(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 101010906 B
(45)授权公告日 2010.05.12

(21)申请号 200580029825.5
(22)申请日 2005.09.06
(30)优先权数据
259213/2004 2004.09.07 JP
(85)PCT申请进入国家阶段日
2007.03.06
(86)PCT申请的申请数据
PCT/JP2005/016335 2005.09.06
(87)PCT申请的公布数据
WO2006/028094 JA 2006.03.16
(73)专利权人 松下电器产业株式会社
地址 日本大阪府
(72)发明人 绫木靖 饭塚裕之 臼木直司
(74)专利代理机构 北京德琦知识产权代理有限公司 11018
代理人 陆弋 宋志强
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 12/28(2006.01)
G09C 1/00(2006.01)
H04L 12/56(2006.01)
(56)对比文件
JP 2004180010 A,2004.06.24, 全文.
CN 1365474 A,2002.08.21, 全文.
JP 2004194295 A,2004.07.08, 全文.
审查员 张博

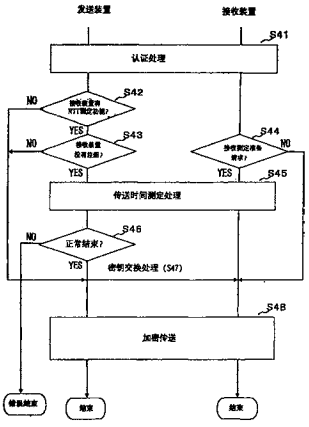
权利要求书 5 页 说明书 11 页 附图 11 页

(54)发明名称

通信装置、通信系统及通信方法

(57)摘要

现有的数据发送接收系统，存在以下问题：测定时验证处理时间被加入至传送时间而不能正确地测定，对传送时间测定处理的必要的认证处理需要采用另外的方法，会执行无用的密钥交换处理。发送装置，(a)与请求发送内容数据的请求方之间共享认证信息，(b)将使用认证信息生成的测定请求，向所述请求方发送，(c)将使用请求方共享的认证信息生成的测定应答，作为对测定请求的应答从请求方接收，(d)将从发送测定请求到接收测定应答的时间，作为往返延迟时间测定，(e)发送测定请求前，将测定准备请求，向请求方发送，用于请求为生成测定应答需要的预先准备，(f)往返延迟时间测定后，往返延迟时间在标准值以下，验证测定应答为正确，并且验证请求方中测定请求正确的情况下，判断请求方作为内容数据的发送对象为合格的装置。



CN 101010906 B

1. 对于内容数据的发送的请求进行应答的通信装置，其特征在于，包括：

认证部件，用于与请求所述内容数据的发送的请求方之间共享认证信息；

测定请求发送部件，用于向所述请求方发送使用所述认证信息而生成的测定请求；

测定应答接收部件，用于从所述请求方接收使用所述请求方共享的认证信息而生成的测定应答，作为对于所述测定请求的应答；

往返延迟时间测定部件，用于测定从发送所述测定请求到接收所述测定应答的时间，作为往返延迟时间；

判定部件，用于在所述往返延迟时间测定后，所述往返延迟时间在标准值以下，验证所述测定应答为正确，并且确认已验证所述请求方中所述测定请求为正确的情况下，判定所述请求方作为所述内容数据的发送对象为合格的装置。

2. 根据权利要求 1 所述的通信装置，其特征在于，所述通信装置进一步包括：

测定准备请求发送部件，在发送所述测定请求之前，向所述请求方发送测定准备请求，该测定准备请求用于请求为生成所述测定应答所需的预先准备。

3. 根据权利要求 2 所述的通信装置，其特征在于：

所述判定部件，当使用所述认证信息生成的第一验证信息与在所述请求方中使用所述认证信息生成的第二验证信息一致的情况下，验证所述测定应答为正确。

4. 根据权利要求 3 所述的通信装置，其特征在于：

所述认证信息，包括规定所述请求方是否具有往返延迟时间测定的相应功能的标志与关于所述标志的证明信息；

所述通信装置，更进一步包括测定功能判断部件，用于基于所述标志，判断所述请求方是否具有往返延迟时间测定的相应功能；

所述测定准备请求发送部件，在具有所述功能的情况下，发送所述测定准备请求；在不具有所述功能的情况下，不发送所述测定准备请求。

5. 根据权利要求 3 所述的通信装置，其特征在于，

所述通信装置，更进一步包括：

注册部件，用于在所述请求方作为所述内容数据的发送对象为合格的装置的情况下，所述请求方将识别出的装置识别信息注册到一览表；以及

注册确认部件，用于在将所述测定准备请求向所述请求方发送之前，确认所述装置识别信息在所述一览表是否已注册；并且

所述测定准备请求发送部件，已在所述一览表注册的情况下，不发送所述测定准备请求，当未在一览表注册的情况下，发送所述测定准备请求。

6. 根据权利要求 5 所述的通信装置，其特征在于，

所述通信装置，更进一步包括注册取消部件，用于如果所述装置识别信息中设定的注册有效时间经过后，取消所述装置识别信息的注册。

7. 根据权利要求 3 所述的通信装置，其特征在于，

作为所述预先准备，所述请求方，从接收所述测定准备请求到接收到所述测定请求之间，使用与发送所述内容数据的通信装置之间共享的认证信息，生成请求方信息，将所述请求方信息分割而生成第一请求方部分信息和第二请求方部分信息的情况下，

所述通信装置，更进一步包括，

测定准备部件，用于使用所述认证信息，生成与所述请求方信息一致的请求对象信息，将所述请求对象信息分割而生成第一请求对象部分信息和第二请求对象部分信息；以及

请求方验证部件，用于在所述第二请求方部分信息与所述第一请求对象部分信息一致的情况下，判断所述测定应答的发送方是真正的请求方；并且

所述测定应答接收部件，作为所述测定应答从所述请求方接收包含所述第二请求方部分信息的应答。

8. 根据权利要求 7 所述的通信装置，其特征在于，

所述请求方，当所述第二请求对象部分信息和所述第一请求方部分信息一致的情况下，判断所述测定请求的发送方是真正的请求对象，生成所述第二验证信息的情况下，

所述验证部件，包括：

验证请求发送部件，用于将请求验证所述测定请求的发送方是否为真正的请求对象的验证请求，向所述请求方发送；以及

验证应答接收部件，用于将包含所述第二验证信息的验证应答，作为对于所述验证请求的应答，从所述请求方接收；并且

所述测定请求发送部件，

将包含所述第二请求对象部分信息的请求，作为所述测定请求向所述请求方发送。

9. 根据权利要求 6 所述的通信装置，其特征在于，

所述通信装置，更进一步包括：

测定开始判定部件，用于基于到所述装置识别信息的注册取消为止的剩余时间，判定所述往返延迟时间的测定是否开始；

测定开始请求发送部件，用于在所述剩余时间在预定的时间以下的情况下，将测定开始请求向所述请求方发送；以及

测定开始应答接收部件，用于作为对于所述测定开始请求的应答从所述请求方接收测定开始应答；并且

从所述请求方接收所述测定开始应答之后，所述认证部件与所述请求方之间共享认证信息。

10. 根据权利要求 1 所述的通信装置，其特征在于，

所述通信装置，更进一步，包括：

测定开始判定部件，用于判定所述往返延迟时间的测定是否开始；

测定开始请求发送部件，用于在开始所述往返延迟时间测定的情况下，将通知所述往返延迟时间的测定开始的测定开始请求，向所述请求方发送；以及

测定开始应答接收部件，用于作为对于所述测定开始请求的应答从所述请求方接收测定开始应答；并且

从所述请求方接收所述测定开始应答之后，所述认证部件与所述请求方之间共享认证信息。

11. 根据权利要求 1 所述的通信装置，其特征在于，

所述通信装置，更进一步，包括：

测定开始请求接收部件，用于从所述请求方接收请求开始所述往返延迟时间测定的测定开始请求；以及

测定开始应答发送部件，用于作为对于所述测定开始请求的应答向所述请求方发送测定开始应答；并且

将所述测定开始应答向所述请求方发送之后，所述认证部件与所述请求方之间共享认证信息。

12. 一种请求内容数据的发送的通信装置，其特征在于，包括：

认证部件，用于与对所述内容数据的发送的请求进行应答的请求对象之间共享认证信息；

测定请求接收部件，用于从所述请求对象接收使用在所述请求对象中共享的认证信息而生成的测定请求；

测定应答发送部件，用于向所述请求对象返回发送使用所述认证信息生成的测定应答，作为对于所述测定请求的应答；以及

判定部件，用于验证所述测定请求是否正确。

13. 根据权利要求 12 所述的通信装置，其特征在于，

所述通信装置，更进一步，包括：

测定准备请求接收部件，在接收所述测定请求之前，从所述请求对象接收测定准备请求，该测定准备请求用于请求为生成所述测定应答所需的预先准备。

14. 根据权利要求 13 所述的通信装置，其特征在于，

所述请求对象，使用与所述通信装置之间共享的认证信息，生成请求对象信息，分割所述请求对象信息而生成第一请求对象部分信息和第二请求对象部分信息的情况下，

所述通信装置，更进一步，包括：

测定准备部件，用于作为所述预先准备，在从接收所述测定准备请求到接收所述测定请求之间，使用所述认证信息，生成与所述请求对象信息一致的请求方信息，分割所述请求方信息而生成第一请求方部分信息和第二请求方部分信息；

验证请求接收部件，用于从所述请求对象接收请求验证所述测定请求的发送方是否为真正的请求对象的验证请求；

请求对象验证部件，用于在所述第二请求对象部分信息和所述第一请求方部分信息一致的情况下，判断所述测定请求的发送方为真正的请求对象；

验证信息生成部件，用于在所述测定请求的发送方为真正的请求对象的情况下，使用所述认证信息，生成通知在所述请求对象之间进行了所述往返延迟时间测定的验证信息；以及

验证应答发送部件，用于作为对于所述验证请求的应答向所述请求对象发送包含所述验证信息的验证应答；并且

所述测定请求接收部件，作为所述测定请求，从所述请求对象接收包含所述第二请求对象部分信息的请求。

15. 根据权利要求 14 所述的通信装置，其特征在于：

所述请求对象，在所述第二请求方部分信息与所述第一请求对象部分信息一致的情况下，判断所述测定应答的发送方为真正的请求方的情况下，

所述测定应答发送部件，作为所述测定应答，向所述请求对象发送包含所述第二请求方部分信息的应答。

16. 根据权利要求 12 记述的所述通信装置，其特征在于，所述通信装置进一步包括：

测定开始判定部件，用于判定是否开始所述往返延迟时间的测定；

测定开始请求发送部件，用于在开始所述往返延迟时间的测定的情况下，向所述请求对象发送请求开始对所述往返延迟时间的测定的测定开始请求；以及

测定开始应答接收部件，用于作为对所述测定开始请求的应答从所述请求对象接收测定开始应答；并且

从所述请求对象接收所述测定开始应答之后，所述认证部件与所述请求对象之间共享认证信息。

17. 根据权利要求 16 所述的通信装置，其特征在于，

所述测定开始判定部件，判定所述内容数据的接收是否结束；

所述测定开始请求发送部件，在已结束接收所述内容数据的情况下，向所述请求对象发送所述测定开始请求。

18. 根据权利要求 16 所述的通信装置，其特征在于，所述通信装置进一步包括：

密钥交换部件，用于交换所述内容数据发送中使用的密钥；并且

所述测定开始判定部件，从进行认证到进行密钥交换之间，判定所述往返延迟时间是否被测定，

所述测定开始请求发送部件，在所述往返延迟时间未被测定的情况下，在交换所述密钥之后，向所述请求对象发送所述测定开始请求。

19. 根据权利要求 12 所述通信装置，其特征在于，所述通信装置进一步包括：

测定开始请求接收部件，用于从所述请求对象接收通知开始所述往返时间的测定的测定开始请求；以及

测定开始应答发送部件，用于向所述请求对象发送作为对所述测定开始请求的应答的测定开始应答；并且

向所述请求对象发送所述测定开始应答之后，所述认证部件与所述请求对象之间共享认证信息。

20. 一种通信系统，其特征在于，其包括通过数据通信网而互相连接的权利要求 1 所述的通信装置，以及权利要求 12 所述的通信装置。

21. 一种通信方法，用于控制对内容数据的发送的请求进行应答的请求对象的通信装置与请求所述内容数据的发送的请求方的通信装置之间的通信，其特征在于，所述通信方法包括：

请求对象认证步骤，在所述请求对象，与所述请求方之间共享认证信息；

请求方认证步骤，在所述请求方，与所述请求对象之间共享认证信息；

测定请求发送步骤，在所述请求对象，向所述请求方发送使用所述认证信息而生成的测定请求；

测定请求接收步骤，在所述请求方，从所述请求对象接收使用所述请求对象共享的认证信息而生成的测定请求；

测定应答发送步骤，在所述请求方，向所述请求对象返回发送使用所述认证信息而生成的测定应答，作为对于所述测定请求的应答；

测定应答接收步骤，在所述请求对象，从所述请求方接收使用所述请求方共享的认证

信息而生成的测定应答，作为对所述测定请求的应答；

往返延迟时间测定步骤，在所述请求对象，测定从发送所述测定请求到接收所述测定应答的时间，作为往返延迟时间；

测定准备请求发送步骤，在所述请求对象，在发送所述测定请求之前，向所述请求方发送测定准备请求，该测定准备请求用于请求为生成所述测定应答所需的预先准备；

测定准备请求接收步骤，在所述请求方，在接收所述测定请求之前，从所述请求对象接收测定准备请求，该测定准备请求用于请求为生成所述测定应答所需的预先准备；以及

判定步骤，在所述请求对象，在测定所述往返延迟时间之后，所述往返延迟时间在标准值以下，验证所述测定应答为正确，并且在验证所述请求方中所述测定请求为正确的情况下，判定所述请求方是作为所述内容数据的发送对象的合格的装置。

通信装置、通信系统及通信方法

技术领域

[0001] 本发明涉及关于发送或接收加密内容数据的通信装置。特别是，基于传送时间，限制内容数据的接收方或发送方的通信装置。

背景技术

[0002] 近年，家庭内的装置由网络连接，正在实现使各种内容共享的家庭内部网络。作为家庭内部网络的实施方式之一，考虑为下述实施方式：在家庭内部设置路由器，将 PC 和数字电视等各个装置、存储内容的 AV 服务器以星型连接在路由器上。路由器，是用来连接家庭内部网络与家庭外部网络的。家庭内部的 AV 服务器，具有下述功能：将通过此路由器从家庭外部网络取得的各种内容，和由网络之外的方法，例如由数字广播播放的各种内容等暂时存储，再根据各个机器的请求将各种内容发送给已请求的接收装置。

[0003] 另一方面，在对待新创作的电影和收费播放的电视节目、音乐等的需要进行著作权保护的数据时，必须要保护著作权。作为保护著作权的有力的方法，有将需要进行著作权保护的数据加密，从而对数据的利用加以限制的方法。

[0004] 例如，利用网络传送图像声音数据（下称 AV 数据）时，在需要进行 AV 数据著作权保护的情况，将该 AV 数据加密再传送。作为实例，DTCP-IP(Digital Trans mission Protection over Internet Protocol) 方式已被标准化。

[0005] DTCP-IP 方式，具备认证功能和密钥的无效化功能，在 AV 数据传送时，排除不正确的机器，通过将 AV 数据等需要进行著作权保护的数据加密再传送以实现对著作权的保护。

[0006] 另外，关于需要进行著作权保护的 AV 数据的利用，由于一般限定为家庭内部个人利用，从而也有必要限制从家庭内部的 AV 服务器向家庭外部的不特定接收装置无限制地发布 AV 数据。

[0007] DTCP-IP 方式，为了限制发送命令的到达范围，使用生存时间 (TTL：Time To Live)。另外，TTL，是表示 IPv4 包的生存时间 (Time To Live 字段的值)，与 IPv6 的中继数 (Hop Limit 字段的值）相当。使用 TTL，可以根据包含在 IP 包头内的 TTL 字段的设定值，设定使 IP 包可通过的路由器的数目。

[0008] 不过，由于对 IP 包头的 TTL 字段的更改未受保护，存在其可能通过中继机器被更改的问题。

[0009] 因此，在DTCP-IP方式中，提案如下的发送接收系统：测定作为发送AV数据的发送装置与接收AV数据的接收装置之间的往返传送时间的RTT(Round Trip Time)，在判断其小于规定的限制时间的情况下，许可认证（例如参照专利文献 1。）。

[0010] 这样的数据发送接收系统，通过测定从发送测定请求后，至其收到其应答为止的时间而测定往返传送时间 RTT 的情况下，如果不正确的机器存在其间，则存在测定出的 RTT 比实际要短的可能性。因此，为了验证在测定请求与请求应答之间的信号交换中是否存在不正确的机器，有必要在接收测定请求的装置端和接收请求应答的装置端这两方都执行验证处理。

[0011] 下面，参照图 10 和图 11 对现有的数据发送接收系统进行说明。

[0012] 图 10 为在发送装置和接收装置中加密传送时从认证处理到加密传送的处理流程图。

[0013] 如图 10 所示，首先，接收装置将认证请求发送至发送装置，开始执行测定用认证处理 S101，发送装置和接收装置在认证处理 S101 结束后，执行传送时间测定处理 S102，测定接收装置的 RTT，RTT 在标准值以下的情况，执行密钥交换用认证处理 S103，如果认证处理成功，执行密钥交换处理 S104。

[0014] 密钥交换处理结束后，发送装置将 AV 数据加密再发送，接收装置使用密钥交换处理中接收的交换密钥生成解密密钥，对加密的接收数据进行解密处理。(S105)。

[0015] 图 11 为传送时间测定处理 S102 的详细处理流程图。

[0016] 首先，发送装置生成发送装置测定信息，放置于测定请求内发送 (S111)。接收装置验证接收的发送装置测定信息 (S112)，如果为不正确则以错误结束，如果为正确的，则生成接收机测定信息 (S113)，放置于测定请求应答内发送，发送装置接收测定请求应答并测定 RTT(S114)。

[0017] 接下来，发送装置检查 RTT 的测定值 (S115)，如果在标准值 (Tmax) 以下，则结束测定后继续进行下面的处理。大于标准值的情况下，检查测定次数 (S116)，未达到规定次数时，返回到步骤 S111，重复进行测定。接收装置，发送测定请求应答后，变为等待接收请求的状态，接收到测定请求时，返回到步骤 S111，重复进行测定 (S117)。

[0018] 然后，发送装置验证放置于接收的测定请求应答中的接收装置测定信息是否正确 (S118)，如果不正确则以错误结束。如果为正确的则判定为测定值在标准值以下并且为正确的值。

[0019] [专利文献 1] 日本专利特开 2004-194295 号公报 (第十一页)

[0020] 然而，上述的现有数据发送接收系统中的传送时间测定处理，由于在接收装置接收测定请求时要验证发送装置测定信息后再发送测定请求应答，测定时验证处理时间要加入至传送时间，存在不能测定出正确的 RTT 的问题。另外，现有的数据发送接收系统，存在因为用于传送时间测定处理的认证处理以其他途径进行而使处理变得复杂的问题，以及即使只想进行传送时间测定的情况下，也执行无用的密钥交换处理的问题。

发明内容

[0021] 因此，本发明的目的在于提供在能够正确测定传送时间的同时，能共用用于加密传送的认证处理，并且，不执行无用的密钥交换处理的通信装置、通信系统及通信方法。

[0022] 为了达成上述的目的，本发明涉及的通信装置，是 (a) 对于内容数据的发送的请求进行应答的通信装置，具有 (a1) 认证部件，用于与请求所述内容数据的发送的请求方之间共享认证信息 ；(a2) 测定请求发送部件，用于向所述请求方发送使用所述认证信息而生成的测定请求 ；(a3) 测定应答接收部件，用于从所述请求方接收使用所述请求方共享的认证信息而生成的测定应答，作为对于所述测定请求的应答 ；(a4) 往返延迟时间测定部件，用于测定从发送所述测定请求到接收所述测定应答的时间，作为往返延迟时间 ；(a5) 判定部件，用于在所述往返延迟时间测定后，在确认了所述往返延迟时间在标准值以下，验证所述测定应答为正确，并且已验证所述请求方中所述测定请求为正确的情况下，判定所述请

求方作为所述内容数据的发送对象为合格的装置。

[0023] 进一步，(a6) 所述通信装置还可以具有：测定准备请求发送部件，在发送所述测定请求之前，向所述请求方发送测定准备请求，该测定准备请求用于请求为生成所述测定应答所需的预先准备。

[0024] 更进一步，(a7) 所述判定部件，当使用所述认证信息生成的第一验证信息与在所述请求方中使用认证信息生成的第二验证信息一致的情况下，也可以验证所述测定应答为正确。

[0025] 或者，为了达成上述目的，本发明涉及的通信装置，是 (b) 请求内容数据发送的通信装置，具有 (b1) 认证部件，用于与对所述内容数据的发送请求进行应答的请求对象之间共享认证信息；(b2) 测定请求接收部件，用于从所述请求对象接收使用在所述请求对象中共享的认证信息而生成的测定请求；(b3) 测定应答发送部件，用于向所述请求对象返回发送使用所述认证信息生成的测定应答，作为对于所述测定请求的应答；(b4) 验证所述测定请求是否正确的判定部件。

[0026] 进一步，还可以具有：(b5) 测定准备请求接收部件，在接收所述测定请求之前，从所述请求对象接收测定准备请求，该测定准备请求用于请求为生成所述测定应答所需的预先准备。

[0027] 另外，本发明，不仅实现为通信装置，也可以作为具有通过数据通信网互相连接的请求对象的通信装置（服务器）和请求方的通信装置（客户端）的通信系统。

[0028] 另外，也可以实现为：控制通信装置（服务器或者客户端）的通信方法。

[0029] 由上述可以理解，本发明能够提供传送时间测定方法以及数据发送接收系统，其中的传送时间测定方法：当测定值在标准值以下时执行接收装置端的验证处理，在用于加密传送的认证处理中共用用于传送时间测定的认证处理，利用测定开始请求启动测定的情况下，只执行测定处理和注册处理，由此，在可以正确地测定传送时间的同时，可以共享既有的认证处理，并且不执行无用的密钥交换处理。

附图说明

[0030] 图 1 是表示本发明第一实施方式以及第二实施方式中，数据发送接收系统结构的图。

[0031] 图 2 是表示本发明第一实施方式中，发送装置结构的图。

[0032] 图 3 是表示本发明第一实施方式中，接收装置结构的图。

[0033] 图 4 是表示本发明第一实施方式中，加密传送时的处理顺序的图。

[0034] 图 5 是表示本发明第一实施方式中，传送时间测定处理的处理顺序的图。

[0035] 图 6 是表示本发明第二实施方式中，发送装置结构的图。

[0036] 图 7 是表示本发明第二实施方式中，接收装置结构的图。

[0037] 图 8 是表示本发明第二实施方式中，发送装置启动传送时间测定时的处理顺序的图。

[0038] 图 9 是表示本发明第二实施方式中，接收装置启动传送时间测定时的处理顺序的图。

[0039] 图 10 是表示现有的数据发送接收系统中，加密传送时的处理顺序的图。

[0040] 图 11 是表示现有的数据发送接收系统中，传送时间测定处理的处理顺序的图。

[0041] 附图标记说明

[0042] 1 AV 服务器

[0043] 2 数字电视

[0044] 3 PC

[0045] 4 路由器

[0046] 5 路由器

[0047] 6 PC

[0048] 7 数字电视

[0049] 21 发送接收部

[0050] 22 密码处理部

[0051] 23 密钥交换处理部

[0052] 24 认证处理部

[0053] 25 传送时间测定处理部

[0054] 26,27 接收装置注册部

[0055] 28 测定开始处理部

[0056] 31 发送接收部

[0057] 32 解密处理部

[0058] 33 密钥交换处理部

[0059] 34 认证处理部

[0060] 35 传送时间测定处理部

[0061] 36 测定开始处理部

具体实施方式

[0062] （第一实施方式）

[0063] 下面，利用图 1 至图 5 对本发明第一实施方式进行详细说明。

[0064] ＜概要＞

[0065] 在本实施方式中，(a) 对于内容数据的发送的请求进行应答的通信装置（以下，称为发送装置），具有下述特征：(a1) 与请求内容数据的发送的请求方之间共享认证信息；(a2) 向请求方发送使用认证信息而生成的测定请求；(a3) 从请求方接收使用请求方共享的认证信息而生成的测定应答，作为对于测定请求的应答；(a4) 测定从发送测定请求到接收测定应答的时间，作为往返延迟时间；(a5) 在发送测定请求之前，向请求方发送测定准备请求，该测定准备请求用于请求为生成测定应答所需的预先准备；(a6) 在往返延迟时间测定后，往返延迟时间在标准值以下，验证测定应答为正确，并且已验证请求方中测定请求为正确的情况下，判定请求方作为内容数据的发送对象为合格的装置。

[0066] 另外，(b) 请求内容数据的发送的通信装置（以下，称为接收装置），具有下述特征：(b1) 与对内容数据发送请求进行应答的请求对象之间共享认证信息；(b2) 从请求对象接收使用在请求对象中共享的认证信息而生成的测定请求；(b3) 向请求对象返回发送使用认证信息生成的测定应答，作为对于测定请求的应答；(b4) 在接收测定请求之前，从请

求对象接收测定准备请求，该测定准备请求用于请求为生成测定应答所需的预先准备。

[0067] 然后，在具有通过数据通信网互相连接的发送装置和接收装置的通信系统中（以下，称为数据发送接收系统），基于本实施方式的传送时间测定方法，在通过测定步骤测定的测定值在规定值以下的情况下，验证互相从对方装置接收的测定信息是否正确，在正确的情况则判断测定值为正确值。

[0068] 另外，本实施方式的数据发送接收系统，在执行认证处理后，发送装置，在接收装置未注册的情况下，由测定部件测定往返延迟时间，由判定部件在判定测定值为正确值的情况下执行密钥交换处理，接收装置已注册的情况下，继续进行密钥交换处理。

[0069] 根据以上观点，说明本实施方式中的数据发送接收系统，以及传送时间测定方法。

[0070] ＜结构＞

[0071] 图 1，为表示构成本实施方式的数据发送接收系统的发送装置以及接收装置的图，也是作为发送装置的 AV 服务器、作为接收装置的 PC、数字电视以及路由器的连接图。

[0072] 如图 1 所示，在家庭内部，设置有，AV 服务器 1、数字电视 2、PC3、以及路由器 4。路由器 4 与 AV 服务器 1、数字电视 2 通过以大网（注册商标）相连接，路由器 4 与 PC3 通过无线方式（IEEE802.11b）相连接。

[0073] 另外，路由器 4，通过因特网与家庭外部的路由器 5 相连接。路由器 5，与作为接收装置的 PC6、数字电视 7 相连接。这里，路由器 5 和 PC6 通过以太网（注册商标）相连接，路由器 5 和数字电视 7 通过无线方式（IEEE802.11b）相连接。

[0074] 图 2，表示作为发送装置的 AV 服务器 1 的结构。

[0075] 如图 2 所示，AV 服务器 1，由发送接收部 21，密码处理部 22，密钥交换处理部 23，认证处理部 24，传送时间测定处理部 25，接收装置注册部 26 构成。这里，传送时间测定处理部 25，在本发明中，对应为：测定准备请求发送部件，测定准备应答接收部件，测定准备部件，测定请求发送部件，测定应答接收部件，测定部件以及判定部件。接收装置注册部 26 与注册部件及注册确认部件对应。

[0076] 发送接收部 21，将 AV 数据向网络发送，也是为了与连接到网络上的其他机器之间发送接收指令的数字接口。

[0077] 密码处理部 22，将从内容存储部（图中未表示）再生的 AV 数据进行加密。

[0078] 密钥交换处理部 23，生成接收装置为了将 AV 数据的密码进行解密而使用的交换密钥，使用从认证处理部 24 接收的认证信息进行加密，并通过发送接收部 21 输出。

[0079] 认证处理部 24，从接收装置接收认证请求进行认证处理，并与接收装置共享认证信息，同时，一起接收表示接收装置的 RTT 测定功能有无的标志信息与证明信息。

[0080] 传送时间测定处理部 25，生成测定准备请求和测定请求，通过发送接收部 21 发送，并处理接收到的测定准备请求应答和测定请求应答。另外，测定作为从发送测定请求到接收测定请求应答的往返延迟时间的 RTT，在其为规定的标准值以下的情况下，生成验证请求并通过发送接收部 21 发送，处理接收到的验证请求应答，判断测定的 RTT 是否正确。

[0081] 接收装置注册部 26，存储由传送时间测定处理部 25 判定 RTT 在标准值以下的接收装置的设备 ID。这里，所谓设备 ID，是预先从密钥管理中心分配的、用于确定机器的信息。

[0082] 作为接收装置的数字电视 2、PC3、PC6、数字电视 7 的数据发送接收部分别具有同样的结构。图 3 表示了接收装置（数字电视 2 等）的数据发送接收部的结构。

[0083] 如图 3 所示，接收装置（数字电视 2 等），由发送接收部 31，解密处理部 32，密钥交换处理部 33，认证处理部 34，传送时间测定处理部 35 构成。这里，传送时间测定处理部 35 在本发明中对应：测定准备请求接收部件，测定准备应答发送部件，测定准备部件，测定请求接收部件，测定应答发送部件以及验证部件。

[0084] 发送接收部 31，通过网络接收已发送的 AV 数据，也是为了与连接到网络上的其他机器之间发送接收指令的数字接口。

[0085] 解密处理部 32，接收从密钥交换处理部 33 发送的交换密钥，使用已接收的交换密钥生成解密密钥，通过发送接收部 31 接收 AV 数据，将已接收的 AV 数据的密码进行解密。经解密处理部 32 进行解密已变为明文的 AV 数据，经解码器（图中未表示）进行解码，并显示在监视器（图中未表示）上。

[0086] 密钥交换处理部 33，通过发送接收部 31 接收交换密钥，另外，接收从认证处理部 34 发送的认证信息，使用已接收的认证信息，将已接收的交换密钥进行处理并向解密处理部 32 发送。

[0087] 认证处理部 34，通过发送接收部 31，向 AV 服务器 1 的认证处理部 24 请求认证开始，执行认证处理并与 AV 服务器 1 的认证处理部 24 共享认证信息。另外，将表示接收装置的 RTT 测定功能有无的标志信息与证明信息一起通过发送接收部 31 向 AV 服务器 1 发送。

[0088] 传送时间测定处理部 35，通过发送接收部 31，将从 AV 服务器 1 发送的测定准备请求、测定请求、验证请求进行接收处理，生成测定准备请求、测定请求应答和验证请求应答，并通过发送接收部 31 向 AV 服务器 1 发送。

[0089] ＜动作＞

[0090] 下面，对于上述结构的本实施方式的动作进行说明。

[0091] 图 4，为发送装置 (AV 服务器 1) 和接收装置（数字电视 2) 中做加密传送时从认证处理到加密传送的处理流程图。

[0092] 如图 4 所示，首先，接收装置的认证处理部 34，将认证请求向发送装置发送并开始认证处理 (S41)。

[0093] 认证处理 (S41) 结束后，发送装置的传送时间测定处理部 25，检查认证处理 (S41) 中接收的表示接收装置的 RTT 测定功能有无的标志信息 (S42)，如果具有 RTT 测定功能则进行下一步的处理 (S43)。如果不具有 RTT 测定功能则进行密钥交换处理 (S47)。

[0094] 下面，发送装置的接收装置注册部 26，判定接收装置是否已注册 (S43)，如果未注册，则进行下面的传送时间测定处理 (S45)，如果已注册，则进行密钥交换处理 (S47)。

[0095] 接收装置，在认证处理 (S41) 结束后，变为等待接收请求状态，检查接收到的请求 (S44)，在接收了测定准备请求的情况下，进入传送时间测定处理 (S45)。在接收了交换密钥的情况下，进入密钥交换处理 (S47)。

[0096] 发送装置，在传送时间测定处理 (S45) 结束后，确认传送时间测定处理是否正常结束 (S46)，如果正常结束，则执行密钥交换处理 (S47)，如果未正常结束，则以错误结束发送处理。

[0097] 接收装置，在传送时间测定处理 (S45) 结束后，变为等待接收请求状态，在接收了交换密钥的情况下，执行密钥交换处理 (S47)。

[0098] 发送装置，如果密钥交换处理 (S47) 结束，则将内容数据加密并发送。接收装置，

接收加密的内容数据，并做解密处理 (S48)。

[0099] 图 5，为表示传送时间测定处理 (S45) 的详细的处理流程图。

[0100] 如图 5 所示，首先，发送装置和接收装置，作为测定准备步骤，执行测定准备请求发送步骤 (S51) 至测定准备步骤 (S53)。发送装置，向接收装置发送包括测定号码 N 的测定准备请求 (S51)，生成发送装置测定信息。接收装置，作为对测定准备请求的应答，向发送装置发送测定准备请求应答 (S52)。发送装置，如果接收到测定准备请求应答，则准备测定处理。另外，接收装置，在发送测定准备应答后，生成接收装置测定信息，进行测定处理的准备 (S53)。

[0101] 在测定准备步骤中，按照以下的次序生成发送装置测定信息和接收装置测定信息。首先，使用由认证处理部 24 或者由认证处理部 34 提供的 Kauth(96bit) 和测定次数值 N(初始值为 0)，生成作为共享保密信息的共享验证信息 Kvrfy(160bit)。将共享验证信息 Kvrfy(160bit) 分为 Kvrfy(高位 80bit) 和 Kvrfy(低位 80bit)。发送装置将 Kvrfy(高位 80bit) 作为发送装置测定信息，将 Kvrfy(低位 80bit) 作为接收装置测定信息的验证用信息。接收装置将 Kvrfy(低位 80bit) 作为接收装置测定信息，将 Kvrfy(高位 80bit) 作为发送装置测定信息的验证用信息。

[0102] 下面，发送装置和接收装置，作为测定步骤，执行测定请求发送步骤 (S54) 以及 RTT 测定步骤 (S55)。发送装置，将发送装置测定信息放置于测定请求并发送。接收装置，作为测定步骤，将接收装置测定信息放置于测定请求应答并发送 (S54)。这时，发送装置接收由接收装置应答的测定请求应答并测定 RTT(S55)。

[0103] 接着，发送装置和接收装置，作为判定步骤，执行标准值判定步骤 (S56) 至接收装置验证信息验证步骤 (S64)。发送装置，检查测定值 (RTT)(S56)，如果在标准值 (Tmax) 以下 (S56 :YES)，结束测定，继续进行下面的处理。大于标准值的情况下 (S56 :NO)，检查测定次数 (S57)，未达到规定次数时 (S57 :YES)，返回至测定准备请求发送步骤 (S51) 重复进行测定。这时，接收装置，在发送测定请求应答后，变为等待接收请求状态，在接收了测定准备请求时，返回至测定准备请求应答步骤 (S52)。然后，进行重复测定的交互 (S58)。

[0104] 然后，发送装置，将放置于已接收的测定请求应答的接收装置测定信息，与所准备的验证用信息相比较 (S59)，不一致的情况下 (S59 :NO)，以错误结束。一致的情况下 (S59 :YES)，发送验证请求 (S60)。接收装置，接收验证请求，将放置于测定请求的发送装置测定信息，与所准备的验证用信息相比较 (S61)，不一致的情况下 (S61 :NO)，以错误结束，一致的情况下 (S61 :YES)，从认证信息 Kauth 生成接收装置验证信息 (S62)，将接收装置验证信息放置于验证请求应答中并发送 (S63)。

[0105] 发送装置，验证已接收的接收装置验证信息，并对测定值是否正确进行最终验证 (S64)，不正确的情况下 (S64 :NO)，以错误结束，正确的情况下 (S64 :YES)，继续下面的注册处理。

[0106] 最后，发送装置，在接收装置注册部 26 中注册接收装置的设备 ID，该接收装置在判定处理中的测定值在标准值以下并且被判定为正确 (S65)。

[0107] 例如，图 1 中各个装置间的传送中，以太网 (注册商标) 的往返延迟时间为 0.02ms(毫秒)，无线 (802.11b) 的往返延迟时间为 3ms，路由器的处理延迟时间为 0.5ms，因特网的往返延迟时间为 10ms，接收装置的处理延迟时间为 0.2ms。并且，在这里设想为路

径上存在两台路由器的情况。据此，作为发送装置的AV服务器1与各个接收装置之间的传送时间(RTT)，在家庭内部装置之间，为以下的式(1)和式(2)。另外，在家庭内部装置与家庭外部装置之间，为以下的式(3)和式(4)。

[0108] (家庭内部装置之间)

[0109] (1)与数字电视2的RTT(T1) = 0.02+0.02+0.2 = 0.24ms

[0110] (2)与PC3的RTT(T2) = 0.02+3+0.2 = 3.22ms

[0111] (家庭内部装置与家庭外部装置之间)

[0112] (3)与PC6的RTT(T3) = 0.02+0.5×4+10+0.02+0.2 = 12.24ms

[0113] (4)与数字电视7的RTT(T4) = 0.02+0.5×4+10+3+0.2 = 15.22ms

[0114] 这里，如果标准值Tmax = 7ms，对于家庭内部装置的数字电视2和PC3，因为RTT在7ms以下，接收装置被注册。接着，在这些家庭内部的装置间，执行密钥交换处理(S47)、加密传送处理(S48)。另外一方面，对于家庭外部装置的PC6以及数字电视7，由于RTT大于7ms，接收装置不被注册。因此，在这些家庭外部的装置间，不执行密钥交换处理(S47)、加密传送处理(S48)。

[0115] 根据上述动作，RTT的测定值在标准值以下，并且作为接收装置的RTT判定为正确时，执行密钥交换处理，接收装置可以将加密的数据进行解密。

[0116] 如上所述，本实施方式的传送时间测定方法，用测定步骤测定的测定值在规定值以下的情况下，验证互相从对方装置接收的测定信息是否正确。因此，接收装置，因为在测定请求处理中不执行验证处理，验证处理时间不被加入至传送时间，就可以测定正确的往返延迟时间。这样，可以得到本实施方式的特有效果。

[0117] 还有，本实施方式的数据发送接收系统，在执行认证处理后，发送装置，在接收装置未注册的情况下，由测定部件测定往返延迟时间，由判定部件在判定测定值为正确的值的情况下，执行密钥交换处理。另外一方面，接收装置已注册的情况下，由于接着执行密钥交换处理，不变更为了执行密钥交换的认证处理，可作为为了测定传送时间的认证处理而共用。这样，可得到本实施方式的特有效果。

[0118] 另外，在本实施方式中，测定信息是从认证信息生成共享验证信息，将共享验证信息分为接收装置测定信息和发送装置测定信息而生成的。但是，也可以采用其它方法生成测定信息。

[0119] 还有，本实施方式中，发送装置，在发送测定准备请求后才生成发送装置测定信息。但是，只要是在发送测定请求前，也可以在其它的时间(timing)

[0120] 生成。

[0121] 还有，本实施方式中，说明的是接收装置台数为4台的情况。但是，并不局限于此，也可以连接其他任意台数。

[0122] 还有，本实施方式中，作为网络的传送媒介，用以太网(注册商标)和IEEE802.11b的情况进行了说明。但是，也可以使用IEEE802.11a/g/n和Bluetooth等其他的传送媒介。

[0123] 并且，本实施方式中，以7ms为标准值，但是，并不局限于此，设定为其他的标准值也可以。

[0124] (第二实施方式)

[0125] 下面，参照图6至图9对第二实施方式进行详细说明。

[0126] 〈概要〉

[0127] 本实施方式中的数据发送接收系统，发送装置或者接收装置发送测定开始请求的情况下，执行认证处理后，由测定部件测定传送时间，由判定部件判定测定值为正确值的情况下注册接收装置，不执行密钥交换处理。

[0128] 〈结构〉

[0129] 构成本实施方式的数据发送接收系统的发送装置以及接收装置，与第一实施方式同样地用图 1 表示。

[0130] 图 6，表示本实施方式中作为发送装置的 AV 服务器 1 的结构。

[0131] AV 服务器 1，由发送接收部 21，密码处理部 22，密钥交换处理部 23，认证处理部 24，传送时间测定处理部 25，接收装置注册部 27，测定开始处理部 28 构成。这里，传送时间测定处理部 25 与本发明中的测定准备部件，测定部件以及判定部件对应；接收装置注册部 27 对应于注册部件，注册确认部件以及注册取消部件；测定开始处理部 28 与测定开始部件相对应。

[0132] 本实施方式中接收装置的结构与第一实施方式的结构的不同为接收装置注册部 27 和测定开始处理部 28，其他部分的结构相同故省略说明。

[0133] 接收装置注册部 27，保存由传送时间测定处理部 25 判定 RTT 在标准值以下的接收装置的设备 ID，注册接收装置。另外，当注册后经过规定的有效时间后，取消注册。

[0134] 测定开始处理部 28，检查所述有效时间的剩余时间，当剩余时间变为 0 时，发送测定开始请求，开始为了测定处理的认证处理。另外，在接收到测定开始请求的情况下，也开始为了测定处理的认证处理。

[0135] 图 7 为表示接收装置（数字电视 2）的数据发送接收部的结构。

[0136] 接收装置，由发送接收部 31，解密处理部 32，密钥交换处理部 33，认证处理部 34，传送时间测定处理部 35，测定开始处理部 36 构成。这里，传送时间测定处理部 35，在本发明中对应为：测定准备请求接收部件，测定准备应答发送部件，测定准备部件，测定请求接收部件，测定应答发送部件以及验证部件；测定开始处理部 36，与测定开始判定部件，测定开始请求发送部件，测定开始应答接收部件相对应。

[0137] 本实施方式中接收装置的结构与第一实施方式的结构的不同为测定开始处理部 36，其他部分的结构相同故省略说明。

[0138] 测定开始处理部 36，在完成接收加密数据时，或者，在认证处理和密钥交换处理之间未执行传送时间测定处理的情况下则在密钥交换处理结束时，发送测定开始请求，并开始为了测定处理的认证处理。另外，在接收到测定开始请求的情况下也开始为了测定处理的认证处理。

[0139] 〈动作〉

[0140] 参照图 8 以及图 9 对本实施方式中数据发送系统的动作进行说明。

[0141] 图 8 表示本实施方式中，在发送装置启动测定处理情况下的动作顺序。

[0142] 发送装置的测定开始处理部 28，检查由接收装置注册部 27 管理的注册有效时间 (S81)，判定有效时间的剩余时间是否为 0，为 0 时向接收装置发送测定开始请求 (S83)。接收装置的测定开始处理部 36，检查接收的请求 (S82)，如果接收到测定开始请求，就发送应答 (S84)，向认证处理部 34 请求认证开始。认证处理部 34，发行认证请求并执行认证处理

(S85)。这里的认证处理(S85),共用与执行密钥交换处理情况下的认证处理(S41)相同的处理。

[0143] 如果认证处理(S85)结束后,发送装置的传送时间测定处理部25,执行传送时间测定处理(S86),当测定值在标准值以下,并且判定测定值为正确的情况下,注册接收装置,结束处理。由发送测定开始请求而启动测定的情况下,不执行密钥交换处理。传送时间测定处理(S86)的详细动作与图5表示的第一实施方式中的传送时间测定处理(S45)相同。

[0144] 这种情况下,可使接收装置的注册始终有效。因此,为了加密传送而执行密钥交换处理时,没有必要执行传送时间测定处理。

[0145] 图9,表示在本实施方式中,在接收装置启动测定处理情况下的动作顺序。

[0146] 接收装置的测定开始处理部36,检查接收的数据,在完成接收加密的数据时,或者,在认证处理和密钥交换处理之间未执行传送时间测定处理的情况下则在通过密钥交换处理而接收交换密钥时,决定测定开始(S92),向发送装置发送测定开始请求(S93)。发送装置的测定开始处理部28,检查接收的请求(S91),如果接收到测定开始请求,则发送应答(S94)。然后,接收装置,如果接收到应答,则向认证处理部34请求认证开始。认证处理部34,发行认证请求并执行认证处理(S95)。这里的认证处理(S95),共用与执行密钥交换处理情况下的认证处理(S41)相同的处理。

[0147] 如果认证处理(S95)结束后,发送装置的传送时间测定处理部25,执行传送时间测定处理(S96),当测定值在标准值以下,并且判定测定值为正确的情况下,注册接收装置,结束处理。利用发送测定开始请求而启动测定的情况下,不执行密钥交换处理。传送时间测定处理(S96)的详细动作,与图5所示的第一实施方式中的传送时间测定处理(S45)相同。

[0148] 这种情况下,可使接收装置的注册始终为有效。因此,为了加密传送而执行密钥交换处理时,没有必要执行传送时间测定处理。

[0149] 如上所述,本实施方式的数据发送接收系统,在发送装置或者接收装置发送了测定开始请求的情况下,在执行认证处理之后,由测定部件测定传送时间,由判定部件判定测定值为正确值的情况下,注册接收装置。据此,用于执行密钥交换的认证处理不进行变更,可作为用于传送时间测定的认证处理而共用,并且可以得到不执行无用的密钥交换处理的本实施方式的特有效果。

[0150] 另外,本实施方式的数据发送接收系统中的发送装置,由于检查注册有效时间的剩余时间而启动传送时间测定,注册没变为无效,在进行为了实现加密传送的认证处理以及密钥交换处理时,就没有必要执行传送时间测定处理,因此,可得到缩短传送开始时的延迟时间的本实施方式的特有效果。

[0151] 另外,本实施方式的数据发送接收系统中的接收装置,在完成接收加密数据时,或者,当认证处理和密钥交换处理之间传送时间测定处理未执行时则在接收交换密钥时,启动传送时间测定,因而注册没变为无效,在进行为了实现加密传送的认证处理以及密钥交换处理时,就没有必要执行传送时间测定处理,因此,可以得到缩短传送开始时的延迟时间的本实施方式的特有效果。更进一步,在接收交换密钥时启动传送时间测定的情况下,可以得到能使用与认证密钥交换处理相同的连接而执行测定开始处理以及测定处理的本实施方式的特有效果。

[0152] 还有，本实施方式中，发送装置，当注册的有效时间的剩余时间归 0 时启动传送时间测定，但也可以在剩余时间在规定值以下的情况下启动，也可以在剩余时间和其他条件组合下启动。

[0153] 更进一步，本实施方式中，接收装置，在完成接收加密数据时，或者接收交换密钥时启动传送时间测定，但根据发送装置中自身装置的注册剩余时间进行推定，推定为剩余时间富余的情况下，可以不启动传送时间测定。

[0154] 更进一步，具有以下特征的介质也属于本发明：保存有为了将本发明的数据发送接收系统的功能通过计算机执行的程序以及 / 或者数据的，通过计算机能够进行处理的介质。

[0155] 更进一步，具有以下特征的信息集合体也属于本发明：为了将本发明的数据发送接收系统的功能通过计算机执行的程序以及 / 或者数据。

[0156] 更进一步，本发明所谓的数据，包含数据结构，数据格式，数据的种类等。

[0157] 更进一步，本发明所谓的介质，包含 ROM 等存储介质，因特网等传送介质，光、电波、声波等传送介质。

[0158] 更进一步，本发明所谓的保存的介质包括：例如，存储程序以及 / 或者数据的存储介质，和传送程序以及 / 或者数据的传送介质。

[0159] 更进一步，本发明所谓的由计算机能够进行处理包括：例如，如果为 ROM 等的存储介质的情况下，计算机可读；如果为传送介质的情况下，作为将成为传送对象的程序以及 / 或者数据进行传送的结果，可以由计算机进行存取。

[0160] 更进一步，本发明所谓的信息集合体，包含例如程序以及 / 或者数据等的软件。

[0161] 更进一步，如上所述，本发明的结构，可以用软件来实现，也可以用硬件来实现。

[0162] 本发明，涉及发送接收加密数据的发送接收系统、传送时间的测定方法，对于基于家庭内部网络等的 AV 数据传送是有用的。

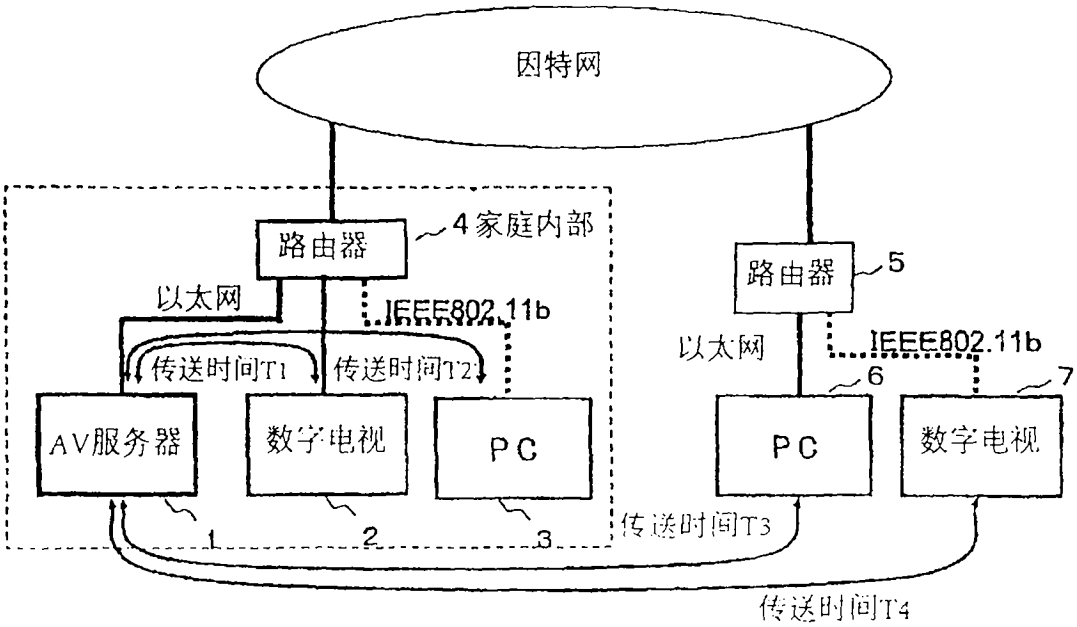

因特网
路由器
4 家庭内部
以太网
IEEE802.11b
传送时间T1
传送时间T2
AV服务器
数字电视
PC
1
2
3
路由器
5
以太网
IEEE802.11b
6
7
PC
数字电视
传送时间T3
传送时间T4

图 1

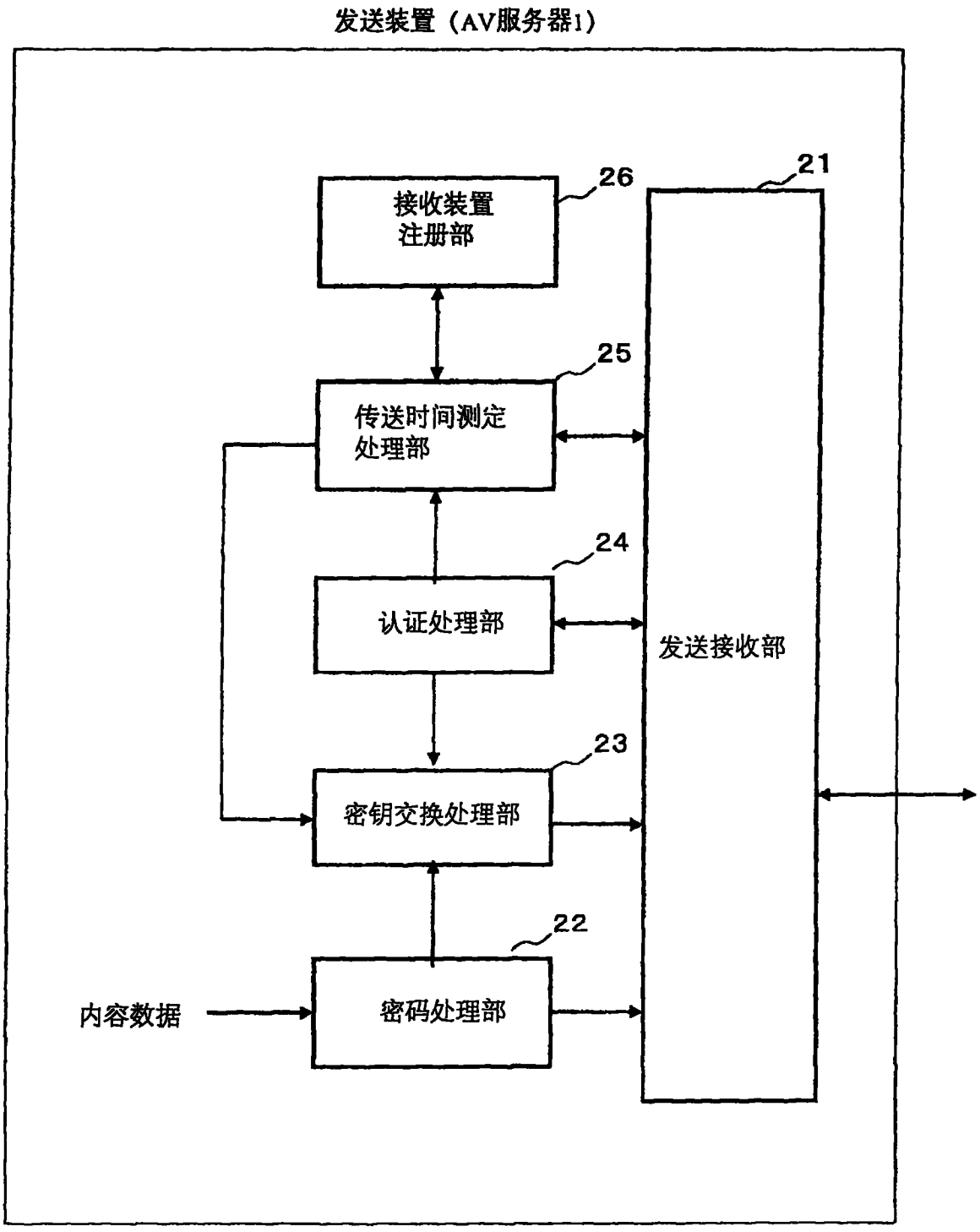

发送装置（AV服务器1）
接收装置
注册部
26
21
25
传送时间测定
处理部
24
认证处理部
发送接收部
23
密钥交换处理部
22
内容数据
密码处理部

图 2

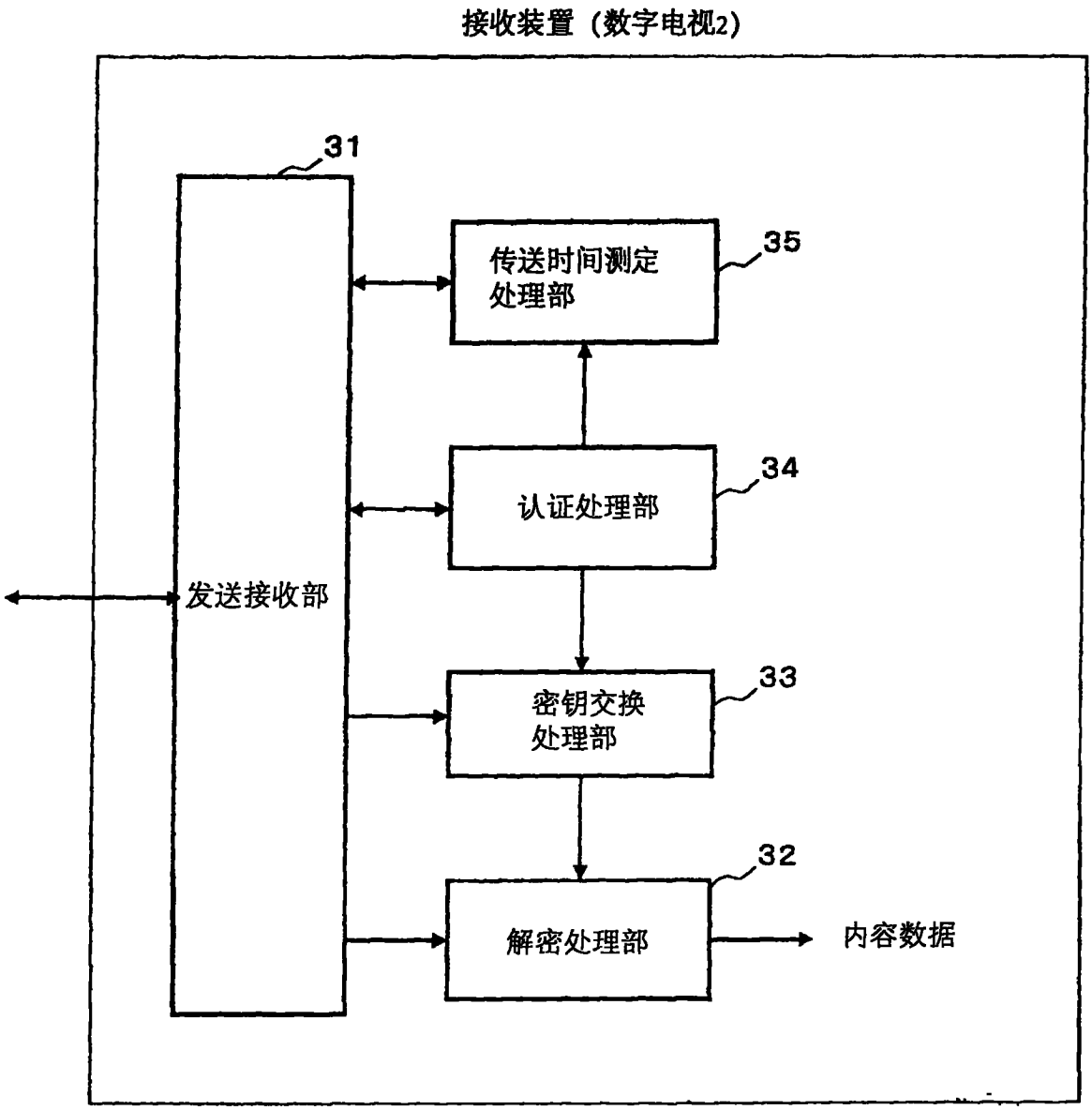

接收装置（数字电视2）
31
传送时间测定
处理部
35
认证处理部
34
发送接收部
密钥交换
处理部
33
32
解密处理部
内容数据

图 3

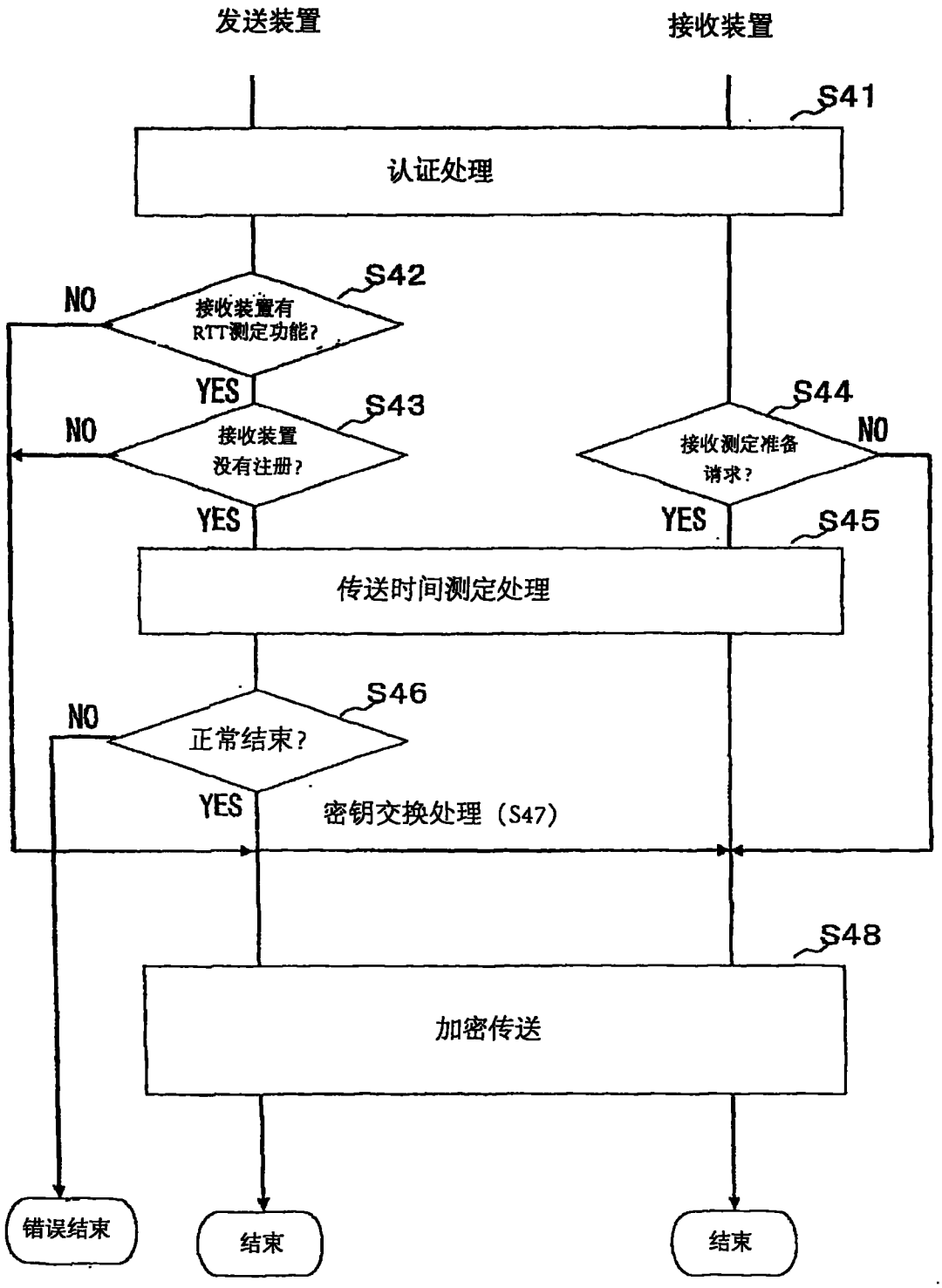

发送装置
接收装置
S41
认证处理
S42
NO
接收装置有
RTT测定功能?
YES
S43
NO
接收装置
没有注册?
YES
S44
接收测定准备
请求?
NO
YES
S45
传送时间测定处理
S46
NO
正常结束?
YES
密钥交换处理（S47）
S48
加密传送
错误结束
结束
结束

图 4

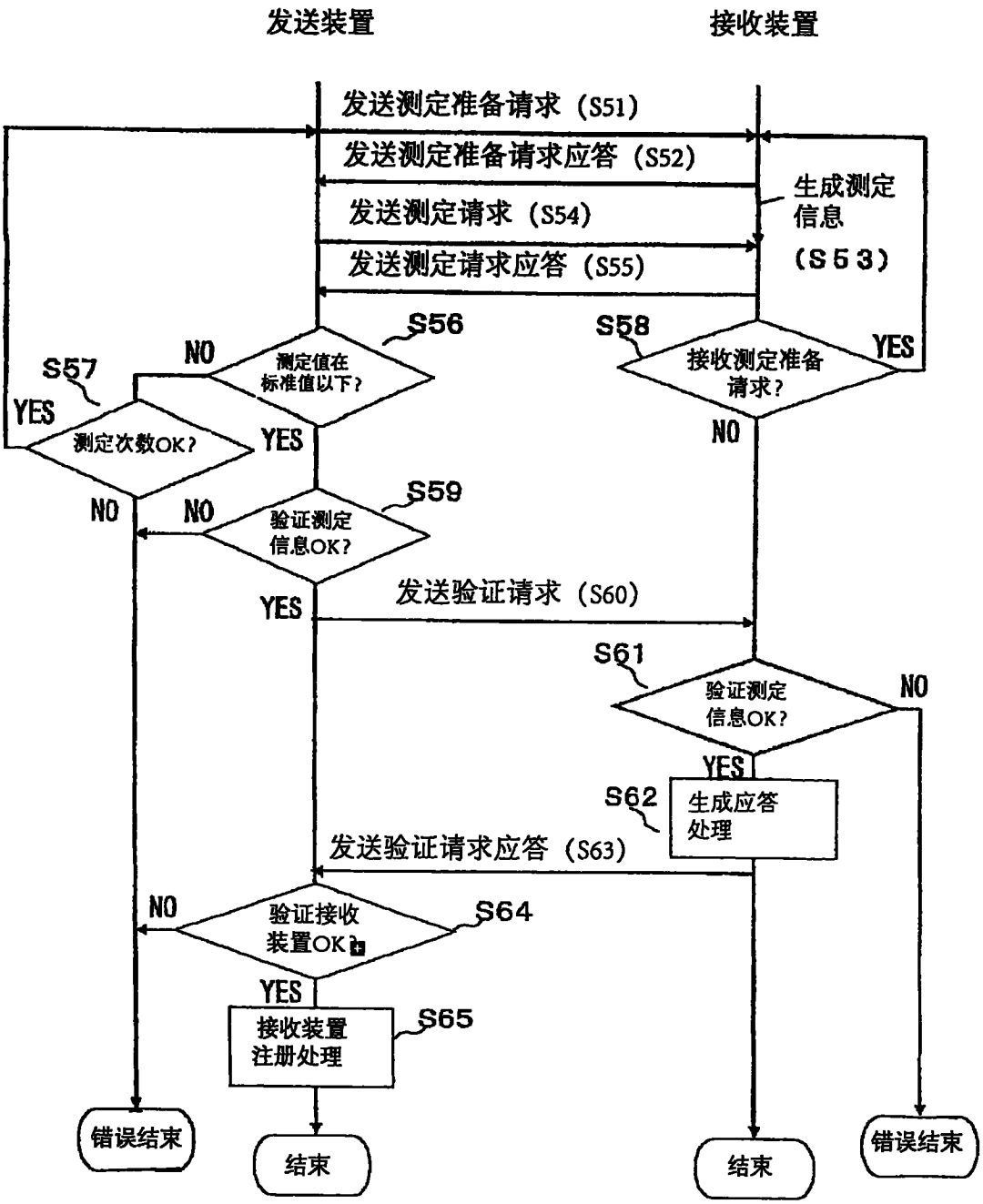

发送装置
接收装置
发送测定准备请求（S51）
发送测定准备请求应答（S52）
发送测定请求（S54）
发送测定请求应答（S55）
生成测定信息（S53）
S56
测定值在标准值以下？
NO
YES
S57
测定次数OK？
YES
NO
S58
接收测定准备请求？
YES
NO
S59
验证测定信息OK？
NO
YES
发送验证请求（S60）
S61
验证测定信息OK？
NO
YES
S62
生成应答处理
发送验证请求应答（S63）
S64
验证接收装置OK？
NO
YES
S65
接收装置注册处理
错误结束
结束
结束
错误结束

图 5

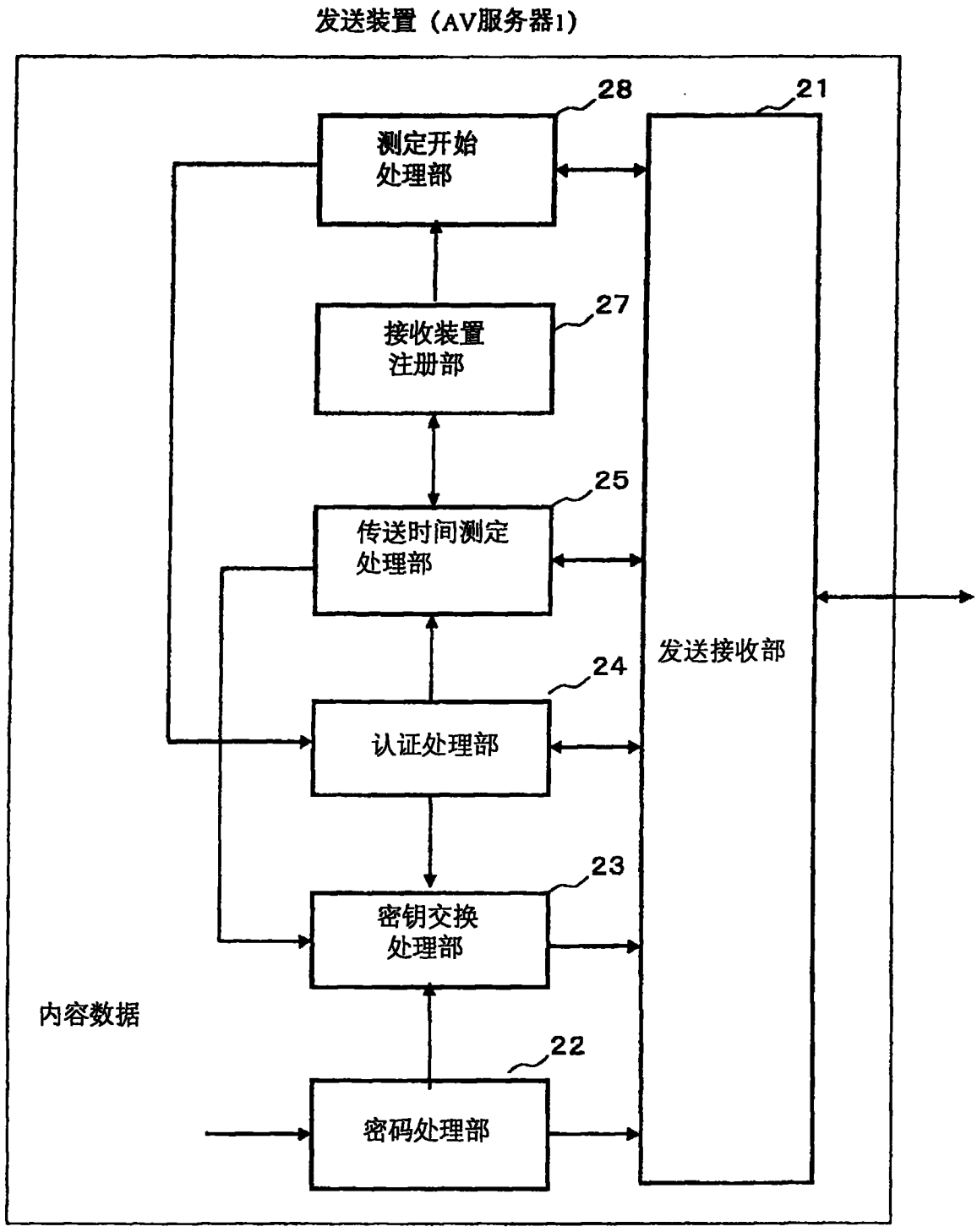

发送装置（AV服务器1）
28
21
测定开始
处理部
27
接收装置
注册部
25
传送时间测定
处理部
发送接收部
24
认证处理部
23
密钥交换
处理部
内容数据
22
密码处理部

图 6

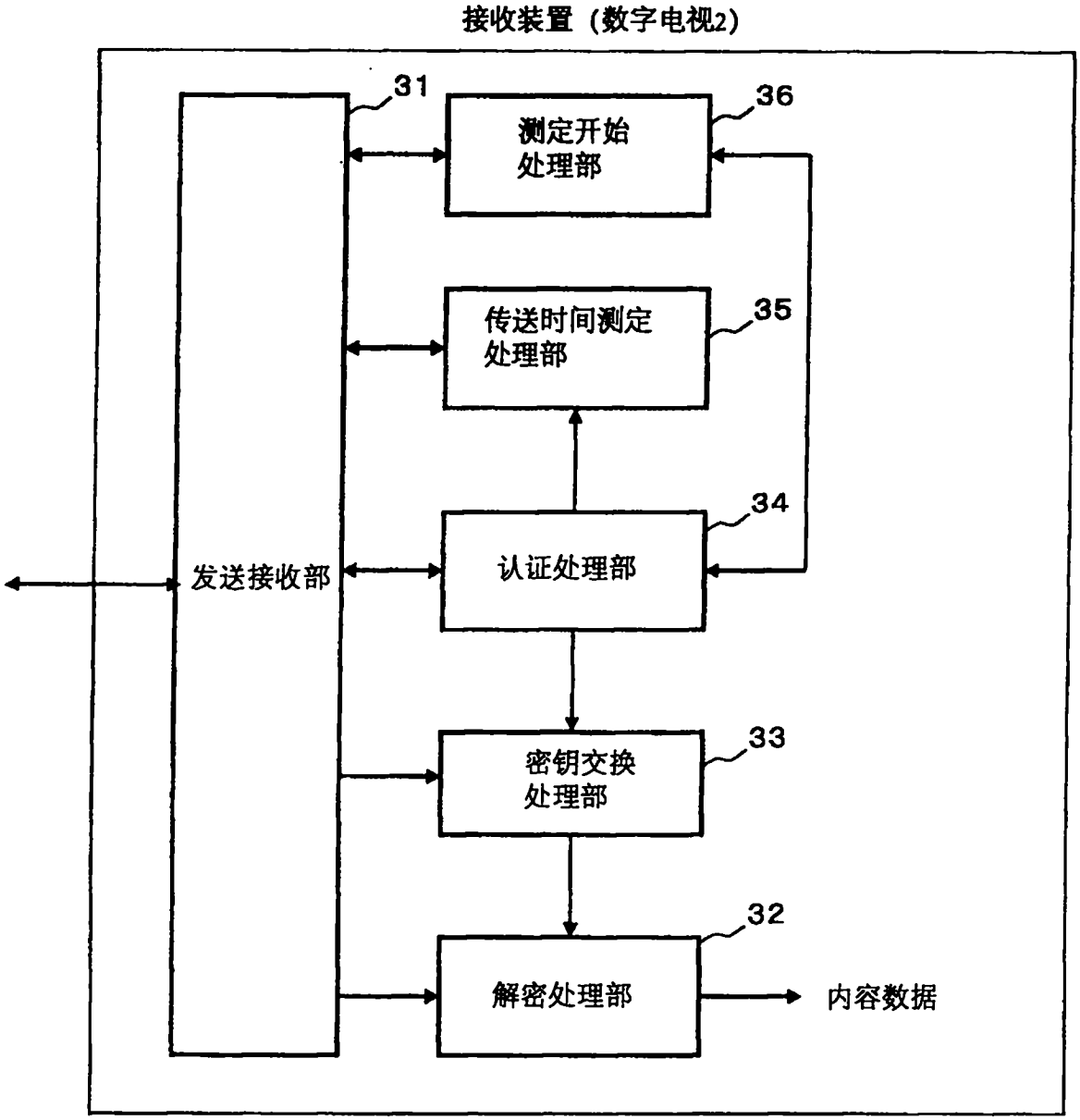

接收装置（数字电视2）
31
测定开始
处理部
36
传送时间测定
处理部
35
34
发送接收部
认证处理部
密钥交换
处理部
33
32
解密处理部
内容数据

图 7

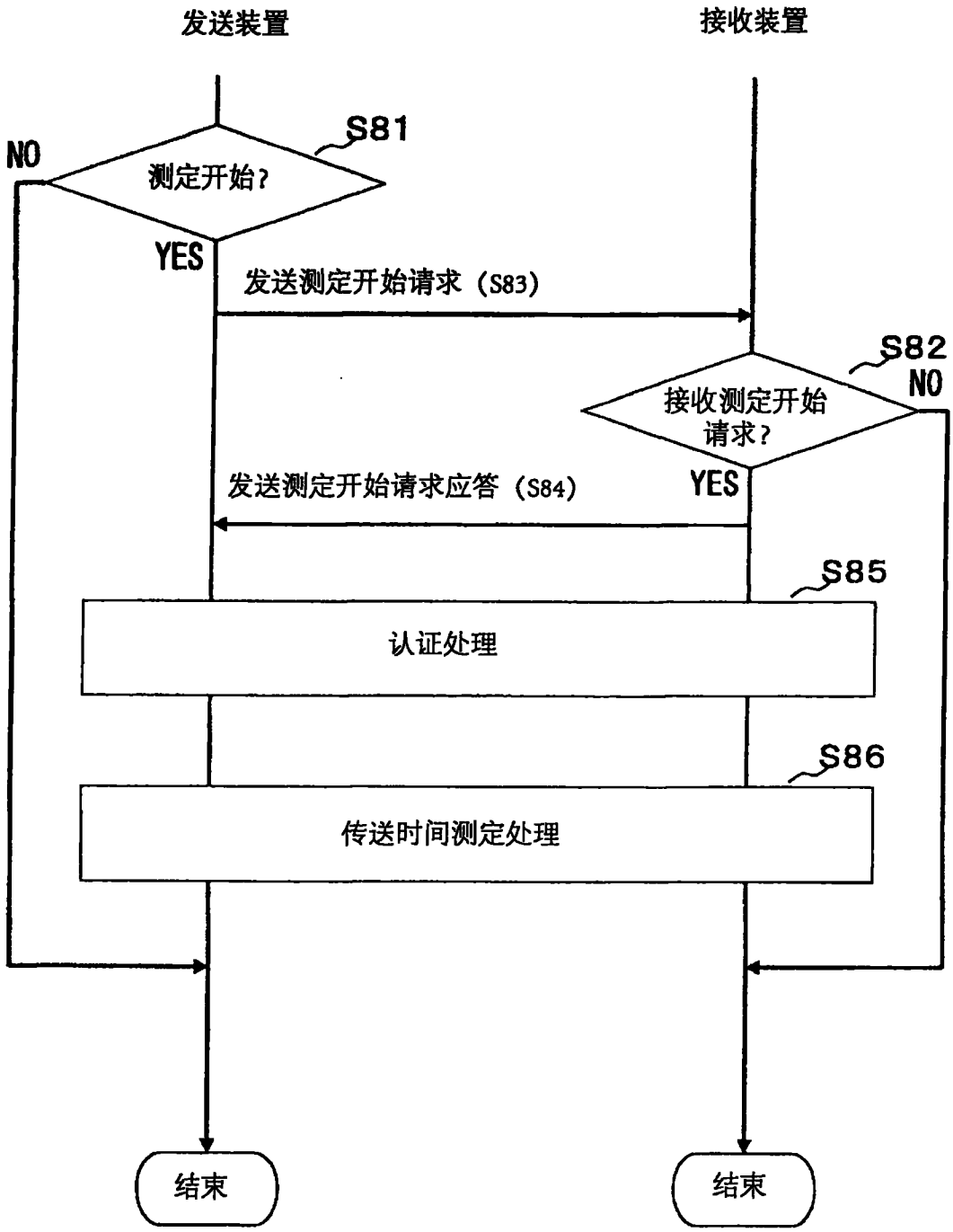

发送装置
接收装置
S81
NO
测定开始?
YES
发送测定开始请求（S83）
S82
NO
接收测定开始请求?
YES
发送测定开始请求应答（S84）
S85
认证处理
S86
传送时间测定处理
结束
结束

图 8

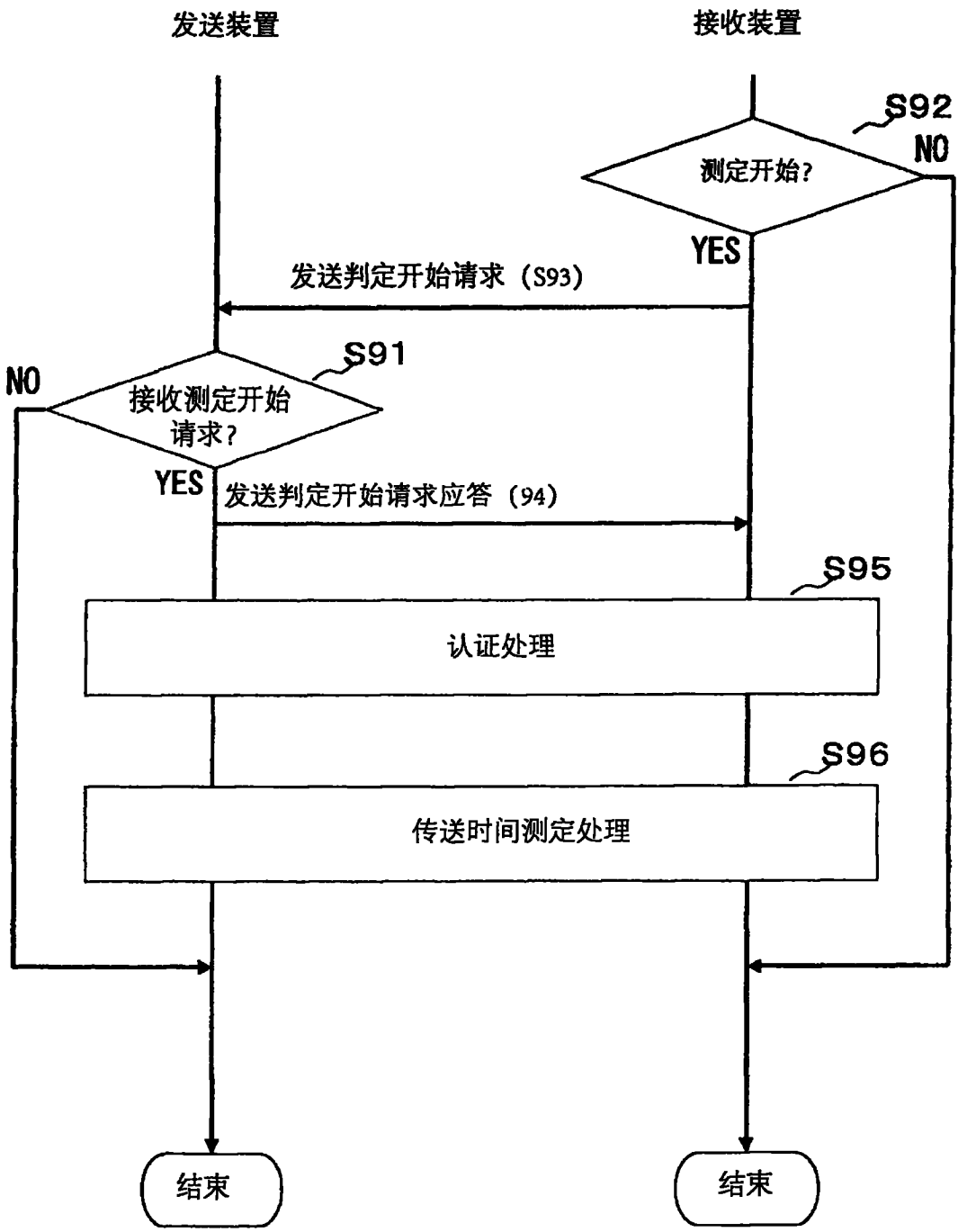

发送装置
接收装置
S92
测定开始?
NO
YES
发送判定开始请求（S93）
S91
NO
接收测定开始请求?
YES
发送判定开始请求应答（94）
S95
认证处理
S96
传送时间测定处理
结束
结束

图 9

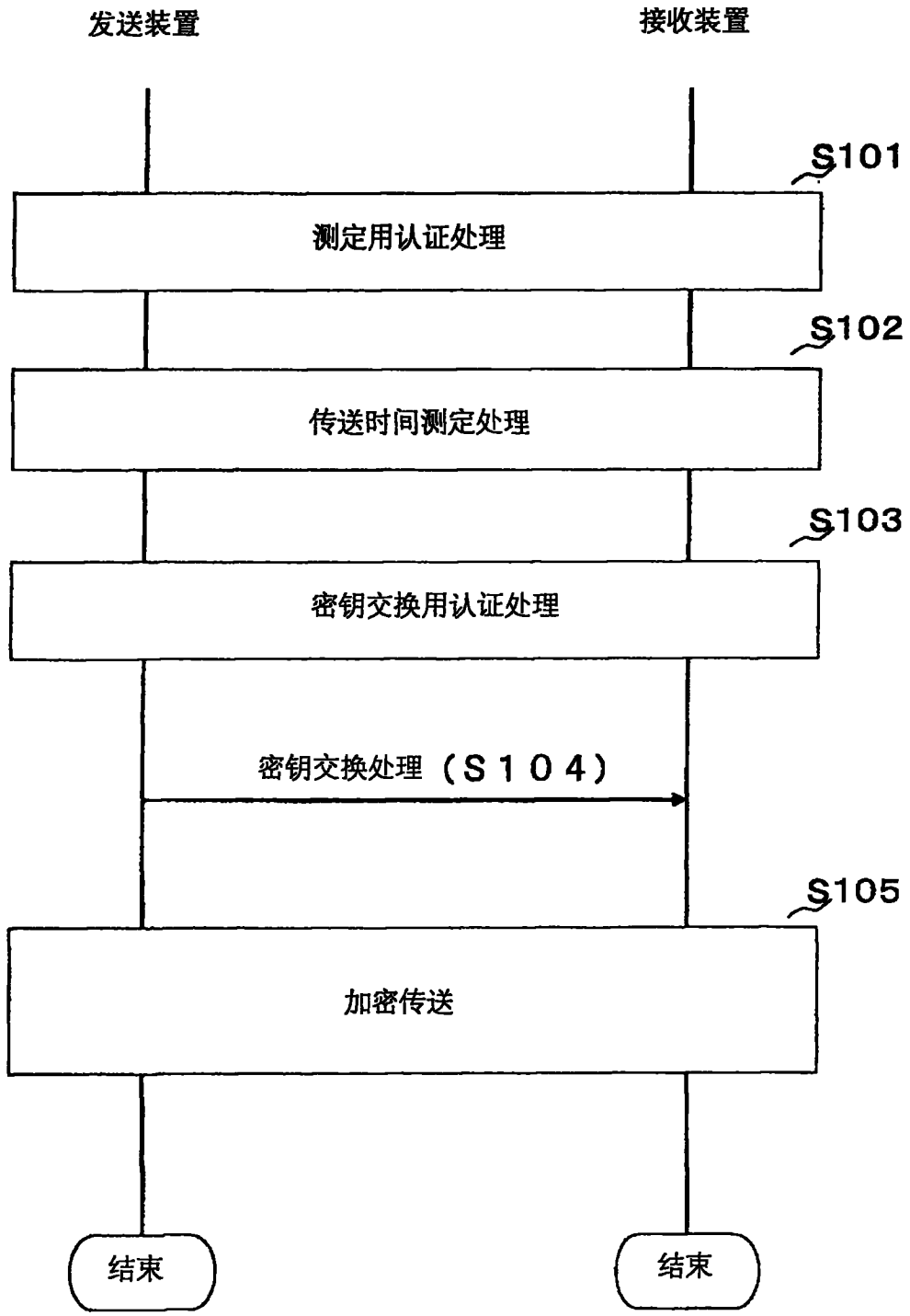

发送装置
接收装置
S101
测定用认证处理
S102
传送时间测定处理
S103
密钥交换用认证处理
密钥交换处理（S104）
S105
加密传送
结束
结束

图 10

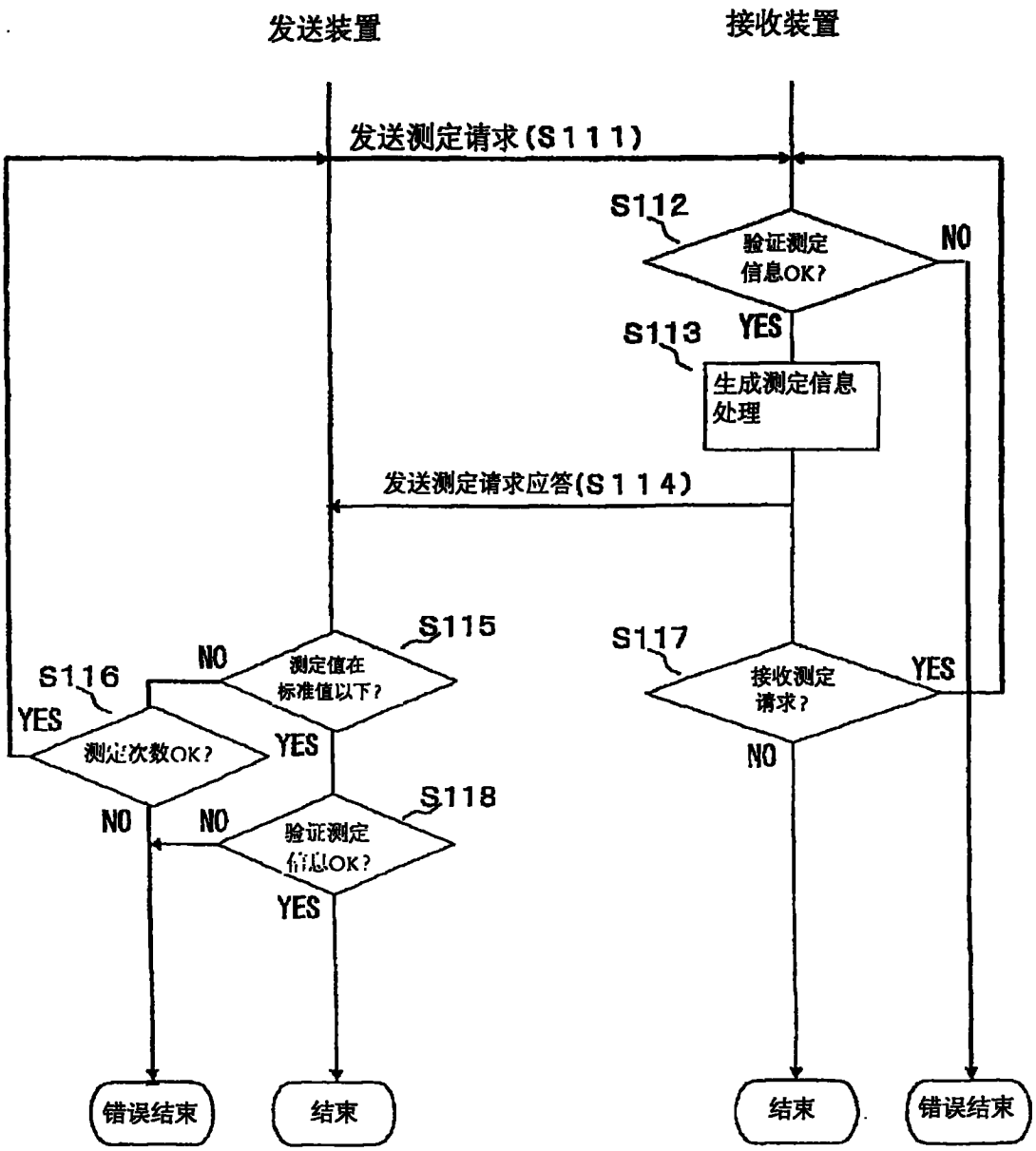

发送装置
接收装置
发送测定请求(S111)
S112
验证测定信息OK?
NO
YES
S113
生成测定信息处理
发送测定请求应答(S114)
S115
测定值在标准值以下?
NO
YES
S116
测定次数OK?
YES
NO
S117
接收测定请求?
YES
NO
S118
验证测定信息OK?
NO
YES
错误结束
结束
结束
错误结束

图 11