MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA
INSTITUTO MILITAR DE ENGENHARIA
CURSO DE MESTRADO EM SISTEMAS E COMPUTAÇÃO

PROPOSTA DE DISSERTAÇÃO DE MESTRADO

CHANDLER KLÜSER CHANTRE

ANÁLISE DE VULNERABILIDADES E MITIGAÇÃO DE ATAQUES PARA O PROTOCOLO MAVLINK

Rio de Janeiro
2025

CHANDLER KLÜSER CHANTRE

ANÁLISE DE VULNERABILIDADES E MITIGAÇÃO DE ATAQUES PARA O PROTOCOLO MAVLINK

Proposta de Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Engenharia de Sistemas e Computação do Instituto Militar de Engenharia, no âmbito da Linha de Pesquisa em Sistemas de Computação, como requisito parcial para obtenção do título de Mestre em Engenharia de Sistemas e Computação.

Orientadores: Paulo Fernando Ferreira Rosa, Ph.D.
Cel. R/1 Anderson Fernandes Pereira dos Santos, D.Sc.

Resultado: (X) SATISFATÓRIO
( ) SATISFATÓRIO COM RESTRIÇÕES
( ) NÃO SATISFATÓRIO

gov.br Documento assinado digitalmente
CHANDLER KLUSER CHANTRE
Data: 03/02/2025 09:38:57-0300
Verifique em https://validar.iti.gov.br

CT (EN) Chandler Klüser Chantre (SC 24105)
Aluno

gov.br Documento assinado digitalmente
PAULO FERNANDO FERREIRA ROSA
Data: 03/02/2025 09:01:29-0300
Verifique em https://validar.iti.gov.br

Paulo Fernando Ferreira Rosa, Ph.D.
Orientador

Cel. R/1 Anderson Fernandes Pereira dos Santos, D.Sc.
Orientador

Maj. Gabriela Moutinho de Souza Dias, D.Sc.
Coordenador de Pós-graduação

Concordo com a presente Proposta de Dissertação e declaro que as necessidades para sua execução serão garantidas pela Seção.
IME, em 29 de Janeiro de 2025.

Cel. Julio Cesar Duarte, D.Sc.
CHEFE da SE/9

RESUMO

O crescente uso de Veículos Aéreos Não Tripulados (VANTs) em aplicações comerciais, industriais e militares ressalta a necessidade de protocolos de comunicação seguros. Esta proposta foca na análise de vulnerabilidades do protocolo MAVLink e no desenvolvimento de medidas de proteção para mitigar ameaças cibernéticas, como o sequestro, controle do veículo e a interceptação de dados trafegados. Por meio de experimentos realizados em ambientes virtuais e eventuais testes com dispositivos reais, a pesquisa identificará vulnerabilidades, classificará suas implicações e realizará a proposição de soluções que garantam a integridade, confidencialidade e disponibilidade das comunicações. Além disso, o trabalho propõe-se a avaliar a eficácia e o consumo energético das soluções propostas, contribuindo para a segurança e a confiabilidade das operações com drones em cenários críticos.

Palavras-chave: VANTs. MAVLink. Protocolo. Segurança. Cibernética.

ABSTRACT

The increasing use of Unmanned Aerial Vehicles (UAVs) in commercial, industrial, and military applications highlights the need for secure communication protocols. This proposal focuses on analyzing vulnerabilities in the MAVLink protocol and developing protective measures to mitigate cyber threats such as hijacking, vehicle control takeover, and interception of transmitted data. Through experiments conducted in virtual environments and potential tests with real devices, the research will identify vulnerabilities, classify their implications, and propose solutions to ensure the integrity, confidentiality, and availability of communications. Additionally, the study aims to evaluate the effectiveness and energy consumption of the proposed solutions, contributing to the security and reliability of drone operations in critical scenarios.

Palavras-chave: UAVs. MAVLink. Protocol. Cybersecurity.

SUMÁRIO

Título da Proposta de Dissertação:

Análise de Vulnerabilidades e Mitigação de Ataques para o Protocolo MAVLink

Título da Capa:

Análise de Vulnerabilidades e Mitigação de Ataques para o Protocolo MAVLink

Área de Concentração:

Ciência da Computação

Linha de Pesquisa:

Sistemas de Computação

1 INTRODUÇÃO

Para acompanhar o crescimento e a popularidade dos *drones* em diversas áreas, de logística a segurança pública, a pesquisa de protocolos de segurança em *drones* se faz necessária. Como esse tipo de tecnologia tem acesso a espaços aéreos e executa funções críticas, a segurança é essencial para impedir ataques cibernéticos. É importante destacar a diferença entre o desenvolvimento de protocolos e a análise/avaliação de segurança nos protocolos.

O desenvolvimento de protocolos é focado em criar regras e procedimentos que permitam a comunicação eficiente e funcional entre sistemas ou dispositivos, incluindo a estruturação de mensagens, definição de canais de comunicação e estabelecimento de regras de comunicação e demais mecanismos auxiliares, como controle de erros. A análise da segurança em protocolos tem por objetivo identificar e avaliar vulnerabilidades em protocolos para garantir que eles resistam a ataques, falhas e tentativas de exploração. Realizada tal distinção, é essencial desenvolver protocolos robustos que garantam a disponibilidade, confidencialidade e integridade [1] de dados trafegados por *drones*, protegendo-os contra ações espúrias.

Uma das principais preocupações no campo de segurança em *drones* é a vulnerabilidade a ataques cibernéticos, incluindo sequestro de controle e interceptação de dados, o que compromete a integridade das informações e a privacidade dos usuários durante os voos [2, 3].

O desenvolvimento de medidas de segurança favorecem a comunicação segura do *drone* com veículos e estações de controle, e também aprimoram os mecanismos de garantia integridade e a confidencialidade das informações transmitidas. Isto é essencial quando aplicado a fins comerciais ou governamentais, nos quais a segurança das informações e a continuidade das operações são importantes [4].

A implementação de medidas de segurança na comunicação com *drones* está relacionada à prevenção de acidentes e colisões tendo em vista que mais *drones* estão sendo lançados e usados no espaço aéreo em conjunto com a existência de sistemas integrados de detecção e evasão de obstáculos [5].

1.1 CONTEXTUALIZAÇÃO E MOTIVAÇÃO

O MAVLink *(Micro Air Vehicle Communication Protocol)* é um dos protocolos de comunicação mais difundidos com a utilização de Veículos Aéreos Não Tripulados (VANTs).

Trata-se de um protocolo baseado em mensagens que será apresentado posteriormente. Ele foi projetado para permitir a transferência de dados em tempo real entre tais veículos e controladores, que pode ser um piloto ou um sistema de controle terrestre. Esse protocolo suporta a transmissão de telemetria, comandos de navegação e informações detalhadas sobre o estado dos sensores, facilitando tanto a execução de missões autônomas quanto o monitoramento contínuo do estado do veículo [6].

A pesquisa sobre protocolos de segurança na comunicação entre dispositivos, como o protocolo MAVLink, é essencial para proteger sistemas críticos de *drones* de agentes mal intencionados. Por analogia, da mesma forma que sistemas de automóveis conectados utilizam o protocolo CAN [7, 8], o MAVLink é amplamente adotado para troca de dados entre *drones* e estações de controle.

A ausência de mecanismos de segurança robustos nesse protocolo, que será apresentado posteriormente, pode deixar as comunicações vulneráveis a ataques [4], como injeção de comandos e interceptação de dados. A aplicação de estratégias de segurança, como emprego de criptografia se alinha com as necessidades de proteção em sistemas de comunicação que são críticos como o MAVLink, aumentando a confiabilidade das operações e garantindo que dados sensíveis permaneçam íntegros e confidenciais.

A popularidade do protocolo é devido a sua simplicidade e flexibilidade, o que permite que ele seja usado em um grande número de projetos de *drones*. À medida que a exploração de *drones* se torna mais comum em áreas comerciais, de segurança e militares, o protocolo MAVLink tornou-se um vetor de ataques de agentes maliciosos [9].

O protocolo MAVLink original, que será apresentado posteriormente, não possui camadas de segurança robustas, como criptografia ponta a ponta ou autenticação de mensagem. Isso pode fornecer a agentes maliciosos a possibilidade de interceptar, modificar ou controlar de *drones* [9, 10, 11] durante a execução, ameaçando tanto a área de segurança quanto a privacidade dos dados, a Figura 1.1 ilustra uma interceptação de um atacante em uma comunicação entre *drone* e a sua Estação Terrestre de Controle com o intuito de controlar as ações do VANT. Esta comunicação pode ser feita por meio do protocolo MAVLink.

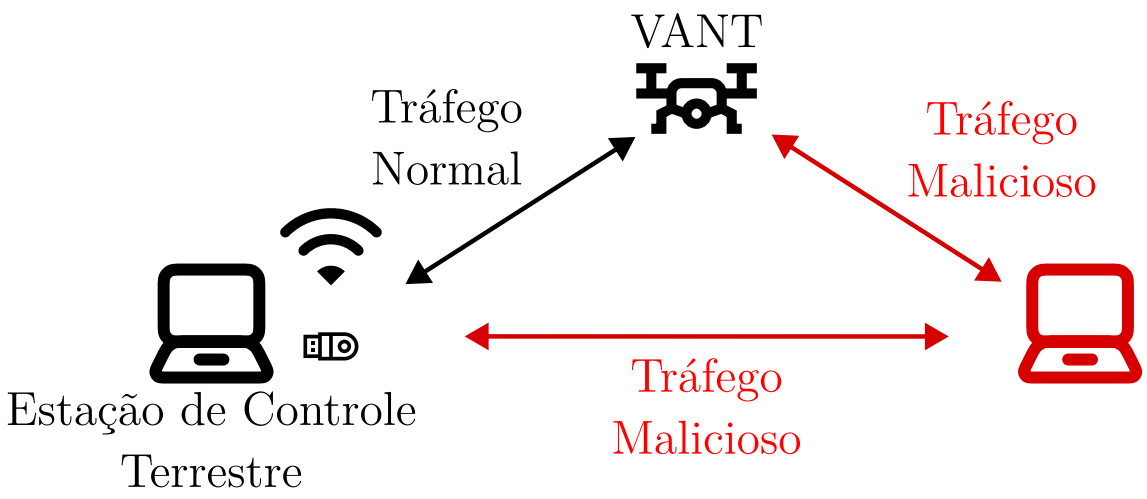


FIG. 1.1: Exemplo de ataque a drone por sequestro (Adaptado de [9]).

1.2 TEMA E PROBLEMA DA PESQUISA

O protocolo MAVLink, amplamente utilizado em *drones*, desempenha um papel crítico na comunicação entre veículos e estações de controle. No entanto, sua popularidade e simplicidade o tornam um alvo atrativo para ataques cibernéticos. Originalmente projetado para priorizar eficiência e flexibilidade, o MAVLink não incorporou camadas robustas de segurança, como criptografia ponta a ponta. Como resultado, a ausência de mecanismos nativos de proteção expõe o protocolo a diversas vulnerabilidades, incluindo ataques de injeção de comandos, interceptação de dados e sequestro de veículo. Esses riscos comprometem não apenas a integridade das operações, mas também a segurança de dados sensíveis trafegados em missões críticas.

O problema é agravado pela crescente integração de *drones* em aplicações comerciais e militares, onde a segurança da comunicação se torna indispensável. Em cenários comerciais, como entregas autônomas, a interceptação de dados pode resultar em perdas financeiras e comprometer a privacidade dos clientes. Em contextos militares ou de segurança pública, ataques cibernéticos, que podem utilizar o protocolo MAVLink como vetor, podem sabotar operações e acessar informações sigilosas.

O problema de pesquisa se concentra na necessidade de compreender e mitigar as vulnerabilidades do MAVLink no contexto de ameaças cibernéticas. Para isso, é essencial realizar uma análise detalhada das falhas de segurança do protocolo, simulando e classificando ataques. Além disso, o desenvolvimento de soluções práticas, como a implementação de criptografia e técnicas de prevenção de ataques, torna-se fundamental para

fortalecer o MAVLink e proteger sistemas críticos que utilizam este protocolo. O objetivo final é aumentar a confiabilidade das operações e assegurar que o MAVLink possa ser utilizado de forma segura em um mundo cada vez mais dependente de veículos conectados.

1.3 OBJETIVO DA PROPOSTA

1.3.1 OBJETIVO GERAL

Investigar vulnerabilidades e desenvolver medidas de proteção para o protocolo MAVLink, com foco em ataques cibernéticos que afetam a comunicação em sistemas de veículos aéreos não tripulados (VANTs).

1.3.2 OBJETIVOS ESPECÍFICOS

a) Identificação e análise de vulnerabilidades do protocolo MAVLink

b) Análise de Impacto e Classificação de Ataques

c) Desenvolvimento de Medidas de Proteção

d) Validação Experimental e Ensaios em Ambientes Reais

1.4 JUSTIFICATIVA DA PROPOSTA

Esta Proposta enquadra-se na área de concentração "Defesa Cibernética" em conformidade com a Portaria Nº 99 do Diretor de Pessoal da Marinha, em 17 de Janeiro de 2024.

1.5 ESTRUTURA DA PROPOSTA

Este trabalho, com exceção desta introdução, possui a seguinte estrutura:

- **Capítulo 2 - Conceitos Básicos**: será apresentada brevemente uma fundamentação teórica de conceitos necessários para o entendimento da Proposta.
- **Capítulo 3 - Trabalhos Relacionados**: será realizada uma apresentação da revisão da literatura, com trabalhos que possuem melhor relação com esta Proposta.
- **Capítulo 4 - a Proposta**: apresentação da Proposta propriamente dita, com elementos de definição como o Problema de Pesquisa, Hipótese, sua Justificativa, Métodos e as Contribuições Esperadas para a Literatura.

- **Capítulo 5 - Plano de Ação**: definição do Projeto de Pesquisa proposto com a divisão das fases de pesquisa.
- **Capítulo 6 - Conclusão**: será apresentada a conclusão da Proposta de Pesquisa.

2 CONCEITOS BÁSICOS

A seguir, serão apresentados alguns conceitos importantes utilizados neste trabalho. Definições como Sistemas embarcados, *drones*, VANTs, Comunicações e seus Protocolos aplicados a Sistemas Embarcados, além de alguns conceitos relacionados a Defesa Cibernética e ao Protocolo MAVLink em particular.

2.1 SISTEMAS EMBARCADOS

Um sistema embarcado é um sistema de computação especializado e dedicado a uma função específica [12]. Diferente dos computadores de propósito geral, que executam tarefas de propósito geral e são projetados para que possam realizar outras tarefas, os sistemas embarcados são projetados para atender funções particulares [13, 14], operando de forma autônoma ou em colaboração com outros sistemas. Geralmente, esses sistemas são compostos por *hardware* e *software* integrados, e são programados para realizar tarefas em tempo real, o que significa que devem responder de forma imediata e precisa a eventos externos. Os sistemas embarcados são amplamente utilizados em diversas áreas, como automóveis, dispositivos médicos, sistemas de telecomunicações, robôs, armas e *drones*.

A arquitetura de um sistema embarcado costuma ser projetada de forma a otimizar o desempenho e o consumo de energia, uma vez que muitos dispositivos em que estão integrados possuem limitações de recursos. Essas restrições exigem que o sistema seja compacto, eficiente e, muitas vezes, que seja resistente a falhas, dado que muitos dispositivos embarcados são implementados em ambientes de operação crítica, como em aeronaves ou equipamentos hospitalares. Por isso, um projeto de um sistema embarcado frequentemente inclui uma combinação de microcontroladores ou microprocessadores, sensores, atuadores e um sistema operacional leve, ou até mesmo a ausência de um sistema operacional, dependendo da complexidade da aplicação.

O conceito de sistemas embarcados em tempo real é amplamente discutido na literatura, geralmente associado à cibernética ou sistemas ciber-físicos [14] em virtude de seu elevado nível de interação com o meio ambiente quando comparado a um sistema computacional de emprego geral.

Sistemas embarcados também referem-se a sistemas que precisam processar dados e

responder a eventos dentro de um limite de tempo específico, onde qualquer atraso pode resultar em falhas no sistema ou até mesmo em riscos à vida humana.

2.2 COMUNICAÇÃO EM SISTEMAS EMBARCADOS

Uma de suas principais classificações é a respeito da temporização da transmissão de dados. Em sistemas embarcados, a comunicação síncrona e assíncrona é empregada de acordo com as necessidades específicas de cada componente [13]. A comunicação síncrona, onde os dispositivos compartilham um sinal de *clock* (relógio, ou temporizador) comum, é utilizada para tarefas de controle e estabilização que exigem baixa latência e precisão temporal. Isso permite que sensores como acelerômetros e giroscópios trabalhem de forma sincronizada com os atuadores, ajustando a orientação e a altitude em tempo real. Alguns exemplos de comunicação síncrona são protocolos como SPI, I2C e DVI [15].

A comunicação assíncrona, por outro lado, é útil para transmissão de dados que não exigem alta precisão temporal, como o envio de imagens e vídeos capturados pela câmera para a base. A utilização de métodos de compressão ajudam a otimizar o envio desses dados, reduzindo a sobrecarga de processamento e consumo de energia, desejáveis em *drones* em virtude das restrições de bateria. Alguns exemplos de comunicação assíncrona são protocolos como o *XBee*, RS-232 e UART.

2.3 PROTOCOLO MAVLINK

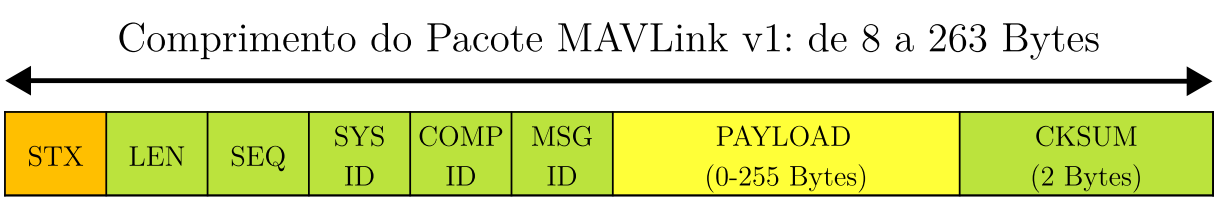
O MAVLink (*Micro Air Vehicle Link*) é um protocolo de comunicação amplamente utilizado em sistemas de VANTs e outras plataformas robóticas. Criado inicialmente para possibilitar a comunicação entre *drones* e estações de controle, o MAVLink se destaca pela simplicidade e eficiência, sendo amplamente adotado em sistemas de controle remoto e automação. Ele opera como um protocolo de mensagens, permitindo a troca de dados como telemetria, comandos de controle e informações de estado do veículo. Sua estrutura baseada em mensagens simplificadas é ideal para aplicações em tempo real e para a comunicação entre dispositivos com recursos limitados, como sensores e atuadores embarcados em *drones*.

Um dos principais elementos do MAVLink é sua organização em mensagens de pacotes (ou *frames*), cada uma das quais contém informações específicas que vão desde comandos básicos de navegação até dados de sensores e informações de diagnóstico. Esses pacotes

são codificados de forma compacta, o que permite reduzir o uso de banda, fator essencial para a comunicação em tempo real e para o controle de dispositivos de baixa potência.

Por atuar na camada de aplicação [4, 16], o MAVLink pode ser utilizado com tecnologias de transmissão, como rádio e Wi-Fi, o que amplia sua flexibilidade para diferentes tipos de operações de veículos aéreos e terrestres, independentemente do ambiente ou da configuração do sistema de comunicação.

Um *frame* é composto por uma sequência de dados agrupados por um ou múltiplos Bytes, cada sequência recebe o nome representado na Figura 2.1 por meio da coluna "Conteúdo", que corresponde à sigla representada em cada seção da representação gráfica do *frame* na parte superior, em ordem temporal crescente lido da esquerda para a direita. É possível relacionar a estrutura de dados do *frame* contida na Figura 2.1 com um exemplo capturado, apresentado posteriormente na Figura 2.4



Índice do Byte no Frame	Conteúdo	Valor	Explicação
0	*Packet start marker*	0xFE	Valor fixo característico do início da mensagem, corresponde ao Byte 0xFE (MAVLink v1)
1	*Payload length*	0 - 255	Comprimento do *Payload* do frame atual.
2	*Packet sequence number*	0 - 255	Sequência de números que incrementa a cada nova mensagem enviada. Aprimora a detecção de pacotes perdidos.
3	*System ID*	1 - 255	Identificador do Veículo (*drone*, estação terrestre...)
4	*Component ID*	1 - 255	Identificador do Componente do Sistema, Podendo ser sensores, câmeras, piloto automático...
5	*Message ID*	0 - 255	Identificador de Tipo de Mensagem (posição GPS, *heartbeat*...)
Para *payload* de n-Bytes: n=0: N/A, n=1: 6, n>=2: 6 a (5+n)	*Payload*	Mensagem propriamente dita. Conteúdo depende do tipo de Mensagem (MSG ID, por exemplo).	
Para *payload* de n-Bytes: (n+6) a (n+7)	*Checksum* (*low* Byte, *high* Byte)	CRC-16/MCRF4XX para a mensagem.	

FIG. 2.1: Organização do *Frame* de uma mensagem de protocolo MAVLink v1 (Adaptado de [17]).

A segurança do protocolo MAVLink é um tema de relevância crescente, dado que a comunicação entre o drone e a estação de controle pode ser alvo de interceptação ou interferência maliciosa. Originalmente, o MAVLink foi desenvolvido sem uma camada de criptografia, o que torna possível que agentes mal-intencionados capturem e alterem pacotes de dados transmitidos. Entretanto, com a popularização do uso de *drones* para aplicações civis e militares, surgiram extensões e adaptações do MAVLink com técnicas de criptografia e autenticação, aumentando a segurança das operações. Tais medidas são essenciais para proteger informações sensíveis, como dados de missão e rotas de navegação, contra acessos não autorizados.

A evolução do MAVLink também inclui o desenvolvimento de novas versões do protocolo, como o MAVLink v2, que trouxe melhorias significativas em termos de segurança. Esta versão mais recente apresenta mecanismos de checagem de erros e a capacidade de autenticação de mensagens, que mitiga ataques como a injeção de comandos falsos e a manipulação de dados. A introdução do protocolo MAVLink v2 é um avanço importante para o uso seguro de *drones* em ambientes complexos, onde a precisão e a integridade dos dados de comunicação são essenciais. Com isso, o MAVLink segue como um protocolo robusto e versátil, ajustando-se às necessidades crescentes de segurança e eficiência no controle de veículos autônomos, com o custo de um aumento no comprimento do frame para o limite superior de 280 Bytes.

Comprimento do Pacote MAVLink v2: de 12 a 280 Bytes

Índice do Byte no Frame	Conteúdo	Valor	Explicação
0	*Packet start marker*	0xFD	Valor fixo característico do início da mensagem, corresponde ao Byte 0xFD (MAVLink v2)
1	*Payload length*	0 - 255	Comprimento do *Payload* do frame atual.
2	*Incompatibility Flags*	*Flags* que devem ser corretamente interpretadas pelo protocolo MAVLink.	
3	*Compatibility Flags*	*Flags* que podem ser ignoradas caso não sejam devidamente interpretadas.	
4	*Packet sequence number*	0 - 255	Sequência de números que incrementa a cada nova mensagem enviada. Aprimora a detecção de pacotes perdidos.
5	*System ID*	1 - 255	Identificador do Veículo (*drone*, estação terrestre...)
6	*Component ID*	1 - 255	Identificador do Componente do Sistema, Podendo ser sensores, câmeras, piloto automático...
7 a 9	*Message ID*	0 – 2^{32}-1 (16777215)	Identificador de Tipo de Mensagem (posição GPS, *heartbeat*...)
Para *payload* de n-Bytes: n=0: N/A, n=1:10, n>=2: 10 a (9+n)	*Payload*	Mensagem propriamente dita. Conteúdo depende do tipo de Mensagem (MSG ID, por exemplo).	
Para *payload* de n-Bytes: (n+10) a (n+11)	*Checksum* (*low* Byte, *high* Byte)	CRC-16/MCRF4XX para a mensagem.	
Para *payload* de n-Bytes: (n+12) a (n+25)	*Signature*	Opcional: Assinatura para verificação de autenticidade	

FIG. 2.2: Organização do *Frame* de uma mensagem de protocolo MAVLink v2 (Adaptado de [17]).

A Figura 2.2 representa o protocolo MAVLink v2 da mesma forma que a Figura 2.1 representa o protocolo MAVLink v1.

O Protocolo MAVLink v2 oferece retrocompatibilidade através da negociação inicial (*handshake*) com dispositivos. De acordo com o apresentado na Figura 2.3, uma Estação de Controle Terrestre envia uma mensagem do tipo `MAV_CMD_REQUEST_PROTOCOL_VERSION`, é feita uma contagem temporal para aguardar a resposta do *drone*, que responde com uma mensagem do tipo `PROTOCOL_VERSION` no padrão MAVLink v2, se a mensagem foi devidamente recebida, a transmissão passa a ocorrer pelo protocolo MAVLink v2.

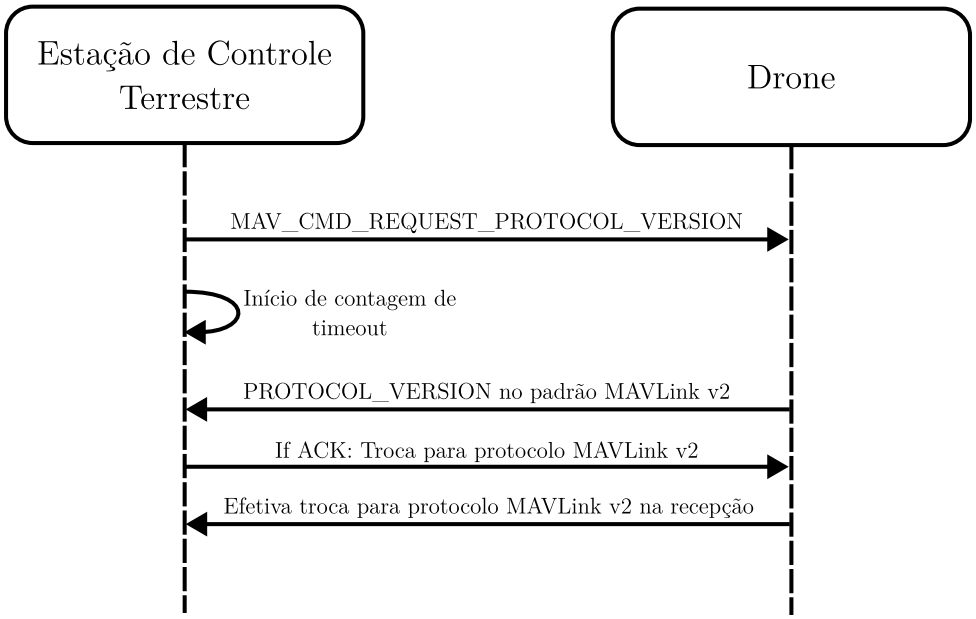


FIG. 2.3: Retrocompatibilidade do protocolo MAVLink v1 e v2 no *handshake* (Adaptado de [17]).

Para exemplificar, encontra-se na Tabela 2.1 um *Frame* enviado por uma Estação Terrestre de número `ID` 255 com um *payload* de 9 Bytes de comprimento enviando um comando do tipo `HEARTBEAT`, cujo propósito é monitorar o estado e a presença de um veículo. Ela fornece informações básicas sobre o tipo de veículo, sua condição operacional e suas capacidades.

Na Figura 2.4 encontra-se um relatório do pacote capturado pelo dispositivo representante do VANT identificando todos os Bytes dos campos relativos ao conteúdo das Figuras 2.1 e 2.2, bem como a distribuição de todos os Bytes apresentados na Tabela 2.1 no *frame*.

TAB. 2.1: *Frame*, escrito em hexadecimal, MAVLink v1 de Exemplo com 9 Bytes de *payload*.

Bytes	**00**	**01**	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**0A**	**0B**	**0C**	**0D**	**0E**	**0F**
00	FE	09	01	FF	00	00	00	00	00	00	00	03	04	04	03	D0
10	EF															

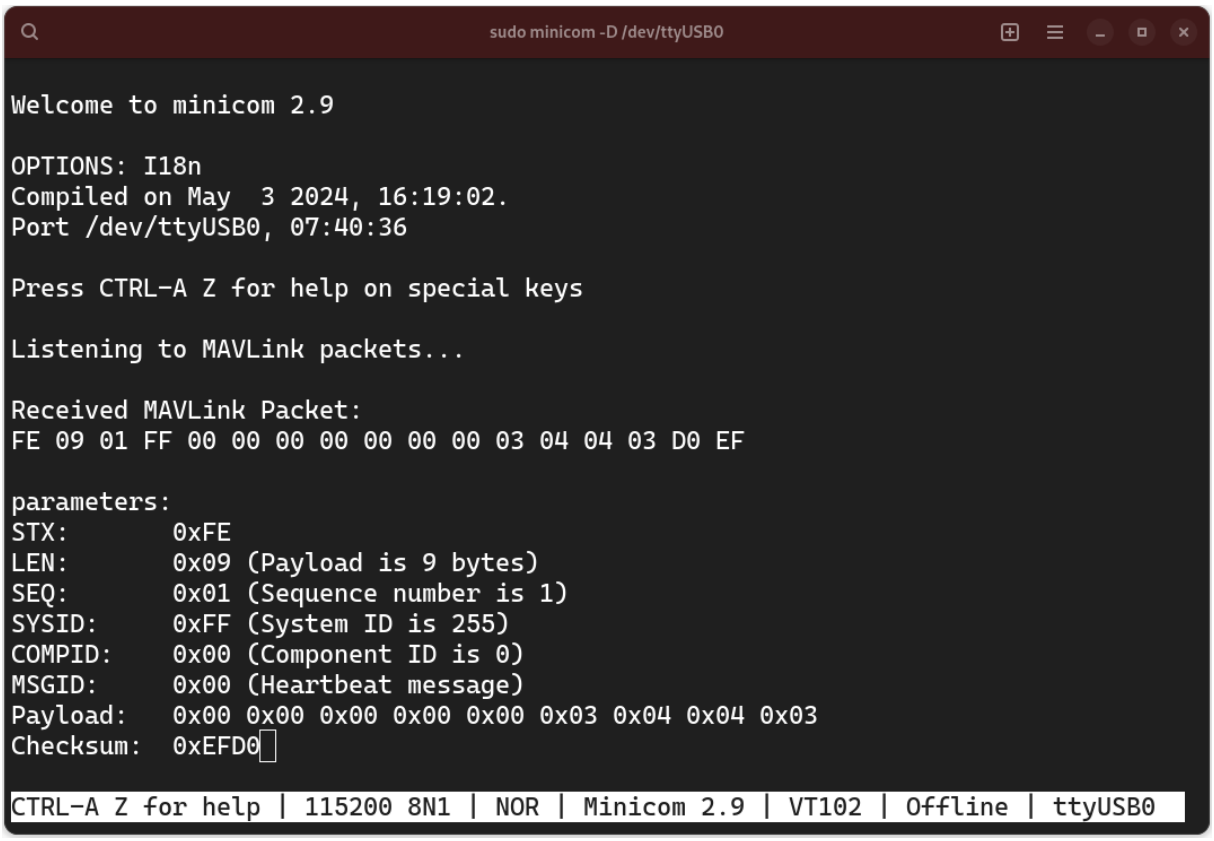


FIG. 2.4: *Frame* de uma mensagem do tipo *heartbeat* capturada, de protocolo MAVLink v1 (Elaboração Própria).

2.4 SEGURANÇA CIBERNÉTICA, VULNERABILIDADES E ATAQUES

Segurança Cibernética faz referência à proteção e garantia de utilização de ativos de informação estratégicos, principalmente os ligados às infraestruturas críticas da informação, abrangendo redes de comunicações, de computadores e seus sistemas informatizados [18].

Este campo é essencial na era digital, onde a interconexão de dispositivos e o armazenamento de dados em redes online aumentam a exposição a potenciais riscos. O conceito de segurança cibernética envolve a implementação de protocolos e a adoção de tecnologias que visam manter a confidencialidade, integridade e disponibilidade das informações.

Além disso, a cibersegurança abrange tanto a proteção de infraestrutura física quanto de ambientes digitais, garantindo que sistemas críticos estejam protegidos de potenciais ataques e interrupções.

De acordo com o Marco Civil da Internet [19], o Estado deve garantir que todas as operações de coleta, armazenamento e tratamento de dados ocorram sob a legislação brasileira, inclusive quando serviços são oferecidos por empresas estrangeiras que atuam no Brasil, além de estabelecer que também é dever do Estado e dos responsáveis pela transmissão de dados assegurar a preservação da estabilidade, segurança e funcionalidade da internet. Além disso, devem ser adotadas boas práticas e padrões internacionais para garantir a segurança.

Dentro desse contexto, as ameaças cibernéticas representam quaisquer fatores ou agentes que possam comprometer a segurança de sistemas e dados. Elas podem ser internas, originadas de dentro da própria organização, ou externas, como agentes mal-intencionados que exploram vulnerabilidades em redes e sistemas. Entre as ameaças mais comuns estão o *malware*, *phishing* e ataques de força bruta, cada um com mecanismos distintos para obter acesso não autorizado ou causar danos ao sistema. Esses agentes de ameaça podem ser criminosos cibernéticos, *hackers* ativistas ou mesmo nações com interesses de espionagem e sabotagem, demonstrando a variedade de perfis envolvidos na prática de ataques cibernéticos [20, 21].

As vulnerabilidades, por sua vez, referem-se a falhas ou pontos fracos em sistemas e *softwares* que podem ser explorados por agentes maliciosos para realizar um ataque. Essas fragilidades podem existir devido a erros de configuração, *bugs* no código-fonte ou até mesmo deficiências na política de segurança de uma organização. Vulnerabilidades conhecidas, como o *SQL Injection* e o *Cross-Site Scripting* (XSS), exemplificam pontos de entrada comuns para invasores em sistemas mal protegidos. É fundamental que essas vulnerabilidades sejam monitoradas e corrigidas por meio de atualizações e *patches* de segurança, visando minimizar as chances de exploração.

Os ataques cibernéticos são a materialização de ameaças que se aproveitam de vulnerabilidades para comprometer a integridade, confidencialidade ou disponibilidade de sistemas e dados. Entre os tipos mais frequentes estão os ataques de negação de serviço (DoS), ataques *ransomware* e exfiltração de dados. Esses ataques podem causar desde prejuízos financeiros até danos irreparáveis à reputação das organizações. A detecção e prevenção de ataques exigem a adoção de práticas de monitoramento contínuo,

além do uso de tecnologias de defesa, como *firewalls*, criptografia e sistemas de detecção de intrusões. Com o avanço das ameaças, a segurança cibernética se torna uma área em constante evolução, necessitando de atualização contínua para proteger contra novas técnicas de ataque e ameaças emergentes.

2.5 CRIPTOGRAFIA ASSIMÉTRICA E *BLOCKCHAIN*

A criptografia é uma técnica fundamental no campo da segurança digital cujas aplicações servem para garantia de sigilo, autenticidade e integridade de dados. Ela é baseada em algoritmos matemáticos que transformam dados legíveis em dados codificados, permitindo que apenas pessoas com a chave correta possam acessá-los. Existem dois tipos principais de criptografia: a criptografia simétrica, onde a mesma chave é usada para encriptação e decriptação, e a criptografia assimétrica, onde é utilizado um par de chaves — uma pública e outra privada — para proteger as informações.

Uma aplicação da criptografia é a *blockchain*, que é uma tecnologia de registro distribuído e descentralizado que emprega criptografia para criar registros seguros e transparentes [22]. Cada transação é armazenada em um "bloco", que é então ligado aos blocos anteriores, formando uma cadeia. Essa estrutura garante que, uma vez registrada, a informação é difícil de ser alterada. A principal função do blockchain é estabelecer confiança entre as partes sem a necessidade de intermediários, como bancos [23], permitindo que todos na rede mantenham uma cópia do registro. Essa transparência e segurança tornam o blockchain adequado para aplicações além das finanças, incluindo contratos, votações e gerenciamento de cadeias de suprimentos.

A *blockchain*, em sua essência, é um livro digital (*ledger*) que registra transações e dados de maneira organizada em blocos, conectados sequencialmente. Cada bloco contém um conjunto de transações e uma referência ao bloco anterior, criando uma cadeia (ou "*chain*") de blocos (ou "*blocks*"). Isso torna qualquer tentativa de adulteração de informações praticamente impossível, pois qualquer alteração em um bloco exigiria a alteração de todos os blocos subsequentes, além de um consenso de mais de 50% dos nós da rede. Essa estrutura inovadora de segurança e descentralização tem sido amplamente adotada em aplicações financeiras, cadeias de suprimentos, votações eletrônicas e contratos inteligentes.

Existe um custo, obviamente, na implementação desta tecnologia. No caso da *blockchain*, os impactos geralmente desaguam em atrasos no processamento para formação

do consenso na rede, um custo computacional associado à mineração dos blocos e maior consumo energético (decorrente do maior custo computacional).

A criptografia na *blockchain* é essencial para assegurar a autenticidade das transações e informações registradas. A combinação de criptografia assimétrica, usada para gerar assinaturas digitais únicas para cada transação, e de algoritmos de *hashing*, que criam uma representação fixa de dados variáveis, assegura que as informações registradas na *blockchain* sejam imutáveis e verificáveis. O algoritmo de *hashing* é usado para gerar um identificador único para cada bloco, chamado de *hash*, que referencia o conteúdo do bloco e o *hash* do bloco anterior. Isso forma a base da integridade dos dados na *blockchain*, pois qualquer tentativa de alterar o conteúdo de um bloco mudaria seu *hash*, quebrando a cadeia e alertando todos os participantes da rede.

O uso *blockchain* robustece a segurança e transparência, sendo essa a razão pela qual a tecnologia tem se expandido para além do setor financeiro. Sua natureza descentralizada elimina a necessidade de intermediários de confiança, como bancos e governos, permitindo transações entre pares (*peer-to-peer*, ou P2P) com segurança e privacidade. Além disso, o uso de contratos inteligentes, códigos autoexecutáveis armazenados na *blockchain*, permite a automação de processos complexos de forma transparente e imutável. Essas características fazem da *blockchain* e da criptografia ferramentas poderosas para enfrentar desafios contemporâneos de segurança e privacidade, tornando-as temas relevantes e promissores para estudos acadêmicos e inovações tecnológicas

3 TRABALHOS RELACIONADOS

Neste capítulo serão apresentados trabalhos que possuem relação com o protocolo MAVLink no contexto de segurança cibernética. É importante ressaltar que os trabalhos citados a seguir não exaurem a literatura acadêmica.

3.1 USO DE *BLOCKCHAINS*

Existem trabalhos [24, 25, 26, 27] disponíveis na literatura de Gestão de Identidade e Coordenação de Enxames de *Drones* usando *blockchain*. Trabalhos com *blockchain* majoritariamente abordam identificação e validação de informações em enxames, como ilustra a Figura 3.1.

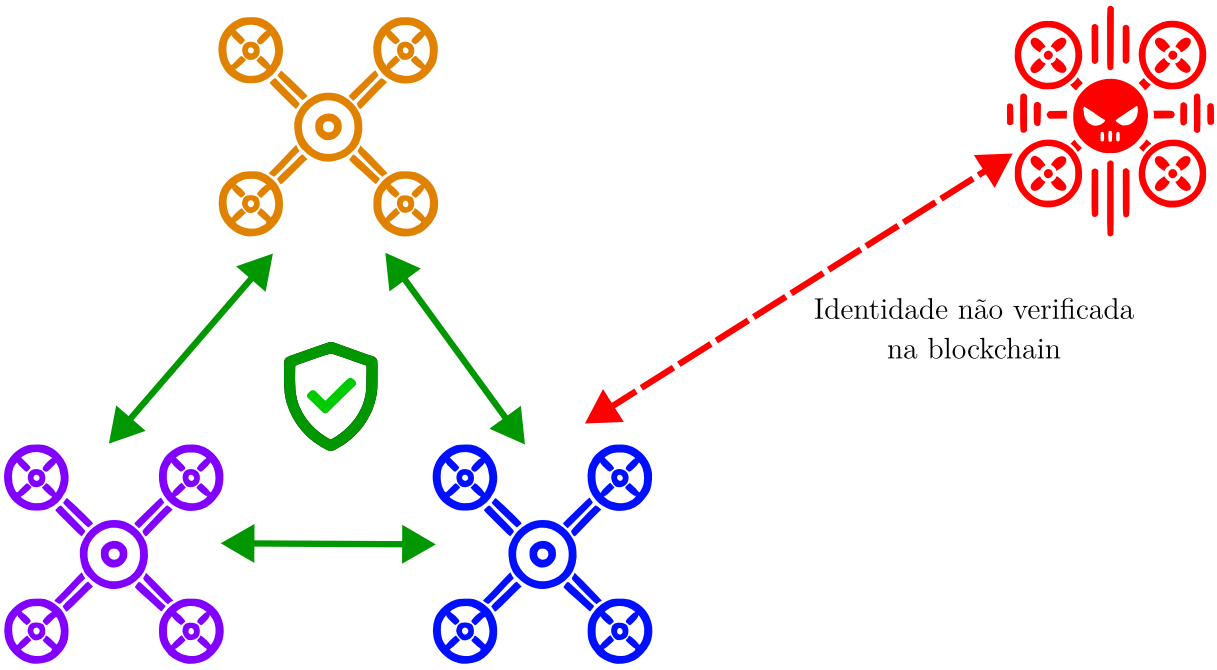


FIG. 3.1: Controle de Acesso e Validação de Comunicação em Enxame de *Drones* (Elaboração Própria).

A Figura 3.1 representa um enxame de *drones* em missão comunicando-se entre si com auxílio de *blockchain* com o intuito de verificar a legitimidade dos dados trafegados por mecanismo de consenso, além de registrar as transações de maneira descentralizada. Ao lado do enxame existe um *drone* malicioso com o objetivo de interferir na coordenação

do enxame.

Recentemente na literatura introduziu-se o uso de *blockchains* para acrescentar segurança na comunicação entre robôs ou entre robôs e estações de controle.

Salimi *et al.* [24] exploram a integração entre a *blockchain Hyperledger Fabric* e o sistema ROS 2 (*Robot Operating System*) em robôs móveis autônomos, buscando resolver desafios relacionados à segurança e gerenciamento de identidade em sistemas distribuídos de robótica. Essa abordagem estrutura uma *blockchain* para gerenciar a identidade dos robôs, permite o controle seguro por meio de contratos inteligentes e assegura a integridade dos dados compartilhados entre robôs em um ambiente industrial.

A proposta é especialmente relevante para aplicações que demandam segurança como vigilância, por exemplo, pois a *blockchain Hyperledger Fabric* oferece controle de acesso em uma rede permissionada, onde somente participantes autorizados interagem e compartilham dados de maneira segura e confiável.

Os resultados experimentais mostram que o impacto da camada de *blockchain* no uso de recursos computacionais, como CPU não superam 30% em um teste de estresse computacional. Além disso, a estrutura foi testada para avaliar sua escalabilidade, o trabalho concluiu que o sistema pode processar transações com frequências de transação superiores a 100Hz, gerando blocos de dados rapidamente, o que é crucial para aplicações em tempo real.

A integração entre ROS 2 e *Hyperledger Fabric* é realizada com uma aplicação, que conecta robôs ao sistema de *blockchain* para armazenar e compartilhar dados, mantendo a integridade e auditabilidade das operações realizadas.

Algumas vantagens da aplicação da ferramenta proposta pelo autor no Protocolo MAVLink são:

a) **Gestão de Identidade e Controle de Acesso**: Em sistemas de *Drones* com MAVLink, o gerenciamento de identidade de cada *drone* é fundamental para evitar acessos não autorizados e falsificação de dados. Com a *blockchain Hyperledger Fabric*, seria possível criar uma camada de autenticação baseada em contratos inteligentes, onde cada *drone* teria uma identidade única registrada na *blockchain*, custodiada entre os participantes autorizados da rede.

b) **Imutabilidade dos Dados de Missão e Auditoria**: Dados de telemetria e *logs* de missão trocados via MAVLink poderiam ser registrados na *blockchain*, garantindo

sua imutabilidade e auditabilidade. Isso é especialmente importante em cenários onde é necessário rastrear e verificar o histórico de cada missão de *drones* para segurança e conformidade.

c) **Consenso e Coordenação de Enxames de *Drones***: Em operações que envolvem enxames de *drones*, como missões de vigilância ou de busca e resgate, o MAVLink facilita a comunicação e coordenação em virtude do acréscimo de um elemento garantidor da integridade para todo o enxame. A integração com uma *blockchain* permissionada poderia adicionar uma camada de consenso entre os *drones*, possibilitando a execução de decisões colaborativas através de contratos inteligentes.

d) **Segurança nas Comunicações**: O MAVLink é um protocolo eficiente, mas não foi projetado com foco em segurança. Integrar *blockchain* para registrar ou validar mensagens MAVLink pode fornecer uma camada adicional de integridade dos dados.

Bendiab *et al.* [27] exploram várias ameaças de segurança cibernética em veículos autônomos e discute o uso potencial de tecnologias de *blockchain* e Inteligência Artificial (IA) para mitigá-las. No contexto de *drones*, esses sistemas autônomos enfrentam desafios semelhantes de segurança, especialmente no que diz respeito à interceptação de dados, ataques de injeção e intrusão em redes de comunicação. *Drones*, como veículos autônomos, utilizam canais de comunicação sem fio, incluindo Wi-Fi, Bluetooth e redes móveis, que são suscetíveis a ataques *man-in-the-middle* (MITM), onde invasores podem interceptar e manipular dados transmitidos entre *drones* e suas unidades de controle.

Ademais, o trabalho destaca a aplicabilidade da IA para detectar anomalias em tempo real nos sistemas de navegação dos *drones*, o que é fundamental para prevenir manipulações de sensores, como radar e LiDAR, que podem comprometer a precisão dos dados de localização. Modelos de aprendizado profundo são mencionados como ferramentas eficazes para identificar padrões anômalos que indicam tentativas de invasão.

Esse mecanismo é particularmente relevante para *drones*, cujos sensores podem ser alvo de ataques de "ofuscamento de sensores" (*sensor blinding*), prejudicando a operação autônoma segura e a navegação eficiente.

Além disso, o artigo explora o potencial da *blockchain* para proteger redes de *drones*, atuando como uma plataforma segura e confiável para armazenamento e compartilhamento de dados. Em redes de *drones*, a *blockchain* pode ser usada para autenticar e verificar cada comunicação, dificultando ataques baseados em identidade e prevenindo a

alteração maliciosa de dados. Essa arquitetura distribui a responsabilidade de segurança por uma rede descentralizada, reduzindo a dependência de um único ponto vulnerável e aumentando a resiliência contra ataques de negação de serviço

Por fim, o estudo sugere que uma abordagem colaborativa, como o uso de aprendizado de máquina combinado com *blockchain*, pode reforçar ainda mais a segurança de *drones* ao permitir a atualização e treinamento de modelos de segurança distribuídos, sem a necessidade de compartilhamento direto de dados sensíveis. Essa configuração é vantajosa para cenários de *drones* em que a privacidade dos dados é crucial, como em operações de vigilância e monitoramento de áreas restritas. No entanto, o artigo também identifica que a aplicação dessas tecnologias ainda está em fase experimental, e que desafios como a escalabilidade e o consumo de energia precisam ser abordados para uma implementação prática e eficiente.

Em 2024, Bo Sullivan e Khan [25] exploram o protocolo OBSERVE, uma solução baseada em *blockchain* e modelos leves de aprendizado de máquina para aplicar o conceito de *Zero Trust* em veículos conectados e autônomos (CAVs). O objetivo do OBSERVE é permitir que os veículos validem, em tempo real, as trajetórias de seus vizinhos para uma navegação segura e coordenada, principalmente em ambientes onde é necessário confiar nos dados de localização de outros veículos.

Para cumprir tal missão, OBSERVE utiliza um *blockchain* permissionado para registrar informações de confiabilidade sobre os trajetos validados, promovendo segurança, eficiência energética e precisão na previsão das trajetórias. Ao contrário de abordagens que usam algoritmos de visão computacional. O protocolo aposta em modelos de aprendizado de máquina leves, que reduzem o consumo de recursos e aumentam a eficiência em ambientes com restrições de energia.

Este trabalho pode melhorar a segurança do Protocolo MAVLink considerando missões com enxame de *drones*, onde a troca de informação sobre a navegação de cada unidade para coordenação de trajetórias pode exigir confiabilidade e sigilo na troca de dados em ambientes hostis.

Algumas vantagens da aplicação da ferramenta proposta pelo autor no Protocolo MAVLink são:

a) **Validação de Trajetórias e Coordenação Segura**: Assim como OBSERVE propõe uma validação de trajetórias entre veículos autônomos, o protocolo MAVLink poderia ser adaptado para uma configuração similar entre *drones*. O MAVLink

pode transmitir dados de telemetria e trajetória em tempo real, e uma camada de *blockchain* poderia armazenar e validar esses dados, criando um sistema onde *drones* coordenam trajetórias uns dos outros. Essa validação colaborativa seria especialmente útil em missões de mapeamento ou vigilância, onde é crucial garantir que as informações de localização e rota sejam autênticas e confiáveis.

b) **Consenso Descentralizado para Coordenação de Missão**: Em operações com múltiplos *drones*, o protocolo OBSERVE poderia ser aplicado para garantir consenso descentralizado em decisões de navegação. Os *drones* poderiam utilizar MAVLink para transmitir dados e *blockchain* para validar e registrar decisões, como pontos de encontro ou mudanças de rota. Isso ajudaria a evitar colisões e garantir uma distribuição eficaz de tarefas, mesmo em cenários onde a comunicação com uma estação base é limitada.

3.2 PROTOCOLOS DE COMPARTILHAMENTO DE CHAVES

Recentemente, Vasudev *et al.* [28] publicaram um trabalho que explora um protocolo chamado *LightKey*, desenvolvido para garantir comunicações seguras e leves entre veículos na Internet de Veículos (IoV). A IoV conecta veículos a infraestruturas e dispositivos, sendo vital para a comunicação segura no trânsito.

A proposta do *LightKey* é uma solução de autenticação e acordo de chaves que visa equilibrar segurança e eficiência operacional. A estrutura do protocolo inclui diversas fases, como pré-registro e autenticação, todas projetadas para serem leves e robustas contra ataques como *replay*, *Man-in-the-Middle* e captura física do veículo. A segurança do *LightKey* é validada através de uma análise formal usando a ferramenta Scyther, que verifica a resistência do protocolo contra uma série de ataques comuns em redes veiculares. Os resultados indicaram a robustez do *LightKey*, comprovando sua resiliência contra ataques direcionados à interceptação de dados.

Segundo os autores, a análise de desempenho mostra que o *LightKey* consome cerca de 10% menos recursos computacionais que outros protocolos similares, o que o torna adequado para ser implementado na unidade de bordo (OBU) dos veículos. Essa eficiência é atribuída ao uso de operações criptográficas leves, como funções de hash e operações de cifra, mantendo a segurança do sistema. Em comparação com protocolos concorrentes, *LightKey* se destacou não apenas pela rapidez, mas também por oferecer resistência a

uma gama mais ampla de ataques.

Como conclusão, o *LightKey* mostra-se uma solução promissora para sistemas de IoV, equilibrando segurança e desempenho, essenciais para um ambiente de tráfego cada vez mais conectado. A proposta ainda deixa margem para futuros estudos que envolvam a implementação do *LightKey* em cenários reais, com a expectativa de validar seu desempenho e segurança em aplicações práticas e em tempo real, outro fator a se considerar é que o protocolo diferencia-se ao usar um canal público para registro, embora isso torne o sistema mais vulnerável a ataques.

3.3 ESTUDOS DE VULNERABILIDADES

A literatura tem se debruçado por meio de trabalhos [2, 10, 29, 30] ao inserir veículos inteligentes, sejam eles autônomos ou semiautônomos, na categorização de ataques e estudar suas vulnerabilidades.

Para Elkhail *et al.* [29], sistemas de telemática são destacados como vulnerabilidades críticas em veículos inteligentes modernos. Sistemas de telemática, que monitoram e relatam dados veiculares (como velocidade, posição, eficiência do combustível ou baterias, entre outros), permitem a comunicação em redes, abrindo caminho para ataques remotos. Pesquisas mostraram que, com técnicas de engenharia reversa, é possível acessar o sistema operacional de dispositivos de telemática, explorando vulnerabilidades em *frameworks* baseados em Android, o que permite que um atacante acesse e controle remotamente funções do veículo como ligar/desligar seus motores.

Apesar de tal artigo concentrar-se mais veículos terrestres, tais veículos assemelham-se muito com enxames de *drones* sob o ponto de vista da conectividade externa, tendo em vista que são altamente dependentes de conectividade em rede. Essas vulnerabilidades mostram a importância de implementar medidas de segurança rigorosas para proteger esses sistemas, que, além de serem essenciais para o conforto e a conectividade dos veículos, podem representar um grande risco se forem comprometidos.

Mais especificamente no protocolo MAVLink, existe uma *survey* recente [30] que aborda especificamente suas principais vulnerabilidades e que apresenta muitos pontos em comum com veículos terrestres abordados no trabalho de Elkhail *et al.* [29]:

- **Foco nas Vulnerabilidades dos Protocolos de Comunicação**: Ambos os artigos examinam as fraquezas de segurança em protocolos críticos de comunicação. O

artigo *Vehicle Security* explora vulnerabilidades em protocolos como o barramento CAN para veículos, enquanto o artigo sobre o Protocolo MAVLink analisa o MAVLink, um protocolo comum para comandos e telemetria de *drones*. Em ambos os casos, esses protocolos são suscetíveis a vários tipos de ataques devido às características limitadas de segurança nativa.

- **Riscos de Ataques Remotos**: Os artigos destacam a suscetibilidade desses sistemas a ataques remotos, como interceptação, spoofing e negação de serviço (DoS). A natureza não segura das comunicações sem fio constitui um grande fator de risco, expondo tanto veículos quanto *drones* a interceptações e controle não autorizado.

- **Vetor de Ataque e Modelos de Ameaça**: Cada artigo apresenta um modelo de ameaças, detalhando os possíveis vetores de ataque que atores mal-intencionados poderiam explorar. Para os veículos, os pontos de entrada incluem portas OBD-II, sistemas de infotainment e redes sem fio. Para os *drones*, são identificadas vulnerabilidades nas assinaturas de mensagens e nos recursos de timestamp do protocolo MAVLink, que podem levar a ataques de *spoofing* e *replay*.

- **Impacto nos Sistemas de Controle**: Ambos os artigos enfatizam o impacto crítico que sistemas de controle comprometidos podem ter. Em veículos, os invasores podem interromper funcionalidades, afetando sistemas de segurança como freios e direção. De forma semelhante, em *drones*, um invasor pode sequestrar o controle ou interromper a missão, o que pode gerar consequências perigosas.

- **Estratégias de Mitigação**: Ambos os trabalhos recomendam estratégias para melhorar a segurança. Para veículos, sugerem-se métodos como o fortalecimento da criptografia das redes e a implementação de sistemas de detecção de intrusão. Para *drones*, as recomendações incluem melhorias na segurança do MAVLink, como tornar obrigatória a assinatura de mensagens e aprimorar as práticas de gerenciamento de chaves.

De acordo com Ficco *et al.* [30], as principais vulnerabilidades do protocolo MAVLink, são:

- **Falta de Assinatura Padrão nas Mensagens**: A assinatura das mensagens não é ativada por padrão, contrariando o princípio de "Segurança por Padrão".

Isso permite que agentes maliciosos injetem pacotes sem autenticação, assumindo controle sobre o VANT.

- **Exposição da Chave Secreta**: A mensagem "SETUP SIGNING"contém a chave secreta em texto claro, o que permite que qualquer interceptador na rede possa capturar essa chave, comprometendo a segurança da comunicação entre o VANT e a Estação de Controle em Terra (GCS).

- **Fragilidade na Implementação de Assinatura**: A assinatura do MAVLink 2.0 utiliza um hash de apenas 48 bits de um SHA-256, o que torna a assinatura vulnerável a ataques de colisão e forjamento, permitindo que invasores gerem assinaturas falsas.

- **Chaves Fracas**: A geração da chave secreta não exige senhas fortes, facilitando ataques de dicionário para descobrir a chave e comprometer a integridade das mensagens.

- **Problemas com *Timestamps***: Falhas na gestão de *timestamps* permitem ataques de repetição e injeção de mensagens. Se uma mensagem com timestamp muito à frente é recebida, as mensagens subsequentes podem ser rejeitadas, abrindo caminho para ataques de negação de serviço (DoS).

A adoção de criptografia ponta a ponta no protocolo MAVLink é um passo importante para garantir o sigilo das comunicações entre drones e estações de controle, protegendo contra ataques de interceptação e manipulação de dados. Com uma abordagem de ponta a ponta, as mensagens são criptografadas no ponto de envio e somente descriptografadas no ponto de recepção, impedindo que intermediários acessem ou alterem os dados transmitidos. No entanto, dado o crescente risco de ataques cibernéticos mais sofisticados como ataques do tipo “Harvest Now, Decrypt Later” (HNDL) [31], é necessário considerar soluções resistentes, ampliando a proteção do MAVLink contra ameaças futuras e preservando a integridade de missões críticas.

Em 2024, a Apple Inc. [32] apresentou o protocolo PQ3 como uma atualização para o seu aplicativo de mensagem instantânea “iMessage”. O uso está baseado em criptografia pós-quântica ponta a ponta para o estabelecimento de um canal de comunicação seguro para o seu serviço. Além disso, o protocolo também implementa atualização de chaves

(*rekeying*) periódico e propriedades de "autocura", garantindo que eventuais comprometimentos de chaves de segurança pontuais não impactem mensagens futuras.

Apesar da criptografia pós-quântica não encontrar-se no escopo desta Proposta, a adoção de criptografia ponta a ponta e um mecanismo de gerenciamento de chaves encontram-se no escopo desta Proposta.

3.4 QUADRO COMPARATIVO

Na Tabela 3.1 há um breve resumo comparativo acerca dos principais trabalhos relacionados ao Problema de Pesquisa:

TAB. 3.1: Principais trabalhos encontrados para a Área de Pesquisa.

Categoria	Foco de Pesquisa	Referência
Estudos de Vulnerabilidades	Estado da Arte do Protocolo MAVLink	Koubâa et al. (2023)
	Análise de Vulnerabilidades do Protocolo MAVLink em drones	Ficco et al. (2022)
	Estado da Arte em Vulnerabilidades em Automóveis Autônomos	Elkhail et al. (2021)
	Resenha de segurança cibernética em automóveis autônomos	Kim et al. (2021)
	Resenha de segurança cibernética em drones	Wang et al. (2023)
	Análise Experimental de vulnerabilidades do Protocolo MAVLink	Xu et al. (2021)
	Análise de Vulnerabilidades do Protocolo MAVLink em drones	Allouch et al. (2019)
Protocolos de Compartilhamento de Chaves	Protocolo de Negociação de Chaves em Automóveis Autônomos	Vasudev et al. (2024)
	Protocolo de Negociação de Chaves para autenticação em IoV	Cui et al. (2024)
Blockchain	Protocolo de Coordenação de Trajetórias para Automóveis Autônomos	Sullivan et Khan (2024)
	Implementação de Blockchain para Coordenação de Tarefas em Robótica	Salimi et al. (2023)
	Implementação de Blockchain para aprimorar a segurança de veículos elétricos	Kaur et al. (2021)
	Blockhain para preservação de dados em automóveis autônomos	Yang et al. (2024)
	Blockchain e Inteligência Artificial para aprimoramento de segurança em automóveis autônomos	Bendiab et al. (2023)
Inteligência Artificial	Resenha de segurança cibernética em automóveis autônomos	Kim et al. (2021)
	Uso de Inteligência Artificial para segurança em automóveis autônomos	Saoud et al. (2024)
Criptografia Ponta a Ponta	Criptografia pós-quântica ponta a ponta com mecanismo de gerenciamento de chaves	Apple Inc. (2024)

4 A PROPOSTA

Este trabalho se propõe a desenvolver um projeto de pesquisa de forma a atender o objetivo e questões abaixo descritos:

4.1 PROBLEMA DE PESQUISA

Como a segurança do protocolo MAVLink pode ser aprimorada?

Obviamente, em decorrência da investigação de tal pergunta surgem outras como:

- A que ameaças os veículos que utilizam este protocolo estão sujeitos?
- Quais medidas de proteção podem ser implementadas para aprimorar a segurança do protocolo?
- Qual é a eficiência energética das medidas de proteção sugeridas?
- Qual é a eficácia de tais medidas de proteção?

4.2 HIPÓTESE

Hipótese 1. *É possível aprimorar a segurança do protocolo MAVLink.*

4.2.1 JUSTIFICATIVA DA HIPÓTESE

Através da análise sistemática de vulnerabilidades, bem como a proposta de medidas de proteção será possível responder às perguntas do problema de pesquisa.

4.3 MÉTODO

Em primeiro lugar, uma bancada de testes em dispositivos virtuais em uma rede controlada será implementada para reproduzir ensaios de segurança envolvendo o protocolo MAVLink.

Em seguida, testes de segurança serão realizados em tal ambiente virtual com análise de estatísticas, anomalias e falhas, com posterior classificação de ataques.

Além da referida análise, esta fase da pesquisa também possui sua importância sobretudo para definir a reprodutibilidade dos testes para a Comunidade Acadêmica em eventuais publicações de artigos, dando publicidade às ferramentas de virtualização com todas as configurações e parâmetros necessários para tal.

Identificadas as principais vulnerabilidades, serão propostas medidas de proteção aos dispositivos atacados e serão verificadas a eficiência e eficácia de suas implementações. Comparações com o estado do experimento inicial também se incluem nesta fase.

Nesta fase da pesquisa, haverá a oportunidade de realizar publicações de artigos comparando os resultados obtidos com o da Literatura Acadêmica.

Os experimentos realizados em ambiente virtual serão testados em um ambiente controlado com dispositivos reais.

A depender da evolução da pesquisa, algumas sugestões de melhoria na segurança poderão também ser testadas e avaliadas com modelos de *drones* em voos reais e comparadas com os resultados anteriores.

Por fim, será feito um comparativo acompanhado de suas conclusões, respondendo, portanto, o problema de pesquisa.

4.4 CONTRIBUIÇÕES ESPERADAS

A Dissertação contribuirá tecnicamente com:

- a implementação de medidas de proteção ao protocolo MAVLink; e
- a apresentação de um comparativo de consumo energético das medidas de proteção sugeridas com o cenário sem as medidas implementadas

e, também, contribuirá cientificamente com:

- a proposição de um ambiente virtual para testes e reprodutibilidade das experiências; e
- a consolidação de métricas de eficácia das medidas de proteção sugeridas.

5 PLANO DE AÇÃO

O plano para o desenvolvimento desta proposta de pesquisa inclui as atividades descritas na Tabela 5.1:

TAB. 5.1: Lista de Atividades

	Atividade
1	Revisão Bibliográfica e Fundamentação Teórica
2	Apresentação da Proposta
3	Identificação de Vulnerabilidades e Simulação de Ataques no MAVLink
4	Análise de Impacto e Classificação de Ataques
5	Desenvolvimento de Medidas de Proteção
6	Validação Experimental e Testes em Ambientes Reais
7	Submissão em Periódicos
8	Defesa da Dissertação

5.1 VIABILIDADE

As atividades descritas são consideradas factíveis considerando as instalações do Instituto Militar de Engenharia, especialmente do Laboratório de Segurança Cibernética de Infraestruturas Críticas (LaSC) para prestar apoio nas simulações de cenários de ataques virtuais com múltiplos dispositivos e do Laboratório de Inteligência Artificial, Robótica e Cibernética (LIARC) em eventuais atividades práticas com seus veículos e *hardware* para comunicações em Sistemas Embarcados.

5.2 CRONOGRAMA

A Proposta de Pesquisa prevê tanto o estudo de segurança do protocolo em um ambiente virtual controlado quanto em testes com equipamentos reais. O cronograma para o desenvolvimento das atividades relacionadas pode ser visto na Tabela 5.2.

Em um cenário otimista, será possível identificar as vulnerabilidades, apresentar suas soluções em ação em um ambiente real, apresentar vantagens e desvantagens de soluções para as vulnerabilidades, bem como sua validação experimental e, por fim, avaliar a efetividade das implementações.

Em um cenário de grandes dificuldades, ainda será possível identificar as vulnerabilidades, a apresentação de soluções poderá ser realizada somente em ambiente virtual, haverá uma certa degradação na análise de vantagens e desvantagens em virtude da falta de validação em ambiente real, porém ainda será possível realizar uma avaliação, ainda que limitada, da efetividade das implementações.

TAB. 5.2: Cronograma de Atividades (2025)

Tarefa	**JAN**	**FEV**	**MAR**	**ABR**	**MAIO**	**JUN**	**JUL**	**AGO**	**SET**	**OUT**	**NOV**	**DEZ**
Revisão Bibliográfica e Fundamentação Teórica	X											
Apresentação da Proposta	X	X										
Identificação de Vulnerabilidades e Simulação de Ataques no MAVLink		X	X	X								
Análise de Impacto e Classificação de Ataques				X	X	X						
Desenvolvimento de Medidas de Proteção						X	X	X	X			
Validação Experimental e Testes em Ambientes Reais									X	X	X	
Submissão em Periódicos					X	X						
Defesa da Dissertação												X

6 CONCLUSÃO

Esta Proposta de Dissertação destaca a importância da segurança no protocolo MAVLink, utilizado amplamente na comunicação entre veículos aéreos não tripulados e suas respectivas estações de controle. A popularização dos *drones* em diversas áreas, incluindo aplicações comerciais, industriais e militares, reforça a necessidade de um protocolo de comunicação robusto e seguro. A análise das vulnerabilidades do MAVLink é fundamental para compreender as ameaças cibernéticas às quais esses sistemas estão expostos, como sequestros, injeção de comandos maliciosos e interceptação de dados.

Com base em uma metodologia estruturada, a Pesquisa Proposta busca identificar e classificar as vulnerabilidades do protocolo MAVLink, além de desenvolver e validar medidas de mitigação. Os experimentos serão conduzidos tanto em ambientes virtuais quanto em dispositivos reais, garantindo uma abordagem abrangente para avaliação da segurança do protocolo. Além disso, a comparação das soluções implementadas com o estado atual da literatura permitirá uma melhor compreensão da eficácia das propostas e seu impacto no consumo energético dos sistemas embarcados.

Espera-se que os resultados desta pesquisa contribuam significativamente para a segurança das comunicações entre *drones* e estações de controle, propondo soluções eficazes para reduzir os riscos associados ao uso do protocolo MAVLink. A implementação de técnicas como criptografia ponta a ponta, autenticação e outros mecanismos de proteção pode aumentar a resiliência desses sistemas frente a ataques cibernéticos, tornando a operação de VANTs mais segura em diferentes cenários de aplicação.

Por fim, esta Proposta pretende fornecer um ambiente experimental replicável para futuras pesquisas na área de segurança cibernética em sistemas embarcados. A proposta de um ambiente virtual para testes permitirá que a comunidade acadêmica continue aprimorando as soluções de segurança para o protocolo MAVLink, promovendo o desenvolvimento de estratégias cada vez mais eficientes para a proteção da comunicação entre *drones* e seus sistemas de controle.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] ISO 20252:2019 third edition: Market, opinion and social research, including insights and data analytics — vocabulary and service requirements, February 2019.

[2] Arslan Shafique, Abid Mehmood, and Mourad Elhadef. Survey of Security Protocols and Vulnerabilities in Unmanned Aerial Vehicles. *IEEE Access*, 9:46927–46948, 2021. Conference Name: IEEE Access.

[3] Trupil Limbasiya, Debasis Das, and Sajal K. Das. MComIoV: Secure and Energy-Efficient Message Communication Protocols for Internet of Vehicles. *IEEE/ACM Transactions on Networking*, 29(3):1349–1361, June 2021. Conference Name: IEEE/ACM Transactions on Networking.

[4] Anis Koubâa, Azza Allouch, Maram Alajlan, Yasir Javed, Abdelfettah Belghith, and Mohamed Khalgui. Micro Air Vehicle Link (MAVlink) in a Nutshell: A Survey. *IEEE Access*, 7:87658–87680, 2019. Conference Name: IEEE Access.

[5] Rafael G. Braga, Roberto C. da Silva, Alexandre C. B. Ramos, and Felix Mora-Camino. Collision Avoidance Based on Reynolds Rules: A Case Study Using Quadrotors. In Shahram Latifi, editor, *Information Technology - New Generations*, pages 773–780, Cham, 2018. Springer International Publishing.

[6] Young-Min Kwon, Jaemin Yu, Byeong-Moon Cho, Yongsoon Eun, and Kyung-Joon Park. Empirical Analysis of MAVLink Protocol Vulnerability for Attacking Unmanned Aerial Vehicles. *IEEE Access*, 6:43203–43212, 2018. Conference Name: IEEE Access.

[7] Steve Corrigan. Introduction to the Controller Area Network (CAN). Application Report, Texas Instruments, May 2016.

[8] Yu Luo, Yehua Wei, Defeng Ding, and Jiaying Xie. An In-Vehicle Network Security Protocol Based on Dynamic Encryption. In *2020 7th International Conference on Information Science and Control Engineering (ICISCE)*, pages 286–290, December 2020.

[9] Yassine Mekdad, Abbas Acar, Ahmet Aris, Abdeslam El Fergougui, Mauro Conti, Riccardo Lazzeretti, and Selcuk Uluagac. Exploring Jamming and Hijacking At-

tacks for Micro Aerial Drones. In *ICC 2024 - IEEE International Conference on Communications*, pages 1939–1944, June 2024. ISSN: 1938-1883.

[10] Brúnó Krasnyánszki, Sándor Tihamér Brassai, and András Németh. UAV weaknesses against deauthentication based hijacking attacks. In *2024 IEEE 22nd World Symposium on Applied Machine Intelligence and Informatics (SAMI)*, pages 000493–000498, January 2024. ISSN: 2767-9438.

[11] Vuk Lesi, Ilija Jovanov, and Miroslav Pajic. Security-Aware Scheduling of Embedded Control Tasks. *ACM Trans. Embed. Comput. Syst.*, 16(5s):188:1–188:21, September 2017.

[12] Steve Heath. *Embedded Systems Design*. Elsevier Science, 2nd edition, October 2002.

[13] Kiyofumi Tanaka. *Embedded Systems - High Performance Systems, Applications and Projects*. March 2012.

[14] Edward Ashford Lee and Sanjit Arunkumar Seshia. *Introduction to Embedded Systems, A Cyber-Physical Systems Approach*. MIT Press, second edition, 2017.

[15] Dimitrios Slamaris. *Embedded Systems Security and TrustZone*.

[16] ISO/IEC 7498-1:1994 Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model, 1994.

[17] MAVLink Developer Guide. https://mavlink.io/en/.

[18] Brasil Presidência da República Secretaria de Assuntos Estratégicos and Ulisses de Mesquita (Org) Gomes. Desafios estratégicos para segurança e defesa cibernética. 2011. Accepted: 2012-11-07T17:00:33Z.

[19] Câmara dos Deputados. Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014, 2014.

[20] BRASIL. Estratégia Nacional de Defesa, September 2024.

[21] International Organization for Standardization. *ISO/IEC 27001:2022, Third Edition: Information security, cybersecurity and privacy protection - Information security management systems - Requirements*. Multiple. Distributed through American National Standards Institute, October 2022.

[22] Alan T. Norman. *Blockchain Technology Explained: The Ultimate Beginner's Guide About Blockchain Wallet, Mining, Bitcoin, Ethereum, Litecoin, Zcash, Monero, Ripple, Dash, IOTA And Smart Contracts*. Independently published, March 2021.

[23] Nurul Hassan, Nishchay Jain, and Vinay Chandna. *BLOCKCHAIN, CRYPTOCURRENCY AND BITCOIN*. April 2018.

[24] Salma Salimi, Jorge Peña Queralta, and Tomi Westerlund. Hyperledger Fabric Blockchain and ROS 2 Integration for Autonomous Mobile Robots. In *2023 IEEE/SICE International Symposium on System Integration (SII)*, pages 1–8, January 2023. ISSN: 2474-2325.

[25] Bo Sullivan and Junaid Ahmed Khan. OBSERVE: Blockchain-Based Zero Trust Security Protocol for Connected and Autonomous Vehicles (CAVs) Data Using Simple Machine Learning. In *2024 International Conference on Computing, Networking and Communications (ICNC)*, pages 554–559, February 2024. ISSN: 2473-7585.

[26] Kuljeet Kaur, Georges Kaddoum, and Sherali Zeadally. Blockchain-Based Cyber-Physical Security for Electrical Vehicle Aided Smart Grid Ecosystem. *IEEE Transactions on Intelligent Transportation Systems*, 22(8):5178–5189, August 2021. Conference Name: IEEE Transactions on Intelligent Transportation Systems.

[27] Gueltoum Bendiab, Amina Hameurlaine, Georgios Germanos, Nicholas Kolokotronis, and Stavros Shiaeles. Autonomous Vehicles Security: Challenges and Solutions Using Blockchain and Artificial Intelligence. *IEEE Transactions on Intelligent Transportation Systems*, 24(4):3614–3637, April 2023. Conference Name: IEEE Transactions on Intelligent Transportation Systems.

[28] Harsha Vasudev, Mohd Shariq, Sanjeev Kumar Dwivedi, and Mauro Conti. LightKey: Lightweight and Secure Key Agreement Protocol for Effective Communication in Internet of Vehicles. In *Proceedings of the 25th International Conference on Distributed Computing and Networking*, ICDCN '24, pages 209–216, New York, NY, USA, January 2024. Association for Computing Machinery.

[29] Abdulrahman Abu Elkhail, Rafi Ud Daula Refat, Ricardo Habre, Azeem Hafeez, Anys Bacha, and Hafiz Malik. Vehicle Security: A Survey of Security Issues and

Vulnerabilities, Malware Attacks and Defenses. *IEEE Access*, 9:162401–162437, 2021. Conference Name: IEEE Access.

[30] Massimo Ficco, Raffaele Palmiero, Massimiliano Rak, and Daniele Granata. MAVLink Protocol for Unmanned Aerial Vehicle: Vulnerabilities Analysis. In *2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, pages 1–6, September 2022.

[31] Keyfactor. Harvest Now, Decrypt Later: A New Form of Attack. https://www.keyfactor.com/blog/harvest-now-decrypt-later-a-new-form-of-attack/. Accessed on 2025-01-15.

[32] APPLE. iMessage with PQ3: The new state of the art in quantum-secure messaging at scale - Apple Security Research. https://security.apple.com/blog/imessage-pq3/ . Accessed on 2025-01-15.

[33] Fatma S. Alrayes, Mohammed Aljebreen, Mohammed Maray, Asma Alshuhail, Faheed A.F. Alrslani, and Ahmed S. Salama. Optimizing Security Protocol: A Synergy of Bio-inspired Planet Optimization Algorithm with Ensemble Learning-based Attack Detection for Connected and Autonomous Vehicles. *IEEE Access*, pages 1–1, 2024. Conference Name: IEEE Access.

[34] Nancy Alshaer, Ahmed Moawad, and Tawfik Ismail. Reliability and Security Analysis of an Entanglement-Based QKD Protocol in a Dynamic Ground-to-UAV FSO Communications System. *IEEE Access*, 9:168052–168067, 2021. Conference Name: IEEE Access.

[35] Meili Cui, Zhenhu Ning, Junchen Gao, and Jin Peng. Security Key Management Protocol for Cross-domain Authentication of Internet of Vehicles. In *2024 4th International Conference on Information Communication and Software Engineering (ICICSE)*, pages 126–130, May 2024.

[36] Hamaciré El Hadj Kalil, Ahmed Dooguy Kora, and Selma Boumerdassi. Security in VANETs: Lightweight Protocol for Group-of-Vehicles Masters (LPGVM). In *2020*

22nd International Conference on Advanced Communication Technology (ICACT), pages 6–11, February 2020. ISSN: 1738-9445.

[37] Mahmoud Elfar, Haibei Zhu, M. L. Cummings, and Miroslav Pajic. Security-Aware Synthesis of Human-UAV Protocols. In *2019 International Conference on Robotics and Automation (ICRA)*, pages 8011–8017, May 2019. ISSN: 2577-087X.

[38] Vivian Gao, Nanlin Lei, Shaoqing He, Xiaoyu Jia, Chaoshuo Wang, Qiang Zhang, and Qiuye Yu. Security Vehicle Solution of Vehicle Protocol Technology in Special Scenarios. In *2021 IEEE 5th Information Technology,Networking,Electronic and Automation Control Conference (ITNEC)*, volume 5, pages 1295–1299, October 2021. ISSN: 2693-3128.

[39] Yunyao Guo. Research on Security Analysis and Protection Measure of Internet of Vehicles Communication Protocol under Physical Layer Attack. In *2024 4th Asia-Pacific Conference on Communications Technology and Computer Science (ACCTCS)*, pages 375–380, February 2024.

[40] Timm Lauser and Christoph Krauß. Formal Security Analysis of Vehicle Diagnostic Protocols. In *Proceedings of the 18th International Conference on Availability, Reliability and Security*, ARES '23, pages 1–11, New York, NY, USA, August 2023. Association for Computing Machinery.

[41] Timm Lauser, Daniel Zelle, Dustin Kern, Christoph Krauß, and Lars Völker. Security Protocols for Ethernet-Based In-Vehicle Communication. In *2024 IEEE Vehicular Networking Conference (VNC)*, pages 148–155, May 2024. ISSN: 2157-9865.

[42] Yuan Lei, Lining Zeng, Yan-Xing Li, Mei-Xia Wang, and Haisheng Qin. A Lightweight Authentication Protocol for UAV Networks Based on Security and Computational Resource Optimization. *IEEE Access*, 9:53769–53785, 2021. Conference Name: IEEE Access.

[43] Hua Yi Lin, Meng-Yen Hsieh, and Kuan-Ching Li. A Multi-level Security Key Management Protocol Based on Dynamic M-tree Structures for Internet of Vehicles. In *2021 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*, pages 1–5, July 2021.

[44] Teng Long and Yu Dong. Security Analysis and Improvement of Railway Vehicle-to-ground Authentication and Key Negotiation Protocol. In *2023 5th International Conference on Communications, Information System and Computer Engineering (CISCE)*, pages 272–275, April 2023. ISSN: 2833-2423.

[45] Monowar Hasan, Ashish Kashinath, Chienying Chen, and Sibin Mohan. SoK: Security in Real-Time Systems | ACM Computing Surveys.

[46] Jorge Peña Queralta, Qingqing Li, Eduardo Castelló Ferrer, and Tomi Westerlund. Secure Encoded Instruction Graphs for End-to-End Data Validation in Autonomous Robots. *IEEE Internet of Things Journal*, 9(18):18028–18040, September 2022. Conference Name: IEEE Internet of Things Journal.

[47] Haisong Xu, Heng Zhang, Jianwei Sun, Weiwei Xu, Wenshuo Wang, Hongran Li, and Jian Zhang. Experimental Analysis of MAVLink Protocol Vulnerability on UAVs Security Experiment Platform. In *2021 3rd International Conference on Industrial Artificial Intelligence (IAI)*, pages 1–6, November 2021.

[48] Sadeq Almeaibed, Saba Al-Rubaye, Antonios Tsourdos, and Nicolas P. Avdelidis. Digital Twin Analysis to Promote Safety and Security in Autonomous Vehicles. *IEEE Communications Standards Magazine*, 5(1):40–46, March 2021. Conference Name: IEEE Communications Standards Magazine.

[49] Anupam Chattopadhyay, Kwok-Yan Lam, and Yaswanth Tavva. Autonomous Vehicle: Security by Design. *IEEE Transactions on Intelligent Transportation Systems*, 22(11):7015–7029, November 2021. Conference Name: IEEE Transactions on Intelligent Transportation Systems.

[50] Li Teng, Ma Jianfeng, Feng Pengbin, Meng Yue, Ma Xindi, Zhang Jiawei, Chenyang Gao, and Lu Di. Lightweight Security Authentication Mechanism Towards UAV Networks. In *2019 International Conference on Networking and Network Applications (NaNA)*, pages 379–384, October 2019.

[51] Zadid Khan, Mashrur Chowdhury, Mhafuzul Islam, Chin-Ya Huang, and Mizanur Rahman. Long Short-Term Memory Neural Network-Based Attack Detection Model for In-Vehicle Network Security. *IEEE Sensors Letters*, 4(6):1–4, June 2020. Conference Name: IEEE Sensors Letters.

[52] Mainak Adhikari, Ambigavathi Munusamy, Abhishek Hazra, Varun G Menon, Vijay Anavangot, and Deepak Puthal. Security in Edge-Centric Intelligent Internet of Vehicles: Issues and Remedies. *IEEE Consumer Electronics Magazine*, 11(6):24–31, November 2022. Conference Name: IEEE Consumer Electronics Magazine.

[53] Mahmood A. Al-Shareeda, Mohammed Anbar, Murtadha A. Alazzawi, Selvakumar Manickam, and Ahmed Shakir Al-Hiti. LSWBVM: A Lightweight Security Without Using Batch Verification Method Scheme for a Vehicle Ad Hoc Network. *IEEE Access*, 8:170507–170518, 2020. Conference Name: IEEE Access.

[54] NIST. NIST 800-53: Security and Privacy Controls for Information Systems and Organizations. Technical Report NIST Special Publication (SP) 800-53 Rev. 5, National Institute of Standards and Technology, December 2020.

[55] Vitelio Brustolin, Israel Aono Nunes, and Juliana Zaniboni De Assunção. Análise estrutural das estratégias de segurança cibernética do Brasil e dos Estados Unidos. *Revista Brasileira de Estudos de Defesa*, 9(2), June 2023.

[56] Jim Ledin. *Architecting High-Performance Embedded Systems: Design and build high-performance real-time digital systems based on FPGAs and custom circuits*. Packt Publishing, Birmingham Mumbai, February 2021.

[57] Peter Marwedel. *Embedded System Design: Embedded Systems Foundations of Cyber-Physical Systems, and the Internet of Things*. Springer, Cham, 4th ed. 2021 edition edition, January 2021.

[58] Donald G. Bailey. *Design for Embedded Image Processing on FPGAs*. Wiley, Hoboken, NJ, 2nd edition edition, August 2023.

[59] Hans Baars, Kees Hintzbergen, Jule Hintzbergen, and André Smulders. *Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002*. BRASPORT, 1st edition edition, January 2018.

[60] International Organization for Standardization. ISO/SAE 21434:2021, First edition: Road vehicles — Cybersecurity engineering, 2021.