Testing NMEA2000, SAE J1939, ISO11783, RV-C Networks Vulnerability to Address Claim Hunter Cyberattack

Dr. Chris Quigley, Warwick Control Technologies Limited

25th April 2023

Abstract

Protocols based on SAE J1939 using the Self-Configurable Address mechanism for claiming a Source Address enjoy the ability to be networks to automatically set themselves up with no user intervention by a defined plug and play method. There are 252 or more unique Source Addresses available, and each device will attempt to claim a unique one of these dynamically. If a device is not able to claim a unique Source Address, it signifies this by a Cannot Claim Address message and then does not participate in any further network communication activity.

Whilst this feature provides a lot of flexibility, it also means that devices that support the Self-Configurable Address feature are susceptible to an attack by an Address Claim Hunter algorithm, resulting in a Denial Of Service (DoS). Such attacks can leave many devices disabled or at worst case disable the entire network. Depending on how safety critical the devices on the network are, the outcome could at a minimum be an annoyance or endanger life.

This paper describes the problem in detail to highlight that care must be taken when using the dynamic address claim mechanism. Suggestions are made on how to design such systems with proposals for the introduction of protection mechanisms which can reduce or eliminate the vulnerability from an attack by an Address Claim Hunter algorithm. An example Kvaser T-Script is shown which can be used to test for this vulnerability.

1 Introduction

Cybersecurity in control systems is now receiving a lot of attention. A lot of the network technologies that are successfully used in many control systems have unfortunately been found to be susceptible to attacks from malicious parties.

This paper will explore a particular weakness in protocols based on SAE J1939 to raise awareness of this issue and proposes a number of mitigation strategies. These protocols include:

- SAE J1939 – Truck, bus, heavy vehicles
- NMEA2000 – Marine
- ISO11783 (ISO-Bus) – Agriculture
- RV-C – Recreational Vehicle

There are a number of other protocols that have been implemented that use SAE J1939 mechanisms as a basis and may also have the vulnerability which is subject of this paper.

This particular weakness involves the following steps:

- gain access to the CAN bus so that a malicious algorithm can be deployed
- disable a device such as a water speed sensor using an Address Claim Hunter algorithm
- Claim the device's old source address on the network and spoof the network by sending incorrect vessel water speed signals over the CAN-based network

The first studies known to report a vulnerability in the SAE J1939 address claim functionality were in 2018 [1, 2]. These were particularly concerned with any protocol from the SAE J1939 "family" of protocols that uses the dynamic address claim such as NMEA2000. One of the vulnerabilities that was highlighted by the aforementioned study was that a device on the network could be upset by having to continually deal with address claim messages from a malicious device. This is true and would be the case if the malicious device were to transmit valid address claim messages, perhaps mimicking the NAME of valid devices. However, testing carried out by the author on a variety of devices shows that this situation is in fact more serious than first thought. It has been found that most were vulnerable to address claim messages that contained an invalid NAME field. This is referred to as an Address Claim Hunter algorithm because it hunts address claim messages and attempts to kill devices by forcing them into the state where they cannot claim a valid address.

To be able to attack one of these CAN-based networks, the attacker just needs to be able to access the network. Examples of these include:

- physically add small device whose aim is to disrupt network, e.g. see Figure *1*
- Putting a USB key into a PC on the vessel. If the PC itself
- reflash or reconfigure an ECU
- via IoT or internet connected type device

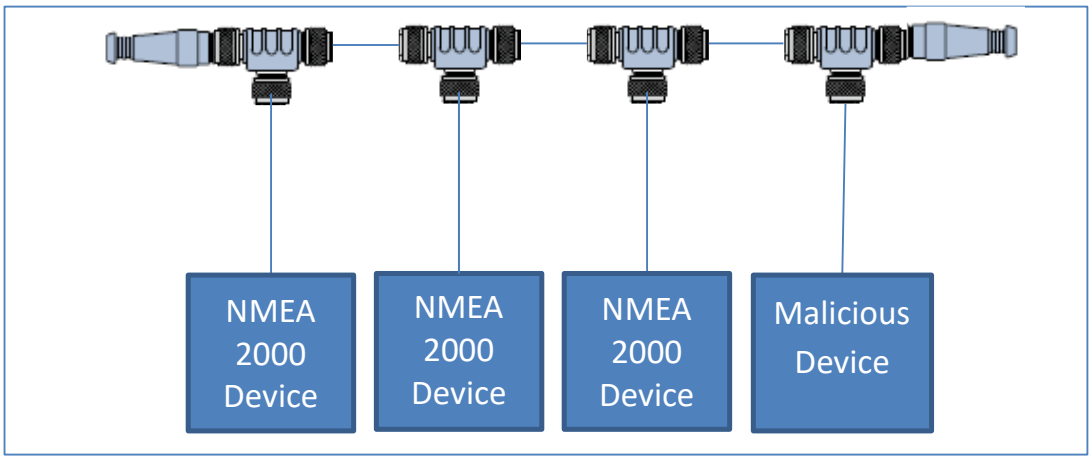

Figure 1 Typical installation for NMEA2000

Figure *1* shows the typical configuration of a NMEA2000 network in which off-the-shelf cables and connectors are simply screwed together via m12 connectors of the appropriate genders. It is easy just to add a T-connector and add the malicious device. NMEA2000's easy wiring is an advantage for installation but also an advantage for hiding a malicious device behind a panel.

Other networks such as SAE J1939 on truck could also easily have a malicious device added in secret.

There is no standard mechanism for detecting this and therefore the likelihood of this succeeding is quite high. An example of this could be that a malicious device could be installed on a vessel and wait for a trigger to occur before executing the attack. This could be vessel location, speed etc. When the trigger conditions are met then the attack is initiated. This mechanism is explored in the following sections.

2 SAE J1939 Family Protocols and Address Claim

The SAE J1939 family of protocols (SAE J1939, NMEA2000, ISO11783, RV-C) support dynamic address claiming so that each ECU claims a unique Source Address. This feature is incredibly flexible so that devices can be easily added to a network. However, this functionality is also vulnerable to a Cyber Attack that can stop some or all nodes from working.

There are a few different address claim mechanisms defined in SAEJ1939 part 81 for Network Management. The final of these is concerned with dynamic addressing and referred to as “Self-Configurable Address” ECUs which enables a plug and play functionality. If two ECUs have the same “Source Address”, the clash is dealt with and the process re-assigns each “Source Address” automatically.

Whilst address claiming is taking place, a device or ECU cannot send its normal PGNs onto the CAN bus, therefore the system is disrupted at this time.

Arbitration when two nodes claim the same Source Address is dealt with using the NAME field (Address Claim Field in RV-C) which is the 8-byte data field (64-bits) of the Address Claimed message. The lower numerical value of this 64-bit value wins the Address Claim and in theory a data field of all zeroes is therefore the highest priority and will always win the claim for a Source Address.

The Data Field with all zeros (e.g. 00 00 00 00 00 00 00 00) is however an invalid setting. The following explains why. The NAME or Address Claim field across the four protocols is compared below:

<u>SAE J1939 – NAME Convention</u>

Arbitrary Address Capable	Industry Group	Vehicle System Instance	Vehicle System	Reserved	Function	Function Instance	ECU Instance	Manufacturer Code	Identity Number
1 bit	3 bit	4 bit	7 bit	1 bit	8 bit	5 bit	3 bit	11 bit	21 bit

ISO11783 – NAME Convention

Self Con-figurable Address	Industry Group	Device Class Instance	Device Class	Reserved	Function	Function Instance	ECU Instance	Manufacturer Code	Unique Number
1 bit	3 bit	4 bit	7 bit	1 bit	8 bit	5 bit	3 bit	11 bit	21 bit

NMEA2000 – NAME Convention

Reserved (set to 1)	Industry Group	System Instance	Device Class	Reserved	Device Function	Device Instance (Upper)	Device Instance (Lower)	Manufacturer Code	Unique Number
1 bit	3 bit	4 bit	7 bit	1 bit	8 bit	5 bit	3 bit	11 bit	21 bit

RV-C – Address Claim Field

Arbitrary Address Capable	Compatibility Field			Reserved	Compat-ibility Field	Function Instance	Node Instance	Manufacturer Code	Serial Number
1 bit	3-bit	4 bit	7 bit	1 bit	8 bit	5 bit	3 bit	11 bit	21 bit

The first part to examine why all zeroes in the Address Claim data field is invalid is to look at the left-most bit which is called *Arbitrary Address Capable* in SAEJ1939 and RV-C. This should be set to 1 if to correctly indicate that the ECU does support Self-Configurable Addressing. In NMEA2000 it is called *Reserved* and always set to 1. The *Reserved* Bit should always be set to 1. For NMEA2000, which is a marine protocol, the *Industry Group* will always be set to 4. In SAEJ1939, *Manufacturer Code* of 0 is not allowed and is a reserved value. This means that a NAME field set to all zeros (e.g. 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00) should not occur on these networks in practice. However, many devices in the market will lose the address claim process to a NAME with all zeroes. According to NMEA2000 Appendix D– D4.3, NMEA2000 does not support an unknown or not available state or value for any of the NAME fields. However, from testing carried out it is clear that this is not the case.

3 Address Claim Hunter Algorithm and Impact on a SAE J1939 / NMEA2000 Self-Configurable Device

The Address Claim Hunter algorithm is a simple method to force one or many devices from their source address so that they eventually run out of source addresses to claim. This results in the affected devices to not be able to claim an address, issue the Cannot Claim Address message and then no longer participate in NMEA2000 network communications.

It is possible to use this method to attack all devices (all source addresses) or a specific manufacturer code. Example simple algorithms are shown below to illustrate the simplicity of this approach.

Example Algorithm1 Running in Malicious Device

If (Address Claim Msg Received)

THEN Send Address Claim Msg with NAME 00 00 00 00 00 00 00 00

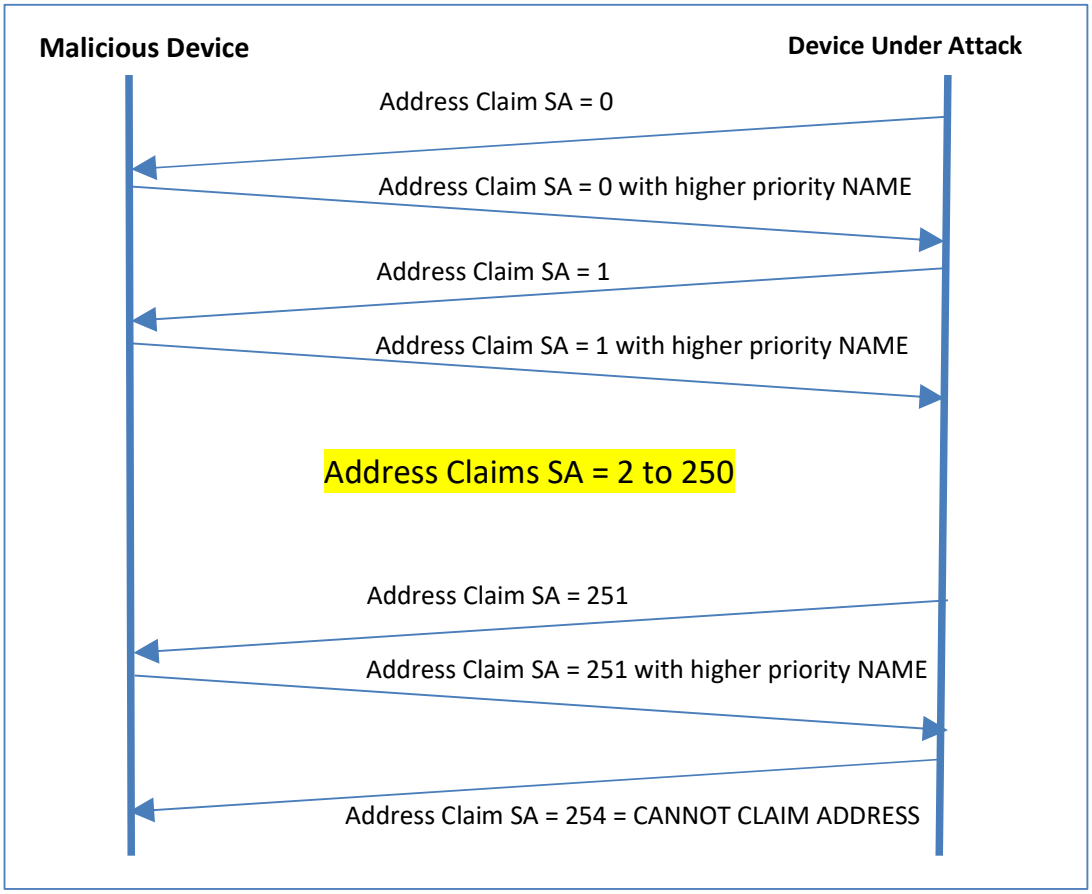

Figure 2 : Address Claim Hunter Algorithm Sequence

This would give you a sequence of events as shown in Figure 2. The process starts with an attempt by a device (Device Under Attack) to claim Source Address (SA) as 0. This device is then attacked by a Malicious Device which claims SA = 0. Then the Device Under Attack attempts to claim addresses 1 through to 251, but each time the Malicious Device claims the Source Address using a higher priority NAME field. The process ends with the Device Under Attack having tried to claim every possible Source Address, issues a CANNOT CLAIM ADDRESS message with Source Address = 254. It then takes part in no further network activity. Once this has happened it is usual that some kind of external intervention is needed to reset the device such as an ignition / power cycle.

Example Algorithm2 Running in Malicious Device

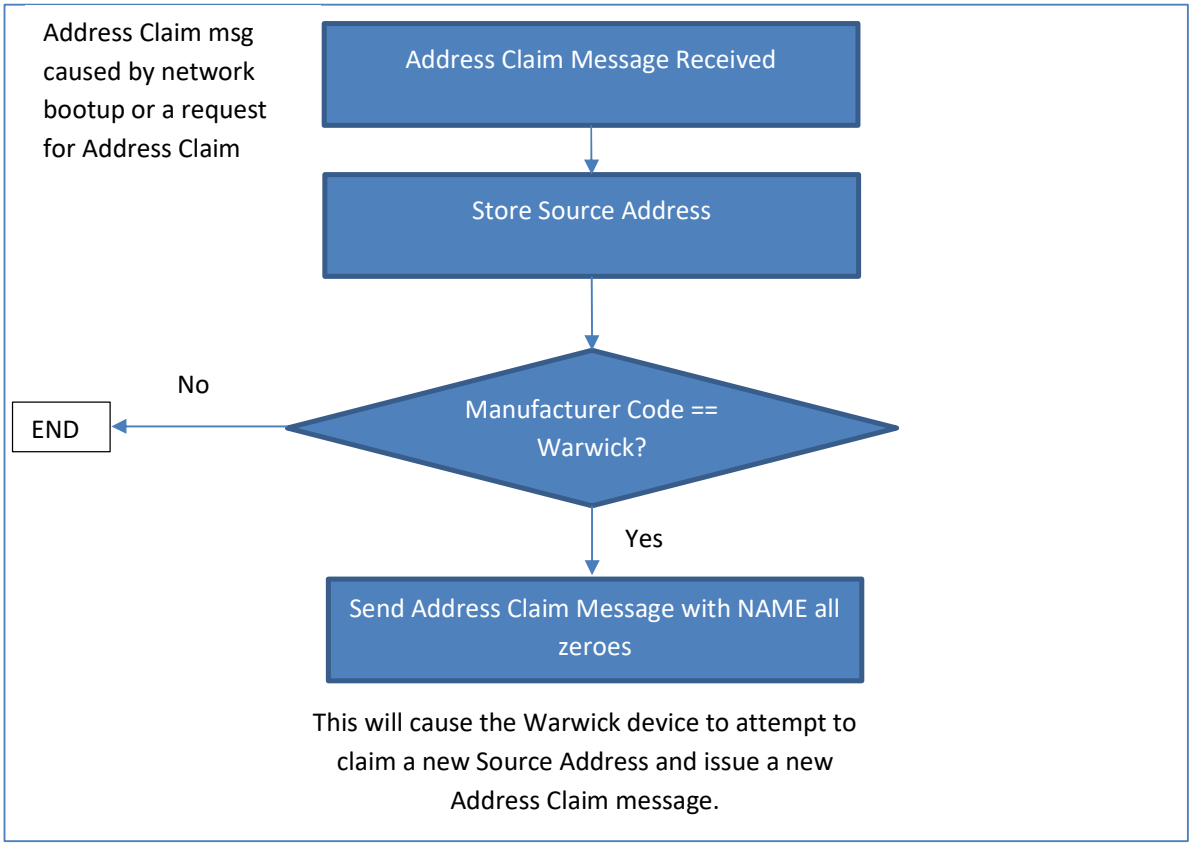

Figure 3 : An Address Claim Hunter Algorithm

A simple Address Claim Hunter algorithm for an example attack on a fictional Warwick device is shown in Figure 3. This has a simple approach to attack a particular device manufacturer, e.g.

Send ISO Request for Address Claimed to all devices

If ((Address Claim Msg Received) AND (**Manufacturer Code** is Warwick))

THEN Send Address Claim Msg with NAME 00 00 00 00 00 00 00 00

The result of this attack is that a device under attack:

- will try to claim new Source Addresses thus upsetting the network
- whilst claiming a new Source Address, all control PGNs will normally be suspended because the device does not know which Source Address it should be using and receiving devices do not know which Source Address to expect to receive the PGNs from
- Once all possible Source Addresses have been tried by the device, it will issue a Cannot Claim Address message (on the Null address 0xFE) and cease all communications. Usually the only way to make this device to go online again is some kind of operator intervention.

Potentially the severity of this is dependent upon the type of device that is attacked. For example, does your system remain safe if it uses GPS location or water speed? What if a system providing Thruster feedback information is taken down, what will the system do?

Address Claim Hunter Followed By a Spoof Attack

It is possible to use the Address Claim Hunter algorithm to spoof the network. The process for this is to take the device down using one of the previously described Address Claim Hunter algorithms. Once the device has been taken down, spoof PGNs can be sent, potentially using incorrect values with the intent of sending malicious damage. For example, actual vessel speed could be 3m/s when it is actually 0m/s.

4 Kvaser CAN Interface T-Script for Testing Address Claim Hunter Vulnerability

T-Script is a real-time scripting language for testing and simulation that is supported by all Kvaser Professional level CAN interfaces. It is a C-like language which is downloaded into the CAN interface. Here, an example Address Claim Hunter Algorithm is shown in T-Script. The example T-Script is available from Warwick Control and the main part of it is an **on CanMessage** hook that looks for received Address Claim messages on the network (see below). It uses an **on key 'A'** hook to make an ISO Request for Address Claimed which will kick the process off.

```
on CanMessage [*] {
        CanMessage msg;
        int i;
        ID =  this.id;
        Src = this.id & 0xff;
        PGN = (this.id & 0xffff00) >> 8;

        if( (0xeeff == PGN) )
        {
                if(0 == AddClmRxdflag)
                {
                        AddClmRxdflag = 1;
                        printf ("Address Claim Received\n");
                }

                msg.id      = (0x18EEFF00 | Src);
                msg.dlc     = 8;
                msg.flags    = canMSG_EXT;

                // load data field with zeroes
                for(i=0; i<8;i++)
                {
                        msg.data[i]  = 0;
                }

                canWrite(channel_1,msg);
        }
}
```

5 Possible Protection Mechanisms

The problems with dynamic address assignment methods of the SAE J1939 family of protocols has been discussed in this paper. In this section, proposals for protecting against this are outlined. This is by no means exhaustive but merely some initial suggestions for designer to consider:

NAME/Address Claim Field Plausibility Checks – Below are some recommendations of plausibility checks that can be made on the NAME field:

- Reserved (NMEA2000) / Arbitrary Address Capable (SAE J1939) / Self-Configurable Address (ISO11783) Should Equal 1 – this is the easiest of checks to carry out. In NMEA2000, two of the fields in the NAME are nominated as Reserved and should be set to 1.
- Allow/Deny List of Manufacturer Codes, Function Code and Class – More sophisticated protection can be achieved by a simple plausibility check of the fields within the NAME field such as Manufacturer Code, Function Code and Class. A vessel manufacturer will know which

combinations are valid for a specific model and from the NMEA a list of certified products and their attributes is available so that these can be cross-checked for plausibility using a combination of Allow and Deny lists. Upon receipt of an Address Claim message, it would be possible to check which combinations are valid from the published NMEA list of certified products. This approach reduces the openness, interoperability and plug & play capabilities of the NMEA2000 protocol. Devices would need a firmware update to be able to accept a newly fitted device. However, this could be an important feature for safety critical systems.

Fixed Address for Safety Critical Devices – In SAEJ1939 a number of devices have recommended fixed source addresses, e.g. the engine is always 0. Such devices do not take part in any dynamic source address assignment activity. There is usually a range of source addresses that are reserved for devices that take part in dynamic source address assignment. As the networks grow with the addition of new PGNs which can be considered to be used for safety critical systems (e.g. electric propulsion, steering controls etc.) then a limited area of recommended fixed addresses would protect such devices from attacks such as the Address Claim Hunter.

Wait then Recover – a way for a device that Cannot Claim Address to wait for an application specific time and then attempt to recycle again. The trigger could be a prompt on a MFD or tablet to allow user intervention or some automatic application software triggering to lead to an attempt to claim an address again (e.g. searching for a gap using ISO request).

Address Claim NAME Tracking - apply an additional rule to the Address Claim process, e.g. has the same device (NAME) made another address claim, when no other device has requested that address? Example, Device A has address 10, it receives an ISO Address Claim from a device with NAME 0x00000000, which Device A relinquishes and gets an address 11. It then receives another ISO Address Claim from a device with the same NAME 0x00000000 for address 11, but no other device requested address 10, so it rejects the Address Claim and transmits a new Alert PGN for "Suspicious Network Activity Detected". Therefore, a device would simply need to remember its last valid CAN Address, the NAME of the device that requested it and if any other device has requested its last valid CAN address.

6 Conclusion and Recommendations

This paper has highlighted a particular vulnerability that the family of SAEJ1939 protocols have to a cybersecurity attack that exploits part of the protocol that deals with dynamic address claiming for self-configurable ECUs and devices. The dynamic address claim feature is one of the benefits of these protocols that allows a plug and play type functionality for adding new devices to the network. However, it has been shown that this can be exploited and result in a complete network shutdown for susceptible devices. The impact of this can range from being an annoyance through to being a serious safety concern with these protocols being used increasingly for more important control applications. Not all SAE J1939 protocol family implementations will be susceptible. The susceptibility will depend upon how the dynamic address claim functionality is implemented. The

good news is that the implementation of some additional checks and balances can reduce the risk. Designers of systems based on these network technologies should consider implementing various address claim plausibility checks to ensure that this weakness within this family of protocols cannot be exploited.

References

1. Murvay P.S. and Groza B. (2018); "Security Shortcomings and Countermeasures for the SAE J1939 Commercial Vehicle Bus Protocol," in *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4325-4339, May 2018.
2. Daily J. (2018); "Introduction to SAE J1939" Cybertruck Presentation, page 124 – https://www.cybertruckchallenge.org/wp-content/uploads/2022/06/Introduction-to-SAE-J1939-CyberTruck-2022.pdf.
3. SAE J1939-81 "Network Management"
4. ISO11773-5 "Network Management"
5. NMEA2000 Specification Package v3.0
6. RV-C – Recreation Vehicle Communications - clause 3.3.