Patents of Prof. Dr. Christoph Ruland

July 29, 2019

Granted Patents

DE10 2008 040 797: Verfahren zum Empfangen eines Datenblocks, 2010

DE10 2008 055 139: Verfahren zum Senden und Empfangen eines Datenblocks, 2010

DE10 2008 021 933: Verfahren zur Bestimmung einer Kette von Schlüsseln, Verfahren zur Übertragung einer Teilkette der Schlüssel, Computersystem und Chipkarte, 2010

DE 10 2009 026 936: Vorrichtung zum Anschluss an ein elektrisches Energieversorgungsnetz und Transportsystem, 2012

US 8,196, 015: Method for transmitting and receiving a data block and a corresponding transmitter and receiver, 2012

DE 10 2011 088 827: Roulettetisch und Brettspiel mit elektronischer Bestimmung der räumlichen Position eines Objekts, 2012

US 8,737,515 B2: Method for determining the spatial position of an object, electronic circuit and electronic system, 2014

DE 10 2014 215 737: Verifizierung von Zeitzeichen, 2014

DE 10 2011 079 870 B4: Mobile Ladestation für Elektrofahrzeuge und Ladesystem, 2015

DE 10 2012 223 385 B4: Verfahren zur Bestimmung der räumlichen Position eines Objektes, elektronische Schaltung und elektronisches System, 2015

EP 3 001 592: Verifizierung von Zeitzeichen, 2017

EP 2 551 145: Mobile Ladestation für Elektrofahrzeuge und Ladesystem, 2017

US 10,165,530: Verification of Time Information transmitted by Time Signals or Time Telegrams, 2018

Patents of Prof. Dr. Christoph Ruland

July 29, 2019

Patent Families with Abstracts

1. Patent family „Verification of Time Information transmitted by Time Signals or Time Telegrams"

1.1. DE 10 2014 215 737, Verifizierung von Zeitzeichen, granted 2014

There are different possibilities to distribute the actual time information. Many systems require the actual and correct time information to switch on or off devices. Time information distributed over the internet or other media can not be trusted. Man-in-themiddle attacks are possible.

The method in this patent is applied to time information services, which broadcast time information via wired or wireless transmission media, for example by long waves, radio services or ripple control. Nevertheless, also this broadcast time information can be manipulated.

The method describes, how the time information, which is contained in time signals or time telegrams, can be verified by counting the periods of the modulated carrier frequency. The number of counted periods is converted to time information. Then the time interval, which is calculated by subsequent time information contained in time signals or time telegrams, is compared with the time interval, which is calculated by counting the periods of the modulated carrier. That means, the time difference, calculated by logical time data, is compared by time the interval determined by a physical process, which can not be manipulated. The physical time information can not be manipulated, otherwise the logical time data would be erroneous. The carrier signal must be a continuous carrier signal.

1.2. EP 3 001 592, Verifizierung von Zeitzeichen, granted 2017

Abstract: see **DE 10 2014 215 737**

1.3. US 10,165,530, Verification of Time Information transmitted by Time Signals or Time Telegrams, 2018

Abstract

The granted patents **DE 10 2014 215 737/EP 3 001 592** have been extended essentially. The US patent covers also satellite system based time services (like GPS, Galileo, GLONASS).

2. Patent family „e-Mobility“

2.1. DE 10 2011 079 870, Mobile Ladestation für Elektrofahrzeuge und Ladesystem, granted 2015

Abstract

Principle: not the electric vehicle comes to the charging station, which will be blocked as long as the vehicle is parked in front of the charging station, even after the end of the charging process, but the charging station comes to the vehicle.

Electric vehicles should not block parking space equipped with a charging station, for example in a parking lot/house, during the owner is on a (one day) trip, but only during the effective time of charging. Therefore the charging points are transported to the vehicles, so they can be charged as appointed. After the end of the charging process, the charging station may be brought to another vehicle to be charged, and so on. For this purpose power conductor lines are installed in the ground or in a certain height or at the ceiling and the mobile charging stations can be clipped at any place, where they are needed. Also, the data transmission for authentication, billing and management are performed via the power conductor line.

2.2. EP Mobile Ladestation für Elektrofahrzeuge und Ladesystem, grant is confirmed, under final publication process, 2017

Abstract:

Similar to **DE 10 2011 079 870**

2.3. DE 10 2009 026 936, Vorrichtung zum Anschluss an ein elektrisches Energieversorgungsnetz und Transportsystem, granted 2012

Abstract

This includes a method related to Power Line Communication (= data transmission via electric power lines).

Data to be transmitted via power lines are modulated by a carrier frequency. In the general case, data can only be transmitted, if there is also power transmitted, i.e. voltage exists between source and sink.

This patent describes a method, how data can be transmitted via electric power line without an applied voltage. Only a physical electric conductor has to be established between transmitter and receiver.

Motivation of this solution was the development of a simple and cost efficient charging station for electric vehicles. The control functions used in this concept are shared between the vehicle and a concentrator. The concentrator is able to control many charging points, for example in a parking lot or park house. If a vehicle is connected to the charging point, an identification and authentication protocol is performed by data exchange between charging point (information may come from the vehicle electronics) and the concentrator via power line communication. No power is transmitted during this phase. Power transmission and charging is only started after successful authentication and negotiation of billing, etc.

„Powerline Communication without Power" is the key word, which describes the method shortly the best.

3. Patent family „Localization"

3.1. DE 10 2012 223 385, Verfahren zu Bestimmung der räumlichen Position eines Objektes und elektronisches System, granted 2015

Abstract

A method is described, how an object can recognize its own position, and its position is not localized from outside.

This principle is motivated by the old navy method: a ship sees light houses, which use different light signals and intervals, which are unique in an area. By combination of the visible light signals and maps the ship is able to determine its position. Then the ship can transmit its position or the list of visible light houses or visible signals to a center, so the center can send navigation commands or other instructions to the ship.

In case of this patent the visible light signals sent by light houses are replaced by antennas, which emit continuously or periodically CDMA sequences, which are orthogonal to each other (cross correlation is equal 0). The receiver of the object recognizes by correlation, which CDMA signals it receives simultaneously. Based on this information and some knowledge about the identified antennas it is able to calculate its position and to navigate, or to send this information to another station and to wait for further instructions.

This method works for the two-dimensional as well as for the three-dimensional case. For example, robots can autonomously navigate in logistic centers, or be controlled from a control center based on the information received from the robot.

This method is very useful, if satellite based navigation systems like GPS, Galileo or Glonass can not be used, for example in halls, building, caves, or if the precision of these system is not sufficient in a small scale.

3.2. DE 10 2011 088 827, Roulettetisch und Brettspiel mit elektronischer Bestimmung der räumlichen Position eines Objektes, granted 2013

Abstract

This is special case of **DE 10 2012 223 385** (see above, this patent was granted before **DE 10 2012 223 385**).

This method solves the problem to determine exactly the position of a jeton on a Roulette tableau. The solution is, that each jeton recognizes itself its position and transmits the position to a center. The wireless power supply can happen by induction or capacity via the surface of the game table. The horizontal and vertical lines of the tableau are marked with antennas, which emit different, orthogonal CDMA sequences. The jetons recognize the different CMA sequences by correlation during a monitoring phase, and transmit the identifiers related to the recognized sequences to a center during a transmission phase. The center is able to calculate and to show the exact positions of the jetons. RFID-technology can be used for the transmission phase.

The system, the croupier and the players can see exactly the position of the set jetons. Discussions about the positions and movements of positions become obsolete.

The patent is extended also to games, which are played over social networks, when the positions of figures have to be recognizes without doubt.

3.3. US 8,737,515, Method for determining the spatial position of an object, electronic circuit and electronic system, granted 2014

Abstract

US-Version of DE 10 2011 088 827, 2013, Roulettetisch und Brettspiel mit elektronischer Bestimmung der räumlichen Position eines Objektes.

4. Patent family „Error Recognition and Correction“

4.1. DE 10 2008 050 797:, Verfahren zum Empfangen eines Datenblocks , granted 2010

Abstract

A method for increasing the correction rate of erroneously received data blocks.

A data block to be transmitted is split into two (or more) sub blocks, which are protected by (cryptographic or non-cryptographic) checksums, and then they are bitwise interleaved. The decoding and correction is achieved by using SISO (Soft Input Soft Output) method and feedback of reliability values of the sub blocks exploiting the avalanche effect of the checksum calculation. The correction rate can be increased by 1000 times.

4.2. US 8,196,015, Method for Transmitting and receiving a data block and a corresponding transmitter and Receiver, granted 2012

Abstract

US-Version of **DE 10 2008 050 797,** see above

4.3. DE 10 2008 055 139: Verfahren zum Empfangen eines Datenblocks, granted 2010

Abstract

An additional possibility to **DE 10 2008 040 797** to improve the correction capability of corrupted data blocks.

It concerns an alternative to the above mentioned patent, where the second sub block is a known, previously agreed sub block or a sub block generated on both sides by the same method, which is added for the encoding, but need not necessarily to be transmitted. Since the bits introduced at the receiving end before decoding are 100% correct, the others can be decoded much better using the feedback mechanisms of SISO decoding.

5. Patent family „Cryptography“

5.1. DE 10 2008 021 933, Verfahren zur Bestimmung einer Kette von Schlüsseln, Verfahren zur Übertragung einer Teilkette von Schlüsseln Computersystem und Chipkarte, granted 2011

Abstract

This method describes a cryptographic mechanism: group key management. It overlaps almost completely with the international standard ISO 11770-5 (Group Key Management).

Chains of keys are defined in such a way, that users, for example subscribers of a service, can calculate the next valid key(s) by themselves. This means, that no secret keys have to be transmitted via (insecure) network, which would cause a lot of practical problems. The authorized user, or subscriber receives at the beginning of his authorized relation, for example subscription ,a key, which he can use to calculate all of the following keys, but not the preceding keys, which were valid before the start of his authorized subscription. This key chain is the forward key chain. Nevertheless, the authorized user should not be able to calculate all following keys (forever), but only those, which become valid during his authorized period. There exists another key chain, which starts at the end of his authorization period. So he receives a second key, which will be valid at the end of his subscription period, and starting with this key he can calculate all keys of a key chain, which are valid before the end of his authorization period (backward key chain). Only the combination of the keys of partial forward and backward key chains enables the user to calculate the actual keys which are used by the provider between begin and end of his contract. He can calculate a predefined number of keys, which may be assigned to timely events. So, also a time period of authorization can be defined.