

Comboios baseados em sistemas veiculares ciber-físicos: conceito, aplicações, arquitetura, protocolos e aspectos de segurança.

Flávio Simões

TP-546-Internet das coisas e redes veiculares
Instituto Nacional de Telecomunicações - INATEL
Santa Rita do Sapucaí-MG, Brazil
flavio.simoes@mtel.inatel.br

Resumo—Este artigo explora o conceito de comboios baseados em sistemas veiculares ciber-físicos (PVCPS), destacando suas aplicações, arquitetura, protocolos e aspectos de segurança. O estudo aborda a integração de tecnologias avançadas de comunicação e controle, incluindo o uso de blockchain para gerenciamento de reputação e segurança cooperativa para proteger a transmissão de dados. Também são apresentados os benefícios do modelo PVCPS, como eficiência no tráfego, redução de emissões e maior segurança, bem como estratégias para mitigar desafios relacionados à conectividade e ataques cibernéticos. Além disso, discute-se o papel transformador da sexta geração de redes de comunicação (6G), que promete taxas de transmissão extremamente altas, comunicação de baixa latência e integração de tecnologias emergentes como superfícies reflexivas inteligentes e comunicação em espectros de terahertz, reforçando a segurança e a eficiência dos sistemas veiculares ciber-físicos.

Palavras chaves—comboios baseados em sistemas veiculares ciber-físicos (PVCPS), Comunicação entre veículos e infraestrutura (V2I), comunicação entre veículos (V2V), redes veiculares, comboios autônomos.

I. INTRODUÇÃO

A indústria automobilística vem alcançando transformações importantes com a evolução tecnológica, onde a sustentabilidade com veículos menos poluentes e mais eficientes tem sido grande preocupação, e motivando o incremento de inúmeros sensores e conexões permitindo até sua condução de forma autônoma. A implementação de produtos de hardware e software podem incluir sensores com a finalidade de perceber alterações no ambiente, atuadores com a finalidade de executar fisicamente estas alterações no veículo e até 100 unidades de controle eletrônico (ECUs), capazes de executar ações, realizar diversas medições e coletar dados. Estas ECUs aplicadas nas redes veiculares constroem um sistema de transporte inteligente com a redução de problemas considerados críticos como acidentes de trânsito, congestionamentos e poluição [7].

Em [11] o sistema de comboio é caracterizado como veículos movendo de forma autônoma e mantendo movimentos e posições precisas entre eles. A utilização das redes veiculares objetivando veículos viajando em grupos, baseado

em comboios, surge como solução à construção de novas rodovias ou a ampliação das existentes que muitas vezes são soluções difíceis de serem implementadas, como por exemplo, estradas em regiões de proteção ambiental e o alto custo destas ampliações e construções [7]. Em [1],[7], a operação em comboios apresentam vantagens como: aumento da capacidade das estradas, redução no consumo de energia e emissão de poluentes, conforto e segurança do motorista e por fim o desenvolvimento de aplicações de comunicação coletiva considerando a posição relativamente fixa dos veículos em um mesmo comboio.

Neste contexto, o comboio baseado em sistemas veiculares ciber-físicos (PVCPS), em [7], em que os veículos se comunicam via redes sem fio e se movem em um padrão coordenado, com troca constante de informações entre o processo cibernético e o processo físico. Sistemas estes que se correlacionam intimamente entre as unidades computacionais (cibernéticas) e os sistemas físicos compondo os sistemas ciber-físicos, que mesclam estratégias de controle, sistemas embarcados, sistemas em tempo real e engenharia de software. Apesar do comboio ser uma sistema físico complexo, com as evoluções tecnológicas sistemas desenvolvidos para contribuir com a condução dos veículos pelos motoristas tem surgido como exemplos podemos citar o controle de cruzeiro adaptativo (ACC) que utiliza de sensores para detectar a distância entre os veículos e maneira autônoma manter a velocidade e distância, sistema de alerta de ponto cego, sistema de alerta de permanência de faixa, sistema de frenagem de emergência, sistema de detecção de pedestres e estacionamento autônomo, combinado a isto, o comboio poderá por meio do uso de tecnologias de comunicação sem fio dispor de um sistema inteligente de transporte[1].

Neste artigo é apresentado na seção II o conceito do comboio baseado em sistemas veiculares ciber-físicos, com as aplicações, conectividade, arquitetura e protocolos, em seguida é tratado os aspectos de segurança na seção III, onde são analisadas soluções que asseguram a integridade e a confidencialidade das comunicações nos comboios. O uso de protocolos distribuídos de chaves secretas protege os dados

transmitidos, enquanto a aplicação de blockchain para o gerenciamento de reputação ajuda a mitigar riscos cibernéticos e a fortalecer a confiança no sistema, na seção IV é apresentado direcionamento para trabalhos futuros com a sexta geração de redes de comunicação (6G) que marca uma transformação profunda na conectividade veicular e como conclusão na seção V, apresenta um resumo com os principais achados do estudo, destacando o impacto das soluções propostas no desenvolvimento de sistemas de transporte mais inteligentes, seguros e conectados, com potencial para transformar a mobilidade urbana e interurbana.

II. COMBOIO BASEADO EM SISTEMAS VEICULARES CIBER-FÍSICOS

A construção de comboios baseado em sistemas veiculares ciber-físicos surgem como solução inteligente objetivando melhoria da capacidade de estradas, segurança na condução de um grupo de veículos a partir de um ponto inicial até a um outro no destino, a exemplo da Rodovia Imigrantes que interliga a Capital Paulista a Baixada Santista, onde este tipo de operação ocorre de forma isenta de tecnologia, conduzida por uma viatura e agrupando uma quantidade de veículos na praça de pedágio quando da baixa visibilidade do trecho de serra. Neste sentido o comboio sempre terá o líder que será conduzido de forma manual ou autônoma e determinará as ações do movimento dos demais veículos como velocidade, direção aceleração e desaceleração [3]. Em [1], o PVCPS tem como característica a junção estreita entre a dinâmica física dos veículos e os comportamentos da redes veiculares, construído a partir de um plano físico representando a mobilidade do comboio e as condições de tráfego e de um plano cibernético que representa as redes veiculares formadas pelos veículos adjacentes e seus comportamentos, como ilustrado na Fig. 1. Nesse sistema, cada veículo troca dados com os veículos vizinhos por meio de redes de comunicação de curto alcance dedicadas (DSRC)

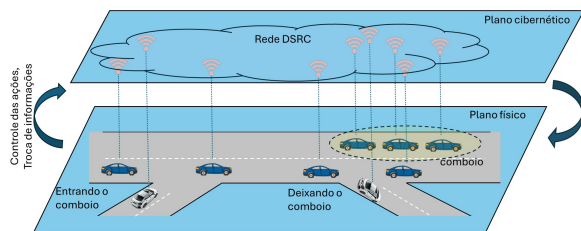


Fig. 1. Comboio sobre plano ciber-físico

A. Aplicações

Em [1], temos que implementação de sistemas baseados em comboios de veículos tem como objetivos principais a otimização do fluxo de tráfego e a promoção de um trânsito mais sustentável e eficiente. Esses sistemas visam reduzir congestionamentos, melhorar a capacidade das vias, economizar tempo de viagem e diminuir o impacto ambiental do transporte.

Um exemplo significativo é o projeto California Partners for Advanced Transit and Highways (PATH), iniciado em 1986, que buscou aumentar a fluidez do tráfego com a utilização de comboios em rodovias. Outro destaque é o Grand Cooperative Driving Challenge (GCDC), onde equipes testaram veículos com controle adaptativo de cruzeiro cooperativo (CACC) e os compararam com os de outros competidores, promovendo o desenvolvimento e integração de sistemas cooperativos de direção. Tecnologias emergentes de redes veiculares têm facilitado o uso de comboios, como demonstrado no programa europeu SARTRE, realizado entre 2009 e 2012. Este programa testou um comboio em rodovias, liderado por um caminhão seguido por carros dirigidos autonomamente em formações compactas. Os testes indicaram velocidades de até 90 km/h com espaçamento de apenas 6 metros entre os veículos.

Além da otimização do tráfego, sistemas baseados em comboios buscam tornar o trânsito mais ecológico e econômico. Projetos como o Energy ITS, no Japão, focaram na redução de emissões de gás carbônico CO₂, implementando comboios automatizados de caminhões e avaliando os impactos de tecnologias de transporte inteligente (ITS). Outras iniciativas propuseram alocações descentralizadas de faixas para reduzir o tempo de viagem e aumentar a capacidade do tráfego, bem como métodos de controle robusto para projetar perfis de velocidade de comboios, considerando consumo de combustível, inclinações da estrada e emissões. Adicionalmente, abordagens como o controle longitudinal de caminhões pesados demonstraram potencial na redução do consumo de combustível.

Por fim, as comunicações sem fio expandem o escopo dos comboios para aplicações de entretenimento. Elas possibilitam entregas de dados específicas entre veículos no comboio, acesso à internet em movimento e serviços locais cooperativos, tornando as redes veiculares mais versáteis e conectadas.

B. Conectividade

A rede de comboio pode ser aprimorada aplicando o uso de tecnologias de comunicação sem fio, além das tecnologias utilizadas de forma isolada, que desempenham um papel fundamental no avanço dos sistemas de transporte inteligentes (ITS). Especificamente, a integração de interfaces de comunicação a bordo, conhecidas como unidades embarcadas (OBU), permite que veículos em operação coletem informações tanto de outros veículos próximos quanto de infraestruturas viárias, chamadas unidades de beira de estrada (RSU). Isso contribui para uma experiência de condução mais segura e eficiente.

Na prática, veículos equipados com tecnologia de comunicação podem formar redes sem fio móveis nas vias, conhecidas como redes ad hoc veiculares (VANET). Essas redes, consideradas uma solução promissora, viabilizam dois tipos principais de comunicação sem fio: comunicação entre veículos (V2V) e comunicação entre veículos e infraestrutura (V2I). Em redes VANETs, cada veículo tem a capacidade de gerar informações sobre as condições da estrada, como alertas de congestionamento ou relatórios de acidentes. Essas informações podem ser transmitidas para outros veículos próximos ou para unidades RSU. Combinado a isto, as redes

veiculares podem receber um complemento com as redes de sensores sem fio (WSNs) implantadas ao longo das estradas objetivando segurança e tráfego eficiente. No entanto, devido as características limitantes das WSNs em termos de memória, alcance de transmissão e energia, ainda é um desafio a utilização deste tipo de rede [1], a combinação destas infraestruturas formam os principais elementos da rede nas estradas, conforme demonstrada na figura 2. No contexto PVCPS, as mensagens de controle e os dados necessários para operação são emitidos exclusivamente pelo veículo líder, que é responsável por coordenar em tempo real os movimentos dos veículos autônomos que compõem o comboio e compartilhar informações sobre a posição e o status dos demais veículos após a realização de qualquer manobra, assegurando a estabilidade do comboio. Além disso, o líder também tem a função de monitorar as condições de condução do comboio, designar tarefas específicas de entrega aos veículos seguidores e determinar a rota de cada um, entre outras responsabilidades [11].

Esse tipo de sistema integra de forma estreita as tecnologias de computação, comunicação e controle, configurando-se como um comboio baseado em sistemas ciber-físico veicular. Nesse contexto, todos os veículos se comunicam por meio de redes veiculares e operam em padrões de comboio, estabelecendo um ciclo fechado de troca de informações entre processos físicos e cibernéticos.

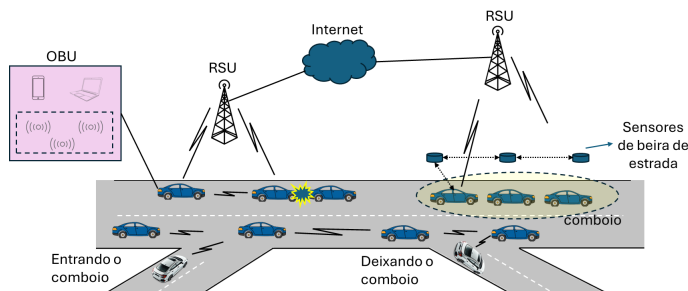


Fig. 2. Principais elementos de rede

C. Arquitetura e protocolos

O propósito central das redes veiculares é viabilizar a troca de dados através de comunicações V2V e V2I, atendendo a diversas aplicações no contexto veicular. Os tipos de informações transmitidas incluem monitoramento de estado, pacotes de controle, dados de entretenimento e mensagens de alerta.

As limitações de latência podem variar entre milissegundos e segundos, dependendo, tanto do tipo de informação, quanto do modo de disseminação utilizado (unicast, multicast ou broadcast). Além disso, esses dados podem ser gerados de forma periódica ou ativados por eventos específicos.

Para orquestrar toda esta comunicação os protocolos existentes para redes veiculares e suas arquiteturas, devem atender às demandas das aplicações em PVCPS [1].

1) *Comunicação V2V*: Em, [1], a Comunicação V2V Baseada em comboio é essencial para viabilizar aplicações como a formação de comboio de veículos e serviços de entretenimento, demandando uma arquitetura eficiente em comboios baseados em sistemas ciber-físicos veiculares. As principais preocupações incluem a disseminação de mensagens dentro dos comboios e entre diferentes comboios, bem como a melhoria da conectividade entre veículos e infraestruturas, como as RSUs.

Na comunicação intra-comboio, cada veículo deve compartilhar regularmente seu estado, incluindo informações como posição, velocidade e aceleração, com os demais veículos do grupo. Esse processo é suportado por padrões como o IEEE 1609.4 e o ETSI ITS-G5. O padrão IEEE 1609.4 organiza o acesso ao canal em intervalos sincronizados, incluindo o Canal de Controle e o Canal de Serviço. Além de um canal dedicado exclusivamente a mensagens de segurança, foi implementado para garantir melhor desempenho. Por sua vez, o ETSI ITS-G5 utiliza mensagens de consciência cooperativa, transmitidas no canal de controle, e adota um controle descentralizado de congestionamento, que ajusta parâmetros como potência de transmissão, taxa de dados e intervalo entre pacotes com base na carga do canal.

Apesar dessas medidas, o congestionamento no canal em condições de tráfego denso pode reduzir a taxa de recepção e prejudicar a transmissão de dados não relacionados à segurança em fluxos de tráfego esparsos. Para resolver esse problema, foram desenvolvidas abordagens baseadas em contenção, que ajustam parâmetros como frequência de beacon, potência de transmissão e tamanho da janela de contenção, e soluções sem contenção, que utilizam alocação de intervalos TDMA por líderes de clusters. Soluções mais avançadas, como o algoritmo FARE, regulam adaptativamente a frequência de mensagens com base na densidade local de veículos, enquanto esquemas de retransmissão mitigam colisões de dados.

Na comunicação inter-comboios, a conectividade VANET é uma tecnologia importante, com estudos indicando que o aumento da densidade de tráfego e do alcance de transmissão melhora as métricas de conectividade, neste tipo de rede. A conectividade em cenários com comboios se mostra mais robusta do que em redes sem essa organização. Além disso, RSUs desempenham um papel importante na retransmissão de mensagens entre veículos desconectados, aumentando a taxa de penetração de mensagens e melhorando a conectividade em redes de baixa densidade. Em resumo, a comunicação V2V em comboios exige abordagens robustas para lidar com desafios como congestionamento de canais e a necessidade de respostas rápidas às condições dinâmicas do tráfego.

2) *Comunicação V2I*: Em [1] é relatado que, a Comunicação V2I Baseada em comboio, também conhecida como acesso à Internet em movimento (drive-thru Internet), é uma aplicação central em comboios baseados em sistemas veiculares ciber-físicos. Nesse contexto, os veículos podem acessar serviços de Internet por meio de RSUs enquanto estão dentro da área de cobertura de transmissão. No entanto,

esse cenário apresenta desafios, como o tempo limitado de conexão, altas taxas de erro na transmissão e desigualdades no tempo de serviço, especialmente em condições de tráfego denso, onde o mecanismo CSMA/CA do IEEE 802.11p pode levar a perdas significativas de pacotes e atrasos médios elevados. Diversos estudos analisaram e propuseram soluções para melhorar o desempenho da comunicação em cenários de drive-thru Internet. Foi avaliado o impacto da densidade do tráfego, da velocidade dos veículos, do alcance de transmissão das RSUs e das taxas de bits no desempenho de download. Modelos baseados em cadeias de Markov foram usados para representar o estado de nós móveis no processo de drive-thru, incorporando aspectos como zonas espaciais e transições de pacotes. Para melhorar a qualidade do enlace em regiões limitadas de cobertura, esquemas de retransmissão V2V foram propostos, utilizando veículos como proxies confiáveis para estender o alcance das RSUs e manter uma alta taxa de transferência de dados. Algumas abordagens exploraram a mobilidade baseada em comboios para aumentar a eficiência do sistema. Por exemplo, esquemas cooperativos de retransmissão permitiram que veículos ajudassem na retransmissão de dados de seus vizinhos em casos de falha na transmissão. Estratégias de agendamento multi-fluxo também selecionaram veículos próximos às RSUs com as maiores taxas para otimizar os downloads, enquanto a cooperação entre veículos aumentou ainda mais a taxa de transferência do sistema.

A alocação de espectro foi outra técnica utilizada para atender aos requisitos de QoS das aplicações veiculares. Veículos foram agrupados em clusters, com canais de uso compartilhado para comunicação entre clusters e canais exclusivos para comunicação intra-cluster. Além disso, ajustes no tamanho mínimo da janela de contenção, baseados na velocidade dos veículos, ajudaram a resolver desigualdades no acesso à Internet, permitindo chances iguais para veículos com diferentes tempos de permanência na cobertura da RSU.

Por fim, a otimização de desempenho em VANETs foi explorada utilizando estratégias de controle de posição para veículos com mobilidade controlável, maximizando a taxa média de dados no elo de gargalo. Essa otimização foi abordada tanto por métodos teóricos de otimização, que requerem informações completas da rede, quanto por métodos baseados em teoria dos jogos, nos quais os veículos ajustam suas posições de forma distribuída, utilizando apenas informações de seus vizinhos.

Em resumo, as dinâmicas do tráfego têm um impacto significativo nos sistemas de drive-thru Internet. Uma solução eficiente para melhorar o desempenho é explorar características como o padrão de condução baseado em comboios ou a distribuição controlada da posição dos veículos, permitindo acesso cooperativo e otimizado às RSUs.

3) *Protocolo VANET*: Em [1], o protocolo VANET para se tornar viável, diversas organizações e institutos têm trabalhado na padronização da comunicação veicular nos últimos anos, como o CEN TC278, ISO TC204, ETSI TC ITS, IEEE 1609 e IETF. Nos Estados Unidos, o Departamento de Transporte (DOT) propôs que todos os novos veículos

fossem equipados com interfaces de rádio V2V baseadas em comunicações de curto alcance dedicadas (DSRC) até o início de 2017.

Entre os principais protocolos utilizados, destacam-se: a IEEE acesso sem fio em ambiente veicular (WAVE) e as extensões de mobilidade para IP desenvolvidas pela IETF.

A WAVE é amplamente reconhecida como o protocolo padrão para redes veiculares baseadas na tecnologia DSRC. Ela estabelece a arquitetura e os serviços necessários para que dispositivos DSRC/WAVE de múltiplos canais possam se comunicar em um ambiente móvel. Essa família integra o IEEE 802.11p e o conjunto de protocolos IEEE 1609 [1], cobrindo desde a camada física até a camada de aplicação/serviço, demonstrado na figura 3.

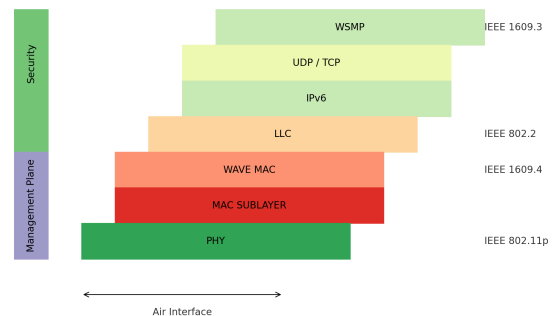


Fig. 3. Arquitetura e protocolos WAVE

Na camada física, o IEEE 802.11p utiliza uma banda de 75 MHz no espectro de 5 GHz, conforme especificado pelo padrão DSRC dos EUA. Essa banda é dividida em um Canal de Controle (CCH) e seis Canais de Serviço (SCHs). Já na camada MAC, o IEEE 802.11p expande o conjunto de serviços básicos (BSS) padronizado no IEEE 802.11 e adota o mecanismo de Acesso Distribuído Aprimorado (EDCA), introduzido no IEEE 802.11e, que categoriza diferentes fluxos de dados em classes de acesso (ACs).

Além do IEEE 802.11p, o conjunto de protocolos IEEE 1609 adiciona funcionalidades avançadas. Por exemplo, a subcamada MAC do IEEE 1609.4 (Operação em Múltiplos Canais) gerencia o tempo e a alternância entre CCH e SCHs, permitindo a operação simultânea de aplicações de segurança e não segurança em um único dispositivo de rádio. Já o IEEE 1609.3 (Serviços de Rede) define os serviços de endereçamento e entrega de dados no sistema WAVE, com suporte ao IPv6 e ao Protocolo de Mensagem Curta do WAVE (WSMP). Na camada de aplicação, o IEEE 1609.11 (Pagamento Eletrônico) estabelece um protocolo interoperável de pagamento baseado em padrões ISO. Outras especificações para aplicações industriais ainda estão em desenvolvimento.

Uma família de padrões relacionada são as comunicações ITS, especificadas pelo ETSI. Essas comunicações compartilham algumas tecnologias DSRC com o IEEE WAVE, mas diferem no gerenciamento de múltiplos canais [1].

Apesar de suportar tanto a comunicação V2V quanto V2I, o WAVE oferece uma conectividade V2V/V2I limitada e de

curta duração, devido à alta velocidade dos veículos e à natureza dinâmica das topologias das VANETs nas estradas. Para aprimorar a transmissão de informações em veículos baseados em IP, diversos protocolos móveis de IP emergentes podem ser utilizados, conforme definidos pelo órgão Força-Tarefa de Engenharia da Internet (IETF). Em particular, o IETF ampliou o MIPv6 para incluir suporte à mobilidade de redes, conhecido como protocolo básico de suporte NEMO [1]. Nesse modelo, os nós de rede móvel (MNNs) são acessíveis exclusivamente através de um roteador móvel (MR). Para a aplicação do NEMO em redes veiculares, dois métodos foram propostos em [1]: um focado em MNNs (MNNs-centric) e outro focado em NEMO (NEMO-centric), dependendo da posição do NEMO dentro da pilha de protocolos.

Relata [1], que além das funções básicas, o IP Móvel e o NEMO ainda enfrentam diversos desafios em cenários de tráfego altamente dinâmico. Entre esses desafios estão os atrasos na transmissão de ponta a ponta, causados pela sobrecarga de tunelamento entre o agente doméstico (HA) e o roteador móvel (MR), bem como a dificuldade em definir a localização ideal para o HA, entre outros. Para superar essas dificuldades, várias estratégias de otimização de rotas foram sugeridas, como por exemplo, introdução do protocolo VARON, que visa melhorar tanto a largura de banda quanto a latência nas comunicações entre veículos. Ele combina uma rede de infraestrutura (como uma rede 3G para acesso à Internet) com uma VANET, utilizada para comunicações em múltiplos saltos (multi-hop) e ainda uma abordagem inovadora para o gerenciamento de NEMO, em que veículos próximos com padrões de movimento semelhantes são organizados como um "ônibus virtual" (semelhante a um comboio), permitindo que todos os MRs sejam conectados. Isso possibilita que o MR líder realize um pré-handoff, minimizando o atraso do handoff para os MRs que o seguem e ainda uma abordagem similar, onde os veículos foram agrupados em clusters, e o líder de cada cluster foi designado como o MR, responsável por manter a mobilidade IP dos veículos do grupo. Outra estratégia se baseiam em redes IEEE 802.11 genéricas para V2I, propondo o framework Vehicular IP in WAVE (VIP-WAVE). Esse framework estabelece a configuração de IP para serviços estendidos e não estendidos, além de oferecer um esquema de gerenciamento de mobilidade baseado no Proxy Mobile IPv6 sobre WAVE. Os resultados mostraram que esse framework pode melhorar a Qualidade de Serviço (QoS) do WAVE/IEEE 802.11p utilizando mecanismos de sinalização e detecção de movimento.

4) *Arquitetura de redes veiculares:* Devido à mobilidade dos veículos e ao alcance limitado de transmissão do IEEE 802.11p, a conectividade em VANETs tende a ser instável, dificultando a redução da latência durante o processo de handoff. Para mitigar esses problemas, uma abordagem eficiente é desenvolver uma arquitetura híbrida que integre as VANETs com redes celulares [1], permitindo maior cobertura e desempenho elevado. Como proposição, [1] descreve uma apresentação de arquitetura que integra VANET e sistema universal de telecomunicações móveis (UMTS), onde as RSUs

estão conectadas à interface do UMTS. Nessa abordagem, os veículos são agrupados dinamicamente com base em três métricas principais: força do sinal recebido do UMTS, padrões de movimento dos veículos e distância entre eles. Esses clusters utilizam o menor número possível de gateways móveis otimizados, equipados com interfaces IEEE 802.11p e a rede de acesso via rádio (UTRAN), para conectar a VANET às redes 3G por meio de um mecanismo de seleção baseado em múltiplas métricas. Para realizar a transição entre gateways de forma eficiente, utiliza-se um mecanismo de handoff, enquanto operações de anúncio e descoberta de gateways informam os nós da VANET sobre o novo gateway selecionado. Com a crescente expansão das redes celulares e o aumento no uso de aplicativos em celulares, estudos recentes sugerem a utilização de celulares como alternativa econômica para suportar aplicações em VANETs, relata [1] em uma pesquisa que demonstrou que dispositivos móveis equipados com LTE são viáveis para comunicação V2I, considerando o rápido avanço das redes 4G onde exemplos de aplicações incluem a estimativa de tempo de viagem em estradas com auxílio de dispositivos móveis e a identificação de acidentes de trânsito utilizando sensores como acelerômetros e microfones dos celulares.

Dado que as redes veiculares são essencialmente compostas por máquinas que se comunicam sem intervenção humana, esse processo também pode ser descrito como comunicações máquina-a-máquina (M2M) [1]. Em particular, os padrões LTE-Advanced, que estão em constante evolução, passaram a suportar comunicações do tipo máquina (MTC), permitindo que dispositivos em larga escala troquem informações de forma autônoma. Assim, o LTE-Advanced com suporte a MTC pode viabilizar diversas aplicações veiculares, como coleta de dados de veículos em movimento (FCD), diagnóstico automotivo e gerenciamento de frotas. Em um estudo [1] diz que foi explorado o uso de sensores embarcados como fonte de dados para previsões dinâmicas de tráfego. Para reduzir o impacto do tráfego MTC na qualidade de serviço de comunicações humanas, o estudo propôs uma estratégia de transmissão orientada ao canal, na qual os veículos transmitem FCD de maneira probabilística com base na relação sinal-ruído detectada.

Além das redes mencionadas, que se concentram principalmente em comunicações sem fio, as redes veiculares podem ser aprimoradas com o uso de tecnologias emergentes, como computação em nuvem móvel e soluções sensíveis ao contexto [1],[2], apresentando uma arquitetura chamada V-Cloud, que combina os conceitos de VANET, sistemas ciber-físicos (CPS) e computação em nuvem para garantir maior segurança, conforto ao motorista e melhores condições ambientais. A arquitetura sugerida possui três camadas: CPS veiculares embarcados, redes V2V e redes V2I. E [1] relata que trabalhos semelhantes foram apresentados, onde a computação em nuvem foi incorporada às redes veiculares, permitindo que os veículos compartilhem recursos de processamento, armazenamento e largura de banda.

III. ASPECTOS DE SEGURANÇA

A conectividade do comboio baseado em sistemas veiculares ciber-físicos, carregam além dos benefícios, o impacto dos ataques cibernéticos que devem ser combatidos, uma vez que a segurança neste tipo de aplicação deve ser intenso, devido o envolvimento de risco de morte.

A transmissão de dados sem fio em PVCPS está suscetível a ataques de interceptação devido à característica de difusão ampla (broadcast) do rádio. Um veículo interceptador que esteja dentro do alcance de comunicação do PVCPS pode captar as transmissões do comboio e acessar informações sensíveis, como horário, localização, identificação do veículo, detalhes técnicos e outros dados da viagem, comprometendo a privacidade dos motoristas.

Os dados transmitidos nos PVCPS geralmente incluem informações cruciais de segurança relacionadas ao estado de condução. Com essas informações em mãos, o veículo interceptador pode realizar ataques de falsificação (spoofing) ou de reprodução (replay), inserindo mensagens de controle fraudulentas e manipulando padrões de mobilidade, como alterar a velocidade ou a direção do comboio. Essas ações poderiam colocar em risco a segurança e a eficiência do comboio, além de ameaçar a integridade de pedestres e outros veículos nas proximidades [3].

Nesta seção será relatado dois estudos que visam a manter a integridade dos dados trocados entre o comboio.

A. Protocolo distribuído de chave secreta

Em [3] é apresentado um estudo com foco na segurança durante a condução em que os PVCPS devem assegurar a confidencialidade na disseminação de dados para prevenir ataques de interceptação, além de garantir uma transmissão de informações ágil para o controle de cruzeiro e o gerenciamento do comboio, fazendo uso da segurança cooperativa de baixa latência (LLCS), fornecendo Confidencialidade e Pontualidade (CAT) na transmissão de dados em PVCPS.

O LLCS utiliza chaves unânimes geradas de forma cooperativa pelos veículos do comboio para proteger os dados transmitidos, garantindo criptografia e descryptografia eficazes. Para agilizar a transmissão, o LLCS otimiza a distribuição da taxa de transmissão em cada veículo, ajustando-se às mudanças temporais dos canais de comunicação em cada etapa, como demonstrado na figura 4. O desempenho da disseminação de dados é analisado com base na Probabilidade de acordo de chave, que reflete a eficiência e a confiabilidade na geração de chaves e na latência na disseminação, que avalia o tempo necessário para a transmissão dos dados.

O acordo de chave secreta no LLCS ocorre em três etapas:

a) *Estimativa de Canal*:: Os veículos do comboio medem a qualidade do canal entre o veículo líder e seu seguidor imediato, estimando o ganho do canal.

b) *Quantização do indicador de qualidade do canal (CQI)*:: A aleatoriedade do canal é convertida em vetores binários por meio de intervalos de quantização otimizados, maximizando a consistência entre os veículos.

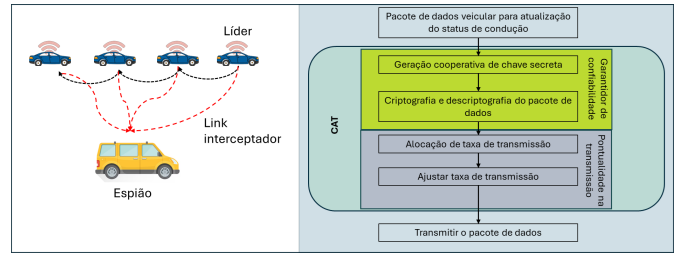


Fig. 4. Fluxo de mensagens em PVCPS: Comunicação do veículo líder aos seguidores, protegida por protocolo de segurança cooperativo contra interceptação.

c) *Acordo de Chave Secreta*:: Os veículos codificam o ganho do canal usando técnicas como Gray ou Gillham, gerando uma chave secreta simétrica compartilhada.

Para melhorar a eficiência e a pontualidade na disseminação segura de dados em PVCPS, o LLCS propõe uma alocação otimizada de taxa de transmissão de baixa latência. Essa abordagem garante uma transmissão rápida e confiável dos dados para cada veículo do comboio. Quando a transmissão é bem-sucedida, o veículo seguinte envia um reconhecimento (ACK); caso contrário, a taxa de transmissão é ajustada para retransmissão.

Taxas de transmissão muito altas podem acelerar o envio de dados, mas aumentam as perdas de pacotes (BER) e o consumo de energia. Por outro lado, taxas muito baixas tornam a transmissão mais lenta. Para equilibrar esses fatores, o LLCS otimiza a taxa de transmissão para minimizar a latência na disseminação de dados.

A alocação de taxa de transmissão gera dois cenários possíveis: transmissão bem-sucedida, em que a latência depende do tempo de transmissão da taxa alocada, ou falha na transmissão, em que a latência permanece igual à do veículo anterior. Para reduzir a latência total, a taxa de transmissão é ajustada com base no BER e na potência de transmissão, considerando as dependências entre veículos no comboio.

O LLCS usa programação dinâmica (DP) para calcular a taxa de transmissão ideal de forma recursiva, dividindo o problema em subproblemas interdependentes. Cada estado avaliado representa a latência acumulada pelos veículos anteriores. As soluções de cada subproblema são armazenadas em uma tabela de consulta, evitando cálculos redundantes. O algoritmo determina as taxas ideais começando pelo último veículo e retrocedendo até o líder, utilizando indução reversa.

As taxas de transmissão otimizadas podem ser pré-calculadas e armazenadas em uma tabela no veículo líder, que as compartilha com os demais veículos por meio de pacotes ou tokens. Informações como RSSI e CSI, disponíveis nos OBUs atuais, além de padrões como DSRC e ITS-G5, possibilitam a implementação do LLCS com mínimas modificações no hardware ou firmware, graças à adaptação dinâmica dos esquemas de modulação às condições do canal.

B. Blockchain

Em [11], é relatado o estudo com técnicas de blockchain, que originalmente foi desenvolvido para o Bitcoin, como sendo uma solução promissora para enfrentar os desafios de gerenciamento de reputação em redes veiculares, graças à sua descentralização, consistência e proteção contra adulterações. Essa tecnologia também se destaca na criação de um ecossistema ITS seguro e confiável, ao facilitar a confiança mútua entre as entidades por meio do consenso descentralizado sobre a validade dos dados.

Entre os métodos de consenso disponíveis, o Delegated Proof-of-Stake (DPoS) se destaca por ser eficiente, escalável e com baixa demanda computacional, tornando-o ideal para implementar a Internet de Veículos com suporte a blockchain (BIOV). Descreve o estudo em que o DPoS foi adaptado para incentivar maior participação das RSUs no sistema BIOV, embora não tenha abordado as exigências de tempo real no gerenciamento de reputação em redes veiculares e ainda outro estudo com um sistema de confiança descentralizado baseado em blockchain, utilizando uma combinação de Proof-of-Work (PoW) e Proof-of-Stake (PoS) para atualizar rapidamente os valores de reputação dos veículos, que contém limitações, como a dependência de RSUs para o processo de consenso, o que pode ser inviável em cenários sem essas unidades. Além disso, o esquema gera um alto overhead de comunicação, já que cada veículo precisa reportar suas avaliações sobre outros veículos às RSUs.

O estudo em [11], apresenta um esquema de atualização do líder de comboio veicular para prevenir ataques internos, como a exclusão de líderes maliciosos. Por meio de um sistema de gerenciamento de reputação baseado em blockchain em redes veiculares, o esquema avalia a reputação de cada membro do comboio de forma ágil. A estrutura do bloco e o processo de consenso do blockchain são projetados para reduzir significativamente o uso de recursos de comunicação sem fio em comparação com esquemas de gerenciamento de reputação existentes, eliminando a necessidade de os veículos transmitirem suas avaliações sobre outros.

1) *Estrutura:* Em [11], O blockchain é amplamente reconhecido como uma inovação disruptiva, com potencial significativo para aplicações em finanças, economia e sistemas sociais em larga escala. O esquema de consenso DPoS é especialmente indicado para a criação de uma Internet de Veículos baseada em blockchain (BIOV). Com isso, foi desenvolvido um sistema de blockchain utilizando DPoS para gerenciar a reputação em comboios veiculares, onde as transações representam ajustes de reputação calculados, e os mineradores são escolhidos entre os membros do comboio.

A estrutura do blockchain funciona da seguinte forma: o bloco gênese, ou primeiro bloco, é gerado durante a inicialização do sistema, atribuindo a todos os membros do comboio o mesmo valor inicial de reputação, exemplo: +5. Após essa etapa, os mineradores iniciam o processo de geração de blocos onde cada bloco segue o mesmo formato, composto por um cabeçalho e um corpo.

O cabeçalho, de acordo com o esquema de consenso DPoS, inclui uma referência ao bloco anterior, a hora atual em GMT, a raiz de Merkle dos ajustes de reputação e uma assinatura criada com a chave privada do minerador, conforme demonstrado na figura 5. Para que o bloco seja válido, sua assinatura deve ser verificada. O corpo do bloco contém o identificador do líder atual do comboio e uma lista de transações que registra os ajustes de reputação gerados pelos mineradores. Cada ajuste de reputação é apresentado no formato (ej, Ik, ajuste de reputação, valor geral de reputação), onde Ik é o identificador do veículo k, membro do comboio, relacionado ao evento ej. O valor geral de reputação registrado na última transação confirmada reflete o status atual de reputação do membro do comboio.

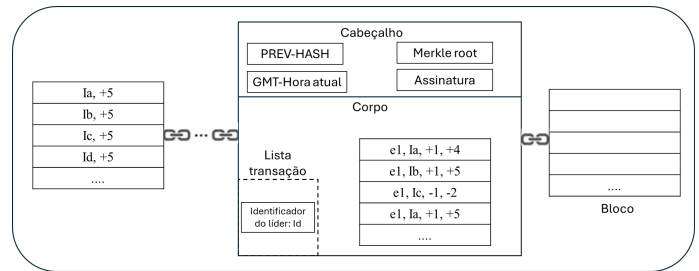


Fig. 5. Estrutura blockchain

2) *Etapas atualização do comboio baseado em blockchain:* O estudo em [11], apresenta o esquema que reduz consideravelmente o overhead de comunicação em comparação com métodos tradicionais, eliminando a necessidade de troca direta de informações de reputação entre os veículos, com a atualização do líder de comboio veicular baseado em blockchain, organizado em cinco etapas principais:

a) *Etapa 1: Configuração do Sistema:* Cada veículo do comboio é equipado com uma Unidade de Bordo (OBU). Utilizando tecnologia da Internet das Coisas (IoT), chips específicos nas OBUs transformam esses dispositivos em plataformas de mineração conectadas à rede blockchain. O sistema opera como uma rede peer-to-peer (P2P), onde cada membro do comboio funciona como um nó cliente completo. Antes do início do blockchain, o sistema emprega assinaturas digitais baseadas em curvas elípticas e criptografia assimétrica. Após a autenticação de identidade realizada por uma Autoridade de Confiança (TA), os membros recebem chaves públicas e privadas, além de certificados para comunicações criptografadas. Todos os membros autenticados, exceto aqueles na lista negra, podem atuar como candidatos a mineradores e eleitores no modelo de consenso DPoS.

b) *Etapa 2: Cálculo da Reputação:* Os membros do comboio monitoram continuamente seus próprios ajustes de reputação e os dos demais membros. Após cada rodada do processo de consenso, um novo bloco é recebido, e os ajustes de reputação locais mais antigos que o horário GMT do bloco são descartados. Os valores de reputação registrados na última transação confirmada no blockchain são usados pelos eleitores para selecionar novos líderes de comboio, combinando-os com ajustes de reputação locais ainda não verificados.

c) *Etapla 3: Seleção de Mineradores e Atualização do Líder:* Os eleitores escolhem k candidatos a mineradores com base nos valores finais de reputação. O número k é ímpar, e todos os eleitores possuem peso igual no processo de votação. Após a contagem, os k candidatos mais bem avaliados formam o novo grupo de mineradores. Essa etapa é executada somente quando o valor geral de reputação de um minerador cai abaixo de um limite predefinido ou quando um minerador não consegue produzir blocos. Caso o líder atual não esteja no novo grupo, o minerador com a maior reputação geral é eleito como novo líder, enquanto os líderes anteriores são adicionados à lista negra.

d) *Etapla 4: Geração de Blocos:* Os mineradores revezam-se na geração de blocos. Em cada intervalo de tempo, um minerador cria um bloco não verificado e o transmite aos outros mineradores, que agem como verificadores. Em seguida, o minerador que gerou o bloco assume o papel de verificador, e outro minerador passa a gerar o próximo bloco.

e) *Etapla 5: Processo de Consenso:* Após receber um bloco não verificado, os verificadores analisam sua lista de transações, comparando cada item de ajuste de reputação com seus registros locais. Se a lista de transações estiver correta, o verificador envia uma resposta positiva assinada ao gerenciador do bloco; caso contrário, envia uma resposta negativa. O gerenciador do bloco avalia as respostas recebidas e valida o bloco se mais de dois terços forem positivas. Caso contrário, o gerenciador é substituído e adicionado à lista negra. Durante esse processo, os membros do comboio geram ajustes de reputação positivos para verificadores que participaram corretamente e negativos para aqueles que não atuaram adequadamente.

IV. TRABALHOS FUTUROS

Em trabalhos futuros, poderá ser aprofundado a aplicação, como em [12], que trata da sexta geração de redes de comunicação (6G) e que marca uma transformação profunda na conectividade veicular, posicionando-se como um catalisador essencial para a evolução das comunicações V2X. Essa tecnologia visa não apenas atender às demandas de veículos autônomos conectados, mas também abrir caminho para soluções revolucionárias, como interfaces aéreas mais robustas, computação distribuída e inteligência artificial integrada, adaptando-se a ambientes altamente dinâmicos. O 6G promete taxas de transmissão em escala de terabits por segundo, confiabilidade ultrarrápida e comunicação de latência quase nula, habilitando casos de uso futurísticos, como a interação cérebro-veículo, comunicação tátil que integra percepção sensorial em tempo real e sistemas de sensores avançados combinados com mapeamento e localização de precisão milimétrica. Além disso, tecnologias emergentes, como superfícies reflexivas inteligentes (IRSs), blockchain e comunicação em espectros de terahertz, reforçarão a segurança, a eficiência energética e a cobertura em cenários urbanos e rurais. Espera-se que esses avanços sejam ainda mais explorados no que tange as redes PVCPS, com foco na integração de sistemas heterogêneos, no uso de inteligência artificial para decisões em tempo real e

no desenvolvimento de soluções que enfrentem desafios de alocação eficiente de recursos, confiabilidade em ambientes adversos e sustentabilidade energética, consolidando o 6G como a base para sistemas de transporte verdadeiramente inteligentes, seguros e sustentáveis.

V. CONCLUSÃO

Com base nos conceitos e análises apresentados, conclui-se que os sistemas de comboios baseados em redes veiculares ciber-físicas (PVCPS) representam uma solução promissora para melhorar a eficiência, segurança e sustentabilidade do transporte rodoviário. Esses sistemas integram avanços em tecnologias de comunicação, computação e controle, permitindo a coordenação em tempo real entre os veículos, o que reduz o consumo de energia, aumenta a capacidade das rodovias e minimiza riscos de acidentes.

Adicionalmente, a utilização de protocolos como o LLCS e o blockchain para o gerenciamento de segurança e reputação dentro dos comboios demonstra ser uma abordagem eficaz para mitigar riscos de ataques cibernéticos e assegurar a confiabilidade das operações. A geração e distribuição otimizada de chaves secretas, aliada à descentralização e consistência do blockchain, garante maior robustez ao sistema, diminuindo a necessidade de troca constante de dados entre os veículos e reduzindo o overhead de comunicação.

Nesse contexto, o avanço das redes de comunicação para a sexta geração (6G) promete trazer uma revolução para os PVCPS. Com taxas de transmissão em escala de terabits por segundo, confiabilidade ultrarrápida e comunicação de latência quase nula, o 6G possibilitará a coordenação ainda mais precisa entre os veículos e a adoção de tecnologias como superfícies reflexivas inteligentes (IRSs) e comunicação em espectros de terahertz. Essas inovações também reforçarão a segurança, eficiência energética e cobertura em cenários urbanos e rurais, viabilizando novos casos de uso, como interação cérebro-veículo e sensores integrados para mapeamento de alta precisão.

Embora desafios técnicos e de implementação ainda existam, como a necessidade de maior integração com infraestruturas viárias e a adaptação dinâmica às condições de tráfego, o progresso contínuo em tecnologias de redes veiculares e sistemas inteligentes fortalece o potencial de adoção dos PVCPS em larga escala. Dessa forma, esses sistemas, aliados ao potencial transformador do 6G, representam um passo significativo em direção a um futuro de transporte mais conectado, eficiente e seguro.

REFERÊNCIAS

- [1] Jia, Dongyao, et al. "A survey on platoon-based vehicular cyber-physical systems." *IEEE communications surveys & tutorials* 18.1 (2015): 263-284.
- [2] Wan, Jiafu, et al. "Context-aware vehicular cyber-physical systems with cloud support: architecture, challenges, and solutions." *IEEE Communications Magazine* 52.8 (2014): 106-113.
- [3] Li, Kai, et al. "Confidentiality and timeliness of data dissemination in platoon-based vehicular cyber-physical systems." *IEEE Network* 35.4 (2021): 248-254.

- [4] Xiao, Shunyuan, et al. "Secure distributed adaptive platooning control of automated vehicles over vehicular ad-hoc networks under denial-of-service attacks." *IEEE Transactions on Cybernetics* 52.11 (2021): 12003-12015.
- [5] Wu, Jia, Fei Yan, and Jianxing Liu. "Effectiveness proving and control of platoon-based vehicular cyber-physical systems." *IEEE Access* 6 (2018): 21140-21151.
- [6] Yuan, Z. H. A. O., et al. "Distributed resilient platoon control of vehicular cyber physical systems subject to DoS attacks." 2020 39th Chinese control conference (CCC). IEEE, 2020.
- [7] Tiganasu, Alexandru, Corneliu Lazar, and Constantin Florin Caruntu. "Cyber physical systems-oriented design of cooperative control for vehicle platooning." 2017 21st International Conference on Control Systems and Computer Science (CSCS). IEEE, 2017.
- [8] Zhao, Yuan, Zhongchang Liu, and Wing Shing Wong. "Resilient platoon control of vehicular cyber physical systems under DoS attacks and multiple disturbances." *IEEE Transactions on Intelligent Transportation Systems* 23.8 (2021): 10945-10956.
- [9] Sargolzaei, Arman, et al. "A machine learning approach for fault detection in vehicular cyber-physical systems." 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA). IEEE, 2016.
- [10] El-Zaher, Madeleine, Baudouin Dafflon, and Franck Gechter. "A cyber-physical model for platoon system." 2015 9th International Conference on Software, Knowledge, Information Management and Applications (SKIMA). IEEE, 2015.
- [11] Ji, Yongxin, et al. "A blockchain-based vehicle platoon leader updating scheme." ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, 2020.
- [12] Noor-A-Rahim, Md, et al. "6G for vehicle-to-everything (V2X) communications: Enabling technologies, challenges, and opportunities." *Proceedings of the IEEE* 110.6 (2022): 712-734.