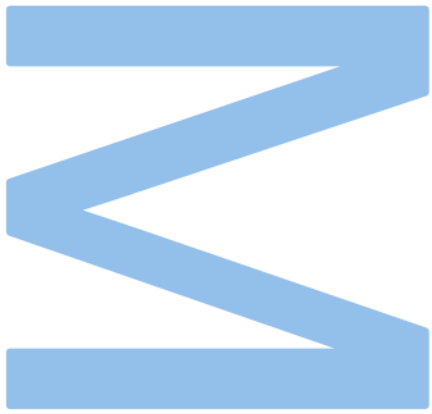
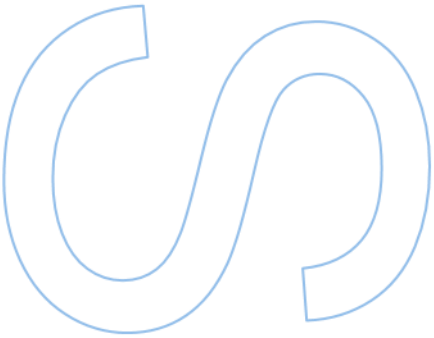
Trustworthy and Robust Intra-Vehicle Communication



Patrícia Adelaide Lopes Machado
Mestrado em Segurança Informática
Departamento de Ciência de Computadores
2022

Orientador
Prof. Dr. Bernardo Portela, Faculdade de Ciências

Coorientador
Prof. Dr. Rolando Martins, Faculdade de Ciências




U.PORTO
FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

Declaração de Honra

Eu, Patrícia Adelaide Lopes Machado, inscrita no Mestrado em Segurança Informática da Faculdade de Ciências da Universidade do Porto declaro, nos termos do disposto na alínea a) do artigo 14.º do Código Ético de Conduta Académica da U.Porto, que o conteúdo da presente dissertação reflete as perspetivas, o trabalho de investigação e as minhas interpretações no momento da sua entrega.

Ao entregar esta dissertação, declaro, ainda, que a mesma é resultado do meu próprio trabalho de investigação e contém contributos que não foram utilizados previamente noutros trabalhos apresentados a esta ou outra instituição.

Mais declaro que todas as referências a outros autores respeitam escrupulosamente as regras da atribuição, encontrando-se devidamente citadas no corpo do texto e identificadas na secção de referências bibliográficas. Não são divulgados na presente dissertação quaisquer conteúdos cuja reprodução esteja vedada por direitos de autor.

Tenho consciência de que a prática de plágio e auto-plágio constitui um ilícito académico.

Patrícia Adelaide Lopes Machado

Mirandela, 30 de Novembro de 2022

Abstract

Intra-vehicular communication is a very broad field which has been recently getting more attention from researchers. The technological evolution present in a modern vehicle was exponentially accelerated, without any sort of cryptographic auditing process to go with it. As a result, we now observe a very urgent need to properly identify and secure the car systems's sensitive information.

More technology dependent vehicles without proper security mechanisms will inevitably make said vehicles highly susceptible to attacks. More often than not in many of these attacks adversaries are capable of controlling vehicle functionality, blocking physical access to the vehicle, inject messages to the network or infect the vehicle with malware. Cryptographic mechanisms are presented as the solution to these problems currently being faced by the automotive industry, but they were not designed to respond to such challenges.

The main communication channels used by the automotive industry, Control Area Network (CAN), Local Interconnect Network (LIN), Ethernet, Media Oriented Systems Transport (MOST) and FlexRay, naturally have limitations and requirements such as bandwidth capacity, data rate, speed, performance and cost. Such requirements end up restricting the usage of some cryptographic mechanism, which turns the securing process more difficult.

Every one of the aforementioned topics, leads to the existence of a substantially large effort in searching for solutions. From the choice of using safe hardware, to propositions for different typologies, to even different communication channels.

Keywords: Intra-vehicle communication, Cryptography, Topology, Safe Hardware.

Resumo

Comunicação intra veículo é um tema muito abrangente que tem vindo a ser estudado cada vez mais. A evolução tecnológica presente num veículo não foi acompanhada por mecanismos criptográficos de forma a proteger o sistema em questão. Neste sentido observamos uma urgente necessidade de identificar e proteger a informação sensível do sistema.

Veículos cada vez mais dependentes da tecnologia sem uma camada de segurança, acaba por deixar os mesmos suscetíveis a ataques, onde muitas vezes conseguem controlar funcionalidade do veículo, impedir o acesso físico ao mesmo, injetar mensagens na rede ou infetar o veículo com malware. Mecanismos criptográficos são a solução apresentada para os problemas da indústria automotive, mas, estes não desenhados para responder a tais desafios.

Os canais de comunicação utilizados na industria automotive, Control Area Network (CAN), Local Interconnect Network (LIN), Ethernet, Media Oriented Systems Transport (MOST) e FlexRay, possuem limitações e requisitos como capacidade de banda, data rate, velocidade, performance e custo. Estes requisitos ou limitações podem restringem a utilização de alguns mecanismos criptográficos, o que acaba por dificultar o processo.

Todos os pontos apresentados anteriormente, levam a que exista um esforço de procura de soluções. Desde utilização de hardware seguro, a propostas de diferentes topologias, ou propostas de utilização de canais de comunicação diferentes.

Palavras-chave: Comunicação intra veículo, Criptografia, Topologia, Hardware seguro.

Agradecimentos

Gostaria de começar por agradecer ao meu orientador, Professor Bernardo Portela, e coorientador, Professor Rolando Martins, pela orientação e partilha de conhecimentos durante este percurso.

Gostaria também de agradecer à Continental por me permitirem trabalhar numa empresa tão conceituada. Um agradecimento especial ao Luís Silva, por me acompanhar e pela partilha de conhecimento deste mundo automotive.

Queria ainda agradecer à minha família, em especial à minha irmã, que mesmo longe estava sempre perto.

Para finalizar, gostaria de agradecer ao meu melhor amigo, João Pedro, por me apoiar e ter ajudado a que isto fosse possível.

Dedico a mim.

Conteúdo

Abstract i

Resumo iii

Agradecimentos v

Conteúdo ix

Lista de Tabelas xi

Lista de Figuras xiv

Acrónimos xv

1 Introdução 1

1.1 Motivação 1

1.2 Objetivos 2

1.3 Organização 2

2 Preliminares 5

2.1 Criptografia 5

2.1.1 Confidencialidade 6

2.1.2 Integridade 6

2.1.3 Autenticidade 7

2.2 Hardware Confiável 7

2.3 Eletronic Control Unit (ECU) . . . 8
2.4 Ataques . . . 9
2.5 Pontos críticos . . . 11
2.5.1 Sistema infotainment . . . 11
2.5.2 Porta On-Board Diagnostic (OBD) . . . 11
2.5.3 Bluetooth . . . 12
2.5.4 Sistema Global Positioning System (GPS) . . . 13
2.6 Comunicações . . . 13
2.6.1 Domínios . . . 13
2.6.2 Control Area Network (CAN) . . . 15
2.6.3 Local Interconnect Network (LIN) . . . 16
2.6.4 Automotive Ethernet . . . 17
2.6.5 Media Oriented Systems Transport (MOST) . . . 18
2.6.6 FlexRay . . . 18
2.7 Topologias de Rede . . . 19
2.8 Conectividade . . . 20

3 Segurança Intra Veículo **23**
3.1 Modelo de Sistema . . . 23
3.2 Pontos de Entrada . . . 25
3.2.1 Sistema infotainment . . . 25
3.2.2 Porta OBD . . . 26
3.2.3 Bluetooth . . . 26
3.2.4 Sistema GPS . . . 27
3.3 Requisitos de Segurança . . . 27
3.4 Adversário no Sistema . . . 29

4 Abordagem **33**
4.1 Mecanismos de segurança vs limitações de comunicação . . . 33

4.2 Canais de comunicação alternativos 34
4.3 Topologias alternativas 40
4.4 Hardware Confiável 42
4.5 Conclusão 43

5 Conclusões e Trabalho Futuro **45**

5.1 Conclusões 45
5.2 Trabalho Futuro 46

Bibliografia **47**

Lista de Tabelas

2.1 Classificação canais de comunicação 19

4.1 Local Interconnect Network (LIN) *vs* Control Area Network (CAN) [22] 36

4.2 FlexRay *vs* CAN 37

4.3 Media Oriented Systems Transport (MOST) *vs* CAN 38

4.4 Automotive Ethernet *vs* CAN 39

Lista de Figuras

2.1 Componentes de hardware das Eletronic Control Unit (ECU)s [38] 8

2.2 Vetores de ataque mais comuns 2010-2021 [4] 9

2.3 Classificação de ataques 10

2.4 Domínios de um veículo [48] 14

2.5 Classes canais de comunicação [38] 15

2.6 Control Area Network (CAN) frame [38] 16

2.7 Frame master e slave do Local Interconnect Network (LIN) [38] 17

2.8 Ethernet frame [38] 17

2.9 Media Oriented Systems Transport (MOST) frame [38] 18

2.10 FlexRay frame [38] 18

2.11 Topologias de Rede [25] 20

2.12 Tipos de conectividade [1] 21

3.1 Topologia do sistema 23

3.2 Flow conta quilómetros 27

3.3 Flow flag travões 28

3.4 Flow Global Positioning System (GPS) 28

3.5 Modelo adversarial 29

4.1 Sistema conectado por LIN 35

4.2 Sistema conectado por FlexRay 36

4.3 Sistema conectado por MOST 38

4.4 Sistema conectado por Automotive Ethernet 39
4.5 Topologia alternativa star 40
4.6 Topologia alternativa ring 41
4.7 Solução proposta em [39] 43
4.8 Proposta de solução 44

Acrónimos

ADAS Advanced Driver Assistance System

AES Advanced Encryption Standard

BCM Brake Control Module

CAN Control Area Network

CAN FD Control Area Network Flexible Data-rate

CD Compact Disc

CRC Cyclic Redundancy Check

CVE Common Vulnerabilities and Exposures

DMS Driver Monitoring System

DoS Denial of Service

ECM Engine Control Module

ECU Eletronic Control Unit

FPGA Field-Programmable Gate Array

GPS Global Positioning System

HMAC Hash-based Message Authentication Code

HSM Hardware Security Module

IPSec Internet Protocol Security

LFSR Linear Feedback Shift Register

LIN Local Interconnect Network

MAC Message Authentication Code

MAP Manifold Absolute Pressure

MCU Microcontroller Unit

MITM Man In The Middle

MOST Media Oriented Systems Transport

MPU Microprocessor Unit

OBD On-Board Diagnostic

PIN Personal Identification Number

PoC Proof of Concept

PRF Pseudorandom Function

RPM Revolutions Per Minute

RSA Rivest-Shamir-Adleman

SHE Secure Hardware Extension

SSH Secure Shell

TCU Telematic Control Module

TCM Transmission Control Module

TLS Transport Layer Security

TPM Trusted Platform Module

TPS Throttle Position Sensor

USB Universal Serial Bus

V2C Vehicle to Cloud

V2I Vehicle to Infrastructure

V2P Vehicle to Pedestrian

V2V Vehicle to Vehicle

V2X Vehicle to Everything

Capítulo 1

Introdução

1.1 Motivação

A indústria automóvel tem vindo a sofrer alterações relativamente à forma e ao tipo de veículos que produzem. Veículos que inicialmente se moviam a vapor, podem muito brevemente passar a conduzir-se sozinhos, isto, em prol de uma experiência de condução mais confortável ao condutor e passageiros. Passamos a ter autênticos "computadores sobre rodas"com mais de 200 milhões de linhas de código [50], tornando-se num dos sistemas mais complexos usados no dia-a-dia.

Esta evolução permite ao condutor uma maior comodidade de condução e, controlo sobre os vários parâmetros do seu veículo [43]. Passa assim, a ser possível a conexão do veículo à Internet, permitindo aos seus passageiros o acesso à mesma. Com esta conexão, os veículos passaram a conseguir comunicar com outros veículos, e, com várias estruturas que permitem o acesso em tempo real do que se passa nas estradas, o que permite a adaptação da condução ou a rota a tomar. Os fabricantes dos veículos, fornecem apps, que permitem a monitorização e realização de ações sobre o mesmo, de forma remota. Ações estas como, abrir/fechar o veículo, ligar/desligar o motor do veículo, controlar o ar condicionado, ligar/desligar luzes e ainda apitar. Através da app, também é possível localizar o veículo, através das coordenadas Global Positioning System (GPS).

Com todas estas novas comodidades dentro de um veículo, leva a que novos e mais componentes sejam acrescentados ao mesmo. Fomos observando o aumento exponencial do número de sistemas eletrónicos, o que leva a que em 2005, um veículo possuí cerca de 40 Eletronic Control Unit (ECU)s [32], nos dias de hoje já podem conter mais de 200 ECUs [50]. Graças à performance e confiança destes novos componentes eletrónicos, passou a ser possível a implementação de várias funções complexas, que garantem o conforto e segurança num veículo. Tudo isto leva a que um veículo seja um sistema bastante complexo, o que se reflete bastante na comunicação intra veículo.

Consequentemente, a evolução presente nos veículos dos dias de hoje, leva a que indivíduos com intenções maliciosas tenham uma maior superfície de ataque. O aumento da integração de componentes eletrónicos significa um aumento de pontos de contacto com o exterior e com

ameaças. Inicialmente, era necessário ter acesso físico ao veículo para realizar um ataque, hoje em dia, com toda a conectividade num veículo, é possível atacá-lo remotamente, o que, consequentemente aumentou o número de ataques [3].

Desta forma, passou a ser urgente estudar e investigar temas deste domínio, uma vez que houve uma grande evolução tecnológica, sobre a qual ainda existe muito para investigar. Tudo, com o objetivo de tornar estes "computadores sobre rodas"mais seguros contra possíveis ataques de segurança.

1.2 Objetivos

O trabalho em questão foca-se na comunicação intra veículo de uma zona especifica do veículo, onde os objetivos são os seguintes:

1. Recolha e analise dos ataques realizados sobre os vetores de ataque de um veículo composto por várias ECUs;
2. Levantamento de requisitos para definição de segurança;
3. Caracterização de um modelo adversarial intra veículo, considerando os canais de comunicação entre os componentes lógicos;
4. Desenho e avaliação de canais de comunicação e topologias que facilitem a utilização de mecanismos criptográficos;
5. Análise de segurança das abordagens propostas sobre os requisitos levantados.

1.3 Organização

Este documento encontra-se organizado da seguinte forma:

- No capítulo 2, apresentamos vários conceitos que se relacionam e ajudar a uma melhor compreensão do tema abordado neste documento. Definições e mecanismos criptográficas, hardware confiável, ECUs, ataques ao sistema, alguns exemplos de canais de comunicação utilizados na industria automotive e, por fim, conectividade de um veículo.
- Capítulo 3 apresenta o modelo de sistema, os pontos de entrada do sistema, requisitos de segurança, identificação do adversário no sistema e no final, apresentação do problema em mãos.
- No capítulo 4, apresentamos a nossa abordagem ao problema, começando por apresentar as limitações para a utilização de mecanismos de segurança e canais de comunicação. Analisamos alternativas de canais de comunicação, topologias de sistema e componentes de hardware seguro no sistema apresentado. Terminando com uma proposta de um sistema.

- Capítulo 5, último capítulo do documento, são descritas as conclusões a que chegamos após o desenvolvimento deste projeto. Propomos também, algumas melhorias e pontos a acrescentar no futuro deste projeto.

Capítulo 2

Preliminares

Ao longo deste capítulo 2, são apresentados vários conceitos fulcrais ao tema. Apresentamos as garantias de segurança que pretendemos assegurar, relativamente à informação transmitida dentro de um veículo, assim como, explorar o tipo de atacantes que a industria automotive enfrenta. Apresentamos também alguns exemplos de ataques já conseguidos, como forma de representar a urgência de medidas de segurança na industria.

Também neste capítulo, são apresentados vários conceitos específicos ao tema, como Eletronic Control Unit (ECU)s, onde explicamos o que são, a sua arquitetura e alguns dos diferentes tipos. De seguida, abordamos os vários canais de comunicação utilizados na indústria.

2.1 Criptografia

Durante o desenvolvimento deste projeto, verificamos que seria necessário aplicar garantias de segurança sobre certas informações trocadas dentro de um veículo. Desta forma, podemos recorrer a dois grupos de opções, criptografia simétrica e criptografia assimétrica.

- **Criptografia simétrica**, sistemas criptográficos mais simples e mais leves, onde é necessária a pré-partilha de chaves. Permite a utilização de cifras e Message Authentication Code (MAC)s. Apresentamos alguns exemplos em seguida:
  - **Advanced Encryption Standard (AES):** Cifra por blocos, que consegue processar blocos de 128 bits e utiliza uma chave secreta de 128, 192 ou 256 bits. A chave por norma mais utilizada é de 128 bits, uma vez que torna o processo de cifrar ligeiramente mais rápido, e a diferença do nível de segurança entre esta e 256 bits não é relevante para grande parte das aplicações. Esta cifra olha para o plaintext como um array, sobre o qual aplica ações para obter o criptograma [16].
  - **Hash-based Message Authentication Code (HMAC):** Permite a criação de um MAC a partir de uma função de hash. Permite a geração de Pseudorandom Function (PRF), desde que o hash escolhido seja resistente a colisões, no entanto,

caso isso não se verifique, o HMAC ainda permitirá gerar uma PRF segura se a função de compressão do hash for uma PRF. Graças a estas propriedades, o HMAC foi extensivamente utilizado em protocolos de comunicação segura como: Internet Protocol Security (IPSec), Transport Layer Security (TLS) e Secure Shell (SSH) [16].

- **Criptografia assimétrica**, sistemas criptográficos mais pesados, mas sem necessidade de pré-partilha de chaves. Permite a utilização de cifras e assinaturas digitais. Apesar de não existir a necessidade de pré-partilha de chaves, a criptografia assimétrica necessita de mais poder de processamento, o que acaba por tornar, tanto o processo de cifrar como decifrar, mais lento. Apresentamos alguns exemplos em seguida:

  – **Rivest-Shamir-Adleman (RSA):** Utiliza um par de chaves, pública e privada. A chave pública é utilizada para cifrar mensagens, enquanto a chave privada é utilizada para decifrar mensagens. Toda a gente pode ter conhecer a chave pública, já a privada deve-se manter privada. Isto permite que toda a gente possa enviar mensagens, mas apenas o portador da chave privada consegue decifra-las [16].

2.1.1 Confidencialidade

Quando falamos em confidencialidade, estamos a dizer que vamos delimitar certos valores que queremos que para todas as zonas de incidência do adversário, ou seja, todos os pontos onde o adversário pode interagir, os valores vão estar protegidos de um forma ou de outra.

Para um grupo de valores, [**K T G**], onde **K** é o valor dos quilómetros do veículo, **T** é a flag dos travões e **G** são as coordenadas Global Positioning System (GPS), pretendemos que mesmo que um atacante consiga aceder à informação armazenada ou transmitida pelas ECUs, o mesmo não conseguirá distinguir [**K T G**], de outros valores aleatórios.

Com o protocolo de segurança AES, conseguimos garantir a confidencialidade da informação transmitida entre os sistemas do veículo.

2.1.2 Integridade

Com integridade, pretendemos garantir que a informação não é alterada pelo adversário, mas, no caso de existirem alterações não autorizadas, sejamos capazes de as identificar.

Uma entidade define um valor, **T**, transmitido pelo sistema, queremos ser capazes de detetar quando esse **T** é recebido como **T'**, sendo que **T != T'**.

Com o protocolo de segurança HMAC, conseguimos garantir a integridade da informação transmitida entre os sistemas do veículo.

2.1.3 Autenticidade

Com autenticidade pretendemos determinar que um mensagem foi produzida ou enviada por uma entidade específica, ou seja, mesmo que um adversário tente replicar um valor, a entidade recetora vai conseguir identificar que o valor recebido não foi produzido nem enviado por entidade confiável.

A entidade **AC** cria e envia o valor **G** para a entidade **AD**, queremos ser capazes de garantir que o valor **G** foi de facto produzida e enviada pela entidade **AC**.

Com o protocolo de segurança HMAC, conseguimos garantir a autenticidade da informação transmitida entre os sistemas do veículo.

2.2 Hardware Confiável

O principal objetivo da aplicação de mecanismos criptográficos é a aplicação de garantias de segurança sobre a informação transmitida na rede. De tal forma, a segurança do sistema, deve começar nos componentes de hardware, ECUs, onde deve ser garantido um boot seguro.

Existem vários módulos de segurança, que atingiram a maturidade suficiente para começarem a ser considerados standards na industria automotive [45]. Apresentamos de seguida alguns desses módulos:

- **Secure Hardware Extension (SHE):** standard aberto e gratuito que descreve a extensão de hardware para funções essenciais de segurança como, modulo de hardware para cifrar, boot seguro, gestão de chaves, entre outras. SHE [45], é implementado como uma extensão on-chip do micro-controlador.
- **Hardware Security Module (HSM):** foram desenvolvido três HSM [26], full, medium e light, para diferentes usos na industria automotive. Estes HSMs são utilizados como uma extensão de Microcontroller Unit (MCU)s e Microprocessor Unit (MPU)s, utilizados na industria como mecanismos de segurança das redes intra veículo.
- **Trusted Platform Module (TPM):** suporta chaves secretas para autenticação e cifrar. O TPM [45] lida com várias operações criptográficas, como geração de chaves simétrica/assimétricas, cifrar/decifrar cifras simétricas/assimétricas, hash e geração de números aleatórios. Este componente é tipicamente um micro-controlador que armazena de forma segura, passwords, chaves digitais e certificados. Pode ser implementado externamente com um bus para comunicação com MCU/MPU, ou como um componente embutido num outro circuito integrado, e.g. controlador ethernet.
- **Arm TrustZone:** sistema proprietário que apoia o desenvolvimento de sistemas embutidos seguros. Este permite o isolamento entre o o mundo real, sistema operativo e camadas

aplicacionais, e o mundo seguro, onde podem ser realizadas operações sensíveis como operações criptográficas, gestão de chaves e verificações de integridade [45].

2.3 ECU

Uma ECU é um computador embutido, que controla os sistemas mecânicos ou eletrónicos de um veículo. Atualmente, um veículo pode conter mais de 200 ECUs [50], sendo estas responsáveis por controlar as várias funcionalidade do veículo, sendo funcionalidades essenciais, ao conforto, segurança e acesso ao interior do mesmo. As várias ECUs encontram-se conectadas por buses de diferentes tipo, e.g., Control Area Network (CAN), Ethernet, Local Interconnect Network (LIN).

No interior de cada ECU existe um chip dedicado, como ilustrado na figura 2.1, com o seu próprio software e firmware, que requer a ligação a uma fonte de alimentação e partilha de dados para funcionar. Cada uma das ECUs presentes num veículo recebem diferentes input, consoante a função pela qual são responsáveis, de sensores ou botões que interagem com os passageiros. Consequentemente, essas mesmas ECUs comunicação com outros componentes do veículo, o tipo de ação a tomar, consoante o input recebido, e.g. A ECU responsável por trancar o veículo, ao receber como input **`"trancar veículo"`**, vai comunicar com o sistema de fecho de forma a trancar o mesmo [40].

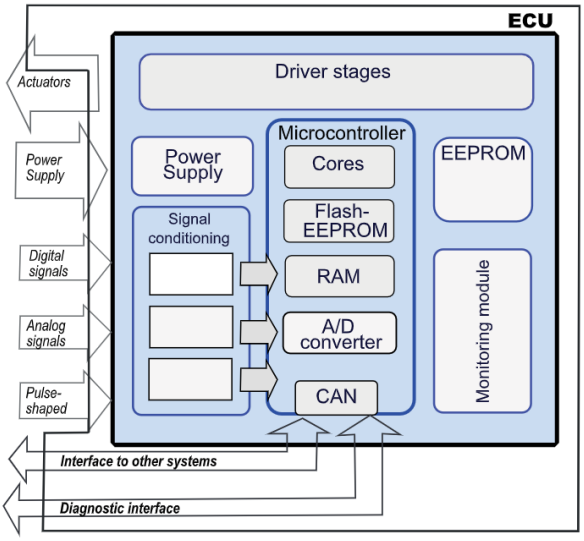


Figura 2.1: Componentes de hardware das ECUs [38]

Como referido em cima, cada ECU é responsável por controlar as várias funções do veículo, existindo assim vários tipos de ECUs. Vamos enumerar alguns tipos [46].

- **Engine Control Module (ECM):** Controla as várias funções do motor, como injeção de combustível, tempo de ignição;

- **Brake Control Module (BCM):** Responsável pelo sistema de travagem;
- **Transmission Control Module (TCM):** Responsável por todo o sistema de transmissão do veículo;
- **Telematic Control Module (TCU):** Disponibiliza GPS, acesso à internet e conectividade entre o veículo e dispositivos móveis.

Mais para a frente neste documento, secção 3.1, apresentamos as ECUs fundamentais para este trabalho, a sua função e os dados produzidos e recebidos.

2.4 Ataques

Com base na literatura analisada [3], [31], [24], [8], em especial o relatório da Upstream 2022 [4], foi possível identificar os pontos de entrada mais utilizados pelos atacantes. Na figura 2.2, temos os vetores de ataque mais comuns entre 2010 e 2021, segundo o relatório da Upstream.

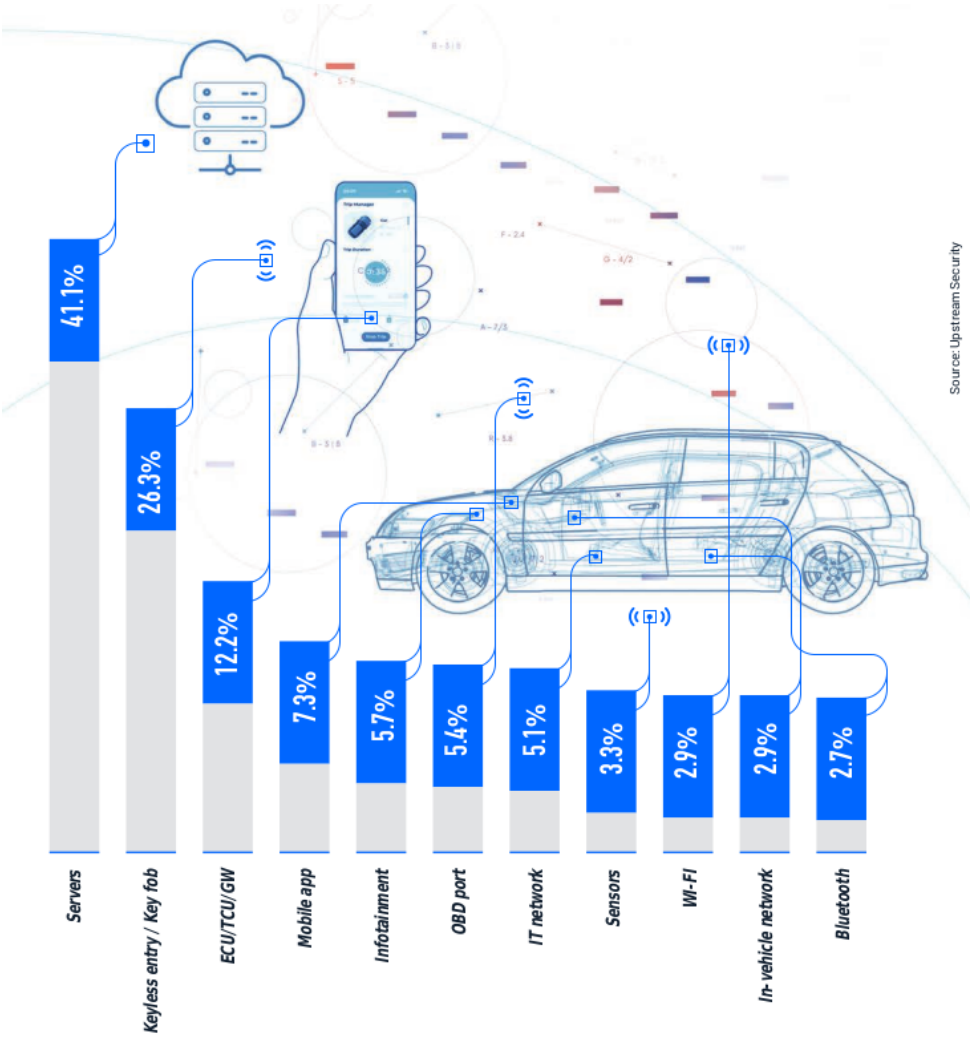


Figura 2.2: Vetores de ataque mais comuns 2010-2021 [4]

Considerando o que pretendemos estudar neste projeto e os vetores de ataque identificados na figura 2.2, apresentados alguns ataques, de forma a ilustrar alguns dos cenários que alguns atacantes conseguem criar.

Realizamos a classificação dos ataques com base nos vetores de ataque mais comuns apresentados na figura 2.2. Esta classificação encontra-se ilustrada na figura 2.3.

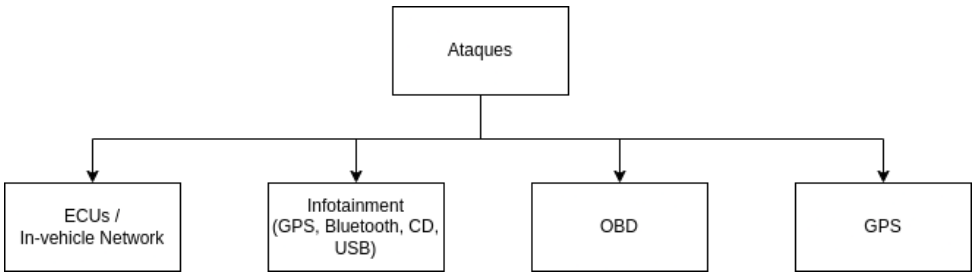


Figura 2.3: Classificação de ataques

1. **ECUs:** Ataques às ECUs do sistema, tendem a começar com a manipulação de features das mesmas, e.g. feature de time-out, impede que um transceiver de CAN mantenha um estado dominante por um longo periodo de tempo [4]. Esta manipulação é feita com o objetivo de manipular as funcionalidades da ECU.

   Em seguida apresentamos alguns exemplos reais.

   - Em Abril de 2020, hackers conseguiram fazer reverse engineer à TCU, responsável pela geolocalização e comunicações móveis, tendo descoberto que podiam utilizar a conexão do sistema telematics para se infiltrarem na rede corporativa e ganhar acessos através das credenciais de admin [13].
   - Hackers conseguiram aceder à rede interna do veículo e estão a manipular o valor do conta quilómetros. Um veículo com o menor número de quilómetros torna-se mais valioso. Esta fraude está a custar às vítimas em média 4,000 dólares cada [12].

2. **Infotainment:** Sistema infotainment faz a conexão entre as ECUs interiores do veículo com o mundo exterior [4]. Isto faz com que um ataque a este sistema tenda a começar nas portas, maioritariamente físicas, com o objetivo de aceder ao sistema interno do veículo.

   De seguida, apresentamos alguns exemplos de ataques reais.

   - Em Maio de 2021, investigadores publicaram a descoberta de várias vulnerabilidades num sistema infotainment, que podiam ser exploradas de forma a hackear o sistema interno do veículo [15].
   - Durante o *Geneva International Motor Show*, muitos veículos sofreram um ataque de GPS spoofing, o que fez com que estes mostrassem a sua localização como estando em Inglaterra e no ano de 2036 [9].
   - Investigadores conseguiram hackear a unidade infotainment de um Nissan Xterra através da exploração de vulnerabilidades da unidade. Conectando-se por Universal Serial Bus (USB) ao veículo, conseguiram ter acesso root à shell do sistema [10].

- Vários veículos da Tesla foram alvos de bluejacking, onde um dispositivo bluetooth faz hijacking a outro dispositivo e enviar anúncios spam ou outro tipo de mensagens não solicitadas [6].
- Foi descoberta uma vulnerabilidade nas configurações do Android Auto, token de referência inseguro, que permitia o bypass nas permissões. Esta vulnerabilidade podia ser acionada localmente sem a necessidade de interação do utilizador [14].

3. **On-Board Diagnostic (OBD):** A porta OBD permite a leitura de informações de diagnóstico das ECUs, dando-lhe acesso a todos os componentes do sistema. Um atacante começa pelo ataque físico à porta, com o objetivo de aceder, ler e manipular as informações das ECUs.

   Em seguida, apresentamos alguns exemplos reais.

   - Investigadores conseguiram fazer reverse enginner à memória, interface gráfica e firmware de um leitor OBD, tornando o numa ferramenta de ataque personalizada. A ferramenta permitia o carregamento de payload, sendo possível de correr no veículo [5].
   - Em Maio de 2020 investigadores usaram hardware e software open-source para construir um dispositivo OBD para interpretar e enviar mensagens CAN. O dispositivo consegui transmitir as coordenadas GPS, velocidade em tempo real, o que permitia a monitorização remota do veículo [7].

2.5 Pontos críticos

Tendo em consideração os ataques analisados na secção anterior, vamos apresentar alguns pontos críticos identificados no nosso sistema.

2.5.1 Sistema infotainment

O termo infotainment consiste na junção das palavras *information* e *entertainment*, que a industria criou de forma a representar o ponto de incidência do sistema [42]. O sistema é responsável pela apresentação centralizada de informação útil ao condutor, GPS, luzes, e entretenimento, rádio, acesso à internet, entre outros. Apresentado na forma de um ecrã interativo, normalmente localizado no centro do painel do veículo.

Permite a instalação de software e aplicações externas e ainda a integração de dispositivos móveis através da conexão bluetooth ou USB.

2.5.2 Porta OBD

Sistema de diagnóstico, build-in no veículo, que tem como principal objetivo auxiliar na deteção de problemas do mesmo. Pode também ser utilizado para atualizar software ou alterar a memória

de uma ECU. OBD surgiu em 1991, resultado da obrigatoriedade de monitorização dos níveis de gases emitidos pelo veículo [29]. O sistema OBD encontra-se conectado a uma porta, que permite ligar um scanner, onde é possível a leitura de dados do veículo. Existem duas versões deste sistema de diagnóstico:

- OBD I

  Instalado em veículos entre 1991 e 1996, onde consegui fazer localização de problemas básicos no motor e registos simples. O principal objetivo desta primeira versão, seria ajudar fabricantes de veículos, a obter informações e conhecimento de como produzir veículos melhores. Devido às limitações desta versão, foi necessário desenvolver uma nova [29].

- OBD II

  Instalado em veículos a partir de 1996, esta nova versão, não é apenas mais atualizada que a anterior, possuí também mais poder de processamento. Com esta atualização, este sistema passou a ser mais útil para os mecânicos, já que passamos a ter diagnósticos em tempo real de todos os sistemas do veículo. Mas não foram só os mecânicos que passaram a usufruir deste sistema, também os proprietários dos veículos, passaram a conseguir realizar diagnósticos [21].

Também as portas OBD de ambas as versões são distintas, o mesmo se aplica aos scanners. Enquanto que um scanner OBD I apenas recebe mensagens com códigos sem qualquer informação detalhada, o mesmo já não e verifica nos scanners OBD II. Passamos a ter diagnósticos mais precisos, informações detalhadas e ainda, em alguns casos, a possibilidade de uma visão geral dos reparos e estimativa de custos.

Já se anda a pensar numa nova versão, OBD III, sendo possível obter o diagnóstico do veículo por Wi-Fi. Acreditam que esta nova versão vai ajudar a diminuir custos e inconvenientes, mas ao mesmo tempo é bastante desafiador devido a questões de privacidade [21].

2.5.3 Bluetooth

Das funcionalidade mais populares, já que permite a conectividade do telemóvel ao carro. Isto permite que no nosso veículo exista uma extensão do nosso telemóvel, o que nos permite realizar algumas funções básicas de forma mais cómoda, como ouvir música, falar com alguém ao telemóvel, entre outras [53].

O problema surge quando esta funcionalidade tão cómoda começa a ser utilizada por atacantes para aceder ao sistema interno do nosso veículo. Se um atacante conseguir comprometer o telemóvel do dono do veículo, através de um site malicioso ou capturar o endereço MAC do telemóvel, pode conseguir entrar no sistema.

2.5.4 Sistema GPS

GPS consiste num sistema de tracking, que permite identificar onde nos localizamos, para onde vamos, a que velocidade e a distância até ao destino. Tudo isto é possível graças à comunicação entre os satélites existentes em órbita e o tracker presente nos nossos veículos [47].

O sistema de navegação embutido no veículo, utiliza as informações recolhidas pelo tracking do GPS para fornecer dados de possíveis rotas e orientar o veículo do ponto de origem até ao ponto de destino pretendido.

2.6 Comunicações

Canais de comunicação permitem a comunicação entre as várias ECU de um veículos e os restantes sensores. Um dos problemas iniciais relativamente à incorporação de ECUs foi o aumento significativo do peso dos veículos devido ao número de cabos que conectavam todos os componentes do mesmo.

Até ao início dos anos 90, os dados eram trocados por meio de links ponto a ponto entre ECUs. Para isso, havia a necessidade de possuí uma quantidade de canais de comunicação na ordem de n^2, onde n corresponde ao número de ECU do sistema. Esta abordagem acabou por ser descontinuada devido ao aumento do número de ECUs, que proporcionalmente levava a um aumento no número de fios, levando depois a problemas de peso, custo e complexidade [43]. O confronto com estes problemas, levou à necessidade de usar redes onde as comunicações são multiplexadas em meio partilhado. Consequentemente foi necessária a utilização de protocolos de comunicação de forma a gerir as comunicações.

Numa fase inicial da evolução eletrónica nos veículos, uma nova funcionalidade era implementada numa stand alone ECU, funciona de forma independente do computador do motor e consegue controlar vários parâmetros do veículo, conectada a sensores e atuadores. Rapidamente foi possível perceber a necessidade da distribuição de funcionalidades por várias ECU e a necessidade de partilha de dados entre os vários sub-sistemas [43].

2.6.1 Domínios

Cada funcionalidade integrada num veículo possuí diferentes necessidades e requisitos para os sistemas de comunicação utilizados. Falamos de necessidades de segurança, requisitos de performance, qualidade do serviço, tempo de resposta, tamanho de banda, tolerância a erros de transmissão, entre outros. Tipicamente, os sistemas embutidos num veículo encontram-se divididos em vários domínios, que correspondem a diferentes características e restrições.

Na figura 2.4, temos uma representação dos domínios, tendo mais a baixo mais alguns detalhes sobre cada domínio.

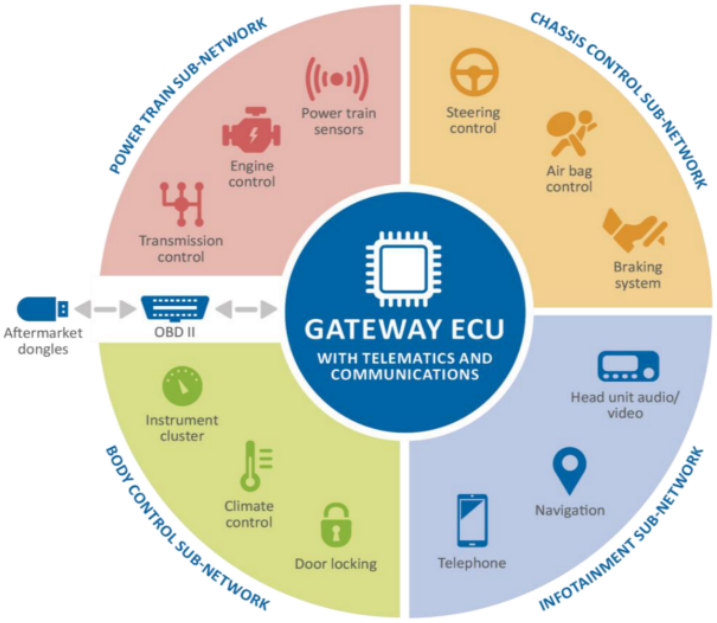


Figura 2.4: Domínios de um veículo [48]

- **Powertrain:** Este domínio, consiste na combinação de vários componentes do veículo, motor, transmissão, veios, rodas, entre outros, que geram energia para que o veículo funcione. Este domínio, pode também incluir sensores e atuadores, de forma a tornar a condução mais confortável, reduzir a emissão de gases, aumentar a eficiência do combustível e reforçar a segurança do veículo [28].
- **Chassis:** Composto por toda a estrutura que suporta o powertrain e todos os outros componentes, à exceção do motor. Também aqui, podem estar integrados sensores e atuadores.
- **Infotainment:** Este domínio possibilita a interação entre o condutor e o veículo. Apresenta informações que recebe a partir dos vários sensores ou ECUs, tudo com o propósito de entretenimento. Este domínio, também permite que dispositivos móveis sejam conectados através de Bluetooth, WiFi ou redes móveis. Através deste domínio, é possível comunicar com todos os outros domínios.
- **Body:** Incluí componentes ajustáveis de conforto como controlo de temperatura, ajuste dos bancos, manuseamento das janelas, luzes, entre outros. Integram também alguns sensores.
- **Telematics & Communications:** Incluí o sistema de monitorização do veículo, sistema de localização de dispositivos e comunicações wireless.

Para os canais de comunicação existentes, foram criadas classes. Cada classe representa a funcionalidade para que são utilizados, assim como as necessidade de comunicação da mesma. A

divisão por classes permite que seja mais fácil identificar o canal de comunicação necessário considerando o sistema e as suas necessidade comunicativas. Na figura 2.5 encontra-se representadas as quatro classes.

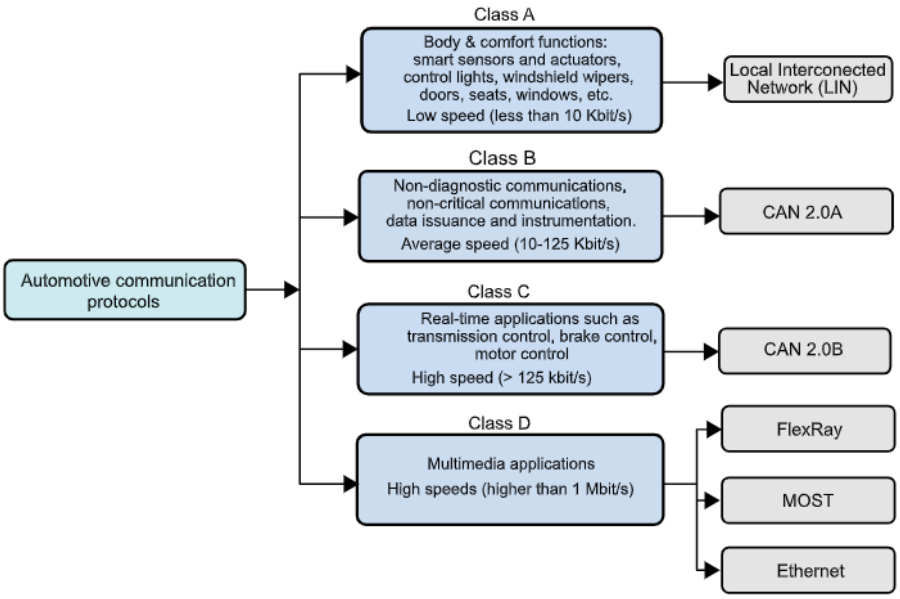


Figura 2.5: Classes canais de comunicação [38]

Nas próximas subsecções são apresentados alguns exemplos de canais de comunicação utilizados na industria automotive. Existem mais para além dos apresentados neste projeto, mas, foram apenas considerados os mais utilizados em sistemas reais da industria. O CAN é o canal utilizado no sistema apresentado no capítulo 3.

2.6.2 CAN

CAN, desenvolvida pela Bosch estando disponível desde 1983, tornou-se na rede mais usada para sistemas automotive. Desenhada para suportar comunicação multiplexing entre as várias ECUs do sistema, conseguindo assim diminuir o comprimento dos fios e a sua quantidade [43]. Numa rede CAN, pequenas mensagens são enviadas em modo broadcast, onde todos os nodes recebem o que foi transmitido. CAN não permite o envio de grandes blocos de informação ponto-a-ponto, ao contrário das redes tradicionais.

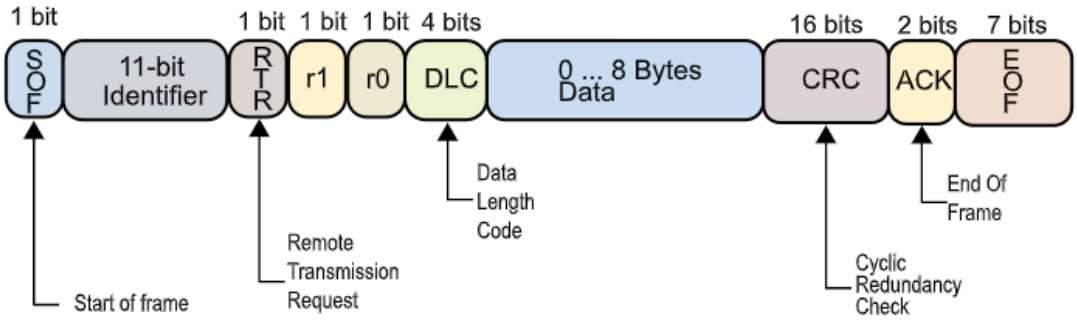


Figura 2.6: CAN frame [38]

Com CAN, a informação é transmitida em frames com o máximo de 8 bytes de informação e um número de bits de controlo. Um frame contém um identificador, que será determinante para a prioridade do mesmo, e, dependendo do formato, standard CAN 2.0A ou extended CAN 2.0B, identificador de 11 bits ou 29 bits, correspondentemente. Na figura 2.6 temos uma representação de um frame standard CAN com um identificador de 11 bits.

2.6.3 LIN

LIN, desenvolvida em 1998 por um grupo de fabricantes de automóveis. Serial bus lento e barato usado em sistemas eletrónicos pertencentes ao domínio body, permitindo uma comunicação eficaz entre sensores e atuadores, onde a largura da banda, velocidade e versatilidade não sejam importantes [52]. Possuí apenas um fio, ao contrário do CAN que possuí dois. É muitas vezes usado como sub bus para CAN e Flexray.

A rede LIN é baseada na arquitetura master-slave, onde existe apenas um master node e vários slave nodes. A comunicação em LIN é sempre iniciada por uma ação do master node, e segue os seguintes passos:

1. Comunicação é iniciada pelo master node;
2. Este envia o header da mensagem e o identificador da mesma;
3. Um slave node recebe e filtra o identificador, o que inicia a transmissão da resposta, com até 8 bytes de informação;
4. A resposta, pode ser envia por um slave ou master node.

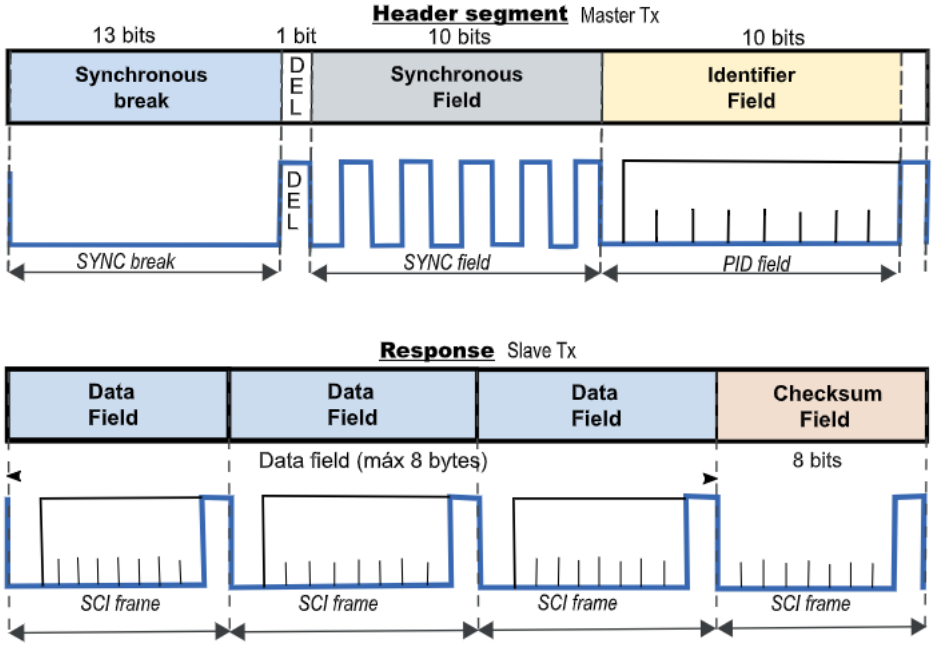


Figura 2.7: Frame master e slave do LIN [38]

Cada LIN frame é composto por um frame header e um frame response, como ilustrado na figura 2.8. É o master node que decide quando e qual dos frames deve ser transmitido de acordo com a tabela onde consta a ordem de transmissão. Quando um frame está programado para ser transmitido, o master node envia o header do frame de forma a convidar um slave node a enviar a informação em resposta. Qualquer node da rede consegue ler os frames transmitidos no bus.

2.6.4 Automotive Ethernet

Tecnologia bastante recente, 2013, que pode correr até 100Mbps. Tem como vantagens a sua velocidade e capacidade de banda. Usada para diagnósticos, no sistema infotainment e ainda para conectar sensores remotos, sistemas que requerem uma grande capacidade de banda e velocidade para manter a segurança do condutor [38].

Algumas das motivações para o uso de Ethernet na industria são o custo reduzido e, a maturidade da tecnologia o que lhe permite oferecer mais capacidade de banda comparativamente as restantes opções.

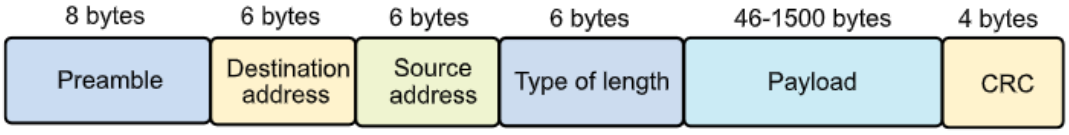


Figura 2.8: Ethernet frame [38]

2.6.5 Media Oriented Systems Transport (MOST)

MOST, o seu desenvolvimento iniciou-se em 1998 pela organização MOST, sendo direcionada para transmitir conteúdos multimédia [19]. Permite a transferência de áudio e vídeo de peer-to-peer, a diferentes data rates. A principal aplicação de MOST é orientada para aplicações multimédia, sistema de rádio, navegador de GPS, transmissão de vídeo e sistemas de entretenimento.

Figura 2.9: MOST frame [38]

- Pode conter até 64 nodes através da topologia ring;
- Tipo de deteção de erros: Cyclic Redundancy Check (CRC);
- Opera em bus de fibra ótica;
- Tem alta taxa de transferência e uma bandwidth dinâmica: possuí canais síncronos/assíncronos onde consegue alocar parte da bandwidth para serviços necessários;
- Tem três versões, MOST25, representado na figura 2.9, com frames de 64 bytes, MOST50 com frames de 128 bytes e MOST150 com frames de 384 bytes.

2.6.6 FlexRay

Disponível desde 2005, FlexRay é um shared serial bus que consegue correr até 10Mbps. Foi desenvolvida pelo grupo FlexRay e contrariamente à CAN, não existe possuí error recovery [19].

Tem como vantagem a sua grande capacidade de banda, mas, como desvantagem, o seu elevado custo e o facto de ser uma shared media.

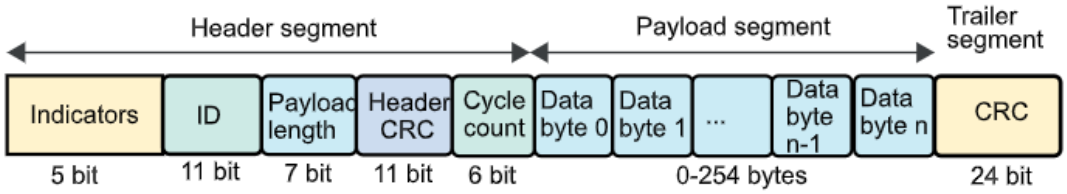


Figura 2.10: FlexRay frame [38]

O frame no FlexRay, representado na figura 2.10, consiste em três partes, cabeçalho, segmento payload e o segmento trailer. O segmento payload pode conter até 254 bytes de dados.

Um node da rede, deve transmitir o frame de modo a que o cabeçalho surja primeiro, em seguida o payload e por fim o trailer.

Alguns dos pontos mencionados em cada um dos canais de comunicação, encontram-se resumidos na tabela 2.1.

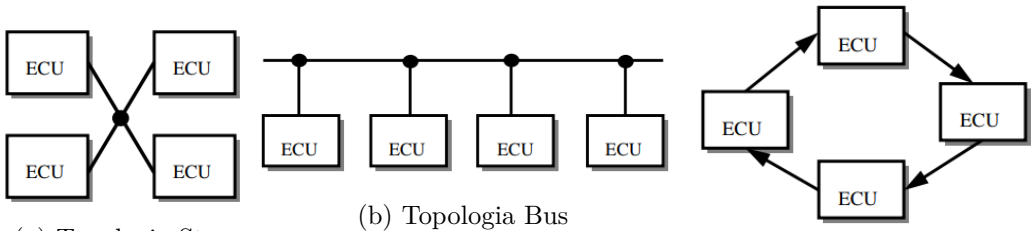
Protocolo	**Domínio**	**Bandwidth**	**Domínio**	**Topologia**
CAN	Powertrain, Body Control	125 Kbps-1 Mbps	Body	Star, Ring, Bus
LIN	Simple Applications (Less time critical)	125 Kbps-1 Mbps	Sistemas não críticos	Bus
FlexRay	Advanced Chassis Control	Até 10 Mbps	Advanced Chassis Control	Star, Bus
MOST	Infotainment Applications	Até 150 Mbps	Multimedia	Ring
Automotive Ethernet	High Bandwidth Applications	Até 100 Mbps	Multimedia	Star, Bus

Tabela 2.1: Classificação canais de comunicação

2.7 Topologias de Rede

Cada sistema adapta a topologia a usar, dependo das características da mesma. Em seguida, fazemos uma menção das topologias existentes [44]:

- **Star**, todos as ECUs estão conectadas a um hub central que, no caso de falhar, a comunicação falha. O mesmo já não se verifica no caso de uma das restantes ECUs falhar. Figura 2.11a ilustra a topologia.
- **Bus**, todas as ECUs estão conectadas ao mesmo cabo principal. No cenário de interrupção do cabo, passamos a ter dois segmentos de cabo, e normalmente continuam o seu funcionamento. A figura 2.11b ilustra a topologia.
- **Ring**, possuí dois tipos, simples e duplo. Na simples, a informação é transmitida numa direção até que chega ao destinatário. Quando um nó falha, a comunicação termina. Na topologia dupla, a informação é enviada para ambas as direções, o que torna a comunicação mais confiável. Na figura 2.11c temos ilustrado a topologia simples.



(a) Topologia Star

(b) Topologia Bus

(c) Topologia Ring

Figura 2.11: Topologias de Rede [25]

2.8 Conectividade

Um veículo é considerado conectado quando existe informação a ser trocada com servidores, apps, e com os vários componentes no interior do sistema de um veículo. Esta partilha de informação permite o funcionamento dos serviços telematics, serviços de smart mobility e muitos outros [3].

Um veículo pode conter 5 modos de conectividade:

1. ***Vehicle to Infrastructure (V2I)***

   Troca wireless entre o veículo e uma infraestrutura rodoviária para obter informações sobre trânsito e estacionamento.

2. ***Vehicle to Vehicle (V2V)***

   Partilha de dados entre veículos, tipicamente, localizações.

3. ***Vehicle to Cloud (V2C)***

   Comunicação entre veículo e sistemas de backend baseados na cloud. Permitem ao veículo o processamento de informações e comandos.

4. ***Vehicle to Pedestrian (V2P)***

   Comunicação entre veículos, a infraestruturas e dispositivos móveis pessoais, para obter informações sobre o ambiente e pedestres.

5. ***Vehicle to Everything (V2X)***

   Comunicação entre um veículo todo o ambiente exterior onde o veículo está enquadrado.

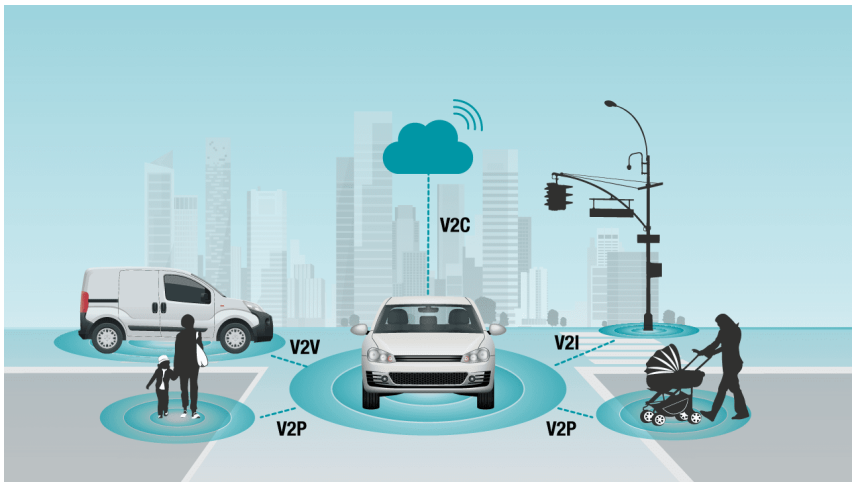


Figura 2.12: Tipos de conectividade [1]

O foco neste projeto, é a comunicação intra veículo. A apresentação dos vários modos de conectividade serve como ponto de demonstração dos pontos exteriores que interagem com o veículo. Estes podem ser usados como passe de entrada no sistema intra veículo.

Capítulo 3

Segurança Intra Veículo

De forma a falarmos de segurança, precisamos saber caracterizar o sistema que pretendemos proteger. Desta forma, e ao longo deste capítulo 3 é feita a caracterização do sistema, ou seja, número de Eletronic Control Unit (ECU)s que constituem o sistema e hardware utilizado. Após caracterizado o sistema, passamos a apresentar os algoritmos que nos ajudaram a conseguir as garantias de segurança apresentadas no capítulo 2.

3.1 Modelo de Sistema

Um veículo consiste num sistema base completo e com modelos bastante heterogéneos, onde cada fabricante possuem um modelo de sistema, com número variado de diferentes componentes, com diferentes topologias, entre outras características.

Por este motivo, estudar um sistema tão heterogéneo e com grande número de ECUs torna-se desafiador. Assim, para este projeto, decidimos limitar o nosso sistema à zona do veículo que consideramos produzir a informação mais interessante e que provavelmente mais necessita de garantias de segurança. Apresentamos em seguida, na figura 3.1, o sistema que estudamos neste projeto.

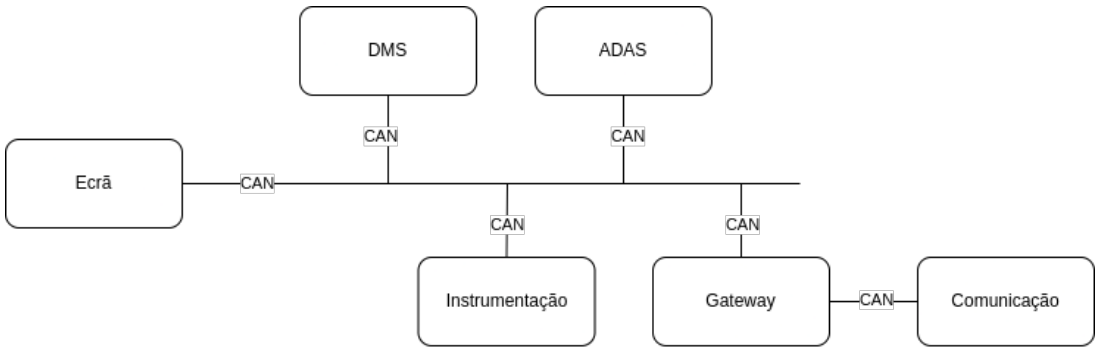


Figura 3.1: Topologia do sistema

Sistema com uma topologia bus, onde as várias ECUs comunicam entre si através de Control Area Network (CAN). Como já mencionado anteriormente, apresentamos algumas alternativas aos canais de comunicação, sendo estes os mais utilizadas em cenários do mundo real. São também consideradas devido ao seu custo de implementação, capacidades comunicativas e capacidade de resposta ao problema proposto.

CAN, bus mais utilizado na indústria automotive onde o protocolo é baseado em vários master nodes. Possuí várias vantagens relativamente à performance de comunicação como comunicação confiável e tolerância a falhas. Isto significa que no caso de uma falha na comunicação de um frame, esta é identificada, e automaticamente, o frame é reenviado.

Apesar das vantagens a nível de performance comunicativo, CAN não possuí mecanismos de encriptação e autenticação, deixando-o suscetível a ataques de replay, onde temos uma ECU adversário a enviar mensagens, fazendo-se passar por uma ECU legítima do sistema. A falta de mecanismo de encriptação e autenticação permite que entidades não autorizadas se juntem à rede e façam parte da comunicação [17]. CAN possuí vários desafios a nível de segurança nas comunicações [35]:

- **Transmissão broadcast:** Os pacotes enviados na rede não possuem endereço de origem nem destinatário. Todos os nodes da rede conseguem ouvir as mensagens transmitidas, já que estas não se encontram encriptadas;
- **Suscetível a Denial of Service (DoS):** No CAN, os pacotes são transmitidos consoante o nível de prioridade. Desta forma, se um node malicioso tiver mais alto nível de prioridade sem ativo, os outros nodes não vão conseguir comunicar.
- **Sem campo de autenticação:** Os pacotes enviado no CAN, não possuem campo de autenticação, o que permite que qualquer entidade maliciosa consiga enviar mensagens sem ser reconhecido, e consegue faz-lo para todas as entidades do sistema.

Vamos agora apresentar as várias ECUs do sistema, quais as suas funcionalidades, a informação que produzem e transmitem.

- **ECU Instrumentação**
  Responsável pelos instrumentos, conta quilómetros , conta rotações, piscas, luzes, entre outros. Produz informações relativas às luzes, piscas, limpa-para-brisas, entre outros. Recebe informações relativas à velocidade, avisos, níveis de energia, hodómetro.
- **ECU Ecrã**
  Tem na sua responsabilidade o ecrã interativo onde temos o sistema infotainment. Este permite ao condutor controlar o ar condicionado, o rádio, Global Positioning System (GPS), luzes do interior do veículo, e ainda acesso à internet. Pretende-se que o condutor aceda ao máximo de informação possível num único painel. Produz informações relativas ao sistema

de navegação e de controlo dos sistemas do carro, rádio, temperatura, entre outros. Recebe dados do telemóvel.

- **ECU Advanced Driver Assistance System (ADAS)**
  Responsável pela assistência na condução humana, realizando várias ações, desde informações sobre tráfego, estradas cortadas ou bloqueadas até assumir controlo em ações mais complicadas com ultrapassagens e estacionamento [33]. Produz informações de instrução aos sistemas do veículo, travões de emergência, estacionamento autonomo. Recebe informações dos sensores externos do veículo.

- **ECU Driver Monitoring System (DMS)**
  Sistema de monitorização do condutor, recurso de segurança que dispõe de câmaras que detetam padrões de sonolência ou distração do condutor [41]. Produz informações relativas ao estado do condutor. Recebe imagens das câmara interiores do veículo.

- **ECU Gateway**
  Serve com gateway do sistema, e, é onde temos a porta On-Board Diagnostic (OBD), responsável por self-diagnostic e capacidade de reportar falhas, de forma a fornecer ao dono ou técnico, acesso ao estado dos vários sub sistemas do veículo. Não produz informações, funciona como a gateway para a ligação com outras redes. Recebe todas as informações.

- **ECU Comunicação**
  Responsável pela comunicação bluetooth e 5G com dispositivos externos. Produz tráfego de conexões bluetooth, 4G.

3.2 Pontos de Entrada

Tendo em conta os ataques descritos na secção 2.4 e os pontos críticos da secção 2.5, vamos especificar os pontos de entrada do nosso adversário:

3.2.1 Sistema infotainment

Este sistema reúne várias informações relativas a alguns componentes do veículo como sistema de navegação GPS, rádio, conexão Bluetooth e entretenimento. É dos sistemas mais vulneráveis em veículos modernos devido à possibilidade de instalação de software e aplicações externas. A comunicação com dispositivos móveis, é também um fator de vulnerabilidade [4], o mesmo acontece com as várias portas físicas que o sistema contém. Este sistema encontra-se suscetível aos seguintes ataques:

- Injeção de malware
- Man In The Middle (MITM)

- Reverse enginnering
- Update de firmware

3.2.2 Porta OBD

Porta que permite a conexão de dispositivos externos com o sistema interno do veículo. Como referido no ponto anterior, estas portas físicas deixam o sistema mais vulnerável e com um ponto de entrada fácil. Nos ataques analisados em 2.4, são mencionados alguns exemplos relativos a esta porta, onde atacantes alteravam o OBD dongle para agir como uma ferramenta de ataque. Esta porta encontra-se suscetível aos seguintes ataques:

- Eavesdropping
- Injeção de malware
- MITM
- DoS
- Ataque de replay

3.2.3 Bluetooth

Permite a conexão de dispositivos móveis com o veículo possibilitando várias ações. Tratando-se de uma conexão wireless, um possível atacante não necessita acesso físico ao veículo, sendo que um atacante pode comprometer um dispositivo móvel que vá posteriormente conectar-se ao veículo. Desta forma, consegue aceder aos contactos, enviar áudio ou obter áudio de chamadas telefónicas. Estes acessos apenas comprometem a privacidade das informações do dono do dispositivo móvel, não parecendo afetar a segurança do veículo. Tudo isto muda, quando graças ao CAN passamos a conseguir realizar ações remotas sobre o veículo. Esta conexão wireless encontra-se vulnerável a ataques:

- Bluejacking
- Malware
- DoS
- MITM
- Sniffing

3.2.4 Sistema GPS

O funcionamento do sensor GPS deve ser confiável e seguro, já que este é um fator crucial para a aceitação de possíveis veículos autónomos. As coordenadas fornecidas pelo sensor, baseiam-se num mapa de alta definição, pelo qual é possível escolher a melhor e mais curta rota. Estas, são essenciais para o funcionamento correto e autónomo do veículo [34]. O sensor de GPS encontra-se suscetível aos seguintes ataques:

- Jamming
- Spoofing

3.3 Requisitos de Segurança

No sistema representado na figura 3.1, foram identificadas informações consideradas sensíveis, sobre as quais pretendemos fornecer garantias de segurança por se tratarem de informações sensíveis. A localização destas variáveis, o seu armazenamento e circulação pelo sistema foram identificados com o conhecimento especializado dos representantes da Continental. Em seguida apresentamos as informações identificadas:

- **Conta Quilómetros** - variável composta por 5 bytes, sendo gerada na ECU de Instrumentação, onde é também armazenado. Apartir desta ECU, é enviado para as retantes ECUs do sistema. Trata-se de um valor muito importante, manipulado pode levar a perdas financeiras [12]. O flow da variável é ilustrado na figura 3.2;

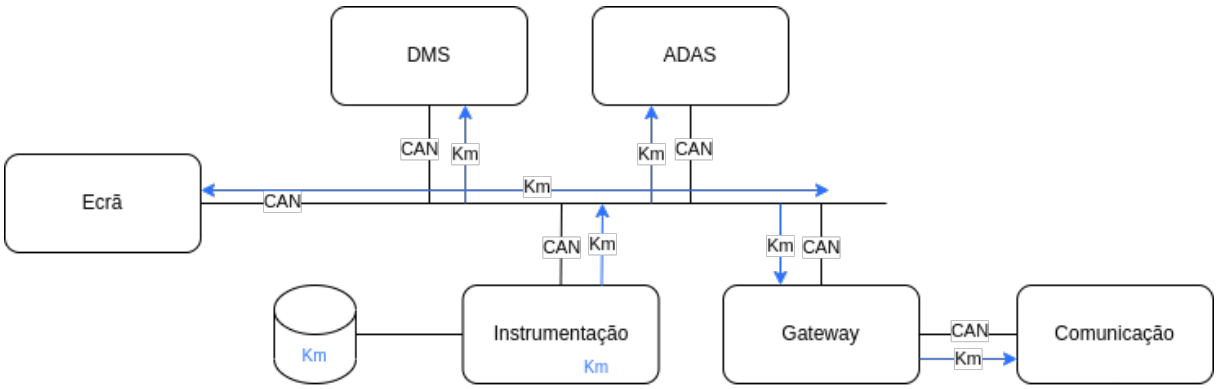


Figura 3.2: Flow conta quilómetros

Para a variável do conta quilómetros, pretendemos fornecer os requisitos de segurança integridade e autenticidade, de forma a que um adversário tentar alterar a informação ou tentar-se fazer passar por uma entidade confiável, o recetor da mensagem vai perceber que a mensagem foi alterada e enviada por uma entidade não autenticada.

- **Flag travões** - trata-se de um boolean gerado pelo ADAS, sendo depois enviado para a ECU Gateway. Trata-se de um valor instantâneo, o que não requer qualquer tipo de armazenamento no sistema. O flow da informação é ilustrado na figura 3.3;

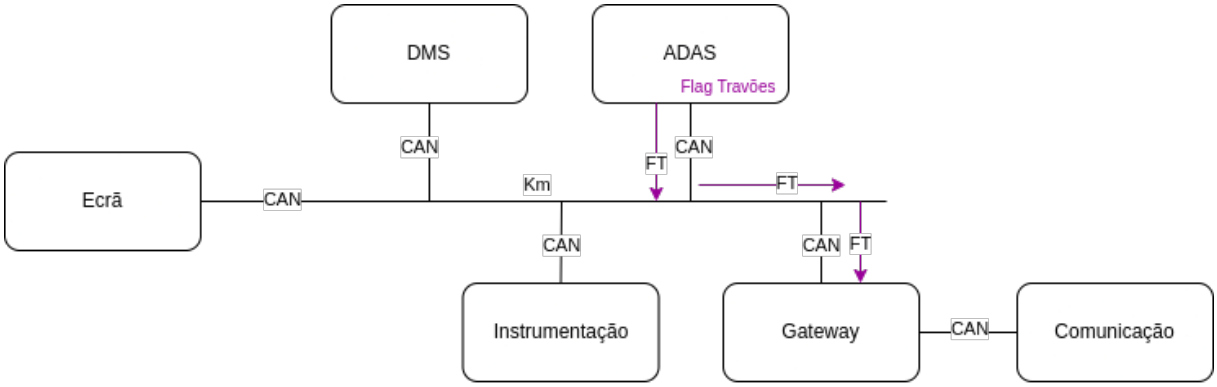


Figura 3.3: Flow flag travões

Igualmente à variável anterior, pretendemos garantir a integridade e autenticidade da informação transmitida no sistema. Com estes requisitos de segurança, pretendemos que uma adversário não consiga manipular a informação transmitida sem ser identificada, nem fazer-se passar por uma entidade confiável.

- **Coordenadas GPS** - constituído por 2 floats, 8 bytes, latitude e longitude, gerados pela ECU comunicação. Este valor é depois enviado para ECU Ecrã, onde é armazenado. O flow do mesmo encontra-se ilustrado na figura 3.3.

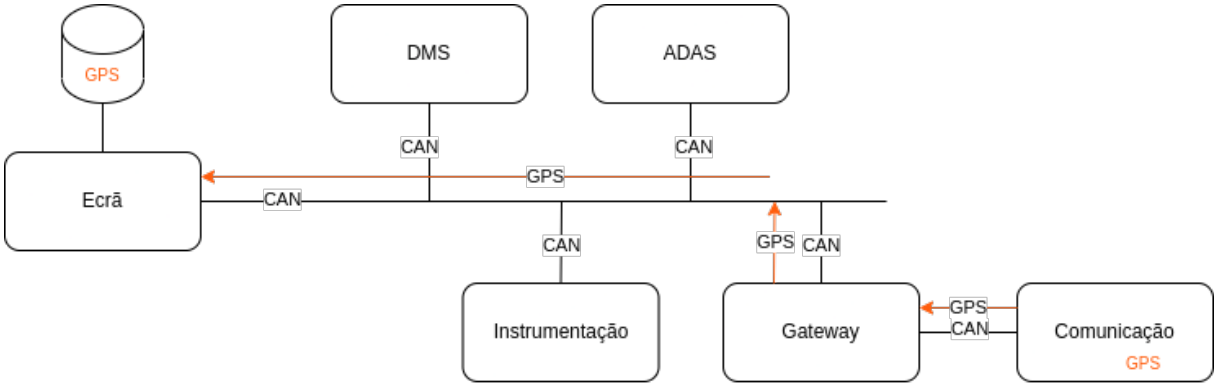


Figura 3.4: Flow GPS

Para a variável coordenadas GPS, pretendemos garantir a confidencialidade, integridade e autenticidade da informação. Desta forma vamos garantir que um atacante não consegue ver a mensagem em texto limpo, não vai conseguir manipular o conteúdo sem ser detetado e por fim, não vai conseguir fazer-se passar por uma entidade confiável do sistema.

3.4 Adversário no Sistema

Com a análise e identificação dos vetores de ataque do nosso sistema, conseguimos identificar onde se localiza o adversário no sistema. Na figura 3.5 apresentamos o adversário no sistema em questão.

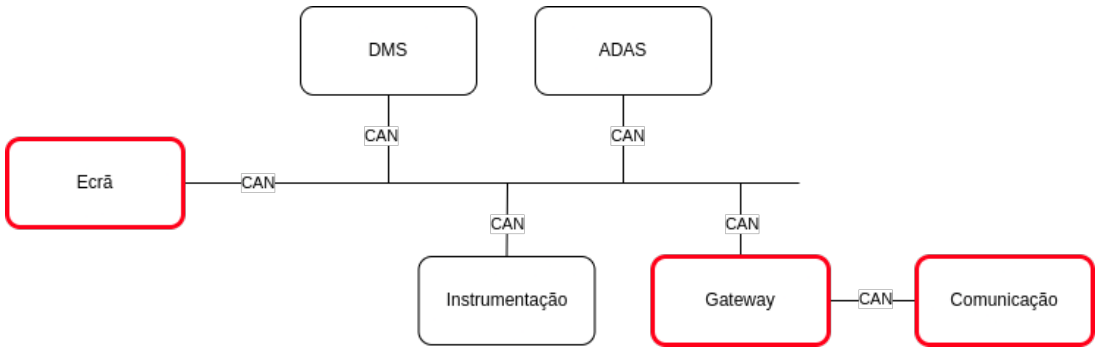


Figura 3.5: Modelo adversarial

As ECUs identificadas no sistema como possíveis adversários têm em consideração os vetores de ataque considerados, já que estas são as responsáveis pelo funcionamento dos mesmos.

1. **Ecrã:** ECU responsável pelo sistema infotainment. O sistema infotainment, como já mencionado anteriormente, é dos sistemas mais vulneráveis num veículo devido aos vários pontos que podem ser explorados por um atacante. Injeção de malware, exploração de vulnerabilidades do sistema, ataques de MITM, reverse enginnering, são alguns exemplos de manipulações deste sistema. Apresentamos em seguida alguns casos reais:

   - Common Vulnerabilities and Exposures (CVE)-2018-18203, onde uma vulnerabilidade no mecanismo de atualizações permitia que um atacante com acesso físico às portas Universal Serial Bus (USB) do veículo conseguia reescrever o firmware da unidade principal o que o permitia ter acesso root e executar código arbitrário [49];
   - Investigadores conseguiram injetar um cavalo de tróia no sistema, através de um Compact Disc (CD). Adicionaram código extra no ficheiro digital da música, que quando lida alterava o firmware do leitor, deixando aos atacante um ponto de entrada no sistema [51];
   - Investigadores conseguiram hackear um Tesla Modelo 3 através do browser embutido no sistema. Através de um bug presente no processo de renderização do browser, conseguiram executar código no firmware do sistema [2];

2. **Gateway:** ECU que comunica com a porta OBD.

   Os veículos possuem várias portas que permitem a conexão com dispositivos externos, com várias funcionalidades, desde carregamento do veículo elétrico, à conexão dos nossos dispositivos móveis, à possibilidade de obter informações e diagnósticos do sistema [20]. O

problema surge quando atacantes tentam converte-las em pontos de entrada do sistema. No cenário de isso acontecer, o atacante fica mais perto de conseguir aceder à rede do veículo, consequentemente conseguindo realizar ataques de eavesdropping e instalação de malware e vírus. Alguns cenários reais em seguida:

- Um hacker conseguiu modificar o dongle OBD e obter informações de algumas ECU do sistema, incluíndo voltagem da bateria, temperatura do líquido de arrefecimento do motor, Revolutions Per Minute (RPM), Manifold Absolute Pressure (MAP) e ainda informações sobre Throttle Position Sensor (TPS) [11].
- Investigadores conseguiram explorar uma vulnerabilidade num dongle da Bosch que os permitiu injetar mensagens maliciosas no CAN bus. Uma fuga de informação permitiu aos investigadores darem brute-force ao Personal Identification Number (PIN) secreto do dongle, conseguindo depois conectar-se a ele via bluetooth. Já com acesso ao dongle, descobriram outra vulnerabilidade no filtro de mensagens, que permitiu a injeção de mensagens maliciosas [36].

3. **Comunicação:** ECU responsável pelas comunicações bluetooth e GPS.

   Serviços wireless foram implementados nos veículos, de forma a proporcionar mais conforto e comodidade para o utilizador. Mas, a implementação destes serviços possibilita aos atacantes a entrada mais cómoda no sistema, sem necessitarem de ter acesso ao veículo. Acedendo ao sistema, estes atacantes conseguem faz sniffing de informação, injeção de malware, spoofing ou jamming.

   - No paper de Checkoway *et al.* [18], descrevem como um atacante consegue comprometer um veículo através de uma aplicação cavalo de tróia. Conseguiram fazer sniff do endereço Message Authentication Code (MAC) do bluetooth do carro, dando depois brute force ao PIN de emparelhamento.
   - No paper de Zeng *et al.* [54], desenvolveram um spoofer portátil e de baixo custo. Através do Raspberry Pi presente no spoofer conseguiram injetar localizações GPS de tempo real.

Ao longo deste documento, apresentamos o sistema estudo, a forma como os vários componentes do sistema comunicam em si. Apresentamos alguns exemplos de ataques reais a veículos, o que nos levou à identificação dos vetores de ataque do nosso sistema. Daqui traçamos um modelo adversarial, onde identificamos o atacante no sistema.

Em suma, temos um sistema onde não existem componentes de hardware ou software dedicados à segurança do sistema, onde a segurança da informação não foi pensada no processo de desenvolvimento da arquitetura de software. Da mesma forma, também não existe implementado nenhum protocolo de comunicação que previna ou mitigue possíveis ataques.

Pretendemos agora apresentar algumas das soluções já propostas, desde hardware a software, canais de comunicação alternativos ou implementação de mecanismos criptográficos sobre os

mesmos. Para concluir, pretendemos apresentar topologias alternativas que respeitem os requisitos de segurança das informações identificadas.

Capítulo 4

Abordagem

A combinação de diferentes tipos de rede, Eletronic Control Unit (ECU)s, sensores e outros componentes eletrónicos, podem resultar em diferentes tipos de topologias de sistemas. Estas topologias dependem do fabricante do veículo, que pretende o design de uma solução igualmente eficiente, conveniente e acessível. Um sistema intra veículo possuí várias limitações e requisitos, que nos impedem de implementar mecanismos de segurança já existentes, e que funcionam nas comunicações standard.

As vulnerabilidade num sistema intra veículo são fortemente influenciadas pelas características do sistema, por exemplo, as características da topologia da rede e os seus endpoints externos [23]. Isto leva-nos a refletir que, diferentes topologias de sistema, podem, de facto trazer melhorias no que diz respeito a segurança intra veículo.

Vamos explorar as várias ferramentas e possibilidade que possam trazer garantias de segurança sobre os dados a que pretendemos garantir requisitos de segurança. Tendo como objetivo final a criação de uma solução de design que forneça garantias de segurança ao sistema.

4.1 Mecanismos de segurança vs limitações de comunicação

Os canais de comunicação utilizados na comunicação intra veículo, não foram pensadas de forma a protegerem as várias mensagens trocas na rede. Desta forma, passa a ser necessária a aplicação de mecanismos de segurança sobre os canais de comunicação. Para tal, é necessário ter em consideração alguns requisitos técnicos [27]:

1. **Algoritmo criptográfico:** O algoritmo deve ser executado eficientemente e deve ser seguro contra crack da chave. O algoritmo utilizado deve ser compatível com os canais de comunicação intra veículo existentes.

2. **Busload rate:** A utilização de mecanismo de segurança com valores superiores aos disponíveis no frame faz com que seja necessária a utilização de vários frames, o que

consequentemente aumenta o busload rate.

3. **Latência da rede:** A latência presente nos mecanismos criptográficos, não deve afetar a comunicação em tempo real, que alguns sistemas necessitam.

4. **Gestão de chaves:** A segurança de chaves, é o básico dos mecanismos criptográficos, por esse motivo, estas devem ser guardadas de forma segura, assim como geradas de forma segura.

Podemos, dividir os mecanismos de segurança em dois tipos [27]:

1. **Autenticação de mensagens:** Garante a autenticidade e integridade das mensagens transferidas. Local Interconnect Network (LIN), Control Area Network (CAN), FlexRay e Ethernet, possuem mecanismos que garantem a integridade das mensagens, checksums e Cyclic Redundancy Check (CRC). Estes não conseguem garantir a autenticidade da informação, o que leva à necessidade da implementação de mecanismos de autenticação, Message Authentication Code (MAC)s e assinaturas digitais. Assinaturas digitais ocupam mais de 40 bytes, enquanto que o MAC pode ocupar 8 ou 16 bytes. Em canais de comunicação como CAN e LIN, que possuem um campo de informação máximo de 8 bytes, MAC é a melhor opção. A assinatura digital pode ser utilizada em canais como FlexRay e Ethernet.

   O calculo do MAC, pode causar, em sistemas que exigem uma performance de tempo-real e o busload rate é um aspeto critico, latência e o aumento de frames durante a transmissão de mensagens.

   A chave utilizada para as assinaturas digitais é uma chave assimétrica, o que requer alta performance computacional do Microcontroller Unit (MCU).

2. **Encriptação de mensagens:** Garante a confidencialidade das mensagens transferidas. Na escolha do mecanismo de segurança, deve ser considerada a latência que este pode causar na rede. A utilização de canais de comunicação com maior capacidade de transferência de dados, alarga a possibilidade da utilização de vários mecanismos criptográficos, *e.g.* a utilização do Advanced Encryption Standard (AES)-128 é possível utilizando Control Area Network Flexible Data-rate (CAN FD), enquanto que com CAN já não é.

4.2 Canais de comunicação alternativos

Numa rede intra veículo, podem existir várias sub redes, cenário do mundo real, onde são agrupadas as várias ECUs por domínios. Estas ECUs comunicam entre elas através de canais de comunicação que respondem às necessidades da sub rede. É também possível termos apenas uma rede, que interliga todos os componentes do sistema. Esta abordagem leva a que atacantes explorem vulnerabilidades dos pontos mais sensíveis do sistema para conseguir chegar a componentes responsáveis por funções críticas de segurança do sistema. O desafio acaba

por ser o balanço entre segurança e usabilidade: pretendemos componentes isolados, de formar a estarem mais seguros mas, necessitamos a comunicação com os restantes componentes da rede para o funcionamento dos sistemas.

Vamos em seguida apresentar alguns cenários onde combinamos o nosso sistema com canais de comunicação alternativos apresentados anteriormente, de forma a analisar o impacto a nível de performance de comunicação e garantias de segurança da informação transmitida no sistema.

LIN

Bus de baixo custo, destinado a conectar o elevado número de sensores e sistemas auxiliares que são não críticos. Devido ao seu baixo custo, é consequentemente, considerado o menos seguro comparativamente aos restantes canais de comunicação. Este protocolo não suporta streams de audio/video.

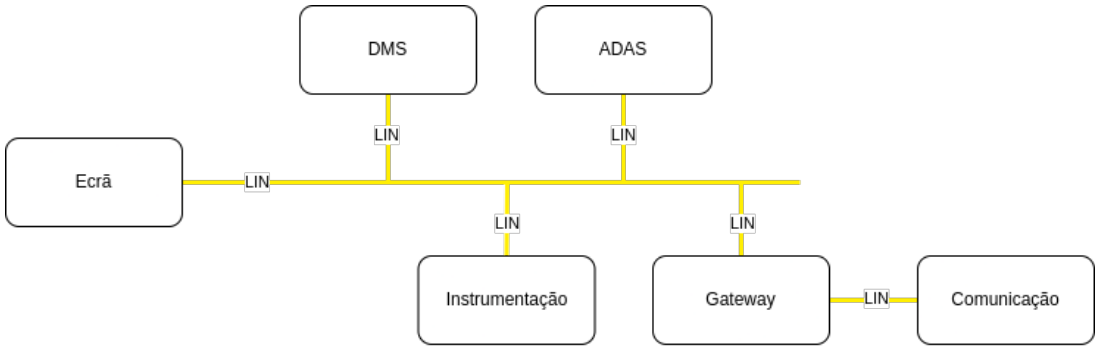


Figura 4.1: Sistema conectado por LIN

Utilizado principalmente em sistemas como cruise control, limpa parabrisas, sensores climáticos, espelhos, fechaduras de portas e motores dos bancos.Lidar com problemas de disponibilidade seria inoportuno mas, sendo estes serviços de sistemas não críticos, faz com que não sejam essenciais.

Na tabela 4.1, são apresentadas algumas diferenças relativamente ao LIN e CAN. Começando pelas diferenças de design, numa rede LIN, se o node master for comprometido, então toda a rede LIN está comprometida, onde o node master consegue enviar informação falsa para o resto do veículo, através dos sensores ligados aos nodes slaves. O comprometimento de um node slave é menos impactante. A utilização de um único fio, torna o LIN mais suscetível a interferências eletromagnéticas.

A nível de segurança do sistema, LIN apresenta alguns problemas:

- Fracos mecanismos de deteção de intrusão;
- Mensagens transmitidas em plaintext;
- Arquitetura limitada;

Parâmetro	**LIN**	**CAN**
Master/Slave design	Single Master	Multiple Master
Max Bus Speed	19.2 Kbps	1 Mbps
Nº Nodes	2 to 16 nodes	4 to 20 nodes
Device ID length	6 bits	11 or 29 bits
Error Detection	8 bits	16 bits
Physical Layer	Single Wire	Twisted Pair

Tabela 4.1: LIN *vs* CAN [22]

- Transmissão das mensagens em broadcast;
- Dependência em slaves e um único master;
- Restrito a funcionalidade não críticas.

O que acontece ao sistema se aplicarmos LIN como canal de comunicação?

LIN é principalmente utilizado em aplicações que necessitam pouca bandwidth, o que acaba por não ser o caso deste sistema, já que temos o sistema de Advanced Driver Assistance System (ADAS) e o sistema infotainment que consomem grande bandwidth. Passaríamos assim, a ter um sistema mais lento e suscetível a interferências nas comunicações. A nível de segurança, continuaríamos a ter um sistema suscetível a ataques de spoofing, o que impacta a autenticidade das informações do sistema.

FlexRay

Principalmente utilizado para aplicações de tempo real e críticas, ou integrado com outros protocolos de comunicação. FlexRay não suporta streams de audio ou vídeo.

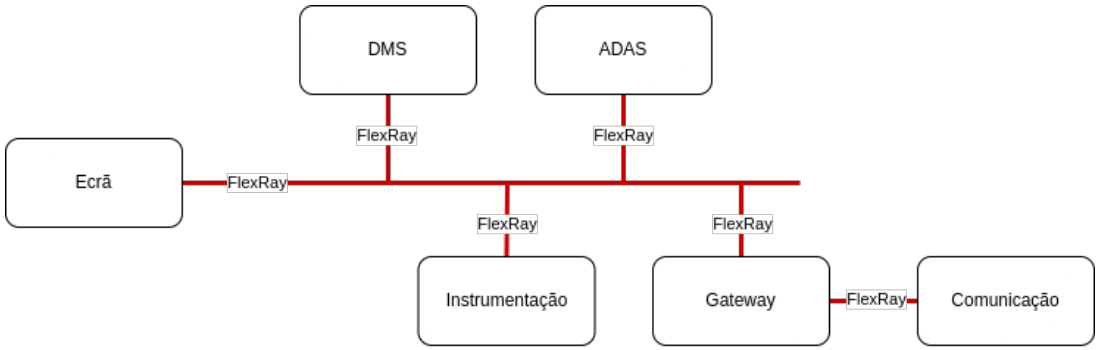


Figura 4.2: Sistema conectado por FlexRay

Desenhado para responder às necessidades dos novos serviços que foram surgindo num veículo, com necessidade de comunicações em tempo real, como telematics e a condução assistida, ADAS. Foi também desenhada para ser mais rápido e mais confiável, comparativamente ao CAN, o que

acaba por torná-lo mais caro.Comparativamente ao CAN, FlexRay, acaba por ter o mesmo custo, já que este protocolo consegue substituir várias sub redes e reduzir o número de sensores numa rede CAN. Comunica através de dois bus separados, que acaba por ser um recurso de segurança, na eventual falha de um dos canais, o sistema continua a funcionar. O mesmo não se verifica com o CAN.

FlexRay consegue enviar mensagens maiores e com menor sobrecarga, comparando com CAN, graças a um data field de 254 bytes. A sobrecarga não diminui comparativamente ao envio de mensagens de menor tamanho.

A tabela 4.2 possuí a comparação entre algumas características dos dois protocolos, de onde é possível verificar uma diferença considerável.

Parâmetro	**FlexRay**	**CAN**
Master/Slave design	Multiple Master	Multiple Master
Max Bus Speed	10 Mbps (each buses)	1 Mbps
Nº Nodes	22	4 to 20 nodes
Device ID length	11 bits	11 or 29 bits
Error Detection	32 bits	16 bits
Physical Layer	Twisted Pair/ Optical Fibre	Twisted Pair

Tabela 4.2: FlexRay *vs* CAN

O que acontece ao sistema se aplicarmos FlexRay como canal de comunicação?

No paper de Pradeep *et al.* realizam uma comparação prática entre os dois protocolos, de onde conseguiram concluir que FlexRay tem mais vantagens em sistemas automotive comparativamente ao CAN. Um valor a notar é o delay, onde FlexRay reduz o delay em 0.79ns, comparativamente ao CAN [30]. Com base no que analisamos podemos dizer que aplicando FlexRay ao nosso sistema, a nível de comunicação teríamos melhorias de performance, devido à maior capacidade de bandwidth e velocidade. A nível de segurança, continuaríamos a ter um sistema suscetível a ataques de eavesdropping, que impactam a confidencialidade das informações trocadas na rede. Temos ainda um sistema suscetível a ataques de replay, injeção de pacotes e masquerading.

MOST

Principalmente utilizado em aplicações multimédia e sistemas infotainment, Media Oriented Systems Transport (MOST) possuí três versões, MOST25 frame com 64 bytes; MOST50 com 128 bytes; MOST150 com 384 bytes. Protocolo com alta velocidade, mas com alto custo comparativamente a outros canais de comunicação. Isto levou alguns fabricantes a desistir da utilização do mesmo. Possuí uma topologia ring para a transmissão de audio, vídeo e voz.

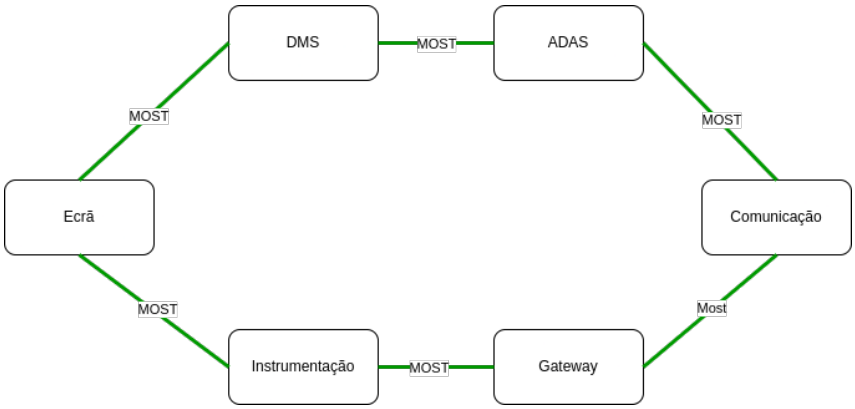


Figura 4.3: Sistema conectado por MOST

MOST tem vindo a evoluir tecnologicamente, de forma a responder às necessidades das comunicações relativamente ao tipo de informações transmitidas e à velocidade de transmissão. Das três versões existentes, acredita-se que a MOST150 é a mais promissora a ser adaptada no futuro na industria.

Na tabela 4.3, apresentamos alguns pontos comparativos a CAN.

Parâmetro	**MOST**	**CAN**
Master/Slave design	Streams/Cyclic Frames	Multiple Master
Max Bus Speed	25 or 50 or 150 Mbps	1 Mbps
Nº Nodes	64	4 to 20 nodes
Device ID length	16 or 48 bits	11 or 29 bits
Error Detection	16 bits	16 bits
Physical Layer	Optical Fibre	Twisted Pair

Tabela 4.3: MOST *vs* CAN

Graças à sua grande capacidade de bandwidth e versatilidade na transmissão de diferentes tipos de informações, realça-se em comparação a alguns dos canais de comunicação alternativos.

O que acontece ao sistema se aplicarmos MOST como canal de comunicação? A nível de comunicação, teríamos um sistema com boa performance, já que temos boa capacidade de bandwidth e alta velocidade. Relativamente à segurança do sistema, teríamos um sistema suscetível a ataques de jamming, interferindo com a disponibilidade do sistema.

Automotive Ethernet

Visto como o futuro das comunicações intra veículo graças à sua bandwidth, que responde às necessidade das novas funcionalidades que têm surgido. Graças à sua conexão point-to-point, Ethernet possuí maiores capacidades de prevenir ataques de eavesdropping, comparativamente

às restantes redes.

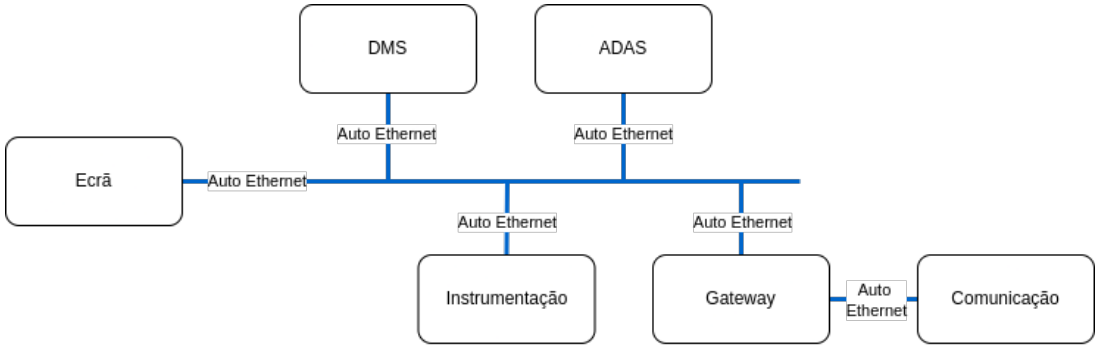


Figura 4.4: Sistema conectado por Automotive Ethernet

Na tabela 4.4 apresentamos alguns parâmetros de comparação entre automotive ethernet e CAN.

Parâmetro	**Automotive Ethernet**	**CAN**
Master/Slave design	Based on IP	Multiple Master
Max Bus Speed	100/1000 Mpbs	1 Mbps
Nº Nodes	Based on Switch ports	4 to 20 nodes
Device ID length	–	11 or 29 bits
Error Detection	32 bits	16 bits
Physical Layer	Twisted Pair	Twisted Pair

Tabela 4.4: Automotive Ethernet *vs* CAN

O que acontece ao sistema se aplicarmos Automotive Ethernet como canal de comunicação? A nível das comunicação, passaríamos a ter melhor performance de comunicação com um sistema mais rápido graças à grande capacidade de bandwidth e alta velocidade. A nível de segurança do sistema, continuaríamos a ter um sistema vulnerável a ataques de integridade e confidencialidade, acesso à rede e ataques de Denial of Service (DoS).

Conclusão: Nenhum canal de comunicação analisado possui mecanismo que respondam as necessidade de segurança da informação. Isto levamos a concluír que, com base nos canais analisados, a implementação de canais alternativos em nada melhora a segurança da informação, contudo, canais com maior capacidade de bandwidth, FlexRay, MOST e Ethernet, facilitam a implementação de mecanismos de autenticação.Vamos assim continuar a análise, passando de seguida para topologias alternativas de sistema.

4.3 Topologias alternativas

No capitulo 2 apresentamos algumas das topologias de rede que podem ser aplicadas num sistema intra veículo. Vamos perceber o impacto da aplicação das várias topologias no sistema estudo neste projeto.

Na figura 4.5, apresentamos um topologia alternativa à existente no nosso sistema, onde temos uma entidade central responsável pela interligação entre as várias ECUs da rede. Isto permite que a rede se encontre menos exposta a riscos de segurança, já que a gestão do tráfego é realizada pela entidade central. A implementação desta topologia permite o isolamento das ECUs da rede, onde facilmente conseguimos adicionar e subtrair ECUs, sem que a rede seja afetada pelo processo. Facilmente são detetadas falhas na rede.

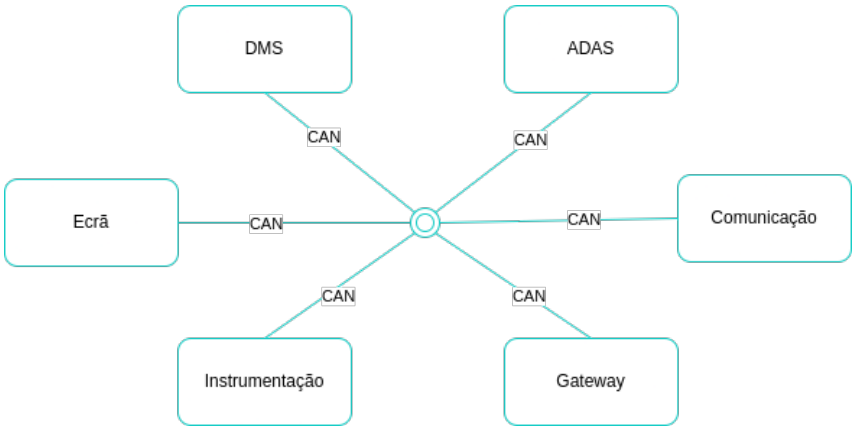


Figura 4.5: Topologia alternativa star

No entanto, a falha na entidade central pode levar à falha total da rede. A entidade central da rede é responsável por grande parte dos procedimento realizados, o que leva à necessidade de uma entidade com grande capacidade, já que uma entidade com pouca capacidade, limita a rede a poucas ECUs. A implementação desta topologia é custoso.

No entanto, uma topologia com uma entidade central, pode ajudar na implementação de mecanismos criptográficos, particularmente no processo de distribuição de chaves criptográficas.

Na figura 4.6, apresentamos agora o sistema numa topologia ring, onde temos um flow de comunicação unidirecional, e onde as ECUs comunicam apenas com a ECU seguinte. Nesta topologia, a gestão do tráfego é realizada pelas ECUs da rede. A topologia ring aguenta melhor a load, comparativamente à topologia bus. Também nesta topologia, o processo de adição ou subtração de ECUs é facilitada, o mesmo acontece com a deteção de falhas.

Contudo, a performance da rede é afetada pelo processo de adição ou subtração de ECUs. A falha numa das ECUs faz com que todo o sistema falhe. A transmissão da informação é feita pelas ECUs intermédias, o que torna este processo mais demorado comparativamente à topologia star. O número de ECUs na rede afeta a velocidade deste processo. A implementação desta

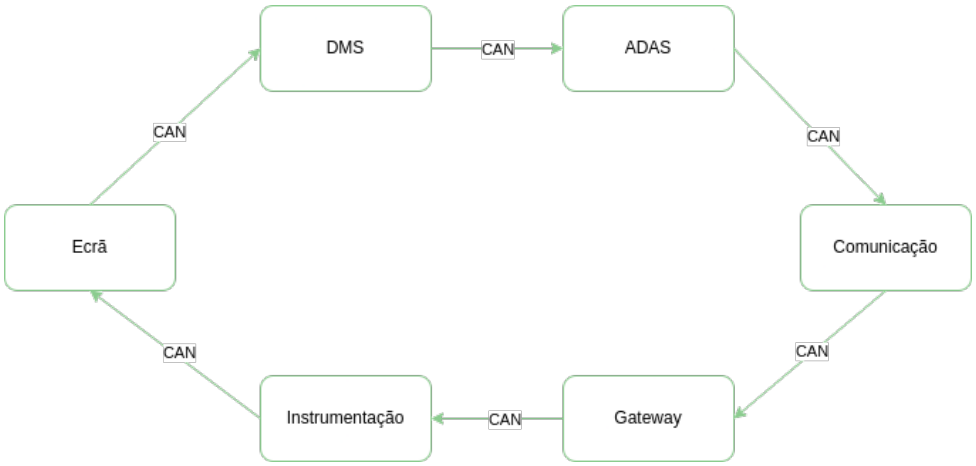


Figura 4.6: Topologia alternativa ring

topologia coloca toda a rede mais vulnerável a possíveis falhas na comunicação, a falha numa das ECUs a rede inteira falha. Comparativamente à star, a sua implementação é mais barata.

Conclusão: Hegde *et al.* [25] realizaram uma comparação de performance entre as duas topologias, ring e star. Simularam um sistema com quatro nodes cada uma, onde cada node transmitia duas mensagens. Através de medições, verificaram que a topologia ring tinha mais 3.93% no valor do bus load, comparativamente à topologia star.

Ambas têm vantagens e desvantagens, mas a topologia star acaba por oferecer características importantes para o sistema em causa. O isolamento das ECUs na topologia, impedem que um atacante que consiga aceder a um ponto da rede, tenha acesso a toda a rede. A existência de uma entidade central pode facilitar no processo de troca de chaves. Desta forma, conseguimos concluir que a topologia escolhida para a rede impacta a segurança do sistema.

De seguida apresentamos alguns papers sobre topologias de sistema, onde é feita uma análise sobre como a topologia de sistema e outros parâmetros afetam a segurança do sistema.

- No paper desenvolvido por Longari *et al.* [37], realizaram uma análise em que apresentam um algoritmo, onde o principio é o desenvolvimento *secure-by-design*. Começa por fazer uma análise de risco da topologia inicial, passando depois a fazer alterações na mesma, inserindo gateways antes das superfícies de ataque identificadas e ainda criando sub-redes, até encontrar uma solução que minimize o risco. No entanto, esta abordagem tem algumas limitações relativamente à definição das limitações, o que acaba por resultar em topologias não viáveis em cenários reais, e.g. limitações relativamente às distancias entre ECUs, ou custos de design, e.g. limite do número de gateways.
- No paper realizado por Ghadi *et al.* [23], conseguiram constatar que a segurança intra veículo, pode ser fortemente afetada pelos mecanismos de proteção de acesso, aplicados nestes três pontos do sistema:

1. Endpoints remotos;
2. Segregação da rede;
3. Localização de ECUs críticas.

Onde, os endpoints, podem facilitar o acesso à rede por entidades maliciosas, e a segregação da rede e a proteção de ECUs criticas, podem melhorar a segurança do veículo. A segregação da rede a nível lógico e físico, deve ser aplicado como forma de prevenção de acessos não autorizados, o que levou, a que os autores deste estudo, considerem a segregação como um recurso vital de segurança [23]. Os endpoints são frequentemente protegidos por gateway, mas devido ao seu custo e complexidade, não é possível a sua aplicação por endpoint.

Durante o estudo, mencionam a importância de olhar para estes pontos sensíveis identificados, já que são ameaças para a segurança do veículo. Isto levou a que os autores considerassem os pontos identificados como base para o nível de vulnerabilidades do sistema.

Através da aplicação de hierarchical clustering, conseguiram classificar e organizar os vários modelos de veículos pelos valores das suas vulnerabilidades, o que facilitou a observação de padrões de vulnerabilidades em certas redes dos veículos. Esta observação de padrões levou à conclusão de que categoria de preço e público-alvo dos veículos, são indicadores de níveis de segurança, e.g. De acordo com a topologia do veículo mais caro da marcar Toyota, este mostra níveis de segurança mais altos, comparativamente a um modelo mais barato da mesma marca. Com o estudo realizado, conseguiram concluir que o aumento do número de rede segregadas, tem um impacto positivo relativamente à segurança no veículo.

4.4 Hardware Confiável

Os canais de comunicação possuem requisitos e limitações de forma a garantir o seu correto funcionamento. Estes requisitos, impedem muitas vezes a aplicação de mecanismos criptográficos devido à carga que trazem para a comunicação. Uma possível solução para estas limitações passa pela utilização de soluções baseadas em hardware.

Secure Hardware Extension (SHE) utilização na ECU Gateway, onde seria responsável pelo armazenamento seguro das credenciais criptográficas.

Hardware Security Module (HSM) aplicado nas ECUs pode ser utilizado para a execução de procedimentos criptográficos num tempo ideal. Isto a utilização de mecanismos criptográficos, sem que os recursos limitados das ECUs impactem esta utilização.

Trusted Platform Module (TPM) aplicar sobre ECUs que necessitem realizar operações criptográficas.

Arm TrustZone reforço do isolamento dos componentes críticos dos não críticos do sistema. Aplicação da execução secure sobre as ECUs críticas do sistema e aplicação da execução non-secure sobre as restantes ECUs do sistema

De seguida apresentamos alguns papers sobre a utilização de componentes de hardware seguro na industria automotive.

- O modulo Arm, foi utilizado no paper [45], onde se focaram na otimização das primitivas criptográficas. Aqui utilizam mecanismos criptográficos como AES e Hash-based Message Authentication Code (HMAC) para aplicar na plataforma ARM. A utilização destes mecanismo é possível, já que a proposta é feita sobe a utilização de CAN FD, que possuí um campo payload com tamanho de 64 bytes. Propõem uma arquitetura para as ECUs, através da qual conseguem garantir três funcionalidades de segurança, confidencialidade e integridade das mensagens, e autenticação das ECUs.

- No paper [39], propõem uma solução baseada em hardware, onde pretendem reduzir o tempo necessário no processo de atualização de chaves num canal CAN. Propõem a separação da componente de segurança do CAN, para que esta possa ser aplicada em hardware Field-Programmable Gate Array (FPGA). Propõem também, a aplicação de Linear Feedback Shift Register (LFSR)s como um gerador pseudo-aleatório para geração e sincronização de chaves.

  Na figura 4.7, ilustra a arquitetura da solução apresentada. Cada node passa a ter AES 128 bits e dois LFSR também de 128 bits, responsáveis pela geração de seeds para a atualização da chave e escolher aleatoriamente a altura de atualização. O pulso de atualização é iniciado pelo head node, sendo que cada node tem de saber o delay entre ele e o último node, tail node.

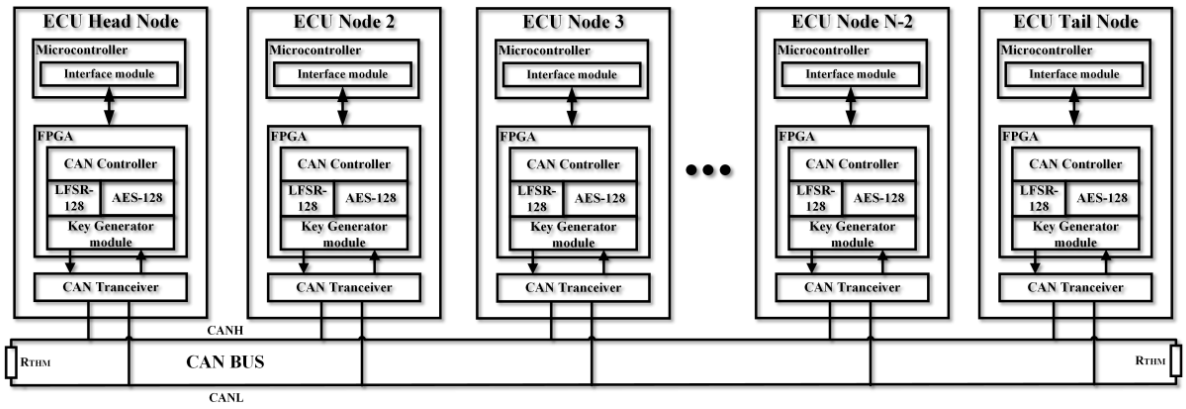


Figura 4.7: Solução proposta em [39]

4.5 Conclusão

Identificamos três características do sistema que pretendemos perceber o impacto a nível da segurança do sistema. Analisamos os canais de comunicação utilizados, a topologia da rede e hardware confiável.

Relativamente aos canais de comunicação, estes não acrescentam relativamente à segurança da informação, mas, alguns têm características que permitem a aplicação de mecanismos criptográficos. Relativamente à topologia do sistema, já possuí um impacto na segurança do sistema. A topologia de rede com uma entidade central, facilita no processo de troca de chaves, e onde podemos considerar a implementação de hardware seguro. Relativamente a hardware seguro, o ideal era um sistema onde todas as ECUs tinham hardware confiável. Este cenário aumentaria o custo de produção do sistema.

Outras características a considerar de forma a termos um sistema mais seguro, segmentação da rede e gateway com firewall, como ilustra a figura 4.8.

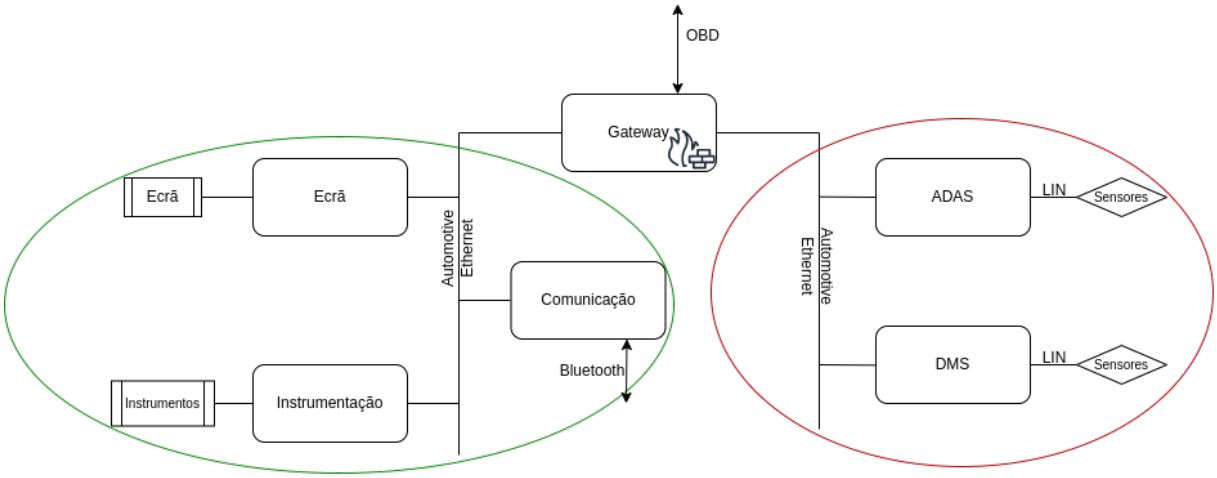


Figura 4.8: Proposta de solução

Com base nas várias funcionalidades que incorporam o sistema estudado, foi feita uma divisão entre funcionalidade de carácter crítico, correspondente às ECUs no cortorno vermelho, e funcionalidade de carácter não crítico, correspondentes às ECUs no contorno verde. Esta divisão permite a segmentação da rede através da Gateway. Outra possível solução para a segmentação da rede seria a aplicação de hardware seguro, como é o caso do Arm TrustZone.

A utilização da gateway com uma firewall aplicada, permite uma maior proteção ao sistema contra entidade externas que queriam aceder através da porta On-Board Diagnostic (OBD).

Utilização de LIN para a comunicação com os sensores, Automotive Ethernet como backbone e para a transmissão de conteúdos multimédia.

Capítulo 5

Conclusões e Trabalho Futuro

5.1 Conclusões

Ao longo deste documento é feito o estudo dos conceitos teóricos existentes da industria automotive, em particular, a comunicação intra veículo. Ao longo deste estudo, verificamos a necessidade de delimitar o sistema total do veículo, devido ao elevado número de componentes que envolve. Assim, ficamos com um sistema com seis Eletronic Control Unit (ECU)s, que representa grande parte das funcionalidades mais interativas com o condutor e restantes passageiros.

Identificamos algumas características do sistema que podem ter um impacto na segurança do sistema, canais de comunicação alternativos, topologia de sistema e hardware confiável. Pretendíamos perceber o impacto na segurança do nosso sistema, então realizamos uma análise.

Os canais de comunicação apresentados neste projeto não fornecem garantias de segurança, alguns deles possuem características que melhoram a performance de comunicação e possibilitam a implementação de mecanismos externos de segurança. No que diz respeito à topologia do sistema, conseguimos observar vantagens e desvantagens das topologias apresentadas. A topologia utilizada impacta a segurança do sistema.

Apresentamos alguns estudo relativos ao impacto da topologia e sobre a utilização de componentes de hardware seguro. Conseguimos observar a realização de muito trabalho na industria automotive, com várias propostas de solução. O grande problema de muitas destas soluções passa pela implementação num cenário real.

O principal problema na aplicação de requisitos de segurança sobe a informação são as várias limitações e requisitos que são necessários ter em consideração. Isto torna a implementação de mecanismos criptográficos seguros e suficientes, impossível.

5.2 Trabalho Futuro

Para trabalho futuro pretende-se:

- Criação de uma Proof of Concept (PoC) do sistema. Emulação do comportamento das ECUs através do log do sistema da Continental. Sobre os canais de comunicação, seriam aplicados mecanismos criptográficos de forma a analisarmos o impacto da sua implementação. Aplicação de componentes de hardware e cablagem necessária no PoC.
- Análise prática do conteúdo deste projeto. Emulação do comportamento das ECUs e analisar o impacto da implementação canais de comunicação alternativos, topologias alternativas e hardware confiável.

Bibliografia

[1] How connected vehicles leverage data: 3 common questions.

[2] Tesla car hacked at pwn2own contest.

[3] 2021 global automotive cybersecurity report, Feb 2021.

[4] 2022 global automotive cybersecurity report, Feb 2022.

[5] Obd-ii enginnered into a custom attack took, Sep 2022.

[6] Hackers targeted vehicles of american oem through bluetooth attack, Sep 2022.

[7] Diy tool used for remote monitoring, Sep 2022.

[8] Autothreat® intelligence cyber incident repository, Sep 2022.

[9] Geneva auto show affected by gps spoofing stunt, Sep 2022.

[10] Hacker exploits vulnerability in oem infotainment system, Sep 2022.

[11] Obd hacked to display data on vehicle dash, Sep 2022.

[12] Odometer fraud on the rise in austin, usa, Sep 2022.

[13] Full control of the corporate network from the tcu, Sep 2022.

[14] Permission bypass vulnerability found in vehicle infotainment os, Sep 2022.

[15] Vulnerabilities found in luxury car infotainment system, Sep 2022.

[16] Jean-Philippe Aumasson. *Serious cryptography: a practical introduction to modern encryption*. No Starch Press, 2017.

[17] Mehmet Bozdal, Mohammad Samie, and Ian Jennions. A survey on can bus protocol: Attacks, challenges, and potential solutions. In *2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*, pages 201–205. IEEE, 2018.

[18] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. Comprehensive experimental analyses of automotive attack surfaces. In *20th USENIX security symposium (USENIX Security 11)*, 2011.

[19] Kevin Van Cleave. A survey of automotive ethernet technologies and protocols, Jul 2021.

[20] Zeinab El-Rewini, Karthikeyan Sadatsharan, Daisy Flora Selvaraj, Siby Jose Plathottam, and Prakash Ranganathan. Cybersecurity challenges in vehicular communications. *Vehicular Communications*, 23:100214, 2020.

[21] CSS Electronics. Obd2 explained - a simple intro [2022], Nov 2021.

[22] Joseph M Ernst and Alan J Michaels. Lin bus security analysis. In *IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society*, pages 2085–2090. IEEE, 2018.

[23] Maen Ghadi, Ádám Sali, Zsolt Szalay, and Árpád Török. A new methodology for analyzing vehicle network topologies for critical hacking. *Journal of Ambient Intelligence and Humanized Computing*, 12(7):7923–7934, 2021.

[24] John Giordani. Cyberattacks on vehicles pose a threat to drivers and manufacturers, Apr 2022.

[25] Rajeshwari Hegde, Siddarth Kumar, and KS Gurumurthy. The impact of network topologies on the performance of the in-vehicle network. *International Journal of Computer Theory and Engineering*, 5(3):405, 2013.

[26] Olaf Henniger. Evita, 2008.

[27] Qiang Hu and Feng Luo. Review of secure communication approaches for in-vehicle network. *International Journal of Automotive Technology*, 19(5):879–894, 2018.

[28] Jun Huang, Mingli Zhao, Yide Zhou, and Cong-Cong Xing. In-vehicle networking: Protocols, challenges, and solutions. *IEEE Network*, 33(1):92–98, 2018.

[29] Pilar DinizPilar is an on-the-road Editor from Brazil living in Bali. On Geeqer she covers phones. Obd i vs obd ii: What is the difference?, Nov 2021.

[30] Pradeep .J, S Sebasteen, and R Dineshkrishna. Comparison of can and flexray protocol for automotive application. *International Journal of Pure and Applied Mathematics*, 119: 1739–1745, 10 2018.

[31] 24 January. Infographic: Potential cyberattacks in connected cars, Jan 2022.

[32] Karl Henrik Johansson, Martin Törngren, and Lars Nielsen. *Vehicle Applications of Controller Area Network*, pages 741–765. Birkhäuser Boston, Boston, MA, 2005. ISBN: 978-0-8176-4404-8. doi:10.1007/0-8176-4404-0$_3$2.

[33] Rahul Kala. 4 - advanced driver assistance systems. In Rahul Kala, editor, *On-Road Intelligent Vehicles*, pages 59–82. Butterworth-Heinemann, 2016. ISBN: 978-0-12-803729-4. doi:https://doi.org/10.1016/B978-0-12-803729-4.00004-0.

[34] Mohsin Kamal, Arnab Barua, Christian Vitale, Christos Laoudias, and Georgios Ellinas. Gps location spoofing attack detection for enhancing the security of autonomous vehicles. In *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*, pages 1–7. IEEE, 2021.

[35] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, et al. Experimental security analysis of a modern automobile. In *2010 IEEE symposium on security and privacy*, pages 447–462. IEEE, 2010.

[36] Alexei Kovelman. A remote attack on the bosch drivelog connector dongle, Mar 2020.

[37] Stefano Longari, Andrea Cannizzo, Michele Carminati, and Stefano Zanero. A secure-by-design framework for automotive on-board network risk analysis. In *2019 IEEE Vehicular Networking Conference (VNC)*, pages 1–8. IEEE, 2019.

[38] Alfonso Martínez-Cruz, Kelsey A Ramírez-Gutiérrez, Claudia Feregrino-Uribe, and Alicia Morales-Reyes. Security on in-vehicle communication protocols: Issues, challenges, and future research directions. *Computer Communications*, 180:1–20, 2021.

[39] Adirek Maruaisap and Pinit Kumhom. A hardware-based security scheme for in-vehicle can. In *2016 International Computer Science and Engineering Conference (ICSEC)*, pages 1–5. IEEE, 2016.

[40] 2020 Mobility Insider April 16. What is an electronic control unit?, Apr 2020.

[41] 2021 Mobility Insider April 26. What is a driver-monitoring system?, Apr 2021.

[42] MotorHowTo.com. Motorhowto.com.

[43] Nicolas Navet and Françoise Simonot-Lion. In-vehicle communication networks-a historical perspective and review. *Industrial Communication Technology Handbook*, 96:1204–1223, 2013.

[44] Zsombor Petho, Intiyaz Khan, and Árpád Torok. Analysis of security vulnerability levels of in-vehicle network topologies applying graph representations. *Journal of Electronic Testing*, 37 (5):613–621, 2021.

[45] Bikash Poudel and Arslan Munir. Design and evaluation of a reconfigurable ecu architecture for secure and dependable automotive cps. *IEEE Transactions on Dependable and Secure Computing*, 18(1):235–252, 2018.

[46] Kartik Rangam. What is an ecu? electronic control unit (ecu) explained, Oct 2020.

[47] GPS Tracking Review. How gps works in cars, Feb 2022.

[48] Michele Scalas and Giorgio Giacinto. Automotive cybersecurity: Foundations for next-generation vehicles. In *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)*, pages 1–6. IEEE, 2019.

[49] Sgayou. Cve-2018-18203, Aug 2020.

[50] Balázs Simacsek. Can we trust our cars? *NXP Semiconductors-Paper*, 2019.

[51] Iain Thomson. Stop the music! booby-trapped song carjacked vehicles – security prof, Jun 2017.

[52] Nikola Velichkov. Lin bus protocol: The ultimate guide (2022), Mar 2021.

[53] Aastha Yadav, Gaurav Bose, Radhika Bhange, Karan Kapoor, NCSN Iyengar, and Ronnie D Caytiles. Security, vulnerability and protection of vehicular on-board diagnostics. *International Journal of Security and Its Applications*, 10(4):405–422, 2016.

[54] Kexiong Curtis Zeng, Shinan Liu, Yuanchao Shu, Dong Wang, Haoyu Li, Yanzhi Dou, Gang Wang, and Yaling Yang. All your {GPS} are belong to us: Towards stealthy manipulation of road navigation systems. In *27th USENIX security symposium (USENIX security 18)*, pages 1527–1544, 2018.