

Attack ECU Project

USER MANUAL

By Jake Hayward

Contents

Attack ECU Project	1
Introduction	2
Starting the Application/Overview	3
How to open the application	3
System Layout	4
Start/Stop of the ECU simulation	4
Logged data	5
Use of Application	8
Attack 1 (simple Message injection)	8
Attack 2 (On Message)	10
Attack 3 (Incremental Change)	12
Attack 4 (ignition off)	14
Attack 5 (Timed)	17

Introduction

The following document is to be used in conjunction with the CANoe application ‘Attack ECU Project’ this application allows a user to create/replicate CAN bus attacks on a simulated vehicle network. From this the results of the attacks can be viewed through logged data taken from the CAN network. The application contains 5 attack profiles each with their own display and control panels. This manual will briefly explain how to use the application in order to achieve results.

Starting the Application/Overview

How to open the application

The Attack ECU Project is in the format of a windows folder this should be given to you (The User) and contains all the Files that enable the application the run on CANoe. Please avoid editing or extracting files from the folder as it could cause a malfunction in the application within CANoe.

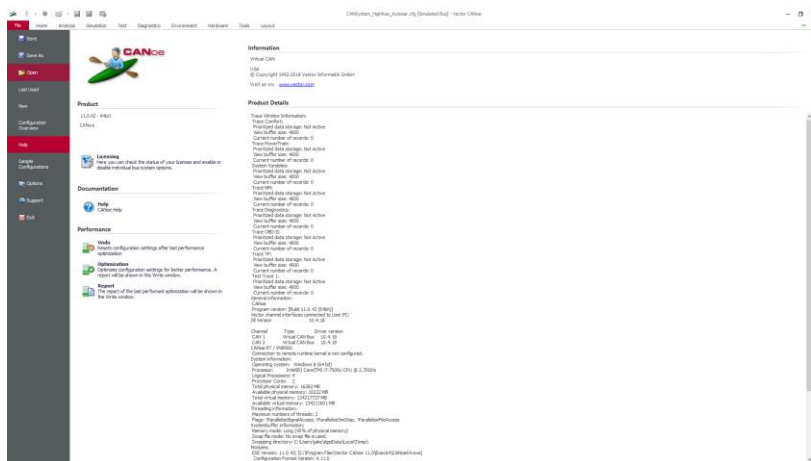


Figure 1- Location for Opening an application within CANoe 11.0

Once in CANoe to open the application: **File > Open.**

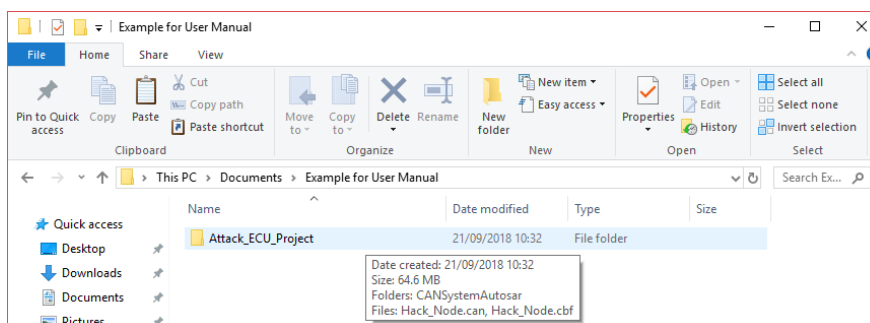


Figure 2- Attack_ECU_Project Folder

The configuration file is located inside the **Attack_ECU_Project** folder.

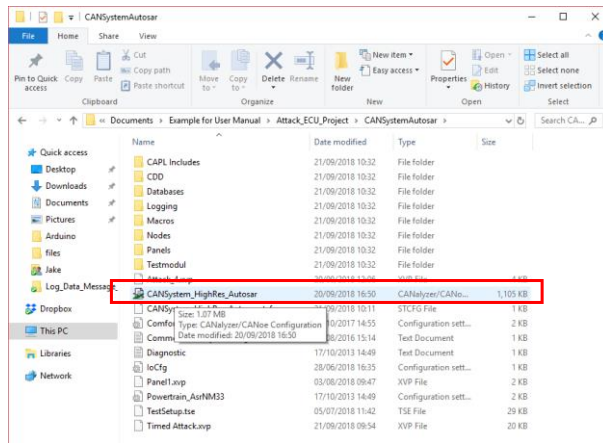


Figure 3- Location of the configuration file inside the 'Attack ECU Project' folder

Commented [JH1]: Explain how the folder is given to the user and how this contains all of the application and the configuration file is within this.

File Location: **Attack_ECU_Project > CANSystemAutosar > CANSystem_HighRes_Autosar.**

System Layout

The location of the attack profiles is highlighted above. The application can be navigated by clicking on each of these tabs to bring up the desired window.

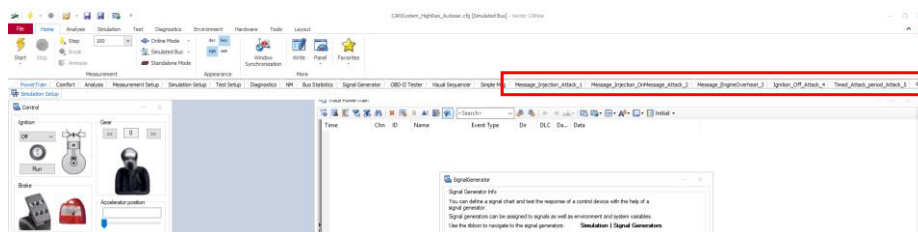


Figure 4- Screenshot displaying the location of the attack profile tabs

Start/Stop of the ECU simulation

The ECU simulation can be started using the toolbar located at the top of the application.

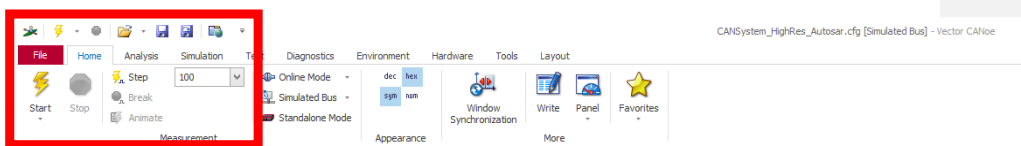


Figure 5- Screenshot of heading tool bar showing simulation control

The ECU simulation can also be controlled using the button located on the control panel for each attack.



Figure 6- START/STOP button used on all control panels.

Logged data

To obtain the bus traffic from the CAN network a logging file must be active.

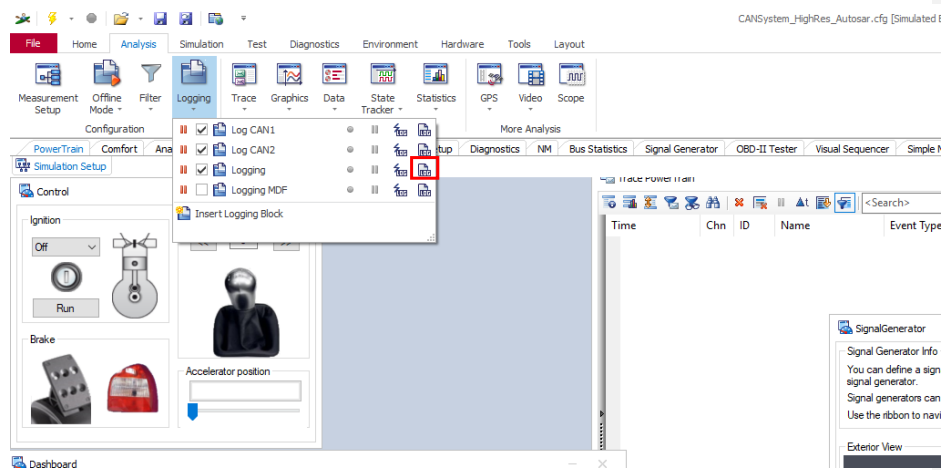



Figure 7- Screen capture of log data location

Activating data logging:

1. Go to **Analysis > Logging**.
2. Tick the **Log CAN1**, **Log CAN2** and **Logging** files.
3. To open the configuration setting click  icon.

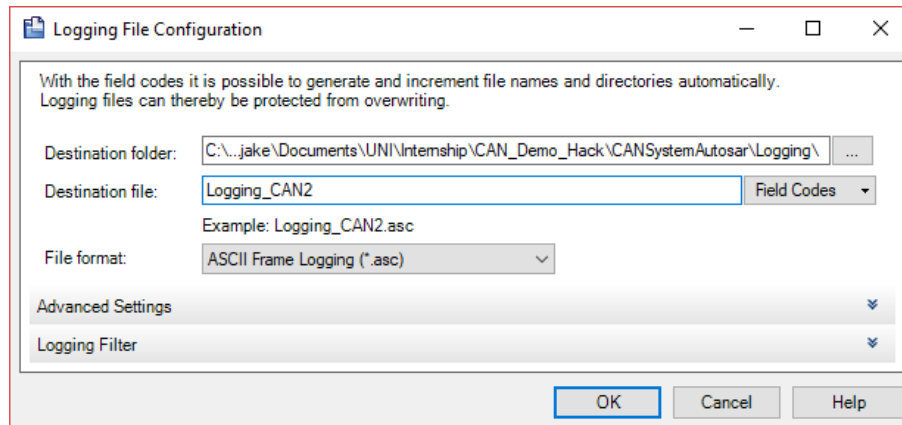


Figure 8- Log Data configuration window

Editing Data logging:

1. Above shows the **file path** for the CAN bus log files.
2. The **file format** can also be changed if required.

You will find the log files inside the Attack_ECU_Project folder.

File location: **Attack_ECU_Project > CANsystemAutosar > Logging.**

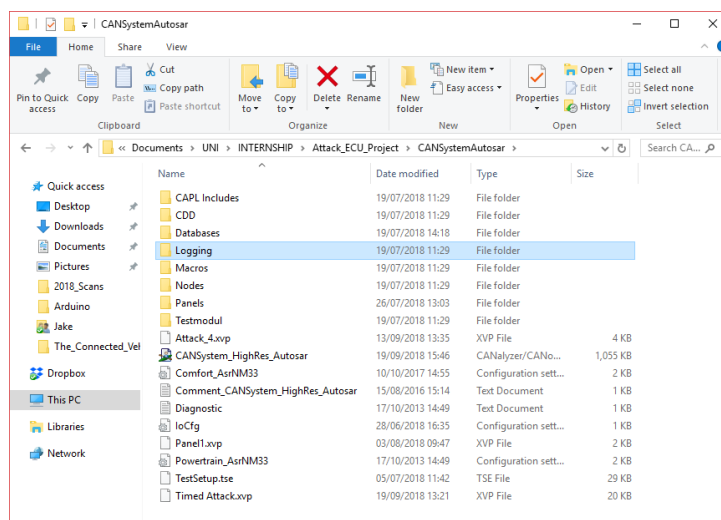


Figure 9- Location of logged data within the 'Attack_ECU_Project' folder.

Note: When using the CANoe application please ensure that the Log files have been renamed and saved before starting the ECU again. When the ECU is started the current log file is overwritten.

CAN message ID

Table showing the CAN messages used in the simulation

Message ID	Message Name	CAPL Denotation
67	Ignition Info	Msg1
C9	ABS data	Msg2
1A0	Console_1	Msg3
64	EngineData	Msg4
1F0	Door_1	N/A

Commented [JH2]: Can node ID table for reference to CAN messages?

Use of Application

Attack 1 (simple Message injection)

The Initiate attack button will instantly place the number of messages created onto the CAN bus. This action can be completed as many times as required. Each message is injected as soon as the bus is available. CAN arbitration applies, so an injected message might take priority for broadcast, or be held from broadcasting depending on the rank of messages also being broadcast.

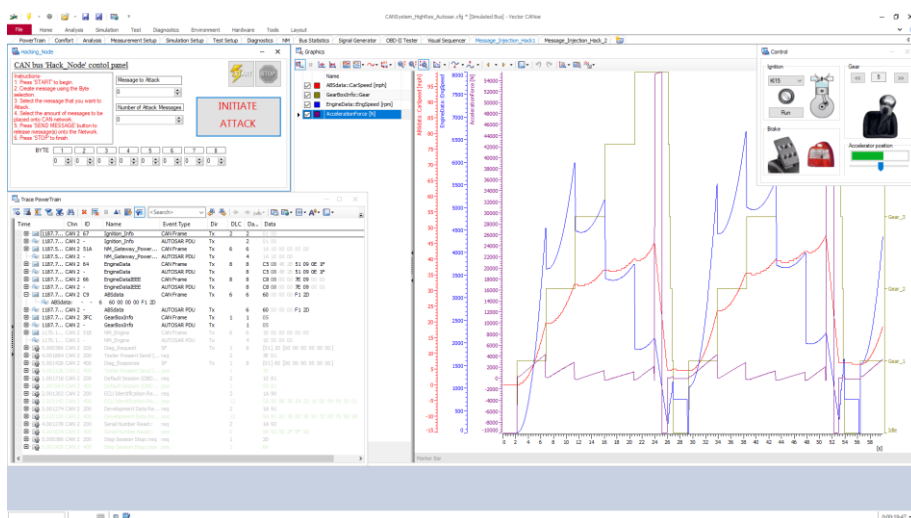


Figure 10- Display for the simple message injection.

Open configuration and select 'Message_Injection_Attack_1' tab.

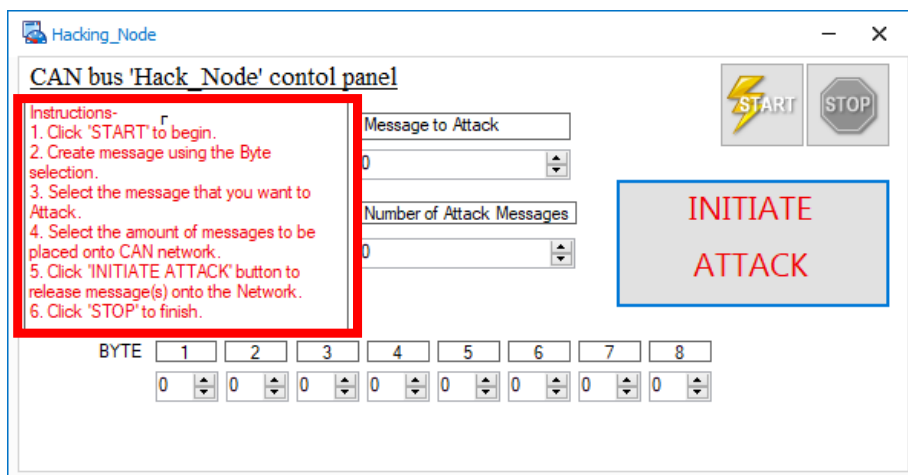


Figure 11- Control Panel for 'Simple message injection' attack.

Use of the control panel is displayed at the top left and is as follows:

1. Click '**START**' button to begin ECU running.
2. Create your desired message using the Byte numerical boxes at bottom of the panel.
(Range of **0-255** which will then be sent out in Hexadecimal format).
3. Select the message you want to attack by inputting a 1 or 2 into the text box.

Message Selection	Message ID	Message Name	CAPL Denotation
1	67	Ignition Info	Msg1
2	C9	ABS data	Msg2

4. Input the number of messages within the attack.
5. Click the '**INITIATE ATTACK**' button to inject the messages onto the CAN bus.
6. Click the '**STOP**' button to end.

Using this you can start the ECU simulation, create the attack message, select the number of messages inject onto the network and then send the attack out to the ECU.

The results of the attack can be observed in the graphical display:

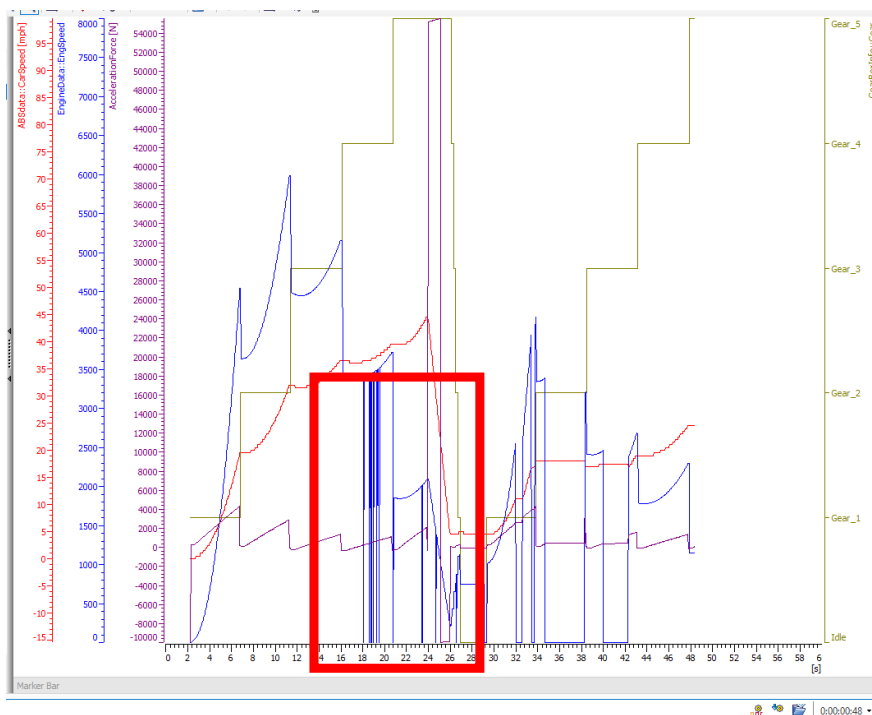


Figure 12- Graphical results of attack 1.

Here in this example the message chosen was the brakes and the result of the attack is a change in the message that feedback the vehicles speed. From the highlighted section above you can see that the vehicle speed outputs a value of 0 at the points of the attack.

Attack 2 (On Message)

The 'on message' attack will search for the windows up message for the left side window and output a message of same node ID, but the contents will be what was input into the Attack Message input box. This Attack will keep triggering as long as the toggle button is activated.

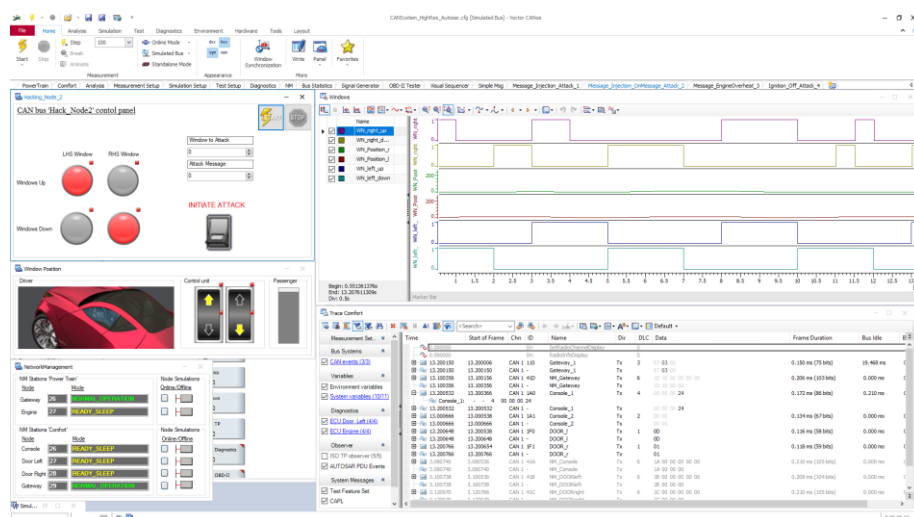


Figure 13- Display for 'on message' attack.

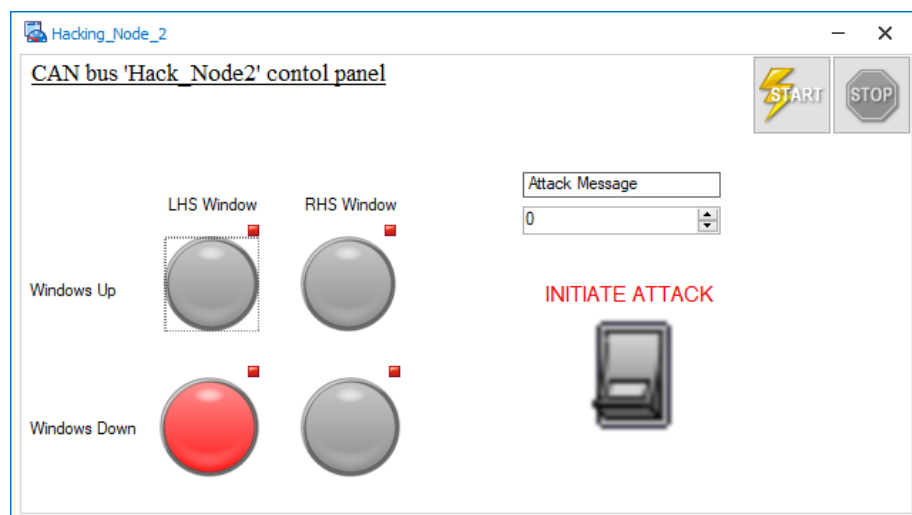


Figure 14- Control Panel for 'on message' attack.

The use of this panel is as follows:

1. Click '**START**' button to begin ECU running.
2. Input the Attack message to send onto the CAN bus.

Message Input	Message action
0	Left side window down.
1	Left side window up.
Other	No Action

3. Toggle the 'INITIATE ATTACK' button to initiate the attack.
4. To finish attack, deactivate the 'INITIATE ATTACK' toggle button.
5. Click 'STOP' button to end.

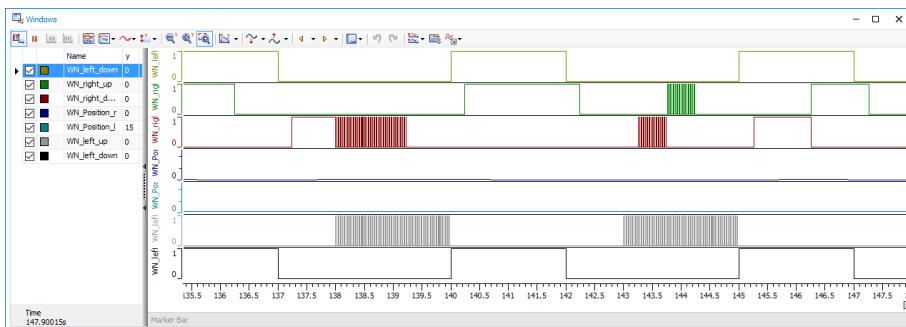


Figure 15- Graphical result of 'on message' attack.

The graph figure 6 shows the effect of the on-message attack. The attack causes a conflict in messages for the Left window of the vehicle.



Figure 16- Vehicle operation display.

It is also evident in the vehicle operation display that the window does not function as intended. The left side window remains down even while the ECU is requesting it to be raised.

Attack 3 (Incremental Change)

This attack should inject a message with CAN ID of the engine oil temperature. This injection will be incremental meaning that the value that changes the feedback oil temperature will increase overtime. The objective of this attack is to cause the oil temperature light to become illuminated.

Commented [JH3]: Rate of increase??

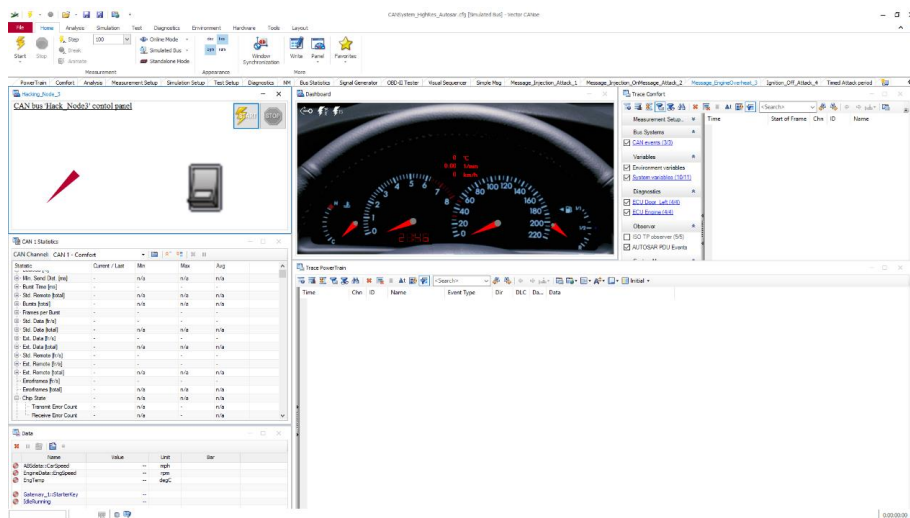


Figure 17- Display for 'Incremental change' attack.

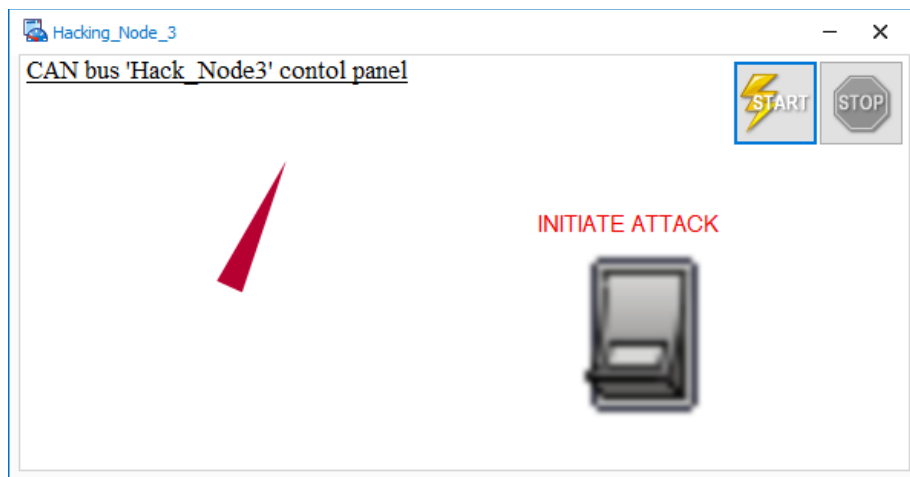


Figure 18- Control panel for 'Incremental change' attack.

Commented [JH4]: Rate of increase

The use of the panel is as follows:

1. Click '**START**' button to begin ECU running.
2. Toggle the '**ATTACK**' button to initiate the attack.
3. To finish attack, deactivate the '**INITIATE ATTACK**' toggle button.
4. Click '**STOP**' button to end.

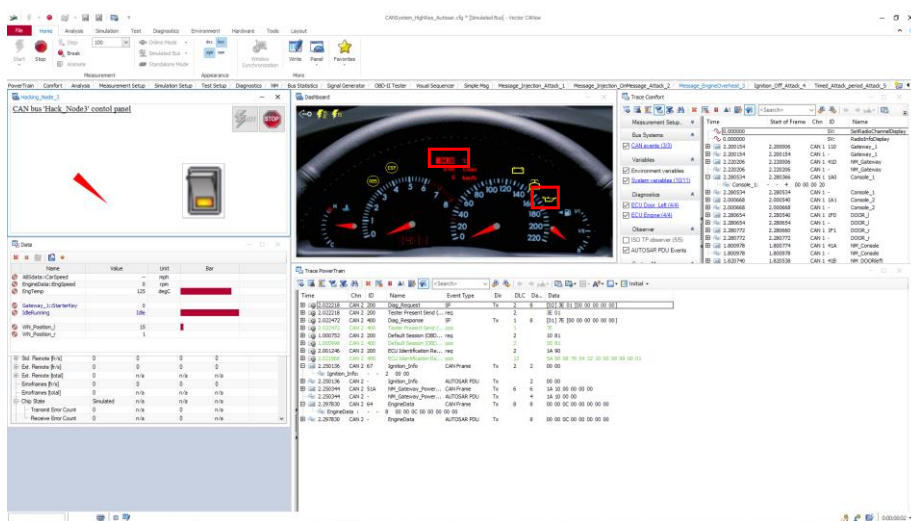


Figure 19- Result of Incremental attack

The result of this attack can be seen in figure 18. The oil temperature feedback nominally stays at 75 degrees. With the attack the temperature will rise to 125 degrees before resetting and rising again. In addition to this the vehicle Oil temperature light become illuminated on the vehicle dashboard display.

Attack 4 (ignition off)

This attack is designed to send a CAN message and receive a response from the vehicle ECU while the vehicle ignition is off. Attack 4 was created to replicate a real-life attack where a hacker will try to operate the vehicle while the ignition is switched off. For this attack 4 messages can be used but the construction of the message can't be altered and is just a single byte, with a value of 0x01.

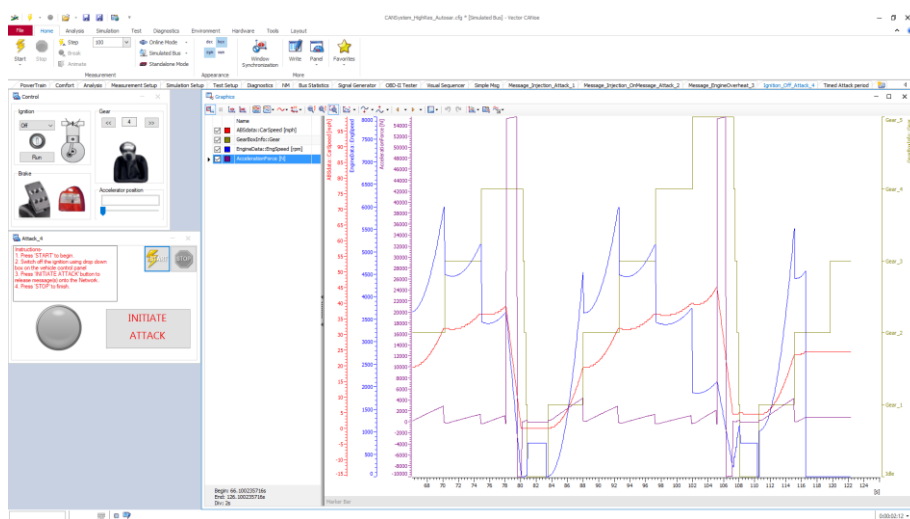


Figure 20- Display for 'ignition off' attack.

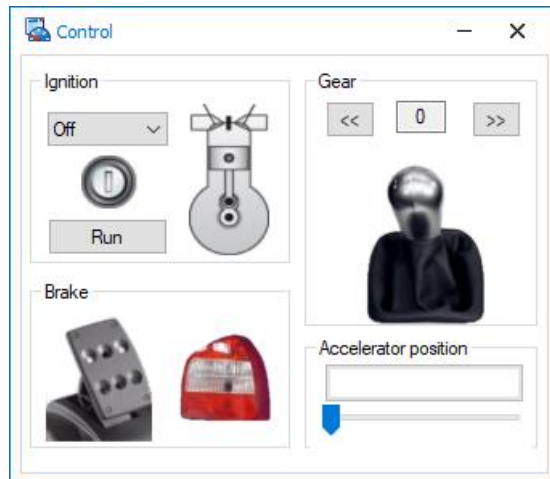


Figure 21- Display panel for vehicle controls.

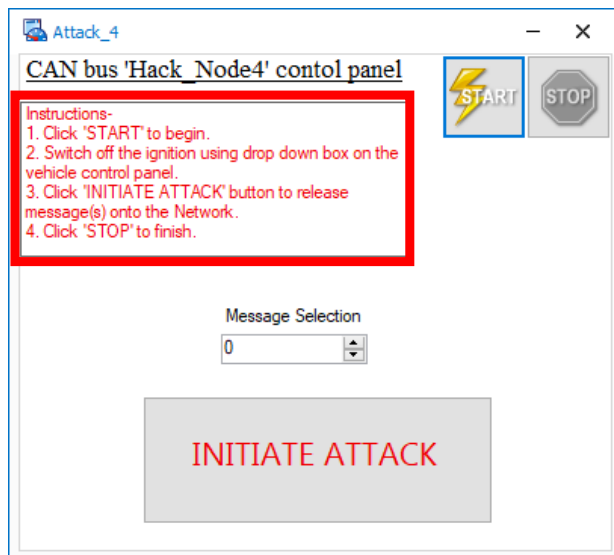


Figure 22- Control Panel for 'ignition off' attack.

The use of the panel is displayed in the textbox in the top left corner and is as follows:

1. Click '**START**' button to begin ECU running.
2. Click the '**INITIATE ATTACK**' button.
3. Click '**STOP**' button to end.

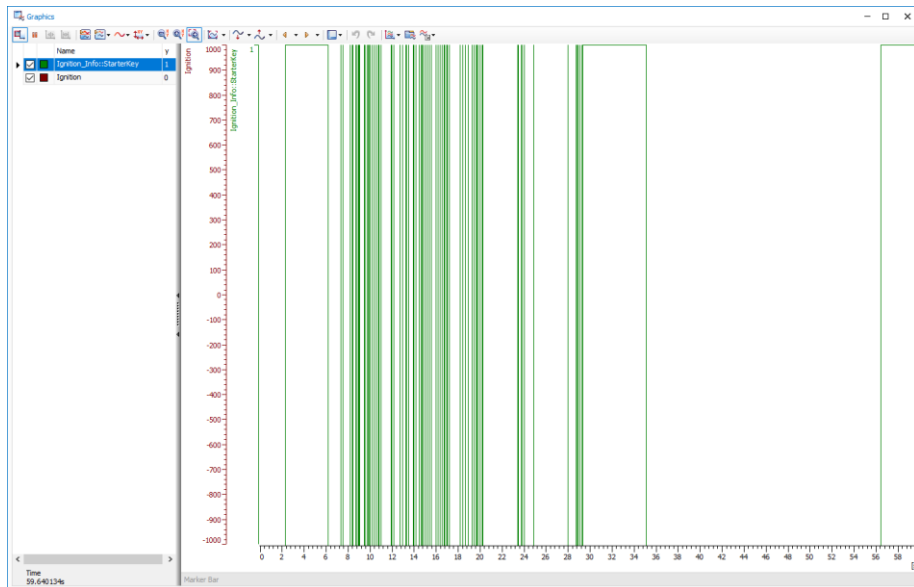


Figure 23- Graphical result of ignition off attack

The result of this attack is a change in the signal sent from the ignition message.

Attack 5 (Timed)

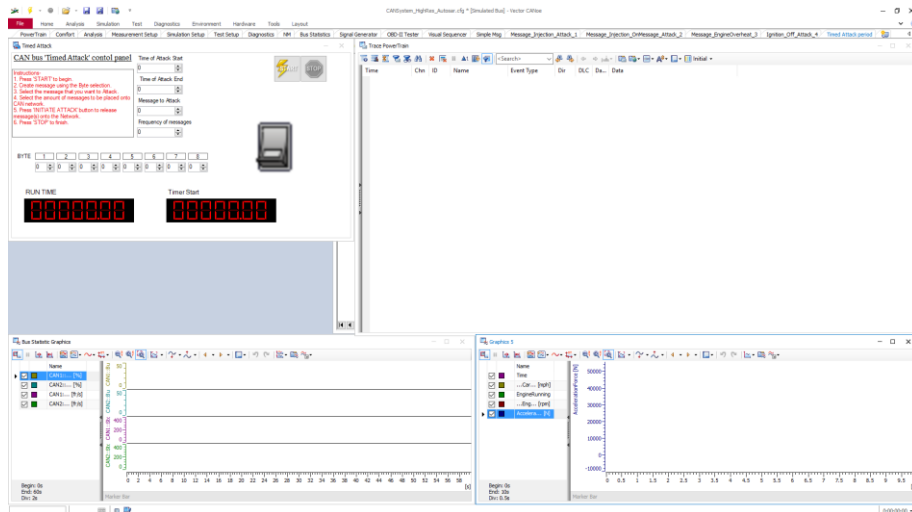


Figure 24- Display for 'Timed' Attack.

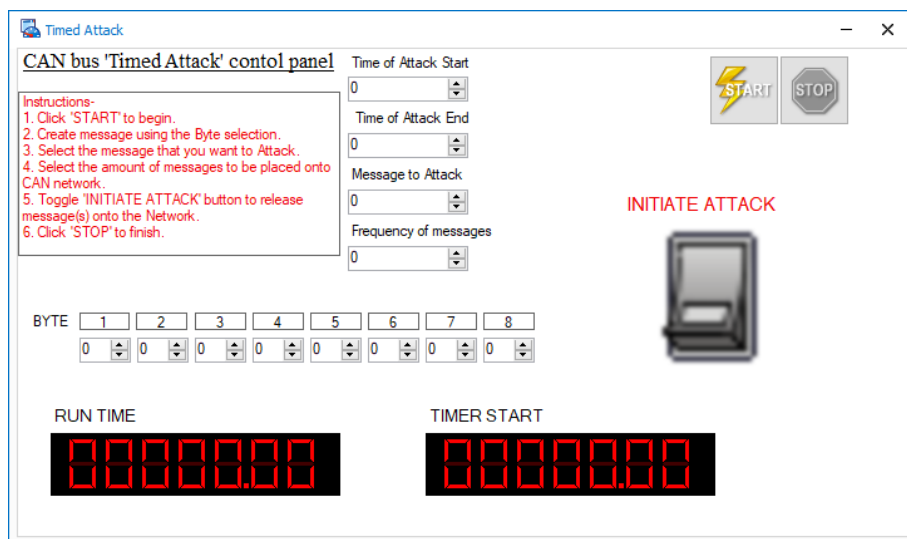


Figure 25- Control panel for 'Timed' attack.

Use of the control panel is displayed at the top left and is as follows:

1. Click '**START**' button to begin ECU running.
2. Pause the ECU using the 'Break' button.
3. Input '**Time if attack start**'.
4. Input '**Time of attack end**' .
5. Create your desired message using the Byte numerical boxes at bottom of the panel.
(Range of **0-255** which will then be sent out in Hexadecimal format).
6. Select the message you want to attack. (**1 > Ignition Info, 2 > ABS data**).
7. Input the number of messages within the attack.
8. Toggle the '**INITIATE ATTACK**' button.
9. Click the '**STOP**' button to end.