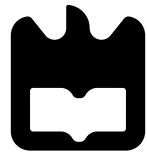


Redes e Sistemas Autónomos
Apontamentos
Parte III

Universidade de Aveiro

Sebastian D. González



Redes e Sistemas Autónomos Apontamentos Parte III

Dept. de Eletrónica, Telecomunicações e Informática
Universidade de Aveiro

sebastian.duque@ua.pt(103690)

25 de junho de 2024

Warning!!

Isto são apenas uns apontamentos realizados por uma pobre alma de MIECT, feitas a partir dos slides da disciplina e outras fontes . Por favor, não usem apenas estes apontamentos como material de estudo.

Dito isto, boa sorte a todos e ámen CT .

Agradecimentos à Prof. Susana Sargento susana@ua.pt por todo o material fornecido nas aulas.

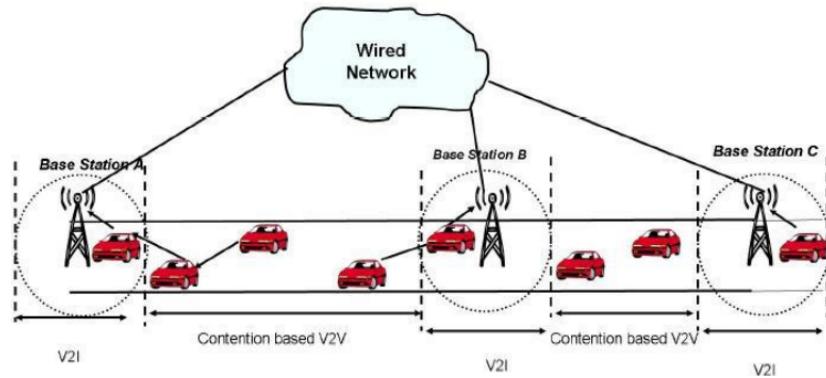
Conteúdo

1	Vehicular Networks	1
1.1	Awareness and Warning Information	1
1.1.1	CAM: Cooperative Awareness Messages:	1
1.1.2	DENM: Decentralized Environmental Notification Messages	2
1.1.3	VAM: Vulnerable Road User Awareness Message	2
1.1.4	CPM: Cooperative Perception Message	3
1.1.5	SPAT: Signal Phase And Timing	4
1.1.6	MAP	5
1.1.7	MCM: Manoeuvre Coordination Message	6
1.1.7.1	Cenário de uso	7
1.1.7.2	MCM Messages	7
1.1.7.3	Maneuver Cooperation Service	8
1.2	Communication Technologies	8
1.2.1	ITS-G5 (DSRC, IEEE 802.11p)	8
1.2.1.1	Challenges	9
1.2.2	Cellular-V2X (LTE-based 3GPP Rel 14)	9
1.2.3	ITS-G5 vs C-V2X	11
2	QoS and Security	12
2.1	Problem: Evaluate TCP	12
2.2	TCP Cubic	12
2.3	QUIC: Quick UDP Internet Connections	13
2.4	TCP Vegas	13
2.5	TCP-BuS	14
2.6	QoS in UDP: trade-offs	14
2.7	QoS Routing	15
2.8	QoS for AODV	15
2.9	Transmission Quality (Batman v.3)	16
2.10	QoS-OLSR	17
2.11	Security	17
2.11.1	Possible routing attacks	17
2.11.1.1	Attacks using modification	18
2.11.1.2	Attacks using impersonation	18

2.11.1.3	Attacks using fabrication	19
2.12	Key Management - basics	20
2.12.1	Symmetric cipher	20
2.12.2	Asymmetric cipher	21
2.13	Key Management in ad-hoc networks	21
2.13.1	SOPKM: Self-organized public key management	22
2.13.1.1	Update repositories of certificate graphs	22
2.13.1.2	Global Connectivity Graph	22
2.13.1.3	Certificate Update and Revocation	23
2.13.1.4	Malicious Users	23
2.13.2	SSAWN: Self-securing ad-hoc wireless networks	24
2.13.2.1	Basic Operation	24
2.13.2.2	Shared secrets	24
2.14	Reputation	25
2.14.1	Reputation into the normal operation of the network	25
3	MEC: Mobile Edge Computing	27
3.1	Edge and Cloud	27
3.2	Examples using Edge Computing	28
3.3	MEC future	28
3.4	What about 6G?	29

Vehicular Networks

As redes veiculares podem proporcionar maior segurança, eficiência, informações detalhadas sobre o tráfego e as condições das vias, alertas de sinalização e dados sobre informações locais. As redes veiculares, que incluem a **comunicação veículo-a-veículo (V2V)** e **veículo-a-infraestrutura (V2I)** e possibilitam a comunicação, routing e execução de aplicações através de unidades embarcadas nos veículos, enquanto as unidades de **Road-side infrastructure units (RSUs)**, chamadas de nós de rede, serão equipadas com módulos de processamento e comunicação sem fio.



1.1 Awareness and Warning Information

1.1.1 CAM: Cooperative Awareness Messages:

São mensagens enviadas periodicamente que contêm informações sobre a estação, como posição e velocidade. Estas são essenciais para criar e manter a consciência sobre veículos na rede rodoviária e das RSUs. O conteúdo das CAMs varia conforme o tipo de sistema ITS-S(Intelligent Transport System Station):

- **Veículos:** As CAMs incluem informações sobre o tempo, posição, estado de movimento, sistemas ativados (como controlo de cruzeiro, pedais, entre

outros), além de atributos como dimensões, tipo de veículo e seu papel no trânsito.

- **RSUs:** Informam sobre o tipo de estação e localização.

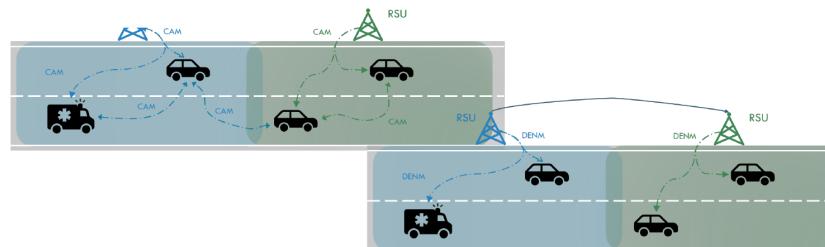
Contém dois tipos de dados:

- **Container de Alta Frequência (HF):** Dados que mudam rapidamente, como localização, direção ou velocidade do veículo. Devem estar presente em todas as mensagens CAM
- **Container de Baixa Frequência (LF):** Dados estáticos ou que mudam lentamente, como status das luzes externas ou dos pedais. Podem ser atualizadas com uma frequência máxima de 5 Hz

A geração de CAMs deve ocorrer com frequência entre 1 Hz e 10 Hz. O processo de geração deve ser eficiente, com uma diferença de tempo entre a geração da CAM e sua entrega à camada de transporte de rede inferior a 50 ms.

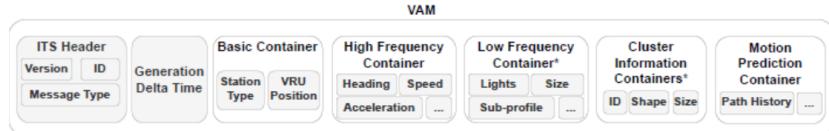
1.1.2 DENM: Decentralized Environmental Notification Messages

São mensagens **assíncronas** que incluem detalhes sobre eventos e a estação que gerou a mensagem. São utilizadas para informar sobre eventos rodoviários, como perigos ou condições de trânsito anormais. Elas são geradas apenas quando um evento ocorre e contêm informações sobre tipo, localização e validade do evento. As DENMs não são periódicas e têm um período de validade. Quando o evento termina, uma DENM de término é enviada para indicar o fim do evento.

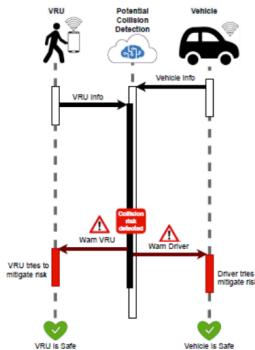


1.1.3 VAM: Vulnerable Road User Awareness Message

São mensagens trocadas periodicamente na rede ITS entre estações para manter consciência sobre **VRUs(Vulnerable Road User)**. Fornecem informações detalhadas como tempo, posição, velocidade, direção, entre outros, específicos para cada tipo de VRU tais como pedestres 🚶, ciclistas 🚲, motociclistas 🚩 e animais 🐾.



A flexibilidade das VAMs permite especificar com precisão o tipo exato e a situação de cada VRU, algo que não seria possível com as mensagens padrão CAM. Isso é crucial para ajustar algoritmos de previsão de acidentes, levando em conta as diferentes dinâmicas de movimento e necessidades de segurança de cada tipo de utilizador vulnerável.



1.1.4 CPM: Cooperative Perception Message

São mensagens **periódicas** trocadas entre estações para transmitir informações sobre o ambiente atual percebido por um ou mais sensores.

⇒ **Uso:** Sensores de veículos, utilizadores Vulneráveis da Estrada (VRUs) e infraestrutura utilizam CPMs para trocar informações coletadas do seu entorno, melhorando assim a consciência situacional.

Sensor Information Container:

- Contém informações sobre o tipo de sensor usado (por exemplo, Radar, Lidar, câmeras de vídeo) ou algoritmos de fusão e especifica a área ou alcance que o sensor cobre.

Perceived Object Container:

- Inclui detalhes sobre objetos percebidos pelo sensor fornecendo classificações dos objetos percebidos. Indica os níveis de confiança nessas classificações e inclui dados dinâmicos como distância, velocidade, aceleração e ângulo relacionados aos objetos percebidos.

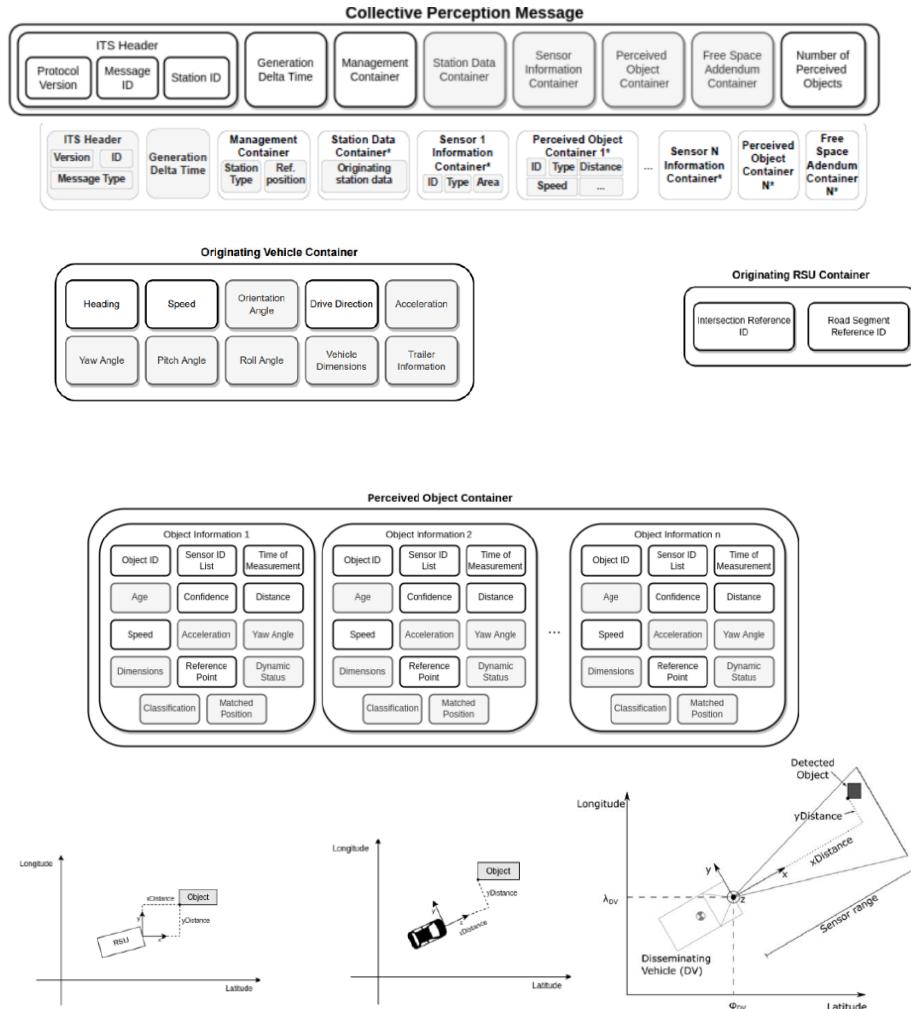


Figura 1.1: Objects information in CPMs

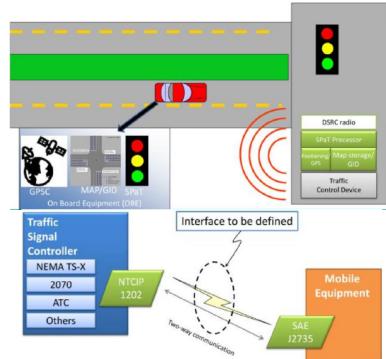
1.1.5 SPAT: Signal Phase And Timing

Permite a comunicação bidirecional entre **controladores de sinais de trânsito e dispositivos móveis** fornecendo o estado atual do movimento de cada fase ativa, essencial para:

- Aplicações de segurança, como alertas para evitar acidentes e violações de sinal vermelho.
- Aplicações de mobilidade para uma gestão dinâmica e eficiente do trâfico.

- Aplicações ambientais que visam a economia de combustível e redução de emissões de CO₂.

Além disso, inclui informações detalhadas sobre o estado de todas as faixas na interseção, incluindo quaisquer active preemption ou prioridades ativas.



Possui dois estados:

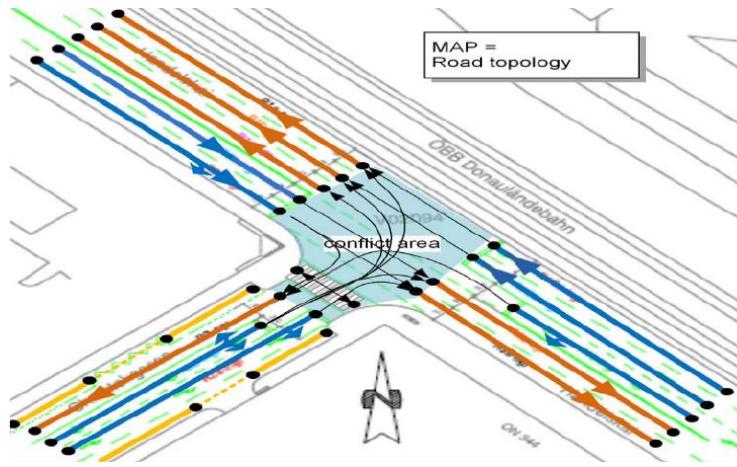
- **Intersection state**
- **Movement State:**
 - Conjunto de faixas (por exemplo, faixas 9-10 estão para o estado de movimento 1).
 - Estado atual (verde, amarelo, vermelho).
 - Tempo restante até a mudança do estado atual do sinal.
- Usado em cooperação com um MAP [1.1.6](#).

1.1.6 MAP

O MAP fornece uma representação detalhada da interseção, essencial para sistemas de transporte e aplicações de segurança e gestão de tráfico, utilizando informações precisas da infraestrutura para melhorar a eficiência e segurança nas vias.

Dados da mensagem:

- Ponto de referência (centro da interseção).
- Número de acessos.
- Número da faixa.
- Largura da faixa.
- Atributos das faixas, como direção (reta, esquerda, direita, virar com sinal vermelho), limite de velocidade, uso para autocarro, entre outros.
- Deslocamentos (offsets): Pontos ao longo de cada faixa, usados para detetar a posição dos veículos.



1.1.7 MCM: Manoeuvre Coordination Message

É uma mensagem que inclui informações sobre manobras planeadas e trajetórias desejadas ou alternativas para veículos.

- **Conteúdo do MCM:**

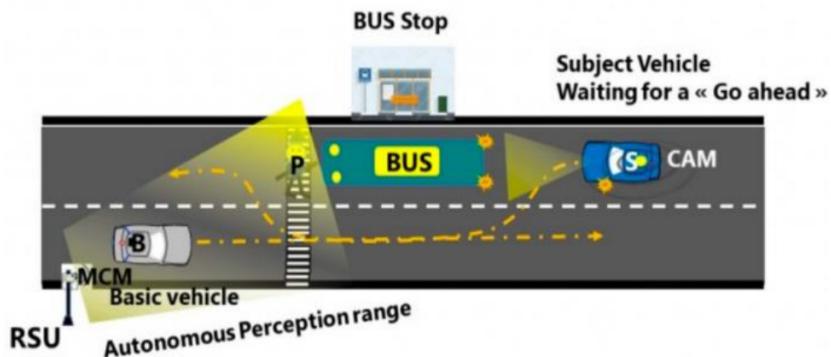
- **Manobras planeadas:** Descreve as manobras que um veículo pretende executar, como, por exemplo, ultrapassar um autocarro parado.
- **Trajetórias Desejadas:** São descrições detalhadas das trajetórias esperadas para os próximos 5 a 10 segundos, incluindo informações espaciais e temporais.

- **Objetivos e Uso:**

- As trajetórias planeadas são usadas por aplicações para prever a posição futura de veículos próximos e identificar possíveis conflitos.
- As trajetórias desejadas são usadas para solicitar coordenação entre veículos que têm como objetivo melhorar a eficiência e segurança do tráfego.
- **Frequência de Geração:** Espera-se que as MCMs sejam geradas continuamente, com frequência variando entre 1 Hz e 10 Hz, dependendo da necessidade de detetar precocemente a necessidade de coordenação de manobras.
- **Aplicações Específicas:** Unidades de beira de estrada também podem transmitir MCMs, geralmente em tamanho menor e com menos frequência do que os veículos. Estas mensagens podem incluir conselhos específicos para veículos, como sugestões de velocidade ou mudança de faixa, para resolver situações de tráfego de forma eficaz e segura.

1.1.7.1 Cenário de uso

No caso em que o veículo S pretende ultrapassar o autocarro parado, qualquer utilizador da estrada pode analisar a situação do tráfego com base nas informações recebidas e nos dados dos sensores. Podem aconselhar o veículo S sobre a melhor forma de realizar a ultrapassagem de forma segura, considerando a visibilidade, o tráfego circundante e as regras de trânsito locais. Esta abordagem garante uma resolução eficiente e segura da situação, promovendo uma coordenação harmoniosa entre os utilizadores da estrada.



1.1.7.2 MCM Messages

MCM Type: Tipo de Manobra (oferta, solicitação..)

MCM Concept & Rational: Custo de cooperação ou objetivo prescritivo da manobra.

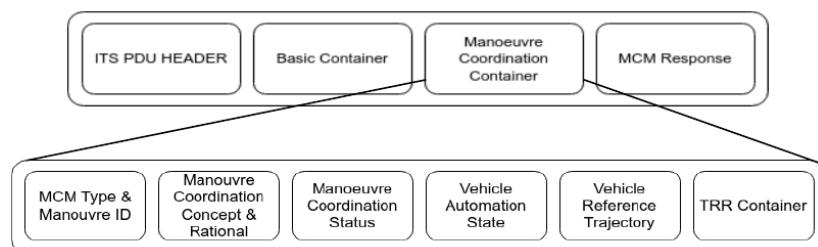
MCM Coordination Status: Elemento de dados que indica o status atual da execução.

Vehicle Automation State: Longitudinal e/ou Lateral

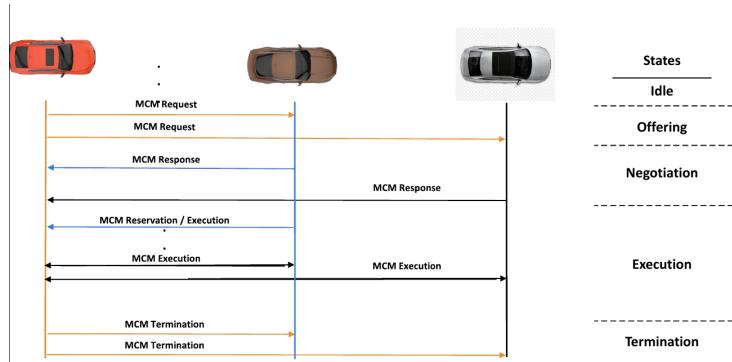
Vehicle Reference Trajectory: Contém a trajetória que os veículos pretendem executar

TRR Container: Trajetória de Referência do Veículo para reserva de recursos de estrada

Structure



1.1.7.3 Maneuver Cooperation Service



1.2 Communication Technologies

Requisitos de Tecnologia de Comunicação:

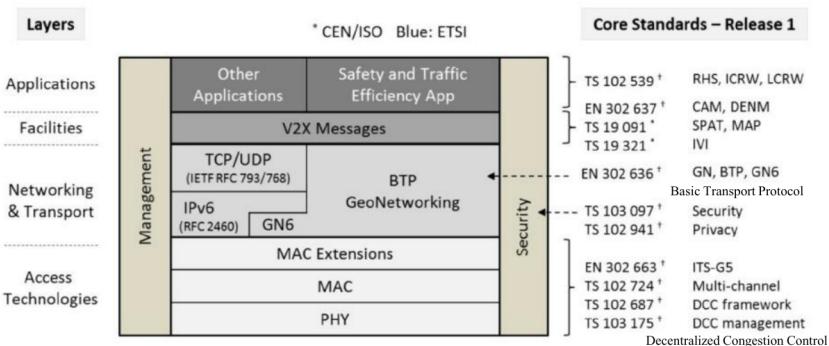
- Precisam ter um alcance de mais de 200 a 400 metros para cobrir áreas urbanas e rodoviárias.
- Devem manter atrasos de transmissão abaixo de 10 milissegundos para respostas rápidas.
- O tempo de comunicação dentro desse alcance deve ser entre 10 a 20 milissegundos para eficiência em tempo real.
- A largura de banda deve ser superior a 10 Mb por segundo, idealmente maximizada para suportar transferências rápidas de grandes volumes de dados, essencial para aplicações avançadas de tecnologia de transporte.

1.2.1 ITS-G5 (DSRC, IEEE 802.11p)

O ITS-G5 (DSRC, IEEE 802.11p) é uma tecnologia desenvolvida para comunicação entre veículos (V2V) que também suporta comunicação veículo-infraestrutura (V2I). É baseada no padrão IEEE 802.11a com extensões PHY e MAC, utilizando **CSMA/CA** (Carrier Sense Multiple Access/Collision Avoidance) para acesso ao meio e adaptado para comunicações críticas de latência (V2X) na faixa dos 5,9 GHz.

- **Frequência de operação:** Utiliza uma banda de 75 MHz no espectro de **5,9 GHz**.
- **Alcance:** Em linha de visão (LoS), pode alcançar até **1 km**, embora seja suscetível a obstruções como edifícios, árvores e veículos.

- **Atraso:** Menos de **10 milissegundos**, adequado para aplicações sensíveis à latência.
- **Tempo de comunicação quando dentro do alcance:** Entre **10 a 20 milissegundos**, garantindo resposta rápida.
- **Taxa de dados:** Pode alcançar até **27 Mb por segundo** no modo mais rápido, com uma taxa usual de **12 Mb por segundo** para comunicações típicas.



1.2.1.1 Challenges

Os desafios enfrentados pelo ITS-G5 incluem a transmissão periódica das mensagens básicas de segurança (BSM), que contêm informações cruciais como posições e velocidades dos veículos, com um tamanho típico de cerca de 300 bytes, incluindo certificação de segurança. Estas mensagens são transmitidas a cada 100 milissegundos para atender aos requisitos de latência e precisão. No entanto, em ambientes densos de tráfego, há o risco de congestionamento de canal, levando a colisões de pacotes e comprometendo a confiabilidade da comunicação. Além disso, a falta de um handshake ou confirmação (ACK) para frames de broadcast e a ausência de suporte a QoS são desafios adicionais. Para enfrentar essas limitações, está a ser desenvolvida a próxima geração do padrão IEEE 802.11bd, com o objetivo de melhorar a eficiência e a robustez das comunicações em sistemas ITS-G5.

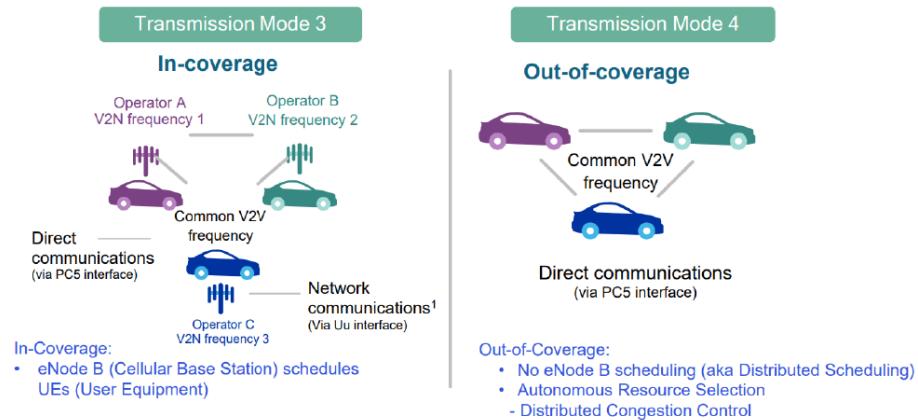
1.2.2 Cellular-V2X (LTE-based 3GPP Rel 14)

O C-V2X (Cellular Vehicle-to-Everything), baseado na especificação 3GPP Release 14, apresenta duas modalidades de transmissão complementares:

- **Comunicação Direta (PC5):** Esta modalidade é independente da rede celular e opera em bandas específicas para ITS (por exemplo, **5,9 GHz**). É destinada à comunicação de baixa latência entre veículos (V2V), veículos

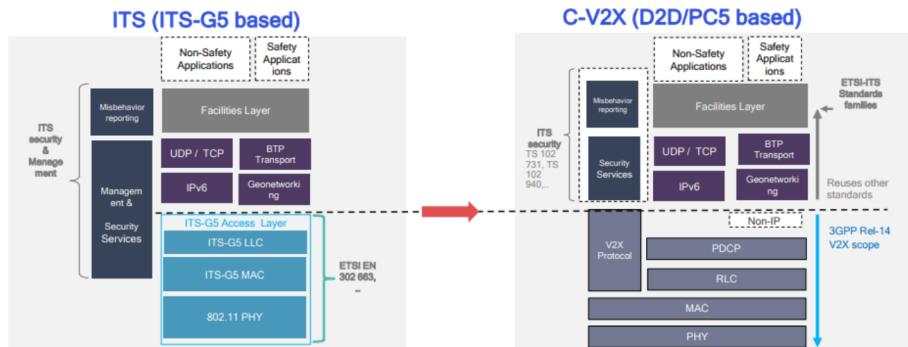
e infraestrutura (V2I) e veículos e pessoas (V2P). Permite comunicações próximas (centenas de metros), é operacional dentro e fora da cobertura, ideal para casos de uso sensíveis à latência, como segurança V2V.

- **Comunicações de Rede (Uu):** Utiliza a interface LTE para transmitir mensagens de um servidor V2X para veículos e vice-versa. Esta modalidade opera nas redes licenciadas dos operadores móveis, suportando comunicações em larga escala e casos de uso menos críticos em termos de latência, como consciência situacional V2N.



Connected Vehicle Challenges	C-V2X Solutions
<p>High relative speeds Leads to significant Doppler shift / frequency offset</p>	Improved signal design E.g. increasing # of ref signal symbols to improve synchronization and channel estimation
<p>High node densities Random resource allocation results in excessive resource collisions</p>	Improved transmission structure Transmit control and data on the same sub-frame to reduce in-band emissions More efficient resource allocation New methods using sensing and semi-persistent resource selection
<p>Time synchronization Lack of synchronization source when out-of-coverage</p>	Allow utilization of GPS timing Enhancements to use satellite (e.g., GNSS) when out-of-coverage

1.2.3 ITS-G5 vs C-V2X



Parameters	ITS-G5	C-V2X (LTE Rel. 14)	Future 5G SA
Currently available technology	Yes	Yes	No Yes, private networks
Field trials (+10 years)	Yes	No	No
Applications	V2V, V2I	V2V, V2I, V2N	V2V, V2I, V2N
Latency	5 ms	20 ms	<5 ms
Data rate	3-27 Mbps	150 Mbps	10 Gbps
Multimedia and cloud services support	No	Yes	Yes

Figura 1.2: ITS-G5, C-V2X, 5G (Standalone)

QoS and Security

2.1 Problem: Evaluate TCP

O TCP, desenvolvido originalmente para redes cabladas, apresenta desempenho insatisfatório em redes ad-hoc ou veiculares. Isto ocorre devido a características específicas destes ambientes, como a alta mobilidade dos nós e requisitos estritos de latência. O TCP assume que todas as perdas de pacotes são causadas por congestionamento da rede, o que não é verdade em redes sem fio. Nesses cenários, falhas de rota e erros de canal são interpretados erroneamente como congestionamento, levando a reduções indevidas na taxa de envio, perdas de pacotes em nós intermediários, timeouts repetidos e retransmissões desnecessárias. Isto causa quedas significativas no desempenho da comunicação. Portanto, é necessário avaliar variantes do TCP ou considerar protocolos alternativos mais adequados para redes ad-hoc e veiculares, que levem em conta suas características específicas, como mobilidade, alta taxa de erros e imprevisibilidade na latência e largura de banda.

2.2 TCP Cubic

O TCP CUBIC é um algoritmo de controlo de congestionamento que usa uma **função cúbica** em vez de uma função linear para aumentar a janela de congestionamento, a fim de melhorar a escalabilidade e a estabilidade em redes rápidas e de longa distância. Sendo independente do tempo de ida e volta (RTT) e baseada no tempo decorrido desde o último evento de congestionamento.

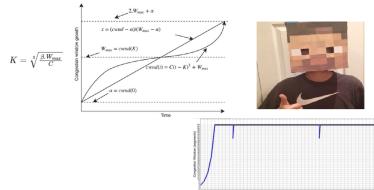


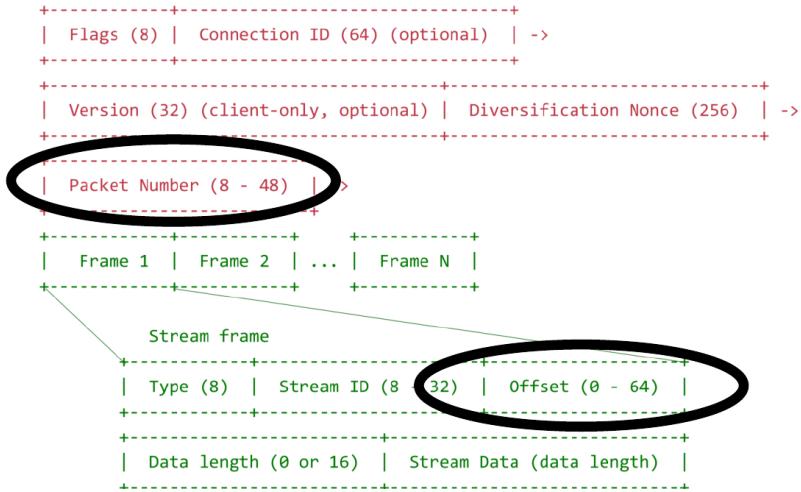
Figura 2.1: TCP CUBIC

2.3 QUIC: Quick UDP Internet Connections

O QUIC oferece várias vantagens, como a separação da confiabilidade e da entrega ordenada de pacotes, o que evita bloqueios na transmissão. Os pacotes QUIC são transportados em datagramas UDP para facilitar melhor a implantação em sistemas e redes existentes. O handshake QUIC combina a negociação de parâmetros criptográficos (TLS) e de transporte, e é estruturado para permitir a troca de dados de aplicação o mais rápido possível.

Também proporciona uma estimativa precisa do tempo de ida e volta (RTT), independente de retransmissões, e utiliza algoritmos de controlo de congestionamento que não dependem do RTT como o CUBIC, o que é crucial em ambientes sem fio.

Além disso, o QUIC possui um controlo de fluxo eficiente, evitando que um único fluxo monopolize os recursos e permite a retransmissão rápida de pacotes não confirmados, reduzindo assim o impacto das perdas. Essas características tornam o QUIC uma solução eficaz para manter a comunicação confiável e com bom desempenho em redes de drones.



O QUIC estima o RTT usando o tempo entre a transmissão de um pacote e o recebimento de seu ACK, com números de pacotes monotonicamente crescentes e independentes da ordem de entrega, e aplica um algoritmo de controlo de congestionamento, como o CUBIC.

2.4 TCP Vegas

Deteta o congestionamento na rede antes que qualquer perda de pacote ocorra e, então, reduz instantaneamente o tamanho da janela de congestionamento.

Regula a taxa de envio com base na diferença entre a taxa esperada (janela de congestionamento dividida pela RTT base) e a taxa real (janela de congestionamento dividida pela RTT atual). O TCP Vegas é mais sensível ao RTT e às perdas de pacotes.

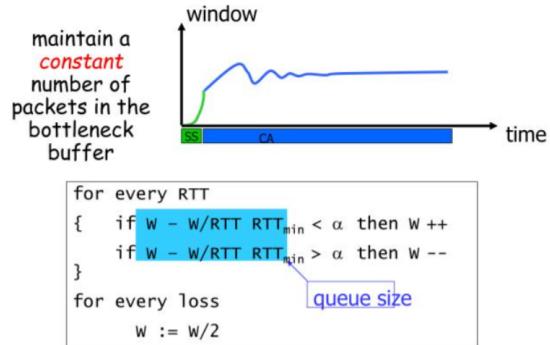


Figura 2.2: TCP/Vegas CA algorithm [1]

2.5 TCP-BuS

O TCP-BuS explora a capacidade de buffering e a informação de sequência para detetar falhas de rota, enviando notificações explícitas e permitindo que os nós intermediários armazenem pacotes pendentes e o remetente ajuste o tempo de retransmissão, evitando timeouts e retransmissões desnecessárias, desde que os protocolos de routing e os nós intermediários sejam compatíveis.

2.6 QoS in UDP: trade-offs

Na implementação de Qualidade de Serviço (QoS) em redes sem fio multi-hop usando UDP, enfrenta-se desafios significativos com os modelos IntServ e DiffServ.

Os mecanismos **IntServ**, que reservam recursos específicos ao longo do caminho para atender requisitos de QoS, são dificultados pela dificuldade em estimar recursos disponíveis num meio partilhado e pela necessidade de coordenação global para evitar violações de reserva devido à dinâmica da largura de banda e mudanças frequentes de rota.

Por outro lado, os mecanismos **DiffServ**, que classificam tráfego em categorias de serviço com garantias de QoS pré-definidas, enfrentam desafios com o controlo de admissão de fluxos e a manutenção de garantias de QoS devido à variação na distribuição de fluxos e flutuações na largura de banda em redes dinâmicas. Em ambos os casos, adaptar esses modelos para redes sem fio multi-hop requer abordagens que possam lidar melhor com a natureza volátil e dinâmica dessas redes.

2.7 QoS Routing

O encaminhamento com QoS é fundamental para informar a origem sobre a disponibilidade de largura de banda e qualidade de serviço (QoS) até o destino. No entanto, integrar requisitos de QoS nas métricas de encaminhamento enfrenta desafios como complexidade de manutenção, sobrecarga adicional na rede e incerteza na garantia contínua de recursos reservados, especialmente considerando a mobilidade dos nós. Para ser eficaz, um sistema deve ser capaz de ajustar rotas e reservas dinamicamente para responder à mobilidade dos nós e às mudanças nas condições da rede.

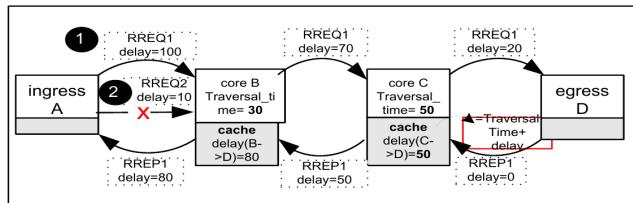
2.8 QoS for AODV

Para implementar QoS no protocolo AODV (Ad Hoc On-Demand Distance Vector), são necessárias extensões nos campos das mensagens de rota (RREQ, RREP) para incorporar requisitos de serviço. Quando um nó recebe um RREQ com a extensão de QoS, ele só deve retransmitir o RREQ se puder atender aos requisitos de serviço especificados (se não estiver em cache). Isso requer mudanças nos campos das tabelas de routing do AODV, que atualmente incluem número de sequência de destino, interface, contagem de saltos, próximo salto e lista de predecessores.

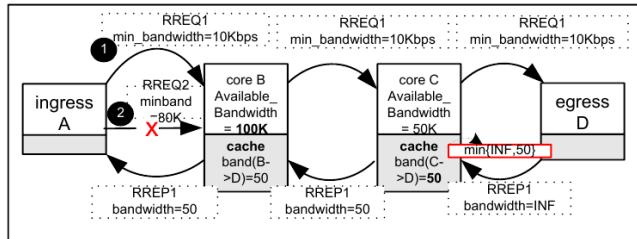
Os quatro novos campos necessários para suportar QoS no AODV incluem:

- **Atraso máximo:** Especifica o limite máximo de atraso aceitável.
- **Largura de banda mínima disponível:** Indica a quantidade mínima de largura de banda necessária.
- **Lista de fontes que solicitam garantias de atraso:** Identifica quais fontes estão a solicitar garantias de atraso.
- **Lista de fontes que solicitam garantias de largura de banda:** Indica quais fontes estão a solicitar garantias de largura de banda.

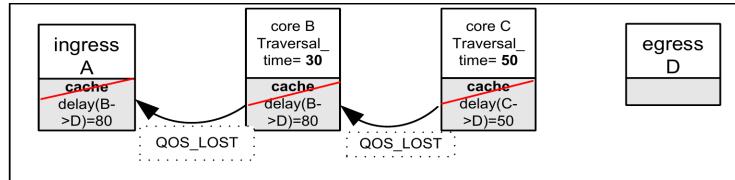
Durante o processo de **descoberta de rota**, o AODV utilizará a extensão de atraso máximo e as listas de fontes que solicitam garantias de atraso para gerir e selecionar rotas que atendam aos requisitos de QoS específicos, garantindo assim que as ligações estabelecidas possam suportar atrasos dentro dos limites aceitáveis.



Em termos de **largura de banda** no protocolo AODV, é necessário estender as mensagens de roting (RREQ, RREP) para incluir requisitos específicos de largura de banda. Isto envolve usar os novos campos de **Largura de banda mínima disponível** e **Lista de fontes que solicitam garantias de largura de banda**. Durante a descoberta de rota, o AODV utiliza essas extensões para selecionar rotas que possam atender aos requisitos de largura de banda necessários para os fluxos de dados, garantindo assim uma QoS adequada para aplicações que dependem de transmissões de alta taxa de dados.

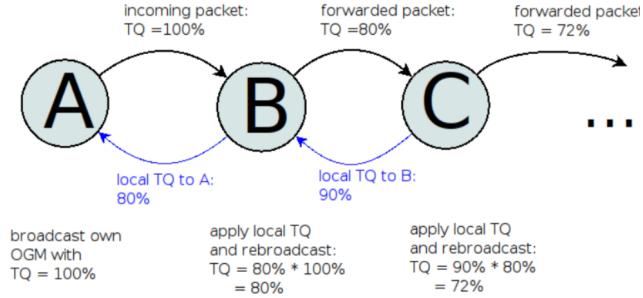


Finalmente, para assegurar **QoS** no AODV, é crucial a monitorização contínua dos parâmetros de QoS durante o processo. Se um nó não puder mais manter os requisitos acordados, ele envia uma mensagem **ICMP QoS_LOST** aos nós dependentes, usando uma lista das fontes que solicitaram garantias de atraso/largura de banda. Isso pode ocorrer devido ao aumento da carga de um nó, quando ele assume mais tarefas do que pode gerir, comprometendo assim a QoS.



2.9 Transmission Quality (Batman v.3)

Na versão 3 do protocolo Batman, a Qualidade de Transmissão (TQ) incorpora a qualidade local da ligação no cálculo. Quando um nó recebe um pacote, calcula o TQ multiplicando o valor de TQ recebido pelo valor local **TQ_local**. Por exemplo, se o Node A envia um pacote com TQ máximo, o Node B que o recebe calcula o seu TQ usando este valor multiplicado pela sua própria qualidade local. Quando o Node C recebe o pacote do Node B, usa o TQ para avaliar a qualidade da ligação com o Node A.

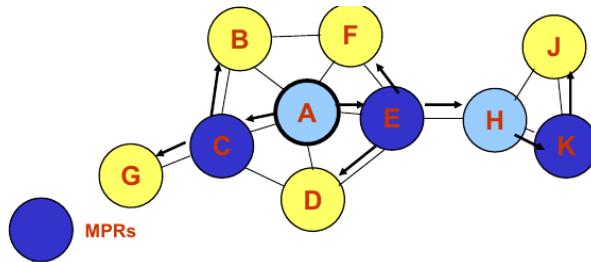


2.10 QoS-OLSR

Fatores utilizados na seleção de nós Multi-Point Relays (MPRs) no protocolo OLSR:

- **AB (Available Bandwidth):** Representa a largura de banda disponível no nó.
- **PoNOS (Percentage of Neighbors on Other Street):** Reflete a diversidade dos vizinhos em termos de localização na rede.
- **LW (Lane Weight):** Peso da Faixa, utilizado para favorecer a seleção de MPRs de faixas que transportam a maioria do fluxo de tráfego, visando aumentar sua estabilidade.

Esses fatores são combinados para determinar quais nós na rede OLSR serão designados como MPRs, desempenhando um papel crucial na eficiência e na confiabilidade do routing de mensagens dentro da rede.



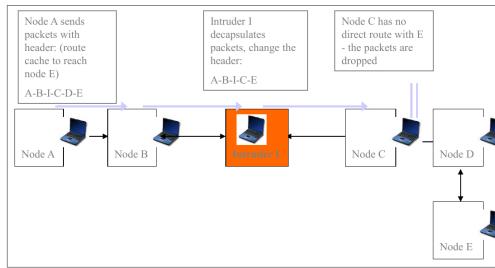
2.11 Security

2.11.1 Possible routing attacks

2.11.1.1 Attacks using modification

Tipos de ataques de routing por modificação:

- **Anúncio de Rotas Falsas:** Um nó malicioso anuncia rotas melhores para ser inserido na rede, alterando números de sequência ou contagens de saltos.
- **Inserção de Nó Malicioso:** Utilizando técnicas anteriores, um nó mal-intencionado integra-se à rede.
- **Modificação de Cabeçalhos de Pacotes:** O nó malicioso altera os cabeçalhos dos pacotes recebidos.
- **Impedimento de Envio de Pacotes:** Como consequência das modificações, os pacotes podem não chegar ao destino, interrompendo a transmissão.

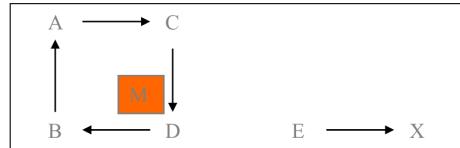


2.11.1.2 Attacks using impersonation

Consiste na usurpação de identidade, um nó malicioso assume a identidade de outro nó para realizar alterações:

- Spoofing do endereço MAC de outros nós.
- Formação de loops ao fazer spoofing do endereço MAC.

⇒ **Cenário de Ataque:** Um nó malicioso M pode ouvir todos os nós na rede. Ele modifica seu próprio endereço MAC para o endereço MAC de outro nó e anuncia para vários nós um caminho mais curto para alcançar um destino X.



Como resultado da formação de loops de routing, o destino X torna-se inacessível, impactando a conectividade na rede comprometendo a integridade do routing ao induzir nós vizinhos a seguir rotas falsas, resultando em loops que prejudicam a entrega eficaz de pacotes na rede.

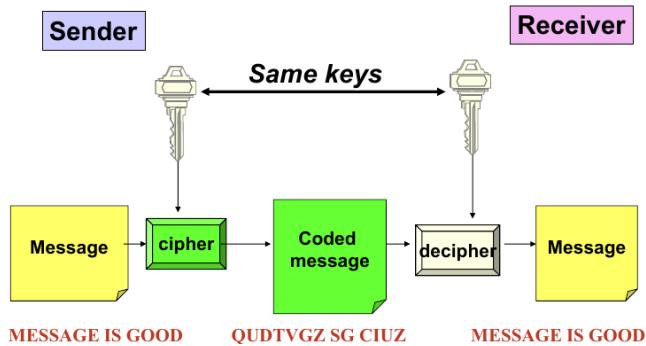
2.11.1.3 Attacks using fabrication

Os ataques de fabricação em redes ad-hoc visam perturbar o routing manipulando informações de forma fraudulenta. Isso inclui enviar mensagens de erro de rota falsas para desviar o tráfego, usar spoofing de endereços IP para interceptar comunicações destinadas a outros nós, e sobreregar os protocolos de routing com informações falsas para causar instabilidade na rede. Essas práticas comprometem a segurança e a eficiência das comunicações entre os nós, exigindo medidas robustas de segurança, como autenticação e criptografia, para mitigar esses riscos.

2.12 Key Management - basics

2.12.1 Symmetric cipher

A Criptografia simétrica é um tipo de criptografia que usa a mesma chave secreta para encriptação e decriptação de dados. A chave deve ser mantida em segredo entre as partes envolvidas na comunicação, pois é a única forma de decriptar os dados encriptados



Vantagens 😊:

- Rápidas e relativamente seguras.
- Proporcionam integridade e privacidade.
- Chaves mais longas aumentam a segurança.

Desvantagens 😞:

- Requerem a partilha de uma chave secreta.
- Administração complexa e não escalável.
- Necessidade de distribuir uma chave para cada receptor.

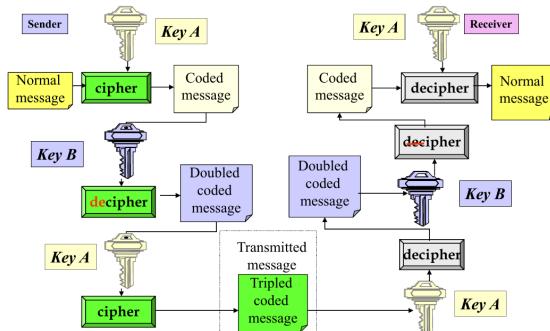


Figura 2.3: Triple symmetric mechanisms (e.g. “3-DES”)

2.12.2 Asymmetric cipher

A criptografia assimétrica, também conhecida como criptografia de chave pública, é um tipo de criptografia que usa um par de chaves diferentes - uma chave pública e uma chave privada - para a encriptação e decriptação de dados.

Vantagens 😎:

- Não é necessário partilhar chaves secretas antecipadamente.
- É escalável e versátil.

Desvantagens 😬:

- Geralmente é intensivo computacionalmente.
- Pode exigir uma autoridade de certificação.
- As chaves privadas têm de ser confidenciais.

Alguns exemplos de algoritmos de criptografia assimétrica incluem RSA e Diffie-Hellman. Mais detalhes sobre RSA e Diffie-Hellman ver os slides .

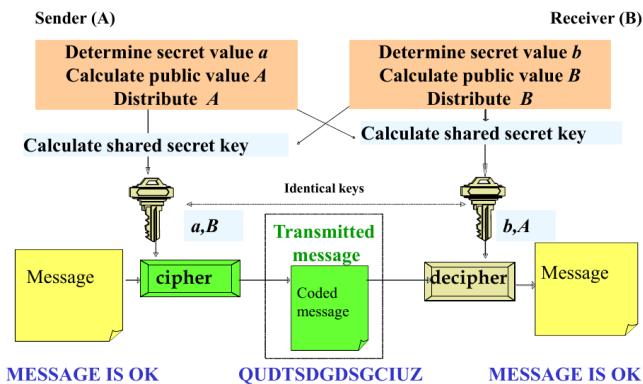


Figura 2.4: Diffie-Hellman Algorithm

2.13 Key Management in ad-hoc networks

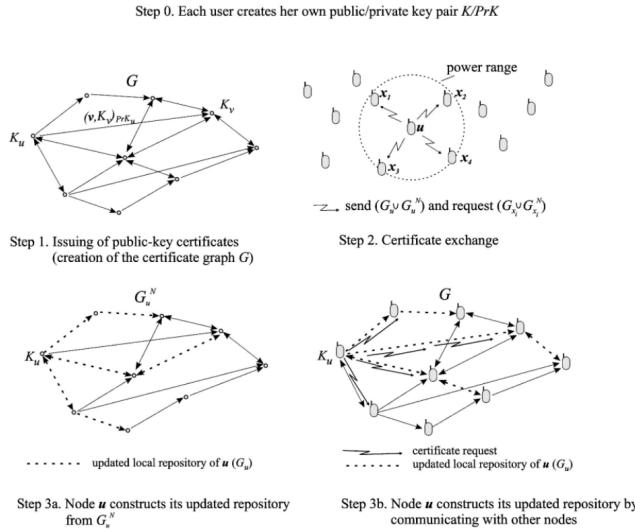
Em redes ad-hoc, a gestão de chaves enfrenta desafios significativos devido à natureza dinâmica e descentralizada dessas redes. Os nós móveis são mais suscetíveis a ataques físicos, aumentando a vulnerabilidade do sistema de segurança. Além disso, a mobilidade dos nós contribui para uma topologia de rede instável, com mudanças rápidas na conectividade que podem resultar em partições na rede. A falta de uma infraestrutura centralizada complica ainda mais a distribuição eficiente de informações de chave entre os nós, dificultando o estabelecimento e a manutenção de comunicações seguras em ambientes ad-hoc.

2.13.1 SOPKM: Self-organized public key management

O SOPKM é um sistema descentralizado onde os próprios nós emitem e distribuem certificados de chaves públicas baseados em relações pessoais de confiança. Cada certificado contém a chave pública do utilizador, a sua identidade e uma assinatura para validar sua autenticidade. Isto permite uma gestão flexível e adaptável das chaves públicas em redes distribuídas, como redes ad-hoc, sem depender de autoridades centralizadas.

No SOPKM, os utilizadores podem emitir certificados de chave pública que associam uma chave pública \mathbf{K}_v a um utilizador v , assinando-o, com cada certificado incluindo tempos de emissão e expiração. Estes certificados são armazenados localmente pelo emissor u no repositório \mathbf{G}_u e enviados para v , garantindo redundância, já que cada certificado é armazenado tanto pelo emissor como pelo destinatário.

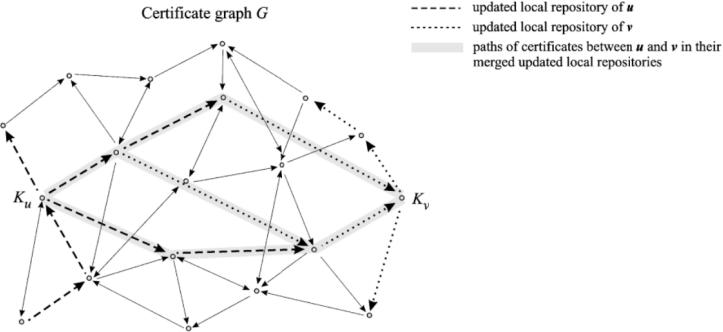
2.13.1.1 Update repositories of certificate graphs



Certificado de u para v , utilizando a chave privada de u ($\text{pr } \mathbf{K}_u(v, \mathbf{K}_v)$), \mathbf{G}_u atualizado, certificado global de u . No update dos repositórios dos grafos de certificados no SOPKM, cada nó envia os dois grafos em simultâneo o updated e o non-updated(envia informação do que tem e do que quer pedir).

2.13.1.2 Global Connectivity Graph

O SOPKM utiliza um grafo de conectividade global baseado em certificados, que explora o fenômeno **Small world**, onde a mobilidade aumenta a conectividade. Os nós móveis trocam suas chaves públicas quando se encontram, com vértices representando chaves públicas de alguns nós e arestas representando certificados de chaves públicas emitidos pelos utilizadores.



2.13.1.3 Certificate Update and Revocation

O SOPKM implementa mecanismos tanto para a atualização quanto para a revogação de certificados que garantem a integridade e eficiência na gestão de chaves públicas.

Atualização de Certificados no SOPKM: Antes do vencimento de um certificado, o emissor emite uma versão atualizada com um prazo de validade estendido, conhecida como atualização de certificado. Cada nó, periodicamente, emite essas atualizações, supondo que os vínculos entre o utilizador e a chave contidos nelas são corretos. Isto requer sincronização de tempo entre os nós e uma decisão cuidadosa sobre o prazo de validade, geralmente de várias semanas.

Revogação de Certificados no SOPKM: Cada utilizador pode revogar um certificado emitido se considerar que o vínculo entre o utilizador e a chave não é mais válido ou se a sua própria chave privada estiver comprometida. A revogação pode ser explícita, mediante emissão de uma declaração de revogação, que é distribuída apenas aos nós que periodicamente atualizam os seus certificados. Alternativamente, pode ser implícita, na qual o certificado vence e os nós atualizam os seus repositórios durante o período de revogação.

2.13.1.4 Malicious Users

O mecanismo de troca de certificados permite que os nós recolham praticamente todos os certificados de um repositório global (G). Os nós verificam os vínculos entre o utilizador e a chave nos certificados que detêm e detectam quaisquer inconsistências, como certificados conflituosos que possuem o mesmo nome de utilizador, mas chaves públicas diferentes, ou certificados que partilham a mesma chave pública, mas estão vinculados a diferentes nomes de utilizador. Caso ocorram conflitos, são necessárias várias trocas de certificados para resolvê-los.

2.13.2 SSAWN: Self-securing ad-hoc wireless networks

Opera sob um modelo de confiança localizado, onde a confiança numa entidade é estabelecida se pelo menos k entidades confiáveis, tipicamente vizinhos imediatos, dentro de um período de tempo específico.

Este modelo visa alcançar alta garantia de segurança e eficiência na comunicação, priorizando a confiabilidade dos vizinhos imediatos para determinar a confiança global de um nó na rede. A rede utiliza um mecanismo de criptografia baseado em chaves assimétricas RSA, onde uma Chave Secreta Global (SK) é distribuída entre os nós para assinar certificados, que por sua vez são verificados pela Chave Pública Correspondente (PK). Esse sistema é considerado um **Threshold secret sharing**, onde cada nó possui uma parte do segredo global, derivado de seu endereço único, permitindo a deteção local de nós mal-intencionados com base na cooperação dos pelo menos K vizinhos próximos.

2.13.2.1 Basic Operation

A operação básica envolve um sistema de infraestrutura de chave pública (PKI) distribuído, onde a chave privada do sistema é dividida entre vários nós servidores. Um quórum de k servidores é necessário para produzir atualizações de certificados. A estrutura de certificados opera em fases que incluem a formação e manutenção do grupo de servidores, atualização e revogação de certificados, além da renovação de chaves partilhadas.

A Chave Secreta Global (SK) não é visível, conhecida ou recuperável por qualquer nó da rede. Cada nó carrega um certificado assinado com SK, e a Chave Pública (PK) é assumida como conhecida para verificação de certificados. Nós sem certificados válidos são impedidos de acessar recursos de rede, como routing e encaminhamento de pacotes.

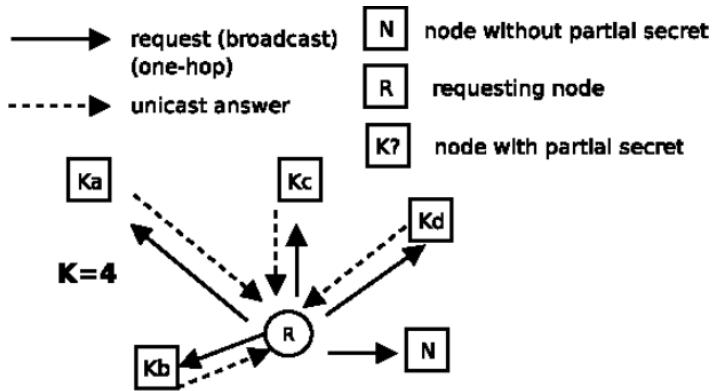


2.13.2.2 Shared secrets

Os segredos partilhados são usados para segurança e gestão de confiança.

- uma chave secreta parcial é gerada usando um polinômio de ordem $K-1$ no início. K nós com partes da chave secreta parcial podem recuperar a Chave Secreta Global (SK) usando interpolação de Lagrange.

- Um nó solicita certificados aos K vizinhos mais próximos que possuem partes da chave secreta.
- Os certificados parciais são combinados para formar um certificado completo, garantindo que apenas nós confiáveis recebam acesso aos recursos da rede.



2.14 Reputation

Abordagens de reputação visam identificar nós bem-comportados em redes:

- Avaliação contínua do comportamento dos nós vizinhos.
- Utilização de nós com alta reputação para routing e comunicação.
- Proteção do tráfego da rede contra nós com comportamento inadequado.
- Minimização da interação com nós considerados não confiáveis.

A reputação de cada nó é avaliada de forma distribuída, onde cada nó monitoriza o comportamento dos nós vizinhos e troca informações periodicamente com eles. Também inclui observar como cada nó trata o encaminhamento de pacotes (encaminhamento, modificação ou injeção de pacotes) e a consideração da confiabilidade das informações recebidas vinda de outros nós.

2.14.1 Reputation into the normal operation of the network

- Combinação da reputação direta (de vizinhos) e indireta (informações de outros nós).
- Distribuição do comportamento de um nó, baseada no número de pacotes observados (transmitidos corretamente, modificados ou não transmitidos).
- Monitorização colaborativa, onde os nós trocam reputação direta e realizam testes de desvio para detetar relatos falsos.

- Utilização de reputação na escolha de nós para rotas, na formação de grafos de certificação e na distribuição de chaves.
- A reputação de um nó pode mudar ao longo do tempo, especialmente quando nós ficam fora da comunicação por períodos específicos.

MEC: Mobile Edge Computing

MEC é um conceito introduzido no contexto do 5G que:

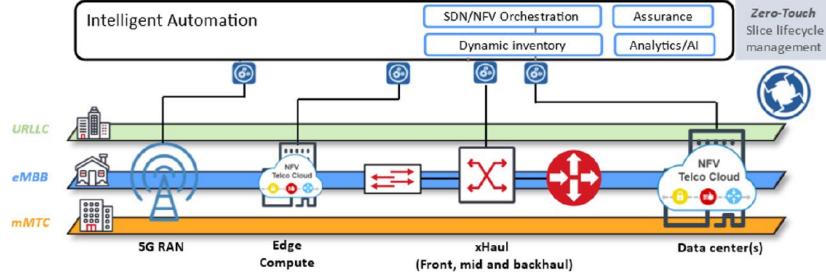
- Aproxima a computação em nuvem para a borda da rede.
- Permite que aplicações de terceiros sejam hospedadas na borda da rede.
- Oferece serviços para melhorar aplicações com informações contextuais, como informações de rede e localização.
- Redireciona o tráfego para garantir latência ultra baixa.
- Facilita a execução de aplicações no local e no momento adequados.

Diferentes soluções de IoT têm requisitos de rede variados, como veículos autónomos e equipamentos médicos, que necessitam de baixa latência para decisões críticas, sendo o edge computing essencial para processamento e decisões rápidas próximas ao ponto de necessidade.

3.1 Edge and Cloud

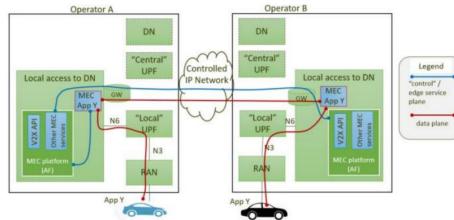
Os dispositivos de edge computing dependem do acesso à Cloud para receber modelos de aprendizagem automática e algoritmos de processamento de eventos complexos e, simultaneamente, enviam dados de sensores e atualizações de estado para a nuvem. A transição do 5G para o 6G é crucial devido a:

- **Altos Requisitos de Banda:** Garantir transferência de dados contínua entre dispositivos de edge e a nuvem.
- **Baixa Latência:** Facilitar resposta em tempo real para aplicações críticas.
- **Suporte para Implantação Massiva de Nós:** Lidar eficientemente com um grande número de dispositivos ligados entre si.



3.2 Examples using Edge Computing

- ⇒ Uma aplicação V2X (Vehicle-to-Everything) pode estar a ser executada num carro conectado ao operador de rede móvel (MNO) 1, equipado com um sistema MEC do fornecedor 1, e a comunicar-se com outra instância da aplicação V2X num segundo carro conectado ao MNO 2, equipado com um sistema MEC do fornecedor 2.
- ⇒ O serviço V2X é implementado com duas instâncias da aplicação "MEC App Y", cada uma comunicando-se com seu respectivo Cliente App, ou seja, "App Y", e também conectada a uma plataforma MEC em cada sistema MEC (domínio) respetivo.



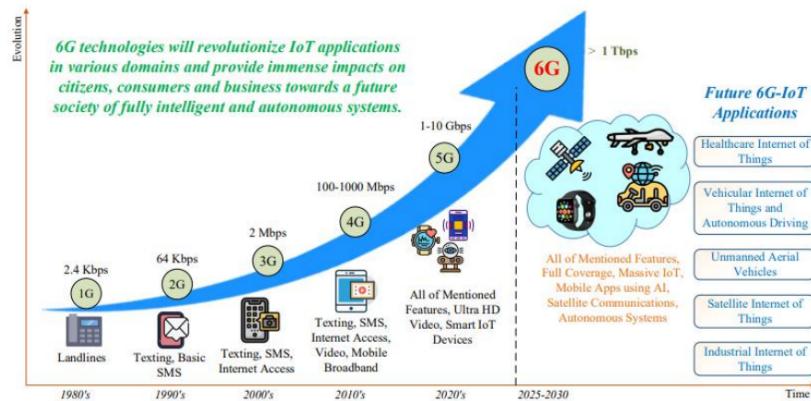
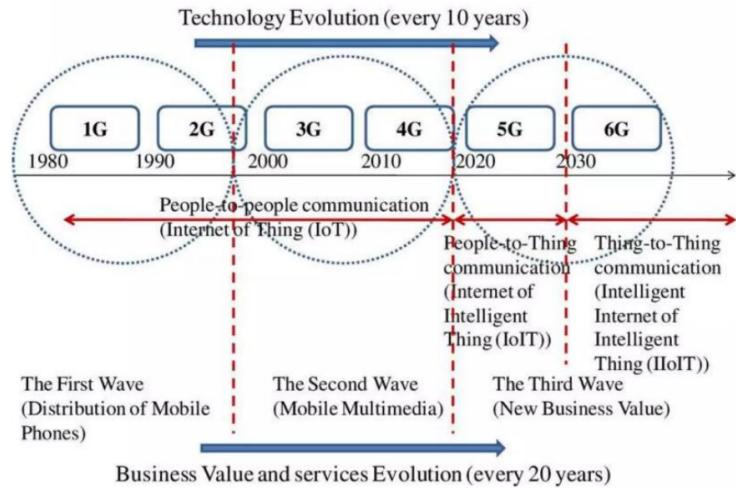
3.3 MEC future

O MEC está posicionado como um elemento crucial para o futuro das tecnologias de comunicação, especialmente no contexto do 5G. Este paradigma arquitetónico não só permite a virtualização e execução de aplicações em ambientes próximos à borda da rede, como também facilita a orquestração dinâmica e o instanciamento de serviços conforme a demanda.

Com sua capacidade de suportar uma variedade de cenários, desde saúde até indústria, IoT, automóvel e meio ambiente, o MEC promove um ambiente onde aplicações críticas podem ser executadas com baixa latência e alta eficiência. Isso não apenas transforma a maneira como os serviços são entregues,

mas também possibilita redes e sistemas autónomos, permitindo assim uma infraestrutura mais ágil e adaptável às necessidades emergentes das tecnologias modernas

3.4 What about 6G?



Bibliografia

- [1] E. Andres, *TCP Reno/Vegas*, <https://www.slideserve.com/eitan/tcp-reno-vegas>, 2014.