UiO : Department of Informatics
University of Oslo

Denial of Service attacks in vehicle platoons

Jamming resistence and mitigation

Georgios Patounas
Master’s Thesis Spring 2015

Denial of Service attacks in vehicle platoons

Georgios Patounas

30th January 2015

Abstract

This master thesis overviews the fields of Intelligent Transportation Systems (ITS) and Vehicular Ad hoc Networks (VANETs) and their role in future transport. It describes the key challenges in security with a focus on low-level attacks and vehicle platooning applications. It points out that denial of service attacks could prove particularly disruptive and dangerous in a vehicular network.

The project focuses on prevention, detection and mitigation of denial of service attacks in a vehicle platoon. To achieve this, a simulator was created using MATLAB and Simulink that can reproduce the physical workings of a vehicle platoon as well as the wireless communication between the vehicles and the possibility of malicious interference. Defence methods are implemented and tested against jamming attacks. These include methods of interference reduction, data redundancy and warning systems based on on-board vehicle sensors.

The results presented are positive and successful in increasing a vehicle platoon's resiliency to attacks. It is the hope of the author that this work along with the simulating environment created, will provide an incentive for further development and examination.

Acknowledgements

I would like to express my gratitude to my supervisors, professor Yan Zhang and professor Stein Gjessing.

The University of Oslo and Norway that provided me with this wonderful opportunity.

Eva, Thiseas and all my friends who supported me throughout my studies.

My family, my parents and most importantly my brother, without whose guidance and support this work would not have been possible.

Contents

List of Figures

List of Tables

Preface

Ad hoc networks have long been envisioned as the solution in scenarios where traditional infrastructure based communication is not practical or desirable. With the establishment of wireless communication technologies and the increase of computing power on small devices, Mobile Ad hoc Networks (MANETs) have found many important applications while research in the field is ongoing.

An application of particular interest is Vehicular Ad hoc Networks (VANETs) for the realization of Intelligent Transport Systems (ITS). ITS have been described since 1939 when General Motors presented their vision for the future where "driver-less" vehicles moved under automated control. Currently, advances in computing technologies, microelectronics and sensors have brought this vision closer with many of its aspects already in widespread use. With the vehicle population exceeding 1 billion worldwide in 2010, Vehicular networks have the potential of being one of the most important applications of Ad hoc networking. The scale and special nature of such a network presents several challenges in regards to communications and security that need to be addressed in this new perspective.

Vehicle platooning is an especially attractive application of ITS that allows vehicles to operate autonomously while providing large benefits in energy consumption, road congestion and safety. For the implementation of such an application the possibility of incidental or malicious interference needs to be addressed and the development of a resilient communication network is imperative.

Part I

Introduction

Chapter 1

Background

1.1 Intelligent Transportation Systems

1.1.1 Overview

As defined by the European Union, “Intelligent Transportation Systems (ITS) are systems in which information and communication technologies are applied in the field of road transport, including infrastructure, vehicles and users and in traffic management and mobility management, as well as for interfacing with other modes of transport” [24].

The IEEE defines Intelligent Transportation Systems (ITS) as "those utilizing synergistic technologies and systems engineering concepts to develop and improve transportation systems of all kinds" [14].

In short, the field is focused on the utilization of communications and information technologies to improve on the use of transportation networks.

ITS have applications in all modes of transport (see figure 1.1):

- **Automotive applications**

  In the automotive industry, automation has long been envisioned as the future. The beginning of modern, mass production of cars can be traced back to 1914. Just 25 years later General Motors presented their vision for the future of transportation in the 1939 World’s Fair in New York. At that time cars were already very popular but the development of infrastructure could not keep up and the road and highway system was practically non existent. The exhibit called "Futurama" introduced life in "the world of tomorrow", a utopia where automated highways connected cities [32].

- **Aviation, Rail, Shipping**

  Even though the term has been closely linked to automotive transportation, intelligent systems are in use in every mode of transport. In the rail and shipping sectors, the first applications of wireless communication goes back to the 70s with analogue radio and remote diagnostics. Nowadays information and communications technologies are an integrated and vital part of the industry and have multiple purposes [19]:

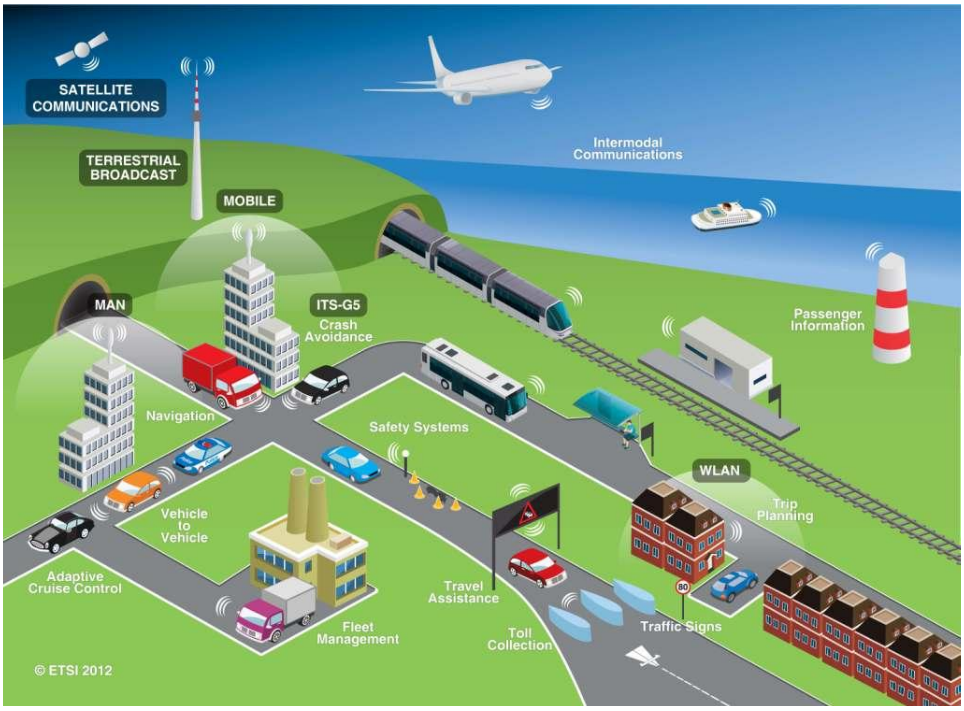


Figure 1.1: A figure of ITS applications and interoperability [3]

  - Signalling systems
  - Vehicle positioning
  - Passenger load, schedule estimation, event messages
  - Diagnostic systems
  - Communication and entertainment systems
  - Weather information

Such systems are even more prevalent and important in aviation. Collision avoidance systems, radio communications and logistic systems have been in use for decades and are at the core of modern commercial flights.

1.1.2 Motivation

The motivation for ITS lies in their several potential benefits:

- Increased efficiency
- Greater commuting speeds
- Accurate and timely status information
- Lower costs
- Increased safety

- Effective demand-response management
- Environmentally friendly commuting
- Increased comfort and convenience

1.1.3 Current status

Despite great efforts in urban planing roadway infrastructure and highway systems, road transport is constantly a source of frustration owing to several problems like unpredictable drivers, accidents and low capacity that ultimately lead to inefficiency in both time and material resources. The most obvious consequence of such problems is congestion in automotive networks. Congestion has been a major issue for a very long time and its severity keeps escalating thanks to the rapidly growing number of vehicles on the roads. Average vehicular speeds have in some cases remained unchanged from 100 years ago when horse-drawn carriages were used [9].

At this time, a review of the related literature indicates a keen interest in several applications and areas of research including system planning, vehicular traffic modelling, vehicle tracking, autonomous driving and GPS-based guidance, signal control, smart braking, lane detection and steering control, intelligent cruise control, disseminating of critical information to drivers, cooperative driving, entertainment and more.

Despite this interest only few applications of ITS can be seen in everyday use, mostly automatic toll collection, traffic monitoring and simple informatory systems (variable message signs, radio announcements). These are easy to introduce, non-intrusive applications with little or no requirements on the vehicle driver's part but their effect on commuting efficiency is correspondingly small.

Larger projects have been held back because of unwillingness to commit to the seemingly immense research and development required. At this point however, ITS seems to be the next logical step:

- The use of electronics and telecommunications has become extremely commonplace and vehicles have integrated increasingly more electronic safety and information systems.
- The cost and complexity of development and deployment of new technologies and services has been radically reduced.
- Experience and research have addressed many of the concerns for reliability and safety.

1.1.4 Communication Requirements

Many different communication standards have been proposed for ITS ranging from optical Line-Of-Site (LOS), short range solutions to long range radio communication. The diversity of applications in the field dictates no one solution to fit every scenario. Some of the prominent communication protocols are described in section 1.4.

1.2 Platooning

1.2.1 Overview

Platooning is the grouping of individuals in a way to provide benefits to the group depending on the application.

- **In nature**

  Animals have been observed to travel in formations. In [2], lobsters travelling in a queue reduced their hydrodynamic drag to roughly half of what is sustained by an individual. More research has focused on migratory birds [20], [13] which have been found to travel up to 70% further when travelling in formation owing to reduction of drag by 45% compared to a single bird. Birds gain additional lift by flying in the up-wash of the ones ahead of them. A second benefit of flying in formation is that communication between the members is preserved as visual contact can be maintained easily.

- **In aviation**

  Formation flying was developed during World War I [6] and quickly became standard practice for fighter aircraft. Similarly to bird formations, this provides better communication and visibility as well as concentration of fire-power. The benefit of reduced drag applies here too but has not been exploited yet in commercial flights due to inadequate research and concerns about safety, however recently there has been renewed interest and extensive research on the subject [23].

- **In automotive**

  Similar benefits apply to road going vehicles. This is especially seen in competitive sports, from bicycle racing to automotive racing. This technique known as drafting allows significant energy savings and higher performance by reducing atmospheric drag.

1.2.2 Motivation

In automotive applications, grouping vehicles into platoons provides a way to increase the capacity of roadway systems while improving efficiency and safety. Platoons exchange information between their members to safely decrease the headway between the vehicles and allow them to move as a single unit. Such a system could be completely autonomous, eliminating the constant need for human interaction. This capability would offer multiple additional benefits including:

- Reduction of the atmospheric drag leading to significantly improved fuel consumption

- Instantaneous reaction times leading to improved safety

- Dampening of acceleration forces leading to reduced vehicle wear and improved comfort for the passengers

- Unattended driving

1.2.3 Current status

A variety of scenarios have been considered for the concept of platooning. Initially, these included significant amounts of modifications to the road infrastructure and vehicles and possibly significant changes in driving procedures such as scheduling of the trip beforehand to coincide with an available platoon or using separate driving lanes and routes. Subsequently, with cheaper electronics and integration of electronic systems into vehicles by the manufacturers efforts moved to more natural solutions where no modifications are required to the road infrastructure and platoons follow a specialized lead vehicle driven by a professional driver [33]. Eventually, systems based solely on equipment that will come standard in commercial vehicles can be envisioned, however due to the complexity and safety critical nature of such a system there are still significant challenges to be solved, for example interactions with conventional traffic on public roads. Acceptability is also an important issue that has yet to be solved.

At this point, important steps have already been taken towards this direction with the introduction of several driving assistance systems into new vehicles by the manufacturers:

- **In-vehicle navigation** systems provide autonomous geo-spatial positioning and guidance.

- **Adaptive Cruise Control** monitors the area around a vehicle and adjusts its speed to maintain a safe distance from other vehicles. Control is imposed based on sensor information from on-board sensors only.

- **Intelligent speed adaptation** adjusts the vehicle's speed to the local speed limit (through map information or sign recognition).

- **Traffic sign recognition** recognizes the traffic signs put on the road (speed limits, stop signs, dangerous turns ahead etc.) and warns the driver.

- **Lane departure warning** warns a driver when the vehicle begins to move out of its lane unintentionally.

- **Blind spot detection** detects vehicles located in areas where view can be obstructed by the design of the vehicle or human anatomy.

- **Collision avoidance** systems use on-board sensors to detect an imminent crash and prevent it or at least reduce its severity and protect the occupants of the vehicle.

1.2.4 Communication Requirements

The principals of operation of platooning dictate the need for an extremely reliable, short to medium range solution of adequate performance. Despite efforts of standardization, there is still considerable debate around this subject and many novel solutions attempting to combine different protocols to offer the best combination of reliability and performance.

1.3 Networking Paradigms

1.3.1 Mobile Ad hoc Networks

A Mobile Ad hoc Network (MANET) is a type of self-organizing network that combines wireless communication with a high-degree node mobility. Unlike conventional networks, they have no fixed infrastructure (base stations, centralized management points etc.). This makes them attractive for many flexible applications where the network topology may change rapidly or the fixed infrastructure may be infeasible or non-operational. Conventional networks use dedicated nodes to carry out basic functions such as packet forwarding, routing, and network management. In ad hoc networks, these are carried out collaboratively by all nodes available. Nodes on MANETs use multi-hop communication: nodes that are within each other's radio range can communicate directly through wireless links, whereas those that are far apart must rely on intermediate nodes to act as routers to relay messages. Mobile nodes can move, leave, and join the network, and routes need to be updated frequently due to the dynamic network topology.

1.3.2 Vehicular Ad hoc Networks

VANETs are a special form of MANETs formed by the use of short-range radios installed in private and public vehicles. The first requirement of VANETs is to have each vehicle equipped with some form of short-range communication facility. Other optional components of a VANET node include those for providing detailed position information, road-side infrastructure units (RSUs), and central authorities responsible for identity management and registration. Communication in these networks involves both Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications. Vehicles communicate with one another when they are within their transmission ranges. Vehicles will also communicate with road-side infrastructure, if and when it is present. The road-side infrastructure will be spread regularly or sporadically depending on the region and extent of deployment. Vehicular Networks have several unique characteristics that significantly affect the development of hardware, software and communication protocols targeted at this field. Examples are:

- Rapid topology changes

- Frequent fragmentation
- High mobility
- Dynamic scale and density
- Real-time requirements
- Location awareness requirements
- Incentive based participation
- Relaxed power constraints (compared to usual MANET applications)
- High privacy requirements (affecting authentication paradigms)
- Failure criticality (critical infrastructures)
- No security separation (completely open and distributed system)
- Vulnerability to physical attacks

These present additional challenges and opportunities when considering issues such as communication protocols and security.

1.4 Communication Protocols

Focusing on VANET applications, there have been several communication protocols proposed.

IEEE 802.11 and DSRC

This is the most prominent protocol in wireless communication and is therefore mentioned here in greater detail. Dedicated Short-Range Communications (DSRC) is based on IEEE 802.11 technology and proceeds toward standardization under the name of IEEE 802.11p. DSRC is attractive due to the large bandwidth and the possibility of using multiple channels. More importantly, the 802.11 wireless specifications have been extremely popular and globally used since 1999 (802.11a) and as such have been under extensive testing and continuous improvements. The IEEE 802.11p standard, looks at issues related to the highly dynamic environment and the extremely short time durations, during which communications must be completed due to the high speed of the communicating vehicles. DSRC has two modes of operations: Ad hoc mode characterized by distributed multi-hop networking [Vehicle to Vehicle (V2V)], Infrastructure mode characterized by a centralized mobile single hop network [Vehicle to Infrastructure (V2I)]. The IEEE is involved in standards development related to the physical, medium access and security issues as well as in defining higher layer services and interfaces for intelligent transport. By the end of 2006, the IEEE P1609 standards for Wireless Access in Vehicular Environments (WAVE) had specified the application layer and message formats for operation in the 5.9 GHz DSRC communications. Specifically [18]:

- IEEE 802.11p is based on the IEEE 802.11a standard and specifies Medium Access Control (MAC) and Physical Layer (PHY) specifications
- IEEE 1609.0 defines services for multi-channel DSRC/WAVE devices to communicate in a vehicular environment
- IEEE 1609.1 specifies methods for system resource management and handling of multiple data streams
- IEEE 1609.2 addresses WAVE security
- IEEE 1609.3 defines networking protocols and services
- IEEE 1609.4 specifies channel management and operation

Focusing on the Physical and MAC layer, 802.11p will have to operate in medium ranges, very high mobility and rapidly changing channel conditions. To cope with the new requirements, 802.11p introduces two changes in the PHY layer as defined by 802.11a . While 802.11a specifies the 5.170-5.230 GHz and 5.735-5.835 GHz bands, 802.11p operates on a higher frequency (5.850-5.925 GHz), free of interference from other devices. Additionally, the channel width is halved to 10 Mhz compared to 20 Mhz for 802.11a. It is stated that "this has a number of cascading side effects, some of which aid in compensating for vehicular wireless channels" [12].

Multiplexing techniques are used in most means of telecommunication to allow multiple signals to be combined into a single one and enable sharing of the transmission medium. There are several types of multiplexing including space-division multiplexing (SDM), frequency-division multiplexing (FDM), time-division multiplexing (TDM) and code division multiplexing (CDM).

Like its predecessor, 802.11p uses Orthogonal Frequency-Division Multiplexing (OFDM) which is a FDM scheme for encoding data on multiple carrier frequencies. In this scheme, the carrier signals are orthogonal to each other. This means that an ideal receiver can easily and completely reject unwanted signals. OFDM compensates for both time and frequency-selective fading and performs well with the dispersive linear channels found in mobile environments [12]. In 802.11p optional, enhanced performance specifications have been provided for both adjacent and non-adjacent channel rejection [1].

There are several other candidates for Vehicular Networking that can be used individually or are envisioned to complement each other depending on the application:

- **Cellular Networks**

  Cellular systems have been evolving rapidly to support the ever increasing demands of mobile networking. 2G systems support data communications at the maximum rate of 9.6kbps. Technologies such as GPRS and EDGE provide higher rate communications. Now 3G systems support much higher data rate and 4G systems will soon be deployed based on all-IP network infrastructure.

- **WiMAX**

  802.16e or WiMAX (Worldwide Interoperability for Microwave Access) aims at enabling the delivery of last mile wireless broadband access as an alternative to cable and xDSL, thus providing wireless data over long distances. This will fill the gap between 3G and WLAN standards, providing the data rate, mobility and coverage required to deliver the Internet access to mobile clients.

- **Bluetooth**

  New versions of the bluetooth standard, popular with mobile devices have been proposed for use in VANETs [7] as a good trade-off between energy requirements, communication range and flexibility.

- **CALM**

  One of the technical committees in the ISO group (ISO/TC 204 Intelligent transport systems) is tasked with "standardization of information, communication and control systems in the field of urban and rural surface transportation" and is responsible for the overall system aspects and infrastructure aspects of ITS [15]. It has produced a framework and set of standards known as Communication Architecture for Land Mobile (CALM). It was designed to support the full spectrum of ITS applications, in a flexible manner. It abstracts the communication protocols from the applications, based on two basic premises:

  - Different countries use different choices and frequencies for ITS media.
  - Different ITS applications have different requirements.

  Therefore, many different technologies are supported, including:

  - CALM 2G/3G mobile networks to support long distance communication
  - CALM IR and MMWAVE operating at 60GHz to support short and medium-range directed communication
  - CALM M5 operating in the frequency range of 5–6 GHz is used for short and medium-range omni-directional communication (derived from DSRC/WAVE)

  Other media such as Bluetooth and WiMAX (IEEE 802.16e) are also expected to be integrated in future.

1.5 Security

1.5.1 Overview

VANETs are susceptible to various types of attacks. These differ according to the situation, attacker's intent, scope and the amount of damage. Attacks on wireless networks can be broadly classified into two categories based on the adversary's proximity to the network:

- **Outsider attacks**

  The adversary is not a part of the network.

- **Insider attacks**

  The adversary is a member of the network he is attacking. These attacks can have more severe consequences and be harder to detect and counter.

Attacks can be further categorized into three main categories based on the kind of threat they present to the network:

- **Threats to availability**

  To ensure availability, we need mechanisms in place that can detect and mitigate those attacks that can deny authenticated users access to the network such as:

  - Denial of Service Attacks
  - Broadcast Tampering
  - Malware
  - Spamming
  - Black Hole Attacks

- **Threats to authenticity**

  Threats to authenticity include [43]:

  - Masquerading
  - Replay Attacks
  - Global Positioning System (GPS) Spoofing
  - Tunnelling
  - Position Faking
  - Message tampering
  - Message Suppression/Fabrication/alteration
  - Key and/or certificate replication
  - Sybil attack

Protecting a vehicular network against these attacks involves identifying legitimate nodes and preventing attackers from infiltrating the network under a false identity, identifying messages that have been tampered with, fake GPS signals and any sort of misinformation introduced in the network.

- **Threats to confidentiality of messages**

  Owing to the wireless and public nature of a vehicular network, it is particularly vulnerable to techniques such as eavesdropping of messages and location information available through the transmission of broadcast messages. Providing location privacy and anonymity is important to vehicle users. This involves obscuring the user's exact location in space and time and concealing user requests by making them indistinguishable from other users' requests.

1.5.2 Security in Ad hoc networks

Due to their special nature, ad hoc networks present additional security challenges. Many of the problems that have been adequately addressed on traditional networks require a different approach in this new environment and completely new vulnerabilities need to be addressed [26].

- **Wireless links**

  The wireless medium opens up new opportunities for attackers. Physical access to the network is not required for attacks such as eavesdropping and jamming. In addition, the -typically- lower bandwidth and higher latency inherent in wireless networks can be of assistance in disrupting communications.

- **Dynamic topology**

  Nodes in an ad hoc network can move around, join or leave the network independently. It is therefore difficult to distinguish between normal behaviour of the network and situations where nodes have become unavailable due to some anomaly.

- **No separation from surrounding**

  Defining the boundaries of a network and the roles of the nodes in it is not a trivial task. Multiple different nodes may need to co-exist and malicious behaviours can be expected in all directions.

- **Limited resources**

  Restrictions in hardware cost and energy consumption lead to limited options in securing communications and finite battery life provides adversaries with new attack options.

1.6 Jamming

Channel jamming is a type of Denial of Service (DoS) attack aiming to block access to a communication channel by high power transmission on the communication channel or by injection of dummy messages [26]. In DoS attacks, an attacker attempts to prevent legitimate and authorized users from the services offered by the network. Due to the unique nature of ad hoc wireless networks, DoS attack can exploit features that are not present in conventional wired networks.

"Of the three principal tenets of information, relevance, accuracy and timeliness, jamming is primarily intended to address the last. If information is successfully exchanged, there is little that jamming can do to impact directly the relevance and accuracy of that information. Jamming activities however can impact on the timeliness of the information exchange. Jamming can also affect the relevance of information because if it arrives at the intended destination too late to be of use, the information has become irrelevant" [31].

There are multiple points of a network that can be targeted by DoS attacks. On the physical layer, the attacker can employ jamming signals that overpower other transmissions on the wireless medium. This is a simple attack where the attacker will usually start by only monitoring the wireless channels. Once he has determined the frequency at which the target is communicating, it can transmit on the same frequency to cause interference and induce errors [22].

Since the network coverage area (e.g. along a highway) can be well-defined at least locally, jamming is a low-effort exploit opportunity: an attacker can relatively easily without compromising cryptographic mechanisms and with limited transmission power, partition the vehicular network. Identifying the presence of an unintentional disruption is the first step in minimizing the impact. Jamming can be detected at the physical layer of the network. In the simplest forms of attacks, the increased background noise results in a faltered noise-to-signal ratio, which can be measured at the client. From there, there are a couple of techniques that can be used to reconfigure the channel and avoid the attack which will be mentioned in section 1.7. However, it is not always simple to detect an attack and selecting a different channel does not always eliminate the threat.

Jamming attacks can be classified based on the transmitting strategy followed by the jammer:

- **Constant jammer**

  Continually emits a strong radio signal.

- **Random jammer**

  Instead of continuously sending out a radio signal, alternates between sleeping and jamming.

- **Reactive jammer**

  Stays quiet when the channel is idle, but starts transmitting a radio signal as soon as it senses activity on the channel.

- **Deceptive jammer**

  Instead of sending out random bits, constantly injects regular packets to the channel without any gap between subsequent packet transmissions.

1.7 Defences

Jamming occurs on the physical layer and thus, given enough resources all RF systems can be jammed. "Being totally free from the effects of RF jamming in a wireless communication environment is an unrealistic goal" [31].

Nonetheless, different techniques for Anti-Jamming have been developed. These are commonly based on hiding the signals so they are hard to detect and thus jam, alternating between multiple frequencies of the spectrum to prevent narrowband receivers from intercepting the signal or to have redundancy coding of digital signals.

More anti-jamming techniques include:

High layer techniques

- **Channel surfing** is a link layer technique, alternating the communication frequency on demand. It is in some ways similar to frequency hopping which will be explained in the physical layer section [40].

- **Spatial Retreats** is a technique not applicable to platooning applications where nodes try to evacuate from the jammed regions.

- **Multipath routing** and routing around a jammed area can be effective in partially jammed networks with many nodes.

Physical layer techniques

Considering jamming attacks, the physical layer (PHY) will be the first and most important part of the communications stack to consider, followed by the Media Access Control sub-layer (MAC).

The PHY layer consists of the basic networking hardware transmission technologies of the network. It is the layer where radio interfaces (frequencies, signal strength, bandwidth) are established and techniques like modulation, multiplexing and carrier sense are applied. Parameters of this layer will affect how sensitive a wireless link is to physical attacks and should be well understood when considering jamming.

In military terminology there are systems that can be classified as Low Probability of Detection (LPD) or Low Probability of Interception (LPI). In LPD systems the goal is to hide the signal in a way that an unintended receiver has difficulty determining that the signal is even present. There are many potential reasons for doing so. In a military setting it might be desirable to be able to communicate in a particular area without anyone knowing the presence of the nodes. Spread Spectrum (SS) is an example of a LPD technology. If a signal cannot achieve LPD then by definition an unintended receiver can detect the presence of the signal. It is still possible to provide some protection of signals however. They can be made to be difficult to intercept and in such cases the signals are referred to as LPI. Frequency-hopping described later is an example of a LPI technology.

An alternative to performing evasion strategies, where the sensor nodes try to evade the jammer in some sense, is to have the sensors attempt to compete against the jammer. In this case the objective should be for the sensors to improve the reliability of the reception of their packets. Another prospect is based on the fact that vehicles can have several wireless technologies on-board. To thwart DoS attacks, communication can be seamlessly switched between primary and backup channels. This could be achieved by a protocol like CALM (see section 1.4).

- **Spread Spectrum**

  Spread Spectrum communications technology was patented by Nicola Tesla as early as 1903 and later on developed by the U.S. Department of Defence as a way to thwart transmission detection, exploitation, and countermeasures by adversaries. These communication technologies are rapidly moving out of the strictly military domain into commercial applications. One of these is the code division multiple access (CDMA) spread spectrum (SS). Another example uses frequency hopping to achieve frequency diversity. SS communication technology was developed as a communication technique to provide some degree of electronic counter-countermeasures (ECCM) for the communicator (given that jamming is an ECM technique). It represents one of the LPI and Low Probability of Exploitation (LPE) techniques. A traditional single-tone jammer has little effect on the performance of such systems, forcing the jammer to adopt different schemes of attack. At the very least, a jammer must be concerned about a much broader frequency range. One of the advantages of DSSS technologies is the ability to reuse the frequency spectrum. This is true for commercial wireless communications as well. Such communications overlay one another in the frequency domain and allow many users to share the same frequencies. CDMA is facilitated by each user having a different code to spread its waveform.

  - **Frequency hopping spread spectrum (FHSS)**

    FHSS is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels, using a pseudo-random sequence known to both transmitter and receiver.

  - **Direct sequence spread spectrum (DSSS)**

    DSSS is a modulation technique. The transmitted signal takes up the full bandwidth (spectrum) of a device's transmitting frequency.

- **Modulation**

  Modulation is the process of converting a message signal (for example a binary bit stream or an analogue audio signal) and adding its information in another signal that can be physically transmitted (electronic, optical, radio-signal).

- **Orthogonal Frequency Division Multiplexing**

  Orthogonal frequency division multiplexing, or OFDM , is not a SS technology but is sometimes referred to as SS because of its similar resilience against interference. A special implementation of OFDM is used in IEEE 802.11g, and it has been widely implemented in IEEE 802.11a technology as well. OFDM offers high data rates and exceptional resistance to interference and corruption. OFDM is a digital modulation method that splits the signal into multiple narrowband sub-carriers at different frequencies. Due to the interference problems encountered if the single high speed or high bandwidth signal were transmitted, the use of multiple lower speed or lower bandwidth sub-carriers actually results in higher data rates. OFDM can be combined with other forms of space diversity such as antenna arrays and MIMO channels.

- **Polarization**

  The polarization of an antenna is the orientation of the electric field of the radio wave with respect to the Earth's surface and is determined by the physical structure of the antenna and by its orientation.

- **Selectivity**

  Selectivity is a measure of a receiver's ability to respond to the frequency it has been tuned to, rejecting adjacent frequencies or broadcast signals[12].

- **Multiple Input Multiple Output**

  Multiple Input Multiple Output (MIMO) is the use of multiple antennas at both the transmitter and receiver to improve communication performance. It is one of several forms of smart antenna technology.

- **Beamforming**

  Beamforming (or spatial filtering) is a signal processing technique that can be used when multiple antennas are available. It allows directivity to be achieved in transmission or reception of signals without the use of directional antennas. This allows for easy and rapid reconfiguration. This technique works by combining the antennas in a way that the interference created between them dissipates the signal in unwanted directions while amplifying the signal in the desired direction [8]. Directivity is a measure of the power density the antenna radiates in the direction of its strongest emission, compared to the power density radiated by an ideal isotropic radiator radiating the same total power. Directivity is often desirable because emissions are intended to go in a particular direction or at least in a particular plane, with emissions in other directions or planes being wasteful or hurtful.

1.8 Simulation

The simulation of VANETs requires the consideration of two very different aspects of a mobile network [12]:

- **Communications simulation**

  Covered by network simulators that are in wide spread use in the network research community (e.g. NS-2/NS-3, OPNET, OMNET++ etc.)

- **Mobility simulation**

  Covered by different vehicular mobility modelling approaches (traffic, flow, random, behavioural, trace, survey)

Because these two simulation environments were not originally designed to interconnect and are controlled separately, the need to develop communication interfaces between them or workarounds that enable them to be used in conjunction have been an important area for the VANETs research community.

The approaches used can be classified into three categories [12]:

- **Isolated mobility models**

  Mobility scenarios are generated by mobility modelling and then loaded into a network simulator. No interaction is possible between the simulator and the pre-generated scenario. This approach was until recently a favourite since it allowed the use of state of the art mobility modelling and network simulation while there was no requirement for interaction between the two environments.

- **Embedded Mobility models**

  Newly developed network simulators with embedded mobility modelling. This approach provides native collaboration between the two environments. Current solutions in this category provide a compromise between the comprehensive capabilities of established simulation environments and their inability to interface with mobility models.

- **Federated mobility models**

  Active interfacing of established network simulators with mobility models. This approach provides both state of the art mobility modelling and network simulation as well as interaction between the two environments. However, the development of an interface and configuration may not be an easy task. Additionally, it is computationally intensive as both environments need to be run synchronously.

Chapter 2

Objectives and Scope

Seeing as platooning applications rely on continuous communication between the member nodes to provide the intended functionality and safety, it is of paramount importance that disruptions of the connectivity between vehicles can be immediately discovered and addressed. As the typical platooning system would largely operate autonomously in small ranges and disconnected from a wider network (as the internet), attacks that can be launched at close proximity with minimal infrastructure or previous knowledge of the system are especially attractive to potential adversaries. Jamming attacks that target the lower layers of communication have these properties that could make them attractive to attackers.

The objective of this master thesis is to:

- **Understand the threats** that can be presented to VANETs, focusing on the application of vehicle platooning and explore the state of the art in preventing and detecting DoS attacks, focusing on communications jamming.

- **Examine the opportunities** presented by the special characteristics of VANET to mitigate the effects of an attack.

- **Develop a simulation environment** capable of modelling the physical operation of a platoon as well as the networking and communication requirements of such an application.

- Implement attacks and **test defence methods** for ensuring minimum operation and full safety can be preserved in case of an attack.

Chapter 3

Related Research

Security of wireless communications is a vast and complicated field, subject to continuous research. It encompasses many different technologies and applications. As such, there is a huge amount of literature ranging from almost philosophical standpoints down to the definition of small details of very specific scenarios.

As most of the protocols developed for use with VANETs are based on existing and widely used wireless protocols, security on the higher layers of the network stack has largely been addressed. However the physical layer is significantly different in VANETs and needs to be examined as such.

Because of the use of Carrier Sense (CS) for Medium Access Control (MAC) used in these protocols, they are "susceptible to simple and severe jamming problems: an adversary can disregard the medium access control and continually transmit on a wireless channel. In that way, he either prevents users from being able to commence with legitimate MAC operations or introduces packet collisions that force repeated backoffs or even jams transmissions" [41].

Jamming has been extensively studied, owing mostly to its significance in military applications of electronic warfare and stealth (see section 1.7). In commercial use however, techniques used by the military may not be feasible due to the different communication requirements or laws restricting wireless communications etiquette and hardware. Additionally, jamming resistance is not always important in commercial applications as potential attacks do not benefit from blocking signals but rather by intercepting and modifying data packets. In safety critical applications however like the platoon scenario and other ITS applications simply preventing some data from reaching their destination in a timely manner can result in severe consequences for the correct operation of the application and even worse, endangerment of human life.

3.1 Jamming

There has been extensive research in the subject of jamming but not many papers have addressed this issue in applications of VANETs.

In [34], the effects of jamming are examined on 802.11p based Vehicle-to-Vehicle communications. Different jamming patterns are described and their effectiveness is characterized in an anechoic chamber followed by measurements in outdoor scenarios. This work demonstrated that a Radio-Frequency jammer can "severely impact VANET communication and the supported applications". They point out improvements that could be made on the 802.11p protocol to increase resilience to jamming and briefly examine a software driven method for controlling radio sensitivity (Ambient Noise Immunity).

In [10], the authors address the effects that a wireless jammer can have on the stability and performance of vehicles in a platoon, using a specific control algorithm [21]. Using the UIUC VANET simulator [11] and the platooning controller proposed in [21], they demonstrated that successful jamming can cause vehicle collisions and proposed a simple solution of an estimator to avoid collisions in scenarios of constant velocity.

Pelechrinis et al. has published several papers related to jamming and focusing on 802.11 networks.

In [28], the effectiveness of Frequency Hoping is analysed and the problem of multiple jammers and energy spill between adjacent channels is examined. It is demonstrated that hoping can be "largely inadequate in coping with jamming attacks in 802.11 networks". In [29], two physical layer functions are assessed in their ability to mitigate jamming, rate adaptation and power control. The authors find that using prominent "rate adaptation algorithms can significantly degrade network performance" and that "appropriate tuning of the carrier sensing threshold allows a transmitter to send packets even when being jammed" and can enable the receiver to capture the original signal. Based on these findings, they build "ARES, an Anti-jamming Reinforcement System, which tunes the parameters of rate adaptation and power control to improve the performance in the presence of jammers". In conclusion, they evaluate ARES in three largely different wireless test-beds to observe an improvement in network throughput across all scenarios. In [27], a comprehensive overview is presented of techniques for jamming, jamming detection and jamming prevention. The writers recognize that every proposed anti-jamming solution "exhibits limitations and there are more things that need to be done in order for the problem to be solved satisfactorily".

3.2 Platooning

Lately there is renewed interest in platooning with major research projects taking place. However problems with jamming have not received the attention they deserve. An effort has been made to present literature that is relevant to platooning, connection quality and requirements.

As far back as 1997, in [36] the authors discuss the impact of multipath fading and interference to vehicle-to-vehicle communications. They compare the reliability of radio links based on Time Division Multiple Access (TDMA), Direct-Sequence Code Division Multiple Access (DS-CDMA) and Frequency-Hopping with TDMA. Their analysis showed a large probability of packet loss due to ground-reflected waves. They investigated using vertical polarization to mitigate the effect and suggested that antenna diversity could also be used to increase performance. They also found the system to be sensitive to co-channel interference and suggested that performance could be largely improved if adjacent lanes used different frequencies.

In [16], the authors examine vehicle-to-vehicle communication based on IEEE 802.11p in a Non-Line-Of-Site (NLOS) environment. With varying obstacles and use cases, they observed packet error rate and consecutive packet loss. They show that a platooning application is not adequately supported in all of their measurement scenarios. In conclusion they provide some suggestions into improving the channel reliability, namely using antenna diversity or Multiple-Input and Multiple-Output (MIMO) radio.

3.3 String stability

This is another area of research that has looked into car following models, communication requirements and the consequences of communication delays is string stability of vehicular systems. String stability is defined [30], as the "uniform boundedness of all the states of the interconnected system for all time if the initial states of the interconnected system are uniformly bounded" [35]. Simply put, in the case of platooning, it means that spacing errors will not amplify along the platoon.

"String stability properties of AHS longitudinal vehicle controllers" [4] considers the platoon as a mass-spring-damper system and compares the string stability properties of a variety of longitudinal vehicle controllers.

In [37], decentralized spacing control of a platoon in the face of lossy data-links is investigated. It is shown that by estimating lead vehicle information in the event of communication drop-outs, weak string stability can be guaranteed. The authors point out that the worst-case scenario is when alternate vehicles along the platoon experience drop-outs simultaneously and that moderately reliable links are sufficient for spacing control as long as they can recover quickly in the event of a failure.

In [25], a Cooperative Adaptive Cruise Control system is studied, regarding string stability under communication constraints. The authors provide "conditions on the uncertain sampling intervals and delays under which string stability can still be guaranteed".

In [39], the effect of information delay on string stability is analysed and simulated. They demonstrate that the effect of information delay on control gains must be considered in controller design. Finally, by comparing three different information frameworks they stress that the choice of proper framework is very important for string stability.

In [42] the authors "conduct a feasibility study of delay-critical safety applications over vehicular ad hoc networks based on the emerging DSRC standard". Through simulations, error performance of the physical and MAC layers of DSRC links was measured under various mobility scenarios. Following that, support for vehicle collision avoidance applications was tested in order to gauge the level of support the DSRC standard provides for this type of applications. Their verdict was that latency performance was satisfactory but throughput needs to be improved especially in cases of high mobility, possibly by exploiting the multi-channel capability of DSRC.

In [17], the authors study IEEE 802.11p in different vehicle-to-vehicle scenarios. A performance analysis under different propagation conditions and modulation schemes is carried out, looking at bit error rate (BER) and signal to noise ratio (SNR). Inter-Symbol and Inter-Carrier interference is shown to be efficiently mitigated but frequency-selective fading is a problem. They propose using a different value of guard interval to improve BER performance.

In [38], vehicle-to-vehicle communication based on IEEE 802.11p is considered, regarding interferences and packet collisions that can lead to the failure of reception of safety-critical information. The authors propose a new protocol along with a distributed transmit power control method aimed at providing fairness, prioritization and congestion control by modifying transmission power.

In [5], a dynamic equalization scheme is proposed, on top of the existing DSRC technology. This is shown to improve reliability in highly dynamic time-varying vehicle-to-vehicle channels. Additionally, the authors investigate the dependence of wireless communication performance (in terms of PER and throughput) on various design parameters like packet length payload size and data rate.

Part II

The project

Chapter 4

Timeline

The steps that were performed and led to the completion of this thesis are as follows:

- Determined the areas of interest: ITS, Smart Grid, Battery Electric Vehicles.

  Surveyed the state of the art in said areas and investigated opportunities for energy efficient transportation systems.

- Focused on communication requirements in vehicular environments (V2V, V2I, V2G) and considered several subjects with the most important being:

  - Vehicle platooning
  - Bottlenecks in the deployment of EVs (range, support infrastructure)
  - Extension of the SG and integration with EVs (EVs as power storage and demand-response management tool, load-balancing)

- Based on the initial research, focus was shifted towards communication issues in a specific ITS scenario utilizing mostly V2V communications in VANETs (Vehicle Platooning).

  Wrote an essay titled "Denial of Service attacks mitigation in vehicle platooning applications" outlining the general background, objectives and approach for the master's thesis.

- General survey on

  - MANET and VANET communications
  - Wireless security

- Performed survey and testing of suitable mobility and network simulators NS-3, NCTuns, EstiNet, iTetris (SUMO & NS-3), VEINS (SUMO & OMNeT++) and more.

  Got familiar with VEINS and built a simple network, suitable for basic testing.

- Wrote the first section of the thesis (Background and related research).
- Determined the objectives and scope of the thesis.
- Developed a simulation environment based on MATLAB and Simulink including:
  - Physical vehicle simulation
  - Network simulation
  - Attack scenarios
  - Defence mechanisms
  - Post Processing and Display suite
- Validated model:
  - Single vehicle operation
  - Multiple vehicle (platoon) operation
  - Jamming operation
- Implemented and tested attack scenarios:
  - Stationary jammer
  - Mobile jammer
- Implemented and tested defences
  - Beamforming
  - Double anchoring
  - GPS verification
  - On-board sensors verification
- Wrote conclusions and future work.
- Finalized thesis.

Chapter 5

Model Construction

Given the problem at hand, and following the literature review, it was decided that the best way to study the issue of platooning and defences to jamming, would be through simulation. An environment was therefore constructed that can simulate the platoon, inter-vehicular communications and jamming and allows the implementation of different defences and assessment of their effectiveness. This was developed from scratch using Simulink and MATLAB. Important sub-systems of the environment are described below.

5.1 Platoon

This is the workspace integrating the individual components including all the vehicles and the network. For the purposes of the present project four vehicles were included, a leader and three followers. This number was selected to allow the examination of dynamic correlations between the vehicles: with four vehicles, there can be a lead vehicle, two intermediate vehicles (if the interaction between intermediate vehicles needs to be examined), and one end vehicle. It is however possible to extend the model to include more vehicles with ease.

Figure 5.1 shows the platoon model as configured in Simulink. There are 5 important parts: the vehicles, the network, P3D outputs (Post-Processing and Display), the jammer and the profile. The vehicles are noted on the left side in red. They are connected to the network noted in blue (see section 5.3) and P3D noted in green (see section 5.4). They have inputs from the network, the jammer (interferer) noted in brown (see section 7) and the global configuration module (profile).

Global configuration

As functions were being added to the vehicles, there was a need to easily control the profile of simulations from a single point. Therefore, a profile module was added to the platoon model (see figure 5.2). It contains separate global controls for the vehicles' R/T (Receive/Transmit) and ECU (Engine Control Unit) modules in the form of binary octets, converted from integers (255 means all systems are enabled, 0 means all systems are

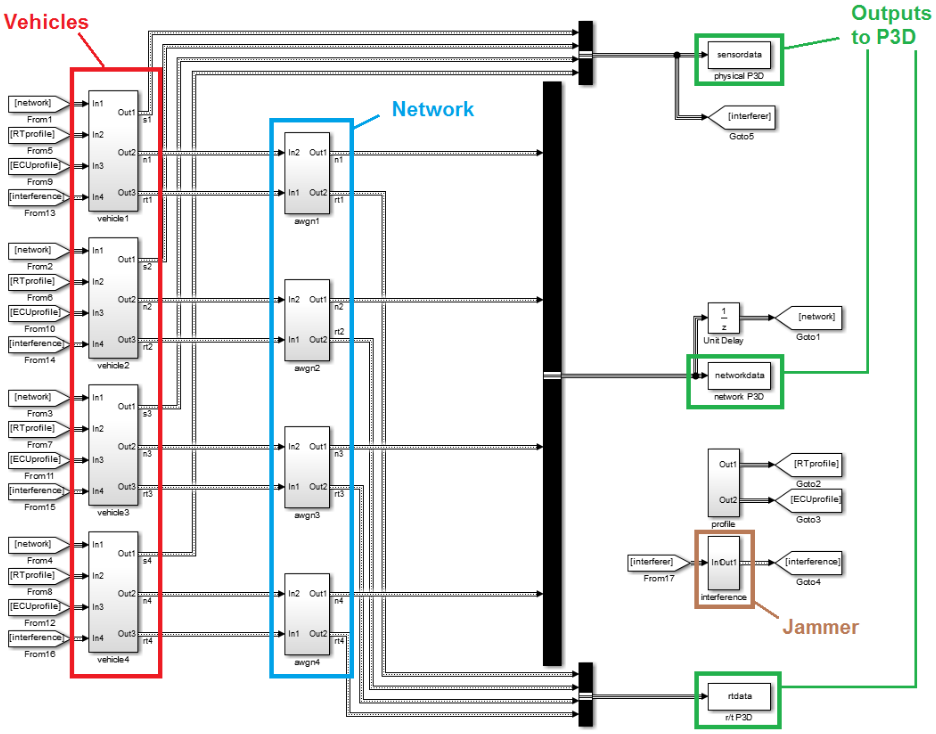


Figure 5.1: Platoon model

disabled). The global controls can be deactivated and each vehicle is then setup through separate controls in its own profile module located in the vehicle subsystem (see figure 5.4).

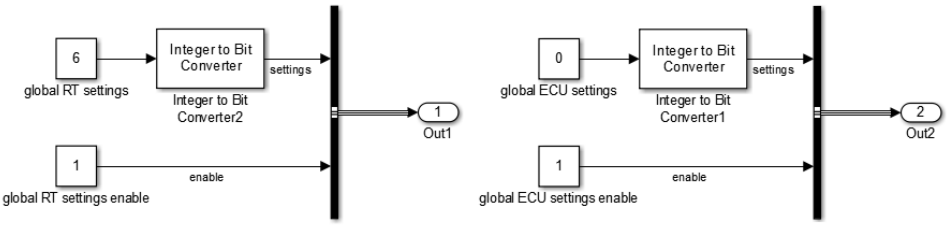


Figure 5.2: Global profile

5.2 Vehicle

The Vehicle sub-system (see figure 5.3) simulates the operation of a single vehicle within the platoon. It uses data from its sensors and the network to simulate how the vehicle responds, returning data to the network and P3D. There are two important modules in the vehicle marked in red: the Engine Control Unit (ECU) and the Receive/Transmit module (R/T). In addition, there are several auxiliary modules marked in orange: the profile, the sensors, the ECU buffer and the R/T buffer. Finally there are several inputs from the platoon workspace and outputs to the platoon and P3D.

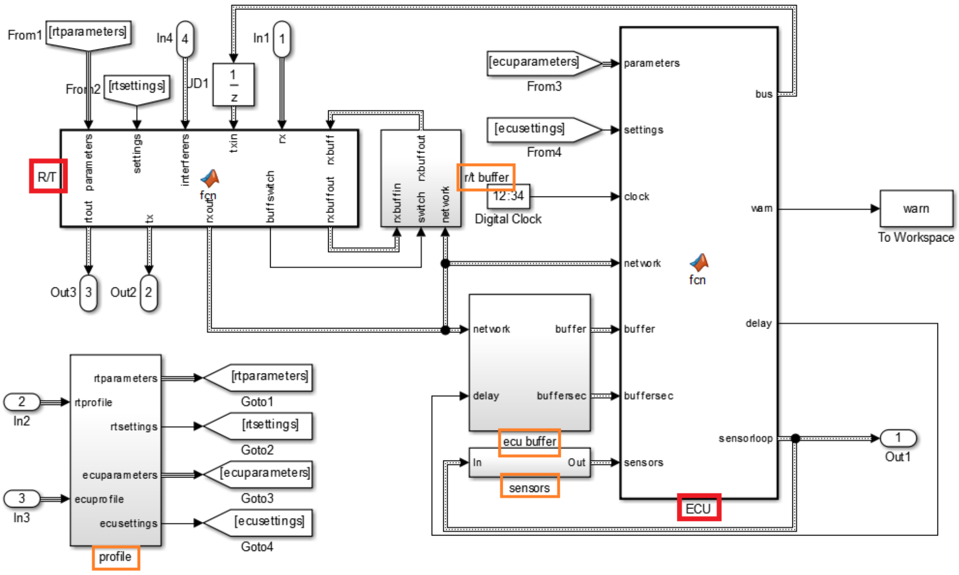


Figure 5.3: Vehicle model

ECU

The Engine Control Unit processes the inputs to determine the state of the vehicle and outputs data to the network and the platoon simulator via the R/T module. Since we do not have actual sensors, the ECU also has the task of determining the state of the vehicle in the next step and translating it to readings that are then fed to the sensors.

The key parameter here is the acceleration of the vehicle. This can be defined by the user for the lead vehicle and determined by the ECU for the follower vehicles, based on readings from the network and the vehicle sensors. Acceleration is then processed to determine the speed, position and heading of the vehicle as well as other parameters regarding its relation to other vehicles and the network state.

The full list of ECU inputs, outputs and parameters is shown in tables 5.1 and 5.2. Many functions were added to the ECU through the course of development that are referred to later in the text (see section 8) as they are related to defence mechanisms implemented and are not strictly relevant to the basic functions of the vehicle.

Sensors

This module simulates the sensors of a vehicle, monitoring its acceleration, speed, coordinates and heading. They receive their values from the ECU and feed them back to the ECU on the next time step.

ECU Buffer

The ECU buffer allows a vehicle to correctly track the path of the leading vehicle. It delays the response to a change of attitude for the appropriate time, related to the distance between the vehicles and their speed.

	Role	Defined by	Used by	Comments
parameters	Input	User	ECU	Initial conditions and constants of the vehicle
settings	Input	Profile	ECU	Profile settings
network	Input	Network	ECU	Data received from the network
buffer	Input	Network+ECU	ECU	Buffered data received from the network
sensors	Input	ECU	ECU	Data received from the vehicle sensors
bus	Output	ECU	Network	Data sent to the network
delay	Output	ECU	Buffer	Buffer delay control
sensorloop	Output	ECU	ECU	Data sent to the vehicle sensors

Table 5.1: ECU Input/Output list

Parameter	Description
Acceleration (x and y axis)	Defined by the user or calculated by the ECU
Speed (x and y axis)	Calculated by the ECU
Heading	Calculated by the ECU
Coordinates(x and y axis)	Calculated by the ECU
Platoon length	Statically defined by the user
Platoon position	Statically defined by the user

Table 5.2: ECU parameters

R/T

The Receive/Transmit module handles the connection of the ECU to the network. This includes calculation of several parameters regarding the communication beam, the network state and the communicating parties.

The full list of R/T inputs, outputs and parameters is shown in tables 5.3 and 5.4. Ports txin-tx and rx-rxout are the main inputs and outputs, that contain the data sent to and received from the network. Ports tx and rx are directly connected to the network, txin and rxout are directly connected to the ECU. The R/T module processes the data and connects the ECU to the network. Ports rxbuff and rxbuffout are inputs and outputs to the R/T buffer.

R/T Buffer

The R/T buffer is used for error correction. It stores the last known correct values received from the network. It is updated by the R/T module and used in case of confirmed network errors to maintain the correct vehicle course and beam settings.

	Role	Defined by	Used by	Comments
parameters	Input	Profile	ECU	Initial conditions and constants of the vehicle
settings	Input	Profile	ECU	Profile settings
interferers	Input	Interferer	R/T, ECU	Interferers profile
txin	Input	ECU	Network	Raw data to be transmitted to the network
rx	Input	Network	R/T	Raw data received from the network
rxbuff	Input	R/T buffer	R/T	Buffered data from network
rtout	Output	R/T	Vehicle R/T	P3D data
tx	Output	R/T	Network	Data transmitted to the network
rxout	Output	R/T	ECU	Processed data received from the network
buffswitch	Output	R/T	R/T buffer	Buffer switch
rxbuffout	Output	R/T	R/T buffer	Network data to be buffered

Table 5.3: R/T module Input/Output list

Parameter	Description
Interference	Calculated based on network input
2nd party bearing	Calculated based network input
Beam direction	Calculated based on 2nd party bearing
Beam width	Calculated based on 2nd party bearing and network

Table 5.4: R/T parameters

Profile

This module (see figure 5.4) provides the static parameters defined by the user and is also used for the initialization of the vehicle in the start of each simulation. It can be controlled separately for each vehicle or through the global configuration module described in section 5.1.

I/O ports

These include all data transmitted through the network, either by other vehicles of the platoon or vehicles and stations unrelated to the platoon (possible interference sources). In addition there are output ports to the P3D module.

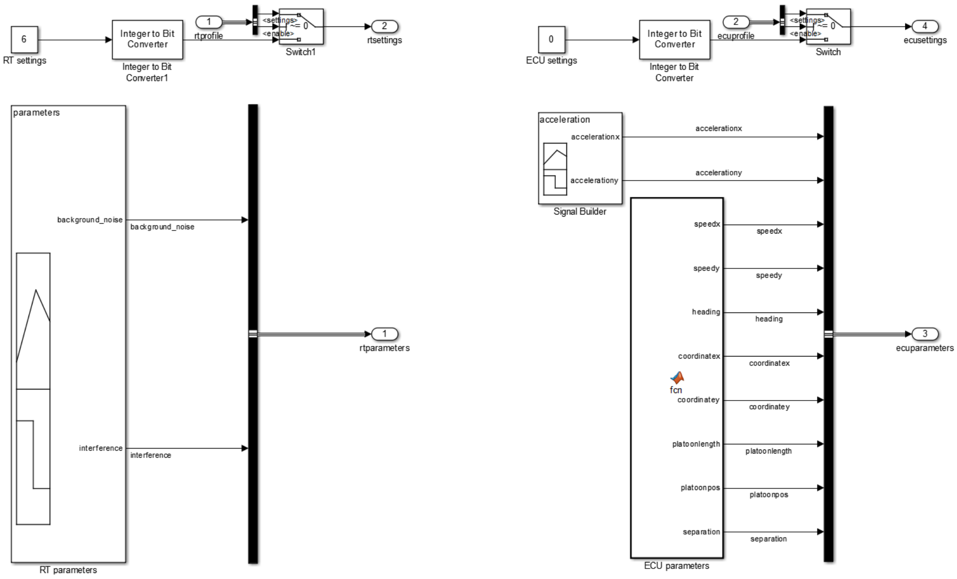


Figure 5.4: Vehicle profile

5.3 Network

To accurately model the behaviour of a real-life network, communication complexity was introduced in three levels, each adding to the previous one.

5.3.1 Level 0

Initially, the vehicles were hard-wired to each other by means of a bus coming from the ECU of each vehicle and multiplexed with the rest into a superbus. This superbus was then used as the input to each vehicle from the network. This configuration was used initially for validation of the simulation of vehicle operation, movement and basic communication.

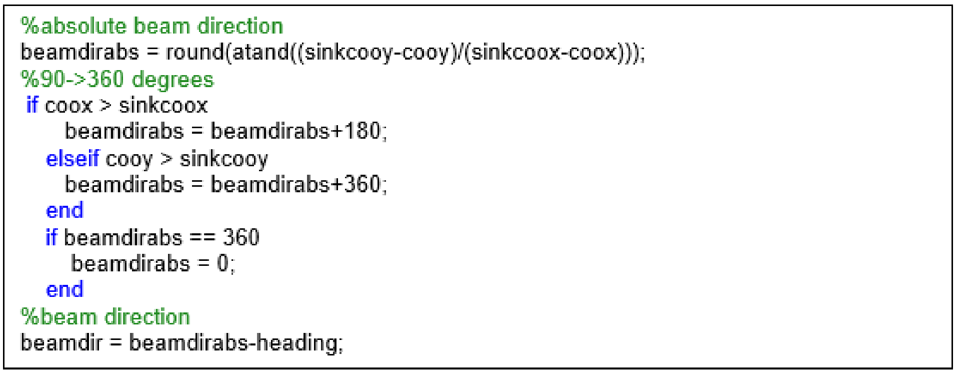
5.3.2 Level 1

In the first level, the basic parameters of the communication system were introduced to allow the simulation of beamforming control and interference. The vehicles were still directly connected with buses.

The R/T module (see figure 5.3) in each vehicle communicates directly with the vehicle's ECU (rxout,txin) and the network (rx,tx). This module handles the transmission and reception of data to and from the network. It also calculates the desired beam angle and direction based on the vehicle heading and the distance between the communicating vehicles (see section 8.1 and figures 8.2, 8.3a and 8.3b).

The R/T module in this level provides predetermined values for wireless signal quality metrics and the network state as no interference functions have been implemented yet. Along with data received from the ECU a number of scenarios can be simulated (not an exact representation but an approximation of the performance).

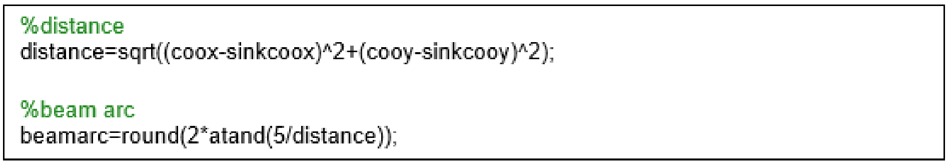
In this level the rudimentary functions for calculating beam arc and direction were formed. Beam direction is calculated based on the relative position of the communicating vehicles and heading of the transmitting vehicle (see figure 5.5).



```
%absolute beam direction
beamdirabs = round(atand((sinkcooy-cooy)/(sinkcoox-coox)));
%90->360 degrees
 if coox > sinkcoox
     beamdirabs = beamdirabs+180;
   elseif cooy > sinkcooy
     beamdirabs = beamdirabs+360;
   end
   if beamdirabs == 360
      beamdirabs = 0;
   end
%beam direction
beamdir = beamdirabs-heading;
```

Figure 5.5: Beam direction code

Beam width is calculated based on the distance between the communicating vehicles and the preset width of the beam at the position of the 2nd party, in this case 5m (see figure 5.6).



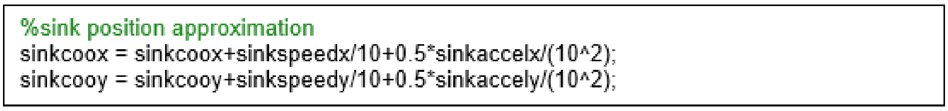
```
%distance
distance=sqrt((coox-sinkcoox)^2+(cooy-sinkcooy)^2);

%beam arc
beamarc=round(2*atand(5/distance));
```

Figure 5.6: Beam width code

Initially, the distance calculation from the 2nd party differed to the real distance measured on P3D. This was because of the delay of communication between the two vehicles. The base delay for this system is 1 step (0.1 seconds). This can affect measurements significantly, depending on the vehicle velocity.

The distance measured by each vehicle differs depending on the position of the 2nd party of the communication in the platoon (preceding or following). This is due to the fact that a vehicle reads its own position instantly and the position of the 2nd party with a one-step delay. Example: Vehicle 1 communicating with vehicle 2 reads its own position instantly but the position of vehicle 2 with a one-step delay (0.1 s). Vehicle 2 communicating with vehicle 1 has the same delay. Because vehicle 1 is moving away from vehicle 2 the distance measured by vehicle 1 is larger than the real distance and accordingly the distance measured by vehicle 2 is smaller than the real distance. This creates a discrepancy in the measured distance dependent on the speed of the platoon (xd=u*td where td=0.2s(2 steps)).

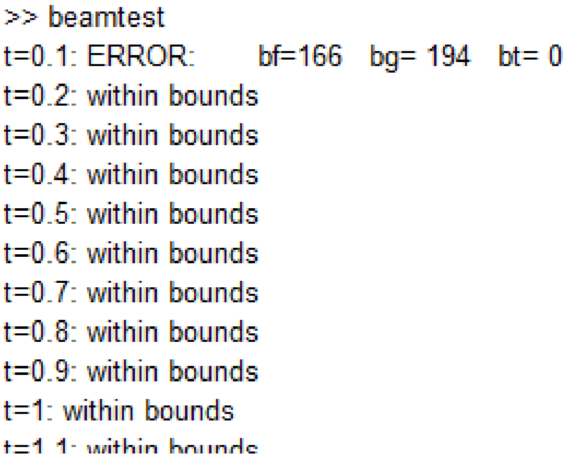
However, based on the last known location, velocity and acceleration of the 2nd party, the correct location can be calculated almost precisely (see figure 5.7).



```
%sink position approximation
sinkcoox = sinkcoox+sinkspeedx/10+0.5*sinkaccelx/(10^2);
sinkcooy = sinkcooy+sinkspeedy/10+0.5*sinkaccely/(10^2);
```

Figure 5.7: Sink position approximation code

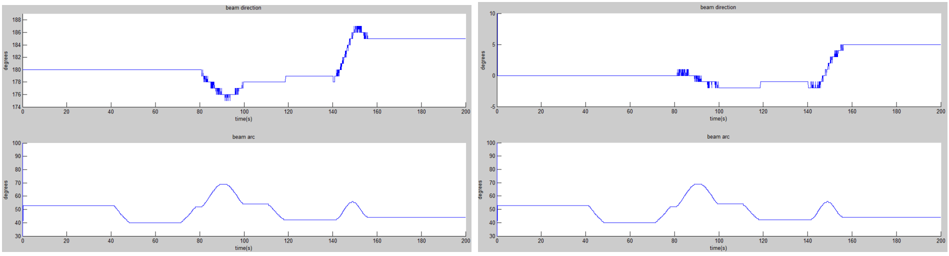
Based on this data (beam arc, beam direction) and the actual positions of the vehicles it is now possible to determine if two vehicles can successfully communicate. In level 1, this was performed in a post-processing script called beamtest or range finding (see figure 5.8).



```
>> beamtest
t=0.1: ERROR:     bf=166   bg= 194   bt= 0
t=0.2: within bounds
t=0.3: within bounds
t=0.4: within bounds
t=0.5: within bounds
t=0.6: within bounds
t=0.7: within bounds
t=0.8: within bounds
t=0.9: within bounds
t=1: within bounds
t=1.1: within bounds
```

Figure 5.8: Beamtest (range finding) script output

The two new variables that are calculated by the R/T module (beam direction and beam arc) were validated using the more complicated profiles (MVP6 –MVP7, see section 6.2). The results for communication between the first two vehicles in MVP6 are shown in table 5.9.



(a) Vehicle 2 to vehicle 1

(b) Vehicle 1 to vehicle 2

Figure 5.9: Beam direction and width validation

5.3.3 Level 2

In this level, a further module (see figure 5.10) was inset between each sender and receiver, to simulate the effects of the wireless medium. Three different approaches were tested. It is placed on the output of each vehicle in the platoon. It has a single input and a single output. Data is received from the transmit bus (tx) of the vehicle's communication module. The effects of the channel are calculated and the signal altered accordingly and then output to an identical bus, to be fed to the input (rx) of a vehicle's communication module. This was later improved to integrate information from the R/T module controlling the amount of interference introduced (see chapter 7 and figure 5.1).

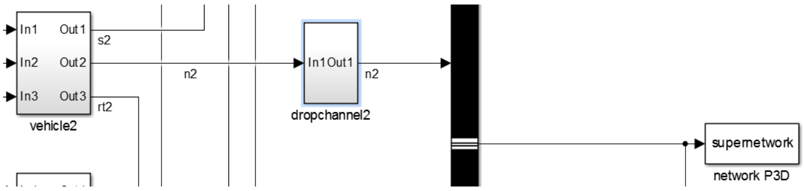


Figure 5.10: Communication channel (level 1)

Other additions include range finding integrated in the R/T module and improved by taking into consideration the possible interference.

With the introduction of interference, it was necessary to perform additional processing of the received data, to ensure that it is logical and therefore possibly correct. Without this additional processing, even with the slightest interference, the platoon would break up. This was performed in the R/T module. A buffer was introduced, to save the latest "correct" data received and use it as input in case corrupt data were received. In future levels (not implemented), this would be performed on a parameter-level, in contrast to frame-level buffering performed in this level.

The communication systems toolbox in MATLAB provides customizable channels to simulate noise and errors in the transmission. For this purpose, two new functions were introduced to convert the bus signals to binary arrays, suitable for transmission and then back to a bus signal on the other end. The placement of the communication channel in the platoon model is shown in figure 5.10.

Packet-Drop Channel

In the packet-drop channel, it is assumed that certain packets are lost in transmission or are received containing irrecoverable errors and are thus discarded. In such a case, a vehicle will only have the last correct data received available. Figure 5.11 shows the packet drop channel and figure 5.15 shows the headway attained by the vehicles under interference causing a 10% packet drop probability and the attitude of the beam throughout the simulation.

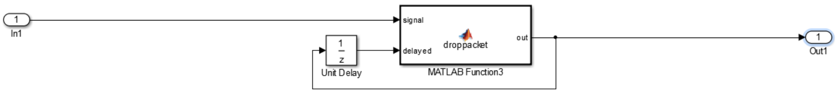


Figure 5.11: Packet Drop channel

Binary Symmetric Channel

In a binary symmetric channel, there is a small possibility that transmitted bits are flipped, resulting in incorrect data. Figure 5.12 shows the packet drop channel and figure 5.14 shows the headway attained by the vehicles under interference causing a 0.00001 bit error probability and the attitude of the beam throughout the simulation.

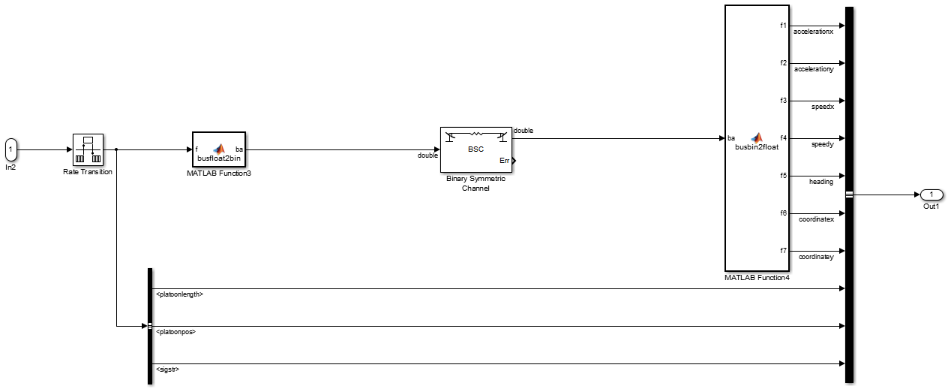


Figure 5.12: Binary Symmetric channel

Additive White Gaussian Noise Channel

The additive white Gaussian noise channel adds uniform, wideband noise to the signal in a normal time distribution. Noise level is defined as Signal-to-Noise Ratio. Figure 5.13 shows the packet drop channel and figure 5.16 shows the headway attained by the vehicles under interference causing a SnR of 9dB and the attitude of the beam throughout the simulation.

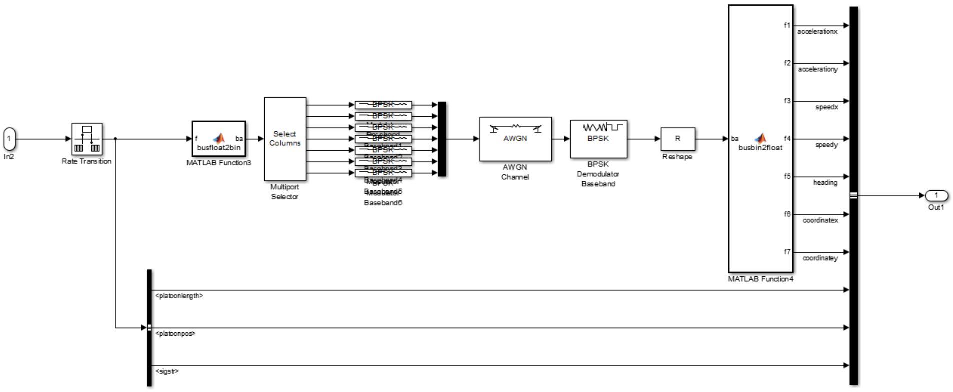
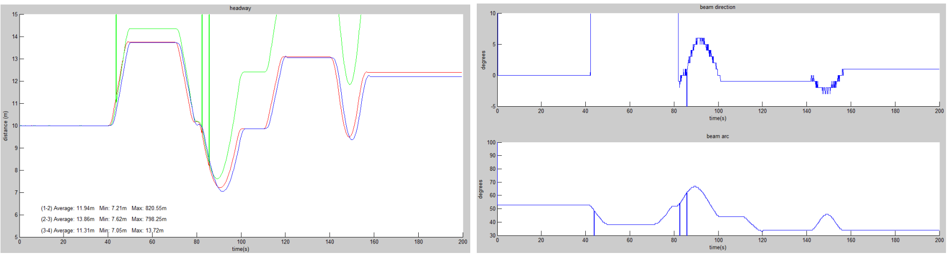


Figure 5.13: Additive White Gaussian Noise channel

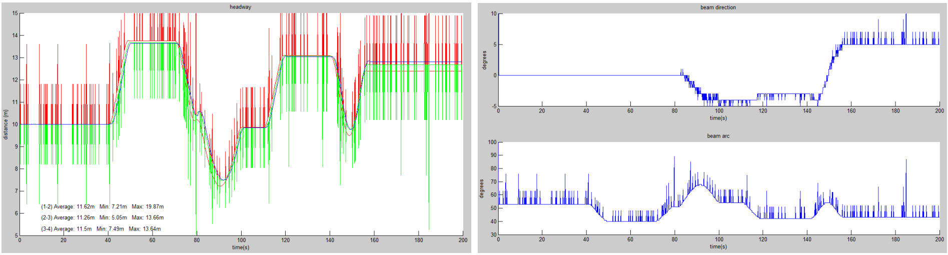
In the end the AWGN channel was selected for this project as it provided the best approximation of interference. In order for the AWGN module to be used, it is necessary for the binary signal to undergo modulation. For this purpose, a Binary Phase Shift Key (BPSK) modulation scheme was used.



(a) Vehicles headway

(b) Beam attitude

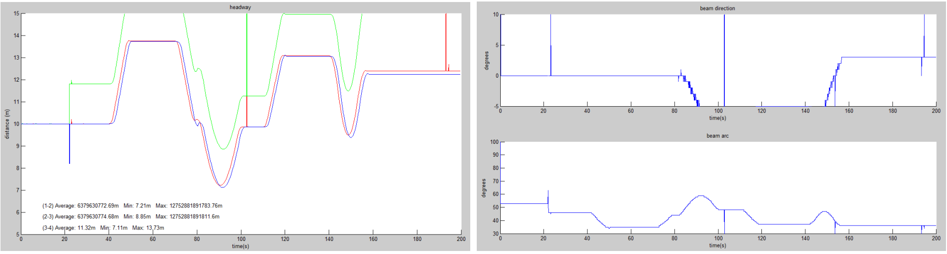
Figure 5.14: Headway and beam with BS channel (0.00001 bit error probability)



(a) Vehicles headway

(b) Beam attitude

Figure 5.15: Headway and beam with PD channel (10% drop probability)



(a) Vehicles headway

(b) Beam attitude

Figure 5.16: Headway and beam with AWGN channel (9dB SnR)

5.4 Platoon Post Processing and Display (P3D)

P3D stands for Platoon Post-Processing and Display. It was constructed specifically for this environment as a suite of MATLAB scripts used to post process the results of the whole platoon simulation and display the routes of individual vehicles, the spatial relations between the vehicles and more. It takes data from the vehicles and network and plots appropriate diagrams. Figure 5.17 shows the flowchart of P3D operation.

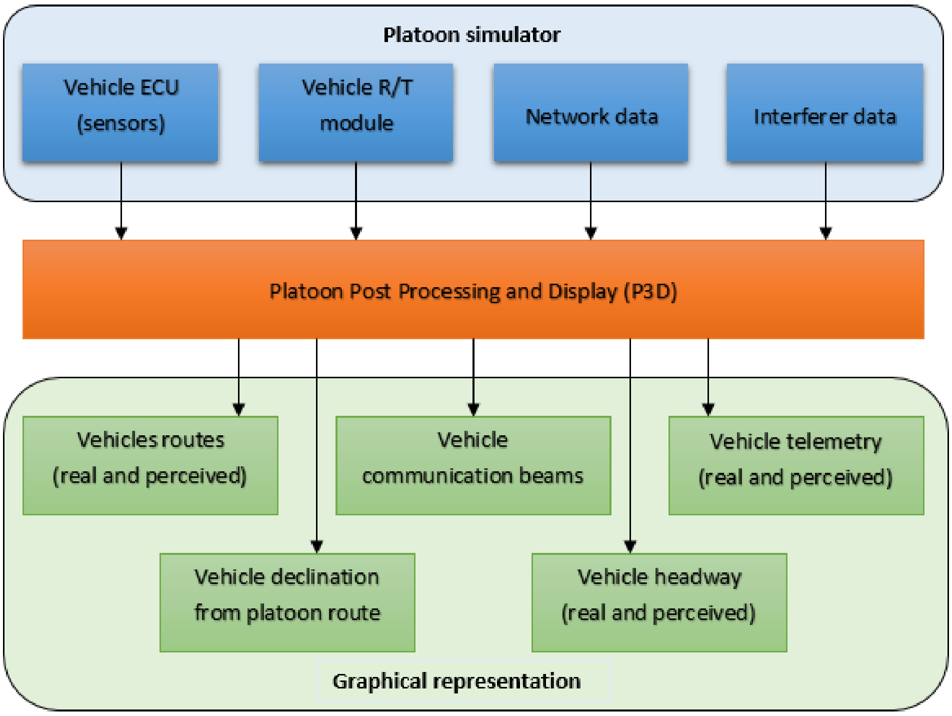

Platoon simulator
Vehicle ECU (sensors)
Vehicle R/T module
Network data
Interferer data
Platoon Post Processing and Display (P3D)
Vehicles routes (real and perceived)
Vehicle communication beams
Vehicle telemetry (real and perceived)
Vehicle declination from platoon route
Vehicle headway (real and perceived)
Graphical representation

Figure 5.17: P3D flowchart

This graphical presentation was necessary to visualize the simulation and easily track important events in each runs' time-line. Each scenario may have different data of interest and P3D can be easily reconfigured accordingly to plot the needed diagrams. The flowchart of P3D in figure shows the basic sources of data and common graphical outputs.

5.4.1 Graphical output

Initially, only spatial data was plotted, to aid in the configuration and validation of the vehicle routes. More functions were added gradually, to include plotting of acceleration, speed, heading, beamforming data as well as to indicate periods of loss of communication. When interference was added, the need was presented to look at actual data coming from the vehicles' sensors as well as possibly erroneous data, transmitted by the vehicles' R/T modules to the network. This data was sent to the MATLAB workspace separately and P3D was separated into two scripts to process them: P3Dnet and P3Dsensor.

As the scripts became more and more complicated, they were separated into smaller parts handling analysis of each vehicle's data separately. Another script was used to calculate and cancel out errors owing to the design of the simulator. With the introduction of defence mechanisms, more scripts were used to handle the warnings generated when a mechanism was triggered. By the end of development, P3D was split up into 14 scripts. Five of those handled real data gathered from sensors. Five handled perceived data gathered from the network. Four handled warnings and one was used to cancel out simulator errors.

The P3D suite was used extensively with the simulator and the graphical presentations generated are an integral part to understanding the results of each run. All the graphs presented in this project are directly generated through P3D.

5.4.2 Animation

In addition to static plots of data gathered during the simulation, an animation function was desirable to provide a clearer understanding of the performance of the platoon under the different scenarios. An animation script was constructed that generates animations that combine data about the movement of the vehicles, the interference and the beamforming of senders and receivers. Figure 5.18 shows a screen-shot from an early version of the animation script. The four vehicles are shown in the process of turning and the communication beam of vehicle 2 is shown, tracking the lead vehicle.

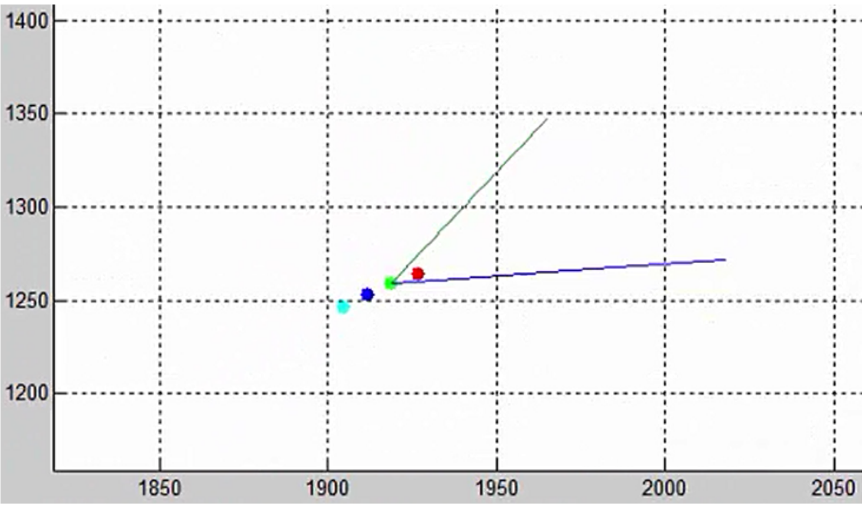


Figure 5.18: Animation script screen-shot

Further screen-shots of the animations are examined in later chapters with the vehicles presented as coloured points, the interferer as a black square and the communication beams as cones stemming from the vehicles.

Chapter 6

Model Validation

As with model construction, the model validation employed a staggered approach whereby successive scenarios of increasing complexity were used to evaluate the performance of the individual routines and validate the operation of the complete model.

6.1 Single Vehicle Operation

Initially the platoon was tested in single vehicle mode to validate the operation of the vehicle sub-routine, its communication with the other modules and to optimize the ergonomics and operation of the P3D script. The correctness of the physical calculations performed by the P3D script was verified against hand calculations based on known simulation parameters.

The validation also served as an opportunity to experiment with, and define the acceleration/movement profiles that would be used in the subsequent full platoon tests. The profiles here are experimental profiles used during the validation of the model and are designated by the format SVP# (Single-vehicle Validation Profile #).

6.1.1 Linear profiles

At first, three linear profiles were ran. These were used to validate the unit conversion (m/s to km/h) and total distance travelled calculations contained in the vehicle and platoon and to tune the ergonomics and information contained in the output display generated by P3D.

During the third profile run, extra functionality was added to calculate the average speed of the vehicle. This was used to compare against coordinate logs to verify the correct execution of the calculations.

On completing a few runs with these profiles, the correct execution of the simulator was assured and P3D was fine-tuned to present relative data in an easy to manage and understandable way.

The route and acceleration-speed parameters of the profiles are shown in figures 6.1, 6.2 and 6.3.

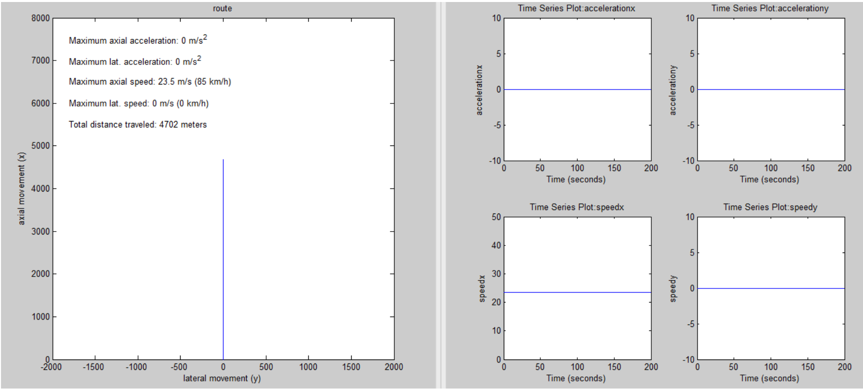


Figure 6.1: SVP1

Steady velocity 85 km/h

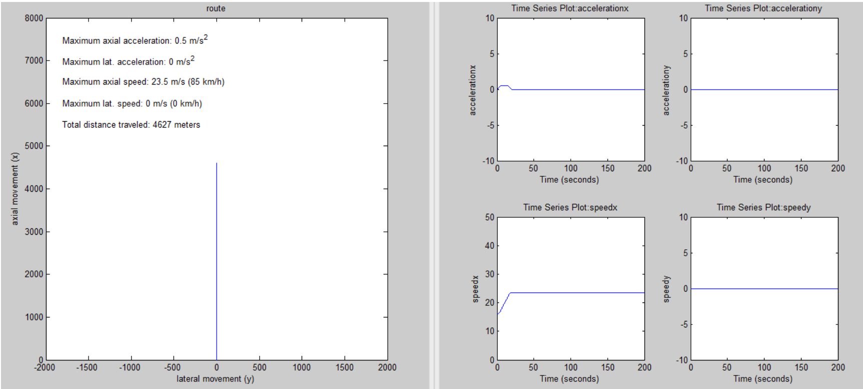


Figure 6.2: SVP2

Acceleration from 65 km/h (18m/s) to 90 km /h (25m/s)

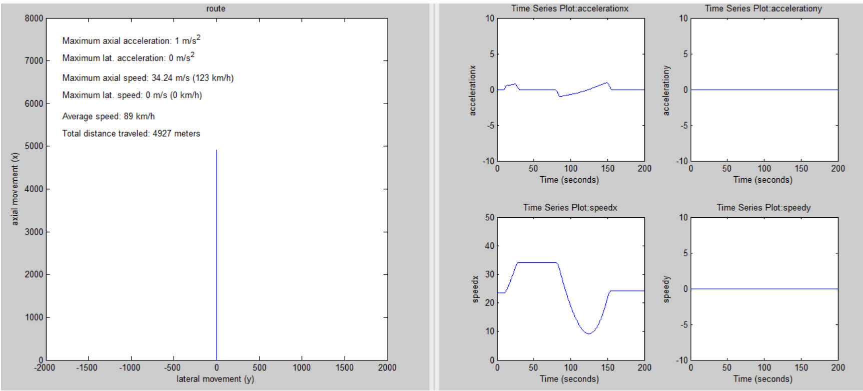


Figure 6.3: SVP3

Multiple accelerations / decelerations from 65 km/h (18m/s) to 90 km/h (25m/s) to 47 km/h (13m/s) to 72 km/h (20m/s)

6.1.2 Curve profiles

Following the initial tests, more complicated profiles were created to test turning, and acceleration. Profile 4 tested the execution of a simple ninety degree turn. Profile 5 added a second turn in the opposite direction. Profile 6 added accelerations and decelerations and turning with increased velocity. Profile 7 was used to test how the simulator and P3D handle movement in every possible direction.

The profiles' route and acceleration-speed parameters are shown in figures 6.4, 6.5, 6.6 and 6.7.

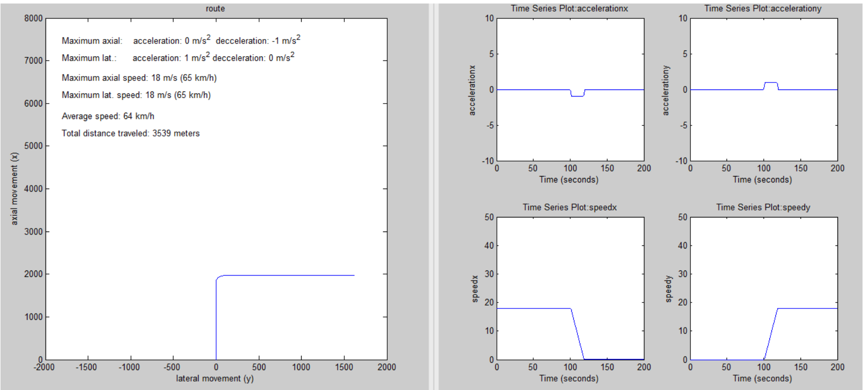


Figure 6.4: SVP4

Right turn (90) with steady velocity (65 km/h) completed within 20 seconds (0.1g)

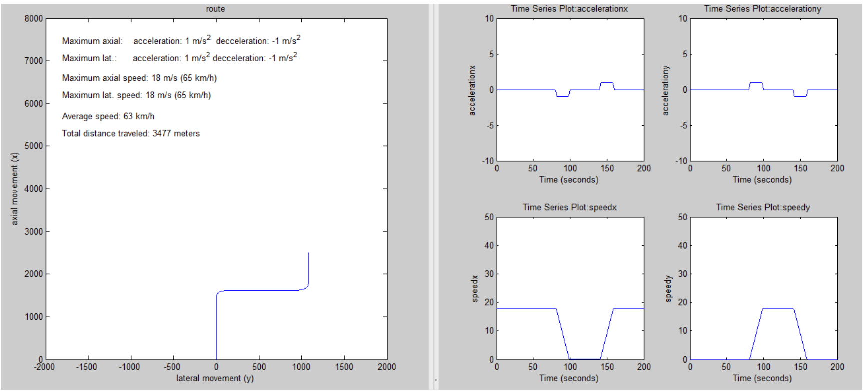


Figure 6.5: SVP5

Successive turns with steady velocity (65 km/h) (0.1g)

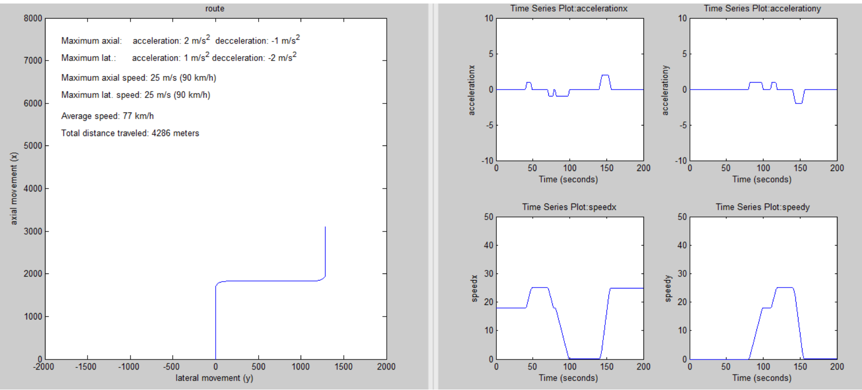


Figure 6.6: SVP6

Successive turns with starting velocity of 65km/h, acceleration to 90km/h, deceleration back to 65 km/h before right turn (0.1g), acceleration to 90km/h and left turn (0.2g)

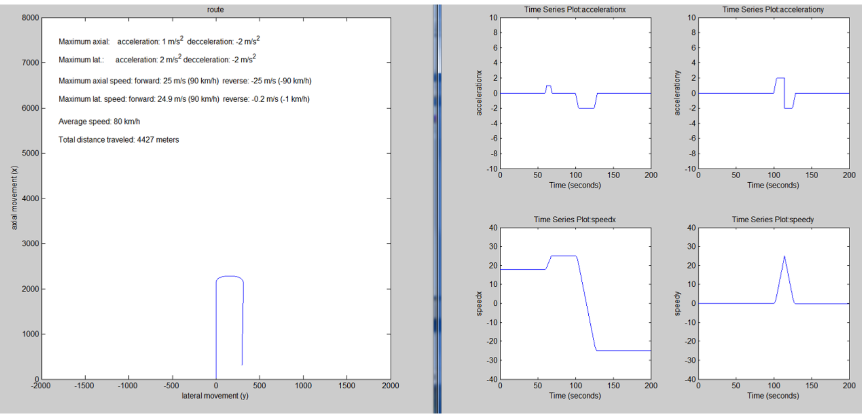
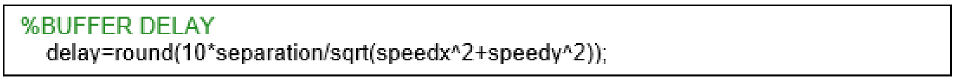


Figure 6.7: SVP7

180 degree turn with starting velocity of 65km/h acceleration to 90km/h and turn with steady velocity (0.2g)

6.2 Multiple Vehicle (Platoon) Operation

Initially, each vehicle instantly matched the acceleration of the preceding vehicle after reading it directly through the MATLAB bus. The lead vehicle had predetermined acceleration data for the simulation runtime, defined in the parameters. This confirmed that the vehicles behaved as expected but certain changes were necessary to achieve realistic behaviour. Each vehicle had to introduce a delay, corresponding to the vehicle's speed and distance from the one ahead (see figure 6.8).



```
%BUFFER DELAY
   delay=round(10*separation/sqrt(speedx^2+speedy^2));
```

Figure 6.8: Buffer delay code

All simulation runs beyond validation, have used profile 6.

6.2.1 Following test

The objective here was to see if the followers follow the leader throughout the profiles tested in single-vehicle validation and test if P3D can post-process the results

The profiles were again tested, this time for 4 vehicles. P3D was enhanced to track the headway between each vehicle. It was confirmed that the vehicles tracked each other as expected in every scenario. Small errors (deviations) are present due to known limitations with the setup but can easily be identified and ignored. A script was created for this reason (see section 5.4).

The profiles here are experimental profiles used during the validation of the model and are designated by the format MVP# (Multi-vehicle Validation Profile #).

All the profiles presented in 6.1 were tested for multiple vehicles. Figures 6.9 and 6.10 show the route and acceleration-speed parameters for profiles 3 and 6. These were chosen as the most representative for a linear and a curve profile. A third plot has now been added, representing the separation between the vehicles. The x and y axes have also been switched in the route diagram to make it clearer.

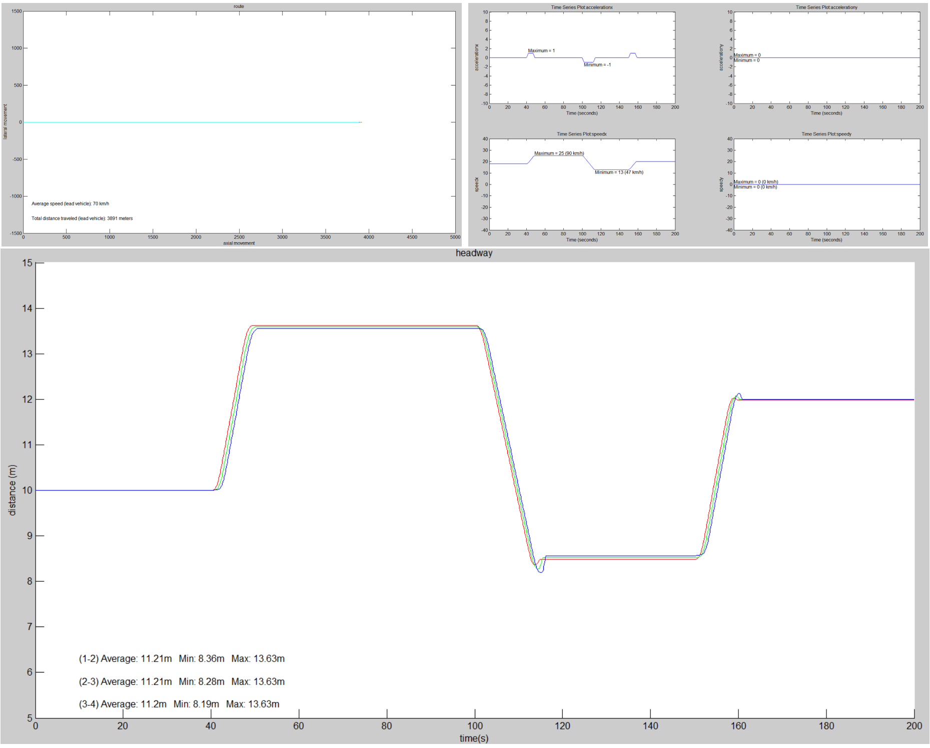


Figure 6.9: MVP3

Multiple accelerations / decelerations from 65 km/h (18m/s) to 90 km/h (25m/s) to 47 km/h (13m/s) to 72 km/h (20m/s)

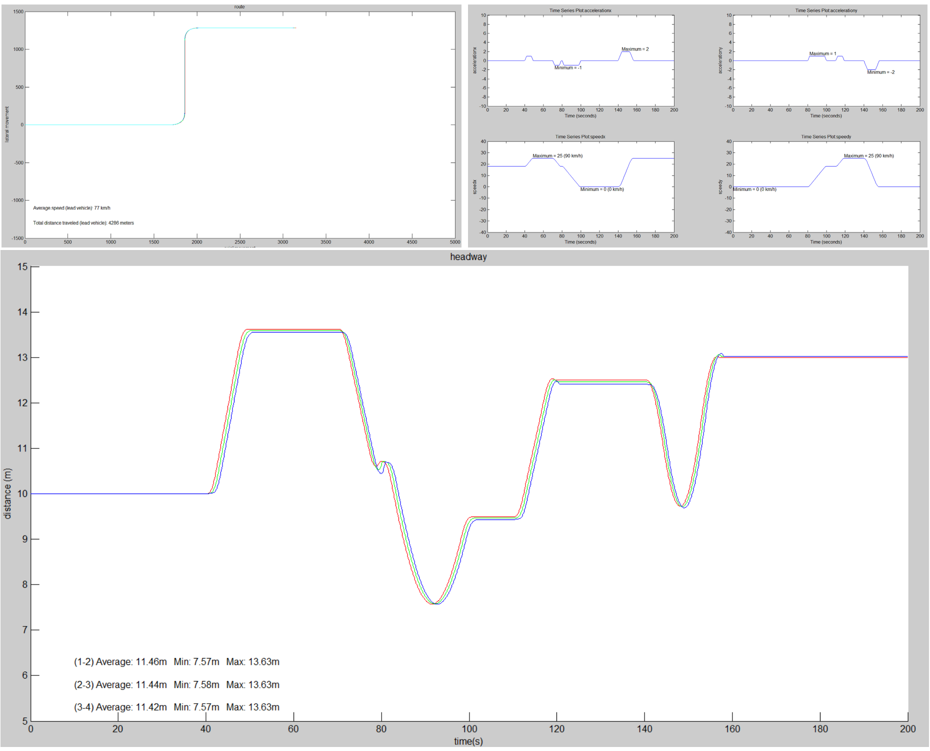


Figure 6.10: MVP6

Successive turns with starting velocity of 65km/h, acceleration to 90km/h, deceleration back to 65 km/h before right turn (0.1g), acceleration to 90km/h and left turn (0.2g)

6.2.2 Platoon break-up tests

The objective here was to artificially break-up the platoon, verify the behaviour of the vehicles and test if P3D can detect and record break-ups.

The limits for the platoon to be considered to have broken are shown in table 6.1.

Parameter	Minimum value	Maximum value
headway	5 m	20 m
deviation	-	5 m

Table 6.1: Platoon breakup limits

An artificial delay was introduced in the link between the 2nd and 3rd vehicle of the platoon (2nd link), to examine how vehicles would behave and how P3D would be used to verify the resulting deviations. The 2nd link was chosen to allow the examination of dynamic correlations between the vehicles. Corrupting the 2nd link allows the examination of a correct link between the first two vehicles, a corrupted link between the second and third vehicle and a correct link in a section of the platoon that has been affected by interference.

Two additional profiles were made for this reason (MVP8 and MVP9), based on profile MVP6.

Figures 6.11 and 6.12 show the route followed by each vehicle and the separation between the vehicles.

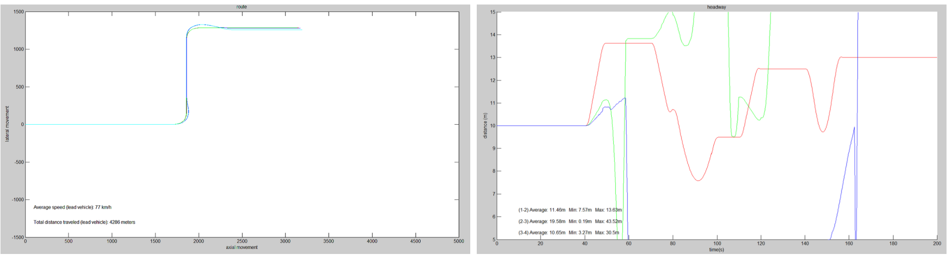


Figure 6.11: MVP8

Artificial delay of (pv5+addelay=10+randi(100)) introduced in the link between 2nd and 3rd vehicle. (Based on MVP6)

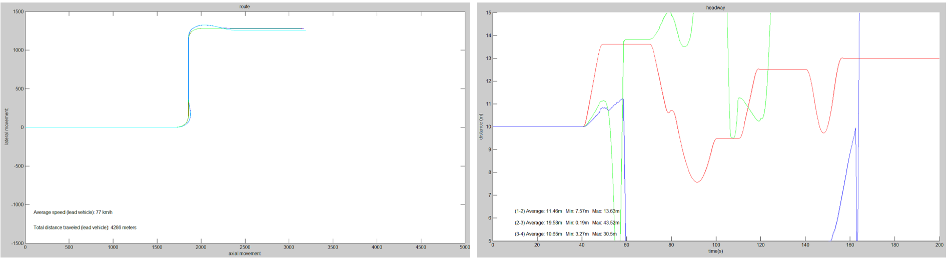


Figure 6.12: MVP9

Artificial delay of (pv5+addelay=20+randi(200)) introduced in the link between 2nd and 3rd vehicle. (Based on MVP6)

Chapter 7

Jamming

This section describes the jammer's implementation in the simulation environment, its operational modes and its effects on the platoon.

7.1 Implementation

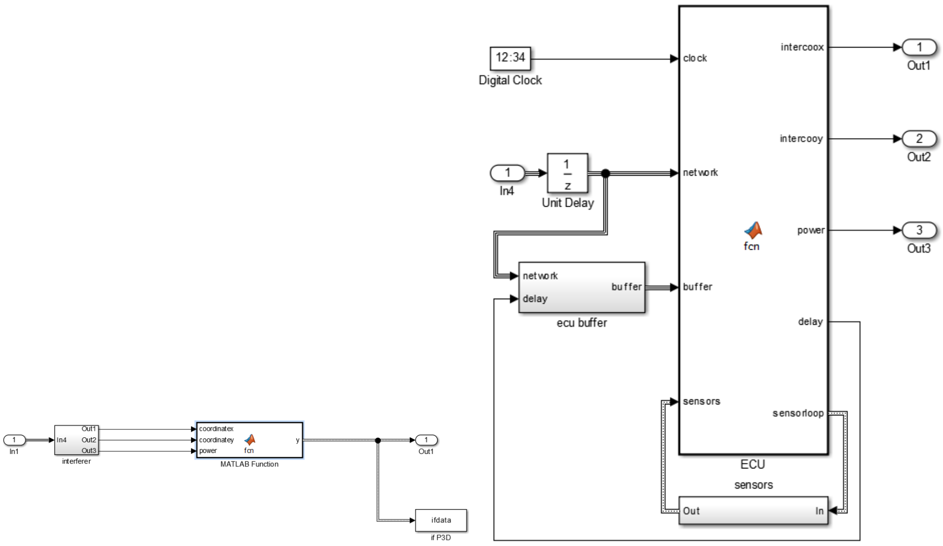
The jammer was initially a simple subsystem. It consisted of a function to statically configure its parameters and outputs to the vehicles' receivers and the P3D module. This was used for the initial tests and configuration of the network and vehicle interactions and the set up of P3D to include jamming data.

For further experimentation, and eventually implementation of an intelligent mobile jammer, this was improved to resemble a normal vehicle that can either move independently on and around the road, or track a vehicle in the platoon (see figure 7.1). As such, it has many of the same basic vehicle functions but also adds the parameter of transmission power, to configure the intensity of jamming. The inputs and outputs of the subsystem are listed in table 7.1. The jammer uses an omnidirectional antenna and can cause interference in a 500 meter radius.

The interferer creates a virtual signal of configurable intensity which is received by the vehicles' R/T module. This is in turn combined with the transmissions from the other vehicles, a Signal-to-Noise Ratio is calculated and passed as a parameter to the Additive White Gaussian Noise channel inside the network. The interference suffered by a vehicle is in direct correlation to its distance to the interferer and the interferer's jamming power. The effect is null for distances greater than 500 meters. The SnR with no interference present is set to 10 and can drop down to 0 when full jamming is achieved.

The interferer receives its data directly from the platoon's sensors and not the network. This is because it can be assumed that a mobile interferer would be placed on a manually driven vehicle that can track the platoon visually, regardless of network inconsistencies.

For the first few tests, the network design was not finalized and there was no simulation of channels or beamforming. This however, did not prohibit the idea of simulating an imperfect medium. This was introduced



(a) Jammer (b) Mobile jammer

Figure 7.1: Jammer model

in the form of arbitrary errors of varying frequency, in the data received by each vehicle. The results, though not representative of a real interference scenario, served well for demonstrating the concept and fine tuning the vehicle dynamics and network synchronization.

With the network setup crystallized, and the different channels tested (see subsection 5.3.3), an interferer was implemented.

	Role	Defined by	Used by	Comments
network	Input	Platoon sensors	ECU	Data received from the platoon sensors
buffer	Input	Platoon sensors + ECU	ECU	Buffered data received from the platoon sensors
sensors	Input	ECU	ECU	Data received from the vehicle sensors
intercoox	Output	ECU	Vehicle R/T	X coordinate of jammer
intercooy	Output	ECU	Vehicle R/T	Y coordinate of jammer
delay	Output	ECU	Buffer	Buffer delay control
sensorloop	Output	ECU	ECU	Data sent to the jammer sensors

Table 7.1: Interferer Input/Output list

7.2 Stationary Jammer

In this section a simple roadside, stationary jammer is considered. This could either be a source of unintentional interference or a malicious interferer.

The stationary jammer was placed in different locations along the platoon's path and tested with different power settings to observe the effects on the platoon. Finally, a location representative of multiple modes of operation (turning, acceleration and deceleration) was selected to examine further, as it was a particularly critical and communications intensive period for the system vulnerable to interference. The placement of the jammer is shown in figure 7.2 relative to the platoon path (there is no interference because the jammer is deactivated).

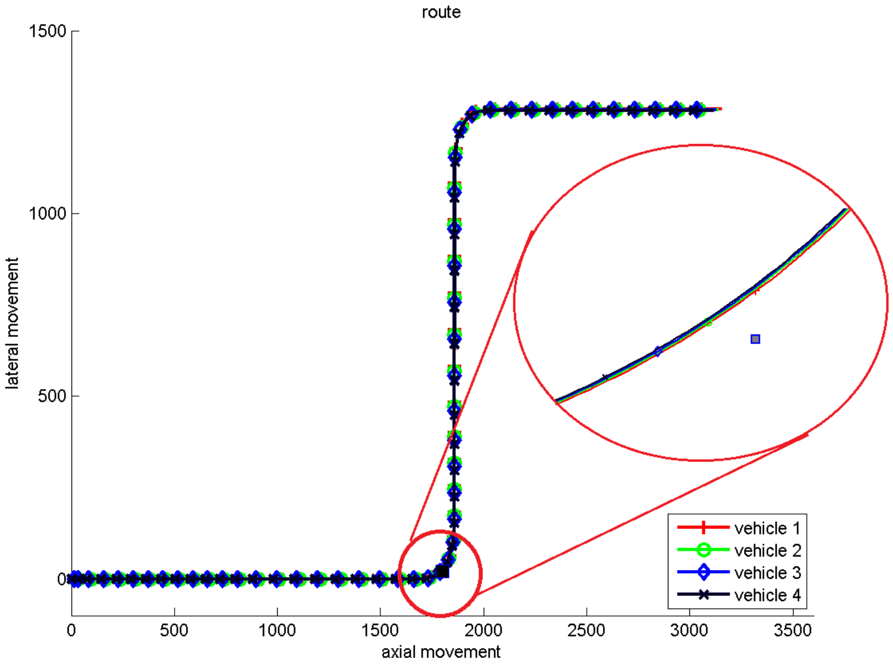
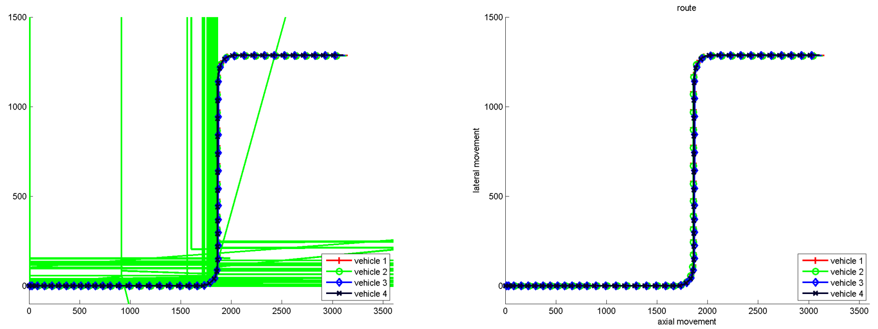


Figure 7.2: Stationary jammer location

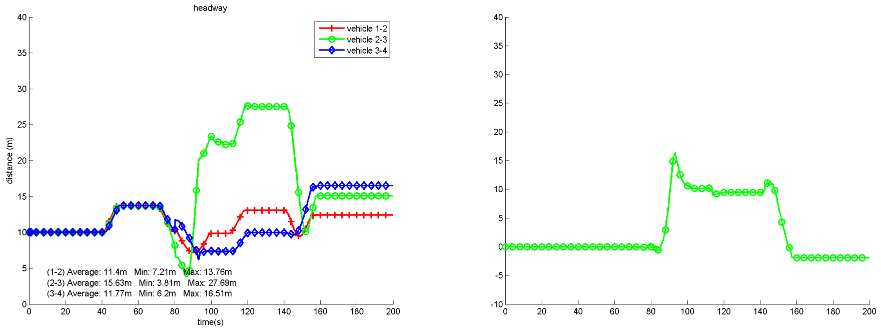
At first, the jammer was configured to only interfere with the communication link between the second and third vehicle. This allowed the examination of one good link, one under attack and one following an attacked link. The first run had vehicles with no defence mechanisms activated beyond basic error correction and a jammer transmitting at 80% power. The route seen by the network is shown on figure 7.3a. It is obvious that vehicle 2 sends erroneous data regarding its position, however vehicle 3 and 4 do not appear to be influenced. This is due to the built in error correction in each vehicle, that disregards improbable data. As can be seen on figure 7.3b there is no extreme deviation from the desired route. However, looking at the headway (figure 7.4a) and deviation (figure 7.4b) data, it is evident that the platoon has in fact broken up at the 90 second mark, where deviation



(a) Network

(b) Sensors

Figure 7.3: Stationary jammer route plots, no defences, 80% power



(a) Headway (sensors)

(b) Vehicle 3 deviation

Figure 7.4: Headway and deviation, no defences, 80% power

exceeds the cut-off point of 5 meters.

An additional run at 100% jamming power gave a much greater deviation that can now be clearly seen in figure 7.5. Vehicle 1 performs normally as well as vehicle 2 which is tracking it. Vehicle 3 has deviated considerably from the desired route and vehicle 4 has tracked it perfectly, also deviating from the desired route.

These tests proved that the setup of the vehicles, network and jammer is sufficient to simulate severe interference that will easily cause a platoon breakup. These results will be used in the following chapters as a benchmark for defences against interference.

7.3 Mobile Jammer

Taking into account the mobile nature of the platoon, it is reasonable to assume that a jammer targeting such a system, would be mobile and able to track the platoon and attack it continuously. In this chapter, additional runs are analysed, where the jammer acts similarly to a vehicle, tracking the platoon and causing continuous interference.

The mobile jammer was setup to follow the platoon leader closely (at a

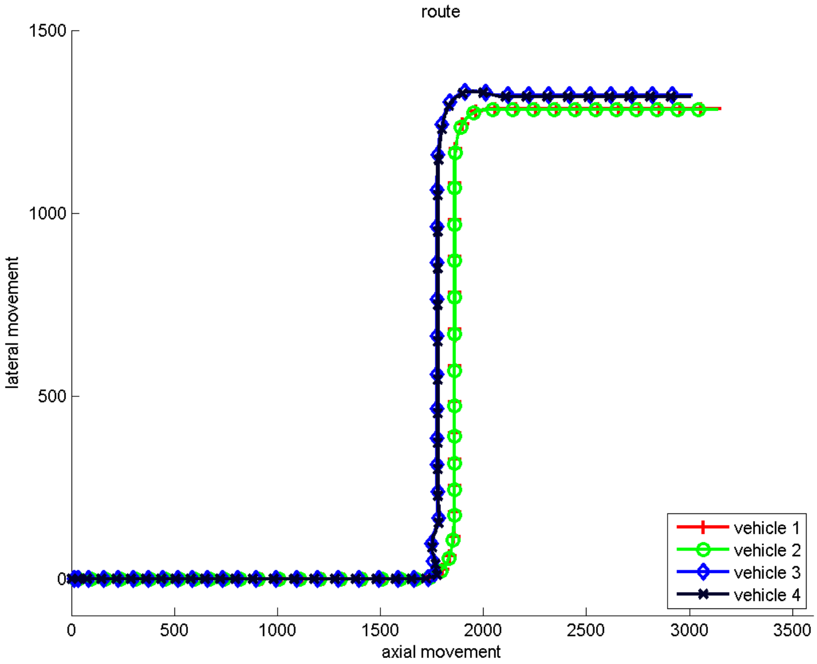
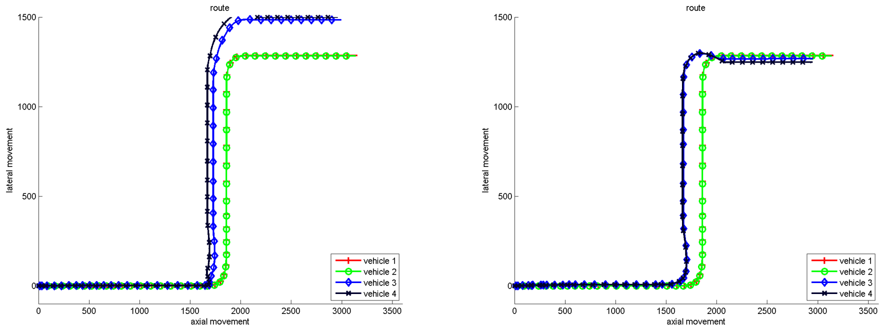


Figure 7.5: Stationary jammer route plot (sensors), no defences, 100% power

maximum distance of 10 meters) and change positions randomly. At this distance, the maximum level of interference is achieved. Combined with the persistence of the attack this presents a very challenging scenario. This is needed as it allows the defence mechanisms that will be presented in the following chapters to be tested to their breaking point.

In this series of runs, a low jamming power setting was sufficient to cause a breakup. The jammer was again configured to only interfere with the communication link between the second and third vehicle. Interference in all links would cause even greater disruptions.

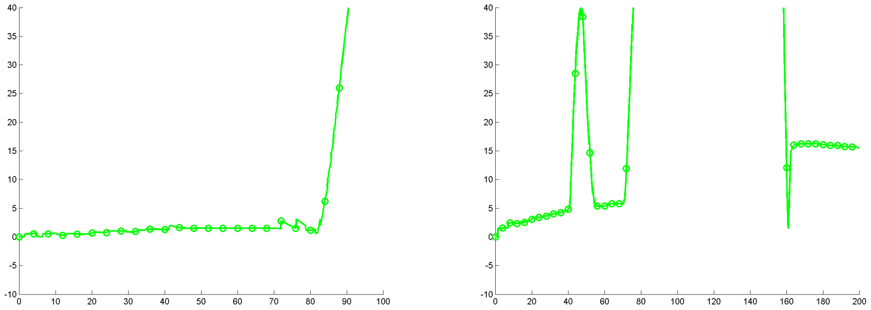
The route of the platoon is shown in figures 7.6a and 7.6b. In both cases, it is clear that the platoon has broken up by the time it reaches the first turning point. If the routes post-breakup were to be compared, it would appear that the low power setting caused more severe interference. However, examination of other parameters, such as speed, acceleration, headway and deviation indicates that breakup has occurred earlier in the case of 100% power. Specifically, figures 7.7a and 7.7b show deviation from the path for vehicle 3 in both cases. The cut-off point for deviation has been set to 5 meters, so these figures indicate a breakup at the 45 second mark for the 100% power case against 90 seconds for the 60% case. Figures 7.8a and 7.8b show headway between the vehicles. The cut-off point for headway has been set to 20 meters, so these figures indicate that breakup actually occurred at the 10 second mark for the 100% power case against 25 seconds for the 60% case.



(a) 60% power

(b) 100% power

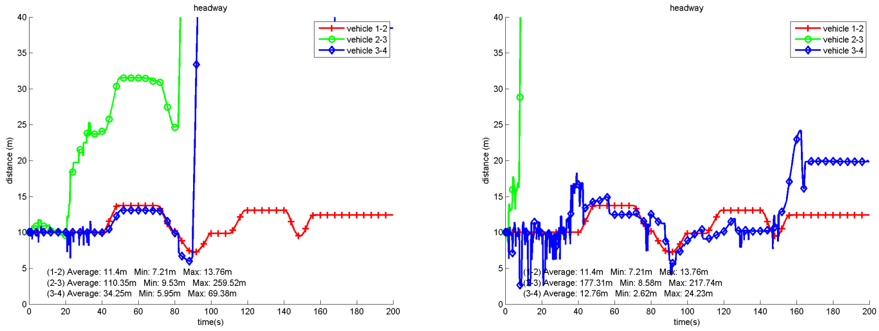
Figure 7.6: Mobile jammer route plots (sensors), no defences



(a) 60% power

(b) 100% power

Figure 7.7: Mobile jammer deviation plots (vehicle 3), no defences



(a) 60% power

(b) 100% power

Figure 7.8: Mobile jammer headway plots (sensors), no defences

Chapter 8

Defences

This chapter describes the defence mechanisms implemented and tested in the simulation. These fall into three categories:

- Interference reduction
- Data redundancy
- Warning systems

They have been examined separately and in combination to determine how effective they are against an attack and provide a solution to:

1. Reduce interference
2. Provide higher interference tolerance
3. Warn the user when possible faults occur

The following four specific methods have been selected:

- **Beamforming**

  This refers to manipulating the receive/transmit beam to achieve interference reduction.

- **Double anchoring**

  This refers to utilizing input from multiple sources to achieve data redundancy and identify possible errors.

- **GPS verification**

  This refers to utilizing a vehicle's GPS module to check the platoon's inputs and provide error correction and warnings.

- **On-board sensor verification**

  This refers to utilizing independent safety systems of a vehicle to verify the platoon's inputs and provide error correction and warnings.

These are presented in the following sections.

8.1 Beamforming

Beamforming is a technique of actively steering the beam of transmission and reception of a wireless communication system in such a way that useful signal reception is maximized while interfering signals reception is diminished. In this section, beamforming is implemented and its performance against interference in a platoon is compared with a regular omnidirectional antenna. An improvement to the simple beamforming called beam sharpening is also implemented and tested.

This technique enables vehicles to actively manipulate their communication beams based on feedback from the network and platoon state. The direction and width of the beam can be set to target specific vehicles in a platoon to reduce external interference and increase the platoon's survivability under attack. In the same way, it can also reduce internal interference between members of the platoon (not implemented).

8.1.1 Implementation

This function is mainly implemented in the R/T module of a vehicle (see section 5.2).

The flowchart in figure 8.1 outlines the operations taking place. Vehicle 2 is using beamforming in this scenario and is referred to as the first party of the communication process and vehicle 1 as the second party.

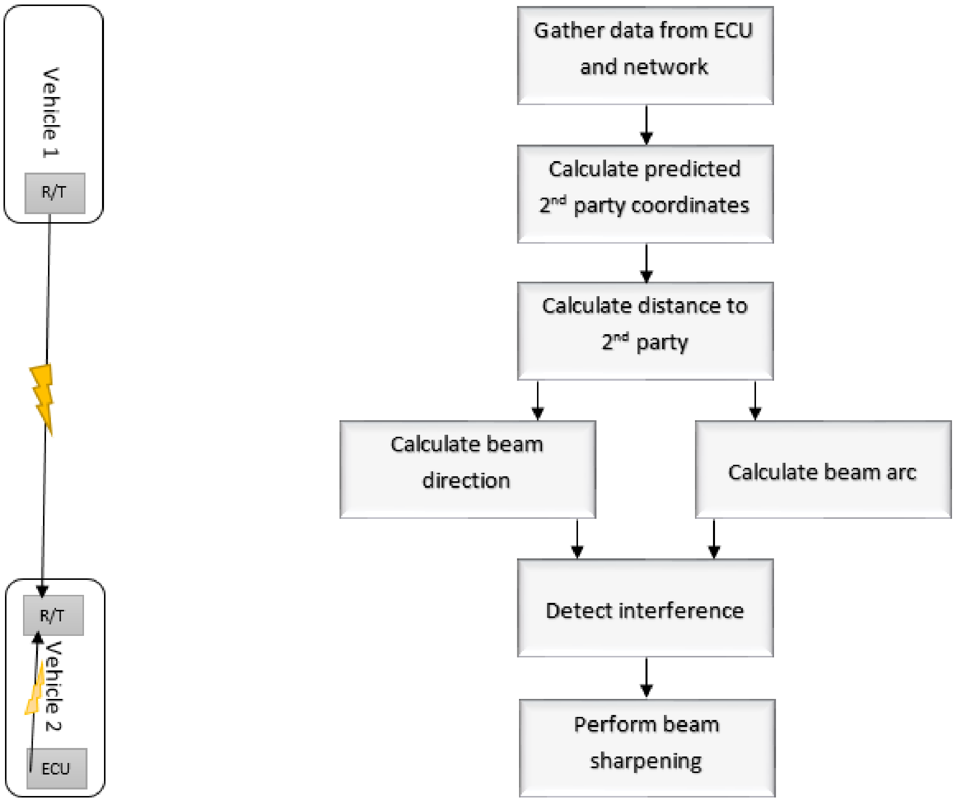


Figure 8.1: Beamforming flowchart

Based on the state of the first party (determined by the data sent from its ECU) and the data received from the second party, several calculations are performed. The predicted position of the second party on the next timestep is calculated, based on its last known position, speed, acceleration and heading. The projected distance between the two vehicles is then calculated.

The absolute beam direction is calculated based on the two vehicles' positions. The relative beam direction is calculated based on the absolute beam direction and the heading of the 1st party. The beam arc is calculated based on the distance between the vehicles and the desired beam width at the location of the second party. This means that under normal operation, the beam width is determined only by the distance between the communicating vehicles. Figure 8.2 demonstrates the concept of beam direction and beam width. Table 5.4 lists the full list of parameters handled by the R/T module.

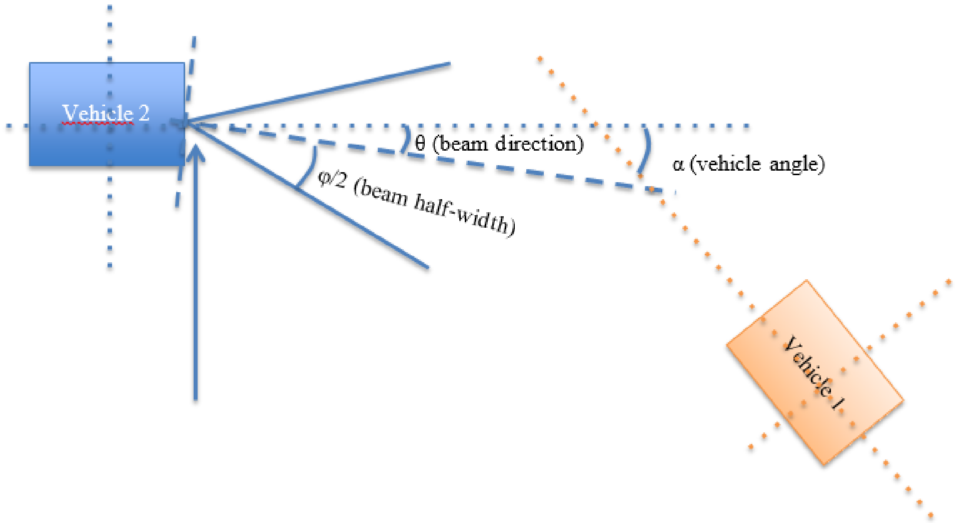
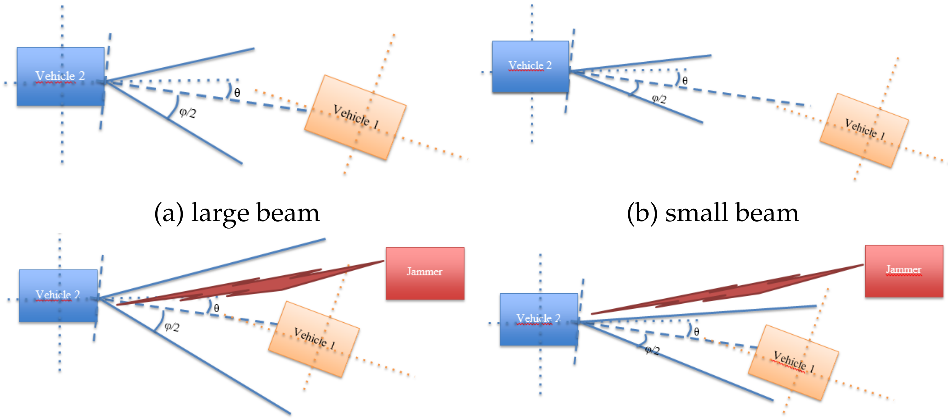


Figure 8.2: Beamforming parameters

If interference is detected, beam sharpening is performed to mitigate its effects. Beam sharpening is activated when interference exceeds a preset limit (set in this simulations to 50% jamming power) and it sharpens the beam progressively until a preset minimum, based on the desired beam width at the location of the second party (set in this simulations to 2,5m, 50% of the regular beam). In this case beam width is determined both by the distance between the communicating vehicles and the presence of interference. This operation is shown in figure 8.3. In figure 8.3a the platoon is in the process of turning: the beam is rotated to closely follow adjacent vehicles and reduce possible interference. In 8.3b the platoon is operating in higher speed: inter-vehicular distances are increased, so beam angle is reduced to keep constant width on target and decrease chances of interference. In 8.3c a mobile jammer is moving alongside the platoon: the jammer positions itself within the main lobe of the beam, making its interference more effective. In figure 8.3d beam sharpening is applied:

on detecting the jamming, the beam is sharpened, thus positioning the jammer outside the main lobe. While the jammer can still interfere, it is considerably less effective. The beam is not a perfect cone and besides the main lobe, smaller side-lobes can still pick up interference, for simplicity the side lobes are not pictured here.



(a) large beam

(b) small beam

(c) jammer in beam

(d) jammer avoided

Figure 8.3: Beamforming operation

8.1.2 Results

In addition to the figures analysed here, more are available in appendix A and electronically upon request.

In all the scenarios presented here, the platoon breaks up when in omnidirectional mode (see tables 8.1 and 8.2). Figure 8.4a shows the case of an attack on one link at a power setting of 80%. Vehicle 3 has exceeded the headway limit of 20m and the platoon has broken up. In figure 8.4b the same attack is performed on all vehicles and the platoon is again broken up as expected with much greater maximum headway recorded and a minimum headway of only 0,4m.

When a single communication link is attacked, plain beamforming is sufficient to defeat an attack with 80% jamming power (figure 8.4c). However, the defence fails against attacks with higher power or ones that target multiple links. For example, when all links were attacked with 80% power (see figure 8.4d) even though headway was maintained bellow 20m, the vehicles approached dangerously close (below the limit of 5m) during the second turn and the platoon broke up.

Since plain beamforming performance was unsatisfactory, beam sharpening was implemented and the attack profiles were tested again. The results were very encouraging. When a single link was attacked, the platoon remained stable even under 100% jamming power. Even when all links were under attack, the platoon did not break up. As seen in figure 8.4e the minimum headway is maintained well above 5m and the maximum values are decreased as well. Figure 8.4f demonstrates the most demanding scenario tested here, with all links under attack at 100% power. Even in this case, the platoon does not break up. However, headway between vehicles 1 and 2 is uncomfortably close to the limits by the end of the second turn.

Attack profile		Defence profile		
Link	Jammer	Omnidirectional	Beamforming	BF with sharpening
2	80%	✗	✓	✓
2	100%	✗	✗	✓
all	80%	✗	✗	✓
all	100%	✗	✗	✓

Table 8.1: Beamforming defence results (stationary jammer)

✗: defence failed ✓: defence successful

Attack profile		Defence profile		
Link	Jammer	Omnidirectional	Beamforming	BF with sharpening
2	80%	✗	✗	✓
2	100%	✗	✗	✓
all	80%	✗	✗	✓
all	100%	✗	✗	✓

Table 8.2: Beamforming defence results (moving jammer)

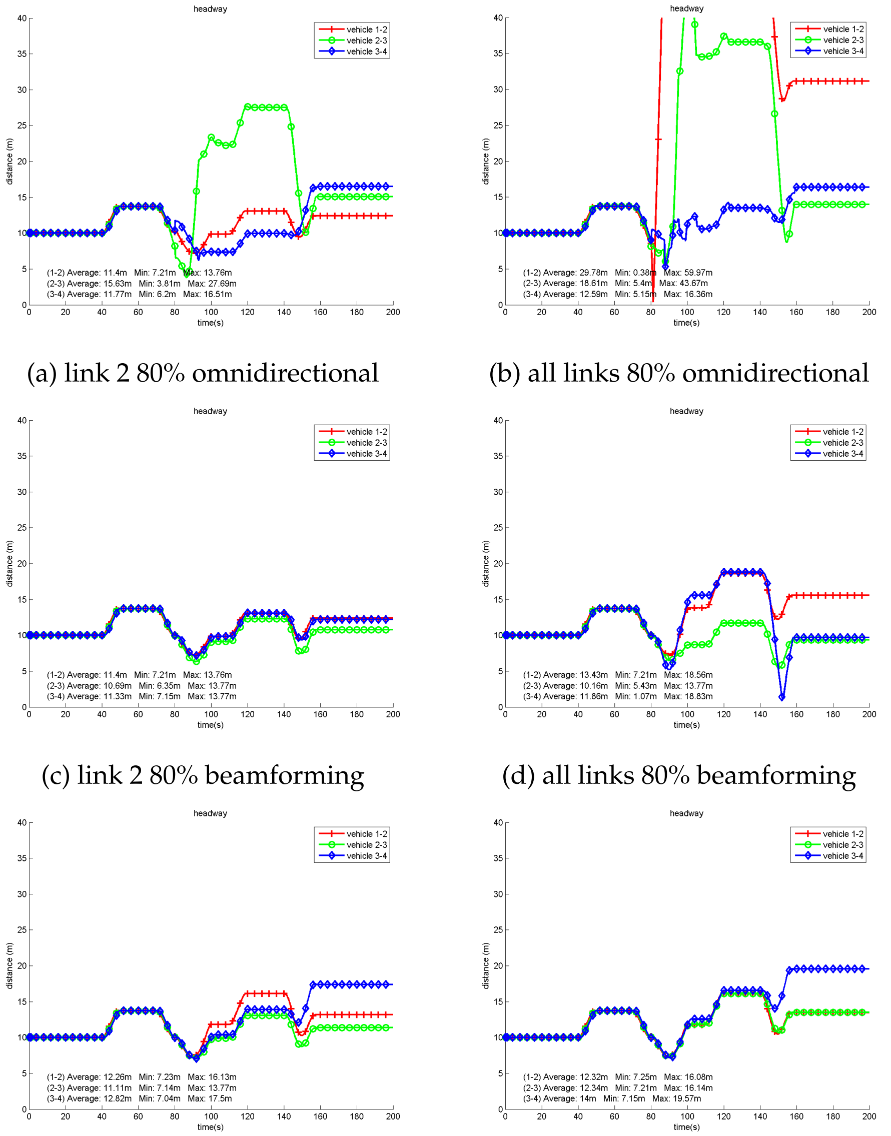
✗: defence failed ✓: defence successful

Table 8.2 shows the results of tests using a mobile jammer. Here the interference persisted throughout the whole simulation. Simple beamforming was not sufficient to defeat any of the previous attacks. Beam sharpening however proved very effective and successfully defeated all the attacks implemented.

Figures 8.5 and 8.6 demonstrate the movement of the platoon and the beams of the vehicles and the jammer (designated by a black square) when beam sharpening is activated or deactivated.

In figure 8.5 beam sharpening is deactivated. Comparing it with figure 8.6 the vehicles maintain sharper beams throughout the simulation. This, in many instances helps keep the jammer outside the beam and significantly reduce its effect. In addition, the sharper beam allows less interference to be picked up compared to the useful communication that is always within the beam. In other instances it may appear that the opposite happens: the jammer is outside the beam when no beam sharpening is used whereas inside when beam sharpening is activated. This is only because in the case of no beam sharpening, the vehicles are misaligned and is in fact a sign of the platoon being affected by interference. This is more evident comparing figures 8.5f and 8.6f.

When beam sharpening is deactivated, the platoon in fact breaks up as the distance between vehicles 2 and 3 slightly exceeds the limit of 20m.



(a) link 2 80% omnidirectional

(b) all links 80% omnidirectional

(c) link 2 80% beamforming

(d) all links 80% beamforming

(e) all links 80% BF with sharpening

(f) all links 100% BF with sharpening

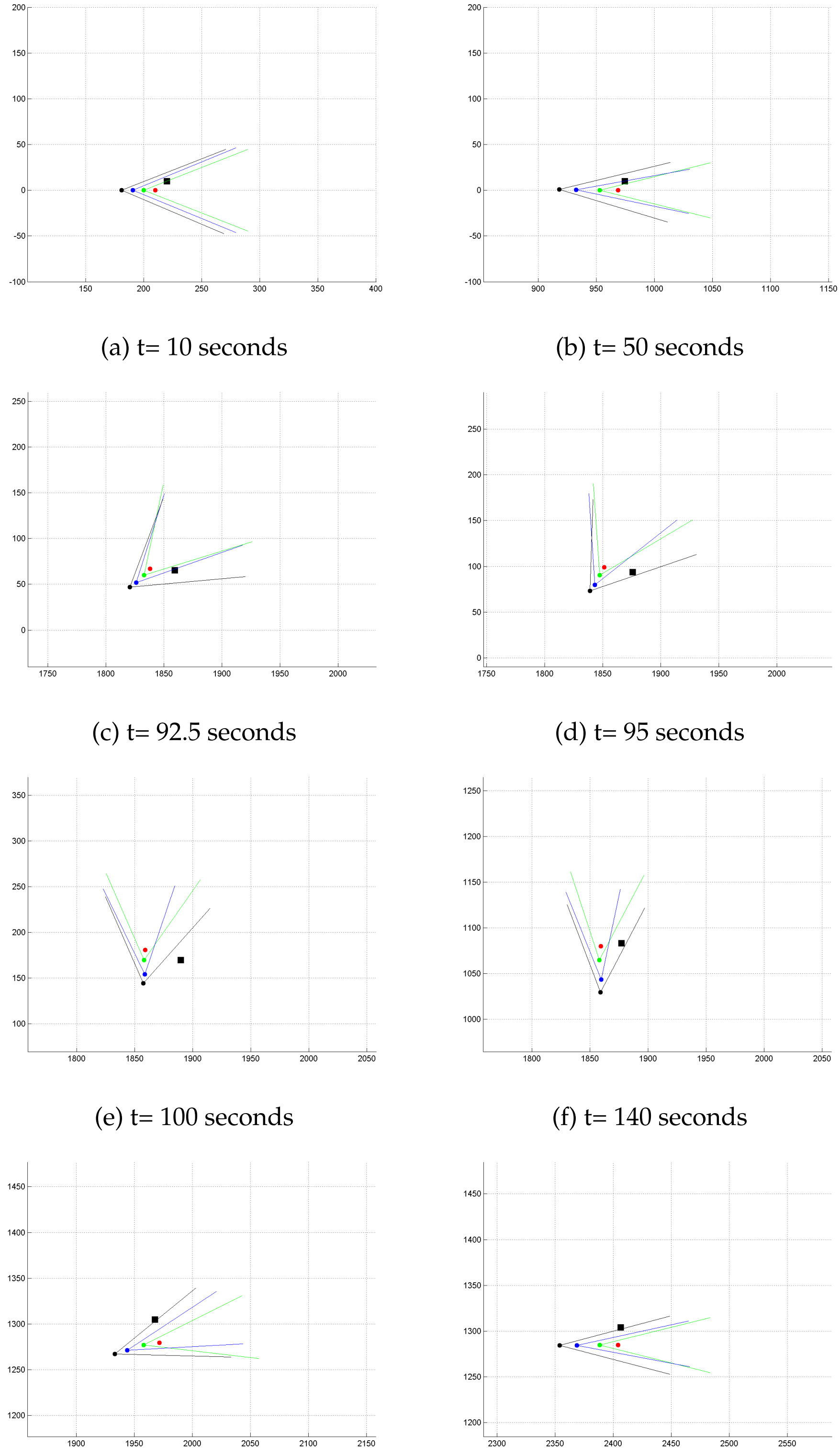
Figure 8.4: Beamforming headway plots (stationary jammer)

8.1.3 Conclusion

Beamforming was implemented and tested in several scenarios. In its simple form, it successfully defended against low power attacks on a single link but was not sufficient against more advanced or powerful attacks.

An improvement was implemented that allowed the beam to be sharpened in the presence of high interference, improving the Signal-to-Noise ratio at the cost of higher risk of misplacing the beam and losing contact during high speed relative movement of the vehicles.

With beam sharpening the results were promising. The platoon was able to resist stronger attacks, and be more stable than before. Even the strongest attack was unsuccessful in breaking the platoon, even though it tested this defence method to its limits. This was an incentive for investigating additional defence mechanisms that could be combined with beamforming.



(a) t= 10 seconds

(b) t= 50 seconds

(c) t= 92.5 seconds

(d) t= 95 seconds

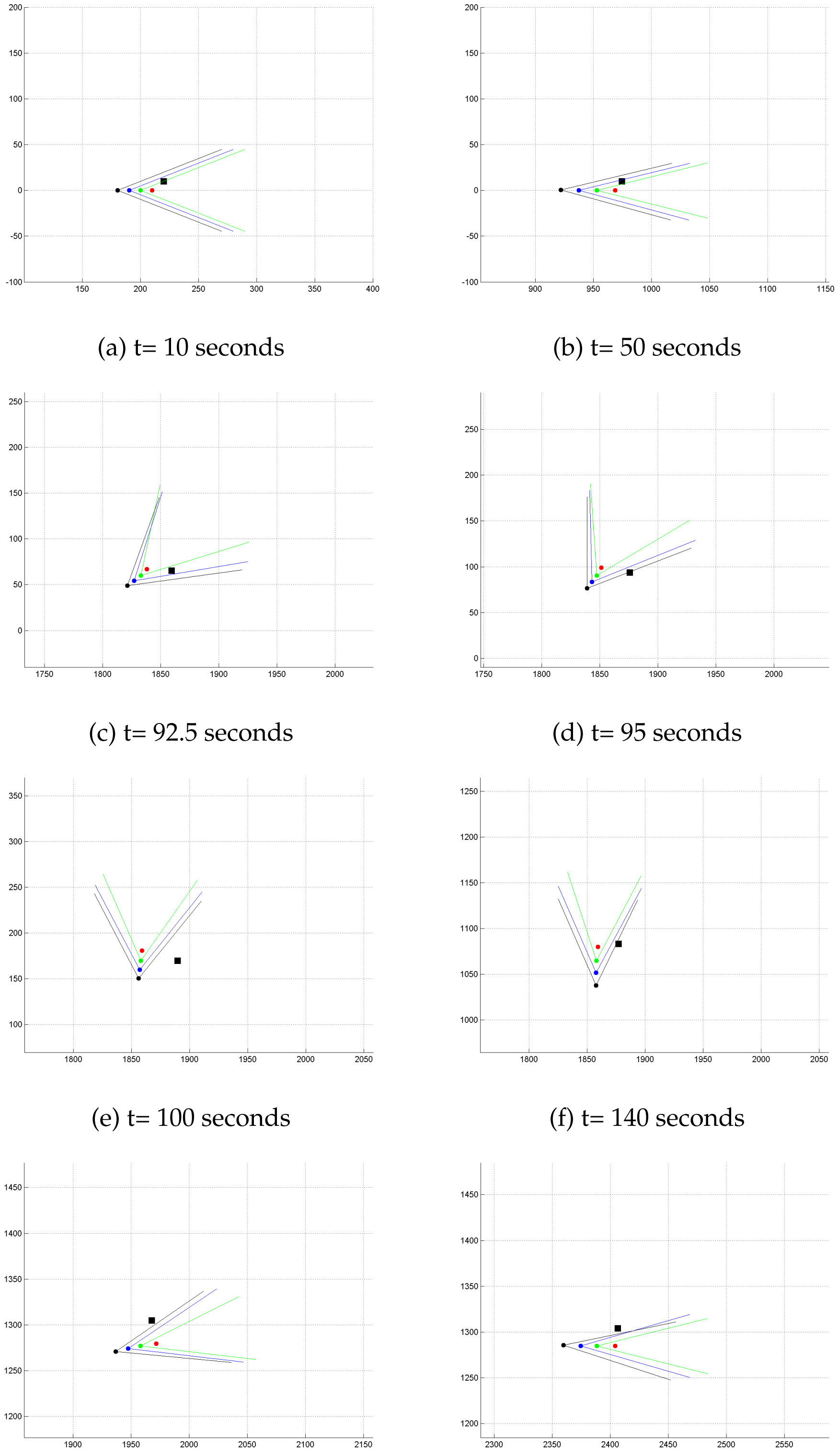
(e) t= 100 seconds

(f) t= 140 seconds

(g) t= 152.5 seconds

(h) t= 170 seconds

Figure 8.5: Platoon animation, beamforming, 80% jamming power



(a) t= 10 seconds

(b) t= 50 seconds

(c) t= 92.5 seconds

(d) t= 95 seconds

(e) t= 100 seconds

(f) t= 140 seconds

(g) t= 152.5 seconds

(h) t= 170 seconds

Figure 8.6: Platoon animation, beamforming with beam sharpening, 80% jamming power

8.2 Double Anchoring

Double anchoring refers to a vehicle that receives data from two vehicles preceding it in the platoon. In this way, data can be checked for inconsistencies and corrected, in case received data from one of the vehicles is determined to be erroneous for any reason.

Under normal operation, this would not be necessary. It can be assumed that if all data is sent and received correctly, only the most relevant information of the preceding vehicle would be enough to safely and accurately control a vehicle.

However when there is only one source of data, if an error occurs the only option would be to operate in a "safe mode". This would mean that automatic control of the vehicle would be lost, a warning would be generated and the driver would have to immediately assume manual control. This would present a very dangerous situation, especially when vehicles in a platoon would normally operate at a closer proximity than would be comfortable for human drivers. This can be made safer by controlled automatic break-up of the platoon, handled by secondary systems (e.g. Adaptive Cruise Control).

To prevent this, a secondary (redundant) source of data can be used if possible. When a fault is detected in the primary source, the vehicle can fall back to the secondary source for a short period until the fault has been addressed.

8.2.1 Implementation

The double anchoring function is implemented in the ECU of the vehicles. The flowchart in figure 8.7 outlines the operations taking place. Any communication in the network is picked up by a vehicle's R/T module and passed to the ECU module. The ECU selects the data relevant to its state (in this example, from vehicles 1 and 2). After discarding any improbable values, the data from the two vehicles is compared. If the data agrees, it is assumed to be correct and used to control the vehicle. If the data is inconsistent, the ECU uses cached data to maintain the vehicle's course and logs a warning. If a certain threshold of warnings is reached, it is assumed that the discrepancies are not due to random errors but there is a problem that needs to be addressed.

Table 8.3 summarizes the results of the tests conducted with the double anchoring function enabled. These include the simple omnidirectional approach as well as the combination of the beamforming defence implemented in section 8.1. With no beamforming defence, the double anchoring defence can provide some but not complete protection from jamming. Combining double anchoring with the beamforming defence, provides additional resistance to jamming. The combined results are better to either the simple omnidirectional defence or beamforming defences (compare with table 8.1).

Selected results are discussed in subsection 8.2.2.

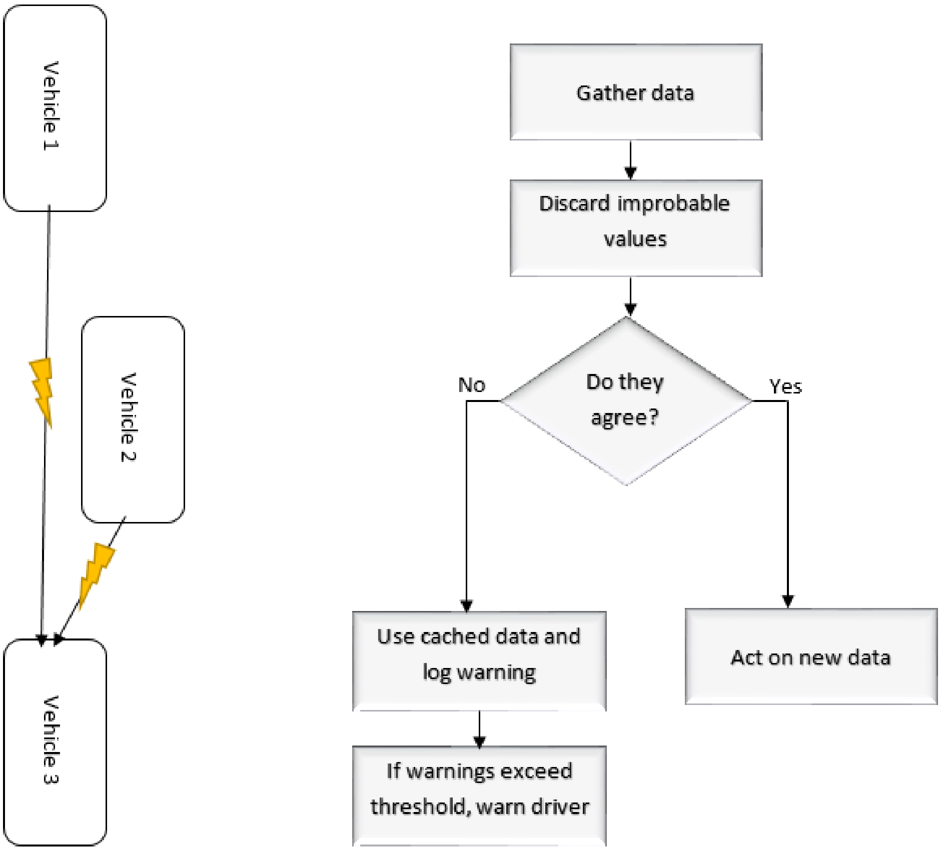

Vehicle 1
Vehicle 2
Vehicle 3
Gather data
Discard improbable values
Do they agree?
No
Yes
Use cached data and log warning
If warnings exceed threshold, warn driver
Act on new data

Figure 8.7: Double anchoring flowchart

8.2.2 Results

In addition to the figures analysed here, more are available in appendix A and electronically upon request.

When a single communication link is attacked, the double anchoring defence is sufficient to defeat an attack with 80% jamming power (figure 8.8a). Without this, the attack would have been successful in breaking up the platoon as seen in figure 8.4a. However, the defence is still not successful against an attack with 100% power. The shortcomings of the double anchoring method are seen when all communication links are attacked. The platoon is broken even under an 80% attack (figure 8.8b). However, that attack is only successful, because double anchoring, leaves the first link unprotected. This happens because there is only one preceding vehicle, making this method impossible to apply for that link.

Given the above success but also the shortcomings of this method, it was combined with the earlier implemented beamforming defence (see section 8.1). As expected, the combination indeed provides better resistance to jamming. The defence for the case of 80% power single node attack, is successful as before (figure 8.8c). However, the platoon is now more stable than plain double anchoring (compare to figure 8.8a) with the maximum headway dropping from 15.86m to 13.77m. Plain beamforming had failed (compare to figure 8.4a) with a headway of 27.69m.

Attack profile		Defence profile		
Link	Jammer	Omnidirectional + DA	Beamforming + DA	BF with sharpening + DA
2	80%	✓	✓	✓
2	100%	✗	✓	✓
all	80%	✗/✓	✓	✓
all	100%	✗	✗	✓

Table 8.3: Double anchoring (DA) (stationary jammer)

✗: defence failed ✓: defence successful

Attack profile		Defence profile		
Link	Jammer	Omnidirectional + DA	Beamforming + DA	BF with sharpening + DA
2	80%	✗	✗	✓
2	100%	✗	✗	✓
all	80%	✗	✗	✓
all	100%	✗	✗	✓

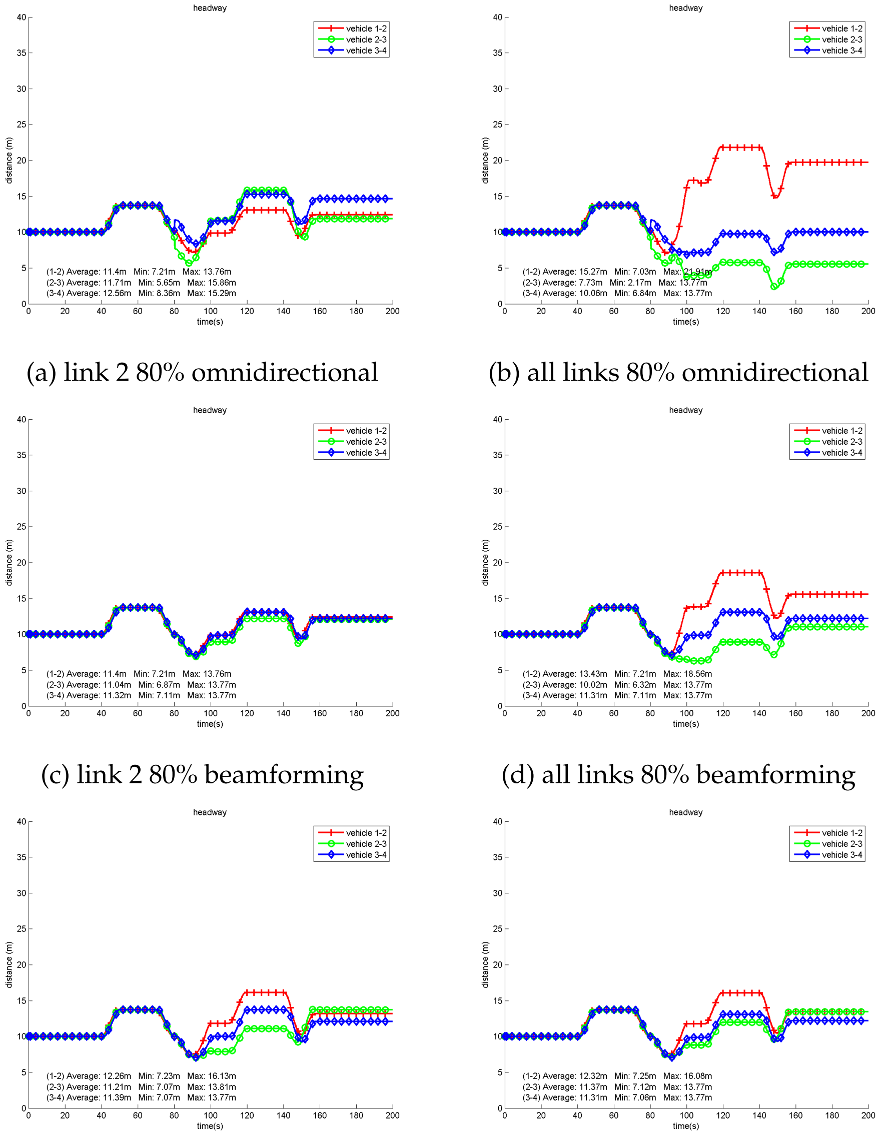
Table 8.4: Double anchoring (DA) (moving jammer)

✗: defence failed ✓: defence successful

The combined defence for the case of 80% power attack on all links is also successful (figure 8.8d). This is a clear improvement over the individual defences which had both failed (compare to figures 8.4d for the beamforming and 8.8b for the double anchoring). However, even the combined defence was not sufficient to defeat the 100% power attack.

The performance of the combined defence can be further improved by using beam sharpening, in addition to beamforming. The 80% all link attack is again defeated but this time, the platoon is more stable (figure 8.8e). This can be seen by the maximum headway dropping from 17.5m to 16.13m (compare to 8.4e). The improvement is also clear in the case of the 100% all link attack (figure 8.8f). Adding beam sharpening, makes the combined defence strong enough to defeat the attack. It is also far more stable to the case of plain beam sharpening with no double anchoring (compare to 8.4f).

Table 8.4 shows the results of tests using a mobile jammer. Here the interference persisted throughout the whole simulation. Simple beamforming was not sufficient to defeat any of the previous attacks. Beam sharpening however proved very effective and successfully defeated all the attacks implemented.



(a) link 2 80% omnidirectional

(b) all links 80% omnidirectional

(c) link 2 80% beamforming

(d) all links 80% beamforming

(e) all links 80% BF with sharpening

(f) all links 100% BF with sharpening

Figure 8.8: Double anchoring headway plots (stationary jammer)

8.2.3 Conclusion

Double anchoring was implemented and tested independently in several scenarios. It successfully defended against low power attacks but presented some shortcomings and was not sufficient on its own to defend against high power attacks. Most importantly, this method can not be applied to the first two vehicles which leaves the first link vulnerable to jamming.

Combined with the beamforming method implemented in section 8.1, the results were promising. The platoon was able to resist to stronger attacks, and be more stable than either of the techniques used independently. Finally when used in combination with beamforming with additional beam sharpening, the platoon was able to resist all of the attacks implemented with relative ease (see table 8.3).

This method introduces a one-step delay to the response time of the vehicles. In this simulations the time-step is 100 milliseconds which is a considerable amount of time when vehicles are moving at high speeds. This is however much faster than any human operator would be able to react. Additionally, in a real-world application the time-step will presumably be even orders of magnitude smaller, making the response time almost instantaneous.

8.3 GPS verification

GPS (Global Positioning System) verification refers to a vehicle that uses data from its GPS module and map data to provide error correction and warnings if it detects that it is deviating from the expected course of the road. It is assumed that any vehicle capable of being a platoon member will need to have a working GPS module and map data. GPS verification is then a simple and inexpensive function to implement.

This provides an independent system to monitor the state of the vehicle that is not subject to the same type of interference as inter-vehicular communications. Because a GPS module can not provide very accurate information, the error correction capabilities of this method are limited. Nevertheless, it is considered a valuable tool for verifying the correctness of platoon operation.

8.3.1 Implementation

As with double anchoring, this function is implemented in the ECU of the vehicles. The flowchart in figure 8.9 outlines the operations taking place.

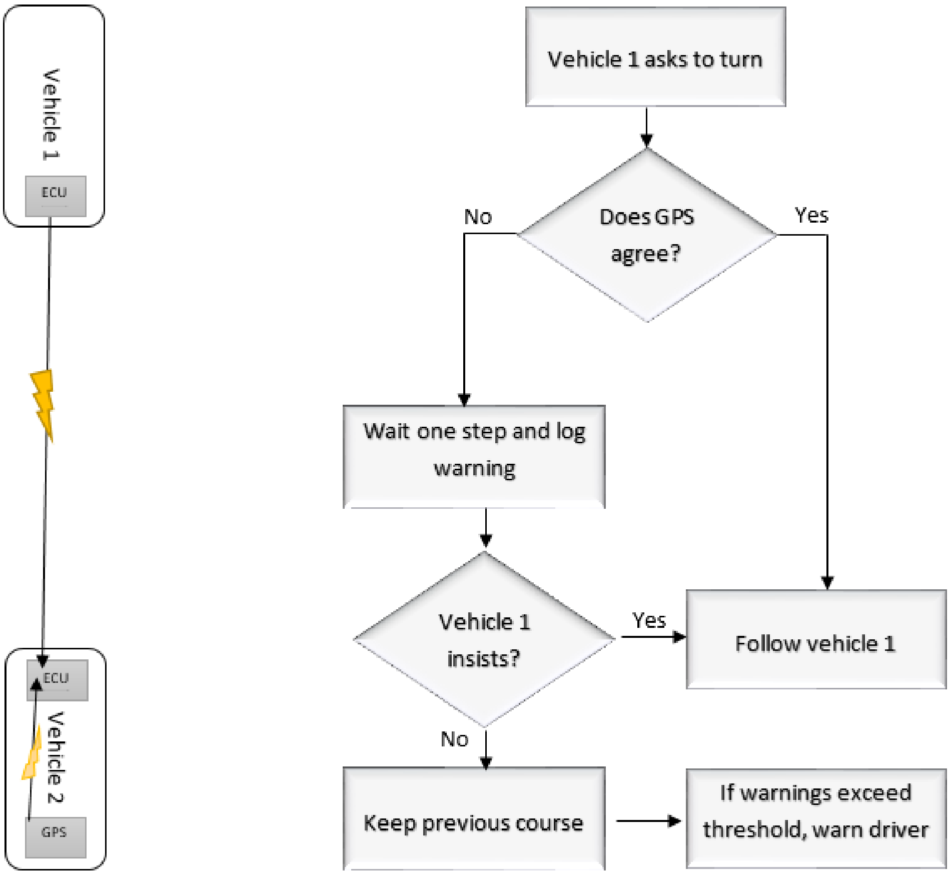


Figure 8.9: GPS verification flowchart

In this setup, data from the GPS and map is collected and compared with data received from the preceding vehicle. When a discrepancy is detected between the map data and the vehicle course (e.g. when the vehicle requests a turn but map data indicates that the road does not contain a change of course in the immediate vicinity), the decision is delayed for a step and the data from two time-steps are compared. If the discrepancy is corrected by the second time-step, the first-step data is discarded. If the discrepancy persists, then the GPS data is ignored but a warning is generated to the driver and the whole platoon. Effectively this is a two-out-of-three voting scheme, with the two votes being the current and previous time-step and the third vote being the GPS data.

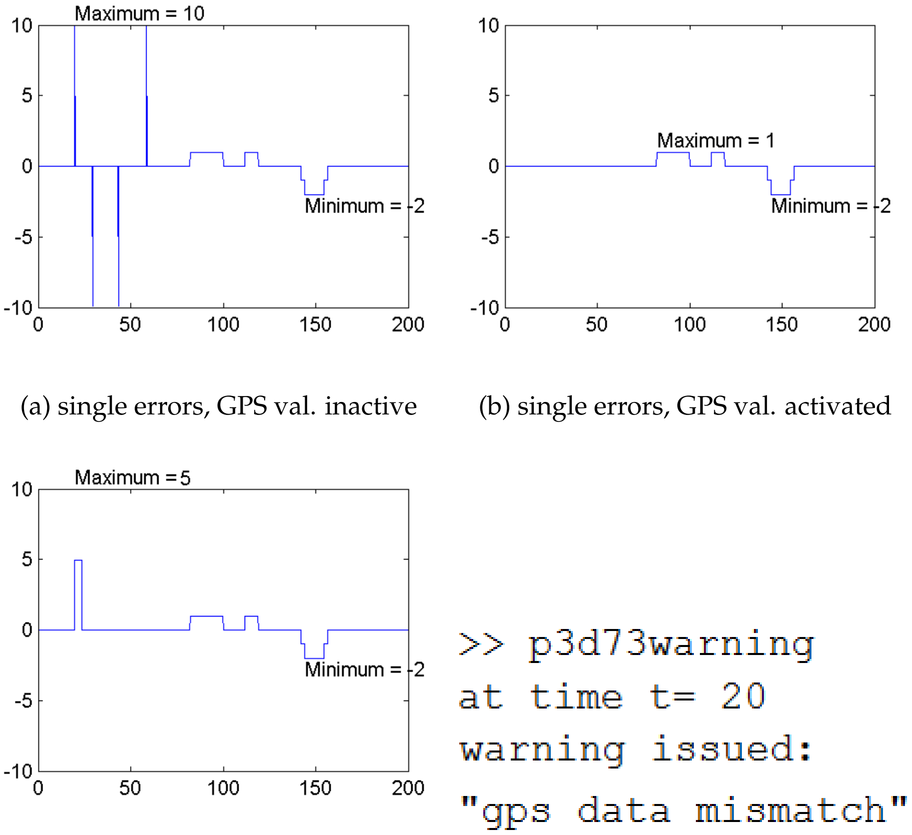
8.3.2 Results

For the scenarios analysed here, errors were forced rather than created by random interference. This approach was selected to create a controlled interference environment where this defence could have a measurable effect. This would be able to be tested in the current attack scenarios with measurable effects if the time steps were smaller and an e.g. 4-out-of-6 voting system was used. However there are limitations with the current simulator set-up, the use of large time-steps and the buffering procedure. Waiting for more time-steps for multiple votes would compromise vehicular safety. Nevertheless, the layout of the simulator would allow these changes to be easily implemented in the future.

A change of course is achieved by changing the acceleration of a vehicle. This is the primary parameter that GPS verification monitors. In figure 8.10 the lateral acceleration of a vehicle is shown in different scenarios. In all the scenarios the vehicle is presented with sudden lateral accelerations. This is manually generated to test the effectiveness of GPS verification. In scenarios (a) and (b), the accelerations are simple errors, that are corrected on the next time-step. In scenario (c), the acceleration is persistent meaning that it is either a persistent error or a valid request for a sudden change of course (e.g. evasion of an obstacle). In the first scenario (see figure 8.10a) GPS verification is inactive while in the second (see figure 8.10b) and third (see figure 8.10c) it is activated.

As can be seen in the figures, with GPS verification inactive (figure 8.10a), any acceleration input is immediately accepted, as there is no way of inferring whether it is valid or simply the result of a network error. This would in the best case be a cause of discomfort to the passengers of the vehicle. More importantly, it would be a serious safety issue as it would destabilize the vehicle and the platoon.

When GPS verification is activated (figure 8.10b) one-step changes in course that are not in agreement with the map data are voted off and so are presumed to be erroneous and ignored. Nevertheless, a warning is logged. When the warnings exceed a threshold, the driver and the platoon are alerted (see figure 8.10d). When the acceleration input is persistent and consistent in its values, it is presumed to be valid and performed as requested (figure 8.10c)). A warning is again generated, alerting the driver and the platoon of the GPS data mismatch.



```
>> p3d73warning
at time t= 20
warning issued:
"gps data mismatch"
```

(a) single errors, GPS val. inactive

(b) single errors, GPS val. activated

(c) persistent error, GPS val. activated

(d) persistent error warning

Figure 8.10: GPS verification scenarios

8.3.3 Conclusion

GPS verification was implemented and manually tested (errors were forced rather than created randomly by interference). It was demonstrated that simple errors can be successfully mitigated based on GPS and map data readily available to any vehicle capable of being a member of a platoon. With the further improvements discussed above this would be an invaluable method of increasing resistance to interference. Even in this stage however, it proved very useful in error correction and pre-emptive warning.

As with double anchoring (see chapter 8.2) this method introduces a one-step delay to the response time of the vehicles. In this simulations the time-step is 100 milliseconds which is a considerable amount of time when vehicles are moving at high speeds. This is however much faster than any human operator would be able to react. Additionally, in a real-world application the time-step will presumably be even orders of magnitude smaller, making the response time almost instantaneous.

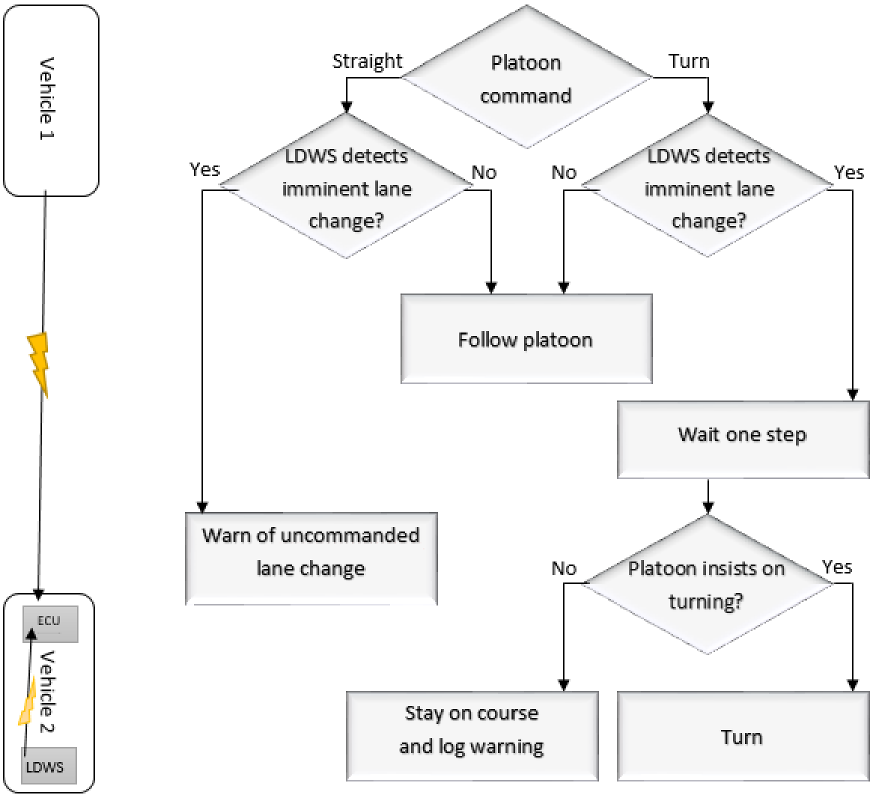
8.4 On-board sensors verification

There are several technologies designed to monitor the state of a vehicle through on-board sensors and provide comfort and safety. In this section, a Lane Departure Warning System (LDWS) is simulated and its usefulness in a vehicle platoon encountering interference is examined.

As with GPS verification (see section 8.3) this will provide an independent system to monitor the state of the vehicle that is not subject to the same type of interference as inter-vehicular communications. LDWS was selected because it is representative of similar technologies being developed aimed at vehicle monitoring and it is already widely offered by manufacturers. Because it is examined in isolation and in a simplified way the error correction capabilities of this method are limited. Nevertheless, it is considered a valuable tool for verifying the correctness of platoon operation. Moreover conclusions drawn from these tests can help envision the usefulness of similar technologies, either used independently or in combination with GPS and LDWS.

8.4.1 Implementation

As with double anchoring and GPS verification, this function is implemented in the ECU of the vehicles. The flowchart in figure 8.11 outlines the operations taking place.



Vehicle 1
ECU
Vehicle 2
LDWS
Platoon command
Straight
Turn
LDWS detects imminent lane change?
Yes
No
LDWS detects imminent lane change?
No
Yes
Follow platoon
Wait one step
Warn of uncommanded lane change
Platoon insists on turning?
No
Yes
Stay on course and log warning
Turn

Figure 8.11: Lane Departure Warning System flowchart

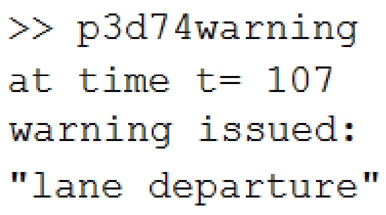
In this setup, data from the LDWS is collected and compared with data received from the preceding vehicle. This includes information from the system's sensors (video, laser or infra-red, depending on the implementation) and acceleration data. Based on this information, LDWS can detect imminent lane changes before they happen. Because a platoon will mostly operate on the same lane, when the LDWS is triggered, a warning is logged and the movement is delayed for one time-step. The data from the next time-step is compared and if it agrees with the previous, the vehicle follows through and a lane change is initiated. If however the data has changed and a lane change is no longer requested, it is assumed that the lane change was uncommanded because of erroneous data. In this case the data is discarded and the error is avoided.

Specifically for the case when the vehicle is travelling in a straight line, only a warning is issued because the vehicle can not decide on the correct turn without input from the platoon. This is because this scenario is based on a simple implementation of an LDWS that can only issue warnings. In future versions it would be possible to implement a more advanced system with lane following capabilities.

8.4.2 Results

As in section 8.3, to test this method, a simplified scenario was run. In this scenario, errors were forced rather than created by random interference. This was done because the fully functional LDWS was not implemented in code as it is outside the scope of the current work. Instead, a simulated LDWS input was created and tested against these controlled, forced errors.

In the example of the scenario of an uncommanded lane change while the platoon is travelling at a straight line, the system did indeed identify the discrepancy and logged a warning, as expected (see figure 8.12).



```
>> p3d74warning
at time t= 107
warning issued:
"lane departure"
```

Figure 8.12: Lane Departure Warning

8.4.3 Conclusion

On-board sensors verification was implemented and manually tested (errors were forced rather than created randomly by interference). It was demonstrated that simple errors can be successfully mitigated based on systems utilizing on-board sensors, readily available to any vehicle capable of being a member of a platoon. Even with the simple setup tested in this section, it proved very useful in error correction and pre-emptive warning.

As with double anchoring (see chapter 8.2) and GPS verification (see chapter 8.3) this method introduces a one-step delay to the response time of the vehicles. In this simulations the time-step is 100 milliseconds which is a considerable amount of time when vehicles are moving at high speeds. This is however much faster than any human operator would be able to react. Additionally, in a real-world application the time-step will presumably be even orders of magnitude smaller, making the response time almost instantaneous.

Despite this delay, this method provides a net benefit for platoon safety. Similar sensors now commonly found in many cars can be combined in a similar way to provide even stronger error correction and warnings. Such sensors could include front and rear radars, infra-red cameras and road sign detectors. In the future this category could be expanded to include systems that may allow identification, localization and characterization of other platoons and vehicles on the road.

Part III

Conclusion

Vehicular networks have the potential of being one of the most important applications of Ad hoc networking. The scale and special nature of such a network presents several challenges in regards to communications and security that need to be addressed in this new perspective.

In a vehicle platoon, safety is the primary consideration. There is need for a resilient Vehicular Ad hoc Network (VANET) in the presence of interference and other potential problems that induce errors in the communication process. This can be achieved by conventional anti-jamming techniques as well as exploitation of the special nature of this specific application (use of on-board sensors, monitoring the state of the VANET members, independent of the network state).

There is a need for a simple and expandable simulator that can take into account the multiple variables in this application.

The following chapters examine the main conclusions of this work, how it addresses the issues raised by the literature review and how it meets the objectives initially set in chapter 2. Namely chapter 9 summarizes the development of the proposed simulator, chapter 10 summarizes the defences implemented and tested to enhance VANET resilience to interference and chapter 11 summarizes the potential areas of future development for this project.

Chapter 9

Model

Using MATLAB and Simulink, a model was created to simulate a number of aspects of a vehicle platoon:

- the **physical operation of the platoon**

  This includes the independent operation of vehicles as well as their ability to follow other vehicles based on data from the network

- the **operation of the Vehicular Ad hoc Network (VANET)**

  Transmission and reception through the wireless medium, communication protocols etc.

- **possible interference to the wireless communication**

  Physical and network simulation of interference sources (static or mobile)

- the **effect of interference on the VANET and the platoon**

  Examination of the physical operation as well as the performance of the network under the effects of interference

The choice to create a new simulation environment was made after a survey of the existing solutions. It was decided that a platform incorporating both the physical and the network aspect of the simulation in a simple solution would be sufficient for this project and an opportunity to better understand the workings of both aspects. It is also the hope of the author that it will attract further development beyond the scope of this project.

The environment consists of two main parts. The simulator itself and the post-processing suite (P3D) used to analyse and display simulation data.

Any number of vehicles can be simulated. In this project 4 vehicles were used, a leader and three followers. This number was selected to allow the examination of dynamic correlations between the vehicles: with four vehicles, there can be a lead vehicle, two intermediate vehicles (if the interaction between intermediate vehicles needs to be examined), and one end vehicle.

On-board sensors can be simulated on a basic level with ease. In this project a GPS module was implemented as well as a Lane Departure Warning System to demonstrate the principal of using on-board sensor verification.

The network simulation is independent to the vehicles. This allows for plugging in different communication protocols simulated in MATLAB/Simulink or exporting of vehicle data to a separate network simulator.

The post-processing suite is easily configurable to present any data generated by the simulator. It incorporates an animation function, providing comprehensive presentation of the platoon's operation.

The whole platform can be used, expanded and modified appropriately to address future projects on the subject of vehicular networks.

Several validation profiles were used to demonstrate the simulator's operation and ability of simulating the needed scenarios. The theoretically expected results were verified using P3D.

Given the construction of this novel simulation environment and its successful use in action, it is the hope of the author that it may be used and developed further in the future and form the basis for further research into the subject.

Chapter 10

Defences

Using the newly developed simulator, a number of jamming attacks were implemented:

- **Stationary jammer**

  A jammer with varying transmission power is placed along the route of the platoon

- **Mobile jammer**

  A jammer with varying transmission power tracks the platoon leader throughout its route

Based on the initial findings and the literature review, defence methods were implemented and examined:

- **Beamforming**

  manipulation of the transmit/receive beam of the vehicles based on the vehicles' and interference sources' positions allows great improvements to the Signal-to-Noise ratio

- **Double anchoring**

  vehicles can communicate with and use movement data from multiple members of the platoon to verify their state and the validity of received information

- **Global Positioning System verification**

  vehicles can use their GPS module to verify their state and validity of received information

- **On-board sensor verification**

  vehicles can use their various on-board sensors to verify their state and validity of received information. As an example of an on-board system, a Lane Departure Warning System was simulated

The defences were examined independently and in combination. The results were encouraging in all cases and showed great potential for mitigating interference.

Beamforming in its simple form successfully defended against low power attacks on a single link but was not sufficient against more advanced or powerful attacks. An improvement that allowed the beam to be sharpened it the presence of high interference, gave promising results. The platoon was able to resist stronger attacks, and be more stable than before. Even the strongest attack was unsuccessful in breaking the platoon, even though it tested this defence method to its limits.

Double anchoring successfully defended against low power attacks but presented some shortcomings and was not sufficient on its own to defend against high power attacks. This method cannot be applied to the first two vehicles of the platoon which leaves the first link vulnerable to jamming. Combined with beamforming however the results were very promising. The platoon was able to resist to stronger attacks, and be more stable than either of the techniques used independently. With beam sharpening, the platoon was able to resist all of the attacks implemented with relative ease.

GPS verification demonstrated that simple errors can be successfully mitigated based on GPS and map data, readily available to any vehicle capable of being a member of a platoon. It proved very useful in error correction and pre-emptive warning and is open to future improvement.

On-board sensors verification demonstrated that simple errors can be successfully mitigated based on systems utilizing on-board sensors, readily available to any vehicle capable of being a member of a platoon. It proved very useful in error correction and pre-emptive warning and is open to future improvement.

Chapter 11

Future Work

The project has been successful in the goals set in chapter 2 and also opens the possibility of expanding on the developed simulation environment to examine scenarios of increasing complexity. The following proposals could be considered for future work:

- The physical model to simulate the vehicle motions has been constructed to a level sufficient for the predetermined scenarios used in this project.
- While the model is already customizable, future work could include improvements to the physical model to accommodate easier customization of the simulation parameters. This could include modelling based on the true bearing and velocity of the vehicle, compared to the use of Cartesian acceleration and coordinates used here.
- A user friendly interface for defining vehicle, interferer, network profiles and other parameters of the simulation would be desirable. Ideally, a GUI should be used to define all the simulation parameters at the start of each run.
- At present, simulation data and errors are manually recorded after each run, using MATLAB error messages and the P3D suite. This could be automated in the future, to create logs of each run's data and any errors or warnings. P3D could be integrated with the simulator to allow run-time monitoring of the simulation and intuitive use. In the future, run-time configuration (man-in-the-loop) could be implemented to introduce infinite scenarios.
- Some parameters are statically defined by the user for the predetermined scenarios in this project. All parameters should be exposed in future versions to allow the dynamic simulation of more scenarios.
- In this project beamforming is only applied on the transmitter side. Receiver beamforming can be easily added implemented.
- Given the customizability of this platform, multiple platoons, independent vehicles, traffic modelling, road modelling, free will, communication protocols

- In this project, a single platoon was examined. In future iterations inter platoon communication and interaction modes could be implemented and tested.
- More attacks scenarios can be implemented, possibly combining multiple stationary and mobile jammers with various jamming profiles.
- More defence mechanisms can be implemented and more on-board systems can be integrated and realistically modelled.

Bibliography

[1] IEEE Standards Association et al. '802.11 p- 2010-IEEE Standard for Information Technology-Local and Metropolitan Area Networks-Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access In Vehicular Environments'. In: *URL http://standards. ieee. org/findstds/standard/802.11 p-2010. html* ().

[2] Robert G Bill and William F Herrnkind. 'Drag reduction by formation movement in spiny lobsters'. In: *Science* 193.4258 (1976), pp. 1146–1148.

[3] ETSI. *The European Telecommunications Standards Institute*. URL: http://www.etsi.org.

[4] J Eyre, D Yanakiev and I Kanellakopoulos. *String stability properties of AHS longitudinal vehicle controllers*. Tech. rep. 1997.

[5] Joseph A Fernandez et al. 'Performance of the 802.11 p physical layer in vehicle-to-vehicle environments'. In: *Vehicular Technology, IEEE Transactions on* 61.1 (2012), pp. 3–14.

[6] Formation flying. *An Introduction to Beamforming*. URL: http://www.britannica.com/EBchecked/topic/1403296/formation-flying.

[7] Raphaël Frank et al. 'Bluetooth Low Energy: An alternative technology for VANET applications'. In: *Wireless On-demand Network Systems and Services (WONS), 2014 11th Annual Conference on*. IEEE. 2014, pp. 104–107.

[8] Andrew A. Ganse. *An Introduction to Beamforming*. URL: http://staff.washington.edu/aganse/beamforming/beamforming.html.

[9] Sumit K Ghosh and Tony S Lee. *Intelligent transportation systems: smart and green infrastructure design*. Vol. 44. CRC PressI Llc, 2010.

[10] Jason J Haas. 'The Effects of Wireless Jamming on Vehicle Platooning'. In: (2009).

[11] Jason J Haas, Yih-Chun Hu and Kenneth P Laberteaux. 'Real-world VANET security protocol performance'. In: *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*. IEEE. 2009, pp. 1–7.

[12] Hannes Hartenstein and Kenneth Laberteaux. *VANET: vehicular applications and inter-networking technologies*. Vol. 1. Wiley Online Library, 2010.

[13] Dietrich Hummel. 'Aerodynamic aspects of formation flight in birds'. In: *Journal of theoretical biology* 104.3 (1983), pp. 321–347.

[14] IEEE. *IEEE Intelligent Transportation Systems Society*. URL: http://sites.ieee.org/itss/.

[15] ISO. *ISO/TC 204 Intelligent transport systems*. URL: http://www.iso.org/iso/iso_technical_committee?commid=54706.

[16] Kristian Karlsson, Carl Bergenhem and Erik Hedin. 'Field Measurements of IEEE 802.11 p Communication in NLOS Environments for a Platooning Application'. In: *Vehicular Technology Conference (VTC Fall), 2012 IEEE*. IEEE. 2012, pp. 1–5.

[17] G Kiokes, A Amditis and NK Uzunoglu. 'Simulation-based performance analysis and improvement of orthogonal frequency division multiplexing-802.11 p system for vehicular communications'. In: *Intelligent Transport Systems, IET* 3.4 (2009), pp. 429–436.

[18] Timo Kosch et al. *Automotive Inter-networking*. Vol. 3. Wiley. com, 2012.

[19] Uwe Kucharzyk. 'Requirements for wireless technology on rolling stock'. In: *Communication Technologies for Vehicles*. Springer, 2011, pp. 1–10.

[20] PBS Lissaman and Carl A Shollenberger. 'Formation flight of birds'. In: *Science* 168.3934 (1970), pp. 1003–1005.

[21] Xiangheng Liu et al. 'Effects of communication delay on string stability in vehicle platoons'. In: *Intelligent Transportation Systems, 2001. Proceedings. 2001 IEEE*. IEEE. 2001, pp. 625–630.

[22] C Siva Ram Murthy and BS Manoj. *Ad hoc wireless networks: Architectures and protocols*. Pearson education, 2004.

[23] Simeon Andrew Ning. *Aircraft drag reduction through extended formation flight*. Stanford University, 2011.

[24] *on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport*. 2010.

[25] Sinan Öncü et al. 'String stability of interconnected vehicles under communication constraints.' In: *CDC*. 2012, pp. 2459–2464.

[26] Al-Sakib Khan Pathan. *Security of self-organizing networks: MANET, WSN, WMN, VANET*. Taylor & Francis, 2010.

[27] Konstantinos Pelechrinis, Marios Iliofotou and Srikanth V Krishnamurthy. 'Denial of service attacks in wireless networks: The case of jammers'. In: *Communications Surveys & Tutorials, IEEE* 13.2 (2011), pp. 245–257.

[28] Konstantinos Pelechrinis, Christos Koufogiannakis and Srikanth V Krishnamurthy. 'Gaming the jammer: Is frequency hopping effective?' In: *Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, 2009. WiOPT 2009. 7th International Symposium on*. IEEE. 2009, pp. 1–10.

[29] Konstantinos Pelechrinis et al. 'ARES: an anti-jamming reinforcement system for 802.11 networks'. In: *Proceedings of the 5th international conference on Emerging networking experiments and technologies*. CoNEXT '09. Rome, Italy: ACM, 2009, pp. 181–192. ISBN: 978-1-60558-636-6. DOI: 10.1145/1658939.1658960. URL: http://doi.acm.org/10.1145/1658939.1658960.

[30] L Peppard. 'String stability of relative-motion PID vehicle control systems'. In: *Automatic Control, IEEE Transactions on* 19.5 (1974), pp. 579–581.

[31] Richard Poisel. *Modern Communications Jamming: Principles and Techniques*. Artech House, 2011.

[32] YangQuan Chen Pooja Kavathekar. 'DRAFT: VEHICLE PLATOONING: A BRIEF SURVEY AND CATEGORIZATION'. In: *Proceedings of The ASME International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*. Ed. by test. 2011.

[33] The SARTRE Project. *Safe Road Trains for the Environment*. URL: http://www.sartre-project.eu/.

[34] Oscar Puñal, Ana Aguiar and James Gross. 'In VANETs we trust?: characterizing RF jamming in vehicular networks'. In: *Proceedings of the ninth ACM international workshop on Vehicular inter-networking, systems, and applications*. ACM. 2012, pp. 83–92.

[35] D Swaroop and JK Hedrick. 'String stability of interconnected systems'. In: *Automatic Control, IEEE Transactions on* 41.3 (1996), pp. 349–357.

[36] Tushar Tank and J-PMG Linnartz. 'Vehicle-to-vehicle communications for AVCS platooning'. In: *Vehicular Technology, IEEE Transactions on* 46.2 (1997), pp. 528–536.

[37] Rodney Teo, DM Stipanovic and CJ Tomlin. 'Decentralized spacing control of a string of multiple vehicles over lossy datalinks'. In: *Decision and Control, 2003. Proceedings. 42nd IEEE Conference on*. Vol. 1. IEEE. 2003, pp. 682–687.

[38] Marc Torrent-Moreno et al. 'Vehicle-to-vehicle communication: fair transmit power control for safety-critical information'. In: *Vehicular Technology, IEEE Transactions on* 58.7 (2009), pp. 3684–3703.

[39] Ling-yun Xiao and Feng Gao. 'Effect of information delay on string stability of platoon of automated vehicles under typical information frameworks'. In: *Journal of Central South University of Technology* 17 (2010), pp. 1271–1278.

[40] Wenyuan Xu et al. 'Jamming sensor networks: attack and defense strategies'. In: *Network, IEEE* 20.3 (2006), pp. 41–47.

[41] Wenyuan Xu et al. 'Jamming sensor networks: attack and defense strategies'. In: *Network, IEEE* 20.3 (2006), pp. 41–47.

[42] Jijun Yin et al. ‘Performance evaluation of safety applications over DSRC vehicular ad hoc networks’. In: *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. ACM. 2004, pp. 1–9.

[43] Sherali Zeadally et al. ‘Vehicular ad hoc networks (VANETS): status, results, and challenges’. In: *Telecommunication Systems* 50.4 (2012), pp. 217–241.

Appendices

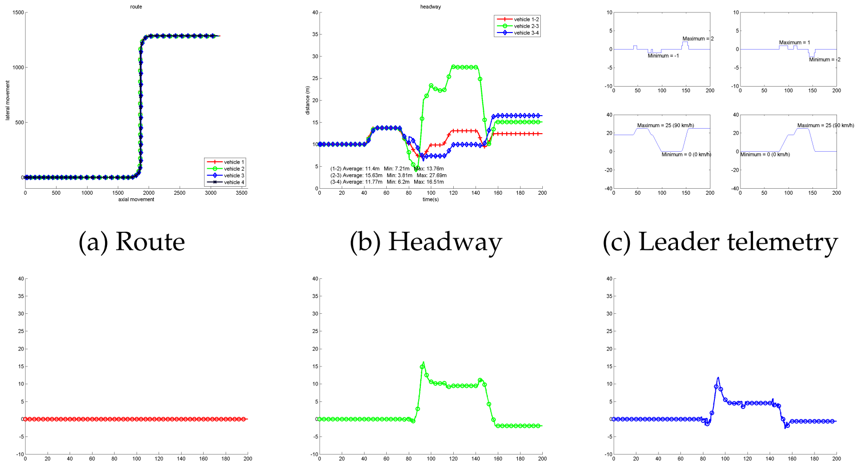
Appendix A

Supplementary figures

This appendix contains additional figures created by P3D as a result of several different simulation runs. As the full number of figures and simulation runs is too large to be distributed on paper, only key figures have been included:

- Vehicles route (sensors)
- Vehicles headway (sensors)
- Leader telemetry (sensors)
- Declination (vehicles 2, 3 and 4)

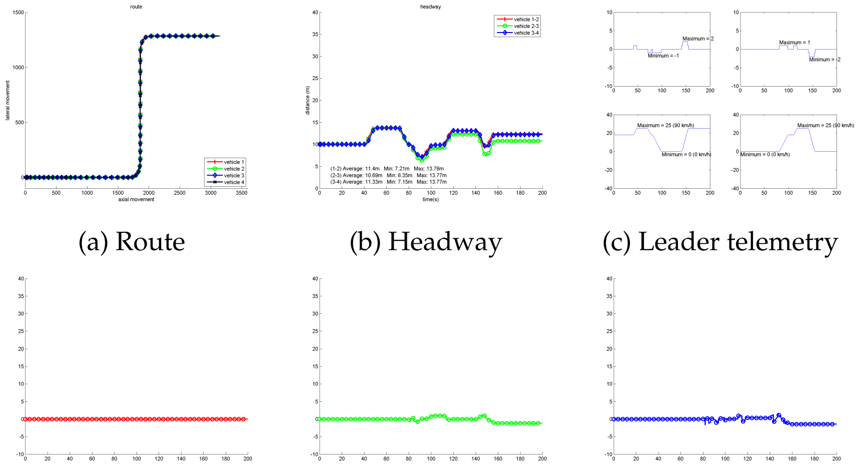
More figures are electronically available upon request.



(a) Route (b) Headway (c) Leader telemetry

(d) Declination (veh. 2) (e) Declination (veh. 3) (f) Declination (veh. 4)

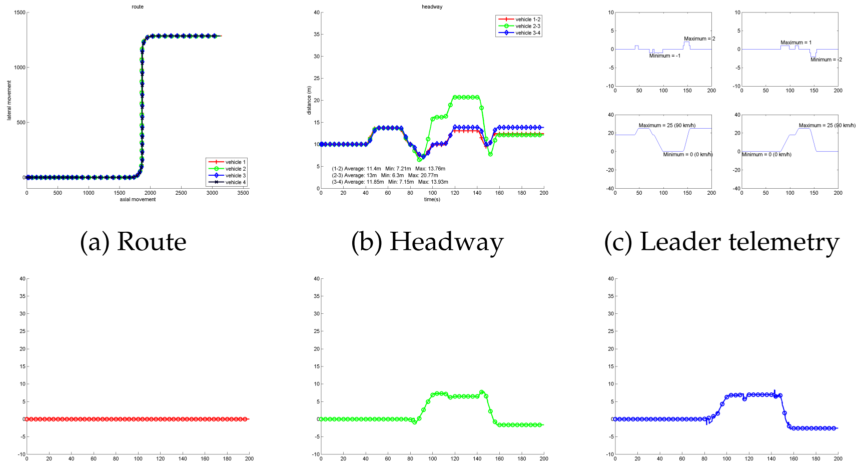
Figure A.1: Stationary jammer. Link 2 under attack. 80% power. Omnidirectional.



(a) Route (b) Headway (c) Leader telemetry

(d) Declination (veh. 2) (e) Declination (veh. 3) (f) Declination (veh. 4)

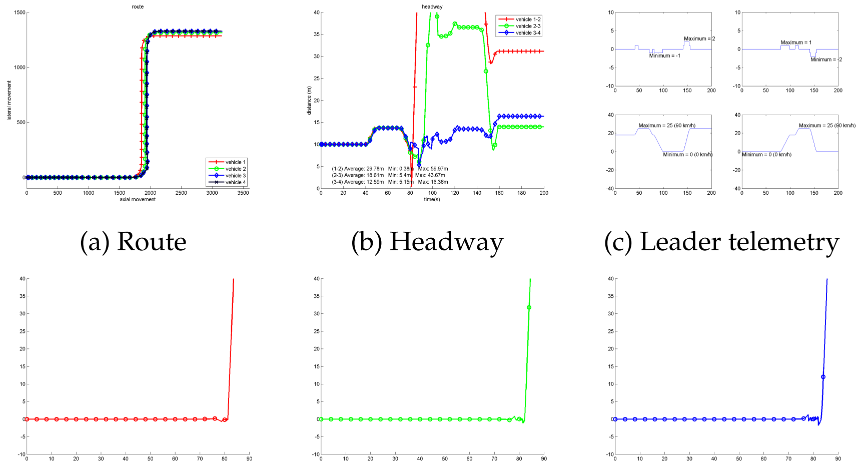
Figure A.2: Stationary jammer. Link 2 under attack. 80% power. Beamforming.



(a) Route (b) Headway (c) Leader telemetry

(d) Declination (veh. 2) (e) Declination (veh. 3) (f) Declination (veh. 4)

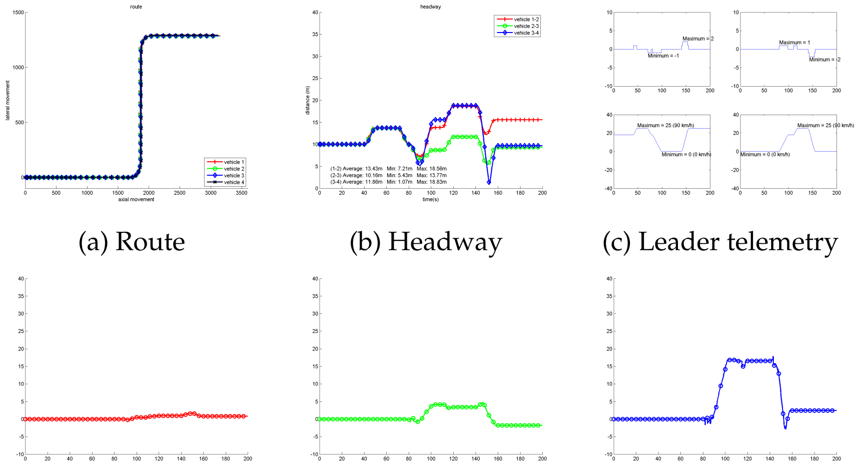
Figure A.3: Stationary jammer. Link 2 under attack. 100% power. Beamforming.



(a) Route (b) Headway (c) Leader telemetry

(d) Declination (veh. 2) (e) Declination (veh. 3) (f) Declination (veh. 4)

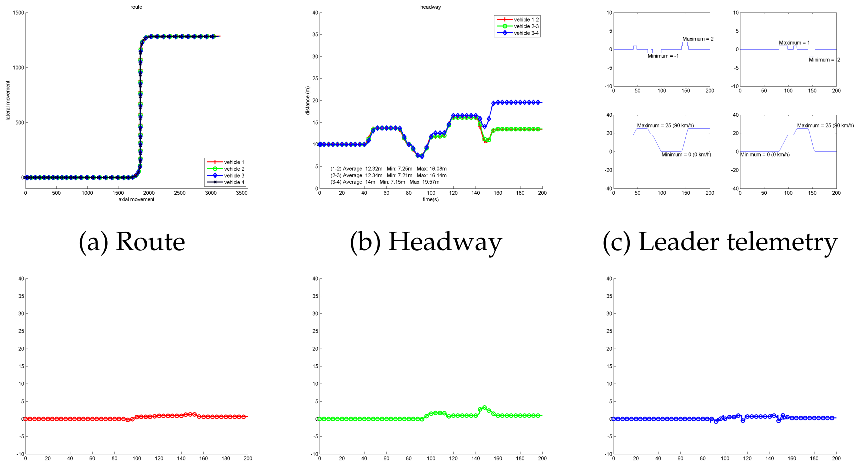
Figure A.4: Stationary jammer. All links under attack. 80% power. Omnidirectional.



(a) Route (b) Headway (c) Leader telemetry

(d) Declination (veh. 2) (e) Declination (veh. 3) (f) Declination (veh. 4)

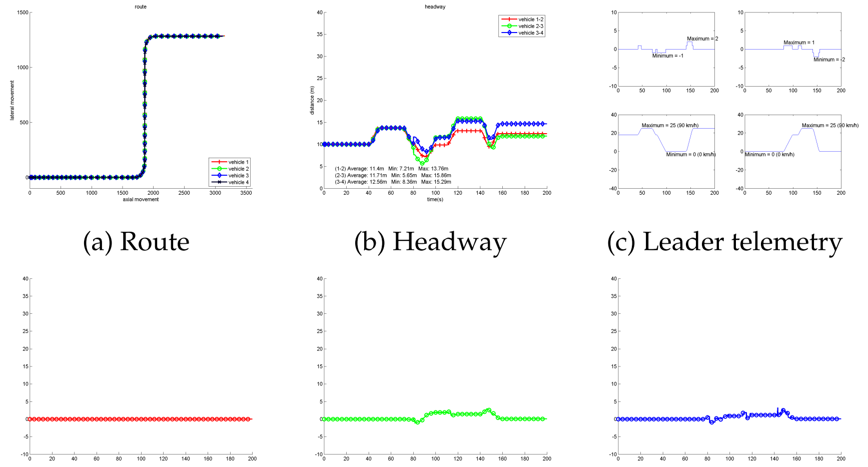
Figure A.5: Stationary jammer. All links under attack. 80% power. Beamforming.



(a) Route (b) Headway (c) Leader telemetry

(d) Declination (veh. 2) (e) Declination (veh. 3) (f) Declination (veh. 4)

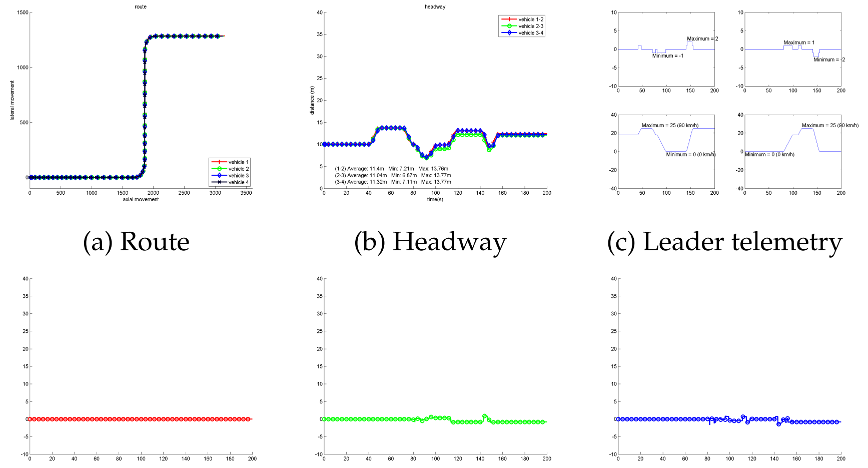
Figure A.6: Stationary jammer. All links under attack. 100% power. Beamforming with beam-sharpening.



(a) Route (b) Headway (c) Leader telemetry

(d) Declination (veh. 2) (e) Declination (veh. 3) (f) Declination (veh. 4)

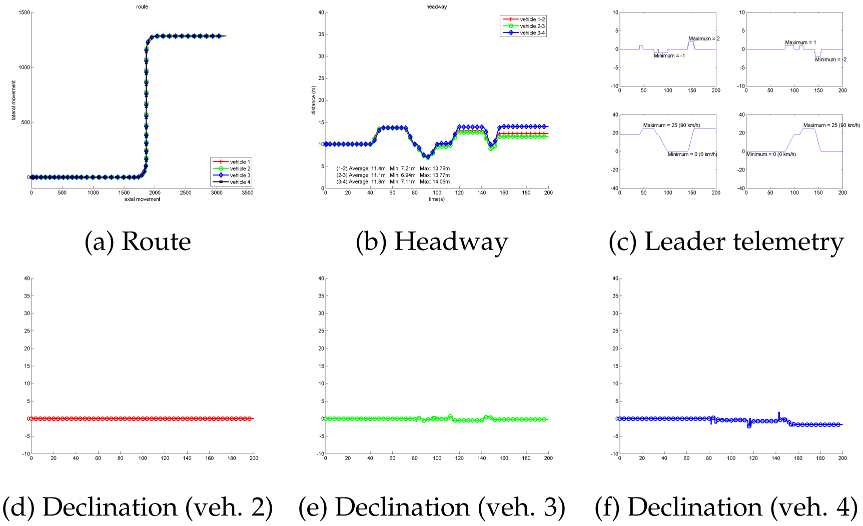
Figure A.7: Stationary jammer. Link 2 under attack. 80% power. Omnidirectional and double anchoring.



(a) Route (b) Headway (c) Leader telemetry

(d) Declination (veh. 2) (e) Declination (veh. 3) (f) Declination (veh. 4)

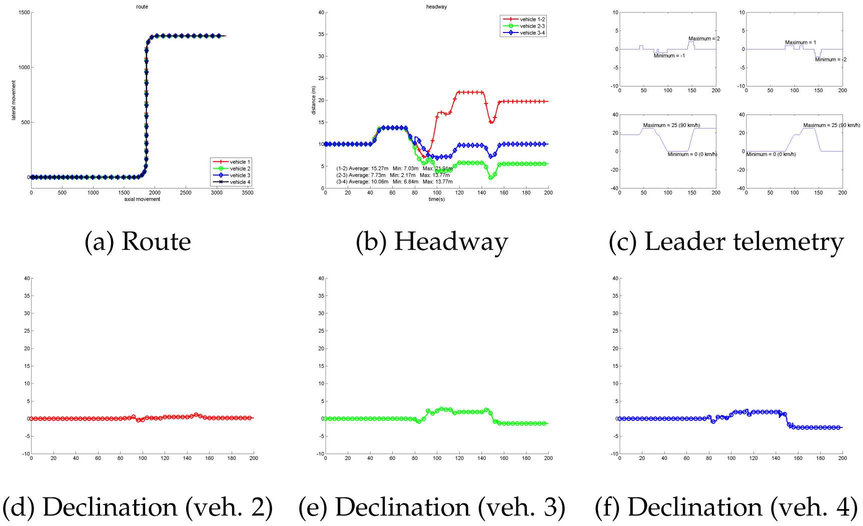
Figure A.8: Stationary jammer. Link 2 under attack. 80% power. Beamforming and double anchoring.



(a) Route (b) Headway (c) Leader telemetry

(d) Declination (veh. 2) (e) Declination (veh. 3) (f) Declination (veh. 4)

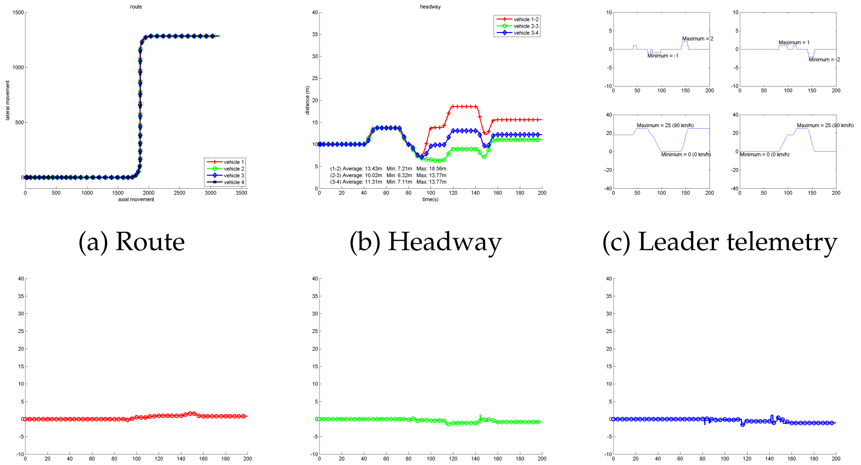
Figure A.9: Stationary jammer. Link 2 under attack. 100% power. Beamforming and double anchoring.



(a) Route (b) Headway (c) Leader telemetry

(d) Declination (veh. 2) (e) Declination (veh. 3) (f) Declination (veh. 4)

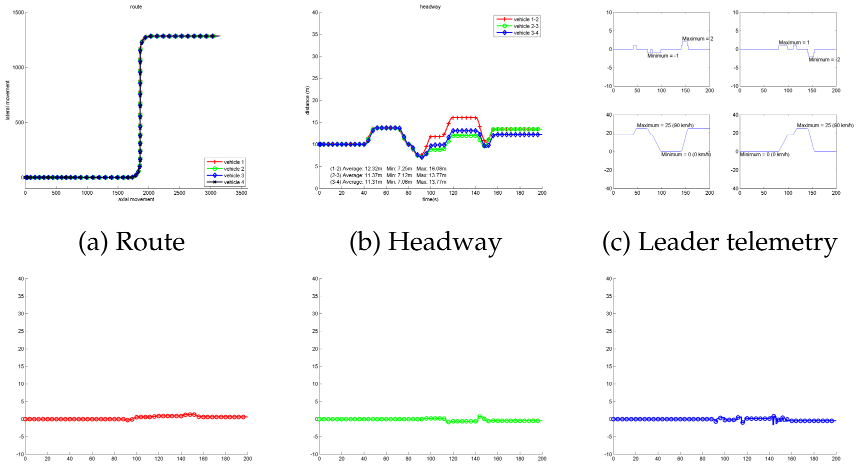
Figure A.10: Stationary jammer. All links under attack. 80% power. Omnidirectional and double anchoring.



(a) Route (b) Headway (c) Leader telemetry

(d) Declination (veh. 2) (e) Declination (veh. 3) (f) Declination (veh. 4)

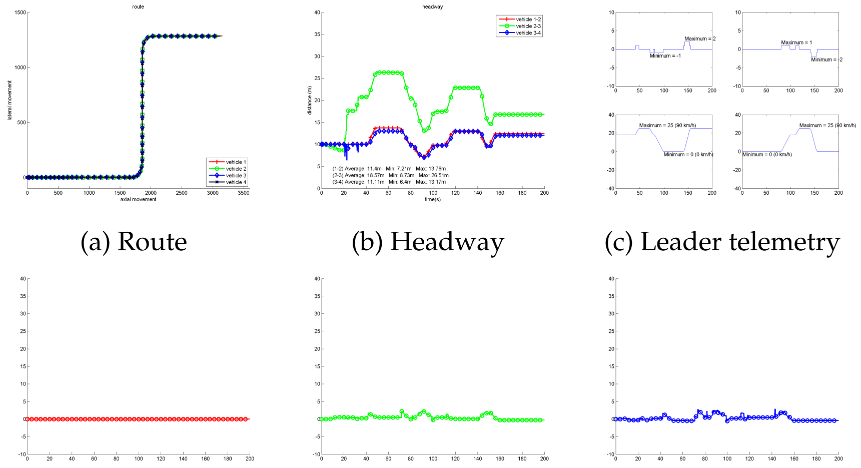
Figure A.11: Stationary jammer. All links under attack. 80% power. Beamforming and double anchoring.



(a) Route (b) Headway (c) Leader telemetry

(d) Declination (veh. 2) (e) Declination (veh. 3) (f) Declination (veh. 4)

Figure A.12: Stationary jammer. All links under attack. 100% power. Beamforming with beam-sharpening and double anchoring.



(a) Route

(b) Headway

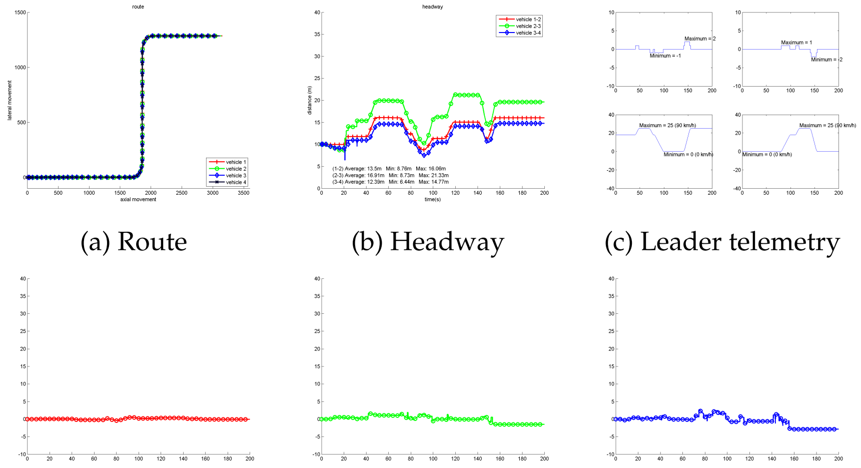
(c) Leader telemetry

(d) Declination (veh. 2)

(e) Declination (veh. 3)

(f) Declination (veh. 4)

Figure A.13: Moving jammer. Link 2 under attack. 80% power. Beamforming.



(a) Route

(b) Headway

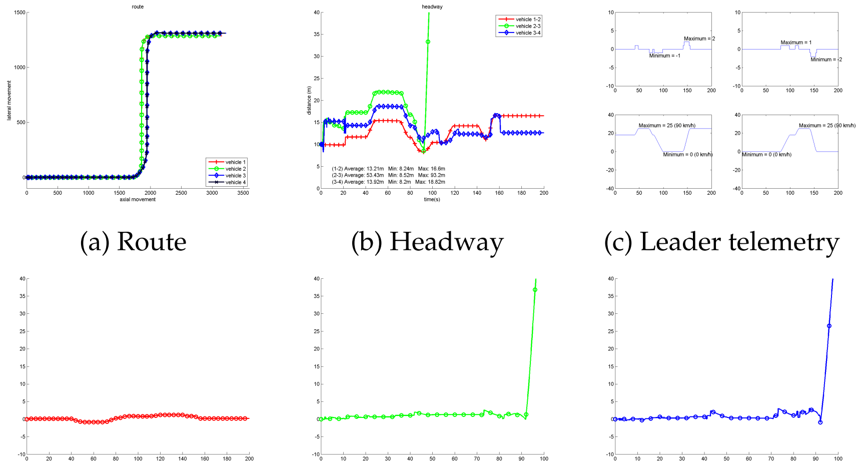
(c) Leader telemetry

(d) Declination (veh. 2)

(e) Declination (veh. 3)

(f) Declination (veh. 4)

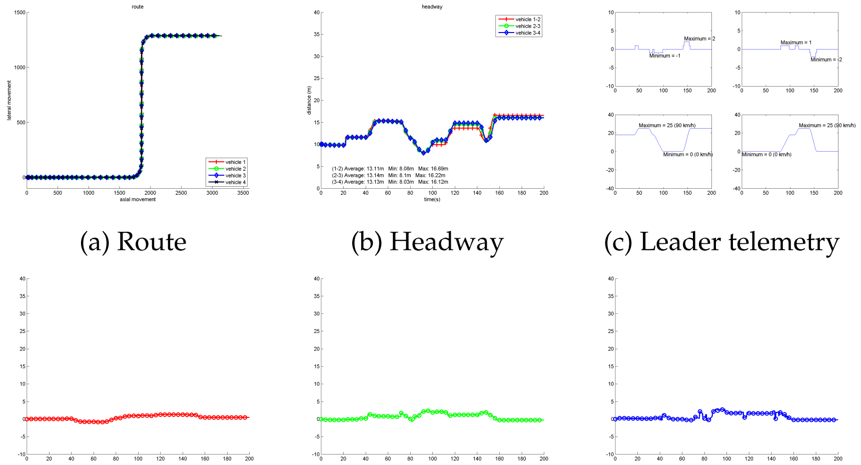
Figure A.14: Moving jammer. All links under attack. 80% power. Beamforming.



(a) Route (b) Headway (c) Leader telemetry

(d) Declination (veh. 2) (e) Declination (veh. 3) (f) Declination (veh. 4)

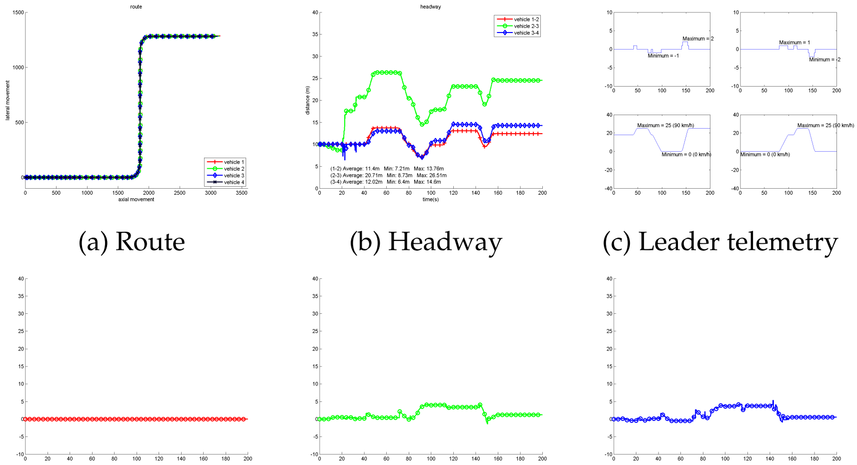
Figure A.15: Moving jammer. All links under attack. 100% power. Beamforming.



(a) Route (b) Headway (c) Leader telemetry

(d) Declination (veh. 2) (e) Declination (veh. 3) (f) Declination (veh. 4)

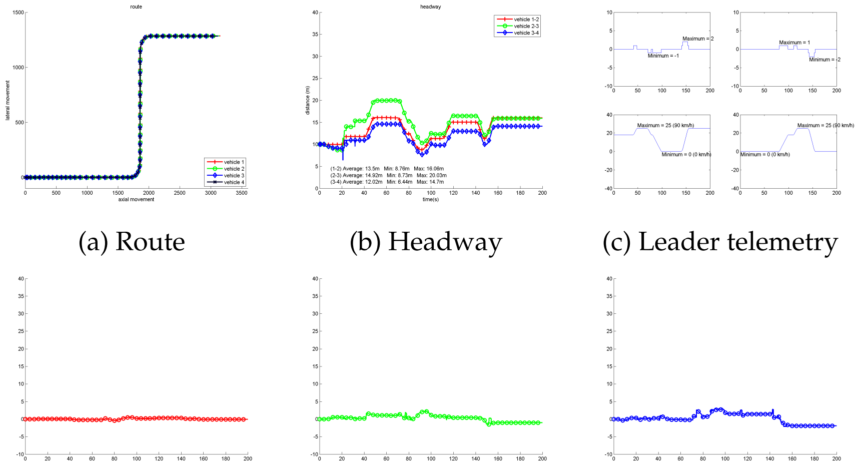
Figure A.16: Moving jammer. All links under attack. 100% power. Beamforming with beam-sharpening.



(a) Route (b) Headway (c) Leader telemetry

(d) Declination (veh. 2) (e) Declination (veh. 3) (f) Declination (veh. 4)

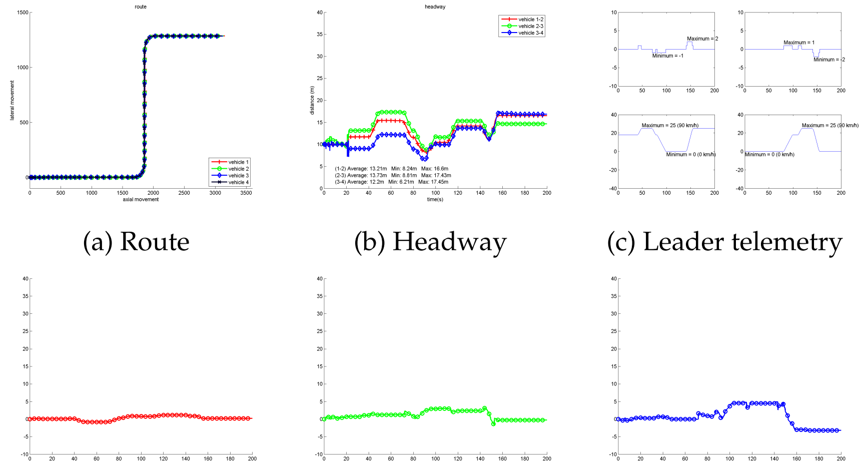
Figure A.17: Moving jammer. Link 2 under attack. 80% power. Beamforming and double anchoring.



(a) Route (b) Headway (c) Leader telemetry

(d) Declination (veh. 2) (e) Declination (veh. 3) (f) Declination (veh. 4)

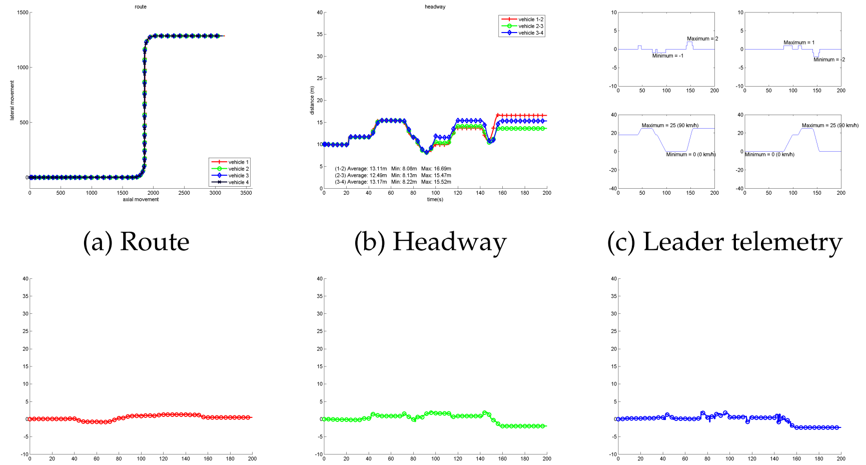
Figure A.18: Moving jammer. All links under attack. 80% power. Beamforming and double anchoring.



(a) Route (b) Headway (c) Leader telemetry

(d) Declination (veh. 2) (e) Declination (veh. 3) (f) Declination (veh. 4)

Figure A.19: Moving jammer. All links under attack. 100% power. Beamforming and double anchoring.



(a) Route (b) Headway (c) Leader telemetry

(d) Declination (veh. 2) (e) Declination (veh. 3) (f) Declination (veh. 4)

Figure A.20: Moving jammer. All links under attack. 100% power. Beamforming with beam-sharpening and double anchoring.