CAN XL made secure

Donjete Elshani, Vivin Richards, Harald Zweck, Laurent Heidt, Infineon Technologies

Security threats on In-vehicle-Network may compromise the safety of the vehicle, showing the importance of security in safety critical application like in the automotive industry. The current CAN communication protocols like Classical CAN and CAN FD use Secure Onboard communication (SecOC) to provide authenticity and replay protection for the CAN frames. Due to security overhead in the payload, it is most likely that the authentication code is truncated, leading to security compromises. Now being in the verge of defining a new protocol CAN XL, which expands the payload size up to 2 Kbytes of the data, gives the opportunity to use complete authentication code as part of the payload. Further, SecOC does not provide encryption of the payload (Confidentiality), unified freshness management, key management methods and easy adoption to future security ciphers. In this paper, we propose a CADsec protocol, which is efficient to implement, performant and flexible for future security needs to achieve secured CAN XL communication.

Introduction

CAN communication is used as the major In-Vehicle-Network for more than 20 years. Although the communication protocol is considered as "safe" by its construction, it does not provide security. Various attack vectors on CAN communication networks were described [1]. In response several security methods were proposed and used for CAN communication in recent years. Known CAN security methods are Secure-Onboard Communication or SecOC by AUTOSAR [2], Secure CAN Transceiver [3] and CANcrypt [4]. All the above-mentioned methods focus on securing Classical CAN / CAN FD communications with minimal or no protocol overhead. With the minimalistic approach, there is always a limitation on the security level achievable by the proposed methods. For example, SecOC focuses only on authenticating the CAN payload but it does not provide "confidentiality" (Encryption-Decryption) because encryption and decryption cannot be provided while meeting the minimum payload data size constraint (when block ciphers are used) for the minimalistic approaches. Additionally, SecOC provides security on a higher layer than OSI layer 3, which makes layer 2 traffic, i.e. time synchronization protocols vulnerable to attacks.

CANcrypt aims to minimize the computing power by choosing a lightweight cipher (for example, an XOR based bit scrambler), while providing a methodology to share "Dynamic Keys" which change during a given time interval.

Secure CAN transceiver applies logical security methods like CAN ID based blacklisting; but it is still vulnerable against physical attacks like replacing the secure CAN transceiver with a normal CAN transceiver. However, CAN XL, a new extension to CAN communication, has increased data bandwidth with higher baud-rate and higher payload size (up to 2 KB). It provides the opportunity to enhance the security method to achieve a state-of-the-art security protection while still minimizing the protocol overhead. In this paper, we propose a new security method for CAN XL communication, called "CAN XL Data link layer Security or CADsec", to achieve state-of-the-art security protection with efficient data handling.

CADsec protocol

CADsec is a security protocol designed for the needs of the automotive bus networks and is tailored to the new protocol CAN XL. It works on the data link layer, layer 2 of the OSI reference model. CADsec can provide the complete security set of authentication, integrity and confidentiality. Due to the properties of a layer 2 protocol, a complete frame of CAN XL is protected by CADsec.

CADsec offers authentication of control field and payload, and the further option to encrypt the payload.

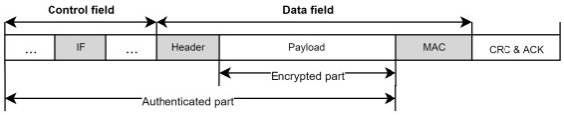


Figure 1: CAN XL frame secured with CADsec protocol format

The structure of CADsec frame is shown in Figure 1, it contains three parts:

i. The indication field (IF) - used to identify that this frame is protected by CADsec protocol. It is part of CAN control field and is separated from CAN ID (not shown);
ii. Header – provides control information and parameters for security operation, and
iii. Message authentication code (MAC).

The CADsec frame overhead is small. It is~4%, in case of CAN XL frames having a data field length greater than 512 Bytes, and reduces to ~1% for data field length of 2kB, as shown in Table 1.

Table 1: CADsec Overhead

CAN XL Data Field length	64 B	512 B	2048 B
Overhead	31 %	3,9 %	0,98 %

The MAC is part of the data field of the CAN XL frame and it is 128-bits wide.
CADsec header is 4 Bytes wide and it provides control information indicating:

i. Which security operation is performed,
ii. Which security key is derived
iii. Freshness value generation and verification,
iv. How a NONCE is derived for use in the security algorithms, and
v. How the variation of secure operation is handled.

CADsec header is shown in Figure 2.

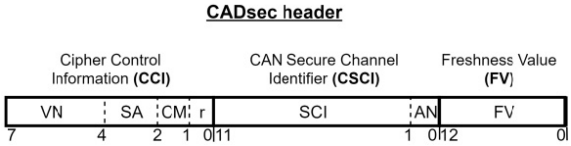


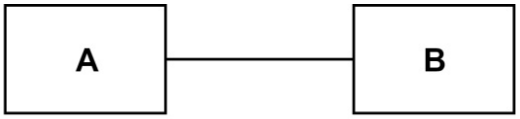
Figure 2: CADsec header

The Cipher Control Information (CCI) contains of the following fields:

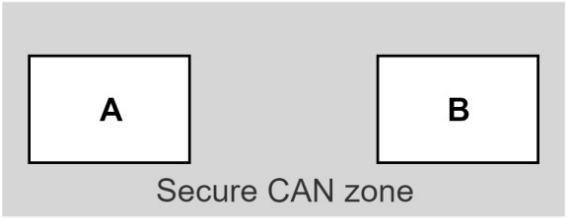
i. Version Number (VN) specifying the version of the CADsec protocol
ii. Security Association configuration (SA), which shows which part of the frame is used to select a secure association. The options are CAN ID, CSCI and a combination of these two.
iii. Cipher Mode (CM), the information of the security operation. This value represents either authentication of data or authenticated encryption with associated data (AEAD).

Secured zone partition

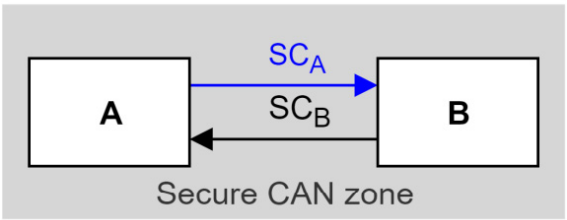
In Figure 3 a), a physical connection, the CAN bus between two nodes of a point to point communication, between CAN Node A and CAN Node B, is shown.
If a secure communication is required between Node A and Node B, then a key agreement protocol can establish a secure communication zone between the two nodes. This is shown in Figure 3 b).



a) Point to point communication of CAN Node A and Node B



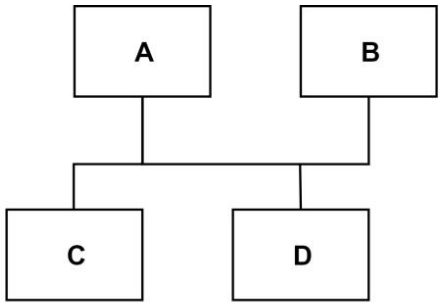
b) Secure zone partition for Node A and Node B



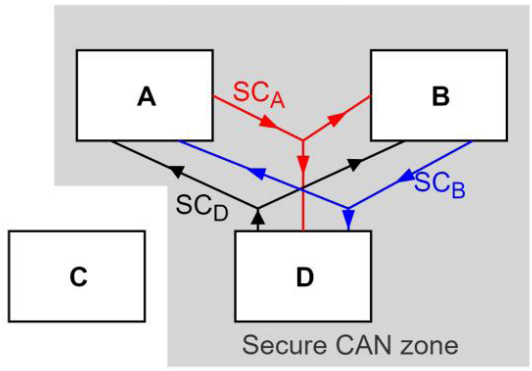
c) Secure communication channels in a secure zone partition

Figure 3: Point to point secure communication

Communication between two nodes in a secure zone uses secure channels (SCs). A SC provides unidirectional point-to-point or point-to-multipoint communication. Thus, for secure communication between Node A and B, two SCs are required, shown in Figure 3 c). Each SC contains at least one Secure Association for secure communication. Similarly, this can be extended to more than two nodes and to point-to-multipoint communication.
In Figure 4 a) shows a CAN bus with four connected nodes. For secure communication between all or few nodes connected in this bus, a secure zone partition has to be defined and its SCs have to be established, Figure 4 b).



a) Point to multipoint communication in CAN bus between Nodes A, B, C, D



b) Secure communication channels in a secure zone partition

Figure 4: Point to multipoint secure communication

In CADsec, each SC is identified by a unique Secure Channel Identifier (SCI), which is 11-bits wide and is part of the header. Within each SC, up to two SAs can be created. At least two SAs are required for each secure channel in order to support key updates. Thus, there is 1-bit called Association Number (AN) in CADsec header, used to distinguish between first and second security association SA in a secure channel SC. These two fields, SCI and AN, form the CSCI, which CADsec uses to select the cipher suite algorithm performing security operations. The CSCI is a unique number in a CAN bus. If a layer 2 gateway is in place between two or more CAN busses, the CSCI shall be a unique number across all the connected busses in this network.
The CSCI identifies the SA and the SC, on which the secure communication happens. SCs are either receive or transmit channels, and their parameters depend on the type of channel. This also holds true for SAs, which are either transmit or receive SAs. The receive SC properties are: SC ID (SCI) and its status (in use or stopped). The receive SA properties are: AN, a reference to a security association key, next Freshness Value (FV), lowest acceptable FV, and optionally a highest acceptable FV. The transmit SC's properties are SC ID (SCI) and the status (in use or stopped). The transmit SA properties are: AN, next FV, a reference to a security association key and confidentiality switch (true if it provides confidentiality as well as integrity for the frames transmitted in this SA).

Freshness value

CADsec uses a monotonic incremented counter of 64-bits as FV, which serves to: provide a unique Initialization Vector or a so called NONCE value for the security algorithm for each frame transmitted in the SC; and prevent replay attacks.
Only the lower 12-bits of the FV are part of the CADsec header and are transmitted with the frame, in order to reduce CADsec header size.

Table 2: Duration required to exchange keys to prevent reply attack; Scenario A: one secure channel used during any transmission; Scenario B: one secure channel used 30% of the time

Payload length	Scenario	Freshness Value	
		32 bit	64 bits
20 B	A	5 days	86 days
	B	18 days	1 year
2048 B	A	64 million years	1 billion years
	B	>>	>>

The FV is initialized by the key agreement protocol and its synchronization during the communication is handled by CADsec. The FV represents a counter, which is increased for each new frame transmitted in a SA of the SC. Each secure frame is assigned to an SA belonging to an SC of a secure zone partition. Thus, there is a maximum amount of frames that can be transmitted in a SA before having to perform key updates, a requirement to perform key updates depending on the length of the FV. The calculation of maximum duration of usage for a SA is shown in Table 2. The calculations are done for a CAN XL frame [5] with two different frame lengths variations, two different dimensions of FV (32-bit FV and 64-bit FV length) and two transmit scenarios. The calculations are done assuming that there is transmission on the CAN bus during the whole span of time, without any error or error handling. The arbitration rate is assumed to be 500kBps and the data rate to be 10Mbps. In Scenario A, one SA of a SC channel is used for transmission of any frame and for Scenario B, one SA of a SC channel is used 30% of the time for transmission of frames. This shows that a 32-bit FV requires frequent key updates for short frames, even if the bus is not used all of the time. This is a motivation to use 64-bit FV in CADsec.
The initialization value of FV and, in case of synchronization lost, its resynchronization are not discussed in this paper.

Freshness handling on transmit SCs

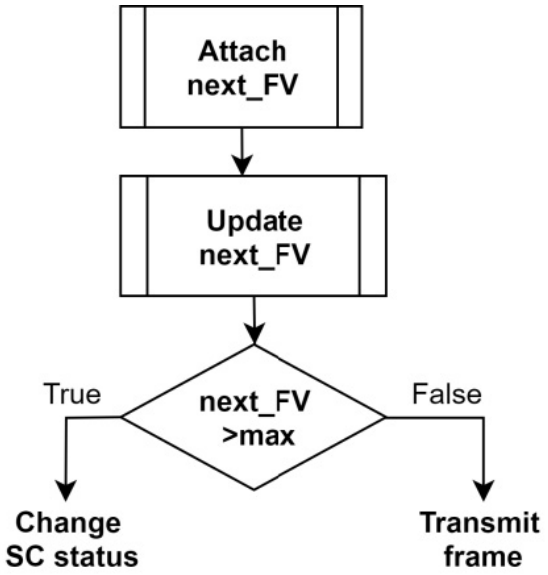


Figure 5: FV for secure frame generation

For the transmit flow, the lowest 12-bits of the next FV (next_FV11-0) are attached to the frame header and the next_FV is incremented by 1. In case that next_FV equals zero or 264, the status of the corresponding SC is switched to “stopped” and a key update is required for further communication on that SC. Otherwise the operation continues and waits for the next frame. This is shown in Figure 5.

Freshness handling on receive SCs

The algorithm for handling the FV for receive frames is shown in Figure 6.

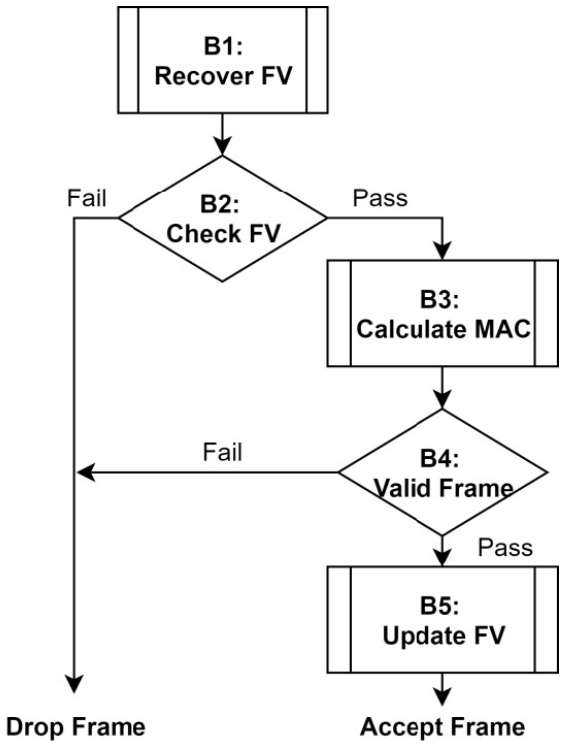


Figure 6: Management control and FV for secure frame verification

Since only part of the FV is transmitted with the CADsec header, a recovery algorithm is required to reconstruct the 64-bit received FV (*r_FV*) from the 12-bit truncated received FV (*header_FV*) in CADsec header.
B1: The recovery algorithm is shown as block B1 in Figure 6. The least significant 12 bits of the *r_FV* are equal to *header_FV*. The 52 most significant bits of the *r_FV* are recovered for each received frame by applying the Top Bit Algorithm [6]. If the 11th bit of the lowest acceptable freshness value ($lowest\_FV_{11}$) is set, and the most significant bit of the truncated received freshness value $header\_FV_{11}$ is not set, the $r\_FV_{63\text{-}12}$ is equal to

lowest_FV$_{63\text{-}12}$ + 1. Otherwise, the *r_FV*$_{63\text{-}12}$ is equal to *lowest_F*$_{V63\text{-}12}$. The combinations and how they are handled are shown in Table 3.

Table 3: Top bit algorithm for freshness value recovery [6]

lowest_FV$_{11}$	0	0	1	1
header_FV$_{11}$	0	1	0	1
r_FV$_{63\text{-}12}$ - *lowest_FV*$_{63\text{-}12}$	0	0	1	0

B2: The FV is validated, frames with a replay window are accepted, where a lowest acceptance value is set, and each frame with an *r_FV* greater than this value is accepted. The *r_FV* is compared to *lowest_FV*. If, *r_FV* is lower or equal *lowest_FV*, the frame is dropped, otherwise the frame is checked.
B3: MAC is calculated.
B4: Frame is checked its integrity verification, if it fails, the frame will be dropped otherwise the frames is processed further.
B5: The update of the FV is done. In this block, if *r_FV* is greater or equal to *next_FV*, *next_FV* is set to *r_FV* + 1 and the *lowest_FV* is set to *next_FV* – replay window and the frame is accepted and forwarded to the higher layer. The maximum replay window size is 2^{10}-1.

CADsec operation in a frame

Figure 7 demonstrates the CADsec operation in a frame for authentication only. The CADsec header is generated. The shown bits of the control field (ID, PT, DLC), CADsec header and the payload are concatenated and authenticated, and the calculated value is added as MAC field in the CADsec frame as part of data field. The value of the initialization vector in derived from the FV, and 12 lowest significant bits of FV are attached to the CADsec header.

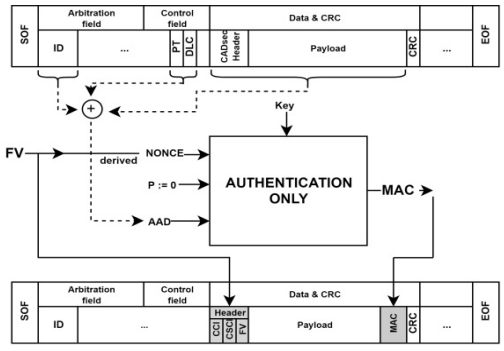


Figure 7: CADsec operation with Only Authentication

In Figure 8, CADsec operation with authentication and encryption of the payload is shown. In difference to the previous one, the payload is authenticated and encrypted and the encrypted payloads attached to the CAN XL data field.

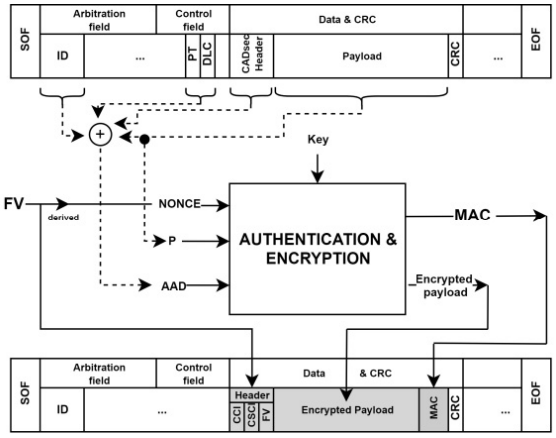


Figure 8: CADsec operation with Authentication and Encryption

Security algorithm and cipher suite

The security provided by each security association key rests on the security provided by the cipher suite, which in turn depends on the guarantees provided by the cryptographic mode of operation and its underlying block cipher, and on the protocols and procedures used to ensure that keys remain secret. One example is using state of the art security algorithm, AES-GCM with 128-bit or 256-bit key. AES-GCM is a symmetric encryption algorithm which supports AEAD or only authorization. Information on the security algorithm are in its specification from NIST [7].
The cipher suite used in CADsec protocol is a default one for each of the SC's and shall be defined with the key agreement process. The key agreement process is not covered in this paper.

CADsec vs SecOC in AUTOSAR

In Figure 9, the data path of a secure frame processed in AUTOSAR is shown. If the authentication result of a frame is valid, the total number of hops before delivering the PDU is 7. In this data path, the integrity of the CAN frame header is not checked, and if part of the header i.e. CAN ID is used to perform routing in PduR (PDU router),

it is possible to change the frame routing information. In case of the authentication result being invalid, the total number of hops before dropping the PDU is 7. SecOC is also used for many other security use cases thus reducing the availability for more CAN XL frames.

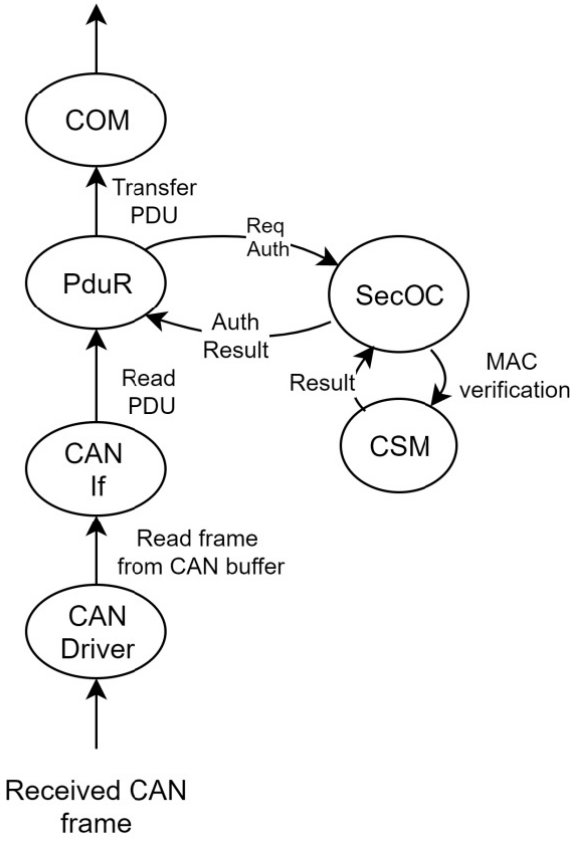


Figure 9: AUTOSAR SecOC secure frame processing

On the other hand, for the CADsec frame processed in the AUTOSAR environment, shown in Figure 10, in the case that authentication result is invalid, the total number of hops before dropping the PDU is 6, reducing processing unit load.
In case of valid authentication code, the total number of hops is 6 and at this point, the CAN frames integrity is checked by checking its headers as well as its data fields. Additionally the Crypto Service Manager (CSM), a crypto driver or a dedicated HW could decrypt and authenticate the frame.

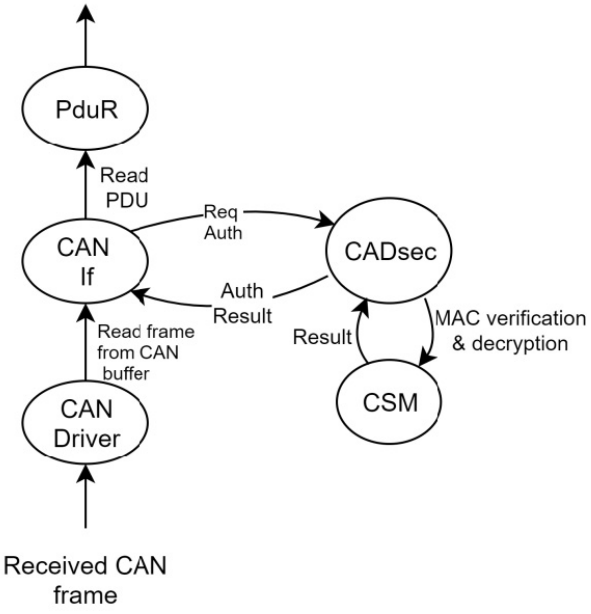


Figure 10: Proposal AUTOSAR CADsec secure frame processing

Summary

In this paper, we proposed a new security method for CAN XL communication, called “CAN XL Data link layer Security or CADsec”, to achieve state-of-the-art security protection with efficient data handling. CADsec provides the full security set: authentication, integrity and confidentiality. CADsec provides security protection while still minimizing the protocol overhead. It defines SCs and SAs which form security zones and partitions on a CAN bus, where secure communication is done between nodes.
It uses the OSI layer 2 protocol and protects the complete CAN XL frame, from layer 2 and upward. CADsec prevents replay attacks by using a freshness value of 64-bits. It introduces a unified method for handling freshness value.
As the current specification of CAN XL is not yet finalized, it may be necessary to modify the CADsec protocol if required by changes in CAN XL.

Donjete Elshani
Infineon Technologies AG
Am Campeon 1-15
DE-85579 Neubiberg
www.infineon.com

Vivin Richards Allimuthu Elavarasu
Infineon Technologies AG
Am Campeon 1-15
DE-85579 Neubiberg
www.infineon.com

Allimuthu Elavarasu
Infineon Technologies AG
Am Campeon 1-15
DE-85579 Neubiberg
www.infineon.com

Harald Zweck
Infineon Technologies AG
Am Campeon 1-15
DE- 85579 Neubiberg
www.infineon.com

Laurent Heidt
Infineon Technologies AG
Am Campeon 1-15
DE-85579 Neubiberg
www.infineon.com

References

[1] CiA CAN Newsletter 4/2019 „Classical CAN/CAN FD security threats," by Olaf Pfeiffer and Christian Keydel.
[2] AUTOSAR, „Specification of Secure Onboard Communication," 2019.
[3] CiA CAN Newsletter 2/2017 „Transceiver with cyber security functions".
[4] CiA Excerpz Edition „Implementing Scalable CAN Security with CANcrypt,"
[5] CiA, „CAN XL Data link layer and physical signaling" October Draft, 2019.
[6] M. Seaman, The XPN recovery algorithm, 2012.
[7] M. Dworkin, „Recommendation for block cipher modes of operation: Methods and techniques. Technical report,," National Institute of Standards & Technology, Gaithersburg, MD, United States, Nr. Spp. 800–38D, 2001.