Unidade Curricular de Segurança de Redes
Mestrado em Segurança Informática
Mestrado em Engenharia de Redes e Sistemas Informáticos

VEHICLE-TO-VEHICLE COMUNICATION

Cláudia da Costa Maia
up201905492@up.pt

Edson Aires Junior Ferreira
up201607407@up.pt

Fabiana Manuela Alves
up201404791@up.pt

***Abstract* — Com o objetivo de diminuir as colisões e acidentes, assim como controlar o trânsito, foram desenvolvidas as Vehicle-to-Everything (V2X) communications. Mais especificamente estas comunicações podem ser: vehicle-to-infrastructure (V2I), vehicle-to-network (V2N), vehicle-to-vehicle (V2V), vehicle-to-pedestrian (V2P), vehicle-to-device (V2D) e ainda vehicle-to-grid (V2G) communications. Estas comunicações consistem em breves mensagens que incluem: a atual posição GPS, a velocidade a que se encontram e para onde se direcionam, e ainda informações de controlo. Neste projeto aprofundaremos as comunicações V2V e V2I, e como elas podem ser comprometidas através de ataques de segurança.**

I. INTRODUÇÃO

As V2V communications usam um protocolo wireless, similar a wi-fi, chamado dedicated short range communications (DSRC). Quando este protocolo é combinado com a tecnologia GPS resulta num sistema de comunicações V2V low cost que providencia um conhecimento dos veículos similarmente equipados dentro do alcance das comunicações (mais de 300 metros). Como dito anteriormente, as mensagens transmitidas pelos veículos incluem as informações de controlo que são: estado de transmissão, estado do travão, ângulo do volante, histórico do caminho do veículo e a previsão do trajeto que vai seguir. Esta tecnologia, alerta os condutores com mensagens visuais, táteis ou audíveis, ou uma combinação das mesmas, habilitando assim o condutor de prevenir colisões.

Tal como em quase todas as tecnologias, existem vários ataques de segurança que podem ocorrer nas comunicações V2V, sendo estas: flood, modify, read, spoof e replay. Assim sendo, é necessário garantir a integridade e disponibilidade dos dados, autenticação e ainda garantir que as mensagens são atuais e não repetições de eventos passados.

II. ESTADO DE ARTE

A. Tipos de ataque

Flood – os atacantes inundam a rede com mensagens de Broadcast de modo a causar denial of service, para que os condutores não sejam avisados dos perigos na estrada.

Modify – os atacantes captam a mensagem de um veículo, alteram-na e enviam-na alterada ao destinatário. Isto pode causar colisões pois como vemos na figura 1, os destinatários são enganados.

Read/eavesdropping - neste tipo de ataque, os atacantes estão à escuta das mensagens enviadas pelos carros de modo a preverem por exemplo para onde se estão a dirigir, ou de onde vieram.

Spoof – uma fonte finge ser confiável e envia mensagens falsas e erróneas aos veículos, fazendo-se passar por exemplo por um carro ou infraestrutura.

Replay – os atacantes intersetam as mensagens enviadas e enviam mensagens desatualizadas de eventos passados.

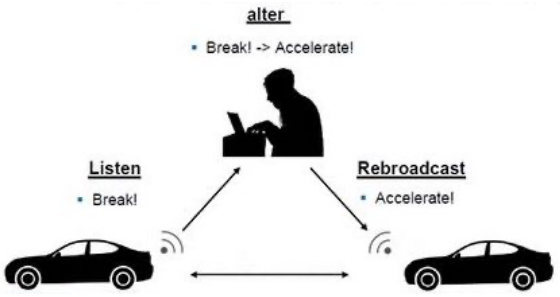

Figura 1 Exemplo da modificação de mensagens V2V.

B. Requisitos de segurança

A transmissão de mensagens *V2V* necessitam de ser protegidas contra ameaças de segurança tais como *message forgery, replay attacks, etc.* A passagem de informação maliciosa numa rede veicular pode resultar em consequências trágicas tais como a perda de vida humana ou a perda de propriedade. Por conseguinte definem-se requerimentos fundamentais de segurança na transmissão de mensagens *V2V*.

Autenticação: De modo a proteger o sistema de utilizadores maliciosos e falsa informação um recetor só pode aceitar mensagens de um transmissor fidedigno. Um transmissor autenticado é verificado através de certificados e pseudónimos.

Confidencialidade: Conjunto de regras que limitam utilizadores não autorizados no acesso a certos recursos e que protegem a informação do sistema. São usadas técnicas de encriptação baseados num mecanismo de gestão de chaves seguras.

Traçabilidade e Revocabilidade: A verdadeira identidade dos veículos deve permanecer anónima a terceiros, mas ao mesmo tempo rastreável para as autoridades competentes de modo a responsabilizar os seus titulares em casos de má conduta ou mau comportamento. Uma autoridade confiável mantém uma lista de revogação.

Eficiência: A carga computacional deve ser reduzida de modo a manter baixo *delay* e assegurar alta eficiência no sistema.

C. Requerimentos de privacidade

Enquanto os requisitos de segurança melhoram a segurança no processamento e troca de informação os requerimentos de privacidade melhoram a confiança entre o sistema e os seus intervenientes.

***Short-term linkability*:** Quando um recetor recebe dois ou mais pacotes de informação num curto período de tempo, este pode associar as duas mensagens com a fonte delas de modo a reduzir o risco de um *Sybil attack.*

***Long-term unlinkability*:** Mensagens transmitidas não podem ser associadas à identidade do seu transmissor preservando assim informação sensível como localização e direção assegurando assim a privacidade dos condutores.

***Forward unlikability*:** Mesmo após um veículo ser incluído a uma lista de revogação as suas futuras mensagens não poderão ser rastreáveis.

Anonimato: São preservados de terceiros a identidade e ações dos usuários. Regularmente é alcançável através do uso de pseudónimos.

Pseudónimo: Normalmente privacidade e anonimato são alcançáveis através do uso pseudo-identidades temporárias e chaves anónimas que permitem aos condutores acesso a diversos serviços sem risco de serem identificados.

***Accountability*:** Entidades não podem recusar transmissão de mensagens pois não existe qualquer tipo de reputação associada aos condutores.

Privacidade de Localização: Todo o tipo de informação relativa a localização e trajetória de veículos é protegida por entidades competentes.

D. Mecanismos de segurança

Os mecanismos de segurança dependem da política de segurança contra os ataques e ameaças às informações de cada empresa, neste caso como o tema é na comunicação entre veículos irão depender das políticas nessa mesma área.

Mecanismos de segurança são necessários para assegurar a autenticidade das mensagens recebidas, mas também para assegurar a fiabilidade de quem envia as mensagens. Estes mecanismos não podem interferir nem com a latência das mensagens nem mesmo afetar a performance das aplicações de segurança.

Certificados anónimos: As mensagens transmitidas são assinadas com certificados anónimos, os mesmos são publicados pela CA (Authority Certificate), preservando assim a identidade original de quem envia.

PKI – Public Key Infrastrutures: São um conjunto de papeis, políticas, hardware, software e de procedimentos necessários para criar, gerir, distribuir, utilizar e armazenar tal como revogar certificados digitais, mas também a gestão da encriptação da chave publica.

PPKI/VPKI - Pseudonym/Vehiculer Public key: É um esquema de arquitetura PKI, mas com uma autoridade de segurança adicional relativa à rastreabilidade. O mesmo sugere que cada veículo, possui um par de chaves públicas/privadas e certificados de curto prazo, incluindo alguns pseudónimos. Após algum tempo, os pseudónimos expiram e os veículos comunicam com o PCA (Pseudonym CA) para os renovar, resultando em despesas gerais de comunicação.

Group Signature Schemes: Os membros do grupo possuem várias chaves privadas, mas apenas partilham uma única chave publica. Quem recebe reconhece a assinatura do grupo, no entanto não sabe a identidade de quem envia.

Clustering cooperative approach: Os veículos são organizados em grupo e possuem um líder do grupo o mesmo é responsável de recolher e enviar pacotes de mensagens expondo assim a sua identidade e privacidade, mas mantem dessa forma as identidades do grupo.

Pseudo-Identity scheme: Os veículos estão equipados com um pseudónimo e uma chave secreta, emitidas pela TA (Trust Authority). Um recetor aceita as mensagens, após a verificação dos parâmetros públicos da TA. Os veículos apenas contactam a TA para renovar periodicamente os seus pseudónimos, a fim de evitar a rastreabilidade.

Digital signature scheme: Cada veículo é fornecido com um par de chaves criptográficas de longo prazo, um secreto e outro público. O CA emite um certificado de longo prazo para a chave pública. O Módulo de Segurança de Hardware de Veículos (HSM) é responsável por armazenar as chaves secretas, gerar assinaturas digitais e gerir as operações das chaves criptográficas. Os esquemas de assinatura digital utilizam a identificação do pseudónimo, a fim de proteger a identidade real dos veículos.

E. Protolos IEEE 802.11p

IEEE 802.11p foi criado com o propósito de adicionar acesso sem fios no meio automotivo (WAVE – Wireless Access for Vehicular Environments program).

O mesmo define melhorias necessárias para oferecer suporte às aplicações de transporte inteligentes (ITS – Intelligent Transportation System) e corre numa banda de frequência de 5.9GHz.

O protocolo foi finalizado em 2012 e sustenta as DSRC (Dedicated Short-Range Communications) comunicações de curto alcance nos Estados Unidos tal como a iniciativa ITS-G5 do sistema de transportes inteligentes cooperativos Europeus (C-ITS - European Cooperative Intelligent Transport Systems).

A comunicação V2X através do protocolo 802.11p vai mais além dos sensores limitados por linha de visão como camaras, radares o mesmo cobre casos de uso de V2V tal como V2I, por exemplo avisos de alerta de colisão, alertas de limite de velocidades, estacionamento eletrónico e pagamentos de portagens.

Vantagens do Protocolo IEEE 802.11p:

- Curto alcance (menos de 1km)
- Baixa latência (~2ms)
- Elevada fiabilidade
- Imune a condições meteorológicas extremas (por exemplo, chuva, nevoeiro, neve, etc.)
- IEEE 802.11p não está dependente da presença de cobertura de rede celular.

F. CAM e DENM

Apesar da grande variedade de aplicações V2V e casos de uso, apenas existem dois tipos de mensagem definidos para transmitir as informações da aplicação.

CAMs (Cooperative Awareness Message) são mensagens transmitidas periodicamente por cada veículo para outro veículo vizinho de modo a fornecer informações de presença, posição, temperatura e estado do carro.

CAMs são geradas num intervalo de pelo menos 100ms a 1000ms no máximo. O tamanho de uma mensagem CAM pode ser no intervalo de 30 a 300 bytes.

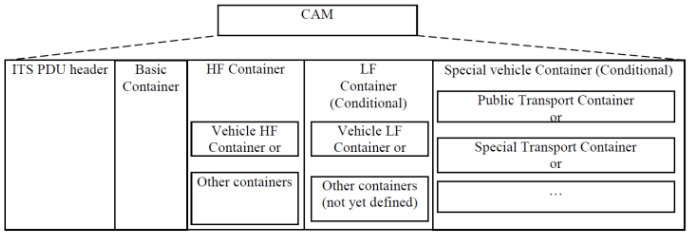

Figura 2 Formato de uma Mensagem CAM

DENMs (Decentralized Environmental Notification Message), são mensagens que são acionadas por eventos, servem para alertar neste caso o condutor de um evento perigoso, situações estranhas no trafico ou até objetos detetados pelos sensores nas estradas. Ao contrário das mensagens CAM, as DENM não são mensagens periódicas.

O tamanho de uma mensagem DENM é variável e pode ser entre 60 e 800 bytes.

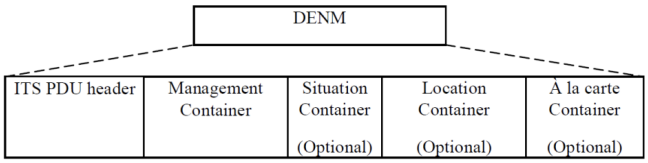

Figura 3 Formato de uma mensagem DENM

Ambas as mensagens são entregues a veículos numa determinada região geográfica, são enviadas para o "vizinho" mais próximo no caso das CAMs, no caso das DENMs são enviadas aos vizinhos da área afetada pelo evento.
CAM e DENM constituem o conjunto básico de mensagens que servem para auxiliar o funcionamento de aplicações ITS (Intelligent Transportation Systems).

G. Protocolo celular V2X ou simplesmente C-V2X

O protocolo C-V2X é visto como principal alternativa ao protocolo IEE 802.11p. Este protocolo oferece pouca latência nas comunicações *vehicle-vehicle(V2V)*, *vehicle-to-infracstructure(V2I)* e *vehicle-to-pedestrian(V2P)*. Através da conexão de veículos individuais e do desenvolvimento de sistemas de transporte cooperativos inteligentes que reduziriam muito o os níveis de poluição e congestionamento. Este protocolo tem o potencial de transformar informação e serviços de segurança tanto em autoestradas como em grandes cidades melhorando muito a deslocação. O protocolo C-V2X usa dois modos de transmissão complementares. Primeiramente opera sobre comunicações diretas *V2V, V2I* e *V2P* de baixa latência através da banda 5.9GHz com o propósito de ativar a troca de mensagens de segurança em situações de perigo iminente. O segundo modo é de comunicação pela rede onde o protocolo V2X usa uma rede móvel convencional para permitir ao veículo a receção de informação convencional como por exemplo o estado do tráfego na sua região.

H. Beneficios do C-V2X

- Integração de sistemas através da rede LTE é custo-efetivo.
- Comunicação direta sobre distâncias maiores.
- Performance aumentada para identificação de obstáculos fora da linha-de-visão do condutor.
- Maior capacidade para receção e transmissão de informação.

- Capacidade superior no controlo de congestão em situações de tráfego intenso.
- Maior confiança na troca de mensagens de segurança.

I. Comparação C-V2X / IEE 802.11p

A principal vantagem do protocolo IEE 802.11p consiste no facto de ter sido desenvolvido e entregue mais cedo pelo que é o protocolo mais usado no presente. Por outro lado, o protocolo C-V2X oferece inequivocamente melhor performance e a habilidade de poder se comunicar diretamente ou através de rede móvel, abrindo um caminho revolucionário para o 5G. Existe uma forte possibilidade de ambos os protocolos se fundirem no futuro, combinando os pontos mais fortes de ambas tecnologias.

V2X Standard	Wi-Fi based IEEE 802.11p	Celular based C-V2X	
Lançamento	2012	2016	2018
Comentários	Desenhado para V2X	V2X em cima de LTE/4G	V2X em cima de 5G
Aplicações Suportadas	Comunicação direta: V2V, V2I.	• Comunicação direta: V2V, V2I • Comunicação indireta: V2N	
Funções	Modo "Out-of-coverage" (Direto V2V)	Modo Out-of coverage (Direto V2V) Modo In-coverage (Conectado à internet)	
Taxa de transferência/Interferência	~6Mbps (10MHz largura de banda) / Nível alto.	~50Mbps (10MHz largura de banda) / Baixo Nível.	~10Gbps V2N e > 100 Mbps V2V / Baixo Nível
Maturidade	+ + +	+ +	+
Conectividade	+	+ + +	+ + + + +
Range	+ +	+ + + +	+ + + +
Fiabilidade	+ +	+ + +	+ + + +
Latência	+ + +	+ + +	+
Compatibilidade	+ +	+ + + +	+ + + + +
Interesse no "Mercado"	+ +	+ + + +	+ + + +

Figura 4 Comparação dos protocolos

J. Use cases:

Platooning - é um método para conduzir um grupo de veículos juntos, para aumentar a capacidade das estradas. Este método diminui a distância entre carros ou camiões usando as mensagens v2v. Platooning resulta numa diminuição do consumo de combustível uma vez que os carros e os camiões deslocam-se numa velocidade constante, travando e acelerando menos. Em específico, as comunicações entre camiões utilizando V2X aumentam a segurança e reduzem os custos de deslocamento. Isto acontece, pois, desta forma, os camiões podem ser conduzidos em conjunto, necessitando apenas de maior atenção do condutor da frente que vai a guiar, permitindo que os outros condutores descansem de longas horas de viagem. Para além disto, os camiões criam uma formação aerodinâmica que poupa até 12% dos gastos de combustível.

Emergency electronic brake light e forward collision warning – o veículo comunica, aos veículos no seu alcance, a paragem de emergência, permitindo assim, aos veículos que recebem a mensagem, determinar a relevância do evento e se é apropriado comunicar um aviso ao condutor com a finalidade de evitar um acidente. Esta aplicação é particularmente útil quando o campo de visão do condutor está obstruído por outros veículos ou devido às más condições climatéricas, pois permite aos condutores ver virtualmente os ângulos mortos.

Intersections movement assist application - avisa os condutores quando não é seguro entrar numa interseção, avisando por exemplo, quando um outro veículo passou num vermelho ou está a fazer uma curva inesperada.

Do not pass application – permite aos condutores saber quando não é seguro ultrapassar um veículo lento, avisando, por exemplo se vem um veículo em direção contraria, ou se, no caso de um camião, não der para ver que, na verdade, o transito está lento.

III. Conclusão

Em suma, podemos verificar que as implementações do protocolo C-V2X têm o potencial para mudar o paradigma na condução automóvel. Com todos os veículos interconectados poderemos evitar muitas situações adversas ou mesmo potencialmente fatais. Colisões, engarrafamentos, acidentes causados por mudança de faixa poderão ser evitados ou no mínimo ocorrer com uma frequência consideravelmente menor. Esta tecnologia pode perfeitamente tornar-se no fator chave para a afirmação definitiva da condução autónoma no mercado automóvel. Infelizmente, com o surgimento de uma nova tecnologia ocorre também o surgimento de potenciais vulnerabilidades. *Replay attacks, spoof atacks* e mais, colocarão em risco a integridade dos condutores, pelo que será sempre um desafio assegurar que esta tecnologia seja segura para os seus usuários. A total afirmação desta tecnologia ainda levará alguns anos e até lá o protocolo IEE 802.11p continuará a ser vastamente requisitado.

References

[1] View of Recent Developments on Security and Privacy of V2V & V2I Communications: A Literature Review. (n.d.). PERIODICA POLYTECHNICA TRANSPORTATION ENGINEERING. Retrieved October 22, 2022, from https://pp.bme.hu/tr/article/view/14955/8724

[2] Science Direct. Retrieved October 22, 2022, from https://www.sciencedirect.com/science/article/pii/S25900056210003

[3] Cybersecurity challenges in vehicular communications. Retrieved October 22, 2022, from https://www.sciencedirect.com/science/article/pii/S221420961930261X

[4] Vehicle-to-vehicle communication. Retrieved October 22, 2022, from https://www.nhtsa.gov/technology-innovation/vehicle-vehicle-communication

[5] Vehicle-to-vehicle (V2V) communication. Retrieved October 22, 2022, from https://www.avnet.com/wps/portal/abacus/solutions/markets/automotive-and-transportation/automotive/communications-and-connectivity/v2v-communication/