

DESCRIPTION

TITLE: Method for securing V2X standard communications, and associated device and protocol

The present invention relates to the field of autonomous vehicles, and, more particularly, to securing communications between the devices of an automated driving system.

Automated driving relies on communicating information in order to extend the operational design domains of the vehicles involved. The operational design domain of a vehicle, or ODD, is the context in which the operation of the vehicle's entire automated driving system is guaranteed.

The V2X standard aims to standardize communications between the devices of an automated driving system.

The V2X ("Vehicle-to-Everything") standard enables a vehicle to exchange information with other elements in its environment, whether another vehicle (V2V, "Vehicle-to-Vehicle"), infrastructure entities (V2I, "Vehicle-to-Infrastructure"), a pedestrian (V2P, "Vehicle-to-Pedestrian"), etc.

The V2X standard is based on communications according to the IEEE 802.11 standard (i.e., Wi-Fi based), in particular the IEEE 802.11p-2010 standard, but an evolution of V2X, called cellular V2X or C-V2X, envisages communications according to the 4G LTE or 5G standard (i.e., GSM based), in particular the LTE-V2X standard (3GPP standard, 2016 version).

To be able to operate a vehicle in automated driving mode, it must be possible to demonstrate that this is safe.

Document CN111726784, for example, proposes a strategy for increasing the overall safety of an automated driving system by establishing cooperation between road users and the infrastructure devices of that road, by leveraging the V2X standard.

However, this strategy does not allow guaranteeing the safety level of each contribution to the overall operation of the system, in particular the communications. The safety level actually achieved by the proposed system is therefore not defined.

Thus it is currently not possible to determine the safety level offered by an automated driving system, on the basis of standard connectivity information.

It is therefore necessary to have a person on board the vehicle to take control in case of danger. This standby attendant may be a driver who monitors the vehicle's progress without touching the steering wheel but ready to do so when danger arises.

The invention therefore aims to solve this problem by proposing communication devices that allow ensuring the safety level of V2X communications between the devices of an autonomous driving system.

To this end, the invention relates to a method for securing communications in the V2X standard between a transmitting device and a receiving device of an automated driving system, characterized in that the method comprises: a step of temporally synchronizing the vital computers of the transmitting and receiving devices, on the basis of at least one common external time source; a step of generating a message in the V2X standard ("V2X message") by means of the transmitting device, consisting of timestamping the message by requesting a current time from the vital computer of the transmitting device and incorporating the current time as the message timestamp in a field of the V2X message; a step of transmitting the V2X message, by the transmitting device; a step of receiving the V2X message, by the receiving device; and a step of verifying the temporal validity of the V2X message received by the receiving device, by comparing a current time given by the vital computer of the receiving device with the transmission time incorporated in the received V2X message.

According to some particular embodiments, this method comprises one or more of the following features, individually or in all technically possible combinations:

- the step of temporally synchronizing the vital computers of the transmitting and receiving devices uses at least a second external time source, referred to as an auxiliary external time source, which may be different for the transmitting and receiving devices, the temporal synchronization of the vital computer of the transmitting device and the vital computer of the receiving device being performed while taking into account the time references provided by the first and second external sources.

- the step of temporally synchronizing a vital computer consists of: initiating the execution of a time server by means of the vital computer; sending a request to the common external time source and receiving a response containing a first time; sending a request to the auxiliary external time source and receiving a response containing a second time; verifying the consistency between the first and second times, and, if inconsistent, repeating the preceding steps, and, if consistent, establishing an internal time reference which is considered to be a common time base for all components of the system; and maintaining the internal time reference.

- the step of generating a V2X message further comprises calculating an authentication code, by means of the transmitting device, based on the fields of the V2X message, and a step of incorporating the calculated authentication code into a field of the message, and the method comprises a step of verifying the integrity of the V2X message received by the receiving device by calculating an expected authentication code on the basis of the fields of the received V2X message and comparing the expected authentication code with the authentication code that is present in the received V2X message.

- an authentication code is calculated based on various fields of the V2X message, by using a hashing algorithm, preferably the SHA-256 algorithm with a dynamic secret hash key known to the various devices of the automated driving system.

- the authentication code is incorporated into the optional field or a proprietary extension field of the V2X standard.

The invention also relates to a communication device compatible with the V2X standard, characterized in that it comprises a vital computer and a radio communication module, the device being configured to implement the steps on the transmitting device side and/or the steps on the receiving device side of the above method.

Preferably, the vital computer is a vital platform of the "2oo2" type.

Even more preferably, the vital platform is capable of guaranteeing a high level of safety, complying with safety integrity level SIL 4 or ASIL D.

The invention also relates to a communication protocol compatible with the V2X standard, in which each V2X message includes a field incorporating a message timestamp for the V2X message and optionally a field incorporating an authentication code for the V2X message.

The invention and its advantages will be better understood by reading the following detailed description of one particular embodiment, given solely as an illustrative and non-limiting example, this description being made with reference to the appended drawings, in which:

[Fig 1] FIG. 1 is a schematic representation of one embodiment of an automated driving system according to the invention;

[Fig 2] FIG. 2 is a timing diagram of the synchronization process for an internal time source such as the one in FIG. 2; and,

[Fig 3] FIG. 3 is a block diagram representation of the method for securing communications according to the invention, implemented in the system of FIG. 1; and,

[Fig 4] FIG. 4 is a representation of the structure of a V2X message as modified according to the present invention.

While remaining compatible with the V2X standard, the invention makes use of reliable mechanisms enabling: synchronizing the communication devices of the automated driving system; timestamping a message by means of the communication device that sends this message; and verifying the timestamp validity of this message by means of the communication device that receives this message.

Preferably, the invention also makes use of reliable mechanisms which allow: securing the data contained in a transmitted message (and consequently the time with which the message was timestamped), and verifying the integrity of the received message.

FIG. 1 schematically represents an automated driving system 1.

This system comprises first and second communication devices 2 and 3 which allow exchanging communications according to the V2X standard.

In the embodiment shown in FIG. 1, the first device 2 is associated with an infrastructure entity 4, and the second device 3 is carried onboard a vehicle 5.

In the embodiment presented in detail here, the infrastructure entity 4 is a three-color traffic light, located at the intersection of two roads. There are three possible values for the state of this entity, which are identified by the colour of the light ("green", "amber", or "red").

The purpose of the V2X communication, between the first device 2 as the transmitting device and the second device 3 as the receiving device, is to inform the vehicle 5 of the presence of an intersection and of the state of the traffic light that protects it, so that the vehicle's control unit 7 can determine a suitable path for the vehicle 5.

The first communication device 2 comprises:

- a geopositioning module 21;
- a V2X radio communication module 22;
- an auxiliary communication module 23;
- a vital computer 24; and
- a routing module 25.

The geopositioning module 21 is specifically designed to receive geopositioning signals emitted by a satellite constellation 11. These signals include, in particular, a clock signal. The satellite constellation 11 therefore constitutes an example of a common external time reference source. The geopositioning module 21 executes, for example, a time server 41 which, in response to a query, indicates a time according to the time reference of the common external source.

The V2X radio communication module 22 allows generating messages according to the V2X standard, transmitting messages according to the V2X standard to other

communication devices of the automated driving system 1, in particular to the second communication device 3, and processing messages according to the V2X standard.

The auxiliary communication module 23 allows establishing a connection with an external network 12, for example an IP network such as the Internet. The module 23 is connected to the external network 12 via a wired connection (Ethernet, for example) or a wireless connection (4G/LTE, for example). This connection allows communication between the first device 2 and a remote control centre 13, which enables an operator to manage the infrastructure entities.

This connection primarily allows the first device 2 to communicate with an external platform 14 constituting a first auxiliary external time reference source. This external platform executes, for example, a time server 42 which, in response to a query, provides a time according to the time reference of the common external source.

The vital computer 24 constitutes, in particular, an internal time reference source. The vital computer 24, for example, executes a time server 43 which, in response to a query, provides a time according to the time reference of the internal source. The vital computer 24 of the first device is synchronized on the basis of the common external source and the first auxiliary external source. According to the invention, a time provided by the vital computer 24 allows timestamping V2X messages transmitted by device 2.

The vital computer 24 is advantageously responsible for verifying the validity of the information from the controller 6, for example by correlating it with measurements performed by the measurement means 15.

The vital computer 24 is also responsible for securely signing or verifying the integrity of the "HMAC field" of a V2X message.

The routing module 25 allows the various modules 21, 22, 23 and 24 to interface with each other and with a controller 6 of the infrastructure entity 4 and with measurement means 15 for measuring the state of the infrastructure entity 4.

The routing module 25 is connected, via an external connection, to the controller 6. This controller 6 is capable of determining the current state of the infrastructure entity 4. As a variant, it is also capable of determining the future state of the infrastructure entity 4. The future state is either the state of the infrastructure entity at the next time increment, or the next state to which the infrastructure entity will switch. In the latter case, the future state includes temporal information corresponding to the expected time of this switch.

The measurement means 15 allow measuring the lamp current of each of the three lamps in the traffic light 4 and applying a suitable measurement signal to the router 25.

The second communication device 3 is preferably identical to the first device 2 just described.

The second device 3 thus comprises:

- a geopositioning module 31;
- a V2X radio communication module 32;
- an auxiliary communication module 33;
- a vital computer 34; and
- a routing module 35.

The geopositioning module 31 is configured to receive geopositioning signals emitted by the satellite constellation 11, which constitutes a common time reference source for devices 2 and 3. The geopositioning module 31 executes, for example, a time server 51 which, in response to a query, indicates a date according to the time reference of the common external source.

The second device 3 is connected such that the communication module 33 is now connected to a second auxiliary external time reference source associated with the vehicle 5, for example a time server 52 running on the vehicle's control unit 7.

The vital computer 34 constitutes an internal time reference source. For example, it executes a time server 53 which, in response to a query, indicates a time according to the internal time reference. The vital computer 34 of the second device is synchronized on the basis of the common external source and the second auxiliary external source. According to the invention, a time provided by the vital computer 34 allows timestamping V2X messages transmitted by device 3.

The vital computer 34 is also responsible for securely signing or verifying the integrity of the "HMAC field" of a V2X message.

The V2X radio communication module 32 is configured to receive a V2X message, verify its integrity, and then its temporal validity, before transmitting the information contained in the received V2X message to the control unit 7 via the routing module 35. This information is, for example, the state of the infrastructure entity 4 associated with the first device 1 from which a message has just been received.

A vital computer such as computer 24 or computer 34 is a "2oo2" ("two out of two") type of vital processing platform, designed to guarantee a high level of safety in the calculations performed, such as determining the internal time reference on the basis of the external time references provided by the two common and auxiliary sources to which the clock module is coupled. The vital computer is compliant, for example, with level 4 of the SIL ("Safety Integrity Level") standard or level D of the ASIL ("Automotive Safety Integrity Level") standard.

The flow of data in the synchronization process 100 of the internal time source of a communication device is shown in FIG. 2:

- in step 110, the clock module initiates the execution of time server 43.

This server is calibrated by querying the common external source and the auxiliary external source. To do this:

- in step 130a, module 24 sends a request to the common external source, more precisely to time server 41 of module 21 (the request is, for example, a request in the "Network Time Protocol" standard - NTP);
- in step 140a, time server 41 of module 21 responds to the request by providing a first time based on the time reference of the common external source (the request being an NTP response for example);
- in step 130b, module 24 sends a request to the auxiliary external source, i.e., time server 42;
- in step 140b, time server 42 responds to the request by providing a second time based on the time reference of the first auxiliary external source;
- then, in step 155, if module 24 concludes that there is consistency between the first and second times, the internal time reference is established, considering it to be a common time base for all components of the system 1. Otherwise, the process 100 loops back to step 110 and is iterated again;
- in step 160, module 24 maintains the internal time reference.

The process 100 is executed periodically, to eliminate any risk of time drift in the internal time source.

Once module 24 is synchronized, the time provided by time server 43 is used to timestamp the V2X messages transmitted by device 2.

A similar description can be given for device 3, for synchronizing the internal time source that consists of module 34.

Referring to FIG. 3, the communication method 200 comprises:

A preliminary step of synchronizing the various devices of the system by implementing, on each device, the process 100 described above.

Then, for the infrastructure entity 4, in order to broadcast the state of this entity, the method comprises a step 210 of determining the state of the infrastructure entity. Determining the state of the infrastructure entity is a vital function. For example, the vital computer 24 compares the state of the traffic light as indicated by the controller 6 and the state corresponding to the lamp current measured by the measurement means 15, in order to determine the vital state.

In step 220, module 22 formats a message in the V2X standard, for example a SPaT message.

The V2X standard defines a SPaT ("Signal Phase and Timing") message, which allows an infrastructure entity to inform the environment about its state.

According to the invention, some of these fields in the payload portion of a message in V2X format are used to transmit information useful to the temporal validity function, and, also preferably, information useful to the integrity verification function according to the invention. This makes it possible to remain compatible with the V2X standard while enabling the implementation of message corruption detection in order to guarantee a high safety level.

For the temporal validity function, the message is timestamped with a message timestamp. The message timestamp incorporated into the message is the one returned by the internal time server 43 at the request of module 22 when it prepares the V2X message to be transmitted.

For the integrity verification function, the message includes an HMAC (hash-based message authentication code).

For example, a truncated 64-bit HMAC code is generated by the vital computer 24, at the request of module 22, based on the various fields of the SPaT message (except for the portion intended to incorporate the HMAC code, which then contains only zeros), preferably using the SHA-256 algorithm and a dynamic 64-byte secret hash key known to the various devices of system 1.

Once the payload of the SPaT message is prepared, the message is encoded in base 64, then communicated to the radio communication unit of module 22 for transmission (step 230).

At the vehicle 5, the V2X message is received and then decoded by device 3 (step 240).

In step 250, in which the integrity of the received V2X message is verified, module 32 decodes the received message. At the request of module 32, the vital computer 34 of the second device 3 calculates an HMAC code based on the fields of the SPaT message (except for the portion incorporating the HMAC code calculated by the transmitter, which then contains only zeros) and compares the calculated HMAC code with the HMAC code contained in the field of the received V2X message. If the comparison fails, the received V2X message is rejected. If the comparison succeeds, the method continues to step 260. This makes it possible to verify the data integrity and the authenticity of the V2X message received.

Next, in step 260, the vital computer 34 of device 3 extracts the message timestamp incorporated in the received V2X message and compares it to the current time of device 3. The latter is obtained by querying the internal time source of device 2. If the message

timestamp differs significantly from the current time of device 3, the V2X message is rejected. Otherwise, the received V2X message is considered temporally valid. This allows verifying the temporal validity of the received V2X message.

If the verification is successful, the information contained in the V2X message (here the state of infrastructure entity 4) is transmitted to the control unit 7 for processing (step 270).

FIG. 4 shows the structure of a SPaT message as an example of a V2X message that can be modified to include a message timestamp and possibly an integrity verification code. Note that a non-optional field in the standard is referred to as an extension field.

The message header contains:

A "Protocol Version" field;

A "Message ID" field;

A "Station ID" field.

The payload contains:

An optional "MoY" field for "Moment of the Year," i.e., the message timestamp;

A "Desc. Name" field, or "Description Name," encoded in 63 bytes;

An "Intersection List" field, encoded in 1 to 32 bytes;

An optional "Regional" field, encoded in 1 to 4 bytes.

According to the invention, the "Desc. Name" field, which provides a text description of the infrastructure entity, is partially reassigned to message protection. Its content is thus adapted to include:

A "Shortened DescName" field, encoded in 1 to 43 bytes;

An "HMAC Tag" field, which is an SHA tag encoded in 4 bytes, with predefined content such as the character string "%#%#" to indicate the presence of the subsequent HMAC field; and

An "HMAC" field encoded in 16 bytes and containing the HMAC code calculated for the integrity verification function.

The information in the "HMAC Tag" and "HMAC" fields is formatted in the IA5 string format of the V2X standard for text fields, to ensure compatibility with this standard.

The "Intersection List" field contains at least one "Intersection State" field, encoded in 1 to 32 bytes, which is used by the invention in the following manner:

An optional "Desc. Name" field, encoded in 63 bytes;

A "Msg Cnt- Rev" or "Message Content" field;

An "Intersection State" field;

A "MoY" field for "Moment of the Year," which is optional in the standard but mandatory in the invention, and which is modified to include the message timestamp;

A "Desc" or "Description" field encoded in 63 bytes;

An optional "Enable Lanes List" field;

A "Movement List" field encoded in 1 to 255 bytes;

An optional "Maneu. Assist" or "Manoeuvre Assist" field; and

5 An optional "Regional" field encoded in 1 to 4 bytes.

While the embodiment described above concerns communication from a transmitting device equipping an infrastructure entity, to a receiving device on board a vehicle, the invention is more general. It could be applied, for example, to guarantee V2X communication messages from a transmitting device on a vehicle to a receiving device associated with an infrastructure entity. For example, this is the case for a priority vehicle (ambulance, police car, etc.) that is able to request a change in the state of the infrastructure entity. For example, the state of the traffic lights protecting an intersection could be adjusted to allow fast passage through the intersection for this priority vehicle.

The invention could also be applied, for example, to guarantee V2X communication messages from a transmitting device on one vehicle to a receiving device on another vehicle.

Furthermore, while the invention has been presented in the context of a SPaT message in particular, other types of messages in the V2X standard can be modified to allow implementing the temporal verification and integrity verification functions.

20 The invention makes it possible to include a temporal signature and, advantageously, also a security signature in a V2X exchange. These signatures are encoded/decoded via a standard implementation of the radio layers of the V2X standard. They therefore do not disrupt the existing operation of the V2X message fields. In other words, an "ordinary" device, i.e., one that does not implement the invention, is still capable of processing V2X messages that have been altered according to the invention. This ordinary device would therefore not be able to verify either the temporal validity or the integrity of the messages.

The invention therefore makes it possible to reliably determine the time of a message and to verify the temporal validity of that message in a safe and secure manner.

30 The invention makes it possible to achieve high safety integrity levels, in particular SIL 4 (according to standard EN 50126-1:2017) or ASIL D (according to standard ISO 26262-1:2018), while remaining compatible with the V2X standard. The proposed solution therefore guarantees the safety level of key traffic information while remaining compatible with the communication standard.

11
CLAIMS

1. A method (200) for securing communications in the V2X standard, in its SAE J2735:2020-07 version, between a transmitting device (2) and a receiving device (3) of an automated driving system (1), characterized in that the method comprises:

5 - a step (100) of temporally synchronizing a vital computer (24) of the transmitting device (2) and a vital computer (34) of the receiving device, on the basis of least one common external time source (11);

- a step (220) of generating a message in the V2X standard by means of the transmitting device (2), consisting of timestamping the message by requesting a current time from the vital computer (24) of the transmitting device and incorporating the current time as the message timestamp in a field of the message in the V2X standard;

10 - a step (230) of transmitting the message in the V2X standard, by the transmitting device (2);

15 - a step (240) of receiving the message in the V2X standard, by the receiving device (3); and

- a step (260) of verifying the temporal validity of the message in the V2X standard, received by the receiving device, by comparing a current time provided by the vital computer of the receiving device with the transmission time incorporated into the received message in the V2X standard.

20

2. Method according to claim 1, wherein the step (100) of temporally synchronizing the vital computers (24, 34) of the transmitting and receiving devices uses at least a second external time source, referred to as an auxiliary external time source, which may be different for the transmitting and receiving devices, the temporal synchronization of the vital computer of the transmitting device and the vital computer of the receiving device being performed while taking into account the time references provided by the first and second external sources.

25

3. Method according to claim 2, wherein the step of temporally synchronizing each vital computer (24, 34) consists of:

30 - initiating (110) the execution of a time server (43, 53) by means of the vital computer;

- sending (130a) a request to the common external time source and receiving (140a) a response containing a first time;

- sending (130b) a request to the auxiliary external time source and receiving (140b) a response containing a second time;

- verifying (155) the consistency between the first and second times, and, if inconsistent, repeating the preceding steps, and, if consistent, establishing an internal time reference which is considered to be a common time base for all components of the system; and
- maintaining (160) the internal time reference.

5 **4.** Method according to any one of the preceding claims, wherein the step (220) of generating a message in the V2X standard further comprises calculating an authentication code, by means of the transmitting device (3), based on the fields of the message in the V2X standard, and a step of incorporating the calculated authentication code into a field of the message, and wherein the method comprises a step (260) of verifying
10 the integrity of the message in the V2X standard, received by the receiving device, by calculating an expected authentication code on the basis of the fields of the received message in the V2X standard and comparing the expected authentication code with the authentication code that is present in the received message in the V2X standard.

5. Method according to claim 4, wherein the authentication code is
15 calculated based on various fields of the message in the V2X standard, by using a hashing algorithm, preferably the SHA-256 algorithm with a dynamic secret hash key known to the various devices of the automated driving system.

6. Method according to claim 4 or claim 5, wherein the authentication code is incorporated into the optional field or a proprietary extension field of the V2X standard.

20 **7.** A communication device compatible with the V2X standard, in its SAE J2735:2020-07 version, characterized in that it comprises a vital computer (24, 34) and a radio communication module, the device being configured to implement the steps on the transmitting device side and/or the steps on the receiving device side of the method according to any one of the preceding claims.

25 **8.** Device according to claim 7, wherein the vital computer is a vital platform of the "2oo2" type.

9. Device according to claim 8, wherein the vital platform is capable of guaranteeing a high level of safety in compliance with safety integrity level SIL 4 or ASIL D.

30 **10.** A communication protocol compatible with the V2X standard, in its SAE J2735:2020-07 version, in which each message in the V2X standard comprises a field incorporating a message timestamp for the message in the V2X standard and optionally a field incorporating an authentication code for the message in the V2X standard.