IoT Transport and Mobility Demonstrator

Cyber Security Testing on National Infrastructure

Carsten Maple and Matthew Bradbury
(CM@warwick.ac.uk, M.Bradbury@warwick.ac.uk)

May 2019

Research Undertaken By

Research Funded By

In Collaboration With

Supported By

Cite this document as:

Carsten Maple, Matthew Bradbury, Haitham Cruickshank, Hu Yuan, Chen Gu, and Phillip Asuquo. IoT Transport and Mobility Demonstrator: Cyber Security Testing on National Infrastructure. Technical Report Version 1.0, University of Warwick, May 2019

Abstract

With the intent for Connected Autonomous Vehicles (CAVs) to be deployed on UK roads in the near future it is vital that they are rigorously tested. Part of this testing will involve the cyber security aspects of these vehicles. This report covers the technical aspects of the IoT-TRaM project, which deployed four cyber security and privacy innovations developed within PETRAS in real world environments. This report describes (i) the four academic innovations, (ii) the requirements and experiences of CAV testbed users and (iii) testbed sites and the protocols for researchers to perform cyber security testing there. Throughout the report recommendations are made to reduce the barriers of entry and ways to improve the experience of performing cyber security testing in real world environments.

Recommendations Summary

As the state of the UK's testing facilities is still in development, this section offers a high level overview of the recommendations made in this report.

For Testbeds

- Focus on deploying communication infrastructure (such as IEEE 802.11p ITS-G5 or 5G cellular) as security testing will involve vehicular communications.
- Aim for testing to be simple:
  - Allow new binaries to be remotely deployed to hardware in the field.
  - Allow logs from devices to be remotely gathered (preferably in realtime, but offline also acceptable).
  - (Possibly) Provide a service in which researchers do not need to visit the testbed for their security testing to be performed.
- Details of licences obtained from Ofcom should be made publicly available, to inform researchers and industry of the testing that can be legally performed on site.
- The types of attacks that can be tested at different testbeds needs to be clearly specified. It is also important to have a subset of testbeds able to accommodate testing attacks such as GNSS jamming or DoS. It is not necessary that all testbeds support testing for these kinds of attacks, as long as a small subset can.
- Where possible, provide details of hardware and their locations to allow digital twins of the sites to be created in popular research networking and mobility simulators (such as NS3 [7] and OMNeT++ [6]). (May not be applicable to testbeds in a public space, or where context of these devices is sensitive.)
- Consider and document how cyber security and communication experiments can be repeated multiple times under nearly identical environmental conditions.

- Support users running local cloud instances that edge communication infrastructure can interact with.
- Testbeds should consider allowing users to deploy custom hardware on site. Masts that would be used should have access to a suitable power source (e.g., mains power or PoE).
- Testbeds should coordinate on producing logs in a common format to simplify post-testing data analysis.
- Testbeds should clearly document the procedure for performing testing on site.

For Communication Hardware Manufacturers

- The technical specifications of hardware should be made publicly available.
- The RF characteristics of the hardware should be summarised to make applying for testing licences easier.
- The SDK should be more easily accessible to allow researchers to prototype new techniques.

For Ofcom

- Consider making performing (certain kinds of) security testing with known V2X hardware not require a licence. Testing DoS or similar malicious usage would still require a licence.
- Improve the user experience of checking if a device is specified as licence exempt in IR 2030 [42] and better publicise this on the website at [43].

For Universities

- The process for obtaining permissions to purchase SDK should be better documented and streamlined, and made available for other institutions.
- Researchers need to consider practical aspects of real world deployments if their work is expected to be applied. For example, not assuming perfectly reliable systems.
- Researchers should develop protocols executing on the Edge that are resilient to temporary or permanent loss of cloud connectivity.

General

- A better translation from popular networking research simulators to real hardware deployments needs to be created. Rewriting simulations introduces the potential for bugs and means the implementation for real hardware is unlikely to match the simulator version. Experience should be taken from the WSN simulator COOJA, which can simulate a compiled binary that can also be run on real hardware.
- Aim to obtain data in a format compatible with existing tools such as Wireshark.
- Researchers should aim to use actual IEEE 802.11p or 5G cellular equipment to perform testing.

Acknowledgements

This research was supported by a Lloyd's Register Foundation grant [GA\100186]. The work was performed in conjunction with the PETRAS: UK Research Hub for Cyber Security of the Internet of Things project [EPSRC Grant EP/N02334X/1].

Technical Team

- Carsten Maple (PI, University of Warwick)
- Haitham Cruickshank (Co-I, University of Surrey)
- Matthew Bradbury (University of Warwick)
- Chen Gu (University of Warwick)
- Hu Yuan (University of Warwick)
- Muhammad Kamarudin (University of Warwick)
- Ao Lei (University of Surrey)
- Philip Asuquo (University of Surrey)

Advisory Board

- Jeremy Morley (Ordnance Survey)
- Kevin Reeves (Costain)
- Kum Wah Choy (Costain)
- David Owens (Telefonica)
- Paul Zanelli (TRL)
- Richard Porter (Zenzic)
- Michael Talbot (CCAV)
- Mike Fisher (BT)
- Craig Ormerod (TÜV SÜD)
- Chris Guy (TÜV SÜD)
- Alistair Ritchie (PETRAS)
- Miles Elsden (Elsden Consultancy Services Ltd)

Additional Acknowledgements

Maps in figures 4.2, 4.3a, 4.3b, 4.1b, 4.1a, 4.6, 4.7, 4.8 and 4.9 presented in this work were generated using Cartopy [35]. Map images in figures 4.2, 4.3a, 4.3b, 4.1b, 4.1a, 4.6, 4.7 and 4.8 © Ordnance Survey 2019. Map image in figure 4.9 © OpenStreetMap contributors.

We would also like to thank the following for their assistance during this project: Jia Liu, Yan Yan, Ivan Ivanov (Warwick), Adam Hancox (Warwick), David Fishlock (Surrey), Andrew Walker (Surrey), Evan Fradkin (Warwick), Jim O'Reilly (OS), Ugur Ilker Atmaca (Warwick), Eren Arugaslan (Warwick), Al-Tariq Sheik (Warwick), Jo Bailey (Warwick) and Chronis Kapalidis (Warwick).

Contents

List of Tables

List of Figures

Acronyms

API Application Programming Interface.

BRAN Broadband Radio Access Networks.

BTP Basic Transport Protocol.

C-ITS Connected Intelligent Transport Systems.

CAM Cooperative Awareness Message.

CAV Connected Autonomous Vehicle.

DPKI Decentralised Public Key Infrastructure.

ECDSA Elliptic Curve Digital Signature Algorithm.

EIRP Equivalent Isotropically Radiated Power.

ETSI European Telecommunications Standards Institute.

IoT Internet of Things.

IoT-TRaM Internet of Things for Transport and Mobility.

ITS Intelligent Transport Systems.

MFM Midlands Future Mobility.

MTU Maximum Transmission Unit.

NEAA North East Automotive Alliance.

OBU Onboard Unit.

PKI Public Key Infrastructure.

RLAN Radio Local Area Network.

RSU Roadside Unit.

SMLL Smart Mobility Living Lab.

TRK Real-time Kinematic.

V2I Connected-Vehicle-to-Infrastructure Communication.

V2V Connected-Vehicle-to-Vehicle Communication.

V2X Connected-Vehicle-to-Everything Communication.

WLAN Wireless Local Area Network.

1 Introduction

The national importance of developing next generation transport and mobility solutions is clear. With the UK Government having invested over £120 million, plus an additional £68 million from industry sources, in related research projects since 2014 [15], it has become evident that the UK Government has clearly recognised the significance of Connected and Autonomous Vehicles (CAV) and the opportunity they present in delivering future UK transport systems. Given the complex nature of the underlying systems that enable such technologies, and the absolute importance that they remain safe and resilient, repeated and extensive testing is required to ensure that CAVs can be viable in public environments. Unfortunately, there is currently no coordinated process that allows system-wide cyber security testing of transport and mobility products and services, nor are there developed approaches or facilities that can adequately support CAV technologies from concept to market.

The IoT-TRaM project began in September 2018 and completed on May 31st 2019 and involved, among other elements, developing four outputs from existing PETRAS projects within the Transport and Mobility constellation and demonstrating them on testing facilities in the UK. This report presents the experiences, lessons learned and recommendations from this testing. This report also describes the protocols for a coherent transport and mobility testing infrastructure that covers a wide range of testing environments.

This project allowed for a unique opportunity for national testing facilities to engage with cutting-edge research being funded through EPSRC and Lloyd's Register Foundation and conducted in collaboration with PETRAS, the UK Research Hub for Cyber Security of the Internet of Things. The sites have benefited from a unique understanding of the latest security and privacy techniques. They have also had the opportunity to have their own engineers and researchers engage with research staff at leading UK universities and be part of an initiative that aims to secure future vehicles and transport infrastructure, and influence national and international policy. In addition, testing sites learned more about how to engage with researchers so that in future their client base can expand and protocols for testing can be improved. It is an anticipated outcome of the project that there will be greater collaboration between academics and testing sites in the future, with testing being written into national and international research proposals, developing a revenue stream for the testing sites and improving the quality and practicality of the research performed at UK universities.

1.1 IoT-TRaM Objectives

The three key objectives of the IoT-TRaM project relevant to this report were:

- To demonstrate the practicality of research related to transport and mobility from PETRAS projects.
- To investigate the key barriers in testing, and translating secure transport and mobility solutions from concepts to practice, focusing on the policy and regulatory framework, technology barriers and cyber security issues.
- To provide guidance with critical insights in the requirements for the involved parties to ensure security and safety assurance of their products and services.

1.2 Deliverables

This document represents a consolidated report covering the following deliverables of the IoT-TRaM project.

- Deliverable 1: Report on the implementation of (i) decentralised public key management to be implemented and tested on national infrastructure; and (ii) group signatures from the P-Cars project to be implemented and tested on national infrastructure.
- Deliverable 2: Report on the implementation of (i) opportunistic authentication from the GEOSEC project to be implemented and tested on national infrastructure; and (ii) pseudonymous certificate management from the B-IoT project to be implemented and tested on national infrastructure.
- Deliverable 3: Comprehensive informative document on the facilities that businesses can use for the safe and secure development of CAV technologies, detailing how certain products fit in the ecosystem and the reason behind the protocols and approaches needed to carry out testing of Transport and Mobility Solutions (TMS).
- Deliverable 4: Guidance document for testing facilities that promotes cyber security testing by providing a view of the associated protocols and best practices.

1.3 Report Structure

The rest of this document is structured as follows: In Chapter 2 the four academic innovations that were implemented and deployed will be described. This includes a group signature scheme that provides authentication of messages plus privacy in the form of long term unlinkability in Section 2.1. A technique to prioritise which messages are authenticated first in Section 2.2. A distributed ledger based technology to perform key distribution in Section 2.3, and a modification of this technique that swaps identities to protect vehicle privacy in Section 2.4. In Chapter 3 the experiences of the IoT-TRaM project performing this testing is described. These experiences and used to inform the requirements of cyber-security researchers from CAV testbeds. Multiple recommendations are made regarding how the state of cyber security testing of CAVs can be improved in the future. Finally, this report concludes in Chapter 5 by presenting a summary of the recommendations to improve the accessibility and process of performing cyber security testing of CAVs on testbeds.

2 Technical Innovations

Future connected and autonomous vehicles will communicate with each other and infrastructure using Dedicated Short Range Communications (DSRC), or between vehicles and infrastructure via 5G cellular for a variety of applications. For example, vehicles will regularly broadcast status information such as speed, heading, and position to nearby vehicles and infrastructure via cooperative awareness messages (CAMs) [8]. Information about events (such as parked cars or vehicle collisions) will also be broadcasted via Decentralised Event Notification Messages (DENMs).

To ensure the integrity of the message and the authenticity of the sender, digital signatures can be used. However, there are a number of downsides of these signatures including the computational cost, size of the signature and privacy issues that need to be addressed. This chapter will describe four academic innovations that were previously analysed and simulated, and were used as the basis for the work in this project. These innovations were enhanced and adapted in order to be deployed on real hardware and tested in real world environments.

2.1 Group Signatures

Group signatures are a type of digital signature that allow a message to be verified as having been sent from a member of a group. It is useful to form a group in scenarios such as platooning, or other collaborative activities on the road. This innovation focuses on (i) reducing the computation cost to sign and verify messages, (ii) providing privacy, and (iii) allowing an authority to revoke the privacy. This innovation is based on the publication: [30] Jia Liu, Liqun Chen, Mehrdad Dianati, Carsten Maple, and Yan Yan. Efficient anonymous signatures with event linkability for V2X communications. In Submission.

To perform the setup the Issuer first generates three keys: (i) the Master Issuing Key (MIK), (ii) the Master Opening Key (MOK), and (iii) the Group Public Key (GPK). Any User wishing to join the group (such as an OBU or RSU) generates their own User Secret Key (USK) and User Public Key (UPK). The GPK is sent to users wishing to join the group. In order to join a group a User sends a JoinRequest to the Issuer. Using their MIK and GPK a Group Signing Key is created for the User and sent to them. When the User receives the GSK they validate it and if successful they are ready to sign messages.

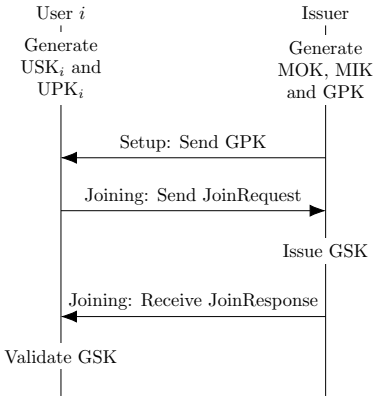


Figure 2.1: Group Signatures Join Protocol

Information	Sign GSig	Verify GSig	Sign ESig	Verify ESig
Message	✓	✓	✓	✓
Event Token (ET)	✓	✓	✓	✓
Group Signing Key (GSK)	✓			
Group Public Key (GPK)	✓	✓	✓	✓
GSig		✓	✓	✓
User Secret Key (USK)			✓	
ESig				✓

Table 2.1: Group Signature Signing and Verifying Requirements

When signing messages, there are two types of digital signatures that can be attached: either a Group Signatures (GSig) or an Event Signature (ESig). Group Signatures are larger and more expensive to compute and verify compared to Event Signatures. Event Signatures require a previously sent/received Group Signature to sign/verify a message. Due to this Group Signatures are sent less frequently that Event Signatures.

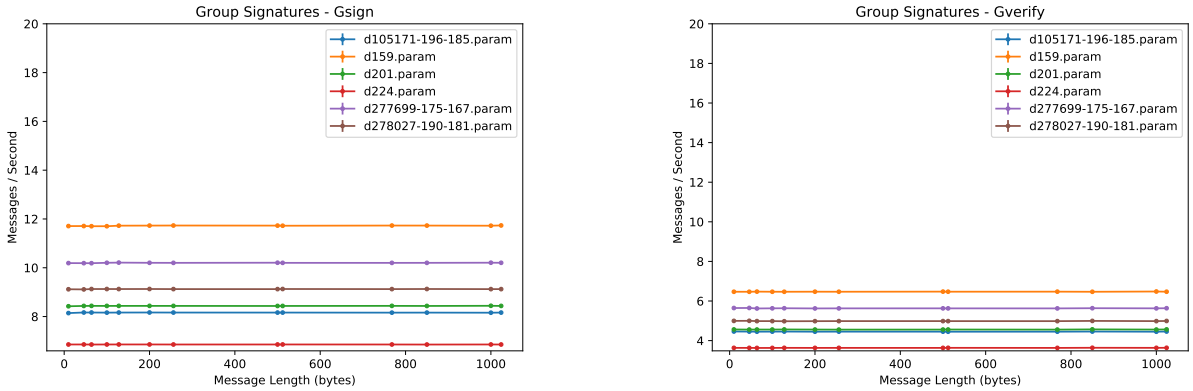
As part of revocation there are three actions that can be performed on messages with signatures: (i) Linking, (ii) Opening, and (iii) Judging. Linking allows a User or Issuer to check if two GSigs are signed by the same GSK. Opening allows the identity of a GSig to be revealed used the MOK and registration information generated during joining. Opening produces a proof which is verified in the Judging step, ensuring the the GSig was indeed generated by the identified vehicle.

For a User to know when to send a GSig or ESig, and for privacy to be provided a concept of Events is required. An event could be a User's location (such as a stretch of road or an intersection) or it could be a period of time (such as a timestamp that changes every 10 minutes). This information is included in a string called the Event Token. All members of the group need to agree on how define an Event Token and how to tell if the Event Token has changed. The Event Token is used as a component to sign and verify both types of signatures. When the event changes a GSig is sent attached to a message, subsequent messages will have an ESig calculated based off this GSig.

This usage of the Event Token leads to short-term linkability and long-term unlinkability. While the event has not changed other Users will be able to identify that messages are being sent from the same vehicle. After the event changes, Users cannot link the new signature identity to the previous identity.

2.1.1 Performing Testing

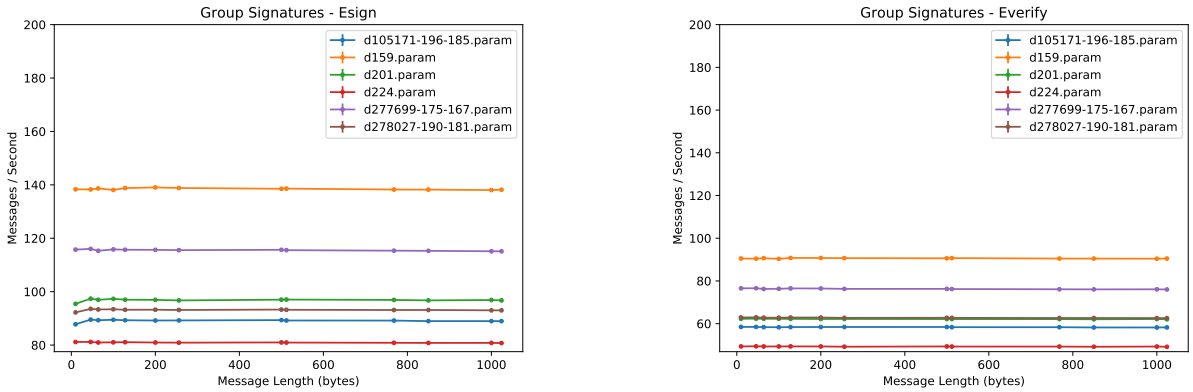
To perform testing three classes of devices would be needed: RSUs, OBUs and an Issuer. To simplify the testing the setup phase was performed offline and keys were deployed to the devices which eliminated the need for a device to act as the Issuer. The testing consisted of RSUs being deployed along a roadside. They were configured as OBUs so they resembled parked cars. An OBU mounted in a vehicle drove past the RSUs and a researcher checked the log output to ensure that messages were being received, and that every 30 seconds the event token changed leading to a change in the signatures attached to messages. To ease testing, signatures were coloured to indicate their identity.



(a) Sign

(b) Verify

Figure 2.2: Group Signatures: Group Signature Performance on Cohda RSU



(a) Sign

(b) Verify

Figure 2.3: Group Signatures: Event Signature Performance on Cohda RSU

2.1.2 Performance Results

To understand the performance cost of using this group signature scheme its performance for creating digital signatures and verifying them for both the group and event signatures was profiled on the Cohda OBUs. Results are shown in Figure 2.2 for GSig and Figure 2.3 for ESig. As expected many fewer GSigs can be signed and verified per second compared to ESigs. This was an expected result from the paper and is the reason why GSigs are sent infrequently and the majority of messages are signed using ESigs. The cost of verifying messages is higher than the cost of signing messages. The message length had no impact on the number of messages that could be signed or verified per second. This is because messages are initially hashed to a fixed length string on which subsequent computation is performed. The time cost of hashing is small in comparison to the subsequent cryptographic computation. These results were gathered on a single thread, so utilising multiple cores will increase the number of messages that can be signed and verified per second.

2.1.3 Testing Results

Three practical issues were encountered when deploying this technique. The first is an implementation issue, where the paper did not specify how a cached GSig in the OBU's memory should be

looked up to verify an ESig. To resolve this issue additional information (the public key) was included in the ESig that can be matched with information found in the GSig.

The second is that clocks between vehicles are not perfectly synchronised (as assumed in the theoretical work). This was an issue as the Event Token was set to change every 30 seconds in our testing and led to vehicles not simultaneously changing their Event Tokens leaving them potentially unable to verify messages around the event change period because vehicles signed or verified messages using different Event Tokens. This typically lead to a vehicle failing to verify one or no messages.

The final practical issue is that real-world communication channels are not perfectly reliable, meaning not all messages sent were received. If a vehicle missed receiving a GSig from a vehicle then it would be unable to verify all subsequent ESigs sent by that vehicle in the event until the next GSig is sent. This means that GSigs will need to be sent under additional circumstances, such as receiving messages from previously unseen vehicles.

Recommendation 1: Researchers that expect their work to be applied, should recognise that practical situations involve imperfect conditions (such as clock drift or unreliable communications channels) as well as physical limitations. Any assumptions and requirements should be clearly specified..

2.2 Authentication Prioritisation

To ensure trusted communications connected vehicles need to have the ability to include proof that they were the sender of a message and receivers need to be able to verify this proof. Digital signatures provide this capability plus the ability to verify the integrity of the message. However, they are expensive to compute and to validate. This is a problem on two fronts, firstly, the devices signing messages and verifying signatures have limited computational ability meaning that they can only verify a limited number of signatures per second at maximum. Secondly, an adversary may attempt to spam these devices with messages to verify that do not provide useful information in an attempt to induce a Denial of Service.

To resolve these issues vehicles will need to prioritise which messages to authenticate, so that the messages most likely to be important are verified first. There are many ways to decide how to prioritise messages, for example, the history of messages received could be used ignore verifying messages informing the vehicle of the same event. If the vehicle has already verified multiple messages about upcoming roadworks, verifying more will not add significantly more utility. Verifying messages informing the vehicle of new information is more useful.

An alternate approach is for the vehicle to selectively verify messages. Messages are verified based on the distance and direction of the communicating vehicles with respect to each other. This method leads to the most relevant packets being verified before less relevant packets. This is the approach shown in Algorithm 1, which uses the location, speed, time and heading of two vehicles (one that sent a message, the other that received it) to calculate a priority of a message. The message will be assigned a higher priority if the transmitting vehicle (A) is moving towards the receiving vehicle (B). This message is then inserted into a priority queue from which messages with the highest priority are verified first.

Algorithm 1 CAM Prioritisation

function CAMPriority(A) ▷ A is the state sent by another vehicle
  $B \leftarrow$ GetState() ▷ B is this vehicle's state
  $dist \leftarrow$ Distance($A_{lon}, A_{lat}, B_{lon}, B_{lat}$) ▷ The euclidean distance between the vehicles
  $t \leftarrow B_{time} - A_{time}$ ▷ Time between A sending and B receiving (incl. processing)
  $dist_{early} \leftarrow$ InterpDistance($dist, B_{speed}, -t$) ▷ Distance when A sent the message
  $dist_{now} \leftarrow$ InterpDistance($dist, A_{speed}, t$) ▷ Distance when B received the message (now)
  $dist' \leftarrow dist_{now} - dist_{early}$ ▷ How is distance changing?
  $heading' \leftarrow \frac{|A_{heading} - B_{heading}|}{180}$ ▷ How does the heading differ?
  if $dist' < 0$ **then** ▷ Moving closer
    $w \leftarrow 1 - \exp\left(dist'\right)$
    return $\max\left(w \times heading', w\right)$
  else if $dist' > 0$ **then** ▷ Moving further
    $w \leftarrow \exp\left(-dist'\right)$
    return $\min\left(w\left(1 - heading'\right), w\right)$
function InterpDistance(d, s, t) ▷ Interpolate distance to estimate it at different points in time
  return $d + st$

2.2.1 Performing Testing

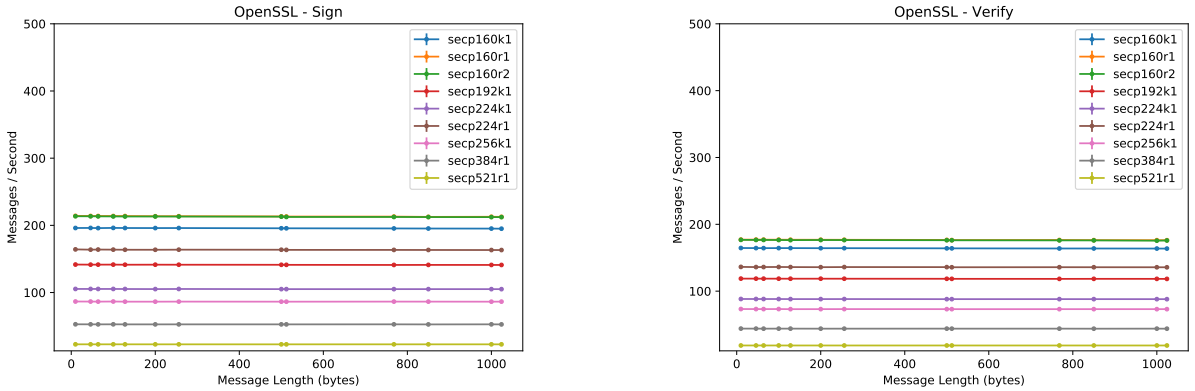
This testing included two classes of devices: OBUs and RSUs. To simplify the testing the setup phase was performed offline and all keys were deployed to the devices. Devices only accessed the keys that they should either already have, or could fetch from a cloud service. The testing consisted of RSUs being deployed along a roadside. They were configured as OBUs so they resembled parked cars and therefore broadcasted CAMs with digital signatures. An OBU mounted in a vehicle drove past the RSUs and a researcher checked the log output to ensure that received messages were being prioritised by a value. As it was not possible to have a large number of vehicles performing the testing, artificial vehicles were simulated based on collected real world data of vehicle movements from CAMs. To ease testing, messages from either real or artificial cars were coloured to indicate their identities.

2.2.2 Performance Results

Creating and signing OpenSSL signatures was also profiled on Cohda OBUs and the results are shown in Figure 2.4. In these results OpenSSL tends to perform better than the group signature scheme in terms of the number of messages that can be signed and verified depending on the parameters used. As with the group signatures, the number of signatures that can be verified per second does not vary with the message length because OpenSSL hashes the input before processing. Also, these tests were only performed on a single thread, so utilising multiple cores will lead to a higher number of messages that can be signed and verified per second. Using Cohda's security layer provided by Aerolink may also lead to higher performance. Unfortunately due to how Aerolink was integrated we were unable to test this.

2.2.3 Testing Results

The first issue encountered was that parts of data in received messages may not be present. For example, a stationary vehicle will not have a heading as it is not moving. This is allowed by the CAM ETSI standard even for values that are mandatory, as they have a special value that is provided to indicate no value is present [8]. Due to implementation bugs we initially failed to prioritise these messages correctly. Future work in this area needs to ensure that they correctly



(a) Sign

(b) Verify

Figure 2.4: OpenSSL Ecliptic Curve Performance on Cohda RSU

handle missing information when calculating a priority and that the way missing information is handled cannot be abused by a malicious entity.

The second issue is that the priority scheme investigated is relatively simple. While it uses a variety of useful information such as location, time, speed and heading. There is a lot of rich information included in CAMs and DENMs that needs to be considered when prioritising messages. It is important to ensure an adversary cannot craft malicious packets that always have a higher priority than genuine packets from well behaved vehicles.

2.3 Decentralised Public Key Infrastructure

The European Telecommunications Standards Institute (ETSI) has mandated that ITS will use public key cryptography to secure the wireless communications of CAVs [4]. However, an important aspect that is still under consideration is how the public key infrastructure (PKI) will be organised. A centralised cloud-based service is simple and convenient. However, CAVs will need very fast response times when querying the PKI for public keys. The reason for this is that connected vehicles will frequently receive messages from new vehicles, for which they do not have a public key. Without the new vehicle's public key, no messages from this vehicle can be verified, potentially leading to safety and security issues due to the inability to assess trust. Better performance can be obtained by distributing the PKI along the Edge nodes of the ITS [27]. In such a decentralised public key infrastructure (DPKI), the Edge nodes (such as RSUs alongside the road) can manage the public key infrastructure. The DPKI can respond to vehicles faster by avoiding additional communication hops back to a cloud server if public keys have been cached on specific RSUs.

To implement this innovation a distributed ledger is used as the distributed data structure to share information across RSUs. As distributed ledgers are the technology that underpins blockchain, the system obtains useful properties, such as an immutable history of public keys. This innovation is based on the work: [27] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. *IEEE Internet of Things Journal*, 4(6):1832–1843, Dec 2017. ISSN 2327-4662. doi: 10.1109/JIOT.2017.2740569. However, many changes were made to the implementation due to the different network topologies assumed by the paper compared to the topology available during deployment.

The paper [27] mostly focuses on the propagation of public keys along the RSUs. The

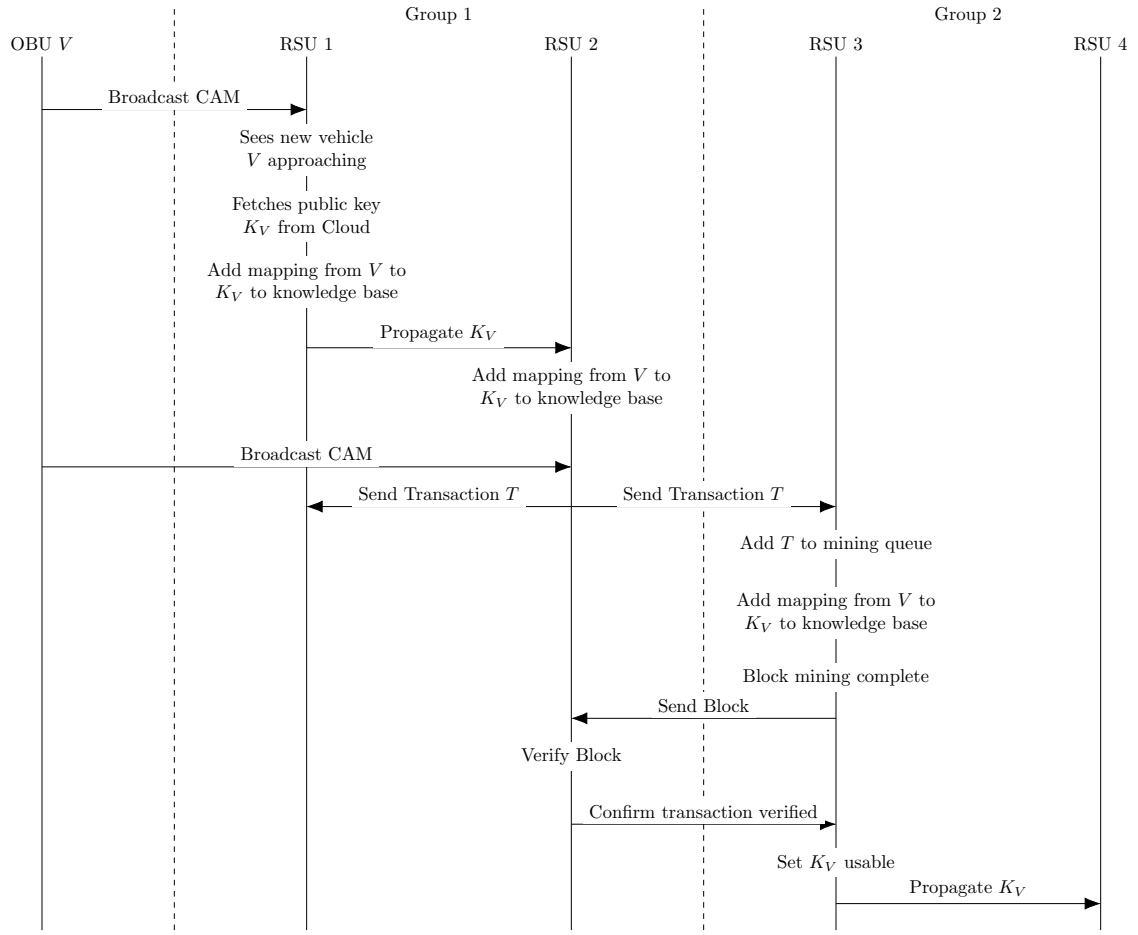


Figure 2.5: Protocol Actions of DPKI

implemented handover protocol between two different groups is illustrated in Figure 2.5 and described below:

1. When a vehicle V approaches RSU 1, the RSU checks if the vehicle is in its knowledge base first, if it not then the RSU fetches V's public key from cloud and inserts it to its knowledge base.

2. RSU 1 propagates this information to all other RSUs within its group.

3. When the vehicle V approaches the ultimate RSU in the group (RSU 2 in this example), the RSU prepares the transaction to handover to a new group. This transaction includes V's identity, V's public key and the destination (RSU 3 in this example).

4. When an RSU receives a transaction:

   - If the RSU is in a different group (RSU 2), it is added to mining queue and mining starts on a separate thread to avoid blocking the communication thread. After the mining is completed the verified block is sent back to the originator.
   - If the RSU is in the same group, no actions are taken.

5. If the block is verified, the public key of V is set to be usable. Therefore the key has been successful transferred from RSU 2 to RSU 3. This preempts needing a cloud request when

vehicle V approaches RSU 3, meaning vehicles can quickly begin verifying messages from V.

2.3.1 Performing Testing

This testing included two classes of devices: OBUs and RSUs. To simplify the testing the setup phase was performed offline and all keys were deployed to the devices. RSUs emulated fetching keys from a cloud server when requested. As the RSUs did not have actual access to the cloud, fetching a key entailed copying it from one keystore to another. OBUs only had access to their own keys and keys they specifically requested from the RSUs. Typically four RSUs were deployed and divided into two groups. The first two were set to be in group 1 and the second two set to be in group 2. A vehicle equipped with an OBU drove down the road broadcasting CAMs. When the vehicle reached the last RSU in group 1 it performed a handover to the first RSU in group 2 to propagate the OBU's public key. RSUs removed keys from their local cache after 5 minutes.

2.3.2 Testing Results

The paper this work is based upon only focuses on the propagation of public keys along the RSUs and did not include a protocol for interacting with OBUs in vehicles on the road [27]. This meant that a crucial aspect of the DPKI needed to be created by the IoT-TRaM technical team to properly implement this scheme and test it.

We also avoided implementing certain aspects from the paper to simplify development of the protocol. One example of this, is that the paper groups transactions together to reduce the cost of performing many small transactions. Our implementation only includes one public key per transactions when a vehicle moves between two groups of RSUs. This keeps the implementation simple, but would be less scalable to higher traffic flows.

2.4 Decentralised Public Key Infrastructure: Pseudonyms

As has been previously discussed in Section 2.1 protecting location privacy of CAVs is going to be important. This innovation extends the DPKI implementation to provide the ability for vehicles to swap keys with the infrastructure. This is necessary because unlike group signatures, the Elliptic Curve Digital Signature Algorithm (ECDSA) used to create digital signatures does not have a built in facility to change how the identity appears to eavesdroppers. So to change a vehicle's identity the actual keys used to create digital signatures needs to change. A vehicle can keep a small cache of these keys locally, but eventually they will run out of *clean* keys that they have not previously used. When this happens they will need to provide the *dirty* keys back to the DPKI and request new clean keys.

This demonstration is based on the publication: [13] Shihan Bao, Ao Lei, Philip Asuquo, Haitham Cruickshank, Zhili Sun, Michael Huth, and Carsten Maple. Pseudonym management through blockchain: Cost-efficient privacy preservation on intelligent transportation systems. (In Submission). However, significant changes needed to be made to this work in order to deploy it. Many of these changes were based on the changes made to the DPKI innovation described in Section 2.3 as this innovation extends the previous innovation. However, a number of additional changes needed to be made to correctly provide and test the privacy preserving ability of the innovation.

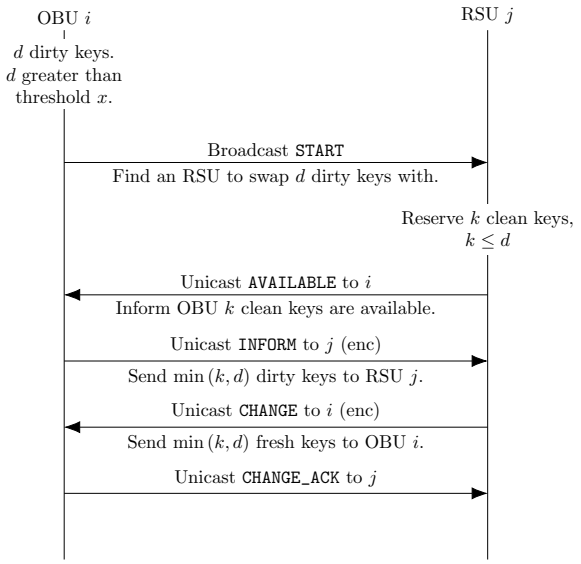


Figure 2.6: DPKI: Pseudonym Management — OBU/RSU Key Swapping

2.4.1 Performing Testing

Performing the testing of this innovation proceeded in a similar manner as described in Subsection 2.3.1. The main difference was that every 30 s the keys used to sign messages changed and the previous keys were marked as dirty. OBUs were set to have a maximum of 5 cached keys and once three out of five of these keys were dirty they were swapped with clean keys from the RSUs. It was assumed that OBUs would not change their identity while swapping keys.

2.4.2 Testing Results

Due to an implementation bug we encountered issues where keys would become exhausted. This was because of two issues that led to a decrease in the number of keys both on the OBUs and RSUs: (i) a bug in RSUs led to valid unused keys being deleted and (ii) OBUs would offer a larger number of keys to swap than a RSU was capable of supplying. Even after these issues were resolved, this DPKI-based pseudonym allocation approach may still be vulnerable to key exhaustion attacks by malicious adversaries or poorly implemented clients. Future work will need to investigate techniques to ensure that such attacks are detected and mitigated.

Another factor that needed to be considered was the Maximum Transmission Unit (MTU) of IEEE 802.11p, which specifies the maximum packet size. The MTU could be set to the conservative Ethernet default of 1500 B [20], the higher 2304 B of the IEEE 802.11 standard [2, Table 9–19], or other higher values allowed by the IEEE 802.11 standard [2] (note that bytes here are assumed to be 8 bit). Due to the large size of the keys, there was a limit to the number of keys that could be swapped in a single packet. Initially too many keys were being swapped, but the Cohda API call `ETSIMSG_SendPacket` did not raise the packet being too long as an error, meaning this issue initially went unnoticed. This issue was resolved by placing a limit on the number of keys included in each BTP packet to be below a conservative length of 1394 B.

2.5 Conclusions

Implementing these four innovations came with a number of challenges that arose due to the deployment on real hardware. Typically these issues fell into four categories:

- The network topology of the simulated environment differed from the available deployed environment.
- Practical limitations prevented the simple implementation used for simulations from being easily ported (e.g., due to packet size limitation, unreliable wireless channels and clock drift)
- Deployment issues of including additional software library dependencies on the hardware.
- Bugs introduced when translating the code written for simulation to code written for deployment.

While some of these issues are relatively minor (deploying custom software libraries), resolving issues such as differing network topologies and rewriting simulation code at the same time led to multiple bugs during development. The process should have been to: (i) modify the simulation to test using the network topology available for deployment, (ii) change the simulation implementation to work for that topology, and finally (iii) implement a middleware such that the same simulation code could be run on the real hardware. Approaching the translation of the academic work to a practical deployment in this way would have avoided many of the issues encountered.

3 Testbed Requirements and Experiences using Testbeds

This chapter will describe the experiences of performing testing during the IoT-TRaM project. Using this experience, the requirements from the perspective of users of CAV testbeds is also documented. These experiences from the IoT-TRaM project are used to present recommendations for simplifying testing protocols in the future and ways in which cyber security testing on CAV testbeds can be made accessible to a broader range of stakeholders.

3.1 Device Selection

To perform cyber security testing for CAVs one of the main aspects that will need to be tested are the communications. The reason for this is that many of the security, privacy and trust protocols that researchers are developing will involve (typically wireless) communication. This communication includes vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) and vehicle-to-everything (V2X). To ensure valid testing the communications need to happen as similar to future technologies as possible. This may mean DSRC IEEE 802.11p equipment such as those from Cohda, Kapsch, or other manufacturers. It could also mean 5G cellular and the associated modems that support 5G technologies.

If the actual communication devices are unobtainable, then alternative devices that operate in the 5 GHz spectrum (such as WiFi or Bluetooth devices) or even devices that use different communication protocols (such as LoRaWAN) could be used to achieve similar results. However, these results will not map as accurately to the results obtained with the actual communication hardware that will be used in CAVS. Therefore obtaining actual IEEE 802.11p or 5G cellular capable OBUs and RSUs is preferable.

Recommendation 2: Where possible, researchers should use actual IEEE 802.11p or 5G hardware to test protocols that will be used with these modes of communication.

Recommendation 3: CAV testbeds should focus on deploying and allowing access to the V2X communication equipment they have installed at the site.

3.2 Licensing of IEEE 802.11p

Permission to perform testing with communications of IEEE 802.11p devices in the UK does not typically require a licence from Ofcom. This is because the frequencies used to communicate are either in the unlicensed ISM band (ITS-G5B), or has a license exemption (ITS-G5A) [11].

Name	Frequency Range	Usage	Licensing Exemption
ITS-G5D	5905 to 5925 MHz	Future ITS applications	
ITS-G5A	5875 to 5905 MHz	ITS road safety applications	[11]
ITS-G5B	5855 to 5875 MHz	ITS non-safety applications	ISM [41]
ITS-G5C	5470 to 5725 MHz	RLAN (BRAN, WLAN)	

Table 3.1: Frequency Allocation for ITS in the EU [1, Table 1]

Name	Channel Type	Frequency Range	IEEE Channel Number	Cohda [16]	Kapsch [26]
ITS-G5D	G5-SCH6	5915 to 5925 MHz	184	✓	✓
	G5-SCH5	5905 to 5915 MHz	182	✓	✓
ITS-G5A	G5-CCH	5895 to 5905 MHz	180	✓	✓
	G5-SCH2	5885 to 5895 MHz	178	✓	✓
	G5-SCH1	5875 to 5885 MHz	176	✓	✓
ITS-G5B	G5-SCH3	5865 to 5875 MHz	174	✓	✓
	G5-SCH4	5855 to 5865 MHz	172	✓	✓
ITS-G5C	G5-SCH7	5470 to 5725 MHz	94–145	✗	✗

Table 3.2: European Channel Allocation [1, Table 3]

The other bands of ITS communication are licensed in the UK (ITS-G5D and ITS-G5C). This means that as long as devices only communicate in ITS-G5A and ITS-G5B, and within transmit power limits of a maximum mean EIRP of 33 dBm [11], no licence is required. We expect that the majority of CAV cyber security testing will fall in this category. However, for testing with ITS-G5D, higher transmit powers, or other considerations, a licence will be required from Ofcom to perform testing. Note that as neither of the latest hardware versions of Cohda (MK5) nor Kapsch (RIS-9160) devices can communicate in the ITS-G5C band, we have not considered the licensing aspects of it.

Of the two manufacturers this report is focusing on (Cohda and Kapsch), neither devices supports transmission in ITS-G5C (channels 94–145 [1, Table 3]). Cohda devices support transmitting and receiving in the channels 168–184 which are outside of the range of ITS-G5C. Kapsch RIS-9160 device operates on frequencies 5860 to 5920 MHz [26] which is also outside of the range of ITS-G5C. The IR 2030 document [42] should be checked to see if the testing is with a licence exempt short range wireless device [40]. However, not all devices are present in IR 2030, meaning users will need to ensure they do or do not need a licence.

To apply for a licence an Ofw225 form [39] should be completed. This licence can be authorised for up to 12 months and will cost £50 for each station or apparatus per location. On receipt of the application it can take Ofcom up to six weeks to process it. More details can be found on the Ofcom website for non-operational licences [43]. In the application form certain details about the 802.11p protocol and the hardware being used is required. The details in Appendix A provide sufficient information to fill in the application form for a Cohda Wireless MK5 device.

3.3 Purchasing Devices and Software Development Kits (SDK)

In order to develop and test novel cyber security techniques for CAVs it is necessary for researchers to have access to the SDK for the device that is being tested on. Without the SDK it is not possible to implement custom security protocols. While some SDKs are supplied with a simulator, practical deployments with real hardware are preferable to test implementations before deploying them at a CAV testbed. This is to ensure that implementation issues can be corrected before a large-scale deployment. Therefore, the IoT-TRaM project purchased the SDK for developing software for Cohda OBUs and RSUs, and also purchased OBU and RSU hardware. This section describes the experiences of purchasing the SDK and the hardware by the teams at the Universities of Surrey and Warwick. This includes the internal procedures to acquire software, with the intention that other universities will have similar policies.

For the SDK:

1. Obtain quote from Cohda for the SDK and the User Licence Agreement [18].
2. Obtain authorisation from the following regarding the User Licence Agreement:
   (a) Contact the IT team to ensure the SDK does not present a risk to the university's IT systems.
   (b) Contact the IT team to ensure that the SDK does not already exist on the university's systems.
   (c) Check that there are no Intellectual Property Rights considerations with using the SDK.
   (d) Decide if an agreement is required to protect the accessibility of the source code.
   (e) Check if the User Licence Agreement contains a Derivative or Embedded Lease.
   (f) Obtain approval from the departmental administrator, head of IT systems and departmental finance team.
3. Obtain signature from central procurement in the University to sign the User Licence Agreement on behalf of the University.

To purchase the hardware a similar set of actions needs to be taken.

1. Obtain quote from Cohda for the hardware
2. Set up Cohda as a supplier to the University.
3. Perform the following checks and obtain authorisation from necessary parties:
   (a) Ensure if the department can meet the obligations in the supplier's Ts&Cs.
   (b) Check with the IT team to ensure there are no data protection issues.
   (c) Check that there are no Intellectual Property Rights considerations.
   (d) Check if there are any warranty or indemnity concerns.
   (e) Check if the User Licence Agreement contains a Derivative or Embedded Lease.
   (f) Obtain approval from the departmental administrator, departmental finance team and procurement.
4. Complete the purchase with the departmental finance team.

Purchasing the SDK and equipment can be a lengthy process due to the number of checks that need to be completed, therefore it is necessary to budget sufficient time for the procurement process to be completed. If a testbed is equipped with a heterogeneous deployment of RSUs then more than one SDK will need to be acquired. A higher number of SDKs to acquire leads to greater difficulty for university staff to test their research.

Recommendation 4: V2X device manufacturers would benefit, as would the research effort in general, if SDKs were more accessible to researchers.

3.4 Translating from Simulation to Deployment

Nearly all novel academic developments in security and privacy of CAVs will first be implemented in a simulator due to the low barriers to entry. Simulators such as NS3 [7] or VEINS [45][1] are popular as they allow the mobility of vehicles and communication to be simulated with ease and no financial cost. The simulators also allow complex network topologies to be created and tested on with ease. Translating these simulations to practical deployments is difficult for two reasons: (i) that code needs to be rewritten to target the SDK of the devices being deployed on, and (ii) the simulated topologies can be difficult to realise in deployment.

Rewriting code is problematic for many reasons. One of the main issues is that it is expensive in terms of time as new practical considerations need to be handled in the code. This is because many of the simulators aim to be hardware agnostic, but deploying on real devices requires that hardware (and platform) specific considerations are taken into account. It is also likely that rewriting code will introduce bugs not previously present.

The topology in the simulator is not easy to replicate in real world scenarios. For example, in two of the academic innovations (DPKI and DPKI: Pseudonyms) cloud services are assumed, however, as the Cohda RSUs were not equipped with cellular connectivity there was no way to create a deployment with a cloud. Instead the implementation needed to be adjusted to be deployed without a cloud, leading to large changes in the implementation. Being able to design and simulate for this kind of environment before deployment would have been useful.

There are solutions for each of these two issues. The first is to write code such that the same code can be simulated and deployed on hardware. Examples have been used in other domains such as Wireless Sensor Networks, where the TOSSIM [28] and COOJA [44] simulators both run the same code that is deployed to the hardware. There is still flexibility in the simulation as TOSSIM does simulation at an event level and COOJA simulates the CPU the compiled code is running on. Vehicular code will be more complex due to the higher complexity of the system, simulating all hardware present is likely to be infeasible. However, targeting a middleware that can then interact with vehicular simulators or OBU/RSU SDKs is the alternative that the software development approach used in this work.

[1] `https://veins.car2x.org`

Recommendation 5: Researchers should make effort to write code such that the same code can be simulated and deployed on V2X hardware.

The second solution is to not test with arbitrary topologies in simulators, but to create digital twins of the real-world sites where testing will be carried out. The main benefit is that no assumptions about the network topology needs to be made, as the real topology is simulated. However, other benefits include: (i) providing a well known topology for other researchers to test with even if they are unable to visit the site and (ii) providing access to a digital twin that has been validated with real-world testing for popular academic simulators.

Recommendation 6: It would be useful if CAV testbed owners created digital models, or digital twins, of their testbeds that can be integrated into the tools used by most commonly used by researchers. This would allow more accurate representation to simulate network connectivity and vehicle mobility.

3.5 Translating to Different Topologies

During the implementation of the two DKPI innovations a number of difficulties were encountered due to the differences in simulated network topology and the available network topology at the testbed. The main issue was the lack of ability to simulate a cloud service that the RSUs or OBUs were connected to. This was partly due to a lack of a network that the Cohda units were able to be connected to (either by Ethernet of cellular - which our model of RSU did not support).

Recommendation 7: Testbeds should aim for a capability that allows the V2X infrastructure to interact with a cloud service as part of the testing.

However, while many protocols will expect to have access to cloud services it would be better to design them to be resilient to not need cloud access. This is because the Infrastructure that forms the V2I edge infrastructure will be of critical importance to the safety and security of vehicles on the road. If possible this infrastructure should be able to operate without access to the Cloud.

Recommendation 8: Researchers should recognise that when developing protocols to be executed on Edge infrastucture, there is a need to consider resilience against temporary or permanent loss of access to cloud services.

3.6 Powering Devices

In order for the testing to be performed the V2X devices need to be powered. Cohda RSUs are powered by PoE and Cohda OBUs require input from a 12 V power supply. This section will detail how we powered the devices assuming no PoE or mains power at testbed sites as shown in Figure 3.1.

3.6.1 Powering External RSUs

It is typically not the case that PoE infrastructure is present externally that these devices can be connected to and powered from. It is also unlikely (in general) that the existing mains power infrastructure can be connected to. Certain testbed sites will have developed their infrastructure in a way that devices can be provided outside access to power and wired communications, but in general such infrastructure may not exist. To resolve this, it is recommended to obtain portable waterproof PoE injectors powered by batteries.

One example of such a device is the battery powered PoE injector by Veracity [47]. While this device is designed with the intent to be used with PoE surveillance cameras, it can be used with other hardware powered via PoE. Some variants of the Veracity devices advertise WiFi capability, where a device can connect to a battery's WiFi hotspot with the intention of viewing the output from the cameras. We were unable to connect to the Cohda units using this WiFi hotspot and the device is unable to use this WiFi capability to connect to an existing WiFi network.

Recommendation 9: CAV testbeds should ensure that equipment that is mounted on masts have access to suitable power sources (such as mains power or Power over Ethernet).

3.6.2 Powering Internal OBUs

To power the OBUs inside a vehicle a 12 V power supply is required. Vehicles typically come with a cigarette lighter socket which can supply the required voltage. However, to perform testing inside an office two components need to be acquired: (i) a *Car Power Inverter* which connects to a vehicle's cigarette lighter port and (ii) a 12 V PSU can be connected to the inverter to provide power. The Cohda OBU plug is unterminated so suitable connectors will need to be purchased and soldered to the connector in order to connect it to the PSU.

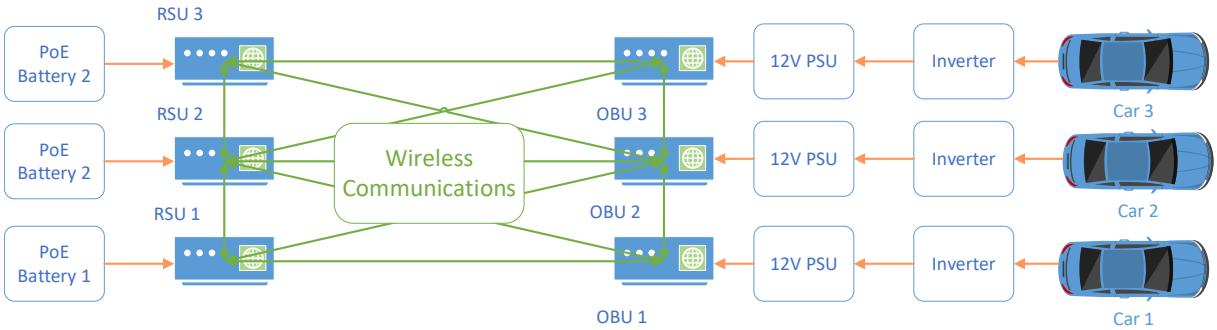


Figure 3.1: Powering and Connectivity of Cohda RSUs and OBUs

3.7 Practical Issues Encountered During Testing

When performing testing a number of practical issues were encountered. This section will detail these issues and the approaches used to overcome them.

3.7.1 Cohda Units in Lab

Testing the Cohda units in a lab environment was difficult. This was due to the Cohda units requiring a GNSS signal for timing information needed to transmit packets. In the building in which we were based the GNSS signal is very poor meaning that we were unable to perform testing inside. Many modern buildings are likely to encounter the same problem. To perform testing in the office we needed to place the devices outside pointing the GNSS antenna towards the sky.

An alternative workaround may have been to purchase an antenna that could be located outside. However, the device would still need to be very close to the antenna to minimise the length of the connecting cable. Due to the simplicity of placing the devices outside, this workaround was not investigated for feasibility.

3.7.2 Cohda Units Outside

When planning for where RSUs will be placed outside there are a number of additional considerations that need to be made:

Firstly, there will be restrictions on where the devices can be located as the devices will need to be attached to existing posts or masts. While mobile masts could be used, they pose additional challenges in terms of obtaining permissions, safety, and logistics, so were avoided for during our testing.

Secondly, the geographies of the area will impact the communications between devices. In our scenarios RSUs needed to be able to communicate with neighbours (in order to form a connected network). This meant that low elevation areas, or areas with physical obstacles (such as buildings or trees) needed to be considered during the deployment.

The duration of the deployment is also important to consider. Our tests intended to have flexible RSU locations, which meant that we frequently took down and reinstalled devices. To mount the Cohda devices on the lamppost or mast selected, two stainless steel straps need to be fed through slots in a steel bracket, looped around the post and then tightened. It is recommended that an electric screwdriver is used to tighten the straps to shorten the time and effort it takes. The Cohda RSUs are supplied with both the mounting bracket and the straps.

3.7.3 Selecting Device Locations

When selecting device locations it was vital that sufficient information is available about a site in order to plan for deployments there. If deploying devices at a custom site then the following is useful information to have about the site:

- What are the locations of posts or masts that can be used?
- What are the diameters of the posts or masts? (Do different mounting brackets need to be used to attach the devices?)
- Is there sufficient capacity in terms of the weight limits of the posts or masts?
- Is there mains power available at the post or mast? Is access to it suitable waterproofed?

- Is there connectivity to a LAN available at the post or mast? Is access to it suitable waterproofed?
- What obstacles are located around the post or mast that might interfere with V2X communications?

The most useful testbed sites will be able to provide at minimum the coordinates of posts/masts that devices can be installed at or are already installed at. But the more information about the capabilities and environment that can be provided the better.

Recommendation 10: Where possible, testbeds should aim to publicly detail what devices are present, the device capabilities (including detailing what use is permitted) and where the devices are located (including their position, height and orientation).

Note: This recommendation is unlikely to be feasible for testbeds in a public space due to security requirements or for testbeds where the context of devices is sensitive.

3.7.4 Deploying New Firmware

For one of the four innovations (Group Signatures, Section 2.1) it was necessary to include an additional library in the Operating System — the Paring-based Cryptography (PBC) [31] library. In order to do this, it was necessary to modify Cohda's firmware compilation to build in the library so it to be deployed as part of a new firmware image to the Cohda hardware. Deploying a custom firmware image also helped ensure that the devices being used for testing all started from the same consistent state. If deploying on devices that had been previously used by other researchers then it will be useful to be able to deploy a custom firmware to have a well-known starting configuration for all devices.

Recommendation 11: Testbeds should consider allowing deploying custom firmware images to V2X devices to allow testing with custom libraries and a known environment configuration.

3.7.5 Issuing Commands and Fetching Results

To issue commands to run the four technical innovation with the correct parameters was a manual process. It required physically connecting an Ethernet cable to the PoE battery or PoE injector, logging into the device via SSH, navigating to the correct directory and executing the relevant command. This was necessary as the devices were not networked together (other than via IEEE 802.11p). Ideally all of the devices would have been accessible via another communications link, such as a hardwired Ethernet LAN or a cellular link. Due to design choices in our deployment we were unable to create a physical Ethernet network and the Cohda units did not support cellular connectivity. Therefore, it was necessary to plan additional time for manual configuration.

Recommendation 12: To simplify using these devices, testbeds should ensure that the devices can be remotely accessed in order to (i) deploy new firmware, (ii) run code and (iii) fetch results.

3.7.6 Using Custom BTP Ports

Due to the need for the four academic innovations to use custom signatures and processing of these messages, it was necessary to re-implement certain ETSI functionality such as CAM generation. Instead of using the standard Basic Transport Protocol (BTP) ports [10] for CAMs a custom port was chosen for each of the four innovations (shown in Table 3.3) and an additional field was added in a custom header to be used an an actual port number. The intent was that each of the four innovations could be run concurrently without processing messages sent by another innovation. This concurrent execution was necessary for two main scenarios: (i) performing testing of multiple innovations concurrently due to time constraints and (ii) performing demonstrations of multiple innovations at the same time. While this approach worked for our use cases, it introduced a number of issues when analysing the data.

Innovation	**BTP Port Number**
Group Signatures	2501
Authentication Prioritisation	2502
DPKI	2503
DPKI: Pseudonyms	2504

Table 3.3: Custom BTP ports used

The first major problem was that by using a custom port number, tools (such as Wireshark) were unable to detect the type of our custom messages. The second issue was that the additional header that was added prevented tools from being able to correctly parse our messages. Overall, the approach taken in this project did not work well and alternative approaches should be used. BTP packets have two types [9]: type A which specifies a *Source port* and a *Destination port* and type B which specifies a *Destination port* plus *Destination port info*. One option would be to use the actual port number in the *Destination port* field and use the *Destination port info* field in a BTP-B header to allow specifying that this message is a variant of the usual message. Alternatively, the a range of *Destination port*s could be reserved for application testing and the *Destination port info* field could be used to specify what would usually be in *Destination port*.

Recommendation 13: It would be helpful if standards bodies (such as ETSI) define a way to mark standard packet types (such as CAMs) that are sent on non-standard ports as that message type. This should allow SDKs from hardware manufacturers to allow researchers and application developers to do custom processing of these messages.

3.7.7 Electrical Testing

Any equipment that is purchased may need to obtain a PAT (Portable Appliance Testing) certificate. If such testing is needed, testbed sites will need to publicly advertise a PAT certificate is required when bringing equipment onto their site.

3.8 Results Format

It is important to consider what data is going to be logged and in what format. The Cohda units used in our experiments provided automatic logging of the sent and received messages in pcap format. While it is vital to log network traffic to understand how the OBUs and RSUs are interacting, there are other pieces of information that will be necessary to be logged in order to understand why a protocol takes the actions it does. Identifying this information early is important to avoid needing to change the log format and the complexities this leads to when performing analysis.

Recommendation 14: Software developers and SDKs should version their log output to support modifying the output format due to changes to the implementation of the software.

Recommendation 15: Software developers and SDKs should output logs in formats that can be used by existing tools. Testbeds should aim to output results in a common format to simplify the analysis of data.

In some cases multiple log outputs needed to be parsed and combined. These logs contained a variety of information, such as calculated metrics about a packet (e.g., its priority), state changes in the program and other events. One option might be to use the (in development) PCAPNG capture file format [46], which had support for adding packet metadata. Allowing packets to be annotated with metadata in such a file format will simplify data analysis as there will not be any need to cross reference outputs about sent or received packets from two different logs.

Recommendation 16: It would be useful if SDKs exposed a way for software developers to attach arbitrary metadata to a specific packet via an API. Doing so allows a tight coupling of a packet and supplementary data without the need for additional scripts to link this information post hoc.

It is also important to consider where logs are going to be stored on devices and if there will be sufficient space for the logs. For example, Cohda RSUs store logs in specific partition for logs, however, the OBUs (by default) store the logs in a temporary directory. When Cohda OBUs are rebooted this temporary directory is cleared, meaning if logs are stored here they will be lost. It

is expected that an SD Card is purchased, inserted into the OBU, and configured for the logs to be stored here (as documented by the Cohda support website). Maintainers of these devices should investigate differences in configurations between models and not assume than an RSU will be configured in the same way as an OBU.

Recommendation 17: The owners of devices should ensure that the devices are correctly configured to provide log persistence across reboots.

3.9 Risk Assessments

To perform testing a risk assessment will need to be performed. This is especially important for testing activities that occur in venues that are accessible to the public. Table 3.4 contains a number of identified risks and their mitigations. This risk assessment was written with the intent to focus on researcher safety. For example, in case of inclement weather (such as heavy rain) we ceased testing. These protocols are going to need to be tested in different environmental conditions other than clear weather. Additional controls will need to be put in place to ensure that safety can be ensured while performing testing in difficult conditions.

Activity Description	**Hazards**	**Controls**
Installation of equipment	Risk to personnel installing equipment	Personnel will wear high-vis jackets.
	Theft risk to devices	A member of staff will stand next to each devices to ensure pedestrians do not interact with the devices.
	Impact to pedestrians	Installation needs to be performed in such a way that pedestrians (including those with specific mobility needs, such as a wheelchair) are not restricted by the installation.
PoE Batteries on floor	Trip risk due to Ethernet cables and battery	Cable ties will be used to keep cables tidy to minimise the likelihood of a pedestrian tripping. If PoE batteries are used, they will be deployed off of the pavement.
Driving to perform testing	Vehicle collision	Testing will only occur during the day. Vehicle occupants will have seat belts on while the vehicle is moving. The vehicle will be checked for issuer prior to testing.
	Distraction to driver	A passenger will control the OBU in the vehicle and allow the driver to focus on driving with minimum distractions.
	Inclement weather during testing	Testing will cease immediately. If appropriate devices will be removed and brought inside. Devices will be waterproofed using supplied tools.

Activity Description	Hazards	Controls
Receive signal from other devices	Incorrect operation of protocols	Devices will ignore any unknown signals.

Table 3.4: Hazards and Controls

Recommendation 18: Testbeds should aim to supply the template for performing a risk assessment early and clearly describe the procedure for completing them.

4 CAV Testbed Sites

To understand the state of the CAV testbed landscape in the UK this report investigated testing at the five following testbed sites: (i) the A2/M2 Connected Corridor, (ii) the Smart Mobility Living Labs, (iii) Midlands Future Mobility, (iv) the 5G Innovation Centre, and (v) Millbrook Proving Ground. Additional testbed sites are also presented. Due to the early development of many of the testbed sites much of the information presented is provisional and expected to change. As this is not intended to be an exhaustive list of testbeds, further information on additional testbed sites can be found in [32].

Recommendation 19: If would be useful for testbed sites to provide a generic facilities email address and phone number, instead of relying on contacting specific people. For example, email addresses might take a format similar to: *enquiries@[site-name].[tld]* or *[testbed-name]@[organisation].[tld]*.

4.1 Prototype Academic Deployments

As many of the UK CAV testbeds are still in the early stages of deployment, it was necessary to perform a deployment of IEEE 802.11p devices at the campuses of the Universities of Warwick and University of Surrey. These deployments allowed researchers to perform validation of the four innovations before deploying on other testbeds.

4.1.1 University of Surrey

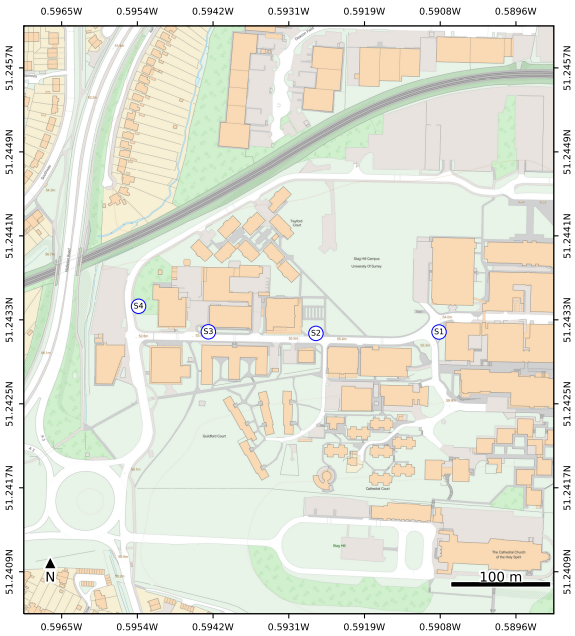
Due to the 5GIC testbed at Surrey focusing on 5G cellular and as our testing needed to be performed with IEEE 802.11p, a prototype deployment of IEEE 802.11p equipment was performed on Surrey's campus. These devices were deployed in the locations shown in Figure 4.1a. The 5GIC van was equipped with an IEEE 802.11p OBU and driven in a loop around the campus.

4.1.2 University of Warwick

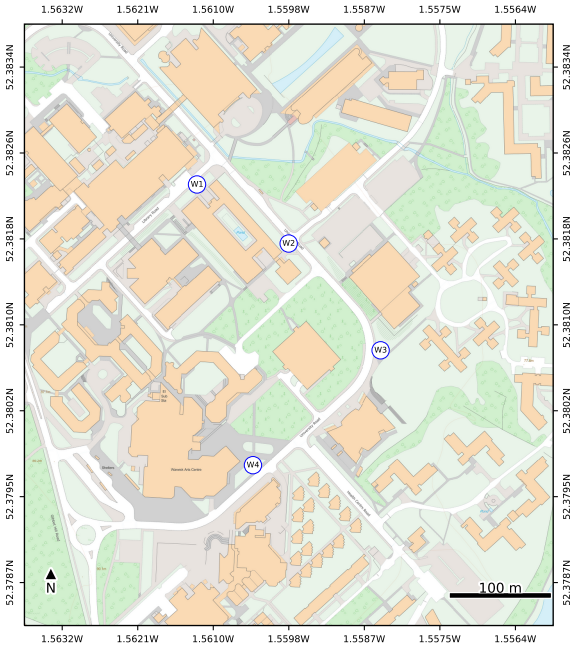
The Midlands Future Mobility testbed (part of which is based at the University of Warwick) was still in an early stage of development and hardware deployment was expected to occur in 2020. Therefore, the technical team at the University of Warwick performed a prototype deployment on campus to inform the development of MFM and highlight use cases for the testbed. The prototype deployment created on University of Warwick's campus was similar to the prototype deployment on University of Surrey's campus. Four Cohda RSUs were deployed in the locations shown in Figure 4.1b. Vehicles were equipped with an IEEE 802.11p OBU and driven in a loop around the campus. If other researchers want to perform a similar deployment, the following are key tasks to perform:

1. Find if there are available outside power sources (mains power/PoE) and network connections.

2. Identify where the devices will be installed.
3. Create a document describing the testing that will be performed.
4. Perform a risk assessment.
5. Request permission for testing and permission to temporarily install equipment.
6. Ensure that the relevant staff have been informed when and where equipment will be installed.



(a) University of Surrey



(b) University of Warwick

Figure 4.1: Prototype Academic Cohda Deployment Locations

4.2 A2/M2 Connected Corridor

The A2/M2 Connected Corridor is a pilot project for a testbed on live roads in London and Kent which are used by actual vehicles. The testbed is a partnership between Highways England, Department for Transport, Transport for London, and Kent County Council with Costain as the lead System Integrator to operate a 100 km connected digital corridor along the A102/A2/M2. As part of the InterCor testfest for Phase 0 of the project, 10 Kapsch RSUs were deployed along the M2 between Junction 3 and Junction 2 [14, Section 3.3.1.1]. The locations of these RSUs [14, Figure 4] are reproduced in Table C.1 and shown in Figure 4.2. There is a *Back-office system interface* providing remote connectivity to the Kapsch RSUs, which are also capable of cellular communications. The project is now in the next phase of development and is expanding the site's area.

URL	`https://intercor-project.eu/homepage/operations-united-kingdom`	
Contacts	Kum Wah Choy	KumWah.Choy@costain.com
Links	DfT Presentation	[21]
	Testfest	`https://intercor-project.eu/intercor-hybrid-testfest`
Time Line	Devices available now	
Comms	IEEE 802.11p (10 Kapsch RSUs)	
Masts	LAN connectivity and power available at the 10 masts	

Table 4.1: A2/M2 Summary

An aspect that needs to be considered when using the A2/M2, is that devices are deployed along a motorway that is constantly in use. This means that installing custom equipment is difficult as a lane would need to be closed to ensure the safety of those performing the installation.

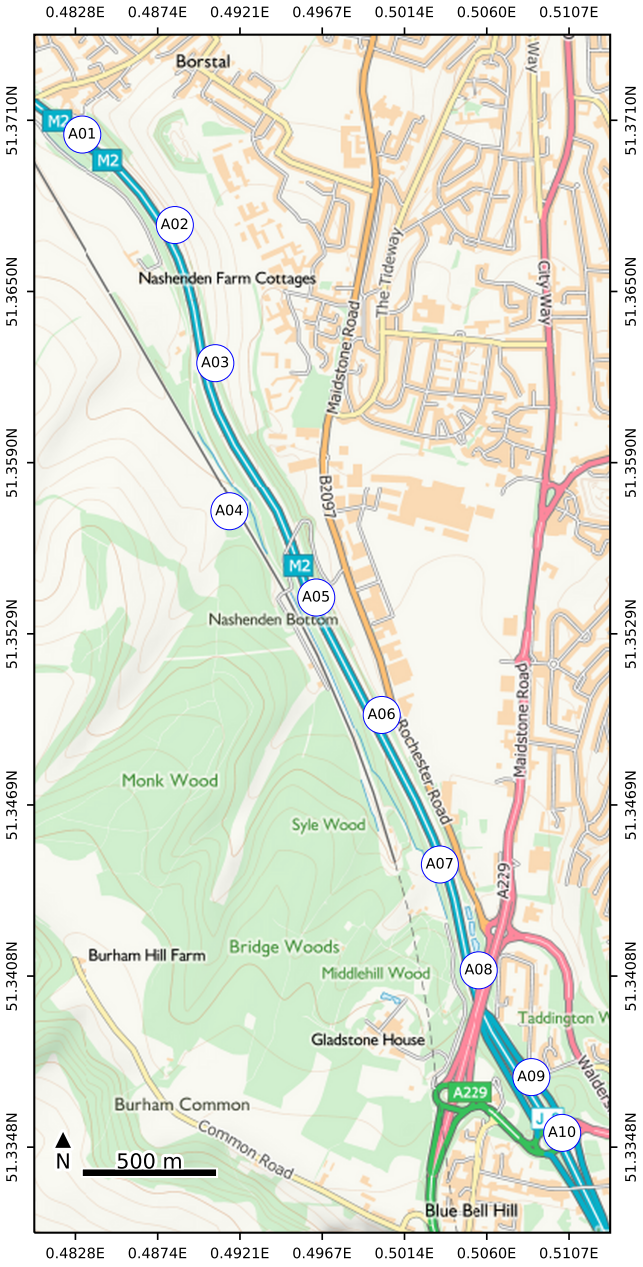


Figure 4.2: Placement of 10 Kapsch RSUs between M2 Junction 2 and Junction 3

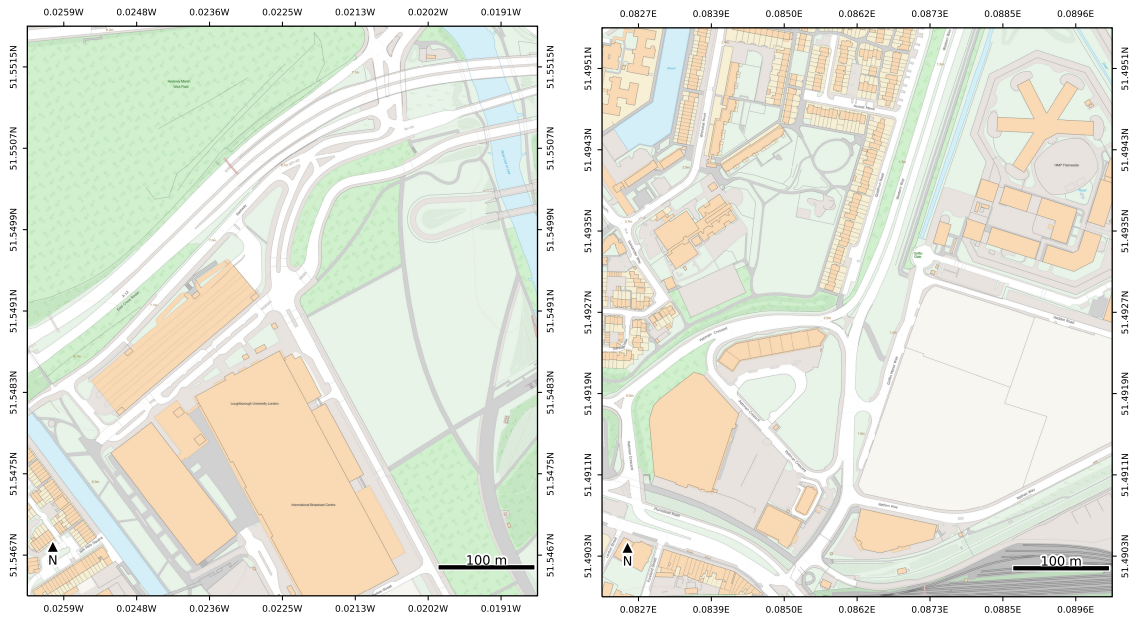
4.3 Smart Mobility Living Lab

The Smart Mobility Living Lab (SMLL) is a testbed aimed at providing a real-world connected environment for testing future mobility technologies, services and business models. The testbed, which is based in London, has two initial pilot sites as shown in Figure 4.3, one in the Royal Borough of Greenwich and a second site at the Queen Elizabeth Olympic Park (QEOP). Future planned developments include adding additional sites and hardware deployed across the QEOP and the Royal Borough of Greenwich. SMLL aims to support testing Intelligent Transport Systems in a real world environment, including deployments of CAVs, automated mobility services, testing commercial fleet operations, and roadside infrastructure deployments. As part of the testbed SMLL will operate a fleet of CAVs that clients can loan to perform their experiments.

SMLL's infrastructure deployment includes posts equipped primarily with WiFi hotspots and CCTV cameras, however others have 4G cellular and IEEE 802.11p V2X Cohda RSU devices deployed. Masts either have access to mains power or PoE.

URL	`https://www.smartmobility.london`
Contacts	James Long jlong@trl.co.uk Thomas Tompkin ttompkin@trl.co.uk
Time Line	Build phase complete by mid 2020
Comms	WiFi on most masts, some equipped with 4G cellular or IEEE 802.11p V2X Cohda RSUs
Masts	Mixture of mains power or PoE supplied to masts

Table 4.2: Smart Mobility Living Labs Summary



(a) Queen Elizabeth Olympic Park (b) Royal Borough of Greenwich

Figure 4.3: Two SMLL Pilot Locations

4.4 Midlands Future Mobility

Midlands Future Mobility (MFM) [5] is a testbed based in the West Midlands with facilities in Coventry, Solihull and Birmingham. There are three main offerings of MFM: (i) the physical infrastructure available to perform testing on public roads, (ii) the digital testing capabilities via a digital twin or the 3xD simulator[1], and (iii) the MFM consortium that provides consulting and facilitates research partnerships. MFM will have deployments of infrastructure over a diverse road network of 80 km including motorways, A roads, B roads, plus rural and unlit roads to enable the testing, deployment and development of CAV systems. A high quality 4G network will be available along the route, with an upgrade to 5G planned for city centres. Future plans include extending the road network available for use in the testbed by over 100 km. The proposed route for MFM is shown in Figure 4.4, of which parts of the deployment reuse aspects of the infrastructure deployed for the UK Connected Intelligent Transport Environment (UK CITE) [3] project. The 3xD simulator will be able to replicate complex scenarios (including the RF environment) found on the route in a repeatable manner. Different procedures will be followed for testing performed on roads compared to using the digital twin/simulator environments for testing. The enquiries contact email address in Table 4.3 should be used to request further information about the testbed or to plan testing.

URL	`https://midlandsfuturemobility.co.uk`
Address	International Digital Laboratory, University of Warwick, University Road, Coventry, CV4 7AL, United Kingdom
Contacts	Enquiries enquiries@midlandsfuturemobility.co.uk
Links	`https://zenzic.io/testbed-uk/midlands-future-mobility`
Time Line	Initial deployment available mid 2020
Comms	120 RSUs and PC5 C-V2X, 5G deployment on Warwick's Campus
Masts	140 CCTV cameras, GNSS RTK Correction

Table 4.3: Midlands Future Mobility Summary

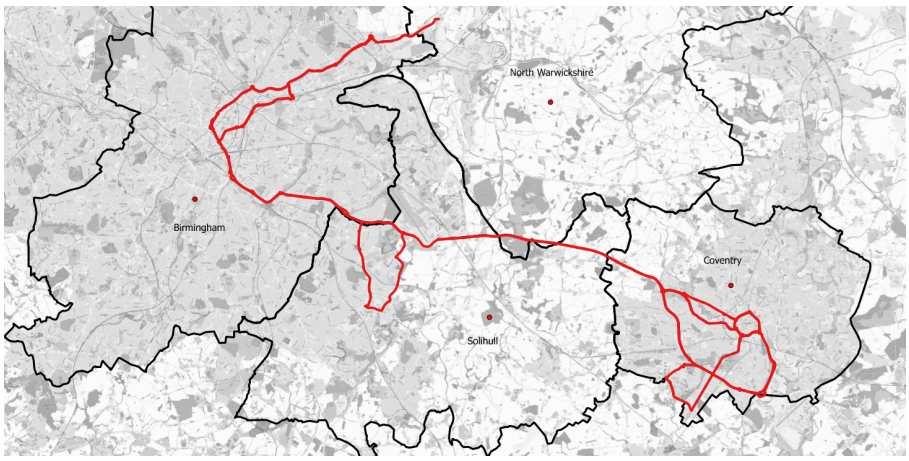


Figure 4.4: Proposed Midlands Future Mobility Test Route

[1] `https://warwick.ac.uk/fac/sci/wmg/research/naic/facilities`

4.5 5G Innovation Centre (5GIC)

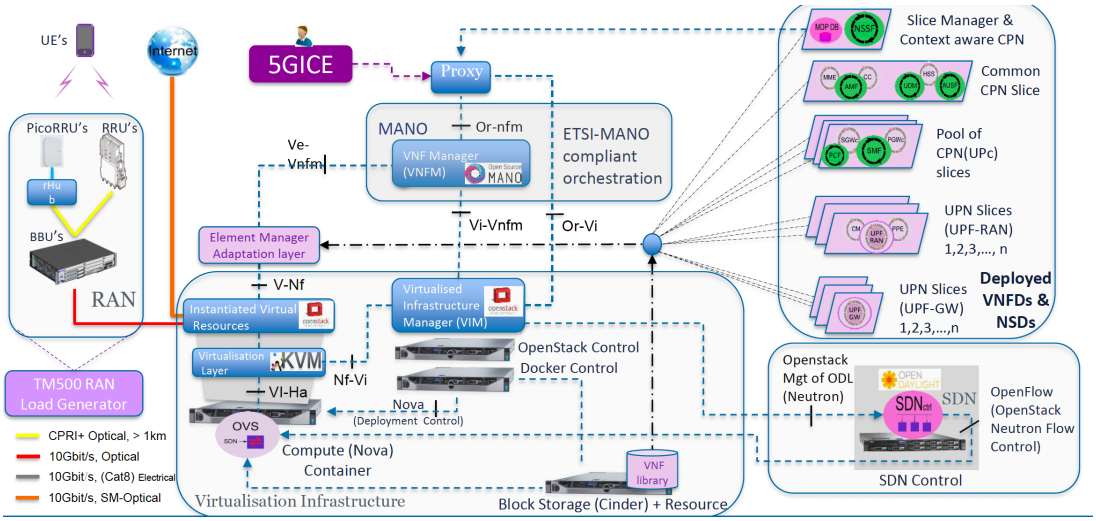


Figure 4.5: 5GIC Virtualisation System Architecture

The 5GIC testbed is not focused on vehicle testing, but instead focuses on testing a real-world deployment of next generation cellular technologies. The testbed covers an area of 4 km^2 comprised of both indoor and outdoor environments, it aims to support broadband mobile devices and Internet of Things devices. This means that C-V2X applications are suitable for testing at the 5GIC tesbed, in the environment of the University of Surry's campus.

Figure 4.5 shows the 5GIC testbed's virtualisation platform, where the virtual mobile core network runs. This involves platforms for network functions virtualisation, OpenStack and ETSI MANO orchestration platform ETSI OSM. The system has been integrated with the 5GIC Exchange (5GICE) middleware which enables user deployment and reservation of network services. The virtualisation platform is connected to the radio access network (RAN) as well as external testbeds, aka islands, via an SDN-enabled transport network.

The testbed is primarily focused on providing testing services to SMEs, telecommunication companies and service companies, it is not intended to be academic focused. There is scope for applications to be deployed to the testbed. In order to do so the testbed team needs to be contacted (the initial contact should be with the 5GIC development team) and there is an approval process which an application will need to go through. Any testing needs to comply with 3GPP security standards. No information on hardware specifications or its location is available without an NDA.

URL	`https://www.surrey.ac.uk/5gic/about/facilities`		
Address	5G Innovation Centre, University of Surrey, Guildford, Surrey, GU2 7XH, UK		
Contacts	5GIC	5gic@surrey.ac.uk	+44 1483 683 622
	Yogaratnam Rahulan	y.rahulan@surrey.ac.uk	+44 1483 683 034
	Haitham Cruickshank	h.cruickshank@surrey.ac.uk	+44 1483 686 007
Comms	NDA Required (No IEEE 802.11p)		
Masts	NDA Required		

Table 4.4: 5GIC Summary

4.6 Millbrook Proving Ground

The Millbrook Proving Ground is located near the village of Millbrook in Bedfordshire and provides testing services on a commercial basis. Millbrook has typically focused on independently aiding members of the automotive industry to develop and test engines, vehicles, tyres, fuels, lubricants and batteries. The site features a wide variety of test tracks, including (i) a high speed bowl capable of emulating a motorway environment, (ii) a hill route with high inclination roads and dense forest, (iii) tracks for testing the handling of a vehicle within a city, (iv) off-road tracks and others [38]. Millbrook can provide a comprehensive test services including vehicles, on-board units, drivers and technical support as required. Millbrook has recently begun expanding its offering to include communications testing with the launch of the AutoAir 5G testbed in February 2019[2]. Millbrook also has a deployment of 40 IEEE 802.11p V2X Cohda RSU devices around the site. Figure 4.6 shows the locations of masts on site, with IEEE 802.11p devices deployed on the MT masts and the majority of the NC and NM masts. Tuning of the Cohda devices is expected to be complete by mid-2019. A number of Cohda on-board units suitable for vehicle mounting are also available for hire.

URL	`https://www.millbrook.co.uk`		
Address	Millbrook, Bedford, MK45 2JQ, United Kingdom		
Contacts	David Kernohan	david.kernohan@millbrook.co.uk	+44 1525 408 720
	Peter Stoker	peter.stoker@millbrook.co.uk	+44 1525 842 519
Links	Track Details	[38]	
	Handbook	[36]	
	Business Ethics	[37]	
Time Line	Devices installed and available mid-2019. A further development of 5G into indoor areas is planned.		
Comms	4G LTE and 5G cellular (77 nodes in 2.3 GHz and 3.7 GHz, 22 in 60 GHz), IEEE 802.11p (40 nodes in flat area and in hills)		
Masts	High bandwidth fibre and mains power available at many masts across the site		

Table 4.5: Millbrook Summary

The following steps need to be completed before commencing testing on site:

1. Create a test plan. This includes a description of the testing that is going to be performed, the resources required and an estimated timetable for the testing.
2. Obtain a quote based on the described test plan through points of contact listed in Table 4.5.
3. Sign the Conditions of Use of the Millbrook facilities agreement.
4. Sign the Terms and and Conditions for Supply of Services agreement.
5. Provide a liability insurance policy of at least £5,000,000.
6. Provide financial details of the user to Millbrook in order to set up the user on Millbrook's financial system.

[2] `https://www.millbrook.co.uk/press-office/news/autoair-5g-test-bed-launched-at-millbrook`

7. Create a Risk Assessment of the testing being carried out.

Due to the multiple companies testing vehicles on site, there is in general no photography allowed unless a day has been deemed a photography allowed day. When entering the site all devices with a camera will have the lens covered to prevent photography. If accompanied by a photo minder then photographs can be taken as long as no other vehicles are present in the picture.

From our experience, Millbrook is open to a number of recommendations that have been made thus far in this document, including:

- Temporarily installing equipment on masts around its site
- Deploying custom firmware and code to their Cohda RSU deployment
- Being able to remotely access devices from a central location across a LAN

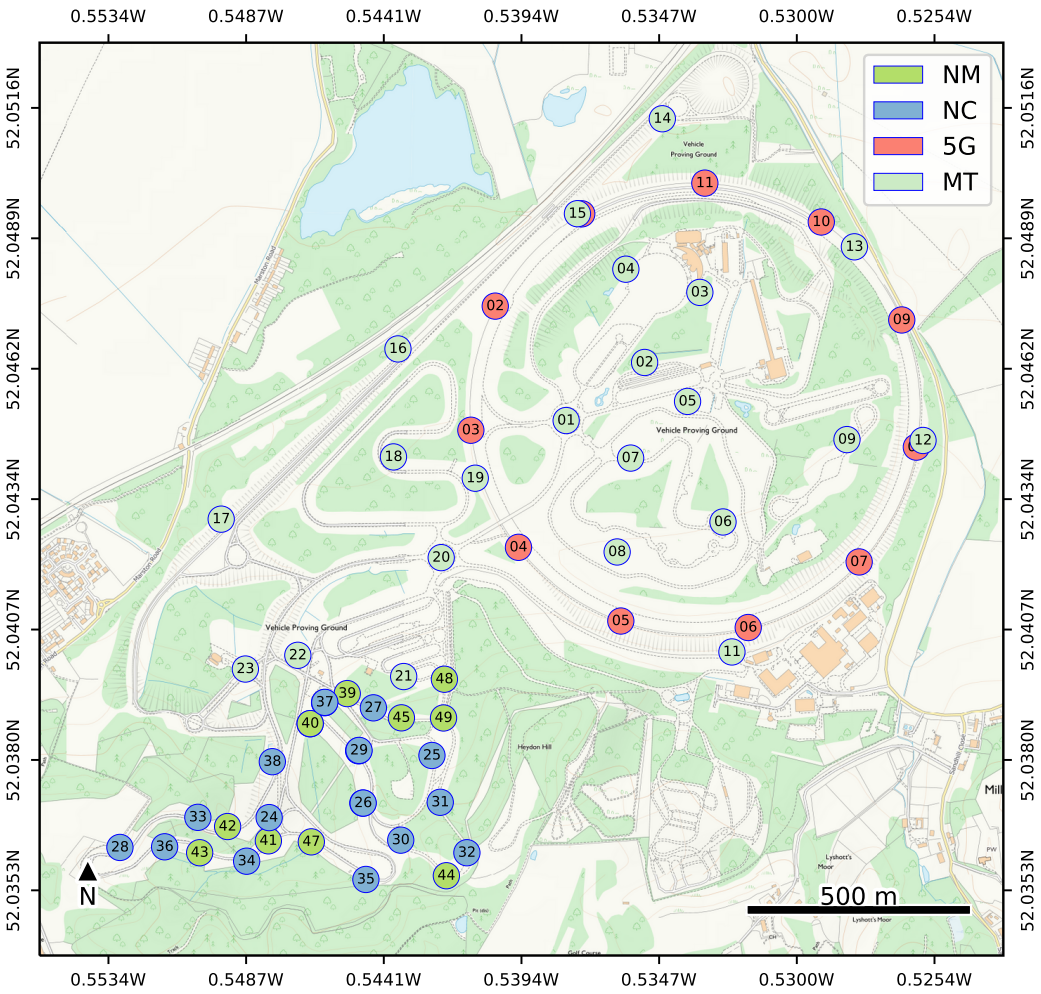


Figure 4.6: Millbrook Mast Locations

Overall, Millbrook currently represents one of the most mature testbed sites for testing in a real but controlled environment. It has the largest deployment of V2X IEEE 802.11p devices of the testbed sites investigated and also a large deployment of masts equipped with 5G infrastructure. As the testbed has well described procedures for performing commercial testing of vehicles, these have been extended to support cyber security aspects of connected vehicle testing.

4.7 HORIBA-MIRA Proving Ground

The HORIBA-MIRA proving ground is located in Nuneaton and provides testing services on a commercial basis. The site serves multiple automotive companies, allowing testing to be performed in a safe and secure environment. The proving ground has a wide variety of tracks totalling more than 95 km over a 750 acre site including: (i) performance circuits, (ii) wet and dry handling areas, (iii) durability surfaces, (iv) cross-country and off-road circuits and (v) a city circuit designed to replicate European/US urban environments with controlled wireless communications infrastructure.

There is also a variety of test equipment usable on site, including: (i) EuroNCAP Vehicle Targets, Guided Soft Targets and Global Vehicle Targets for collision testing, (ii) vulnerable road user targets (with an automated towing system) which includes pedestrian targets, (iii) two robot driver kits (for ADAS testing) and (iv) a RTK-GPS base station.

URL	`https://www.horiba-mira.com/contact/europe-uk-nuneaton/`		
Address	Watling Street, Nuneaton, CV10 0TU, United Kingdom		
Contacts	Site		+44 24 7635 5000
	Tim Edwards	tim.edwards@horiba-mira.com	+44 24 7635 5484
Links	Visitor Information [22]		
Comms	WiFi, IEEE 802.11p DSRC, private GSM network and GPS spoofing		

Table 4.6: HORIBA-MIRA Summary

Due to the multiple companies operating on site, the proving ground operates a no photography policy. If photography is required, permission needs to be obtained more than 24 hours before visiting the site [22].

The procedure to perform testing on site is for potential customers to first examine the capabilities of the testbed site and ensure that their testing requirements can be fulfilled. Once completed, a point of contact listed in Table 4.6 should be contacted to begin inquiring into testing. The technical details of the test plan and the procedures to carry it out can then be discussed between both parties.

The HORIBA-MIRA testbed in Nuneaton offers a variety of unique testing capabilities that will be of interest to researchers performing cyber security testing. Of these capabilities, the ability to spoof GPS signals will be of interest to many researchers. Other capabilities such as the vehicle targets for collision testing will be useful to investigate mitigating cyber-physical attacks.

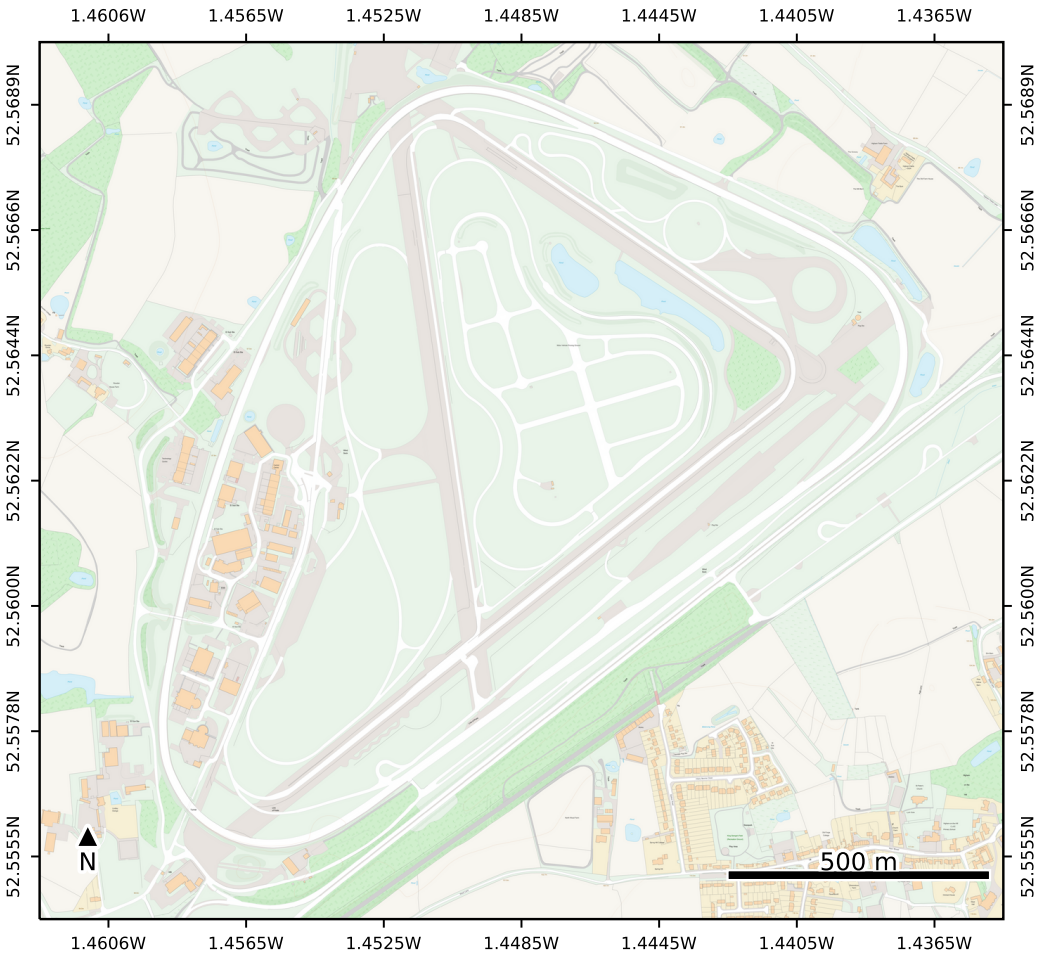


Figure 4.7: HORIBA-MIRA Testbed site

4.8 Bruntingthorpe Proving Ground

The Bruntingthorpe Proving Ground based in Leicestershire is a 670 acre site that offers a variety of commercial services, including: vehicle testing, filming, driver training, highway infrastructure testing and CAV testing. The testbed has a number of tracks and facilities, including: a 6.5 km centre-point circuit featuring a 3.2 km straight, a karting track, off-road circuit and Rough-Terrain Centre. The site features run-off areas intended for the safe testing of autonomous vehicles. Future plans for the site include a £8.4 million development which is expected to be completed by 2020. This enhancement will provide controlled highway test facilities to mimic smart motorways and provide a flexible set of highway intersections for CAV testing.

URL	`http://www.bruntingthorpeprovingground.com` `https://zenzic.io/testbed-uk/cavway`	
Address	Bruntingthorpe Proving Ground, Bath Lane, Bruntingthorpe, Lutterworth, Leicestershire, LE17 5QS, United Kingdom	
Contacts	Site	enquiries@bruntingthorpeprovingground.com +44 116 279 9329
Links	CAV Testing	`https://www.bruntingthorpe.com/proving-ground/services/cav-testing`

Table 4.7: Bruntingthorpe Summary

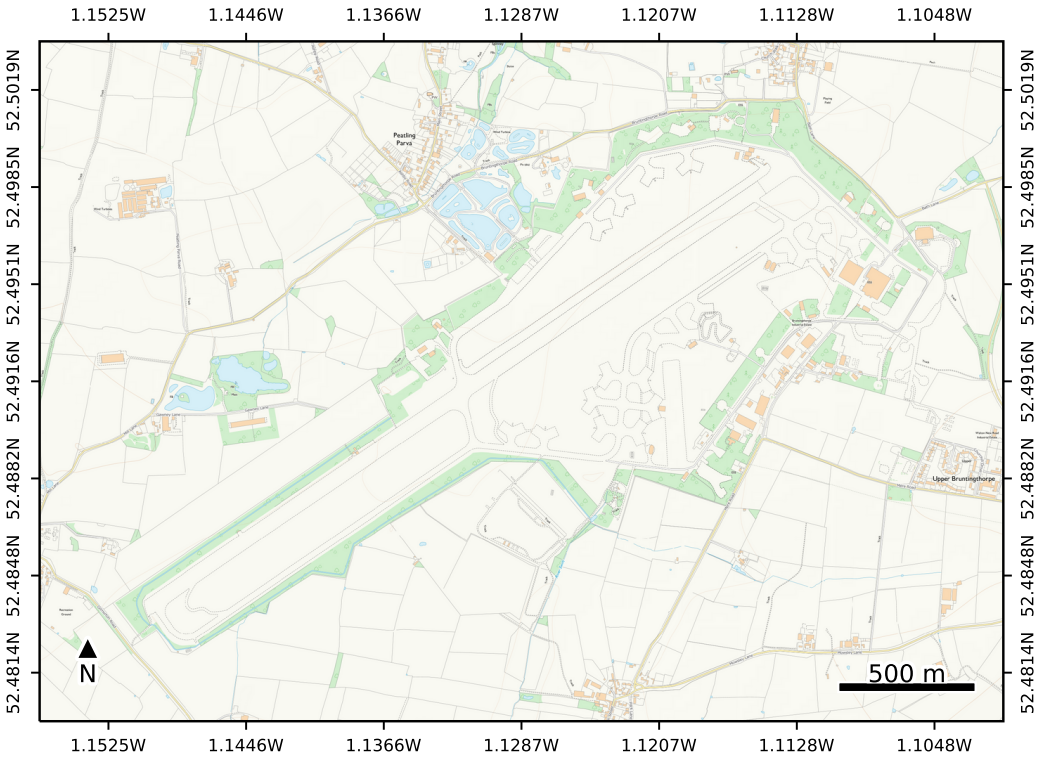


Figure 4.8: Bruntingthorpe Site

4.9 International Context

While this document focuses on examining the CAV testing facilities for cyber security in the UK, it is also important to understand the international context of CAV testing facilities. This section will present details of a select number of international testbeds, however, more details can be found in [32].

4.9.1 InterCor

Interoperable Corridors (InterCor)[3] is a European project which aims to develop collaboration and interoperability between C-ITS corridors in four European nations: (i) Belgium, (ii) France, (iii) the Netherlands and (iv) the UK. The UK component is based along the A2/M2 as has been previously discussed, so this section will focus on the three international components of InterCor. The InterCor project is funded by a €30 million grant co-financed by the European Union under the Connecting Europe Facility. The aim of the project is to investigate vehicular and roadside communication over ITS G5 (IEEE 802.11p), cellular and a combination of the two. By encouraging collaboration the InterCor project aims to develop a set of common standards and specifications to improve interoperability between European nations.

France

URLs	`http://www.scoop.developpement-durable.gouv.fr/en/` `https://intercor-project.eu/homepage/operations-in-france`
Contacts	SCOOP scoop-contact@developpement-durable.gouv.fr
Links	`http://www.scoop.developpement-durable.gouv.fr/en/pilot-sites-a8.html`

Table 4.8: InterCor France Summary

Belgium

URLs	`https://intercor-project.eu/homepage/operations-in-belgium`	
Contacts	InterCor Flanders team (Flemish Agency for Roads and Traffic)	intercor.vlaanderen@wegenenverkeer.be
Links	TESTFEST	`https://intercor-project.eu/cross-border-interoperability-testfest`

Table 4.9: InterCor Belgium Summary

[3] `https://intercor-project.eu`

Netherlands

URLs	`www.its-corridor.nl` `https://intercor-project.eu/homepage/operations-in-the-netherlands`
Contacts	Testbed c-its-corridor@rws.nl
Links	System Concept [19] RSU Locations [24] RSU Placement Guidelines [34]
Comms	3G/4G cellular, IEEE 802.11p (12 nodes)
Future	Plans for the testsite to be extended into the Amsterdam Area within the Concorda project. From summer 2019 LET-V mode 4 will be integrated.

Table 4.10: InterCor Netherlands Summary

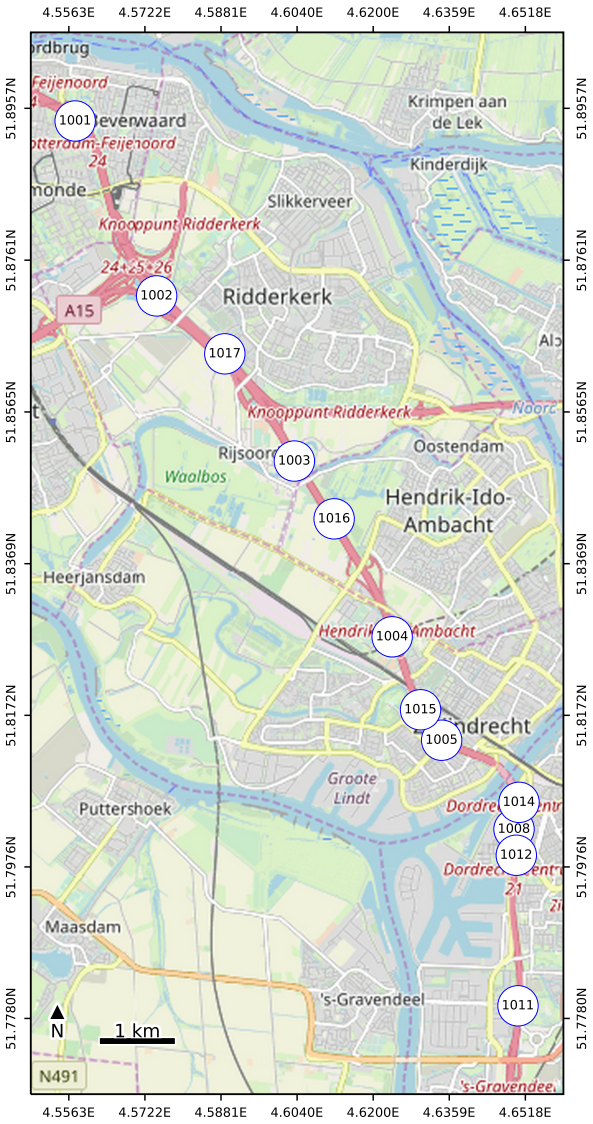


Figure 4.9: Placement of RSUs at InterCor Netherlands

4.9.2 Zala Zone

Zala Zone is a 260 hectare vehicle testbed located in Zalaegerszeg, Hungary funded by a €130 million grant. The majority of the site is still under construction, with some tracks finished in 2018, the majority of tracks expected to be completed in 2020 and smart city developments to be completed by 2022. These tracks will include features such as: a high-speed oval, dynamic surface, braking surfaces, handling courses, motorway section, rural road and a smart city zone. Zala Zone also expects to deploy a variety of ITS technology, including: intelligent traffic control, V2X communications and 5G cellular communications. Expected deployment locations of 27 V2X devices are shown in Figure 4.10. The testbed will host its own telecom and IT environment, and intends to include an automotive cybersecurity test and certification centre.

URL	`https://zalazone.hu/en`
Address	Office Hungary – 1051 Budapest, József nádor tér 2-4. Track Hungary – 8900 Zalaegerszeg, Fészek u. 4.
Contacts	Site zone@apz.hu +36 92 900 117
Time Line	Initial track construction finish 2018, further tracks by 2020 and smart city components by 2022.
Comms	IEEE 802.11p and 5G Cellular (planned)

Table 4.11: Zala Zone Summary

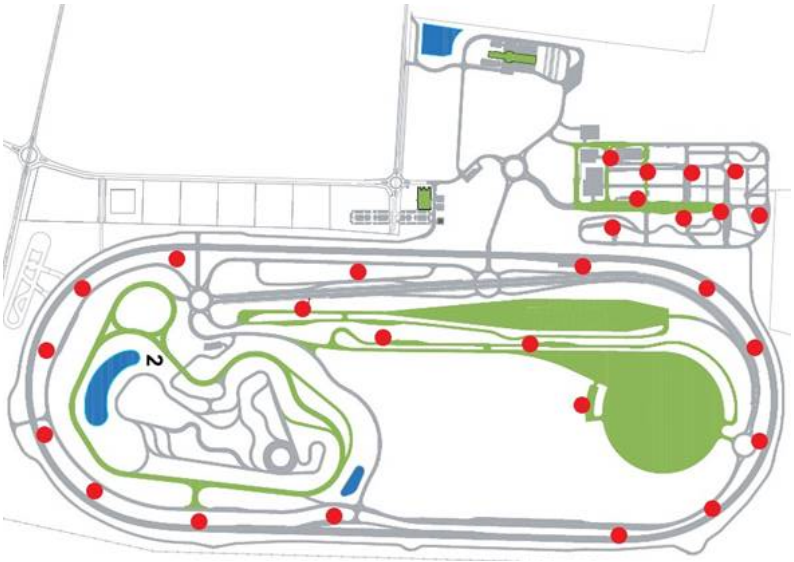


Figure 4.10: Zala Zone Expected V2X Deployment Locations

The target groups of the testbed includes but is not limited to: Developers from Automotive Industry (vehicle functionality) related to V2X applications, V2X application developers, V2X communication technology developers and EuroNCAP active safety tests. The testbed aims to support a number of use cases in client testing, including: (i) Switching between EU and USA V2X standards, (ii) segmentation of the RSU network, (iii) the ability to use a custom PKI system, (iv) C-V2X and (v) the ability to install custom hardware on site. Overall, Zala Zone should be able to provide a number of advanced features useful for performing cyber security testing once the testbed completes construction.

5 Conclusions

In this section we will present the conclusions of the experiences IoT-TRaM project and describe the recommendations to simplify and improve the CAV testing experience in the future.

5.1 Recommended Steps for CAV Cyber Security Testing

From our experiences gained during the IoT-TRaM project these are the recommended steps to perform cyber security testing of CAVs. These stages of testing go from the most accessible to the least accessible, the most repeatable to the least repeatable and the least accurate to the most accurate.

1. Perform experiments in network simulators.

   Aim to test communication protocols between distributed systems. Mobility models needed to simulate moving vehicles. Ability to perfectly reproduce experiments with deterministic simulators.

2. Perform simulations in virtual testbeds.

   Test the impact of a simulated physical environment on the operation of the protocols. The tests become more accurate due to considering more factors but the difficulty of testing and the barriers to performing this testing increases.

3. Perform testing at isolated testbeds (such as Millbrook or HORIBA-MIRA).

   Begin investigating how techniques perform when translated into isolated real world environments. Accuracy of the testing increases due to using real hardware and a real environment, but reproducibility is harder due to the inability to control all factors of a real environment (e.g., weather).

4. Perform testing at testbeds in real world environments (such as university campuses, SMLL or A2/M2).

   Testing is performed in more complicated real world environments. Testing becomes as accurate as is possible in the circumstances because these are the real environments that techniques will be deployed in. Reproducibility is almost impossible due to inability to control the environment. It is important to test at different real world environments from rural to city to motorway environments.

The current state of affairs is that for connected vehicles, most academic researchers will only be able to perform testing in stage #1. This is due to the low accessibility of the later stages.

Recommendation 20: Researchers should aim to test their ideas on testbeds with different environments.

Recommendation 21: Researchers should aim to test on testbeds with equipment from different manufacturers.

5.2 Simplify Deployment for Academia

Performing testing needs to be as simple as possible for testbeds to be adopted by academia. For example, Wireless Sensor Network testbeds (such as FlockLab [29] and FIT/IoT-Lab [12]) allow researchers to upload binaries via a website, have the code automatically tested on the selected devices, and the results returned to the researcher. This happens without the researcher needing to visit a the testbed site. For a number of the communications protocols developed by researchers, an automated test facility available at CAV testbeds would be useful. This could include a V2I device that moves on a track around the testbed site to emulate a moving vehicle. For more complicated (and realistic testing) visiting a testbed site will likely be necessary, however, providing an automated facility that does not require a visit will lower the barriers to entry for academic researchers.

5.3 Digital Models or Digital Twins for Popular Network Simulators

The majority of academic researchers will simulate their contributions on well known simulators (such as NS3 [7] and OMNeT++ [6]). This is because these simulators are free to use, flexible enough to be configured to different scenarios and well known in their communities. CAV testbeds should aim to produce digital models, or digital twins, of their testbeds for these simulators. This information would include roads/tracks, communication equipment locations and environmental features. This information does not need to be highly detailed, as these simulators are used to obtain rough approximations for real-wold performance of novel developments. By providing these configurations testbeds would encourage researchers to undertake a real world deployment on their testbed, as it allows their prior simulated performance to be validated.

5.4 Final Remarks

While the CAV testbeds in the UK are still in early stages of development, it is clear that they will be the future of practical real-world automotive cyber security testing. This report has investigated four academic innovations and the procedures to test them. During this testing a number of challenges have been identified, as well as recommendations to mitigate the risk these challenges pose. Overall, we believe that the recommendations made will reduce the barriers of entry to researchers deploying their work on CAV testbeds and provide realistic measures that testbeds, researchers, industry and government can take to improve the state of CAV cyber security testing.

A Ofcom Application Details

A.1 Cohda

Section C7 For each of the frequency ranges in Table 3.1 the *Bandwidth / class of emission* is **10M0D1D**.

- **10M0** is used because 802.11p specifies a bandwidth of 10 MHz
- **D** is used because 802.11p uses OFDM (a combination of amplitude, frequency, or phase modulation) [23, Section 17]
- **1** is used because 802.11p contains a single digital channel with no subcarrier
- **D** is used because digital data is transmitted

Note that in the FCC application **8M04** is specified as the bandwidth [17], however, this is lower than the 10 MHz bandwidth stated for 802.11p.

Section D1 The *Antenna type* is **Omni-directional Dipole** and the *polarisation* is **Vertical**

Section D2 The *Antenna gain* is 4 dBi

Section D5 The antenna is not directional

Section D6 The proposed transmit power will vary depending on the application. To increase separation of Cohda devices the transmit power will likely be 10 to 13 dBm (−20 to −17 dBW)

Section D7 The maximum transmit power in two antenna mode is 26 dBm (−4 dBW) [16, Table 5]

Other details can be found in the Cohda datasheet, such as the maximum EIRP in [16, Table 6], which may be used in answering **Section D6**.

B Equipment

This appendix lists the equipment purchased plus observations about the equipment. The parts were purchased from RS-Online but they are also likely to be available from other suppliers. The RS-Online catalogue number is provided to allow the same components that were used in this project to be easily found.

Name	Quantity	Unit Price	Link
Cohda SDK	1		
Cohda RSU	6		
Cohda OBU	6		
128 GB MicroSD Card	6	£ 43.44	RS Stock No. 1449019
PoE Battery	4	£393.30	RS Stock No. 1486885
PoE Injector	6	£ 29.42	RS Stock No. 8660089
100 W DC-AC Car Power Inverter	6	£ 30.39	RS Stock No. 5388743
USB 3 to RJ45 Female Ethernet Adaptor	2	£ 25.00	RS Stock No. 1447999
PoE Gigabit Ethernet Switch 8 Port	1	£ 88.64	RS Stock No. 1218132
Green Cat6 Ethernet Cable 3 m	2	£ 3.00	RS Stock No. 0411249
Blue Cat6 Ethernet Cable 3 m	2	£ 2.86	RS Stock No. 0411457
Yellow Cat6 Ethernet Cable 20 m	3	£ 23.04	RS Stock No. 6162564
DC Power Socket 2.1 mm 5 A	6	£ 3.70	RS Stock No. 0487832
DC Power Supply 12 V 2.5 A	6	£ 10.55	RS Stock No. 1440971
2 m Power Cable C13	6	£ 5.42	RS Stock No. 2621154
Viscose Wool Felt Sheet 1 m × 500 mm × 6 mm	1	£ 42.65	RS Stock No. 7336779
Cable Tie 520 mm × 7.7 mm	2 × 100	£ 36.96	RS Stock No. 7538388

Table B.1: Equipment

- Contact Cohda Wireless to obtain a quote for the SDK and hardware. Details of whom to contact can be found at `https://cohdawireless.com/contact`.
- MicroSD cards were needed for the Cohda OBUs to store the logs on. Without these SD cards logs were written to temporary storage and lost on reboot.
- The same number of PoE Injectors were needed as there were RSUs to support deploying all RSUs in the field. The same rationale was used for the number of Car Power Inverters and 12 V PSUs for the OBUs.
- Fewer PoE batteries were purchased than the number of RSUs due to the high cost and the intention that a deployment of four RSUs would be sufficient to perform testing. If mains power is available the other two RSUs are available to be used by the PoE injectors.
- Many laptops no longer come with an Ethernet port, so it is necessary to get an Ethernet adaptor for these devices.

- The Gigabit Switch was useful for deploying to multiple devices simultaneously. If possible test deployments should aim to network the OBUs and RSUs.
- Three 20 m cables were purchased and cut in half to adapt the end of the cable to the M12x1 Cable plug X-coded 8 pol. Cat 6 connector required by the Cohda RSUs. Ethernet cables sold with this connector on one end and an RJ45 on the other were prohibitively expensive (e.g., RS Stock No. 8274524).
- A Wool Felt Sheet was purchased to wrap around the lamp posts RSUs were attached to. This was to prevent scratching to the posts paint due to frequent installation and removal.
- Heavy duty cable ties were purchased to support installing onto masts with a wide diameter. Many of the posts were narrow enough to use the mounting bracket supplied with the RSU. However, for posts that were too wide the cable ties were used instead.

C Device Locations

This appendix contains the locations of devices at different testbed sites. This information is presented with the intention that it is useful to researchers who wish to create digital twins of testbed sites.

ITS-G5 Identifier	Marker Post	Geographic Address	Latitude	Longitude
A1	M2 48/2A	8482A	51.370 542 48	0.483 141 464
A2	M2 48/7A	8487A	51.367 347 67	0.488 374 729
A3	M2 49/2A	8492A	51.362 472 61	0.490 662 534
A4	M2 49/7A	8497A	51.357 245 83	0.491 459 013
A5	M2 50/2A	8502A	51.354 199 72	0.496 369 269
A6	M2 50/8A	8508A	51.350 052 42	0.500 071 270
A7	M2 51/5A	8515A	51.344 772 60	0.503 360 398
A8	M2 51/9A	8519A	51.341 035 08	0.505 553 979
A9	M2 52/3B	8523B	51.337 263 75	0.508 532 577
A10	M2 52/6A	8526A	51.335 293 63	0.510 274 239

Table C.1: Coordinates of Kapsch RSUs along A2/M2 Connected Corridor

ITS-G5 Identifier	Location	Latitude	Longitude
1001	A16Re 22.425	51.894 092	4.557 578
1002	A16Re 25.200	51.871 487	4.574 633
1003	A16Re 28.315	51.850 139	4.603 469
1004	A16Re 31.290	51.827 407	4.623 936
1005	A16Re 32.933	51.814 023	4.634 297
1008	A16Re 34.832	51.802 503	4.649 450
1011	A16Li 37.680	51.779 640	4.650 281
1012	A16Li 35.500	51.799 137	4.649 929
1014	A16Li 34.440	51.805 985	4.650 497
1015	A16Li 32.396	51.817 963	4.629 880
1016	A16Li 29.370	51.842 664	4.611 792
1017	A16Li 26.480	51.864 000	4.588 901

Table C.2: Coordinates of RSUs along InterCor Netherlands [24]

Identifier	Latitude	Longitude
A13P0.4	51.215 978	4.452 957
A13P0.8	51.215 880	4.457 346
A13P1.3	51.211 974	4.461 642
A13P2.1	51.211 190	4.472 604
A13P2.7	51.210 693	4.480 992
A13P3.4	51.211 192	4.491 453
A13P4.2	51.211 539	4.502 529
A13P4.9	51.211 802	4.513 157
A13P5.7	51.212 177	4.524 336
A13P6.5	51.211 740	4.535 233
A13P7.3	51.209 471	4.546 251
A13P8.1	51.206 495	4.557 347
A13P8.8	51.203 977	4.566 204
A13P9.4	51.201 056	4.577 388
A21M11.3	51.202 546	4.597 421
A21N12.5	51.207 450	4.611 264
A21N14.6	51.215 318	4.632 908
A21N15.6	51.224 007	4.648 712
A21N17.6	51.236 131	4.667 921
A21N19.1	51.242 488	4.687 792
A21N21.3	51.243 953	4.720 790
A21N23.2	51.243 830	4.747 280
N12-Liersebaan refpt 13.9	51.244 390	4.592 130
N12-Waterstraat refpt. 15.35	51.251 168	4.609 616

Table C.3: Coordinates of RSUs along InterCor Belgium [25]

Identifier	Latitude	Longitude
M-01	52.043 067	−0.549 526
M-02	52.046 619	−0.543 521
M-03	52.049 489	−0.537 418
M-04	52.051 698	−0.535 089
M-05	52.048 694	−0.527 930
M-06	52.044 670	−0.525 755
M-07	52.040 607	−0.532 402
M-08	52.043 901	−0.540 942
M-09	52.042 241	−0.542 047
M-10	52.039 800	−0.543 348
M-11	52.040 231	−0.546 952
M-12	52.039 865	−0.548 733
M-13	52.044 346	−0.543 708
M-14	52.045 074	−0.537 833
M-15	52.046 442	−0.535 259
M-16	52.047 485	−0.533 670
M-17	52.048 462	−0.535 759
M-18	52.047 938	−0.532 113
M-19	52.045 506	−0.533 561
M-20	52.044 876	−0.528 731
M-21	52.042 991	−0.532 526
M-22	52.044 580	−0.535 518
M-23	52.042 324	−0.536 123

Table C.4: Coordinates of Cohda RSUs at Millbrook

D Requesting Information from Testbeds

The following is a list of questions that was sent to testbeds to request information from them.

- Who should be contacted to organise testing at the site?
- Is the testbed available to academic/industrial researchers?
- What are the procedures for performing testing?
- What equipment is present, where is it located, and what capabilities do they have?
- Are there any datasheets for the hardware available?
- How are the devices connected? (To each other? To the internet?)
- Can programs be deployed to the hardware and what is the process for doing so?
- How can logs of events be obtained from the hardware?
- What format are the logs in?
- If no equipment is present, is the testbed open to researchers bringing their own equipment?
- What are the procedures for setting up custom hardware?
- What are the details of the Ofcom testing licence? Are there any restrictions to the testing that can be performed?
- What developments are expected in the future?

Bibliography

[1] Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band. Standard ETSI EN 302 663, European Telecommunications Standards Institute, July 2013. URL etsi.org/deliver/etsi_en/302600_302699/302663/01.02.01_60/en_302663v010201p.pdf. V1.2.1 (2013-07).

[2] IEEE Standard for Information technology — Telecommunications and information exchange between systems Local and metropolitan area networks — Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)*, pages 1–3534, Dec 2016. doi: 10.1109/IEEESTD.2016.7786995.

[3] UK CITE, 2016–2018. URL https://www.ukcite.co.uk/. Accessed: 2018-11-19.

[4] Intelligent Transport Systems (ITS); Security; Security header and certificate formats. Standard ETSI TS 103 097, European Telecommunications Standards Institute, October 2017. URL https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.03.01_60/ts_103097v010301p.pdf. V1.3.1 (2017-10).

[5] Midlands Future Mobility, 2018. URL https://midlandsfuturemobility.co.uk. Accessed: 2018-11-19.

[6] OMNeT++ Discrete Event Simulator, 2018. URL https://www.omnetpp.org/. Accessed: 2018-11-19.

[7] ns-3 — a discrete-event network simulator for internet systems, 2018. URL https://www.nsnam.org/. Accessed: 2018-11-19.

[8] Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service. Standard Draft ETSI EN 302 637-2, European Telecommunications Standards Institute, November 2018. URL etsi.org/deliver/etsi_en/302600_302699/30263702/01.04.00_20/en_30263702v010400a.pdf. V1.4.0 (2018-08).

[9] Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol. Standard ETSI TS 102 636-5-1, European Telecommunications Standards Institute, May 2019. URL https://www.etsi.org/deliver/etsi_en/302600_302699/3026360501/02.02.01_60/en_3026360501v020201p.pdf. V2.2.1 (2019-05).

[10] Intelligent Transport Systems (ITS); GeoNetworking; Port Numbers for the Basic Transport Protocol (BTP). Standard ETSI TS 103 248, European Telecommunications Standards Institute, April 2019. URL https://www.etsi.org/deliver/etsi_ts/103200_103299/103248/01.03.01_60/ts_103248v010301p.pdf. V1.3.1 (2019-04).

[11] The Wireless Telegraphy (Intelligent Transport Systems) (Exemption) Regulations 2011, (SI 2011/2949). URL http://www.legislation.gov.uk/uksi/2011/2949/made/data.pdf. Accessed: 2018-11-21.

[12] C. Adjih, E. Baccelli, E. Fleury, G. Harter, N. Mitton, T. Noel, R. Pissard-Gibollet, F. Saint-Marcel, G. Schreiner, J. Vandaele, and T. Watteyne. FIT IoT-LAB: A large scale open experimental IoT testbed. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, pages 459–464, Dec 2015. doi: 10.1109/WF-IoT.2015.7389098.

[13] Shihan Bao, Ao Lei, Philip Asuquo, Haitham Cruickshank, Zhili Sun, Michael Huth, and Carsten Maple. Pseudonym management through blockchain: Cost-efficient privacy preservation on intelligent transportation systems. (In Submission).

[14] Jason Burrows. InterCor UK TESTFEST - Plan of Action. Technical report, InterCor, 2018. URL `http://intercor-project.eu/wp-content/uploads/sites/15/2018/08/InterCor_UK-InterCor-Testfest-Action-Plan_v2.pdf`. Accessed 2018-09-12.

[15] Centre for Connected & Autonomous Vehicles. UK Connected & Autonomous Vehicle Research & Development Projects 2018. Guidance Document V3, UK Government, September 2018. URL `https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/737778/ccav-research-and-development-projects.pdf`. Accessed: 2019-05-27.

[16] Cohda Wireless. Cohda Mobility MK5 Module Datasheet, May 2015. URL `https://fccid.io/2AEGPMK5RSU/User-Manual/User-Manual-2618067.html`. Accessed: 2018-09-17 Version: 1.2.0.

[17] Cohda Wireless. Application for Equipment Authorization FCC Form 731 TCB Version, 2017. URL `https://apps.fcc.gov/tcb/GetTcb731Report.do?applicationId=YNexwKnh4MXDAw3X%2FkdoOg%3D%3D&fcc_id=2AEGPMK5RSU`. Accessed: 2019-05-09.

[18] Cohda Wireless. User Licence Agreement. Online, 2018. URL `http://www.cohdawireless.com/sdklicence/`. Accessed: 2018-10-24.

[19] Cooperative ITS Corridor Project Technical Team. *Description of the System Concept: Cooperative ITS Corridor System (ICS)*. Rijkswaterstaat, July 2016. URL `http://intercor.diviprojects.wpengine.com/wp-content/uploads/sites/15/2017/06/Cooperatieve-ITS-Corridor-Description-of-the-System-Concept-Final_v1.0-20160704.pdf`. Accessed: 2019-05-29.

[20] Matt Crawford. Transmission of IPv6 Packets over Ethernet Networks. RFC 2464, December 1998. URL `https://rfc-editor.org/rfc/rfc2464.txt`.

[21] Department for Transport. The A2/M2 (London to Dover) Connected Vehicle Corridor, April 2016. URL `https://www.codecs-project.eu/fileadmin/user_upload/pdfs/Workshop_C-ITS_Deployment_underway_II/Hanson_InterCor_UK.pdf`. Accessed: 2018-09-12.

[22] HORIBA-MIRA. Welcome Information, August 2018. URL `https://www.horiba-mira.com/wp-content/uploads/2018/08/Visitor-Information-Guide-HM.pdf`. Accessed: 2019-05-15.

[23] IEEE Computer Society. IEEE Standard for Information technology — Telecommunications and information exchange between systems — 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. Online, July 2010. URL `https://www.ietf.org/mail-archive/web/its/current/pdfqf992dHy9x.pdf`. Accessed: 2018-10-22.

[24] InterCor. RSU coordinates, June 2017. URL http://intercor.diviprojects.wpengine.com/wp-content/uploads/sites/15/2017/06/TESTFEST-RSU-coordinates.pdf. Accessed: 2019-05-29.

[25] InterCor. InterCor TESTFEST - Flanders Pilot Site - routes (draft), March 2019. URL https://www.google.com/maps/d/viewer?mid=1VQpDUjrhAn04xDi1VZNX8Iay_TZwtelY&ll=51.224342543095425%2C4.59844499999997&z=12.

[26] Kapsch. Declaration of conformity, February 2018. URL https://www.kapsch.net/ktc/downloads/datasheets/rf-field/5-9/DoC-RIS-9160.pdf?lang=en-US. Accessed: 2018-11-21.

[27] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. *IEEE Internet of Things Journal*, 4(6):1832–1843, Dec 2017. ISSN 2327-4662. doi: 10.1109/JIOT.2017.2740569.

[28] Philip Levis, Nelson Lee, Matt Welsh, and David Culler. Tossim: accurate and scalable simulation of entire tinyos applications. In *Proceedings of the 1st international conference on Embedded networked sensor systems*, SenSys '03, pages 126–137. ACM, 2003. ISBN 1-58113-707-9. doi: 10.1145/958491.958506.

[29] R. Lim, F. Ferrari, M. Zimmerling, C. Walser, P. Sommer, and J. Beutel. Flocklab: A testbed for distributed, synchronized tracing and profiling of wireless embedded systems. In *2013 ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, pages 153–165, April 2013. doi: 10.1145/2461381.2461402.

[30] Jia Liu, Liqun Chen, Mehrdad Dianati, Carsten Maple, and Yan Yan. Efficient anonymous signatures with event linkability for V2X communications. In Submission.

[31] Ben Lynn. PBC Library. URL https://crypto.stanford.edu/pbc/. Accessed: 2019-05-24.

[32] Carsten Maple, Duncan Chambers, Jeremy Morley, Jim O'Reilly, Kevin Ghirardello, Miles Elsden, Sylvester Kaczmarek, and Tuan Le. Guidelines: Demonstrators for Secure and Resilient Transport and Mobility. Technical report, University of Warwick. (To Appear).

[33] Carsten Maple, Matthew Bradbury, Haitham Cruickshank, Hu Yuan, Chen Gu, and Phillip Asuquo. IoT Transport and Mobility Demonstrator: Cyber Security Testing on National Infrastructure. Technical Report Version 1.0, University of Warwick, May 2019.

[34] MAPtm. *RSU Placement Guidelines*. Rijkswaterstaat, October 2016. URL http://intercor.diviprojects.wpengine.com/wp-content/uploads/sites/15/2017/06/RSU-Placement-Guidelines_v-1.0.pdf. Accessed: 2019-05-29.

[35] Met Office. *Cartopy: a cartographic python library with a Matplotlib interface*. Exeter, Devon, 2010 - 2015. URL http://scitools.org.uk/cartopy.

[36] Millbrook. Test Tracks, November 2015. URL http://www.millbrook.co.uk/media/1742/tcp002-iss-3-users-handbook.pdf. Accessed: 2019-05-10.

[37] Millbrook. The value of integrity: Code of Business Ethics, 2016. URL https://www.millbrook.co.uk/media/1772/5618_spc_coe_mil_eng_pt.pdf. Accessed: 2019-05-10.

[38] Millbrook. Test Tracks, 2017. URL http://www.millbrook.co.uk/media/1460/track-facilities-brochure_web.pdf. Accessed: 2019-05-10.

[39] Ofcom. Ofw225 Innovation and trial licence application form. URL https://www.ofcom.org.uk/__data/assets/pdf_file/0023/80780/application_form_ofw225.pdf. Accessed: 2018-10-22.

[40] Ofcom. Short Range Devices Information Sheet, July 2010. URL https://www.ofcom.org.uk/spectrum/radio-spectrum-and-the-law/licence-exempt-radio-use/licence-exempt-devices/short-range-devices-information. Accessed: 2019-05-10.

[41] Ofcom. Frequency bands designated for Industrial, Scientific and Medical use (ISM), June 2017. URL https://www.ofcom.org.uk/__data/assets/pdf_file/0022/103297/fat-ism-frequencies.pdf. Accessed: 2018-11-21.

[42] Ofcom. IR 2030 - UK Interface Requirements 2030 Licence Exempt Short Range Devices. https://www.ofcom.org.uk/__data/assets/pdf_file/0028/84970/ir-2030-july-2017.pdf, 2018. Accessed: 2018-11-13.

[43] Ofcom. Innovation and trial licensing. Online, March 2018. URL https://www.ofcom.org.uk/manage-your-licence/radiocommunication-licences/non-operational-licences. Accessed: 2018-10-22.

[44] Fredrik Österlind. A sensor network simulator for the contiki os. Technical report, SICS publications database [http://eprints.sics.se/perl/oai2] (Sweden), 2006.

[45] Christoph Sommer, Reinhard German, and Falko Dressler. Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis. *IEEE Transactions on Mobile Computing*, 10(1):3–15, January 2011. doi: 10.1109/TMC.2010.133.

[46] Michael Tuexen, Fulvio Risso, Jasper Bongertz, Gerald Combs, and Guy Harris. PCAP Next Generation (pcapng) Capture File Format. Internet-Draft draft-tuexen-opsawg-pcapng, IETF Secretariat, May 2019. URL http://xml2rfc.tools.ietf.org/cgi-bin/xml2rfc.cgi?url=https://raw.githubusercontent.com/pcapng/pcapng/3c35b6abf9171e767e4b2470e691c22346b7105e/draft-tuexen-opsawg-pcapng.xml&modeAsFormat=html/ascii&type=ascii. Accessed: 2019-05-14. Expires: 2019-11-15.

[47] Veracity. Battery Powered POE Injector, 2018. URL http://www.veracityglobal.com/products/ip-camera-installation-tools/pointsource-plus.aspx. Accessed: 2018-11-20.