

System and Method of Protecting Transmitted Data in the NMEA Protocols In Vehicle Control Systems

TECHNICAL FIELD

[001] The present application relates to a method of protecting information fields of National Marine Electronics Association (NMEA) protocols, and also to options for building systems that implement this method. These NMEA protocols are used in vehicle control systems.

[002] Recently, the number of cyberattacks has increased dramatically, including in the case of vehicles. Since the existing control systems of vehicles do not have the means of protection against information attacks of this kind, the attacker is not difficult to implement the desired. Using special technical means, an attacker can easily substitute information about the current coordinates of the vehicle, speed, direction of movement, coordinates of neighboring vehicles, etc. This information is used by the control system for subsequent decision-making in automatic or manual mode. Incorrectly transmitted data can lead to undesirable consequences such as:

- Collision with another vehicle;
- Collision with civilian objects;
- Failure of individual subsystems or units;
- Human victims;
- among others.

[003] Thus, there is an urgent need to develop a method of providing protection against cyber attacks of this kind. One option to provide this kind of protection as described in this method.

[004] The main purpose of the method as herein described is to prevent unauthorized attacks (caused, but not limited to the substitution of transmitted data) on the vehicle control system. The implementation of the described method can be represented as a separate system or as an add-in to an existing system. The construction of the system has various options for its implementation: hardware, software or hardware.

[005] The technology as described herein determines a method of protection of transmitted data by the NMEA protocols. Protection against unauthorized intrusion and substitution of information in the data fields of the Protocol is provided. The authentication process between devices is also provided. The implementation is an add-on to the NMEA protocols.

[006] The NMEA protocols define the rules for the organization of data exchange between the equipment of the vehicle (mainly, but not limited to sea and rail transports). The NMEA standard is designed to provide a communication channel between the navigation equipment (time signal receiver) and the control center or control device(s).

BRIEF DESCRIPTION OF THE DRAWINGS

[007] **Figure 1** illustrates a typical topology of connecting devices in a serial bus standard NMEA;

[008] **Figure 2** shows the structure of NMEA fields;

[009] **Figure 3** illustrates a variant of man-in-the-middle attack on a serial NMEA bus;

[0010] **Figure 4** illustrates the format of NMEA messages (CGA identifier);

[0011] **Figure 5** shows the formation (preparation) of a sequence of geographic coordinates data for encryption;

[0012] **Figure 6** shows a functional block diagram of the implementation of the encryption algorithm AES128 (CFB mode) to standard NMEA;

[0013] **Figure 7** shows the distribution of the encrypted text in the fields package of standard NMEA;

[0014] **Figure 8** shows the functional implementation scheme of the block encryption algorithm AES128 (CFB mode) decryption method for the NMEA standard;

[0015] **Figure 9** shows a generalized block diagram of the system implementing the described method.

DETAILED DESCRIPTION

[0016] The present invention deals with a method of protecting individual fields of NMEA message data containing, inter alia, information on the geographical coordinates of the vehicle (but not limited to). This data is the most important element of the information transmitted through NMEA.

[0017] According to the NMEA standard, vehicle navigation coordinates can only be transmitted in two types of messages: talker sentences and proprietary sentences.

[0018] The NMEA standard defines a large number (more than 50) of message variants for the output message type. Each of them is defined in the message ID field (202), namely through the SSS parameter (message ID). The message format for «the output message» type is shown in Figure 2.

[0019] The geographical coordinates of the vehicle for "talker sentences" are transmitted with the following SSS message IDs (202):

- [BEC] Bearing & Distance to Waypoint;
- [BWR] Bearing and Distance to Waypoint;
- [GGA] Global Positioning System Fix Data;
- [GLL] Geographic Position;
- [RMA] Recommended Minimum Navigation Information;
- [RMB] Recommended Minimum Navigation Information;
- [RMC] Recommended Minimum Navigation Information;
- [WPL] Waypoint Location;
- Among others.

[0020] Geographic coordinates of transport for some established "proprietary sentences" are transmitted with the following message identifiers:

- \$PGRMFPosition Fix Sentence;
- \$PGRMISensor Initialisation Information;
- Among others.

[0021] The navigation coordinates of the vessel are determined by two parameters: latitude and longitude.

[0022] The latitude value for the "talker sentences"/ "proprietary sentences" types is located in one of the dataset fields (204) in Figure 2. For each of the SSS message IDs (202), the specified field has a set place in the general sequence of the message fields (according to the NMEA standard).

[0023] The latitude value has the following presentation format – **BBBB.BBBB,a** (BB – degrees; BB.BBBB – whole and fractional minutes; a – N/S).

[0024] The longitude value for the "talker sentences"/ "proprietary sentences" types is in one of the dataset fields (204) Figure 2. For each of the SSS message IDs (202), the specified field has a set place in the General sequence of message fields (according to the NMEA standard).

[0025] The longitude value has the following representation format – **LLLLL.LLLL,a** (LLL– degrees; LL.LLLL – whole and fractional minutes; a – E/W).

[0026] Figure 4 shows a description of the message with the GGA type identifier (Global Positioning System Fix Data). Where data sets represented by field 204 have the following purposes: field observational time (204.1); latitude (204.2 + 204.3); longitude (204.4+204.5); indicator of the quality of observation (204.6); number of satellites in use, may be different from the number in view (204.7); the size of the horizontal geometric factor (204.8); the height above mean sea level (204.9); unit of height – meters (204.10); the excess of the geoid above the ellipsoid WGS-84 (204.11); unit of measurement – meters (204.12); age of differential corrections (204.13); the ID of the differential station (204.14);

[0027] The information intended for protection consists of two components: **BBBB.BBBB,a + LLLLL.LLLL,a** (latitude + longitude).

[0028] As a way to protect these data, it is proposed to use the AES block encryption algorithm with the encryption key length 128 (AES128). However, to use this encryption method, the following conditions must be met - the length of each block must be equal to the length of the encryption key (key), namely 128 bits.

[0029] Figure 5 shows a method of forming the resulting sequence data (211), designed to encrypt. Data sets 204.2, 204.3, 204.4, 204.5 are the initial information for drawing up this sequence of data. The total length of the sequence 211 is 76 bits.

[0030] There are several ways to solve the problem of different length of the cipher key (128 bit) and the message block (76 bit) when using a block encryption algorithm. In the proposed method, the variant of using AES128 in the CFB mode is considered (Cipher Feedback mode).

[0031] To use the AES128 encryption algorithm, all devices must have the same cipher key. Therefore, this information must be communicated to the devices before they can start working. Methods and channels of transmission of the cipher key can be different and determined by organizational activities.

[0032] For CFB mode, you must additionally use the Initialization Vector (IV) parameter. This parameter, as well as the encrypted key, must be identical on all devices.

[0033] In the proposed method, parameter IV is used as a device authentication factor. The same IV can be used on a permanent basis or at each new communication session. Methods can be different and are determined by organizational activities.

Based on the above measures, the NMEA Protocol provides:

- protection (encryption) of data fields; and
- authentication of devices within the NMEA Protocol.

[0034] Figure 1 shows a typical topology of connecting devices to each other according to the NMEA standard. A navigation device (101), an accurate time signal receiver can be any device that supports the NMEA standard in terms of message transmission, as well as defined to work in one or more satellite navigation systems (GPS, GLONASS, DORIS, BeiDou, Galileo & etc.). The control modules (102, 103, 104), which receive information from the device of the receiver of accurate time signals can be any device or system, for example: navigation equipment, satellite antennas, lidars, radars, radar stations,

automated systems of boat traffic, etc.). A specialist in this field of technology should understand that different devices or centers can be used as modules. The number of such devices is determined by the topology of the system and the technical characteristics of the communication interface. Communication lines (111, 112, 113, 114) with which the switching of all devices involved in the exchange of data according to the NMEA standard is performed.

[0035] An asynchronous serial interface RS-422/485 or CAN interface is used as a communication interface to combine the device of the time signal receiver or navigation device (101) and control modules (102, 103, 104).

[0036] The NMEA protocols describe the format of transmitted messages, as well as the speed of exchange. For different standards (NMEA-0183, NMEA-2000), these parameters have different values, which are written directly in the standards.

[0037] The NMEA standard is a text Protocol (ASCII format). Messages can be of three types:

- Talker sentences;
- Query sentences;
- Proprietary sentences.

[0038] Figure 2 shows the generalized structure of the output message fields. Messages begin with "\$" (201) and end with "*" (205). The message is identified by the header (202), where tt is the navigation system ID; sss is the message ID. Further, depending on the message identifier, a set of data (204) is transmitted, the number of which depends on the type. All data fields are separated by "," (203). The "hh" (206) is the result of an 8-bit operation XOR-sum of all characters (including ",") in the string between "\$" and "*" reduced to two uppercase ASCII characters for the 16-bit representation of the byte (0-9,A-F). The "CR" (207) carriage return and "LR" (208) carriage transfer fields are an indication of the end of the message transfer.

[0039] In modern vehicles, especially in shipping and rail transport, the NMEA (serial data transmission) standard is widely used for the transmission of control and control data by ship (including geographical coordinates). These serial

networks are often "connected" at several points to higher-level vessel control networks, including GPS, satellite terminal, ECDIS, etc.

[0040] These serial networks (based on NMEA) are used not only to transmit geographical coordinates, but also to monitor the operation of individual parts, such as steering gears, engines, ballast pumps, etc.

[0041] In particular, due to the fact that the publication of the first versions of the NMEA standard took place in the 90-ies of XX century, this standard is not fully able to ensure the security of the transmitted data.

[0042] However, subsequent versions of the standard (including the new generation of the NMEA-2000 standard) did not solve the above problems. The main drawbacks of the NMEA standard are that all messages do not have authentication, encryption, or validation. All data is transmitted in text format as ASCII characters. This allows an attacker to change data without hindrance when connecting to a serial network (for example, by means of «a man-in-the-middle» attack). For example, using GPS-spoofing can "embed" subtle errors to slowly but surely knock the ship off course or another vehicle. Incorrect information about the position of transport can cause consequences such as:

- Crash of the transport;
- Collision with other vehicles;
- Infrastructure damage;
- Human victims.

[0043] By attacking, intruders change information about the position and speed of transport (but not limited to the substitution of these data) — that is, the data that the control system collects and transmits, for example, the port Manager, to avoid a collision with other ships. An attack on the GPS signal or connection to the control system is fraught with navigation problems up to the collision of vehicles, which always leads to serious damage, and sometimes to human victims.

[0044] The cause of these attacks is a software vulnerability of the NMEA standard. A set of measures to protect, inform, and eliminate such attacks refers

to the information security of vehicles (primarily, but not limited to modern ships, railway transport).

[0045] Figure 3 shows one possible attack (man-in-the-middle) on a serial NMEA data bus. We considered the case when the attacker has performed the connection to your device (121). Thus, it may, at its discretion, change the data fields of the NMEA standard in messages sent by the navigation device (101). And while remaining unnoticed for the other modules (102, 103, 104).

[0046] There are several ways to protect against the presented variants of attacks: protection at the software level; and/or hardware protection.

[0047] The method presented in the present invention is designed to provide protection based on encryption/decryption of data fields of the NMEA standard, without changing the structure and sequence of fields.

Detailed Description of the Preferred Embodiments

[0048] Figure 6 shows a functional diagram of a block encryption algorithm AES128 mode (CFB) cipher text length is 76 bits. The encryption key (301) is 128 bits long, as is the Initialization Vector (302). At the beginning of the algorithm, Initialization Vector (302) is encrypted using the AES128 block encryption algorithm. Encryption takes place in Block Cipher Encryption (303) using the encryption key (301). The result of encryption is a sequence of 128 bits (304). Then the first 76 bits of information are extracted from the obtained sequence and the addition operation is performed modulo two XOR (305). The input data for the addition operation modulo two, in addition to the previously obtained sequence, is the desired prepared field (211). The result of the operation (305) is encrypted text (304), its length is 76 bits.

[0049] After receiving the encrypted text, the NMEA message packet is generated.

[0050] Figure 7 shows the distribution of the ciphertext in the fields of the packet messages of the standard NMEA (for example, CGA). The resulting encrypted text (304) has a length of 76 bits, which corresponds to the number of ASCII

characters equal to 19 (4 bits per character). In figure 7, every 4 bits of information is numbered A1...A19. As previously shown in figure 5, numbered A1...A19 in strict compliance are encapsulated in the package of messages of the standard NMEA.

[0051] The generated final parcel is sent to the communication channel. Becomes available to receivers. After receiving this parcel on the receiver side, the reverse process of de-encapsulation and decryption is performed.

[0052] Figure 8 shows a functional diagram block of the algorithm AES-128 (CFB mode) to decrypt a message length equal to 76 bits. The encryption key (301) is 128 bits long, as is the Initialization Vector (302). At the beginning of the algorithm, Initialization Vector (302) is encrypted using the AES128 algorithm. Encryption takes place in Block Cipher Encryption (303) using the encryption key (301). The result of encryption is a sequence of 128 bits (304). Then the first 76 bits of information are extracted from the obtained sequence and the addition operation is performed modulo 2 XOR (305). The input data for the addition operation modulo 2, in addition to the previously obtained sequence, is the resulting cipher text (304). The result of the operation (211) is the navigation coordinates that can be used by the receiver further to the destination.

[0053] Figure 9 shows a generalized block diagram of the system implementing the specified method of data protection transmitted in the NMEA standard. To implement the algorithms described above, encryption/decryption units (401, 402) are integrated in the time receiver or navigation device (101), as well as in the control device (102). These modules are designed to implement block encryption algorithm AES-128 (CFB mode).

Claims

1. The system of protection of transmitted data for control and control of the vehicle between the navigation device and the vehicle control system according to the NMEA standard, while the system additionally contains an encryption/decryption unit used AES128 block encryption algorithm (CFB mode), made with the ability to encrypt / decrypt fields of the NMEA standard.
2. Method of data protection is applicable to protocols of standard NMEA all existing versions and is designed to protect the fields with the information data of the vehicle to exchange with the adjacent modules on the vehicle through the encryption/decryption algorithm block cipher AES-128 (CFB mode).
3. The method according to claim 2, in which the NMEA standard establishes various types of messages, including those intended for the transmission of geographical coordinates, and these messages are determined by the following identifiers within the NMEA standard: BEC, BWR, GCA, RMA, RMB, RMC, GLL, WPL, \$PGRMFPosition, \$PGRMISensor etc.
4. Method according to claim 3, in which the fields of the NMEA standard contains information about the geographical coordinates of the vessel, having the following format:
 - BBBB.BBBB,a – latitude (36 bit length);
 - LLLLL.LLLL,a – longitude (length 40 bits),each character has an ASCII representation and has a length of 4 bits. Thus, the total length of the geographic coordinate fields is 76 bits.
5. Method according to claim 2, characterized in that the encryption fields NMEA standard containing information about the coordinates of the vessel, a block encryption algorithm is used AES-128.

6. Method according to claim 2, characterized in that the block encryption algorithm AES-128 encryption mode is used CFB (Cipher Feedback) with the length of the encrypted data is 76 bits.
7. Method according to claim 2, characterized in that to solve the problem of encryption/decryption on the devices involved in the exchange of messages according to the NMEA standard installed software (hardware or hardware), which implements the execution of algorithms AES-128 (CFB mode 76 bit length).
8. Method according to claim 6, characterized in that for the implementation of the algorithm AES-128 (CFB mode 76 bit length) adjacent modules use the same cipher keys, which should not be available for reading by an attacker.
9. Method according to claim 6, characterized in that for the implementation of the algorithm AES-128 (CFB mode 76 bit length) adjacent modules use the same Initialization Vector, which can be manually entered by the user.