir situações potencialmente perigosas bem como notificações sobre o trânsito [5]. A seguinte figura exemplifica o funcionamento desta rede veicular:

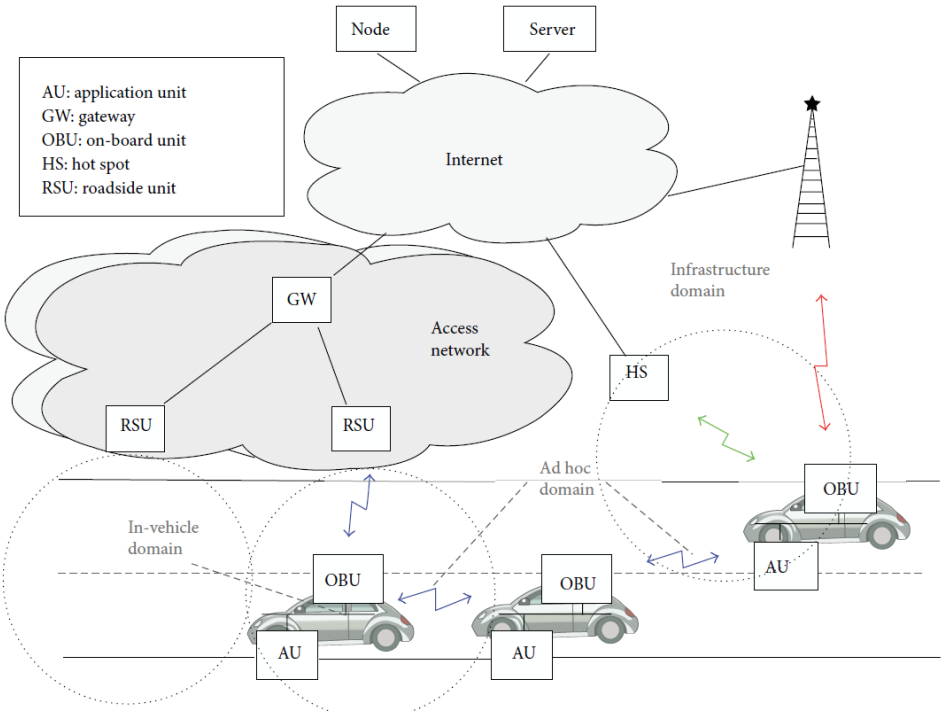

Figura 1. Funcionamento e interligação dos vários componentes da arquitetura VANET [1].

Esta arquitetura permite ainda mais um tipo de comunicação como é possível ver pela figura, sendo essa a comunicação V2B (Vehicle to broadband cloud) [1], onde os veículos podem também transferir informação para a cloud, onde irá ficar armazenada e repleta de informação que irá assistir o condutor na sua condução.

As arquiteturas VANET, ao contário do que seria esperado, não são homogênas, uma vez que estas variam de região para região já que regiões diferentes poderão possuir standards e protocolos diferentes uma vez que a topologia varia imensamente.

2.2 Comunicação

Uma das partes essenciais deste modelo é a comunicação entre os nodos, para tal, foram propostas a utilização de duas tecnologias de comunicação:

1. **IEEE 802.16** (Wireless MAN/WiMAX): útil para estabelecer conecções wireless até 48km.

2. **IEEE 802.11p** (WAVE): utilizado especificamente para VANET, intermediador da comunicação V2V e V2I numa banda de 5.9 GHz.

Destas duas, a forma de comunicação mais predominante na VANET é a norma IEEE 802.11p [6], embora tendo, mesmo assim, alguns problemas de segurança uma vez que este permite que os veículos comuniquem diretamente entre si sem autorização prévia [3], contudo, isto irá ser abordado com mais detalhe nas secções mais à frente.

Mesmo assim a tecnologia do IEE 802.11p é uma tecnologia de ponto comparado com outras mais difundidas tal como Wi-Fi ou até mesmo com a rede celular como é possível analisar na seguinte tabela [6]:

Indicative wireless data link characteristics	Technology			
	802.11p WAVE	Wi-Fi	Cellular	Infrared
Bit rate	3–27 Mb/s	6–54 Mb/s	< 2 Mb/s	< 1 Mb/s < 2 Mb/s
Communication range*	< 1000 m	< 100 m	< 15 km	< 100 m (CALM IR)
Transmission power for mobile (maximum)	760 mW (US) 2 W EIRP (EU)	100 mW	2000 mW (GSM) 380 mW (UMTS)	12800 W/Sr pulse peak
Channel bandwidth	10 MHz 20 MHz	1–40 MHz	25 MHz (GSM) 60 MHz (UMTS)	N/A (optical carrier)
Allocated spectrum	75 MHz (US) 30 MHz (EU)	50 MHz @ 2.5 GHz 300 MHz @ 5 GHz	(Operator-dependent)	N/A (optical carrier)
Suitability for mobility	High	Low	High	Medium
Frequency band(s)	5.86–5.92 GHz	2.4 GHz, 5.2 GHz	800 MHz, 900 MHz 1800 MHz 1900 MHz	835–1035 nm
Standards	IEEE, ISO, ETSI	IEEE	ETSI, 3GPP	ISO

Figura 2. Caraterísticas de várias tecnologias de network [6].

Como é possível verificar pela tabela supracitada, comparado com a rede celular esta nova tecnologia trabalha numa banda de frequência muito maior, e permite também um fluxo de transferência de dados (bits) muito maior, o que é crítico para o bom funcionamento do VANET.

Estas redes VANET também têm de ser capazes de enviar e encaminhar bastante informação, pelo que o routing dos pacotes de dados se tornou também num aspeto importantíssimo a considerar [1]. Foi, então, necessário melhorar os algoritmos já existentes bem como criar novos algoritmos, sendo que este problema de comunicação tem três aspetos principais a ser considerados:

1. **Geocast/Broadcast**: existe um conjunto de protocolos de Geocast/Broadcast para colmatar a necessidade inerente de enviar e distribuir informação em localizações desconhecidas/indeterminadas.
2. **Multicast**: é necessário em situações de grande densidade de trânsito tais como interseções ou filas de trânsito ou até mesmo em situações adversas de piso.
3. **Unicast**: este protocolo pode ser divido em três sub-protocolos
   (a) Greedy: nodos transferem pacotes de dados para os seus vizinhos mais diretos;
   (b) Opportunistic: escolhem a situação certa e oportunamente transferem a informação para o destino;
   (c) Trajectory Based: os nodos calculam os possíveis trajetos para o destino e fornecem a data através de um ou mais desses trajetos calculados.

Na seguinte imagem é possível ver os algoritmos atualmente utilizados em cada uma desta abordagem:

	Protocols/algorithms
Greedy	Geographical source routing (GSR)
	Greedy perimeter geographic routing (GPCR)
	Improved greedy traffic-aware routing (GyTAR)
	Connectivity-aware routing (CAR)
Opportunistic	OPERA: opportunistic packet relaying in disconnected vehicular ad hoc networks
	Topology-assist geo-opportunistic routing
	MaxProp
Trajectory	SiFT
	Geographical opportunistic routing (GeOpps)
	Trajectory-based data forwarding (TBD)
	Two-level trajectory-based routing (TTBR)

Figura 3. Algoritmos utilizados em cada um dos protocolos de routing na VANET [1].

3 Privacidade

Embora o modelo VANET seja um modelo benéfico para a sociedade em geral, este também traz consigo problemas sérios uma vez que se transmite informação sobre a velocidade, aceleração e localização dos veículos. Através destes dados é possível localizar os utentes da VANET [2], logo, é necessário garantir a proteção de todos os utentes da VANET uma vez que esta rede sendo ad hoc está constantemente exposta a ataques potencialmente perigosos [3].

Atualmente este modelo está baseado na tecnologia de comunicação 802.11p (WAVE). Ora, não há qualquer medida de autenticação associado a este standard devido a uma rápida necessidade de estabelecer este network algo que torna ainda mais fácil a intrusão nesta rede, a rápida mudança de topologia também faz com que uma possível intrusão no sistema seja ainda mais fácil, daí ser necessário um modelo de segurança fiável e robusto.

O primeiro modelo de segurança é a **location-based mix zones** onde os veículos mantêm o radio silence, ou seja param de transmitir informação, e mudam os seus pseudónimos, identificação única do nodo, desta forma o intervalo de tempo entre o último sinal mandado com o antigo pseudónimo e o novo sinal com a nova identificação faz com que os dois não possam ser interligados o que poderá afastar um potencial ataque ao sistema [2], contudo, o radio silence torna este modelo impeditivo uma vez que o sistema de ajuda ao condutor não poderá funcionar se não recebe nem transmite informação.

Outro modelo foi elaborado tendo por base o anterior, o modelo **CMIX** em que os utentes da VANET possuem o seu sinal encriptado numa específica zona mudando depois de pseudónimo antes de sair.

O **time based silent periods** é um modelo que se baseia em períodos de tempo onde os veículos mantêm radio silence, mudando de pseudónimo antes de retomar comunicações, contudo o problema do primeiro modelo mantém-se, o uso de radio silence efetivamente torna o VANET inútil.

Embora a segurança seja díficil de quantificar existem métricas que analisam o grau de segurança, como por exemplo, o número de veículos que um intruso não consegue identificar e a taxa de sucesso do intruso, como tal foi elaborado um modelo que tem por base duas variáveis: o trânsito dentro da cidade, baseado em taxi traces em Roma, e trânsito na autoestrada, trânsito sintético nos arredores de Madrid. Como tal, de modo a abordar estas questões de privacidade do modelo VANET, foram usados os mesmos algoritmos que estão na base do VANET [4], e simulando várias vezes ,os resultados encontram-se na seguinte figura:

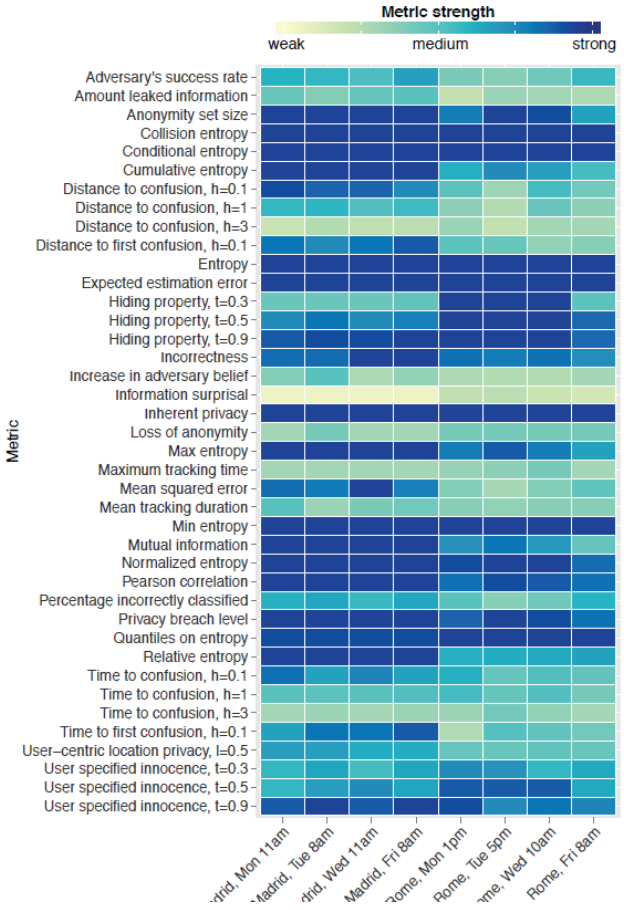

Figura 4. Métricas de privacidade juntamento do respetivo valor onde, a cor amarela representa métrica fraca e azul forte [4].

Como é possível analisar, atualmente o sistema VANET encontra-se num estado de mediocridade no que respeita a privacidade dos seus utentes, logo, é necessário melhorar os algoritmos antes de este sistema estar pronto para o público.

4 Projetos Atuais

Atualmente o maior projeto europeu VANET é o CAR 2 CAR Communication Consortium onde existe um esforço conjunto entre grandes marcas de automóveis europeus, empresas de tecnologia e centros de investigação de modo a conseguir tornar o VANET numa realidade [7].

O consórcio foi criado em 2002 com o objetivo de desenvolver os standards e os prerrequesitos deste tipo de sistema, o objetivo também passa por homogenizar os standards, possibilitando e trabalhando para que estes sejam iguais em qualquer parte do mundo [7].

No panorama nacional, existiu um projeto iniciado em 2009, entretanto foi descontinuado em 2012, que abordava o conceito do VANET. O projeto foi desenvolvido por várias equipas de universidades nacionais bem como uma universidade internacional em parceria com diversas empresas da área tal como a NDrive, empresa sediada no Porto. A componente principal do projeto foi a utilização coletiva de sensores para providenciar informações sobre o trânsito, o que melhora a eficiência e mobilidade de todos os utilizadores. O projeto foi testado em cerca de 500 táxis da região metropolitana do Porto [8].

Figura 5. Detalhes sobre o projeto DRIVE-IN.

5 Conclusão

Como é possível discernir, o sistema VANET ao permitir a comunicação entre carros e com infraestruturas auxiliares possui um potencial elevadissímo no que toca a melhorar a qualidade e segurança de todos os utentes rodoviários. Contudo, este sistema encontra-se ainda no estado embrionário, e traz consigo várias questões e problemas.

É portanto imperativo resolver estes problemas relacionados com a segurança antes do VANET estar pronto para o público em geral. Acima de tudo é necessário um bom algoritmo para a criação e distribuição de keys uma vez que todo o sistema VANET depende destas keys (identificação). A informação também necessita de ser transmitida sem qualquer alteração uma vez que qualquer alteração na informação poderá originar acidentes, para além disto a latência também deverá ser evitada uma vez que a informação necessita de chegar e ser recebida o mais rapidamente possível.

Referências

1. Wenshuang Liang, Zhuorong Li, Hongyang Zhang, Shenling Wang, and Rongfang Bie.: Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends (2015)
2. Andreas Tomandl, Hannes Federrath, Florian Scheuer.: VANET privacy by "Defending and Attacking" (2013)
3. Rashmi Mishra, Akhilesh Singh, Rakesh Kumar.: VANET Security: Issues, Challenges and Solutions (2016)
4. Isabel Wagner.: Measuring Privacy in Vehicular Networks (2017)
5. Pramod Mutalik, Venakangouda C Patil.: A Survey on Vehicular Ad-hoc Network [VANET's] Protocols for improving safety in Urban Cities (2017)
6. Panos Papadimitratros, Arnaud de La Fortelle, Knut Evenssen, Roberto Brignolo, Stefano Cosenza.: Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation (2009)
7. CAR 2 CAR Consortium.: CAR 2 CAR Consortium Communication Consortium (2018)
8. DRIVE-IN.: DRIVE-IN – Distributed Routing and Infotainment through Vehicular Inter-Networking (2009)