Recuperação do Serviço de Pelotão de Veículos Autônomos e Conectados Baseado em Modelos Virtuais Contra Ataques na Rede e Sensores

Everaldo Andrade[1], **Aldri Santos**[1]

[1]Depto. de Ciência da Computação – Universidade Federal de Minas Gerais (UFMG)

{everaldo.andrade, aldri}@dcc.ufmg.br

Abstract. *Platoon formation of autonomous and connected vehicles (CAVs) is the most common topological structure of CAVs, where vehicles travel relatively close together, responding to the leader's commands and providing autonomous and intelligent transport services. However, with the evolution of CAV platoons, various types of attacks that inject false data into networks and sensors have compromised platoon stability, resulting in fragmentation or, in the worst case, serious collisions. This work proposes a mechanism, called PReCAV, for the cooperative recovery of CAVs platoon against false data injection attacks, supported by virtual and physical models of the system, in order to maintain resilience in the midst of network and sensor attacks. A simulation evaluation showed that PReCAV maintained the stability of the platoon by providing resilience, depriving it of variations of 4.42m/s^2 of acceleration, 13m/s of speed and 40m of distance between vehicles in attacks in the network and variations of 4.43m/s^2, 10.7m/s and 33.4m in sensor attacks.*

Resumo. *A formação em pelotão de veículos autônomos e conectados (VACs) é a estrutura topológica mais comum de VACs, onde veículos trafegam relativamente próximos, respondendo aos comandos do líder e provendo serviços de transporte autônomo e inteligente. Contudo, com a evolução dos pelotões de VACs vários tipos de ataques de injeção de dados falsos em redes e sensores têm comprometido a estabilidade do pelotão, resultando na fragmentação ou, no pior caso, em serias colisões. Este trabalho propõe um mecanismo, denominada PReCAV, para a recuperação cooperativa de pelotão de VACs diante de ataques de injeção de dados falsos, apoiada por modelos virtuais e físicos do sistema, a fim de manter resiliência em meio à ataques em rede e sensores. Uma avaliação por simulação mostrou que o PReCAV manteve a estabilidade do pelotão ao prover resiliência, privando-o de variações de 4,42m/s^2 de aceleração, 13m/s de velocidade e 40m de distância entre veículos em ataques na rede e variações de 4,43m/s^2, 10,7m/s e 33,4m em ataques nos sensores.*

1. Introdução

As pesquisas em sistemas de veículos autônomos e conectados (VACs) vem ganhando mais atenção das industrias e academias devido ao seu potencial em auxiliar a reduzir os acidentes fatais [Chen et al. 2019, Rana and Hossain 2021, Khan et al. 2022], restringir a intervenção humana na condução, e à automatização dos serviços de mobilidade urbana. A implantação de veículos autônomos colabora ao desenvolvimento

de serviços e aplicações em Sistemas de Transporte Inteligente Colaborativos voltados ao domínio de segurança e entretenimento. A taxa de inserção de veículos autônomos no mercado está prevista entre 24% e 87% em 2045 [Morando et al. 2018], e uma das aplicações fundamentais em VACs consiste da condução autônoma de veículos em pelotão ("comboio"), em que veículos trafegam coordenadamente em um mesmo sentido sem qualquer ligação mecânica mantendo uma distância segura [Maiti et al. 2020].

No pelotão de VACs, os veículos operam na troca de informações e estabelecimento da comunicação, normalmente em modo *Vehicle to Vehicle (V2V)* ou *Vehicle to Infrastructure (V2I)*, a fim de manter o pelotão estável. A estrutura topológica de um pelotão de VACs compreende o papel do *veiculo líder*, responsável por coordenar a condução através de troca de comandos com os demais veículos do pelotão, e os *veículos membros (ou seguidores)*, quem recebem e executam os comandos do líder em tempo real [Back et al. 2019]. Os algoritmos de pelotão reúnem um conjunto de operações que são essenciais para garantir a segurança e eficiência da condução. Estas operações compreendem as operações realizadas com o pelotão, são operações convencionais realizadas durante a condução e no mesmo pelotão (e.g. des/aceleração, frenagens e mudanças de faixa), e as operações de mudança de estrutura, são as que afetam a estrutura topológica do pelotão (e.g. entrada/saída de veículos e mesclagem de pelotões) [Fakhfakh et al. 2020].

Os sistemas de veículos em pelotão demandam por alta tolerância a falhas em razão das graves consequências geradas em casos de falhas. Logo, requisitos como alta disponibilidade, confiabilidade e segurança são fundamentais para que os VACs em pelotão transitem em alta velocidade nas malhas viárias [Böhm and Kunert 2016]. Uma simples falha ou atraso na comunicação pode gerar interrupção das operações e levar o sistema a um estado crítico, como sua fragmentação. Uma coordenação confiável do sistema de VACs exige a corretude e a integridade dos dados coletados e compartilhados através dos sensores e da rede, a fim de representar o estado real do sistema e do ambiente [Yang and Lv 2021]. O processamento dos dados coletados e as informações são geradas para que decisões sejam tomadas e levem a um estado correto do sistema. As decisões devem ser transmitidas corretamente e em tempo real, através de comandos, entre veículos do pelotão. Assim, dois momentos críticos no sistema são as *leitura dos sensores* sobre o estado do sistema e do ambiente para que decisões sejam tomadas pelos veículos e as *transmissões de decisões na rede* entre os veículos para execução das operações no sistema de VACs em pelotão.

Entretanto, com a evolução dos sistemas de pelotão de VACs, diferentes tipos de ataques como injeção de dados falsos na rede e nos sensores são reportados. Por exemplo, GPS spoofing [Tippenhauer et al. 2011, Trippel et al. 2017], é um tipo de ataque em sensor físico que engana o receptor do sinal GPS através de injeção de sinais de GPS falsos. Em [Shoukry et al. 2013] os atacantes corromperam o sistema de freios antitravamento (do inglês *Antilock Braking System - ABS*) injetando campos magnéticos nos sensores de velocidade das rodas. Além dos ataques em sensores, outros tipos de ataques contribuem no desafio de tornar estes sistemas tolerantes a falhas, como os ataques de injeção de dos falsos entre os veículos em rede [Onishi 2018]. Diferentemente dos ciber ataques em computadores, os ataques em sistemas ciber-físicos, como sistemas de veículos autônomos e conectados, resultam não apenas ao vazamento de informações mas também à desastres físicos [He et al. 2020]. Desta forma, surge a necessidade de estratégias de

defesa que mantenham estes sistemas disponíveis em meio à diferentes tipos de ataques.

Em geral as estratégias existentes focam apenas na detecção do ataque externo [Choi et al. 2018, Junejo and Goh 2016, Mitchell et al. 2015], ao invés de tratar da resiliência do sistema durante o ataque. Outros consideram a resiliência em sistemas não distribuídos, como em [Choi et al. 2020], que propôs uma técnica de recuperação de sensores de veículos robóticos (e.g. *drones* e carros) baseado em sensores *"softerizados"* para representar e predizer os estados dos sensores físicos e, em caso de ataque, o sensor *"softerizado"* assume a atividade a fim de manter o estado operacional do veículo. Contudo, o trabalho não foca na recuperação cooperativa do estado de um sistema distribuído, como um sistema em pelotão de VACs, sob ataques em sensores físicos e na rede. E isso pode gerar inconsistência das informações coletadas e transmitidas pelos veículos e, assim, levar o sistema a um estado crítico, como fragmentação ou colisão do pelotão.

Este trabalho propõe um mecanismo, denominado PReCAV (***P**latoon **Re**covery of **C**onnected and **A**utonomous **V**ehicle*), para a recuperação cooperativa de sistemas de VACs em pelotão contra perturbações externas e continuas ao longo do tempo decorrentes de injeção de dados falsos em sensores embarcados nos veículos e na rede de comunicação. Ela baseia-se em modelos virtuais e físicos do sistema, que auxiliam na detecção de tais ataques e na predição dos estados dos veículos no sistema, a fim de manter a resiliência das operações no pelotão durante a condução. Resultados simulados no NS3 e SUMO mostram que a *PReCAV* manteve a estabilidade do pelotão, privando-o de variações de 9,6m/s de velocidade e 23,4m de distância entre veículos em ataques de injeção de dados falsos na rede e variações de 6,6m/s e 21,94m em ataques nos sensores.

O restante do artigo está estruturado da seguinte maneira: A Seção 2 apresenta os trabalhos relacionados. A Seção 3 apresenta o algoritmo de pelotão de veículos autônomos e conectados adotado neste trabalho. A Seção 3.2 descreve a arquitetura e funcionamento do mecanismo proposto. A Seção 4 detalha a metodologia de avaliação e os resultados alcançados. A Seção 5 apresenta as considerações finais e trabalhos futuros.

2. Trabalhos Relacionados

Na literatura as pesquisas aplicadas em sistemas de pelotões de VACs têm dedicado esforços no estudo da sua estrutura topológica, da formação à manutenção do pelotão, e da segurança, a fim de assegurar resiliência em meio a perturbações no pelotão. Em [Yao et al. 2020], os autores desenvolveram uma estratégia para a formação e controle de pelotões em ambientes com veículos autônomos e não-autônomos, onde um veículo não-autônomo, conduzido manualmente, comanda os veículos autônomos operados em pelotão. A estratégia segue uma estrutura de modelo multi-regime com três estágios (percepção, planejamento e atuação), onde cada estágio opera em conjunto na formação e manutenção do pelotão. Já os autores em [Back et al. 2019] apresentaram um método em tempo real para a análise e seleção de candidatos a lideres do pelotão com base no contexto real da rede. O trabalho apodera-se do fato dos pelotões não se adaptarem rapidamente à situações de emergências e utiliza o algoritmo de consenso *Raft* para a seleção do líder adequado ao contexto. Em [Maiti et al. 2020], um estudo sobre os impactos das operações de formações de pelotões no tráfego e o impacto do tráfego nas operações de formação. Eles levaram em conta três tipos de operações de mesclagem no pelotão (frontal, central e final) sob diferentes densidades e velocidades de

veículos nos cenários, porém ignoraram a presença de eventos anômalos como ataques de injeção de dados de dados falsos na rede ou nos sensores. Em [Bang and Ahn 2017], foi proposta uma estratégia de formação e evolução de pelotão de veículos autônomos e conectados (PsCAV) baseada em aprendizagem comportamental do movimento coletivo de animais ou insetos (*Swarm Intelligence*). O trabalho associa tais comportamentos com um sistema físico Mola-Massa-Amortecedor a fim de manter a estabilidade do sistema de pelotão. Em [Mushtaq et al. 2021] desenvolveu-se uma abordagem baseada em *Swarm Intelligence* para a formação e evolução de pelotões a fim de manter o fluxo do trafego durante congestionamento e evitar colisões ao utilizar comunicações V2V e V2I. Em [Amoozadeh et al. 2015] foi desenvolvido e implementado um protocolo de gerenciamento de pelotão em rede veiculares que utiliza três operações básicas: mesclagem, fragmentação e mudança de faixa, que podem apoiar operação no pelotão, como entrada e saída de veículos. Contudo, os trabalhos acima ignoram a ocorrência de ataques de injeção de dados falsos na rede ou nos sensores embarcados, como geração de interferências, e portanto não tratam da resiliência do sistema de pelotão em meio à tais ataques.

A dependência dos sensores e da comunicação veicular nos pelotões de VACs expõe o sistema à novos ataques, e isso aumenta a sua vulnerabilidade e os tornam alvos fáceis de ciber ataques. Em [Yang and Lv 2021] foi proposto um algoritmo de fusão de sensores capaz de prover estimativas de erros reduzidos e independente dos sinais de ataques nos sensores. Ele explora características de redundância de sensores a fim de detectar e isolar o sensor atacado do VAC no pelotão. Contudo, o trabalho não considera ataques de injeção de dados falsos na rede. Em [Sun et al. 2021], um *framework* para detecção e mitigação de ataques de rede fim-a-fim coleta dados para treinar um modelo de rede neural denominado detector de anomalia. Este *framework* emprega os conceitos de Teoria dos Jogos e de equilíbrio de Nash na reconfiguração do sistema de controle do veículo para mitigar o ataque de rede. Em [Ko and Son 2021], um método de detecção de ataque denominado *LMID (Long short-term memory (LSTM) based Malicious Information Detection* baseia-se nas informações maliciosas transmitidas na rede provenientes dos veículos membros do próprio pelotão. Para a detecção, eles definiram ataques correlacionados e não-correlacionados e treinaram um modelo de rede neural profunda utilizado em cada veículo no teste. No entanto, os dois últimos trabalhos não consideram ataques injeção de dados falsos nos sensores e nem tratam da resiliência do sistema pós ataque. Em [Böhm and Kunert 2016], um *framework* para comunicação oportuna e confiável inter/intra-pelotão denominado DA-RE (*Data Age based REtransmission scheme*) utiliza um canal de controle e um de serviços para dar suporte à requisitos específicos do pelotão. Os autores em [Fernandes and Nunes 2012], propuseram algoritmos para reduzir atrasos de comunicação em pelotões de veículos a fim de realizar operações, como separação e mesclagem de pelotões, de forma estável e segura. Entretanto, estes trabalhos não assumem ocorrência de ataques externos na rede e nos sensores.

Desta forma, diferente dos trabalhos acima que focam apenas na detecção de ataques na rede ou nos sensores dos veículos, este artigo apresenta um mecanismo de detecção e correção cooperativa de dados falsos para a recuperação de serviços de pelotões de VACs baseados em modelos virtuais e físicos do pelotão, e assim garantir a resiliência do pelotão em meio à ataques na rede e nos sensores.

3. PReCAV: Um Mecanismo de Recuperação do Serviço de Pelotão de VACs

Esta seção descreve o mecanismo PReCAV (**P**latoon **Re**covery for **C**onnected and **A**utonomous **V**ehicles), para a recuperação cooperativa do serviço de pelotão de veículos autônomos e conectados (VACs). O PReCAV baseia-se nos modelos virtual e físico do sistema de pelotão para detectar e corrigir informações falsas provenientes de ataques de injeção de dados falsos na rede e nos sensores embarcados nos veículos. Inicialmente é descrito o modelo do sistema de pelotão utilizado neste trabalho. Em seguida, são apresentados a arquitetura e o funcionamento PReCAV.

3.1. Sistema de Pelotão de VACs

A formação topológica em pelotão dos VACs leva em conta a estratégia PsCAV para organização e evolução do sistema de pelotão proposta em [Bang and Ahn 2017]. O PsCAV visa manter o desempenho e a estabilidade do pelotão. O PsCAV se inspira no conceito de *Swarm Intelligence*, que estuda o comportamento auto-organizacional de grupos ou colônias de seres vivos, tais como formigas, abelhas, lobos e outros sistemas naturais, e descrevem por meio de aprendizado como tais seres movimentam-se coletivamente. Estes seres vivos exercem movimentos em conjunto (e.g. pelotão) sem que haja colisões entre eles. Esta estratégia compreende a existência de três zonas formadas com base no conjunto de regras de movimento coletivo de animais: 1) Zona de Atração: onde animais tendem a se aproximar, em razão da baixa proximidade, para evitar desgarramento do grupo; 2) Zona de Alinhamento: onde animais tendem a sincronizar suas velocidades e manter um espaçamento mínimo uns com os outros; e 3) Zona de Repulsão: onde animais tendem a se afastar uns dos outros, em razão da alta proximidade, para evitar colisões, como ilustra a Figura 1(a).

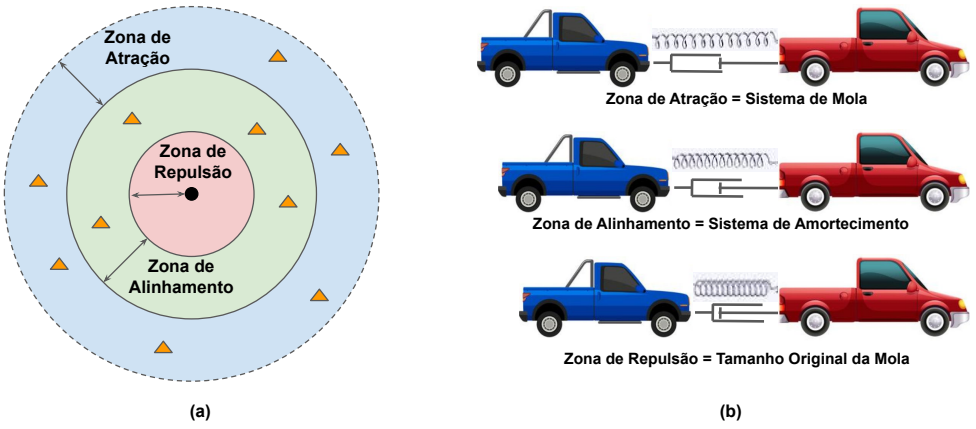

Figura 1. Relação *Swarm Intelligence* e Sistema MMA em VACs

O PsCAV associa o comportamento de tais zonas com um sistema Mola-Massa-Amortecedor (MMA), como ilustra a Figura 1(b). Na Zona de Atração, o veículo autônomo com baixa proximidade, tende a se aproximar (atrair) do veículo predecessor por meio do sistema de mola, provocando uma aceleração. Na Zona de Alinhamento, o veículo tende a manter aceleração, velocidade e distância controlada com o veículo à frente por meio do controle de sistema de mola e amortecedor. Na Zona de Repulsão, o veículo com alta proximidade, tende a se afastar do predecessor por meio do sistema de amortecimento, provocando uma desaceleração. O PsCAV coordena a formação e

evolução do pelotão através do controle da constante de mola e do coeficiente de amortecimento do sistema MMA. A Figura 2 ilustra a operação do PsCAV. Cada veículo do pelotão encontra-se virtualmente conectado com uma mola e um amortecedor, e as forças exercidas por elas são calculadas em cada veículo, com base nos dados transmitidos pelo veículo predecessor, para definir sua aceleração ou desaceleração, e assim controlar a velocidade, bem como a distância entre o predecessor.

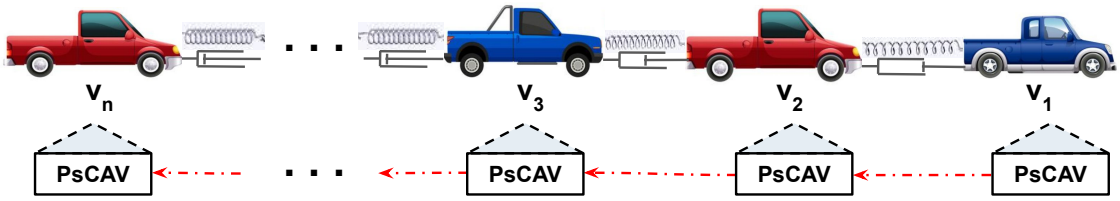

Figura 2. Operação de pelotão de VACs com PsCAV

Contudo, nota-se na operação do PsCAV a dependência crítica da veracidade e integridade dos dados compartilhados entre os veículos, tornando-se uma vulnerabilidade em razão da alta dinamicidade e ameaças à ataques presentes em redes veiculares que comprometem os dados transmitidos. Portanto, caso dados falsos produzidos e entregues por atacantes sejam assumidos como verdadeiros por um veiculo receptor do pelotão, todo pelotão será comprometido resultando na fragmentação ou, no pior caso, em colisões.

3.2. Asserções, Arquitetura e Funcionamento do PReCAV

O PReCAV opera de forma distribuída pelo compartilhamento das informações dos veículos do pelotão e mantém um modelo virtual e físico do pelotão para checagem dupla da veracidade das informações entregues e transmitidas entre os veículos, a fim de manter o sistema no estado estável, isto é, sem variações drásticas de aceleração, velocidade e distância definida pelo sistema de pelotão em meio à perturbações externas. Assume-se que os VACs são equipados com sensores capaz de prover informações de aceleração, velocidade e distância própria e dos seus vizinhos. Além disso, como ocorre em rede veiculares reais, assume-se que estes sensores estão sujeitos à falhas malignas (ataques maliciosos) distribuídas no sistema ao longo do tempo e espaço físico. Ademais, considera-se que: *As.1)* cada veículo conhece sua ordem no pelotão; *As.2)* os ataques na rede e nos sensores são mutuamente exclusivos no mesmo veículo e instante de tempo, i.e. um veículo não sofre um ataque na rede e nos sensores ao mesmo tempo; *As.3)* os ataques são de origem externa e os VACs nunca são invadidos; *As.4)* os sensores só descalibram sob ataques. Em paralelo à operação do PReCAV, o sistema de pelotão PsCAV funciona normalmente consumindo os dados verdadeiros disponibilizados pelo PReCAV e abstraindo o funcionamento deste. O PReCAV prover uma camada de segurança para estratégias de sistemas de pelotões de VACs, as quais utilizam apenas dados validados pelo PReCAV.

A arquitetura do PReCAV, ilustrada na Figura 3, consiste em quatro componentes: Virtual, Físico, de Checagem, e de Comunicação. *O Componente Virtual* (VI) configura e guarda os parâmetros do modelo virtual (MV) do sistema no PReCAV, que calcula a aceleração, velocidade instantâneas e distância entre o veículo predecessor. *O Componente Físico* (FI) configura e mantém o modelo físico (MF) do sistema no PReCAV,

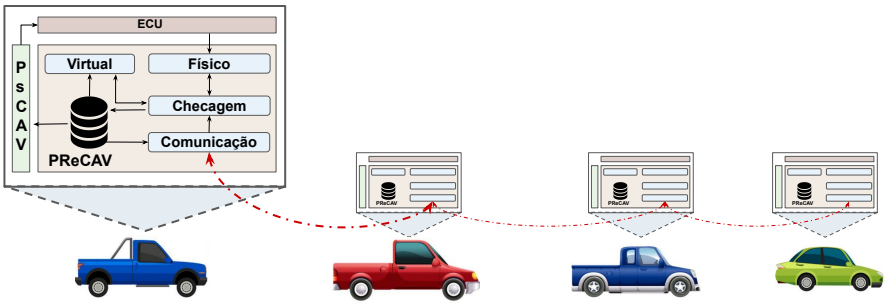

Figura 3. Arquitetura do PReCAV

e baseia-se nas informações próvidas pelos sensores embarcados através da unidade de controle eletrônico (ECU) do veículo. *O Componente de Checagem* (CH) é responsável por detectar e corrigir dados falsos entregues através do mecanismo de recuperação cooperativa e checagem dupla entre modelo físico e virtual do sistema de pelotão. Os dados validados pelo CH são armazenados em uma base de dados e disponibilizados ao sistema de pelotão PsCAV. *O Componente Comunicação* (CO) coordena a entrega e envio das mensagens entre os veículos do pelotão. As mensagens entregues são passadas para o CH enquanto que as mensagens enviadas são consumidas da base de dados. O sistema de pelotão PsCAV leva em conta apenas as informações da base de dados para atuar diretamente, através da comunicação com a *ECU*, no comportamento de aceleração ou desaceleração do veiculo no pelotão.

O PReCAV considera um sistema de pelotão de VACs composto por um conjunto de veículos $V = \{v_1, v_2, v_3, ..., v_n\}$, onde n corresponde ao tamanho do pelotão, v_1 é o líder e os demais $v_2, ...v_n$ são seguidores, como ilustra a Figura 4. Os veículos transitam próximos seguindo na mesma direção. Cada veículo opera com o sistema de pelotão PsCAV que se comunica diretamente com o seu PReCAV para a recuperação de pelotão. O PReCAV compartilha informações com o veículo predecessor a fim de prover informações corretas para o sistema de pelotão. Com o PReCAV, o veículo mantém um modelo virtual e físico dele mesmo e do veículo predecessor no sistema, os quais são utilizados para checar a veracidade das informações entregues.

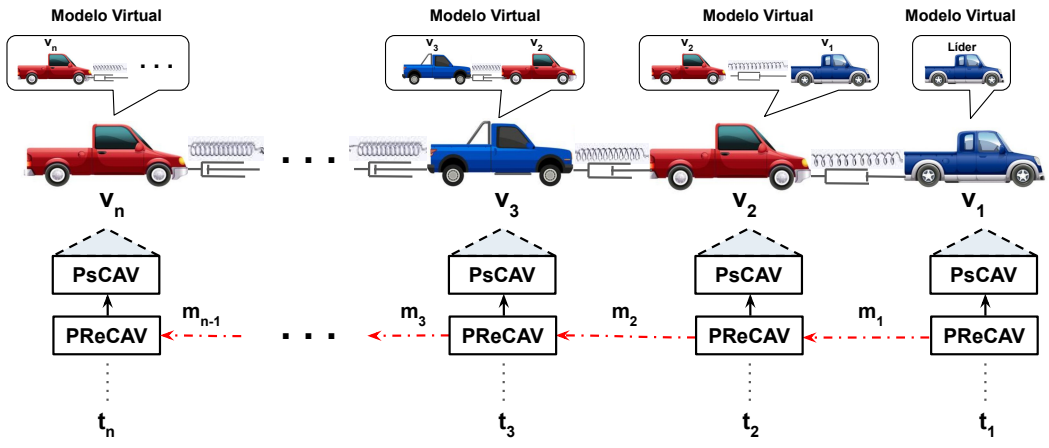

Figura 4. Funcionamento do PReCAV

O modelo virtual do PReCAV aplica fórmulas da mecânica clássica a fim de estimar valores de grandeza no instante atual. Assim, dado um veículo v_i, o modelo virtual calcula a velocidade (v_{v_i}) e aceleração (a_{v_i}) instantâneas de v_i e do seu predecessor, pelas Equações (1) e (2), onde $s_{0_{v_i}}$ e $v_{0_{v_i}}$ correspondem à posição e velocidade inicial do veículo, respectivamente, e t o instante de tempo considerado. O modelo também calcula a distância de v_i com seu predecessor v_{i-1} pela Equação 3, onde s_{v_i} e $s_{v_{i-1}}$ correspondem às posições iniciais de v_i e v_{i-1} respectivamente, conforme a Equação 4. O modelo físico do PReCAV mensura as grandezas de aceleração, velocidade e distância entre os veículos por meio da Unidade de Controle Eletrônico (*Electronic Control Unit - ECU*) do veículo, o qual opera na coordenação dos módulos de sensores e atuadores do veículo.

$$v_{v_i} = \lim_{\Delta t \to 0} \frac{\Delta s_{v_i}}{\Delta t} = \frac{d(s_{0_{v_i}} + v_{0_{v_i}} t + 1/2 a_{v_i} t^2)}{dt} = v_{0_{v_i}} + a_{v_i} t \tag{1}$$

$$a_{v_i} = \lim_{\Delta t \to 0} \frac{\Delta v_{v_i}}{\Delta t} = \frac{d(v_{0_{v_i}} + a_{v_i} t)}{dt} \tag{2}$$

$$dist_{i,i-1} = s_{v_{i-1}} - s_{v_i} \tag{3}$$

$$\begin{aligned} s_{v_i} &= s_{0_{v_i}} + v_{0_{v_i}} t + 1/2 a_{v_i} t^2 \\ s_{v_{i-1}} &= s_{0_{v_{i-1}}} + v_{0_{v_{i-1}}} t + 1/2 a_{v_{i-1}} t^2 \end{aligned} \tag{4}$$

Conforme a Figura 4, o PReCAV funciona sob o sistema de pelotão PsCAV. Pela asserção (As.1), o veículo líder v_1 envia a mensagem m_1 para o seu sucessor v_2, no instante t_1, com suas propriedades físicas. Ao receber m_1 no instante t_2, pela asserção (As.3), o veículo v_2 verifica se os dados de m_1 correspondem aos valores calculados pelos modelos virtual e físico do PReCAV. Caso a mensagem m_1 passe pela estratégia de dupla checagem (MV(V) e MF(V)), ela é assumida como verdadeira (M(V)) e disponibilizada ao PsCAV. Caso a verificação falhe apenas no modelo virtual (MV(F) e MF(V)), assume-se que m_1 é verdadeira e será disponibilizada ao PsCAV, e o modelo virtual (MV) será atualizado pelo modelo físico porque falhou na verificação da mensagem verdadeira. Se a verificação falhar apenas no modelo físico (MV(V) e MF(F)), o PReCAV checa se v_2 sofre um ataque nos seus sensores. Esta verificação procede por meio da comparação entre os modelos virtual e físico com as informações de propriedade de v_2. Na comparação, pela asserção (As.4), uma incompatibilidade entre as propriedades físicas de v_2 mantidas em seus modelos significa que v_2 sofre um ataque nos sensores e, pela asserção (As.2), m_1 é verdadeira e será disponibilizada ao PsCAV. Caso contrário, m_1 é falsa (M(F)) e deve ser corrigida pelo modelo físico e disponibilizada para o PsCAV, e o modelo virtual será atualizado pelo modelo físico. Se a verificação falhar em ambos modelos (MV(F) e MF(F)), o PReCAV checa se v_2 sofre um ataque nos seus sensores. Se v_2 sofre um ataque nos sensores, por (As.2), assume-se que m_1 é verdadeira e será disponibilizada ao PsCAV, e MV será atualizado pelo modelo físico. Caso contrário, assume-se que m_1 é falsa e deve ser corrigida pelo modelo físico e disponibilizada ao PsCAV. Ainda no instante $t2$, o veículo v_2 envia a mensagem m_2 com suas propriedades físicas para o sucessor v_3. Ao receber m_2 no instante t_3, o veículo v_3 realiza o mesmo fluxo de checagem do PReCAV

e envia mensagem $m3$ para o seu sucessor. O processo se repete até o último veículo v_n receber a mensagem m_{n-1} no tempo t_n. Entre t_1 e t_n o veículo líder pode enviar novas mensagens para seu sucessor e um novo ciclo se inicia. Assume-se que o primeiro ciclo de mensagens de v_1 até v_n, fase de definição dos modelos, não há ataques. O líder v_1 mantém modelo virtual e físico apenas dele mesmo por não possuir veículo predecessor. O diagrama de decisão da Figura 5 sumariza o fluxo operacional do PReCAV descrito acima.

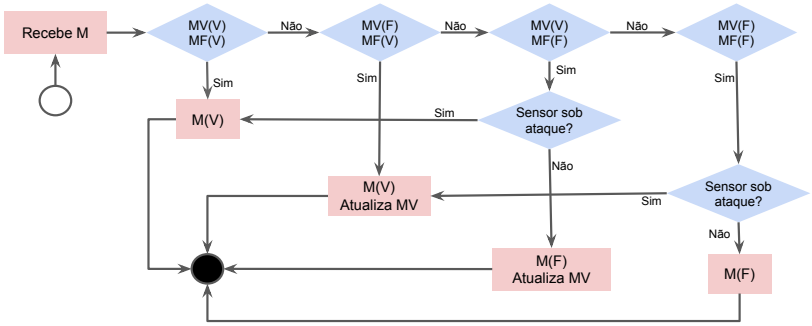

Figura 5. Diagrama do PReCAV para verificação e correção de dados falsos

4. Avaliação

Esta seção apresenta uma avaliação e análise do mecanismo PReCAV para a recuperação cooperativa de sistemas de VACs em pelotão através de experimentos simulados. Verificou-se a capacidade do *PReCAV* em prover a estabilidade do sistema de pelotão em meio à ataques de injeção de dados falsos na rede e nos sensores durante intervalos de tempo específico. O PReCAV[1] e o sistema de pelotão PsCAV foram implementados em C++ e rodados no simulador de rede NS3, versão 3.34, com o apoio do simulador de mobilidade urbana SUMO, versão 1.9.2. O ambiente de avaliação utilizado consiste de um sistema de cinco veículos em formação de pelotão trafegando sob uma via de sentido único com 2,35km de comprimento, como apresenta a Figura 6. Os veículos se comunicam em modo V2V através do padrão IEEE 802.11p. As simulações tiveram duração de dois minutos (120s), onde os veículos V2 e V4 sofreram os ataques em rede ou sensor durante 4s em dois momentos da simulação, instantes 40s e 70s. Para as simulações, uma máquina de 16 GB de RAM com processador Intel i7 8ª geração com SO Ubuntu 18.04.4 LTS foi utilizada. A Tabela 1 apresenta os parâmetros de configuração das simulações.

As avaliações consistiram-se em operar o sistema de pelotão sob seis combinações de cenários: *1) Com ataque na rede e sem PReCAV, 2) Com ataque na rede e com PReCAV, 3) Com ataque no sensor e sem PReCAV, 4) Com ataque no sensor e com PReCAV, 5) Sem ataque e sem PReCAV e 6) Sem ataque e com PReCAV*. Essas combinações possibilitam analisar o impacto do PReCAV no comportamento do sistema de pelotão PsCAV em meio à ataque de injeção de dados falsos na rede e nos sensores. As combinações 5 e 6 analisam o impacto do PReCAV sobre o sistema de pelotão em situações sem perturbações. A fim de avaliar a capacidade do PReCAV em manter a estabilidade do sistema de pelotão em meio às perturbações na rede e sensores, três métricas foram aferidas: *Distância entre Veículos* ($DV_{i,j}$), *Velocidade do Veículo i* (VV) e *Aceleração do*

[1]Disponível para solicitação em: `https://bitbucket.org/everaldoAndrade/precav`

Tabela 1. Parâmetros das simulações

Parâmetro	C1
Tempo da simulação	2 mins
Veloc. máxima dos veículos	22,22 m/s (≈80km/h)
Tamanho do pelotão	5 veículos
Sentido da via	mão única
Número de faixas	1
Duração do ataque	4s
Protocolo de transporte	UPD
Protocolo Físico/MAC	IEEE 802.11p
Modelo de propagação	YANS

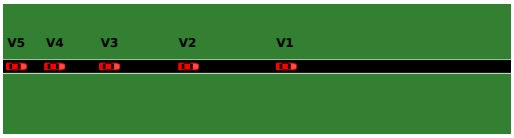

Figura 6. Cenário de avaliação do PReCAV

Veículo i (AV) no pelotão, as quais encontram-se especificadas na Tabela 2. Em situações normais, tais métricas tendem a se manter constantes ao longo tempo. Contudo, durante as perturbações, as operações no sistema de pelotão tendem a se degradar, em razão das variações drásticas destas métricas.

Tabela 2. Especificação das métricas aferidas

Métrica	Descrição	Fórmula
Distância entre Veículos (DV)	Mensura a distância das posições $P_{v_i}(t)$ e $P_{v_j}(t)$ dos veículos v_i e v_j, respectivamente, no instante de tempo *t*.	$D(t) = P_{v_i}(t) - P_{v_{i+1}}(t)$
Velocidade do Veículo (VV)	Mensura a velocidade instantânea $V_i(t)$ do veículo v_i, de velocidade inicial v_{0_i}, no instante de tempo t em aceleração a_i	$V_i(t) = v_{0_i} + a_i * t$
Aceleração do Veículo (AV)	Mensura a aceleração instantânea do veículo v_i no instante de tempo *t*	$A_i(t) = \frac{d(V_i(t))}{dt}$

4.1. Resultados e Análise de Desempenho

Uma comparação do funcionamento do pelotão numa operação normal e do desempenho do PReCAV na configuração e proteção do pelotão diante de ataques na rede[2] é mostrado nos gráficos da Figura 7 sobre as métricas AV, VV, e DV obtidas ao longo do tempo. Inicialmente, entre os instantes 0s e 26s, o sistema inicia o movimento e a formação topológica em pelotão, o que resulta na variação das métricas DV, VV e AV. Após este intervalo, o pelotão tende a alcançar um estado estável, isto é, baixas variações dos valores das métricas ao longo do tempo. Durante os ataques, instantes 40s e 70s (áreas em cinza nos gráficos), os veículos V2 e V4 recebem dados falsos na rede, o que resulta na tomada de decisão incorreta e, consequentemente, na perturbação drástica das métricas DV, VV e AV no sistema de pelotão sem uso do PReCAV (Gráficos 7(a-c)). Por outro lado, com o uso do PReCAV, as métricas DV, VV e AC assumiram valores médios de 30,6m, 22,22m/s e 0m/s^2, respectivamente, ao longo do tempo, o que demonstra a capacidade do PReCAV em manter a estabilidade do sistema (Gráficos 7(d-f)). A métrica AV sofreu variações de até 4,42m/s^2, no cenário sem PReCAV (Gráfico 7(a)). Consequentemente, VV também foi perturbada com variações de até 13,13m/s, em razão da velocidade depender da aceleração no movimento (Gráfico 7(b)). Contudo, a aplicação do PReCAV permitiu a detecção dos dados falsos injetados na rede graças a estratégia de checagem dupla das informações entre o modelo virtual e físico do sistema, o que evitou tais variações drásticas em AV e VV (Gráficos 7(d-e)). Também, as métricas $DV_{1,2}$ e $DV_{3,4}$ apresentaram variações médias de 40m e 24m, respectivamente, no cenário sem

[2]Experimento e visualização do ataque na rede: `https://youtu.be/hmZcPEfcoZ4`

PReCAV devido a injeção de dados falsos ocorrer em V2 e V4 (Gráfico 7(c)). Contudo, com a aplicação do PReCAV, $DV_{1,2}$ e $DV_{3,4}$ mantiveram-se fixas mesmo durante os ataques em rede (Gráfico 7(f)). O que demonstra a capacidade do PReCAV em manter o sistema resiliente em meio a ataques de rede.

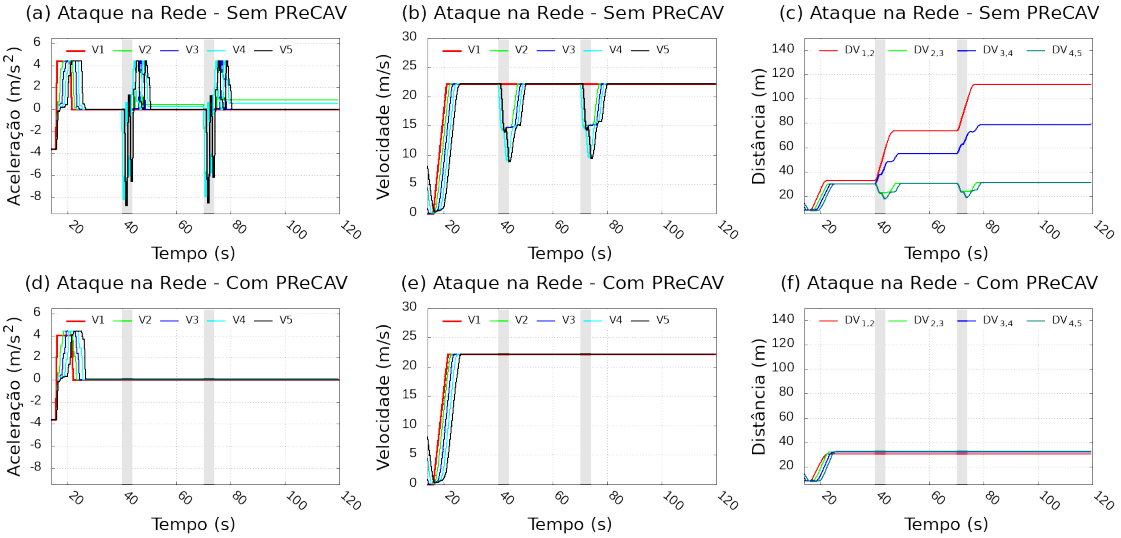

Figura 7. Valores AV, VV e DV no sistema de pelotão com ataques na rede

Uma comparação do funcionamento do pelotão numa operação normal e do desempenho do PReCAV na configuração e proteção do pelotão diante de ataques nos sensores[3] é mostrado nos gráficos da Figura 8 sobre as métricas AV, VV, e DV obtidas ao longo do tempo. Neste contexto, os veículos V2 e V4 sofreram ataques nos sensores (i.e interferências) que comprometeram a leituras das informações do ambiente e do sistema de pelotão (e.g. velocidade e distância dos vizinhos). Nos instantes dos ataques, em 40s e 70s, as métricas AV sofreram variações de até 4,43m/s^2 em razão das desacelerações (frenagens) em cadeia dos veículos ocasionadas pelos leituras incorretas dos sensores de V2 e V4 (Gráfico 8(a)). Por consequência, a métrica VV também apresentaram altas variações de até 10,7m/s, pois um veículo i tende a reduzir ou aumentar VV a medida que recebe informações do veículo predecessor. As métricas DV também apresentaram variações consideráveis em ataques nos sensores, alcançando valores de até 33,4m. Porém, com a aplicação do PReCAV, os veículos V2 e V4 foram capazes de detectar a anomalia na leitura dos sensores embarcados graças e estratégia cooperativa de troca de informações entre os membros do pelotão e a checagem dupla das informações entre o modelo virtual e físico, o que evitou tais perturbações no sistema (Gráficos 8(d-e)) e riscos de colisões em razão da redução drástica de DV, como ocorreu em $DV_{2,3}$ após o primeiro ataque (Gráfico 8(c)). Desta forma, as leituras incorretas do sensores foram substituídas por dados provenientes dos membros ou do modelo virtual mantido pelo veículo atacado.

A fim de aferir a influência do PReCAV sobre o sistema de pelotão, as métricas AV, VV e DV foram aferidas no cenário sem ataque[4]. Os gráficos da Figura 9 apresentam os valores destas métricas em tal cenário. A métrica AV não apresentou divergências

[3]Experimento e visualização do ataque nos sensores: `https://youtu.be/CQ2us0KTLDk`
[4]Experimento e visualização da operação sem ataque: `https://youtu.be/5dNg8erfWSo`

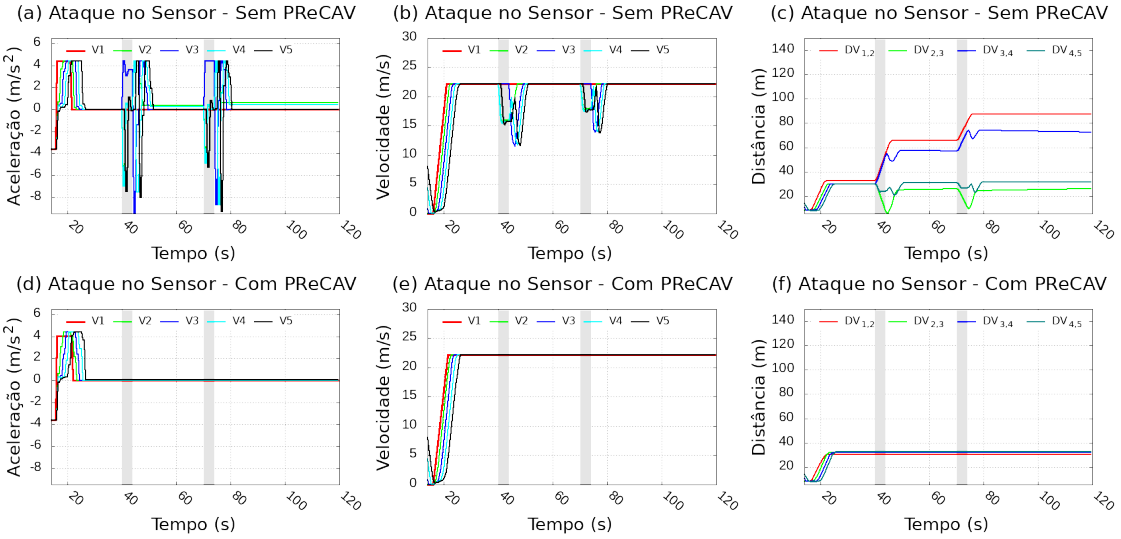

Figura 8. Valores AV, VV e DV no sistema de pelotão com ataques nos sensores

consideráveis nos cenários sem e com PReCAV, como é possível observar nos gráficos 9(a) e 9(d), respectivamente. O mesmo comportamento ocorre na métrica VV, onde os veículos do pelotão mantém velocidades de 22,22m/s (máxima permitida nos experimentos) implicando na estabilidade do sistema, como apresentam os gráficos 9(b) e 9(e). A métrica DV apresentou sutil diferença de até 2,7m entre os cenários sem e com PReCAV em razão de uma tênue divergência entre os modelos virtual e físico calculados durante a checagem dupla. Contudo, tal divergência não interfere no funcionamento do pelotão nem compromete sua segurança física (e.g. colisões), uma vez que os veículos tendem a manter a DV média em 30,6m ao alcançarem estabilidade, como pode ser visto nos gráficos 9(c) e 9(f). Desta forma, o PReCAV não interfere nas operações do sistema de pelotão em cenários sem ataques. O que demonstra sua capacidade em recuperar e manter o sistema estável sob diferentes tipos de cenários.

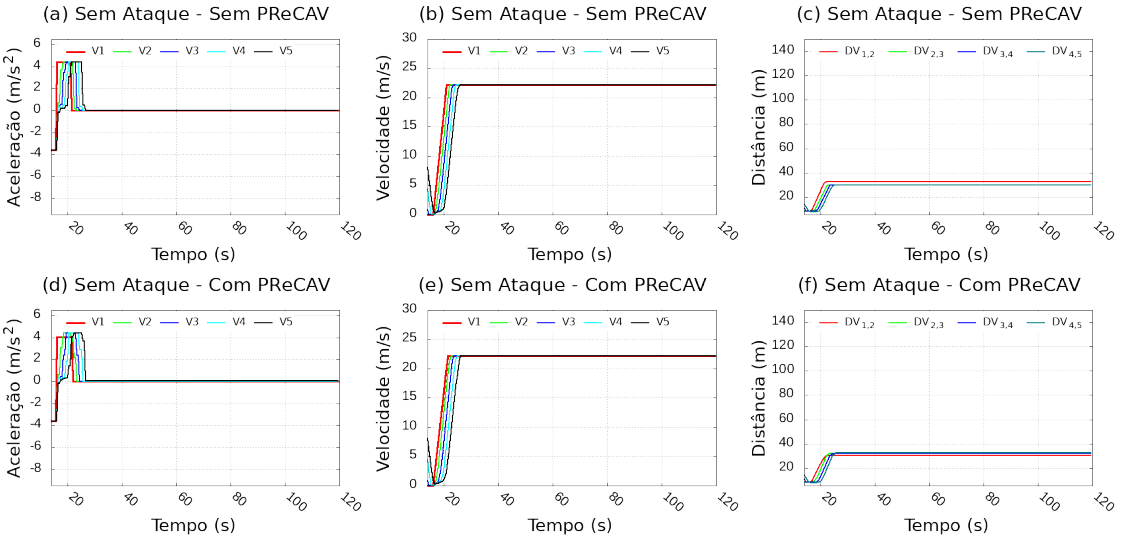

Figura 9. Valores AV, VV e DV no sistema de pelotão sem ataques

Por fim, em ambos ataques, na rede e nos sensores, foi possível observar que sistema manteve um período de instabilidade mesmo após a finalização do ataque. Isso ocorre em razão do pelotão levar um tempo para propagar o ataque (perturbação em cadeia), entrar em estado instável e tentar retornar a um estado estável anterior, o que pode variar em função do número de veículos atacados, tipo de ataque e/ou implementação do sistema de pelotão, o que foge do escopo desta pesquisa. Contudo, o PReCAV foi capaz de manter a resiliência do sistema de veículos em pelotão durante os ataques de injeção de dados falsos na rede e nos sensores (interferências). Por utilizar modelos de mobilidade simulados discretos, o valores das propriedades (e.g. aceleração, velocidade e distância) quase não variam nos períodos em que não há ataques. O mecanismo de recuperação cooperativa e checagem dupla de informações entre os modelos virtual e físico do sistema, aplicados no PReCAV, mostrou ser capaz detectar informações falsas durante os ataques. Ademais, também foi possível observar a baixa influência que o PReCAV exerce no funcionamento e operações do sistema em cenários sem ataque.

5. Conclusões

Este trabalho apresentou o mecanismo PReCAV para a recuperação de sistema de pelotão baseado em PsCAV diante de falhas de injeção de dados falsos. Ele faz uso de uma estratégia cooperativa e utiliza os modelos virtual e físico para detectar e corrigir dados falsos entregues nos VACs durante a condução do sistema de pelotão. Os resultados por simulação mostraram que o PReCAV manteve a estabilidade do pelotão, privando-o de variações de 4,42m/s^2 de aceleração, 13m/s de velocidade e 40m de distância entre veículos em ataques na rede e variações de 4,43m/s^2, 10,7m/s e 33,4m em ataques nos sensores, provendo ao sistema de pelotão resiliência à estes tipos de perturbações. Como trabalhos futuros, pretende-se tratar perturbações como perdas e atrasos de dados e considerar os ataques no mesmo veículo e instante de tempo.

Agradecimentos

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e do CNPq através do projeto No. 313641/2020-0.

Referências

Amoozadeh, M. et al. (2015). Platoon management with cooperative adaptive cruise control enabled by vanet. *Vehicular Communications*, 2(2):110–123.

Back, J., Choi, S., and Shin, Y. (2019). A study on the election of suitable leader vehicle in vehicle platooning using the raft algorithm. In *2019 Eleventh ICUFN*, pages 756–761.

Bang, S. and Ahn, S. (2017). Platooning strategy for connected and autonomous vehicles: Transition from light traffic. *Transportation Research Record*, 2623(1):73–81.

Böhm, A. and Kunert, K. (2016). Data age based mac scheme for fast and reliable communication within and between platoons of vehicles. In *2016 IEEE 12th (WiMob)*, pages 1–9.

Chen, Q., Tang, S., Yang, Q., and Fu, S. (2019). Cooper: Cooperative perception for connected autonomous vehicles based on 3d point clouds. In *2019 IEEE 39th ICDCS*, pages 514–524.

Choi, H. et al. (2018). Detecting attacks against robotic vehicles: A control invariant approach. CCS '18, page 801–816, New York, NY, USA.

Choi, H. et al. (2020). Software-based realtime recovery from sensor attacks on robotic vehicles. In *23rd RAID 2020*, pages 349–364, San Sebastian. USENIX Association.

Fakhfakh, F., Tounsi, M., and Mosbah, M. (2020). Vehicle platooning systems: Review, classification and validation strategies. *IJNDC*, 8:203–213.

Fernandes, P. and Nunes, U. (2012). Platooning with ivc-enabled autonomous vehicles: Strategies to mitigate communication delays, improve safety and traffic flow. *IEEE Transactions on Intelligent Transportation Systems*, 13(1):91–106.

He, Q. et al. (2020). Towards a severity assessment method for potential cyber attacks to connected and autonomous vehicles. *Journal of Advanced Transportation*, 2020:6873273.

Junejo, K. N. and Goh, J. (2016). Behaviour-based attack detection and classification in cyber physical systems using machine learning. In *2nd ACM Interntional Workshop on CPSS*, page 34–43, New York, NY, USA.

Khan, M. A. et al. (2022). Level-5 autonomous driving—are we there yet? a review of research literature. *ACM Comput. Surv.*, 55(2).

Ko, B. and Son, S. H. (2021). An approach to detecting malicious information attacks for platoon safety. *IEEE Access*, 9:101289–101299.

Maiti, S., Winter, S., Kulik, L., and Sarkar, S. (2020). The impact of flexible platoon formation operations. *IEEE Transactions on Intelligent Vehicles*, 5(2):229–239.

Mitchell, R. et al. (2015). Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems. *IEEE Trans. on Depend. and Secure Computing*, 12(1):16–30.

Morando, M. M. et al. (2018). Studying the safety impact of autonomous vehicles using simulation-based surrogate safety measures. *Journal of Advanced Transportation*, 2018.

Mushtaq, A., Haq, I. u., Nabi, W. u., Khan, A., and Shafiq, O. (2021). Traffic flow management of autonomous vehicles using platooning and collision avoidance strategies. *Electronics*, 10(10).

Onishi, H. (2018). A survey: Engineering challenges to implement vanet security. In *2018 IEEE International Conference on Vehicular Electronics and Safety (ICVES)*, pages 1–6.

Rana, M. M. and Hossain, K. (2021). Connected and autonomous vehicles and infrastructures: A literature review. *International Journal of Pavement Research and Technology*.

Shoukry, Y. et al. (2013). Non-invasive spoofing attacks for anti-lock braking systems. In *Cryptographic Hardware and Embedded Systems - CHES 2013*, pages 55–72, Berlin, Heidelberg.

Sun, G. et al. (2021). Strategic mitigation against wireless attacks on autonomous platoons. In *Machine Learning and Knowledge Discovery in Databases. Applied Data Science Track*, pages 69–84, Cham. Springer International Publishing.

Tippenhauer, N. O. et al. (2011). On the requirements for successful gps spoofing attacks. In *Proceedings of the 18th ACM CCCS*, CCS '11, page 75–86, New York, NY, USA.

Trippel, T. et al. (2017). Walnut: Waging doubt on the integrity of mems accelerometers with acoustic injection attacks. In *2017 IEEE EuroS P*, pages 3–18.

Yang, T. and Lv, C. (2021). A secure sensor fusion framework for connected and automated vehicles under sensor attacks. *IEEE Internet of Things Journal*, pages 1–1.

Yao, S. et al. (2020). Managing connected automated vehicles in mixed traffic considering communication reliability: a platooning strategy. *Transportation Research Procedia*, 47:43–50. 22nd EWGT 2019, Barcelona, Spain.