SOLUÇÃO INTELIGENTE USANDO DEEP LEARNING AUTOENCODER CONTRA ATAQUES CIBERNÉTICOS A VEÍCULOS CONECTADOS NO BRASIL: segurança e preservação da vida no trânsito

Resumo

As tecnologias de conectividade veicular sem fio estão surgindo como itens de série em carros no Brasil e com um enorme potencial inexplorado de segurança. Além disso, algumas comodidades como abrir e travar a porta do carro, bem como ligar o próprio carro usando um aplicativo em um celular ou em um relógio digital são algumas facilidades que emergem. O artigo propõe usar a Inteligência Artificial *Deep Learning Autoenconder* (DLA) (Aprendizado Profundo Autocodificador) para combater ataques cibernéticos a veículos conectados (conectividade com outros automóveis, pessoas e serviços), que colocam em risco a vida dos ocupantes dos veículos. O objetivo é apresentar um modelo de DLA como item de série nos veículos inteligentes, detectando e evitando intrusões que violem a integridade, confiabilidade e disponibilidade dos sistemas veiculares, para que a sociedade no trânsito não seja vítima de ameaças cibernéticas. Criminosos podem privar a liberdade do motorista em seu próprio carro, pois um ataque ao carro pode travar as portas e a ignição, bem como pode ocasionar um sinistro no trânsito ceifando as vidas de várias pessoas, já que o criminoso cibernético ao ter o total controle do veículo pode lançá-lo contra outros veículos, ciclistas ou pedestres. A contribuição social dessa proposta é salvar vidas no trânsito, prover o bem-estar dos passageiros, bem como evitar os danos financeiros e de imagem que as fabricantes podem ter com os prejuízos advindos de atentados cibernéticos a seus veículos conectados. Criar maneiras de se evitar um ataque cibernético a um veículo é salvar vidas, pois essa é a preocupação atual de organizações internacionais com o aumento de veículos conectados, principalmente, à internet.
Palavras-chave: Ataque cibernético; *Deep Learning Autoenconder*; Veículo; Trânsito; Vida.

1 Introdução

Em 2022, o Brasil sofreu 103 bilhões de tentativas e ameaças de ataques cibernéticos. Esse número representa cerca de 30% dos casos registrados em toda a América Latina e Caribe, que somaram 360 bilhões. O Brasil é o país que mais sofre ataques cibernéticos na América Latina (SIMPLÍCIO, 2023). Além disso, o Brasil possui uma frota de mais de 115 milhões de veículos (IBGE, 2023). O Brasil já tem veículos com tecnologia embarcada como ponto de acesso *wifi*, 5G, aplicativos e controle de alguns recursos do carro pelo celular ou *smartwatch,* expondo-os a criminosos cibernéticos.

Autoencoder é uma técnica classificada como redes neurais artificiais de aprendizado profundo (*deep learning*), ou seja, é uma Inteligência Artificial (IA). *Autoencoders* são usados na detecção de anomalias e têm sido aplicados com sucesso em problemas de detecção. Essa técnica é amplamente utilizada em segurança cibernética, monitoramento de sistemas e detecção de fraudes. IA possibilita desenvolver sistemas refinados que podem analisar e aprender como o ser humano. Problemas do mundo real, como segurança veicular, podem ser

resolvidos com o uso da IA. O feroz avanço tecnológico veicular torna a segurança cibernética um atrativo a ataques perigosos que representam um perigo à segurança no trânsito. Detectar e bloquear ataques ilícitos contra veículos conectados de forma inteligente e automática por meio da inserção da IA no sistema veicular é o foco deste estudo.

Vale destacar que diversos órgãos no mundo já sofreram ataques em seus sistemas e não é difícil que um carro sofra uma invasão não autorizada. Veículos conectados podem sofrer ataques e ocasionar acidentes automobilísticos causando a perda vidas no trânsito. Diante disso, o atacante pode afetar significativamente a operação do veículo, figura 7, pois pode: (i) desligar remotamente os sistemas de assistência do veículo e do motorista (controle de estabilidade, frenagem de emergência, controle de faixas, entre outros); (ii) desligar ou impedir a ignição do motor do veículo; (iii) girar bruscamente o volante em alta velocidade; (iv) travar as portas; (v) abaixar a janela (causar distração, vento ou chuva forte sobre o rosto); (vi) colocar o ar-condicionado na temperatura mais fria ou mais quente (desconforto térmico); (vii) ligar o som no volume máximo gerando distrações ao motorista; (viii) desativar o cinto de segurança; (ix) acionar ou desativar os *airbags; (x)* afastar o banco elétrico para frente e para trás enquanto o motorista dirige (imagine aproximar o banco o máximo do volante, por exemplo); (xi) acionar o para-brisa esguichando água e o pior ocasionar um sinistro propositalmente (ULLAH, 2022). A imagem abaixo exibe ataques a veículos conectados.

Figura 1: cenários de acidentes devido a ataques cibernéticos (WIEDEMAN, 2016)

Ademais, o termo "EASCY", que significa *Electrified*=elétrico, *Autonomous*=autônomo, *Shared*=compartilhado, *Connected*=conectado, *and updated Yearly*= atualizado anualmente, descreve a direção futura dos veículos que estão sempre conectados a redes externas, como a 5G (LEE, 2020).

Vale, portanto, frisar que em 2015, um *recall* teve que ser feito em larga escala devido a um ataque cibernético bem-sucedido a um carro conectado nos EUA, o que gerou danos econômicos à fabricante e investigações por parte do Estado. Governos e organizações estão

legislando para que defesas cibernéticas sejam implementadas para garantir a segurança dos ocupantes e minimizar perdas financeiras.

Com efeito, uma solução é dada usando um modelo de detecção de invasão por meio de *deep learning autoencoder* para monitorar e proteger os veículos conectados de ataques cibernéticos. *Deep learning autoencoder* teve uma alta taxa de precisão de detecção em relação aos meios tradicionais de detecção.

1.1 Problema

Um veículo conectado, ao ser controlado por um cibercriminoso, pode sofrer um sinistro veicular matando diversas pessoas no Brasil?

1.2 Justificativa

Destaca-se que, em 2014, mais da metade (59%) dos usuários de veículos se mostraram preocupados com a possibilidade do carro ser tomado por cibercriminosos quando o automóvel estiver conectado à internet. 37% dos brasileiros não querem carros conectados devido ao risco de perda de privacidade (HANNON, 2014). Ademais, espera-se mais de 4,4 milhões de carros conectados até 2030 no Brasil, por apenas um grupo veicular **(**LUBIATO, 2022). A cibersegurança de dispositivos veiculares é um aspecto de preocupação e deve ser analisado em todo o fluxo de vida do equipamento para reduzir danos severos as pessoas, evitando, dessa forma, problemas aos usuários de veículos, *recalls* e demandas judiciais.

À medida que as tecnologias de conectividade sem fio vêm de série nos veículos, isso gera uma popularização e desperta o interesse de cibercriminosos, que podem tomar remotamente o controle total de um veículo conectado e ocasionar um sinistro automobilístico. Diante do exposto, é necessário um mecanismo eficiente de IA para proteger as pessoas no trânsito, ou seja, preservar suas vidas, pois o veículo pode sofrer um ataque cibernético e ser jogado contra outros veículos, pedestres e ciclistas, o que pode gerar um atentado com enormes lesões e mortes no trânsito brasileiro.

1.3 Objetivos

1.3.1 Objetivo

Contribuir com uma solução usando a IA (*deep learning autoencoder=dla*) no combate a investidas cibercriminosas contra veículos conectados para se evitar lesões e mortes no trânsito brasileiro. Diante disso, melhorar a defesa e a proteção da vida humana dos ocupantes de veículos e dos pedestres.

1.3.2 Objetivos finalísticos mensurados

(i) Promover o aumento da segurança cibernética veicular usando IA (DLA) com uma precisão de mais de 99% em prol da defesa da vida da população no trânsito brasileiro;

(ii) Implementar em até 1 ano contramedidas *(counter-measures)* contemporâneas (*deep learning autoencoder*) com o propósito de defender os veículos conectados e as pessoas de uma gama mais ampla de ameaças cibernéticas, incluindo extorsão, lesão corporal, assassinato, terrorismo, entre outros problemas potenciais no trânsito brasileiro;

(iii) Ampliar para que 100% dos veículos conectados saiam de fábrica com mecanismos seguros de: encriptação, detecção, bloqueio, autenticação, integridade de mensagens, assim evitando o *eavesdropping*, ou seja, a interceptação ilícita da comunicação sem fio dos sistemas veiculares pelo cibercriminoso, que ocasiona sinistros automobilísticos, bem como o impacto drástico de serviços de socorro e congestionamento no Brasil.

1.4 Público-Alvo

A sociedade brasileira em sua totalidade, desde os motoristas e passageiros nos veículos, bem como os pedestres e ciclistas, pois todos estão vulneráveis a terem suas vidas esfaceladas devido a um atentado cibernético ilícito contra um veículo.

2 Fundamentação teórica

Autoencoders são estruturas de *deep learning* que foram originalmente desenvolvidas para compressão de dados. Eles consistem em uma rede neural que pode ser dividida em duas partes: codificador e decodificador (ASHRAF, 2021).

2.1 Ataques cibernéticos: risco de vida no trânsito

Carros altamente tecnológicos são verdadeiros computadores, comandados por uma central eletrônica de controle. Diferente das redes móveis tradicionais, as redes móveis veiculares 5G suportam um acesso massivo de dados e conexão de dispositivos (JI, 2018). Deve-se ter cuidado com conexões em rede *Wifi* pública, pois está mais vulnerável a ataques (FBI, 2023). A desativação dos freios, desaceleração abrupta do veículo fazendo com que aconteçam colisões traseiras. A figura 2 mostra que o invasor do sistema do veículo pode estender o ataque remotamente a outros carros por encadeamento usando a rede móvel de internet das antenas RSU (*Road Side Unit*) espalhadas pelas vias (CHOWDHURY,2020).

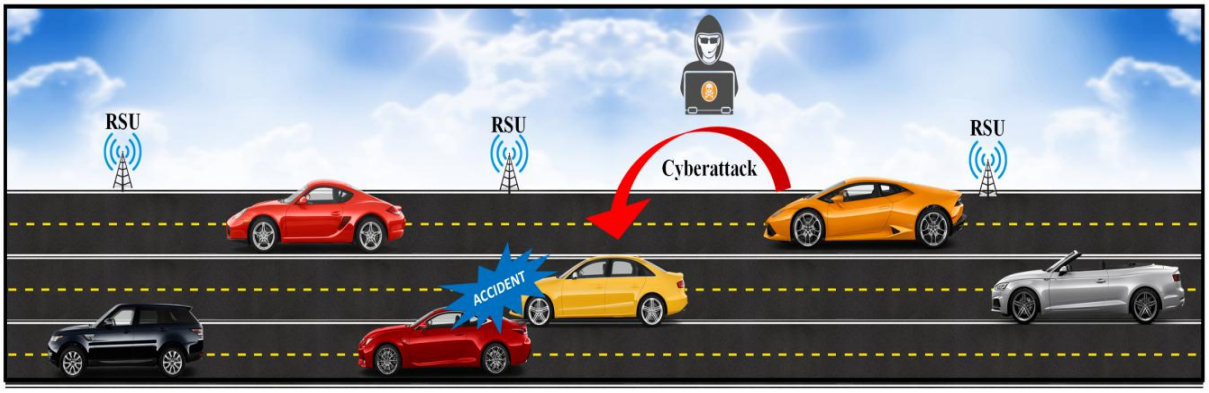

Figura 2: Cenário de ataque cibernético em veículos conectados (ULLAH, 2022)

2.2 Seu carro pode virar um zumbi

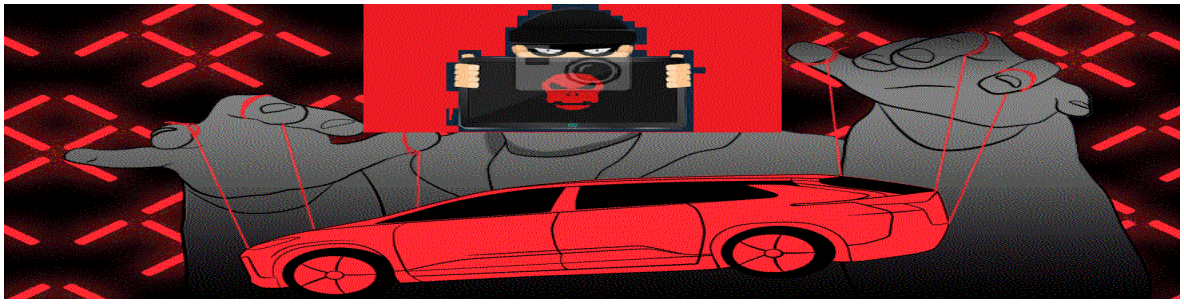

Figura 3: abstração de um veículo tomado pelo invasor (adaptado de O'KANE, 2022)

O condutor é quem conduz o seu veículo, mas imaginar que um veículo com conectividade pode sofrer uma invasão e o carro ser controlado remotamente, tornando o automóvel um zumbi (figura 3) (termo usado na computação quando sistemas são controlados por cibercriminosos). Diante disso, os veículos estão cada vez mais recebendo aplicativos com as mais diversas criativas funcionalidades que se comunicam com o mundo exterior, o que faz com que fiquem expostos a ataques.

2.2.1 Casos de grande repercussão de veículos hackeados remotamente

Os desafios de segurança tornam-se ainda mais complexos pelo conhecimento de que 60% dos veículos de 2016 vêm com recursos de conexão à Internet (KELARESTAGHI, 2019). Os principais fabricantes de equipamentos originais de automóveis apontam que quase 100% dos veículos novos são equipados com tecnologias sem fio. O ataque pode se iniciar não só diretamente pelo veículo, mas pelo celular, já que o aparelho telefônico está conectado ao veículo por meio de aplicativos. Abaixo um caso de ataque a um carro que ganhou grande notoriedade, o que comprova ser possível realizar um ataque remotamente contra um veículo.

Figura 4: Carro foi colocado para fora da rodovia pelos *hacker*s (HASHEM, 2017)

Em 2015, carro, de determinada empresa e vendido no Brasil, foi parado remotamente em uma rodovia nos EUA – figura 4, o que desencadeou um *recall* de 1,4 milhão de veículos (CHOWDHURY, 2020). O carro foi hackeado a quilômetros de distância por meio do sistema de entretenimento (Celular - *Wi-Fi hotspot*) com um motorista a bordo. Conseguiram controlar o motor do carro, os freios, a direção e o ar condicionado. O motorista relatou que

foi uma experiência traumática, pois não tinha controle sobre o veículo enquanto dirigia na rodovia cercado por outros veículos. Teve a privacidade invadida, pois estava sendo rastreado através das coordenadas GPS. Ficou desamparado quando colocaram o som do carro no volume máximo e só lhe restou pedir que parassem o carro e logo foi para fora da rodovia (KELARESTAGHI, 2019). Esse ataque gerou um *recall* associado a outro carro da empresa, fabricados a partir de 2014 até 2015 (NHTSA, 2015). Antes e depois desse caso outros ataques a veículos com conectividade aconteceram.

Em 2018, um atacante assumiu o controle de um carro conectado série 7, o que ocasionou uma colisão, pois o veículo não conseguia estacionar devido à interferência do atacante. Várias vulnerabilidades foram encontradas, comprometida a capacidade de segurança da conexão sem fio (CHOWDHURY, 2020).

Em 2022, hacker, 19 anos, assumiu o controle de mais de 20 veículos conectados em mais de 10 países por meio de um ataque cibernético, na qual lhe permitia ligar os carros, dirigir a distância, desativar sistemas de segurança e até espionar os motoristas, entre outras ações (LIBERATORE, 2022).

2.3 Brasil e as tecnologias dos carros conectados

O Brasil já tem veículos com tecnologia embarcada como *wifi*, 5G, controle de alguns recursos do carro pelo celular ou *smartwatch*. É importante que as pessoas saibam dos riscos tecnológicos que os carros trazem. Abaixo alguns veículos conectados no Brasil que possibilitam uma invasão de um cibercriminoso.

Carro brasileiro, de determinada empresa, possui os Comandos Remotos por meio do assistente virtual *OnStar* no celular, o que permite enviar comandos à distância como: ligar e desligar o veículo, travar e destravar portas e até acionar as luzes e buzinas (ONSTAR, 2023).

Carro brasileiro, de determinada empresa, tem o aplicativo Pass™ Connect em que se pode interagir com o carro em qualquer lugar - figura 5. Com o aplicativo Pass™ no celular é possível dar a partida no veículo, ligar o ar-condicionado e muito mais (PASS™, 2023).

Figura 5: controle do carro pelo aplicativo instalado no smartphone (PASS™, 2023).

Carro brasileiro, de determinada empresa, possui as operações remotas em que o proprietário do carro consegue controlar o carro a quilômetros de distância por meio de um

smartwatch, pode-se travar e destravar as portas e ligar e desligar o carro usando o relógio digital do braço - figura 6. Tem um *Wifi hotspot* que permite se conectar a até 8 dispositivos externos (CONNECT, 2023).

Figura 6: controle do carro pelo relógio e o *wifi* na tela multimídia (CONNECT, 2023).

3 Desenvolvimento

3.1 Metodologia e Estratégia de implementação

Diante de um cenário de veículos conectados, automatizados, elétricos e com diversas tecnologias embarcadas, têm-se um setor vulnerável a crimes. Pensando em uma solução que previna e evite que um veículo seja tomado remotamente por meio de um ataque cibernético é que se faz presente a proposição. Nessa perspectiva, foi realizada diversas pesquisas bibliográficas analíticas de IAs no combate aos ataques cibernéticos veiculares que estão evoluindo e se tornando cada vez mais complexos e difíceis de detectar.

Realizado um estudo aprofundado sobre ameaças cibernéticas para determinar qual o melhor método para ser usado para detectar a invasão e ativar contramedidas. Constatado que a junção de *Deep Learning* com *Autoencoder* geram uma precisão alta de detecção e barreira de invasão contra ataques maliciosos as redes veiculares. O método consiste em uma investigação cientifica qualitativa e quantitativa com perspectiva aplicada sobre casos de ataques cibernéticos a veículos conectados, bem como um estudo sobre a aplicabilidade da IA (*Deep Learning Autoencoder*) na segurança dos veículos no Brasil.

Portanto, cabe salientar a importância da parceria do Estado (normatizando e fiscalizando) que fará o acompanhamento da evolução da solução tecnológica; universidades (desenvolvendo tecnologias veiculares); e empresas de veículos (desenvolvendo e aplicando a solução veicular) para ser possível inserir um sistema que monitore a rede 24h ininterrupta, mantendo o veículo protegido de atentados criminosos. Por meio de aplicação de uma resolução do Contran é possível estabelecer prazos de desenvolvimento e implementação, e de acompanhamentos pré-estabelecidos na consecução do sistema inteligente de IA que proteja o veículo de cibercriminosos. O mecanismo de avaliação dar-se por relatórios com indicadores que garanta a autonomia do motorista na direção de seu veículo para que não seja vítima dentro de seu patrimônio e nem que os pedestres, ciclistas e até mesmo os outros motoristas

sejam alvos de atentados contra a sua integridade física e psicológica. São necessárias mudanças e inovações diante desse pressuposto.

Abaixo, figura 7, é apresentada a proposição do modelo de sistema de detecção de intrusão e bloqueio (SDIB) por meio de codificação e decodificação. Atua no monitoramento das atividades do veículo com o meio externo, evitando operações não autorizadas. A escolha estratégica desse método levou em consideração sua complexidade computacional e eficiência em momentos de detecção e não intrusão a rede veicular.

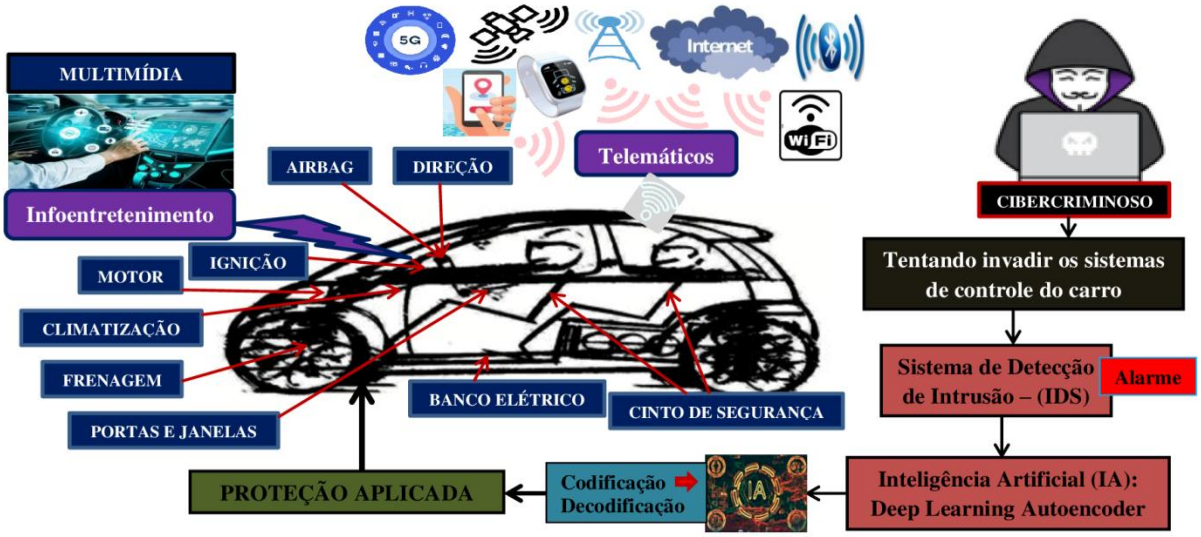

Figura 7: modelo de SDIB por meio de codificação e decodificação (elaborado pelo autor)

O cibercriminoso ao tentar aplicar um ataque à rede veicular vai se deparar com o sistema de detecção que irá emitir um alarme ao proprietário do veículo. O ataque pode ser direto na central do veículo (*wifi*, 5G, *bluetooth*), pelo celular ou relógio do motorista que está conectado ao veículo. A detecção e o bloqueio são dadas pela IA usando aprendizado profundo e codificação/decodificação. O modelo consiste em uma camada na qual compacta os dados de entrada (codificação). Em seguida, é usada uma camada de repetição para espalhar a representação compactada pelas fases de tempo de decodificação. Por fim, a camada de saída do decodificador produz os dados de entrada reconstruídos. Precisamente, grandes erros de reconstrução representam atividades maliciosas.

Assim, se o *autoencoder* for treinado apenas com dados não maliciosos de invasão e mais tarde for colocado para reconstruir as amostras de dados recebidos, ele produzirá pequenos erros de reconstrução para as amostras benignas (acesso lícito) e grandes erros de reconstrução para as amostras que são maliciosas (acesso ilícito). Dessa forma, as detecções são feitas e as invasões bloqueadas.

O desenvolvimento da criação levou em consideração os seguintes pressupostos: as tecnologias de conectividade nos veículos no Brasil aparecem até mesmo em carros populares

e a necessidade continuada de surgir mecanismos de defesa a ataques cibernéticos aos veículos. Além disso, a segurança cibernética veicular corresponde à segurança no trânsito porque facilmente um carro desgovernado por meio de ataque de um criminoso cibernético pode matar os seus ocupantes e quem estiver ao seu redor nas vias. Portanto, deve-se juntamente com o Estado e as empresas privadas criar soluções para que os milhões de veículos passivos de sofrerem atentados cibernéticos estejam protegidos no Brasil.

Deve-se dar um prazo para que as empresas de veículos juntamente com as universidades implementem suas IAs e ofereçam a segurança devida aos consumidores e a sociedade. Diante disso, os veículos deverão sair de fábrica com a IA como item de série e os veículos conectados sem a IA deverão ter gratuitamente instalados a IA.

3.2 Proposta e cronograma de execução

Propor uma IA (*Deep Learning Autoencoder*) no monitoramento constante (24h de vigilância) para detectar e evitar tentativas de invasão ao sistema de veículos conectados no Brasil. Diante disso, não permitir a intrusão maliciosa e avisar ao motorista do veículo sobre a tentativa de tomada ilícita do seu veículo para que a sociedade brasileira no trânsito não seja vítima de atentados cibernéticos em seus veículos conectados.

A primeira etapa deu-se com a busca de resoluções do Contran acerca da segurança cibernética de veículos e constatado que não possui tal legislação. Logo, a importância da regulação do tema. Em seguida, a segunda etapa, foi construída pela coleta de diversos casos de veículos conectados que foram tomados remotamente por um ataque cibernético, para comprovar que é possível tal atitude ilícita. A terceira etapa aconteceu no levantamento de IAs centradas na proteção veicular e mapeado qual a melhor IA para a detecção de intrusão e bloqueio. A quarta etapa foi focada na construção de um modelo de detecção de intrusão e bloqueio de ataques cibernéticos, bem como a propositura do método da IA *Deep Learning Autoencoder* devido ao seu alto nível de assertividade.

Tabela 1: Proposta e cronograma de execução de implementação

1º/2024	Inicialmente, normatizar por meio de Resolução do Contran em que estabeleça um sistema veicular seguro (seja item de série) em que o componente principal é a Inteligência Artificial (DLA).
2º/2024	As empresas com os departamentos de computação das universidades desenvolvam IAs, conforme as especificidades de seus veículos. Um novo patamar de segurança veicular com o uso de IA surgirá nos veículos brasileiros, bem como um excelente marketing de segurança para as marcas de veículos no Brasil. Iniciar a instalação da IA nos veículos conectados que ainda não possuem tal tecnologia.

4 Resultados

À medida que as aplicações de veículos conectados trocam informações entre veículos, infraestrutura rodoviária e dispositivos móveis sem fio, é precípuo um sistema de segurança para garantir a segurança das pessoas. Um sistema de segurança baseado em inteligência artificial (IA) que é capaz de reconhecer e repelir ataques a veículos conectados deve ser desenvolvido.

Nesse toar, codificadores automáticos profundos (*deep learning autoencoder*) para evitar danos associados à segurança veicular e das pessoas. O uso de técnicas defensivas inteligentes e detecção de intrusão rodando no sistema do veículo para proteger as comunicações externas que o veículo realiza com os diferentes dispositivos (celular, relógio, entre outros). O sistema proposto demonstra ser capaz de detectar eficazmente pacotes maliciosos, pela sua alta precisão no monitoramento de sistemas e detecção de fraudes. Algoritmos tradicionais precisam de muito esforço para detectar e bloquear intrusões, já técnicas baseadas em *deep learning autoencoder*, por outro lado, superam estas limitações detectando e bloqueando automaticamente as invasões, garantindo os melhores resultados.

Tabela 2: *Autoencoders* (AEs) (Codificador Automático)

Cenário Atacado	Base de Dados	Resultado
Rede veicular	Car-Hacking	Precisão: 0.99

Fonte: ASHRAF, 2021.

Tabela 3: *Deep Learning (*Aprendizado Profundo)

Cenário Atacado	Base de Dados	Resultado
Rede veicular	OCTANE (Open Car Test-bed and Network Experiments)	Precisão: 0.978

Fonte: KANG, 2016.

Tabela 4: Algoritmos: *K-Nearest Neighbour* (KNN) (K-Vizinho Mais Próximo); *Decision Tree* (DT) (Árvore de Decisão);

Cenário Atacado	Base de Dados	Resultado
Rede veicular	Car-Hacking & UNSW-NB 15	KNN - Precisão: 0.9882 & 0,97 DT - Precisão: 0.99 & 0.9719

Fonte: ALSAADE, 2023.

Tabela 5: *Deep Learning Autoencoder (*Aprendizado profundo codificador automático)

Cenário	Base de Dados	Resultado
Rede veicular	Car-Hacking & UNSW-NB 15	Precisão: 0.9998 & 0,9809

Fonte: ALSAADE, 2023.

Os resultados da tabela 5 mostram que o método proposto *Deep Learning Autoencoder* alcançou a maior taxa de precisão de acertos em comparação com outros métodos de detecção de anomalias veiculares – tabela 4. Do ponto de vista da segurança cibernética, o modelo proposto pode prover uma estrutura altamente segura e precisa para evitar que os veículos sejam invadidos por

invasores e que não haja vítimas fatais de sinistros de trânsito no Brasil devido a ações maldosas de cibercriminosos.

Conclusões

As técnicas de ataques cibernéticos crescem e com isso novas vulnerabilidades aparecem, isso representa um desafio, ou seja, algumas contramedidas de invasão se tornam obsoletas, que exigem uma ação rápida e contínua as ameaças. Os veículos conectados são uma solução para a melhoria da mobilidade das pessoas e com o seu aumento vêm à preocupação com a eficácia da segurança cibernética veicular, pois uma rede veicular segura impede danos corporais. O cibercriminoso só precisa encontrar uma única brecha para lançar um ataque. Os componentes do sistema veicular são interligados e se um desses componentes for invadido, a integridade do sistema inteiro estará vulnerável e consequente às pessoas no trânsito brasileiro podem perder suas vidas.

Para resolver este problema, vários métodos de detecção e bloqueio de ataques cibernéticos usando IA DLA (apresentou alta taxa de acertos) podem ser financiados pelos fabricantes de veículos para prover a segurança necessária à sociedade brasileira. A Inteligência Artificial atua 24 horas por dia reduzindo falhas e otimizando os processos de segurança, monitorando e enviando alertas para uma tomada de decisão mais assertiva, guarnecendo a segurança direta do veículo e do trânsito, pois um ataque ao carro pode gerar mortes de pedestres e de outros motoristas.

Com a introdução de veículos conectados no mercado brasileiro, a IA permite mitigar invasões nos dispositivos e na rede veicular. Monitoração constante do tráfego da rede é uma medida de segurança eficaz para combater invasões nos veículos. Combater o aparecimento de novas formas de ataques cibernéticos são atitudes que devem ser planejadas e implementadas para a segurança da sociedade no trânsito. Situações de perigo tendem a aumentar em um futuro breve, se medidas de segurança não forem estabelecidas no Brasil. Logo, evidenciado que se devem prevenir tais práticas ilegais para se evitar qualquer chance de ceifar vidas. A população necessita de veículos seguros para preservar a vida no trânsito em âmbito social, político e econômico no Brasil.

Referências

ALSAADE, Fawaz Waselallah; AL-ADHAILEH, Mosleh Hmoud. Cyber attack detection for self-driving vehicle networks using deep autoencoder algorithms. Sensors, v. 23, n. 8, p. 4086, 2023.

ASHRAF, Javed et al. “Novel deep learning-enabled lstm autoencoder architecture for discovering anomalous events from intelligent transportation systems,” IEEE Trans. Intelligent Transportation Systems, vol. 22, no. 7, pp. 4507–4518, 2021.

CHOWDHURY, Abdullahi et al. Attacks on self-driving cars and their countermeasures: A survey. IEEE Access, v. 8, p. 207308-207342, 2020.

CONNECT. Fiat Pulse Connect. Disponível em: <https://shre.ink/nlci>. Acesso em: 23 set. 2023.

FBI. WHAT WE INVESTIGATE - Cyber Crime. Disponível em: <https://www.fbi.gov/investigate/cyber>. Acessado em: 01 out. 2023.

HANNON, E. et al. What's Driving the Connected Car | McKinsey. 2014. Disponível em: <https://shre.ink/nxNZ >. Acesso em: 01 out. 2023.

HASHEM, ELIZA M and Ni, Q (2017) DRIVING WITH SHARKS Rethinking Connected Vehicles with Vehicle Cybersecurity. IEEE Vehicular Technology Magazine, ISSN 1556-6072.

IBGE. Frota de veículos do Brasil. 2022. Disponível em: <https://cidades.ibge.gov.br/brasil/pesquisa/22/28120>. Acesso em: 29 set. 2023.

JI, Haojie et al. Comparative performance evaluation of intrusion detection methods for in-vehicle networks. IEEE Access, v. 6, p. 37523-37532, 2018.

KANG, M.J et al. "Intrusion detection system using deep neural network for in-vehicle network security," *PloS One*, vol. 11, no. 6, pp. 1–17, 2016.

KELARESTAGHI, Kaveh Bakhsh et al. Intelligent transportation system security: impact-oriented risk assessment of in-vehicle. IEEE Intelligent Transportation Systems Magazine, 2019.

LEE, Yousik et al. Practical vulnerability-information-sharing architecture for automotive security-risk analysis. IEEE Access, v. 8, p. 120009-120018, 2020.

LIBERATORE, Stacy. Hacker, 19, takes control of more than 20 Tesla vehicles in 10 countries through a flaw. 2022. Disponível em: <https://shre.ink/nXkV>. Acesso em: 29 set. 2023.

LUBIATO, Kelly. Dados de carros conectados abrem oportunidades para mercado de seguros. Apólice. 2022. Disponível em: <https://shre.ink/nlOo>. Acesso em: 29 set. 2023.

O'KANE, Sean. Chinese Tycoon Spent 8 Years, $3 Billion on EV That Went Unbuilt. 2022. Disponível em: <https://shre.ink/nl2S>. Acesso em: 02 out. 2023.

ONSTAR. MyChevrolet. Disponível em: < https://shre.ink/nXG8 >. Acesso em: 23 set. 2023.

PASS™. FordPass™ Connect. Disponível em:< https://shre.ink/nXGd>. Acesso em: 23 set. 2023.

SIMPLÍCIO, Marcos. Brasil sofreu mais de 100 bilhões de tentativas de ataques cibernéticos. Jornal da USP no Ar. 2023. Disponível em: <https://shre.ink/nlc7>. Acesso em: 02 out. 2023.

ULLAH, Safi et al. HDL-IDS: a hybrid deep learning architecture for intrusion detection in the Internet of Vehicles. Sensors, v. 22, n. 4, p. 1340, 2022.

WIEDEMAN, REEVES. Envisioning the Hack That Could Take Down NYC - the big hack. Disponível em: <https://shre.ink/nlcM>. 2016. Acesso em: 02 out. 2023.