(19) LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie

(11) N° de publication : **LU101567**

(12) **BREVET D'INVENTION** **B1**

(21) N° de dépôt: LU101567

(51) Int. Cl.:
H04L 12/28

(22) Date de dépôt: 17/12/2019

(30) Priorité:

(43) Date de mise à disposition du public: 17/06/2021

(47) Date de délivrance: 17/06/2021

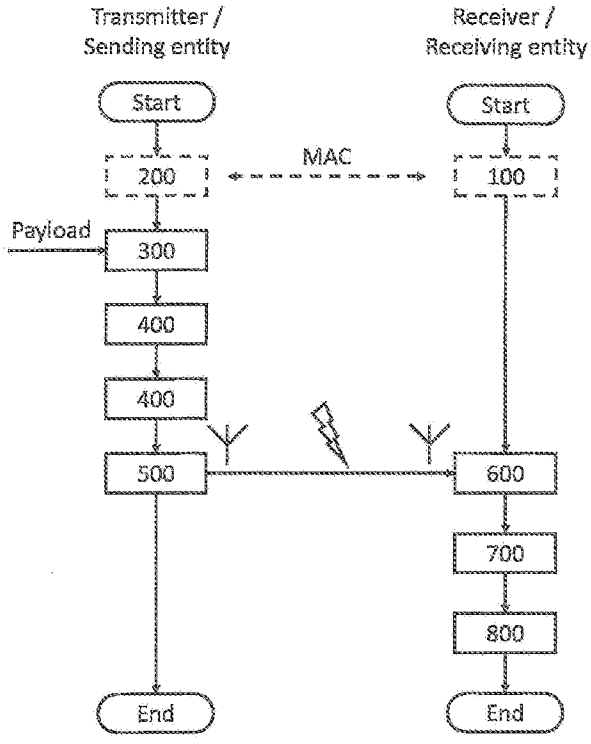
(73) Titulaire(s):
Universität Bremen – 28359 Bremen (Allemagne)

(72) Inventeur(s):
DEMEL Johannes – 28211 Bremen (Allemagne),
BOCKELMANN Carsten – 28832 Achim (Allemagne),
DEKORSY Armin – 28357 Bremen (Allemagne)

(74) Mandataire(s):
RCD-Patent PartG mbB –
52118 Herzogenrath (Allemagne)

(54) **Method for a sending entity and method for a receiving entity in a network environment.**

(57) The invention relates to a method for a sending entity in a network environment, comprising the steps of - Receiving (200) payload information for a specific receiver, - Adding (300) a Message Authentication Code based on a pre-known key of the receiver to thereby form an information for being encoded, - encoding (400) the information for being encoded, - Sending (500) the encoded information towards the receiver. The invention also relates to a method for a receiving entity in a network environment, comprising the steps of - Receiving (600) encoded information, - Decoding (700) the encoded information into decoded information, - Determine (800) whether the decoded information may be authenticated based on a pre-known key of the receiver, and if the authentication is given, passing the decoded information or parts thereof on for further processing. The invention also relates to a corresponding sending entity and a corresponding receiving entity.



Method for a sending entity and method for a receiving entity in a network environment

The invention relates to a method for a sending entity and a method for a receiving entity in a network environment.

Background

It is known that with the ongoing trend to provide devices with communication capabilities data originating from these devices is sent towards one or more recipients.

In the customer set-up this is known as smart devices and is often quoted in context of smart-homes. There different devices such as energy sources or energy consumers provide data regarding to their current status. For example a photovoltaic arrangement may provide data with respect to actual power generation, whether or not a panel provides less energy than others, while a heating may provide data with respect to a current temperature for heating or hot water purposes, actual energy consumption, and the like, temperature sensors and wind sensors may provide actual measurement data. Sensors and actors arranged at different locations are providing status data and/or receive data related to certain operations. For example, screens may be steered to a certain level.

In industry a like scenario is known as Industry 4.0. There, the communication of machines with each other is also known as Machine-to-Machine communication, also known as M2M.

Within transportation, autonomous driving gains interest. Within such a set-up It is envisaged that vehicles may communicate with each other but may also communicate with infrastructure.

While most devices in a household are stationary, it is perceived as a drawback if a wiring has to be provided for connecting these appliances. Also, in transportation related scenarios, including industry 4.0, the devices are typically mobile. Typically, all of the above scenarios are summarized as Internet of things, abbreviated IoT.

17.10.19 BA

To allow for communication, the communication has to be wireless. As the name suggests IoT devices are typically connected to a public network. However, because information in these set-ups may be sensitive, the communication shall be secure and reliable. Consequently, security needs to be deeply integrated into the design of any wireless communication system, especially on the physical layer. Such requirements lead to added overhead to the payload data.

Most of the payload data sent from one entity to another within these scenarios is rather small, e.g. around 128 bit. This type of communication is also known as Machine Type Communication (MTC).

State-of-the-Art communication technologies, such as LTE or WiFi, focus on large file transfers, e.g. video streaming, which efficiently uses large packets. As a consequence, there is a lot of Communication overhead for short packets, e.g. control information, wasting a lot of bandwidth. Typically, in IoT scenarios within given Communication Schemes the overhead exceeds (by far) the payload.

Furthermore, many applications, e.g. autonomous driving or I4.0, require extremely high communication system reliability. This requirement is often referred to as five 9's or 10^{-9}. Failure to deliver such reliability requirements for e.g. I4.0 applications, results in halted production lines. In case of autonomous driving it may result in fatal crashes.

A communication system for IoT applications must provide the required reliability or it cannot be employed for the envisaged application.

Starting from this situation it is an object of the invention to provide methods and devices allowing to reduce overhead while not compromising with reliability and security.

Short description of the invention

The object is solved by the methods according to claims 1 and 2, respectively the entities of claim 13 and 14. Further advantageous embodiments are subject to the dependent claims, as well as the description and the accompanying figures.

Brief description of the drawings

In the following reference will be made towards the figures. In these

Fig. 1 shows a schematic data processing scheme according to prior art,

Fig. 2 shows a schematic data processing scheme according to embodiments of the invention, and

Fig. 3 shows a schematic flowchart of method steps in different entities according to embodiments of the invention.

Detailed Description

The present disclosure describes preferred embodiments with reference to the Figures, in which like reference signs represent the same or similar elements.

Reference throughout this specification to "one embodiment," "an embodiment," or similar language means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, appearances of the phrases "in one embodiment," "in an embodiment" and similar language throughout this specification may, but do not necessarily, all refer to the same embodiment.

The described features, structures, or characteristics of the invention may be combined in any suitable manner in one or more embodiments. In the description, numerous specific details are recited to provide a thorough understanding of embodiments of the invention. I.e., unless indicated as alternative only any feature of an embodiment may also be utilized in another embodiment.

In addition, even though at some occurrences certain features will be described with reference to a single entity, such a description is for illustrative purpose only and actual implementations of the invention may also comprise one or more of these entities. I.e. usage of singular also encompasses plural entities unless indicated.

An exemplary embodiment will now be described with reference to the figure.

In Fig. 1 a typical processing in a state of the art communication system, such as a LTE based communication system, is shown.

There the requirements of security and reliability are embodied by different domains having an independent processing.

In the security domain, the two key targets are data confidentiality and authentication. Encryption keeps data packet contents confidential. Otherwise this information may leak production details to unauthorized third parties.

State-of-the-Art encryption may be facilitated with the Advanced Encryption Standard (AES) standard. Authentication verifies the origin of received packets in order to distinguish authorized from non-authorized data. This is often facilitated with a Message Authentication Code (MAC) in order to verify integrity of a received packet. The most prominent options for this are Keyed-hash Message Authentication Code (HMAC) and Cipher-based Message Authentication Code (CMAC). The key concept is to add a cryptographic checksum (overhead) to the payload for message authentication.

In the reliability domain, the focus is on correct packet reception. Many different forward error channel coding concepts are available in this domain. The integrity of received packets may be verified via Cyclic Redundancy Check (CRC) encoding with a high level of assurance. A CRC adds a checksum (overhead) to each packet for verification. Transmissions are prone to errors, thus, Forward Error Correction (FEC) provides capabilities to correct errors at the receiver.

As already indicated, packet overhead becomes a pronounced problem for short packets which are often observed in M2M communication.

In a more detailed understanding, one may find that both CRC and MAC add a checksum to each packet for integrity verification. There is a minor difference, in that the MAC checksum supports additional functionality, namely authentication. This is due to the common approach that each issue shall be dealt within its own domain and provide independent results.

However, the inventors noticed that in case one would deviate from the layered view of independent purposes, one may obviate processing of one checksum. Therefore, the inventors propose as shown in Fig.2 to make use of the MAC checksum only, while obviating the need of calculating a CRC. Therefore, one may reduce overhead.

The invention therefore proposes a method for a sending entity in a network environment. The method comprises a step of receiving 200 payload information for a specific receiver. The transmitter adds in step 300 a Message Authentication Code based on a pre-known key of the receiver to thereby

17.12.15 BS

form an information for being encoded. Then the information is encoded in step 400 and thereafter conveyed in step 500 towards the receiver.

In embodiments of the invention the coding 400 is a polar encoding or a turbo coding. It is to be noted that there might exist several implementations allowing to combine a decoding with an authentication code, namely the combination of a list decoder and a polar code. However, this is not limiting. Other codes such as turbo codes may provide similar properties. Hence, the coding may be based on this intended usage.

In order to meet high reliability requirements, one may further introduce certain codes for FEC. An example is the usage of polar codes for FEC. Polar codes are known to provide high error correction performance for short packets. For details, see e.g. E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels", IEEE Transactions on Information Theory, (2009).

For the transmitter, one may combine Polar codes with MAC for overhead reduction.

On the receiving side, the invention proposes a method for a receiving entity in a network environment. The method comprises a step of receiving 600 an encoded information, conveyed by the transmitter in step 500. The encoded information is then decoded in step 700 to thereby provide decoded information. Thereafter one may determine in step 800 whether the decoded information may be authenticated based on a pre-known key of the receiver, and if the authentication is given, passing the decoded information or parts thereof on for further processing.

In an embodiment of the receiving method, a message authentication code is used for verifying correct decoding or for feeding back information to the decoding method for enhanced decoding.

It is to be noted that there might exist several implementations allowing to combine a decoding with an authentication code, namely the combination of a list decoder and a polar code. However, this is not limiting. Other codes such as turbo codes may provide similar properties.

E.g. in an embodiment of the receiving method the decoding 700 is based on a candidate list such that candidates of the decoding are subject to the determination until a first candidate is authenticated or the end of the list of candidates is exhausted.

On the side of the receiver, in embodiments of the invention one may then make use of a decoder like Arikan's Successive Cancellation SC decoder to produce a single information word which can be verified by a checksum with the proposed MAC checksum.

More sophisticated decoders can make additional use of this checksum.

17.12.19 BS

Examples of such sophisticated decoders can be found in "List Decoding of Polar Codes", I. Tal and A. Vardy, in IEEE Transactions on Information Theory, (2015), "Low-Complexity Soft-Output Decoding of Polar Codes", U. U. Fayyaz and J. R. Barry, in IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, 32 (2014) and "Dynamic-SCFlip Decoding of Polar Codes", L. Chandesris, V. Savin, and D. Declercq in IEEE Global Communications Conference (GLOBECOM), 2016.

All State-of-the-Art polar decoders use a CRC checksum in order to identify correctly received codewords. We propose to use a MAC checksum instead.

This information may then be used as an early stop criterion for such a decoder or to decide for the correct codeword among many.

In any case the resulting system joins the security and reliability domain. It is more efficient in terms of overhead because the overhead caused by a CRC checksum is eliminated.

The invention may be used in any kind of network environment, in particular a wireless network environment. Furthermore, the invention may be of particular relevance in a mobile network system environment such as a Public Land Mobile Network, e.g. a Network of 2nd, 3rd, 4th, 5th or 6th generation.

In particular, the network environment may be an internet of things environment.

As shown in Figure 3, the pre-known key may be provided towards the transmitter, e.g. via a control channel. There may also be other means to provide the pre-known key. E.g. the pre-known key may be provided by a specialized database service within the network and/or a pre-known key may be preset.

In particular, the (polar-) encoding may provide FEC properties in embodiments of the invention.

Furthermore, the invention proposes a Sending entity respectively a Receiving entity adapted to perform any one of the above highlighted methods.

The invention deviates from the common approach and allows to integrate security and reliability aspects instead of treating them as separate entities. The resulting system is more efficient because overhead can be reduced while it provides like or even error correction performance than currently employed systems.

As such the invention allows for overhead reduction, which is of high importance for short M2M packet transmissions. e.g. for 128 bit packets with a typical CRC 32 bit checksum. This results in about 25 % overhead reduction.

The invention allows to maintain FEC performance.

Usage of polar Codes allow to reduce receiver complexity, especially in conjunction with a checksum.

17.12.19 B

Claims

1. Method for a sending entity in a network environment, comprising the steps of
   - Receiving (200) payload information for a specific receiver,
   - Adding (300) a Message Authentication Code based on a pre-known key of the receiver to thereby form an information for being encoded,
   - encoding (400) the information for being encoded,
   - Sending (500) the encoded information towards the receiver.

2. Method for a receiving entity in a network environment, comprising the steps of
   - Receiving (600) encoded information,
   - Decoding (700) the encoded information into decoded information,
   - Determine (800) whether the decoded information may be authenticated based on a pre-known key of the receiver, and if the authentication is given, passing the decoded information or parts thereof on for further processing.

3. Method according to claim 2, wherein a message authentication code is used for verifying correct decoding or for feeding back information to the decoding method for enhanced decoding.

4. Method according to claim 2 or 3, wherein decoding (700) is based on a candidate list such that candidates of the decoding are subject to the determination until a first candidate is authenticated or the end of the list of candidates is exhausted.

5. Method according to one of the proceeding claims, wherein the coding (400.700) is a polar encoding or a turbo coding.

6. Method according to one of the proceeding claims, wherein the network environment is a wireless network environment.

17.12.18 PS

7. Method according to one of the proceeding claims, wherein the network environment is a mobile network system environment.

8. Method according to one of the proceeding claims, wherein the network environment is an internet of things environment.

9. Method according to one of the proceeding claims, wherein the pre-known key is provided via a control channel.

10. Method according to one of the proceeding claims 1 to 7, wherein the pre-known key is preset.

11. Method according to one of the proceeding claims, wherein encoding provides FEC properties.

12. Method according to one of the proceeding claims, wherein decoding is based on an Arikan's Successive Cancellation decoder.

13. Sending entity adapted to perform a method according to claim 1 or claims 3-12 when being dependent on claim 1.

14. Receiving entity adapted to perform a method according to claim 2 or claims 3-12 when being dependent on claim 2.

Übersetzte Ansprüche

1. Verfahren für eine sendende Einheit in einer Netzwerkumgebung, aufweisend die Schritte
   - Empfangen (200) von Nutzinformationen für einen bestimmten Empfänger,
   - Hinzufügen (300) eines Nachrichtenauthentifizierungscodes basierend auf einem bekannten Schlüssel des Empfängers, um dadurch eine zu kodierende Information zu bilden,
   - Kodierung (400) der zu kodierenden Informationen,
   - Senden (500) der kodierten Informationen in Richtung des Empfängers.

2. Verfahren für eine empfangende Einheit in einer Netzwerkumgebung, aufweisend die Schritte
   - Empfangen (600) von kodierter Information,
   - Dekodierung (700) der kodierten Information in dekodierte Information,
   - Bestimmen (800), ob die dekodierte Information basierend auf einem bekannten Schlüssel des Empfängers authentifiziert werden kann, und falls die Authentizität gegeben ist, weiterleiten der dekodierten Information oder Teil davon an eine weitergehende Verarbeitung.

3. Verfahren gemäß Anspruch 2, wobei ein Nachrichtenauthentifizierungscode verwendet wird, um ein korrektes Dekodieren zu verifizieren oder um Information an das Dekodierverfahren für eine verbessertes Kodieren zurückzuführen.

4. Verfahren gemäß Anspruch 2 oder 3, wobei die Dekodierung (700) auf einer Kandidatenliste basiert ist sodass Kandidaten des Dekodierens Gegenstand für die Bestimmung sind, solange bis ein erster Kandidat authentifiziert ist oder das Ende de Liste von Kandidaten erreicht ist.

5. Verfahren gemäß einem der vorhergehenden Ansprüche, wobei die Kodierung (400.700) eine Polarkodierung oder eine Turbokodierung ist.

6. Verfahren gemäß einem der vorhergehenden Ansprüche, wobei die Netzwerkumgebung eine drahtlose Netzwerkumgebung ist.

7. Verfahren gemäß einem der vorhergehenden Ansprüche, wobei die Netzwerkumgebung eine mobile Netzwerkumgebung ist.

8. Verfahren gemäß einem der vorhergehenden Ansprüche, wobei die Netzwerkumgebung eine „Intenet-der-Dinge"-Umgebung.

9. Verfahren gemäß einem der vorhergehenden Ansprüche, wobei der bekannte Schlüssel über einen Steuerkanal bereitgestellt ist.

10. Verfahren gemäß einem der vorhergehenden Ansprüche 1 bis 7, wobei der bekannte Schlüssel voreingestellt ist.

11. Verfahren gemäß einem der vorhergehenden Ansprüche, wobei Kodieren FEC Eigenschaften zur Verfügung stellt.

12. Verfahren gemäß einem der vorhergehenden Ansprüche, wobei Dekodieren auf einem Arikan's Successive Cancellation Dekoder basiert.

13. Sendende Einheit, eingerichtet um ein Verfahren gemäß einem der Ansprüche 1 oder 3-12, wenn abhängig von Anspruch 1, auszuführen.

14. Empfangende Einheit, eingerichtet, um ein Verfahren gemäß einem der Ansprüche 2 oder 3-12, wenn abhängig von Anspruch 2, auszuführen.

17.12.19 7-5

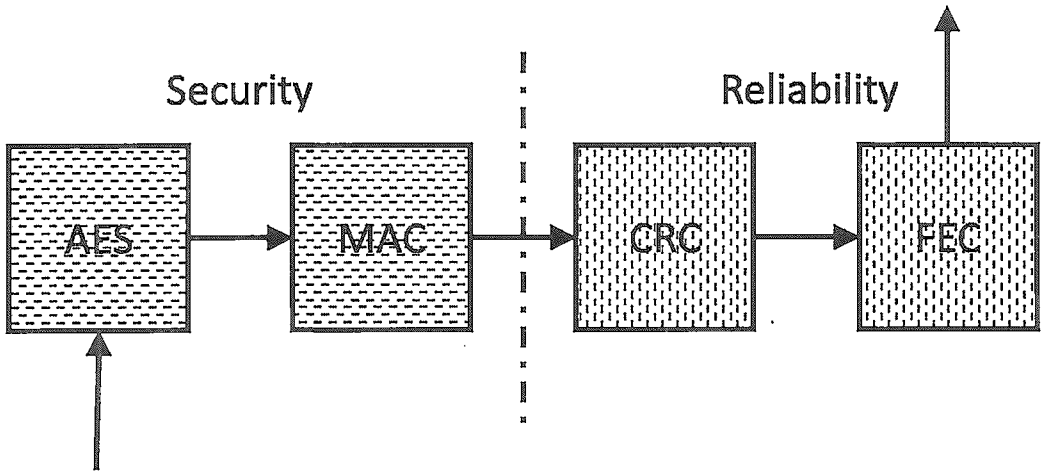


Fig. 1 – Prior Art

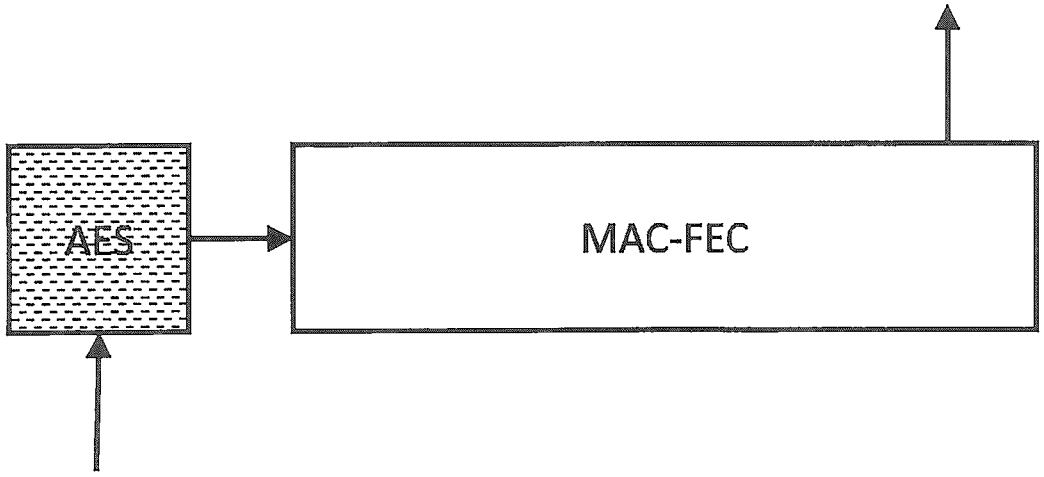


Fig. 2

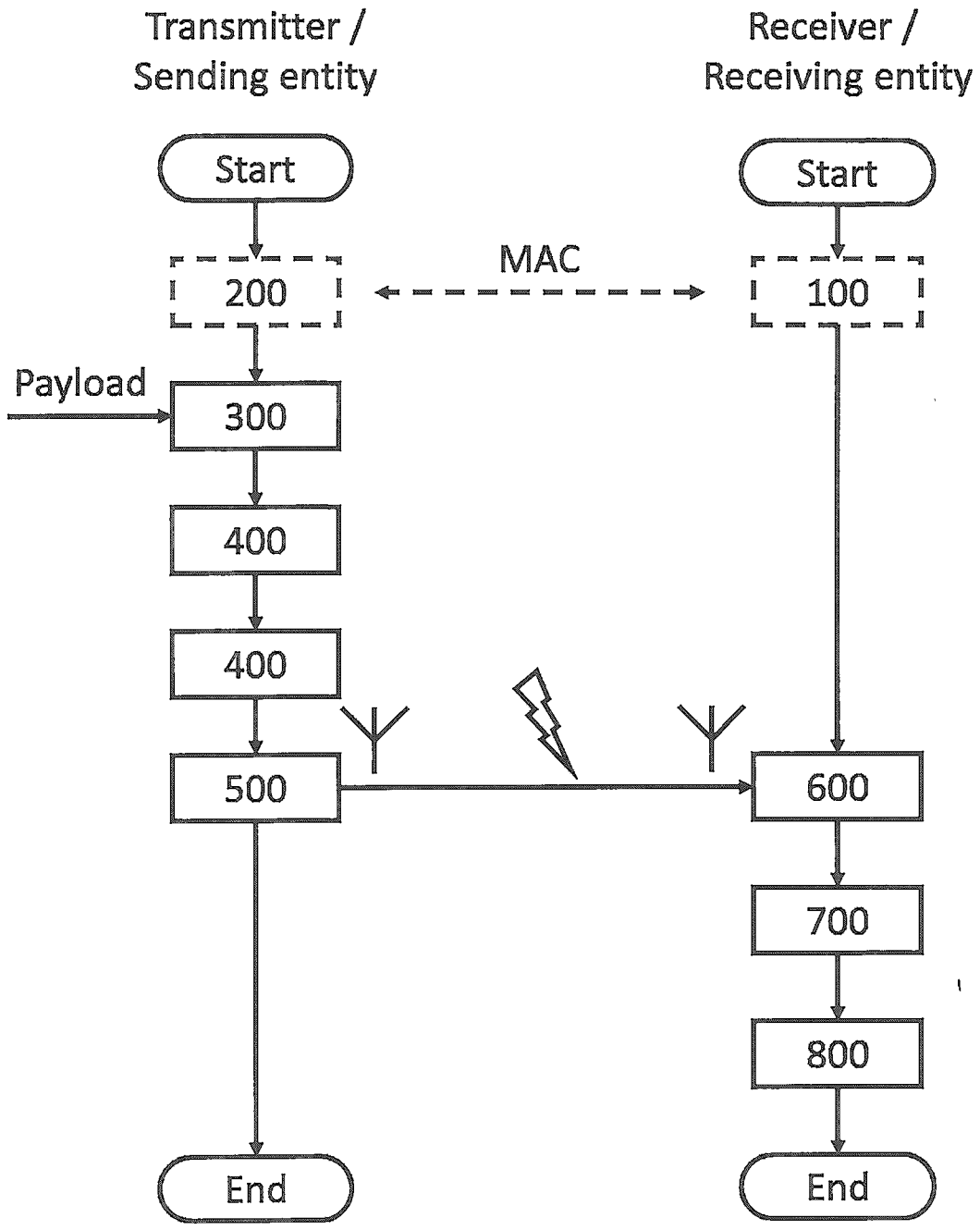


Fig. 3

17.10.19 FF