(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108011867 B
(45)授权公告日 2020.11.06

(21)申请号 201711113164.5

(22)申请日 2017.11.13

(65)同一申请的已公布的文献号
申请公布号 CN 108011867 A

(43)申请公布日 2018.05.08

(73)专利权人 北京全路通信信号研究设计院集团有限公司
地址 100070 北京市丰台区丰台科技园区汽车博物馆南里1号院中国通号大厦

(72)发明人 王一民 刘贞 左林 郭薇薇 黄雅倩

(74)专利代理机构 北京知联天下知识产权代理事务所(普通合伙) 11594
代理人 王冲 吴鑫

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 202711261 U,2013.01.30
CN 204066121 U,2014.12.31
US 2015032946 A1,2015.01.29
CN 104135469 A,2014.11.05
郑长宗等.铁路信号安全协议RSSP的研究.《铁道通信信号》.2011,

审查员 文娟

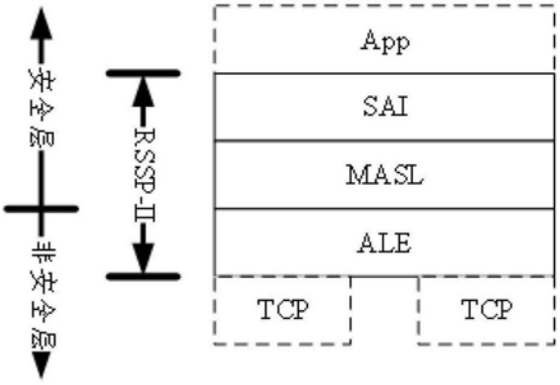
权利要求书2页 说明书3页 附图1页

(54)发明名称

一种铁路信号的安全加密方法及系统

(57)摘要

本发明提出了一种铁路信号安全加密方法和系统,其中所述方法包括:设置多个安全加密接口,其中所述多个安全加密接口分别对应不同的加密算法;从所述多个安全加密接口中选择一个安全加密接口;采用选择的安全加密接口所对应的加密算法对数据进行加密。本发明提出的铁路信号安全加密方法及系统充分考虑了不同的加密算法,可以根据不同类型设备和应用选择不同的加密算法,提高了通信的安全性。



CN 108011867 B

1.一种铁路信号安全加密方法,其特征在于,

设置多个安全加密接口,其中所述多个安全加密接口分别对应不同的加密算法;

从所述多个安全加密接口中选择一个安全加密接口;

采用选择的安全加密接口所对应的加密算法对数据进行加密;

所述加密接口设置在MASL层;

接收加密选择指令,根据加密选择指令选择一个安全加密接口;

多个加密接口包括第一加密接口、第二加密接口,分别与不同的加密硬件连接,多个加密硬件对应各自的一种加密算法;第一加密接口与第一加密硬件连接;第二加密接口与第二加密硬件连接;第一加密硬件执行第一种加密算法、第二加密硬件执行第二种加密算法;

第一加密接口对接第一个加密硬件,所述第一个加密硬件可以执行DES加密算法;第二个加密接口对接第二个加密硬件,所述第二个加密硬件可以执行SM4加密算法;

还包括双方协商确定加密算法的方式:

数据加密之前,数据发送方和数据接收方可以协商所能采用的加密算法,根据协商的加密算法选择通过相应的加密接口发送到相应的硬件加密硬件中;

数据接收方根据自身的设备类型或业务需求,认为接收的数据需要使用DES加密算法进行加密时,数据接收方向数据发送方发送加密选择指令,在该加密选择指令中指示数据发送方需要选用DES加密算法对数据进行加密;

数据发送方接收到数据接收方发送的加密选择指令后,根据所述加密选择指令确定使用DES加密算法对MASL层的数据进行加密;数据发送方加密选择模块将要加密的数据通过第一个加密接口发送到所述第一个加密硬件中,由于所述第一个加密硬件执行DES加密算法,发送到所述第一个加密硬件的数据以DES加密算法进行加密;

如果接收方认为接收的数据需要使用SM4对接收的数据加密时,数据接收方将向数据发送方发送加密选择指令以通知数据发送方选用SM4加密算法对发往所述数据接收方的数据进行加密;所述数据发送方接收到所述加密选择指令后,将要加密的数据通过第二个加密接口发送到所述第二个加密硬件中,由于所述第二个加密硬件执行SM4加密算法,所以发送到所述第二个加密硬件的数据以SM4加密算法进行加密。

2.一种铁路信号安全加密系统,其特征在于,

所述铁路信号安全加密系统包括多个安全加密接口和多个加密硬件,其中,

所述多个安全加密接口分别连接不同加密硬件;

所述铁路信号安全加密系统还包括加密选择单元,所述加密选择单元根据加密选择指令从所述多个安全加密接口中选择一个安全加密接口;

所述多个加密硬件分别执行一种安全加密算法;

所述安全加密接口从MASL从接收需要加密的数据;

多个加密接口包括第一加密接口、第二加密接口,分别与不同的加密硬件连接,多个加密硬件对应各自的一种加密算法;第一加密接口与第一加密硬件连接;第二加密接口与第二加密硬件连接;第一加密硬件执行第一种加密算法、第二加密硬件执行第二种加密算法;

第一加密接口对接第一个加密硬件,所述第一个加密硬件可以执行DES加密算法;第二个加密接口对接第二个加密硬件,所述第二个加密硬件可以执行SM4加密算法;

还包括双方协商确定加密算法的方式:

数据加密之前，数据发送方和数据接收方可以协商所能采用的加密算法，根据协商的加密算法选择通过相应的加密接口发送到相应的硬件加密硬件中；

数据接收方根据自身的设备类型或业务需求，认为接收的数据需要使用DES加密算法进行加密时，数据接收方向数据发送方发送加密选择指令，在该加密选择指令中指示数据发送方需要选用DES加密算法对数据进行加密；

数据发送方接收到数据接收方发送的加密选择指令后，根据所述加密选择指令确定使用DES加密算法对MASL层的数据进行加密；数据发送方加密选择模块将要加密的数据通过第一个加密接口发送到所述第一个加密硬件中，由于所述第一个加密硬件执行DES加密算法，发送到所述第一个加密硬件的数据以DES加密算法进行加密；

如果接收方认为接收的数据需要使用SM4对接收的数据加密时，数据接收方将向数据发送方发送加密选择指令以通知数据发送方选用SM4加密算法对发往所述数据接收方的数据进行加密；所述数据发送方接收到所述加密选择指令后，将要加密的数据通过第二个加密接口发送到所述第二个加密硬件中，由于所述第二个加密硬件执行SM4加密算法，所以发送到所述第二个加密硬件的数据以SM4加密算法进行加密。

一种铁路信号的安全加密方法及系统

技术领域

[0001] 本发明属于加密技术领域,特别涉及一种铁路信号安全加密方法及系统。

背景技术

[0002] RSSP-II(铁路信号安全通信协议II)安全通信协议是一种铁路信号设备间通信采用的协议,其安全完整性等级可达SIL4(安全完整性等级)。目前,已有的RSSP-II协议都是基于DES(美国数据加密标准)和修改后的MAC算法。DES算法是在美国NSA(国家安全局)资助下由IBM公司开发的密码算法,其初衷是为政府非机密的敏感信息提供较强的加密保护。它是美国政府担保的第一种加密算法,并在1977年被正式作为美国联邦信息处理标准。DES主要提供非军事性质的联邦政府机构和私营部门使用,并迅速成为名声最大,使用最广的商用密码算法。

[0003] 2006年我国公布了无限局域网产品使用的SM4(国家商业秘密算法)密码算法。这是我国第一次公布自己的商用密码算法。但是目前为止,RSSP-II安全通信协议中还没有针对SM4算法提出解决方案。

发明内容

[0004] 为了解决上述技术问题,本发明提出了一种铁路信号安全加密方法及系统。

[0005] 本发明提出了一种铁路信号安全加密方法,其特征在于,

[0006] 设置多个安全加密接口,其中所述多个安全加密接口分别对应不同的加密算法;

[0007] 从所述多个安全加密接口中选择一个安全加密接口;

[0008] 采用选择的安全加密接口所对应的加密算法对数据进行加密。

[0009] 进一步地,所述加密算法包括DES加密算法、SM4加密算法。

[0010] 进一步地,所述加密接口设置在MASL层。

[0011] 进一步地,接收加密选择指令,根据加密选择指令选择一个安全加密接口。

[0012] 本发明还提供了一种铁路信号安全加密系统,其特征在于,

[0013] 所述铁路信号安全加密系统包括多个安全加密接口和多个加密硬件,其中

[0014] 所述多个安全加密接口分别连接不同加密硬件。

[0015] 进一步地,所述铁路信号安全加密系统还包括加密选择单元,所述加密选择单元根据加密选择指令从所述多个安全加密接口中选择一个安全加密接口。

[0016] 进一步地,所述多个加密硬件分别执行一种安全加密算法。

[0017] 进一步地,所述安全加密算法包括DES加密算法、SM4加密算法。

[0018] 进一步地,所述安全加密接口从MASL从接收需要加密的数据。

[0019] 本发明提出的铁路信号安全加密方法及系统充分考虑了不同的加密算法,可以根据不同类型设备和应用选择不同的加密算法,提高了通信的安全性。

附图说明

[0020] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0021] 图1示出了根据本发明实施例的安全通信加密协议栈核心逻辑分层示意图。

具体实施方式

[0022] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地说明，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0023] 在RSSP-II安全通信协议中提供多个加密接口，不是一般性例如可以设置第一加密接口、第二加密接口。但是本发明并不限于第一加密接口、第二加密接口这两个加密接口，还可以设置多个加密接口。本发明的多个加密接口可以设置在RSSP-II协议栈的相应层中。如图1所示出的本发明实施例的安全加密协议栈示意图，协议栈包括TCP层(传输控制协议层)、ALE层(适配机冗余管理层)、MASL层(消息鉴定安全层)、SAI层(安全应用层)以及APP层(应用层)。其中SAI层、MASL层和ALE层为RSSP-II安全通信协议层，MASL层、SAI层和APP层属于安全层，而ALE层、TCP层属于非安全层。本发明中将所述加密接口的接口功能设置在所述MASL层中，可以将MASL层的数据通过相应的加密接口发送给相应的硬件加密模块执行加密。

[0024] 所述多个加密接口分别与不同的加密硬件连接，多个加密硬件对应的各自的一种加密算法。不是一般性，例如，第一加密接口与第一加密硬件连接、第二加密接口与第二加密硬件连接，第一加密硬件执行第一种加密算法、第二加密硬件执行第二种加密算法。

[0025] 第一加密接口对接第一个加密硬件，所述第一个加密硬件可以执行DES(美国数据加密标准)加密算法；第二个加密接口对接第二个加密硬件，所述第二个加密硬件可以执行SM4(国家商业秘密算法)加密算法。

[0026] 双方协商确定加密算法的方式：

[0027] 数据加密之前，数据发送方和数据接收方可以协商所能采用的加密算法，根据协商的加密算法选择通过相应的加密接口发送到相应的硬件加密硬件中。

[0028] 不是一般性，数据接收方根据自身的设备类型或业务需求，认为接收的数据需要使用DES加密算法进行加密时，数据接收方向数据发送方发送加密选择指令，在该加密选择指令中指示数据发送方需要选用DES加密算法对数据进行加密。

[0029] 数据发送方接收到数据接收方发送的加密选择指令后，根据所述加密选择指令确定使用DES加密算法对MASL层的数据进行加密。数据发送方的相关模块，例如加密选择模块将要加密的数据通过第一个加密接口发送到所述第一个加密硬件中，由于所述第一个加密硬件执行DES加密算法，所以发送到所述第一个加密硬件的数据以DES加密算法进行加密。

[0030] 类似地，如果接收方认为接收的数据需要使用SM4对接收的数据加密时，数据接收方将向数据发送方发送加密选择指令以通知数据发送方选用SM4加密算法对发往所述数据

接收方的数据进行加密。所述数据发送方接收到所述加密选择指令后，将要加密的数据通过第二个加密接口发送到所述第二个加密硬件中，由于所述第二个加密硬件执行SM4加密算法，所以发送到所述第二个加密硬件的数据以SM4加密算法进行加密。

[0031] 非协商确定加密算法的方式：

[0032] 数据的发送方也可以根据整个数据系统的需要(例如对于安全性的要求、各个国家或地区安全标准的要求等)自行确定使用的加密算法。

[0033] 不是一般性，例如系统要求必须使用SM4加密算法对数据进行加密时，系统向数据发送方的发送加密选择指令。数据发送方的相关模块，例如加密选择模块获得该数据加密选择指令后，根据数据加密选择指令确定相应的加密算法，例如选择DES加密算法还是选择SM4加密算法。然后与“双方协商确定加密算法的方式”的处理方式相同，通过相应的加密接口使用相应的硬件加密单元对数据进行加密。

[0034] 最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制。本发明中所指出的连接并不必然意味是一种直接的电气连接，也含有了间接连接的方式。本发明中所指出的第一、第二等并不必然表示一种前后顺序，可以表示不同的硬件、模块等。

[0035] 尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

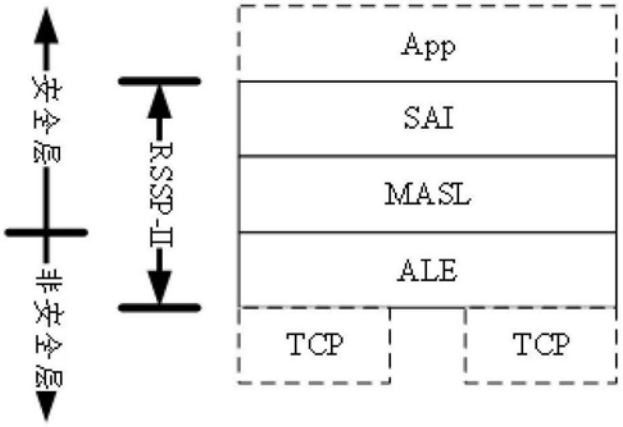


图1