(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111865562 A
(43)申请公布日 2020.10.30

(21)申请号 202010715957.X

(22)申请日 2020.07.23

(71)申请人 积成电子股份有限公司
地址 250104 山东省济南市科航路1677号

(72)发明人 张汉伟 阴法强 常栋梁 李连强

(74)专利代理机构 北京久维律师事务所 11582
代理人 邢江峰

(51)Int.Cl.
H04L 9/06(2006.01)
H04L 9/32(2006.01)
H04L 29/08(2006.01)
G16Y 10/35(2020.01)
G16Y 30/10(2020.01)

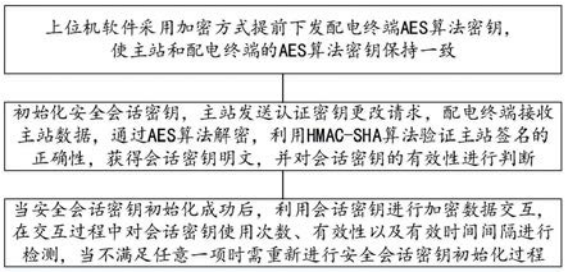
权利要求书1页 说明书4页 附图4页

(54)发明名称

一种配电终端DNP规约中基于AES和HMAC-SHA的加密方法及系统

(57)摘要

本发明提供了一种配电终端DNP规约中基于AES和HMAC-SHA的加密方法及系统，本发明通过引入AES算法对密钥加密，密钥不以明文的形式展示给使用者和攻击者，防止攻击者窃取AES算法密钥，并引入HMAC-SHA算法加密验签，采用最为严格的HMAC-SHA-256方法，进一步提高通信过程安全，另外在通信过程中，增加会话密钥使用次数、有效时间间隔限制及会话密钥有效性的判断，实现会话密钥定期有效更新，从而为提高配电自动化终端的防护水平，制定了一套有效的安全机制方案，可有效提高通信数据的安全性。



CN 111865562 A

1.一种配电终端DNP规约中基于AES和HMAC-SHA的加密方法，其特征在于，所述方法包括以下操作：

上位机软件采用加密方式提前下发配电终端AES算法密钥，使主站和配电终端的AES算法密钥保持一致；

初始化安全会话密钥，主站发送认证密钥更改请求，配电终端接收主站数据，通过AES算法解密，利用HMAC-SHA算法验证主站签名的正确性，获得会话密钥明文，并对会话密钥的有效性进行判断；

当安全会话密钥初始化成功后，利用会话密钥进行加密数据交互，在交互过程中对会话密钥使用次数、有效性以及有效时间间隔进行检测，当不满足任意一项时需重新进行安全会话密钥初始化过程。

2.根据权利要求1所述的一种配电终端DNP规约中基于AES和HMAC-SHA的加密方法，其特征在于，所述对会话密钥的有效性进行判断具体为：

判断接收到的会话密钥是否和之前相同，若不相同，则发送认证会话正确帧，否则发送认证会话错误帧。

3.根据权利要求1所述的一种配电终端DNP规约中基于AES和HMAC-SHA的加密方法，其特征在于，所述加密数据包括遥控数据、直控数据、校时数据、禁止主动上送数据、允许主动上送数据以及清除重启标志位。

4.根据权利要求1所述的一种配电终端DNP规约中基于AES和HMAC-SHA的加密方法，其特征在于，所述会话密钥使用次数以及有效时间间隔需要提前设置，并保持主站和终端的设置一致。

5.根据权利要求1所述的一种配电终端DNP规约中基于AES和HMAC-SHA的加密方法，其特征在于，所述会话密钥使用次数、有效性以及有效时间间隔在满足条件时，接收主站加密数据帧，通过会话密钥以及HMAC-SHA算法计算出HAMC，计算HMAC是否与接收HMAC一致，当一致时执行命令帧相应的操作。

6.一种配电终端DNP规约中基于AES和HMAC-SHA的加密系统，其特征在于，所述系统包括：

AES密钥下发模块，用于上位机软件采用加密方式提前下发配电终端AES算法密钥，使主站和配电终端的AES算法密钥保持一致；

会话密钥初始化模块，用于初始化安全会话密钥，主站发送认证密钥更改请求，配电终端接收主站数据，通过AES算法解密，利用HMAC-SHA算法验证主站签名的正确性，获得会话密钥明文，并对会话密钥的有效性进行判断；

加密数据交互模块，用于当安全会话密钥初始化成功后，利用会话密钥进行加密数据交互，在交互过程中对会话密钥使用次数、有效性以及有效时间间隔进行检测，当不满足任意一项时需重新进行安全会话密钥初始化过程。

7.根据权利要求6所述的一种配电终端DNP规约中基于AES和HMAC-SHA的加密系统，其特征在于，所述加密数据包括遥控数据、直控数据、校时数据、禁止主动上送数据、允许主动上送数据以及清除重启标志位。

一种配电终端DNP规约中基于AES和HMAC-SHA的加密方法及系统

技术领域

[0001] 本发明涉及配电终端数据加密技术领域,特别是涉及一种配电终端DNP规约中基于AES和HMAC-SHA的加密方法及系统。

背景技术

[0002] DNP3.0规约(Distributed Network Protocol,在TC57协议基础上制定的通信规约)是一种分布式协议,适用于要求高度安全、中等速率、中等吞吐量的数据通信领域,在配电网终端领域,DNP3.0通信协议被广泛应用于数据通信,但是该协议在网络应用环境和实际电力系统使用过程中,由于数据格式都是公开的,DNP3.0协议的数据报文在传输过程中,容易被非法入侵者截取和监听,然后对报文修改来达到对终端进行攻击的目的,大大降低了通信数据的安全性,对配电系统造成不可预估的损失。

发明内容

[0003] 本发明的目的是提供一种配电终端DNP规约中基于AES和HMAC-SHA的加密方法及系统,旨在解决现有技术中数据报文在传输中安全性低问题,实现会话密钥不以明文的形式展示给使用者和攻击者,提高数据通信安全性。

[0004] 为达到上述技术目的,本发明提供了一种配电终端DNP规约中基于AES和HMAC-SHA的加密方法,所述方法包括以下操作:

[0005] 上位机软件采用加密方式提前下发配电终端AES算法密钥,使主站和配电终端的AES算法密钥保持一致;

[0006] 初始化安全会话密钥,主站发送认证密钥更改请求,配电终端接收主站数据,通过AES算法解密,利用HMAC-SHA算法验证主站签名的正确性,获得会话密钥明文,并对会话密钥的有效性进行判断;

[0007] 当安全会话密钥初始化成功后,利用会话密钥进行加密数据交互,在交互过程中对会话密钥使用次数、有效性以及有效时间间隔进行检测,当不满足任意一项时需重新进行安全会话密钥初始化过程。

[0008] 优选地,所述对会话密钥的有效性进行判断具体为:

[0009] 判断接收到的会话密钥是否和之前相同,若不相同,则发送认证会话正确帧,否则发送认证会话错误帧。

[0010] 优选地,所述加密数据包括遥控数据、直控数据、校时数据、禁止主动上送数据、允许主动上送数据以及清除重启标志位。

[0011] 优选地,所述会话密钥使用次数以及有效时间间隔需要提前设置,并保持主站和终端的设置一致。

[0012] 优选地,所述会话密钥使用次数、有效性以及有效时间间隔在满足条件时,接收主站加密数据帧,通过会话密钥以及HMAC-SHA算法计算出HAMC,计算HMAC是否与接收HMAC一

致，当一致时执行命令帧相应的操作。

[0013] 本发明还提供了一种配电终端DNP规约中基于AES和HMAC-SHA的加密系统，所述系统包括：

[0014] AES密钥下发模块，用于上位机软件采用加密方式提前下发配电终端AES算法密钥，使主站和配电终端的AES算法密钥保持一致；

[0015] 会话密钥初始化模块，用于初始化安全会话密钥，主站发送认证密钥更改请求，配电终端接收主站数据，通过AES算法解密，利用HMAC-SHA算法验证主站签名的正确性，获得会话密钥明文，并对会话密钥的有效性进行判断；

[0016] 加密数据交互模块，用于当安全会话密钥初始化成功后，利用会话密钥进行加密数据交互，在交互过程中对会话密钥使用次数、有效性以及有效时间间隔进行检测，当不满足任意一项时需重新进行安全会话密钥初始化过程。

[0017] 优选地，所述加密数据包括遥控数据、直控数据、校时数据、禁止主动上送数据、允许主动上送数据以及清除重启标志位。

[0018] 发明内容中提供的效果仅仅是实施例的效果，而不是发明所有的全部效果，上述技术方案中的一个技术方案具有如下优点或有益效果：

[0019] 与现有技术相比，本发明通过引入AES算法对密钥加密，密钥不以明文的形式展示给使用者和攻击者，防止攻击者窃取AES算法密钥，并引入HMAC-SHA算法加密验签，采用最为严格的HMAC-SHA-256方法，进一步提高通信过程安全，另外在通信过程中，增加会话密钥使用次数、有效时间间隔限制及会话密钥有效性的判断，实现会话密钥定期有效更新，从而为提高配电自动化终端的防护水平，制定了一套有效的安全机制方案，可有效提高通信数据的安全性。

附图说明

[0020] 图1为本发明实施例中所提供的一种配电终端DNP规约中基于AES和HMAC-SHA的加密方法流程图；

[0021] 图2为本发明实施例中所提供的密钥初始化流程图；

[0022] 图3为本发明实施例中所提供的加密数据交互流程图；

[0023] 图4为本发明实施例中所提供的一种配电终端DNP规约中基于AES和HMAC-SHA的加密系统框图。

具体实施方式

[0024] 为了能清楚说明本方案的技术特点，下面通过具体实施方式，并结合其附图，对本发明进行详细阐述。下文的公开提供了许多不同的实施例或例子用来实现本发明的不同结构。为了简化本发明的公开，下文中对特定例子的部件和设置进行描述。此外，本发明可以在不同例子中重复参考数字和/或字母。这种重复是为了简化和清楚的目的，其本身不指示所讨论各种实施例和/或设置之间的关系。应当注意，在附图中所图示的部件不一定按比例绘制。本发明省略了对公知组件和处理技术及工艺的描述以避免不必要地限制本发明。

[0025] 下面结合附图对本发明实施例所提供的一种配电终端DNP规约中基于AES和HMAC-SHA的加密方法及系统进行详细说明。

[0026] 如图1所示，本发明实施例公开了一种配电终端DNP规约中基于AES和HMAC-SHA的加密方法，所述方法包括以下操作：

[0027] 上位机软件采用加密方式提前下发配电终端AES算法密钥，使主站和配电终端的AES算法密钥保持一致；

[0028] 初始化安全会话密钥，主站发送认证密钥更改请求，配电终端接收主站数据，通过AES算法解密，利用HMAC-SHA算法验证主站签名的正确性，获得会话密钥明文，并对会话密钥的有效性进行判断；

[0029] 当安全会话密钥初始化成功后，利用会话密钥进行加密数据交互，在交互过程中对会话密钥使用次数、有效性以及有效时间间隔进行检测，当不满足任意一项时需重新进行安全会话密钥初始化过程。

[0030] AES(Advanced Encryption Standard，高级加密标准)算法密钥需要通过上位机软件提前下发给配电终端，该密钥需要主站和配电终端保持一致。所述AES算法密钥采用加密方式，不采用明文方式展示给使用者和攻击者，有效防止攻击者窃取AES密钥。

[0031] 对安全会话密钥进行初始化。主站发送认证会话密钥状态请求，配电终端传输具有密钥状态的认证，会话密钥状态响应表示为“未初始化”。主站发送认证会话密钥更改请求，配电终端接收到主站数据后，用双方协定好的AES算法的密钥对接收到的数据采用AES算法解密，并采用HMAC-SHA算法(Hash-based Message Authentication Code，哈希消息认证码)验证主站签名的正确性，若认证正确，取出主站发送的会话密钥，对会话密钥的有效性进行判断，目前采用的方式是判断接收到的会话密钥是否和之前相同，若不相同，则发送认证会话正确帧，否则发送认证会话错误帧，以后加密数据无法正常执行，例如遥控指令无法正常下发。

[0032] 如图2所示，配电终端通过AES算法对密钥解码，取出AES密钥，并接受主站的会话初始化帧。取出解密后的明文，并判断明文是否完整和正确，并对会话密钥有效性进行判断，取出会话密钥，置会话有效标志。

[0033] 认证会话密钥成功后，使用会话密钥进行加密数据的交互。所述加密数据包括遥控数据、直控数据、校时数据、禁止主动上送数据、允许主动上送数据以及清除重启标志位等。

[0034] 对会话密钥使用次数、有效间隔进行设置以及对有效性进行检测。会话密钥使用次数以及有效间隔需要提前设置，保证主站和终端的设置一致，若该会话密钥超过最大次数或超过最大有效间隔等，加密数据都无法进行正常交互，需要重新进行安全会话密钥的初始化过程，满足要求后，获取新的会话密钥。如图3所示，配电终端接收主站发送的写命令帧，例如遥控、校时等，依次判断会话密钥是否有效、是否超过最大次数以及是否超过有效时间间隔，如果是则发送错误码，如果否则接收主站加密数据帧，通过会话密钥以及HMAC-SHA算法计算出HAMC，计算HMAC是否与接收HMAC一致，当一致时执行命令帧相应的操作。

[0035] 本发明实施例通过引入AES算法对密钥加密，密钥不以明文的形式展示给使用者和攻击者，防止攻击者窃取AES算法密钥，并引入HMAC-SHA算法加密验签，采用最为严格的HMAC-SHA-256方法，进一步提高通信过程安全，另外在通信过程中，增加会话密钥使用次数、有效时间间隔限制及会话密钥有效性的判断，实现会话密钥定期有效更新，从而为提高配电自动化终端的防护水平，制定了一套有效的安全机制方案，可有效提高通信数据的安

全性。

[0036] 如图4所示，本发明实施例还公开了一种配电终端DNP规约中基于AES和HMAC-SHA的加密系统，所述系统包括：

[0037] AES密钥下发模块，用于上位机软件采用加密方式提前下发配电终端AES算法密钥，使主站和配电终端的AES算法密钥保持一致；

[0038] 会话密钥初始化模块，用于初始化安全会话密钥，主站发送认证密钥更改请求，配电终端接收主站数据，通过AES算法解密，利用HMAC-SHA算法验证主站签名的正确性，获得会话密钥明文，并对会话密钥的有效性进行判断；

[0039] 加密数据交互模块，用于当安全会话密钥初始化成功后，利用会话密钥进行加密数据交互，在交互过程中对会话密钥使用次数、有效性以及有效时间间隔进行检测，当不满足任意一项时需重新进行安全会话密钥初始化过程。

[0040] AES算法密钥需要通过上位机软件提前下发给配电终端，该密钥需要主站和配电终端保持一致。所述AES算法密钥采用加密方式，不采用明文方式展示给使用者和攻击者，有效防止攻击者窃取AES密钥。

[0041] 对安全会话密钥进行初始化。主站发送认证会话密钥状态请求，配电终端传输具有密钥状态的认证，会话密钥状态响应表示为“未初始化”。主站发送认证会话密钥更改请求，配电终端接收到主站数据后，用双方协定好的AES算法的密钥对接收到的数据采用AES算法解密，并采用HMAC-SHA算法验证主站签名的正确性，若认证正确，取出主站发送的会话密钥，对会话密钥的有效性进行判断，目前采用的方式是判断接收到的会话密钥是否和之前相同，若不相同，则发送认证会话正确帧，否则发送认证会话错误帧，以后加密数据无法正常执行，例如遥控指令无法正常下发。

[0042] 配电终端通过AES算法对密钥解码，取出AES密钥，并接受主站的会话初始化帧。取出解密后的明文，并判断明文是否完整和正确，并对会话密钥有效性进行判断，取出会话密钥，置会话有效标志。

[0043] 认证会话密钥成功后，使用会话密钥进行加密数据的交互。所述加密数据包括遥控数据、直控数据、校时数据、禁止主动上送数据、允许主动上送数据以及清除重启标志位等。

[0044] 对会话密钥使用次数、有效间隔进行设置以及对有效性进行检测。会话密钥使用次数以及有效间隔需要提前设置，保证主站和终端的设置一致，若该会话密钥超过最大次数或超过最大有效间隔等，加密数据都无法进行正常交互，需要重新进行安全会话密钥的初始化过程，满足要求后，获取新的会话密钥。配电终端接收主站发送的写命令帧，例如遥控、校时等，依次判断会话密钥是否有效、是否超过最大次数以及是否超过有效时间间隔，如果是则发送错误码，如果否则接收主站加密数据帧，通过会话密钥以及HMAC-SHA算法计算出HAMC，计算HMAC是否与接收HMAC一致，当一致时执行命令帧相应的操作。

[0045] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

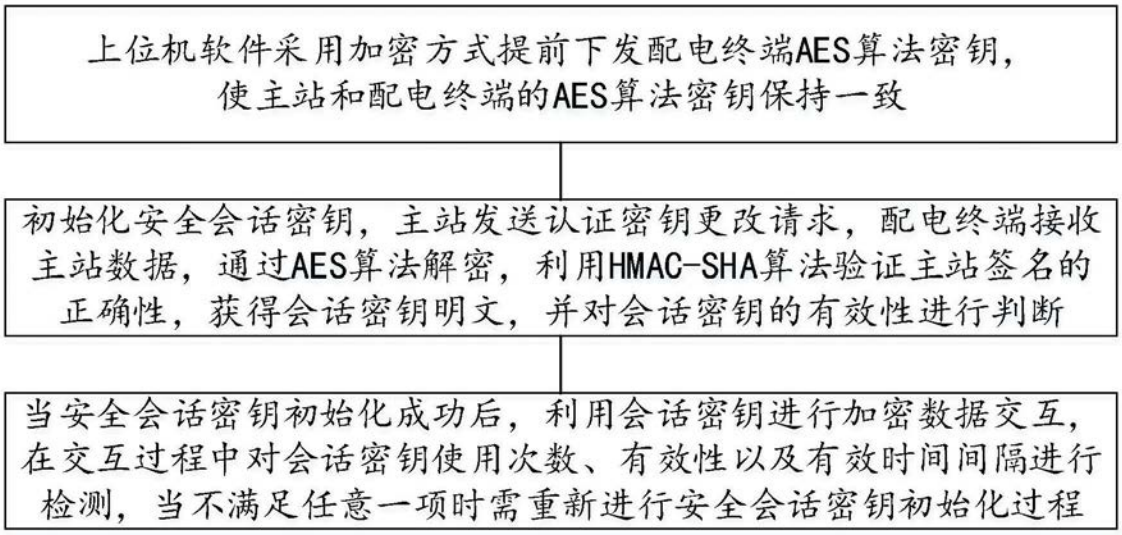

上位机软件采用加密方式提前下发配电终端AES算法密钥，
使主站和配电终端的AES算法密钥保持一致
初始化安全会话密钥，主站发送认证密钥更改请求，配电终端接收
主站数据，通过AES算法解密，利用HMAC-SHA算法验证主站签名的
正确性，获得会话密钥明文，并对会话密钥的有效性进行判断
当安全会话密钥初始化成功后，利用会话密钥进行加密数据交互，
在交互过程中对会话密钥使用次数、有效性以及有效时间间隔进行
检测，当不满足任意一项时需重新进行安全会话密钥初始化过程

图1

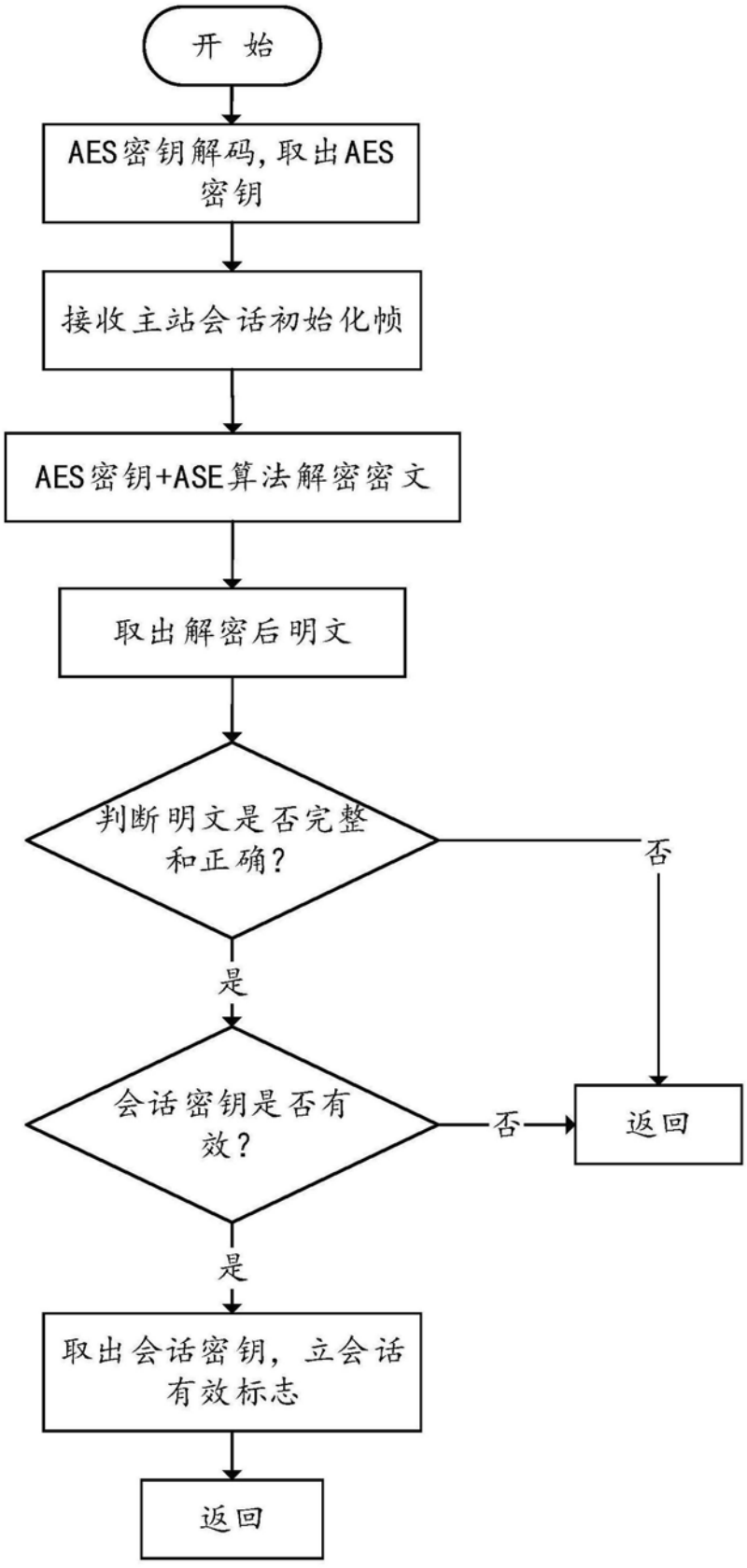

开 始
AES密钥解码,取出AES密钥
接收主站会话初始化帧
AES密钥+ASE算法解密密文
取出解密后明文
判断明文是否完整和正确?
否
是
会话密钥是否有效?
否
返回
是
取出会话密钥，立会话有效标志
返回

图2

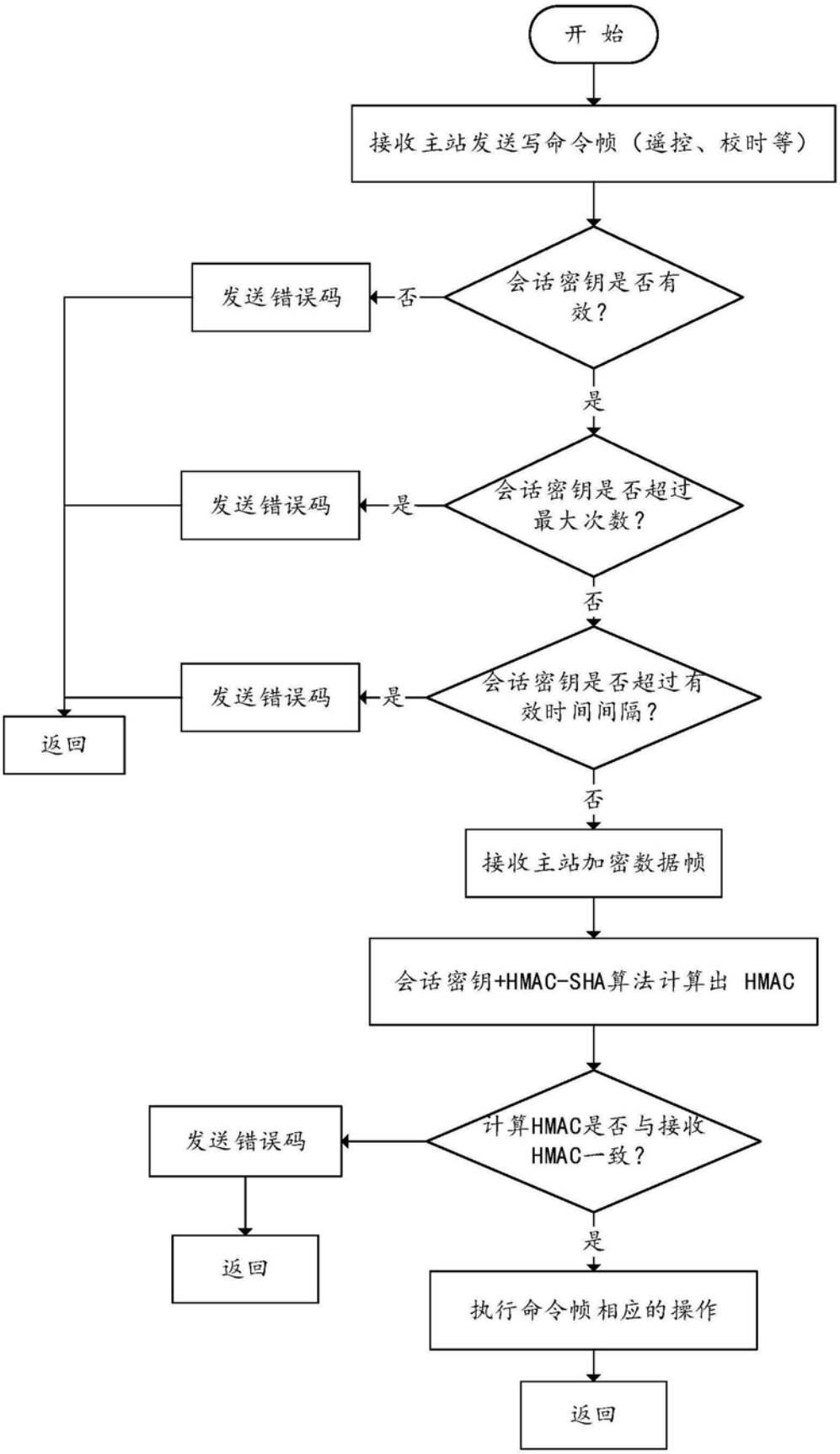

开 始
接收主站发送写命令帧（遥控、校时等）
会话密钥是否有效？
否
发送错误码
是
会话密钥是否超过最大次数？
是
发送错误码
否
会话密钥是否超过有效时间间隔？
是
发送错误码
返回
否
接收主站加密数据帧
会话密钥+HMAC-SHA算法计算出 HMAC
计算HMAC是否与接收HMAC一致？
发送错误码
返回
是
执行命令帧相应的操作
返回

图3

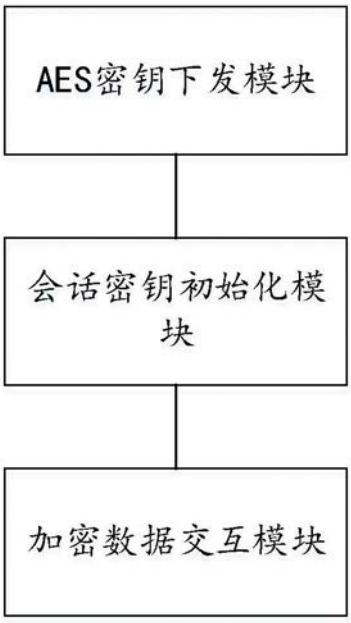


图4