RULE-BASED INCIDENT RESPONSE FOR VEHICLE SAFETY AND SITUATIONAL AWARENESS

Initial Plan

Author and Supervisor:

Author: Mark Burnitt
Supervisor: Neteesh Saxena
Module: CM2303
Credits: 40

Mark Burnitt

Contents

Abstract and Project Description 2
Aims and Objectives 3
Overall Aim 3
Specific Objectives 3
Ethical Considerations 3
Work Plan 4
As a detailed list: 4
As a Gantt Chart: 5
References 6

Abstract and Project Description

There are 38.8 million licensed vehicles [1] on the roads of the UK alone. Of these, the vast majority are cars, then both Light and Heavy Goods Vehicles, as well as buses and coaches and other vehicles (there are also motorcycles, but they are not relevant to this project). Inside each of these vehicles, there are a number of ECUs (Electronic Control Units) that provide basic and advanced functionalities to the vehicle, ranging from the Engine Control Unit, safety critical systems such as the airbags and non-critical systems like the speakers or the air conditioning. These ECUs all need to communicate with one another and to do this, they may use one of three methods, depending on the ECU in question and how old the vehicle in question is. Prior to 1986, these ECUs would have specialized point to point wiring to connect them together, which worked, but was more complicated than it needed to be. After 1986, Bosch released the first CAN bus [2], to allow all of the ECUs a single line of communication to one another, which was (originally) standardized as ISO11898 in 1993. It has been updated several times since then, the latest of these CAN-FD as ISO11898-1 and ISO11898-2 in 2015 and 16. This represents a highly efficient, centralized, and robust system for the vehicle's ECUs to communicate. More modern vehicles may also contain 1 or more LIN bus(es) [3], which are much cheaper than the CAN system, but also carry far less data and are less tolerant of faults. As such, the LIN bus will only be used in non-safety critical applications, such as electric windows and air conditioning systems (vehicles made prior the adoption of the LIN bus will have these ECUs directly on the CAN bus instead).

The CAN system is well designed for what it was intended to do, though it is not without its shortcomings in certain areas. One of these is unfortunately is security, as the system is vulnerable to a variety of different attacks, conducted with or without physical access to the bus via the OnBoard-Diagnostics-II (OBD-II) port (required by US law since 1996 and EU laws from 2002 for petrol and 2007 for diesel cars [4]). CAN systems do not implement (as standard) any kind of encryption or authentication of the messages that travel across them, so a skilled attacker can take advantage of this to perform various types of attack against the vehicle, that can range from sending the usage data remotely to a sever owned by an attacker to disabling safety critical ECUs such as the controller for the ABS system. Most attacks do require access to the OBD-II port, though especially with the rise of cloud computing and the IoT driving ever more devices to be connected to the internet, more and more vehicles themselves are getting connected to the Internet, making the remote attack vector more and more viable [5]. This makes it ever more important to have systems onboard the vehicle to be able to detect and potentially counteract the activities of cyber criminals. Systems for the former is what this project shall consider, and approaches have already been designed and tested. In particular, this paper [6] explored the use of machine learning (specifically a Generative Adversarial Network or GAN) to process the CAN data and be able to identify which frames corresponded to those of an attack and which were normal traffic. This paper [7] also used a machine learning based approach for IDS, though instead of a GAN, they used a Deep Convolutional Neural Network (DCNN) rather than a GAN. This project shall aim to improve on the statistics reported by these two papers, by exploring alternate approaches and network constructions. By using the same dataset as both of them, the statistics may be compared directly.

Aims and Objectives

Overall Aim

To create a software package that increases incident response capabilities by improving the situational awareness of vehicle systems.

Specific Objectives

To achieve the above, I have determined that the system should fulfil all of the described points below:

- Using only the CAN traffic captured from a vehicle, be able to identify whenever a cyber-attack takes place on the given CAN network.
    - The system must be able to take raw CAN traffic as its sole input.
    - The system must be able to classify the malicious CAN packets with a high degree of precision and accuracy
    - The system must be able to be able to identify at minimum, DoS, Spoofing and Fuzzy attack types
    - The system should be able to recognize attacks of an unknown type and still classify them correctly
    - The system must respond very quickly, as CAN is a real time network and should be able to cope with the volumes of data passed across it.
    - The system should achieve better performance than existing systems of a similar nature
    - The system must be able to report its results in an easily understandable format.

Ethical Considerations

This project does not require working with personal data, and as such, does not require approval by the ethics committee.

Work Plan

As a detailed list:

Week 1 (beginning 1st February): Conduct research into the area, to a standard that is necessary for the project to proceed, as well as deliver an Initial Plan that is agreed on by both myself and the Project Supervisor. (First Deliverable: Initial Plan due no later than 8th Feb.)

Week 2 (beginning 8th February): While conducting further research if necessary, select a feasible number of approaches to explore and design further.

Week 3 (beginning 15th February): Once the approaches have been planned, begin to implement the chosen approaches to a functional standard.

Week 4 (beginning 22nd February): Continue to implement the chosen approaches to the necessary standard.

Week 5 (beginning 1st March): Test the approaches for functionality, and then again, recording appropriate metrics for each of them.

Week 6 (beginning 8th March): For the approach that appears the most promising, attempt to adjust and optimize it for improved performance or other desirable characteristics.

Week 7 (beginning 15th March): Continuation of optimization and testing. Potential to return to previous steps if the chosen system does not meet required standards.

Week 8 (beginning 22nd March): Build a GUI or other appropriate system to display results to the users, as well as to tie together the underlying functionality.

Week 9 (beginning 29th March): Finish implementing and conduct testing to an appropriate standard on the GUI.

Week 10 (beginning 5th April): Add any additional features, unit test them and integrate everything into one cohesive package. Unit and user test completed package. (Second Deliverable: Project Code due by 11th April).

Week 11 (beginning 12th April): Start writing final report, as well as conduct additional testing should it be requested or not yet completed to a satisfactory standard.

Week 12 (beginning 19th April): Continue work on the final report.

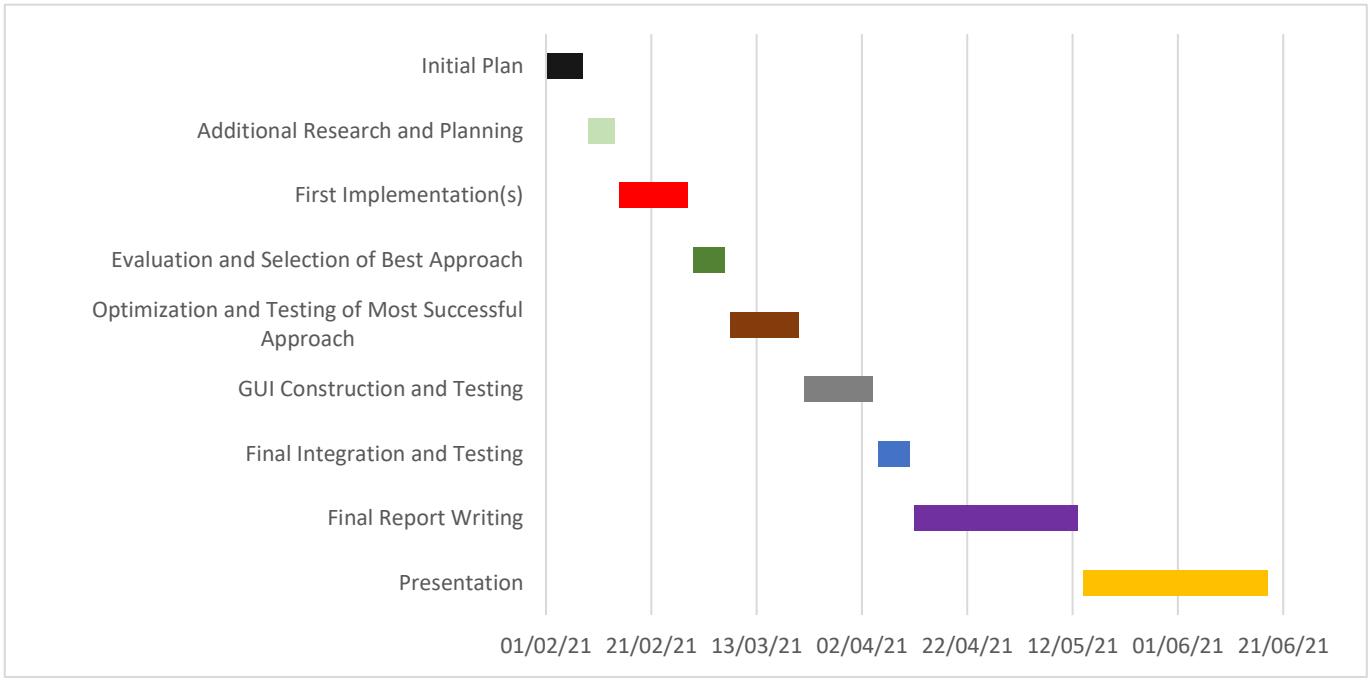
Week 13 (beginning 26th April): Continue work on the final report.

Week 14 (beginning 3rd May): Continue work on the final report.

Week 15 (beginning 10th May): Continue work on the final report. (Third Deliverable: Final Report due no later than 14th May)

Period from 17th May to 18th June: Present the project when scheduled in the timetable (as of this, that has not yet been released).

As a Gantt Chart:



References

[1] https://www.racfoundation.org/motoring-faqs/mobility#a1 01/02/2021 10:43

[2] https://www.csselectronics.com/screen/page/simple-intro-to-can-bus/language/en 01/02/2021 10:52

[3] https://www.csselectronics.com/screen/page/lin-bus-protocol-intro-basics/language/en 01/02/2021 11:03

[4] https://www.scantool.net/blog/how-do-i-know-whether-my-car-is-obd-ii-compliant/ 01/02/2021 13:38

[5] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7219335/ 01/02/2021 13:47

[6] https://arxiv.org/pdf/1907.07377.pdf 06/02/2021 13:04

[7] https://www.sciencedirect.com/science/article/pii/S2214209619302451 06/02/2021 13:20