(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 1753359 B
(45)授权公告日 2011.01.19

(21)申请号 200410080190.9

(22)申请日 2004.09.24

(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 田林一

(51)Int.Cl.
H04L 9/12(2006.01)
H04L 9/14(2006.01)
H04L 7/00(2006.01)

(56)对比文件
US 2003154298 A1,2003.08.14, 全文.
EP 1418713 A1,2004.05.12, 全文.
CN 1305285 A,2001.07.25, 全文.
WO 2004038546 A2,2004.05.06, 全文.
US 2002081995 A1,2002.06.27, 全文.
宋绮虹, 刘宏.SyncML同步协议分析. 电信快报 7.2003,(7),33-35.
SyncML Representation Protocol,version 1.1.2002,10-11.
苏洁,赵仁波.PKI技术在网络信息传输安全上的应用研究. 信息技术28 3.2004,28(3),40-42.

审查员 刘俭

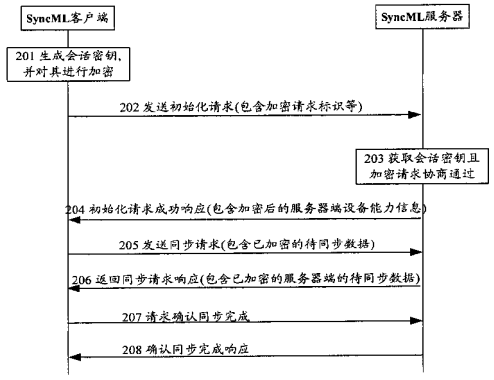
权利要求书 2 页 说明书 7 页 附图 2 页

(54)发明名称

实现传输SyncML同步数据的方法

(57)摘要

本发明提供了实现传输SyncML同步数据的方法,一种是发送端对待传输的用户数据加密后构造SyncML消息,然后按现有方式实现传输;所述的用户数据包括但不限于认证信息,终端能力信息以及待同步数据;另一种是发送端在传输层对该待传输的SyncML消息进行加密后再传输,接收端对接收到的传输层的SyncML消息解密后再进行后续处理,两种方法可单独使用也可以一起使用。如果一起使用,则为SyncML同步数据的传输提供了双层的安全保障。使用本发明,保证了用户数据的安全传输,避免被第三方窃取。



CN 1753359 B

1. 一种实现传输 SyncML 同步数据的方法，其特征在于，该方法包括以下步骤：

a、SyncML 服务器接收到来自 SyncML 客户端的同步初始化请求后，判断该请求中是否有请求加密标识，如果没有，SyncML 服务器给 SyncML 客户端返回失败原因为服务器要求加密而终端没有发送加密请求的同步初始化请求失败响应，如果有，SyncML 服务器进一步判断自身是否支持同步初始化请求中的会话密钥所要求的算法类型和密钥长度，如果不支持，SyncML 服务器给 SyncML 客户端返回失败原因为服务器不支持该密钥的同步初始化请求失败响应，如果支持，则 SyncML 服务器获取同步初始化请求中的 SyncML 客户端生成的会话密钥，并且，SyncML 服务器和 SyncML 客户端之间进行初始化操作；

b、SyncML 客户端向 SyncML 服务器发送使用会话密钥加密后的待同步数据，SyncML 服务器接收到该待同步数据后首先使用会话密钥进行解密，然后再进行同步处理操作，之后，使用会话密钥加密 SyncML 服务器端的待同步数据，再将加密后待同步数据发送给 SyncML 客户端；

c、SyncML 客户端接收到来自 SyncML 服务器的待同步数据后，先使用会话密钥进行解密，然后再进行同步处理操作，之后，判断是否还有待同步数据，如果有，则重复执行步骤 b，否则执行步骤 d；

d、SyncML 客户端向 SyncML 服务器发送同步完成请求，并接收到来自 SyncML 服务器的同步完成确认请求后，结束本流程。

2. 根据权利要求 1 所述的方法，其特征在于，该方法进一步包括：所述 SyncML 服务器使用自身保存的私钥对同步初始化请求中已经公钥加密后的会话密钥进行解密，获取客户端生成的会话密钥，然后再执行所述进一步判断自身是否支持同步初始化请求中的会话密钥所要求的算法类型和密钥长度。

3. 根据权利要求 2 所述的方法，其特征在于，所述 SyncML 客户端加密用的公钥是 SyncML 服务器证书的公钥，所述 SyncML 客户端使用的 SyncML 服务器端证书是预装或预先从网络侧下载后安装的，或者是与 SyncML 服务器交互后得到的。

4. 根据权利要求 1 所述的方法，其特征在于，步骤 a 所述 SyncML 服务器和 SyncML 客户端之间进行初始化操作的过程包括以下步骤：

a001、所述 SyncML 服务器接收到来自 SyncML 客户端的包含已加密的用于初始化的用户数据后，使用已获取的会话密钥对该用户数据进行解密，并执行初始化操作，之后，向 SyncML 客户端发送同步初始化响应，该响应中包含 SyncML 服务器成功接受会话密钥的信息和使用会话密钥加密后的自身设备能力信息；

a002、SyncML 客户端接收到步骤 a001 所述响应，判断出 SyncML 服务器已成功接受会话密钥后，使用自身生成的会话密钥对服务器的设备能力信息进行解密，并执行初始化操作。

5. 根据权利要求 1 所述的方法，其特征在于，步骤 a 所述 SyncML 服务器和 SyncML 客户端之间进行初始化操作的过程包括以下步骤：

a01、所述 SyncML 服务器接收到来自 SyncML 客户端的包含未加密的用于初始化的用户数据后，执行初始化操作，之后，向 SyncML 客户端发送同步初始化响应，该响应中包含服务器成功接受会话密钥的信息和未加密的自身设备能力信息；

a02、SyncML 客户端接收到步骤 a01 所述响应，判断出 SyncML 服务器已成功接受会话密钥后，根据 SyncML 服务器的设备能力信息执行初始化操作。

6. 根据权利要求 4 或 5 所述的方法，其特征在于，所述用于初始化的用户数据包括认证信息和 SyncML 客户端设备的能力信息；所述认证信息至少包括用户名和密码。

7. 根据权利要求 1 所述的方法，其特征在于，SyncML 客户端接收到来自 SyncML 服务器的同步初始化请求失败响应后，判断自身是否能够满足失败原因所需的条件，如果能，则重新向 SyncML 服务器发送同步初始化请求，该请求中包含失败原因所对应的条件，否则，终止向 SyncML 服务器发送同步初始化请求，结束本流程。

8. 根据权利要求 1 所述的方法，其特征在于，所述 SyncML 客户端发送的同步初始化请求中的请求加密标识以标签的形式承载，且该标识中表明会话公钥所需的算法类型及密钥长度。

9. 根据权利要求 1 所述的方法，其特征在于，所述会话密钥为对称密钥或非对称密钥。

10. 根据权利要求 1 所述的方法，其特征在于，该方法进一步包括：

A、发送端构造好待发送的 SyncML 信息后，将该待送的 SyncML 消息转换为传输层协议的请求，并使用安全传输协议对该请求加密后，传送至接收端；

B、接收端接收到步骤 A 所述请求后，使用安全传输协议对接收到的请求进行解密，再将该解密后的传输层协议请求转换为 SyncML 消息，并进行后续处理。

11. 根据权利要求 10 所述的方法，其特征在于，所述发送端为 SyncML 客户端，所述接收端为 SyncML 服务器，或者，所述发送端为 SyncML 服务器，所述接收端为 SyncML 客户端。

12. 根据权利要求 10 所述的方法，其特征在于，所述传输层协议为超文本传输协议、无线会话协议或对象交换协议。

13. 根据权利要求 10 所述的方法，其特征在于，如果所述 SyncML 客户端为移动终端，则所使用安全传输协议为无线传输层安全性协议，如果所述 SyncML 客户端为固定终端，则所使用安全传输协议为安全套接层协议或传输层安全性协议。

实现传输 SyncML 同步数据的方法

技术领域

[0001] 本发明涉及开放移动联盟定义的无线数据同步规范 (SyncML) 技术领域，特别是指实现传输 SyncML 同步数据的方法。

背景技术

[0002] 开发 SyncML 的目的在于，使终端用户、设备开发商、基础构件开发商、数据提供商、使用软件开发商以及服务提供商协同工作，真正实现使用任何终端设备均可随时随地访问任何网络数据。SyncML 的典型应用是移动设备和网络服务之间的数据同步。除此之外，SyncML 还可用于对等的数据同步，如两台 PC 之间。现有技术的 SyncML 同步数据的交换的方法如图 1 所示。

[0003] 图 1 所示为现有技术的实现 SyncML 同步传输的流程示意图。

[0004] 步骤 101 ～步骤 102，SyncML 客户端向 SyncML 服务器发起同步初始化请求，请求服务器进行认证；该同步初始化请求中包括认证信息以及自身的设备能力信息，认证信息中包含用户名和密码；SyncML 服务器接收到该认证请求后，执行初始化操作，并返回认证结果和服务器端的能力信息，SyncML 客户端根据服务器端的能力信息执行初始化操作。至此，初始化完成。上述初始化操作包括对用户信息进行认证、指明要同步的数据库等。

[0005] 上述步骤为流程中的初始化阶段，其主要完成客户端和服务器的相互认证、协商双方的设备能力，如支持的同步类型、数据库等，以及协商待同步的数据库。

[0006] 步骤 103 ～步骤 104，SyncML 客户端发送同步请求到服务器，该同步请求中包含待同步的数据，服务器接收到该请求后，进行同步处理，然后向客户端发送同步请求响应，该响应中包含服务器端待同步的数据。

[0007] 客户端接收到该响应后，进行同步处理，之后，如果还有未处理的待同步数据，重复执行步骤 103 和步骤 104，至所有待同步数据处理完毕。

[0008] 上述步骤为流程中的同步阶段，其主要完成客户端和服务器的之间的数据交换以实现数据同步。

[0009] 步骤 105 ～步骤 106，SyncML 客户端向服务器发送请求确认同步完成信息，服务器确认完成后，向客户端返回确认同步完成的信息。

[0010] 上述步骤为流程中的同步完成阶段，其主要用于客户端和服务器的之间相互确认完成信息。

[0011] 在上述同步交换流程中，初始化阶段时，SyncML 客户端向服务器发送认证信息可以采用明文进行发送，也可以采用 base64 编码或 MD5 加密的方式进行发送，其余的数据，包括客户端和服务器的设备能力信息、待同步数据等均采用明文的方式发送。

[0012] SyncML 客户端和 SyncML 服务器之间的 SyncML 同步数据超文本传输协议 (HTTP)、无线会话协议 (OBEX) 或对象交换协议 (WSP) 等协议的支持下实现传输，虽然 SyncML 协议对使用的传输层协议进行了一些约束，但都不涉及传输安全方面。

[0013] 现有的实现传输 SyncML 同步数据的方法有以下缺陷：

[0014] 1) 客户端所发送的认证信息的方式不安全，认证信息易被第三方窃取。这是因为，采用明文的方式，被截取后可直接获得，采用 BASE64 编码方式，被截取后很容易解码。在 2004 年 8 月份美国加州举行的国际密码学会议上已证实 MD5 加密的方式可破解，这样，即使采用 MD5 加密的方式，被截取后也可以破解，也不十分安全，而且现在市场上大多数设备都不支持该种加密的认证方式。

[0015] 2) 对所传输的待同步数据没有任何保护措施。

[0016] 3) 对于传输层中的数据没有任何保护措施。

发明内容

[0017] 有鉴于此，本发明的目的在于提供实现传输 SyncML 同步数据的方法，保证用户数据的安全传输，避免被第三方窃取。

[0018] 为达到上述目的，本发明的技术方案是这样实现的：

[0019] 一种实现传输 SyncML 同步数据的方法，该方法包括以下步骤：

[0020] a、SyncML 服务器接收到来自 SyncML 客户端的同步初始化请求后，判断该请求中是否有请求加密标识，如果没有，SyncML 服务器给 SyncML 客户端返回失败原因为服务器要求加密而终端没有发送加密请求的同步初始化请求失败响应，如果有，SyncML 服务器进一步判断自身是否支持同步初始化请求中的会话密钥所要求的算法类型和密钥长度，如果不支持，SyncML 服务器给 SyncML 客户端返回失败原因为服务器不支持该密钥的同步初始化请求失败响应，如果支持，则 SyncML 服务器获取同步初始化请求中的 SyncML 客户端生成的会话密钥，并且，SyncML 服务器和 SyncML 客户端之间进行初始化操作；

[0021] b、SyncML 客户端向 SyncML 服务器发送使用会话密钥加密后的待同步数据，SyncML 服务器接收到该待同步数据后首先使用会话密钥进行解密，然后再进行同步处理操作，之后，使用会话密钥加密 SyncML 服务器端的待同步数据，再将加密后待同步数据发送给 SyncML 客户端；

[0022] c、SyncML 客户端接收到来自 SyncML 服务器的待同步数据数据后，先使用会话密钥进行解密，然后再进行同步处理操作，之后，判断是否还有待同步数据，如果有，则重复执行步骤 b，否则执行步骤 d；

[0023] d、SyncML 客户端向 SyncML 服务器发送同步完成请求，并接收到来自 SyncML 服务器的同步完成确认请求后，结束本流程。

[0024] 较佳地，该方法进一步包括：所述 SyncML 服务器使用自身保存的私钥对同步初始化请求中已经公钥加密后的会话密钥进行解密，获取客户端生成的会话密钥，然后再执行所述进一步判断自身是否支持同步初始化请求中的 会话密钥所要求的算法类型和密钥长度。

[0025] 较佳地，所述 SyncML 客户端加密用的公钥是 SyncML 服务器证书的公钥，所述 SyncML 客户端使用的 SyncML 服务器端证书是预装或预先从网络侧下载后安装的，或者是与 SyncML 服务器交互后得到的。

[0026] 较佳地，步骤 a 所述 SyncML 服务器和 SyncML 客户端之间进行初始化操作的过程包括以下步骤：

[0027] a001、所述 SyncML 服务器接收到来自 SyncML 客户端的包含已加密的用于初始化

的用户数据后，使用已获取的会话密钥对用于初始化的用户数据进行解密，并执行初始化操作，之后，向 SyncML 客户端发送同步初始化响应，该响应中包含 SyncML 服务器成功接受会话密钥的信息和使用会话密钥加密后的自身设备能力信息；

[0028] a002、SyncML 客户端接收到步骤 a001 所述响应，判断出 SyncML 服务器已成功接受会话密钥后，使用自身生成的会话密钥对服务器的设备能力信息进行解密，并执行初始化操作。

[0029] 较佳地，步骤 a 所述 SyncML 服务器和 SyncML 客户端之间进行初始化操作的过程包括以下步骤：

[0030] a01、所述 SyncML 服务器接收到来自 SyncML 客户端的包含未加密的用于初始化的用户数据后，执行初始化操作，之后，向 SyncML 客户端发送同步初始化响应，该响应中包含服务器成功接受会话密钥的信息和未加密的自身设备能力信息；

[0031] a02、SyncML 客户端接收到步骤 a01 所述响应，判断出 SyncML 服务器已成功接受会话密钥后，根据 SyncML 服务器的设备能力信息执行初始化操作。

[0032] 较佳地，所述用于初始化的用户数据包括认证信息和 SyncML 客户端设备的能力信息；所述认证信息至少包括用户名和密码。

[0033] 较佳地，SyncML 客户端接收到来自 SyncML 服务器的同步初始化请求 失败响应后，判断自身是否能够满足失败原因所需的条件，如果能，则重新向 SyncML 服务器发送同步初始化请求，该请求中包含失败原因所对应的条件，否则，终止向 SyncML 服务器发送同步初始化请求，结束本流程。

[0034] 较佳地，所述 SyncML 客户端发送的同步初始化请求中的请求加密标识以标签的形式承载，且该标识中表明会话公钥所需的算法类型及密钥长度。

[0035] 较佳地，所述会话密钥为对称密钥或非对称密钥。

[0036] 较佳地，该方法进一步包括：

[0037] A、发送端构造好待发送的 SyncML 信息后，将该待发送的 SyncML 消息转换为传输层协议的请求，并使用安全传输协议对该请求加密后，传送至接收端；

[0038] B、接收端接收到步骤 A 所述请求后，使用安全传输协议对接收到的请求进行解密，再将该解密后的传输层协议请求转换为 SyncML 消息，并进行后续处理。

[0039] 较佳地，所述发送端为 SyncML 客户端，所述接收端为 SyncML 服务器，或者，所述发送端为 SyncML 服务器，所述接收端为 SyncML 客户端。

[0040] 较佳地，所述传输层协议为超文本传输协议、无线会话协议或对象交换协议。

[0041] 较佳地，如果所述 SyncML 客户端为移动终端，则所使用安全传输协议为无线传输层安全性协议，如果所述 SyncML 客户端为固定终端，则所使用安全传输协议为安全套接层协议或传输层安全性协议。

[0042] 本发明中，SyncML 服务器获取 SyncML 客户端生成的会话密钥，并且，SyncML 服务器和 SyncML 客户端之间的初始化操作完毕后；发送端将待同步数据使用会话密钥加密后发送给接收端；接收端首先使用会话密钥进行解密，然后再进行同步处理操作，之后再将自身的待同步数据使用会话密钥加密后发送给对端，如此反复，至所有待同步数据处理完毕为止。最后，SyncML 客户端与 SyncML 服务器之间确认完成后，结束本流程。使用本发明，保证 了用户数据的安全传输，不被第三方窃取，而且满足了要求加密的使用需求，同时，最

大程度上保证了 SyncML 体系架构的完整性和合理性。

[0043] 而且，SyncML 客户端可使用服务器端证书中的公钥将会话密钥加密后再发送给 SyncML 服务器，而 SyncML 服务器则使用自身的私有解密后，才能获取客户端生成的会话密钥。使用证书机制，保证了和客户端通信的服务器是可信任的，解决了信任问题，同时，利用非对称加密技术很好地解决了密钥的安全传输问题。使得每次同步操作均可以使用不同的会话密钥，极大地提高了密钥的安全性，同时也极大保证了用户数据的安全性。

[0044] 另外，用于对用户数据进行加密的会话密钥，可以为任何算法，如高级加密标准 (AES) 加密算法、基于 RC4 的加密算法或者其他对称加密算法等，其能够被大部分终端（包括但不限于手机、PDA、智能手机、PC 客户端等）支持。而且，由于加密算法实现的简单性，能够很好地在仅有有限的内存和处理能力的终端上运行。同时，加密算法的类型可扩展，密钥的长度可以设置，可针对不同的应用场景提供不同的安全级别。

[0045] 再有，本发明对 SyncML 同步数据的传输层也进行了安全约束，保证了 SyncML 同步数据在传输层的安全。而且，对传输层的加密和对用户数据的加密可同时使用，为 SyncML 同步数据的传输提供了双层的安全保障。

[0046] 附图说明

[0047] 图 1 所示为现有技术的实现 SyncML 同步传输的流程示意图；

[0048] 图 2 所示为使用本发明一实施例的实现 SyncML 同步传输的流程示意图；

[0049] 图 3 所示为使用本发明的实现 SyncML 同步时传输层的处理流程示意图。

[0050] 具体实施方式

[0051] 下面结合附图对本发明再做进一步地详细说明。

[0052] 本发明主要提供了两种传输方式，一种是发送端对待传输的用户数据加密后再构造 SyncML 消息，按现有方式实现传输；所述的用户数据包括但不限于认证信息，终端能力信息以及待同步数据；另一种方式是发送端在传输层对该待传输的 SyncML 消息进行加密后，再传输，接收端对接收到的传输层的 SyncML 消息解密后再进行后续处理。

[0053] 下面首先说明对待传输的用户数据加密后再构造 SyncML 消息，然后按现有方式实现传输的方法。

[0054] 图 2 所示为使用本发明一实施例的实现 SyncML 传输的流程示意图。在本实施例中，SyncML 服务器端要求来自客户端用户数据是加密的，且 SyncML 客户端已预装或从网络侧下载服务器端的证书，该证书为非对称密钥，其中的公钥用于客户端加密，其中的私钥用于服务器端解密，而 SyncML 服务器端认为请求接入的客户端是可信的，不要求客户端的证书。

[0055] 步骤 201，SyncML 客户端确认自身已安装服务器端的证书，且该证书处于有效期内后，生成用于加密用户数据的会话密钥，使用服务器端证书的公钥加密已生成的会话密钥，使用已生成的会话密钥加密待传送的用于初始化的用户数据，如，认证信息和客户端自身的设备信息等，其中，认证信息中包括用户名和密码。

[0056] 在本实施例中，上述 SyncML 客户端自身生成用于加密用户数据的会话密钥为对称密钥，其算法可采用高级加密标准 (AES) 加密算法、基于 RC4 的加密算法或者其他对称加密算法。当然，在实际应用中，会话密钥的算法并不限于此，现有的加密算法都可在此实施。

[0057] 当然，也可以不对会话密钥进行加密，而直接将会话密钥发送给 SyncML 服务器，

只是这种方式易被第三方获取，不够安全。

[0058] 步骤 202，SyncML 客户端向 SyncML 服务器发送同步初始化请求，该请求中包含有请求加密标识，经服务器端证书的公钥加密后的会话密钥和经会话密钥加密后的待传送初始化数据。上述请求加密标识以标签的形式承载 在同步初始化请求中，且该标识中表明会话公钥所需的算法类型及密钥长度。

[0059] 步骤 203，SyncML 服务器接收到来自客户端的同步初始化请求，判断出有加密请求标识后，使用自身的私钥对会话标识进行解密，并根据自身的配置判断自身是否支持该会话密钥，即是否支持该会话密钥所要求的算法类型，以及密钥长度，如果支持，则继续执行步骤 204，否则，给 SyncML 客户端返回包含失败原因的同步初始化请求响应，结束本流程。该失败原因中指明 SyncML 服务器不支持该会话密钥，即不支持该会话密钥所要求的算法类型和或密钥长度，同时，还可进一步指明自身所要求的算法类型和或密钥长度。

[0060] 在本步骤中，如果 SyncML 服务器判断出来自客户端的同步初始化请求中没有加密请求标识时，直接向 SyncML 客户端返回包含失败原因的同步初始化请求响应，该失败原因为服务器要求加密而终端没有发送加密请求，且该响应中还可进一步包含 SyncML 服务器支持的算法类型和密钥长度等信息。

[0061] 如果 SyncML 客户端接收到来自 SyncML 服务器的同步初始化请求失败响应，则判断自身是否能够满足失败原因所需的条件，如果能，则重新向 SyncML 服务器发送同步初始化请求，该请求中包含失败原因所对应的条件，否则，终止向 SyncML 服务器发送同步初始化请求，结束本流程。

[0062] 步骤 204，SyncML 服务器继续执行初始化操作，即使用接收到的会话密钥对来自客户端的用于初始化的用户数据进行解密，并应用解密后的用户数据继续后续处理，之后，给客户端返回成功的同步初始化请求响应，该响应中包含服务器成功接收会话密钥的信息，以及使用该会话密钥对自身的设备能力进行加密后的信息。

[0063] SyncML 客户端接收到上述所述响应后，使用自身生成的会话密钥对服务器端的设备能力信息进行解密，然后根据得到的服务器的能力信息继续执 行初始化操作。

[0064] 至此，同步初始化阶段结束。

[0065] 步骤 205，SyncML 客户端使用自身生成的会话密钥对待同时数据进行加密，然后向服务器发送同步请求，该同步请求中包含已加密的待同步数据。

[0066] 步骤 206，SyncML 服务器接收到步骤 205 所述请求后，首先使用会话密钥对待同步数据进行解密，之后进行同步处理，然后向客户端发送同步请求响应，该同步请求响应中包含使用会话密钥加密的服务器端的待同步数据。

[0067] SyncML 客户端收到步骤 206 所述响应后，同样首先使用会话密钥对待同步数据进行解密，之后进行同步处理，如果还有待同步数据则重复执行步骤 205 及步骤 206，直到所有待同步数据全部处理完毕为止，同步阶段结束。如果没有待同步数据，则执行步骤 207，进入同步完成阶段。

[0068] 步骤 207 ～步骤 208，SyncML 客户端向服务器发送请求确认同步完成信息，服务器确认后，向客户端返回确认同步完成的信息。

[0069] 至此，SyncML 同步数据传输完成。SyncML 客户端和 SyncML 服务器之间的 SyncML 同步数据在 HTTP、OBEX 或 WSP 等协议的支持下实现传输，其在传输层的传输方式与现有技

术相同。

[0070] 针对上述实施例，也可以只使用会话密钥对待同步数据进行加密，而不对初始化数据进行加密。此时，步骤 202 中 SyncML 客户端向 SyncML 服务器发送的同步初始化请求中，包含请求加密标识，经服务器端证书的公钥加密后的会话密钥和未加密的初始化数据，步骤 203 中 SyncML 服务器接收到来自客户端的同步初始化请求，且判断出自身支持该会话密钥，直接执行初始化操作，之后，向 SyncML 客户端发送同步初始化响应，该响应中包含服务器成功接受会话密钥的信息和未加密的自身设备能力信息；相应地，SyncML 客户端接收到上述所述响应，判断出 SyncML 服务器已成功接受会话密钥后，根据 SyncML 服务器的设备能力信息执行初始化操作。

[0071] 针对上述实施例，SyncML 客户端也可以不通过预装或下载而获取服务器端的证书，而是在发送同步初始化请求之前，直接向服务器发送请求服务器端证书信息。当然，服务器端也可以认为客户端是不可信的，而要求客户端的证书，此时，会话密钥也可以是非对称密钥。

[0072] 以上所述实施例中，SyncML 服务器端是要求来自客户端的用户数据加密的。如果 SyncML 服务器端不支持来自客户端的用户数据加密，则当 SyncML 服务器接收到的来自客户端的包含加密信息的同步初始化请求时，向 SyncML 客户端返回失败原因为要求客户端发送不包含加密标识的失败的初始化响应；相应地，SyncML 客户端接收到来自 SyncML 服务器的同步初始化请求失败响应，则判断自身是否能够满足失败原因所需的条件，如果能，则重新向 SyncML 服务器发送同步初始化请求，该请求中包含失败原因所对应的条件，否则，终止向 SyncML 服务器发送同步初始化请求，结束本流程。如果 SyncML 服务器接收到来自客户端的未包含加密信息的同步初始化请求，则与现有处理方式完全相同。

[0073] 以上所述实施例中，SyncML 服务器给 SyncML 客户端返回的响应中的状态信息以状态码的方式进行标识，具体某一状态码代表哪个信息可在实际应用中根据需要指定，在此不做限制。以上实施例中的密钥所采用的算法类型，可为现有的任一种对称算法类型。

[0074] 下面说明在传输层加密后实现传输的方法。

[0075] 图 3 所示为使用本发明的对传输层进行加密处理后实现传输 SyncML 同步数据的流程示意图。在本实施例中，使用 HTTP 协议作为传输层的传送协议。

[0076] 步骤 301，发送端构造好待发送的 SyncML 消息后，将待送的 SyncML 消息转换为 HTTP 请求。

[0077] 步骤 302，发送端使用安全传输协议对步骤 301 所述 HTTP 请求加密后，再传输该加密后的 HTTP 请求至接收端。

[0078] 步骤 303，接收端接收到步骤 302 所述请求后，使用安全传输协议对该请求进行解密，将该解密后的 HTTP 请求转换为 SyncML 消息，再并进行后续处理。

[0079] 上述仅以 SyncML 的传输层使用 HTTP 协议为例进行说明，其传输层还可以使用 OBEX 或 WSP 等协议。上述述发送端为 SyncML 客户端，接收端为 SyncML 服务器，或者，上述发送端为 SyncML 服务器，接收端为 SyncML 客户端。

[0080] 如果 SyncML 客户端为移动终端，如手机，则所使用安全传输协议为无限传输层安全性 (WTLS) 协议，如果 SyncML 客户端为固定终端，如 PC 客户端，则所使用安全传输协议为安全套接层 (SSL) 协议或传输层安全性 (TLS) 协议。

[0081] 上述对传输层的数据进行加密的传输方式即可以单独使用，也可以与对待传输的用户数据加密后再构造 SyncML 消息，然后按现有方式实现传输的方法一起使用。如果一起使用，则为 SyncML 同步数据的传输提供了双层的安全保障。

[0082] 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、改进等，均应包含在本发明的保护范围之内。

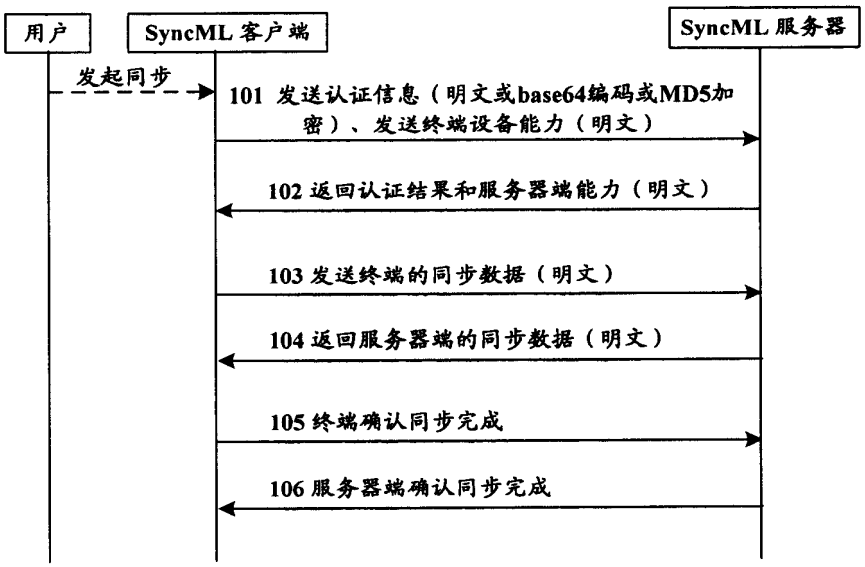

用户
SyncML 客户端
SyncML 服务器
发起同步
101 发送认证信息（明文或base64编码或MD5加密）、发送终端设备能力（明文）
102 返回认证结果和服务器端能力（明文）
103 发送终端的同步数据（明文）
104 返回服务器端的同步数据（明文）
105 终端确认同步完成
106 服务器端确认同步完成

图 1

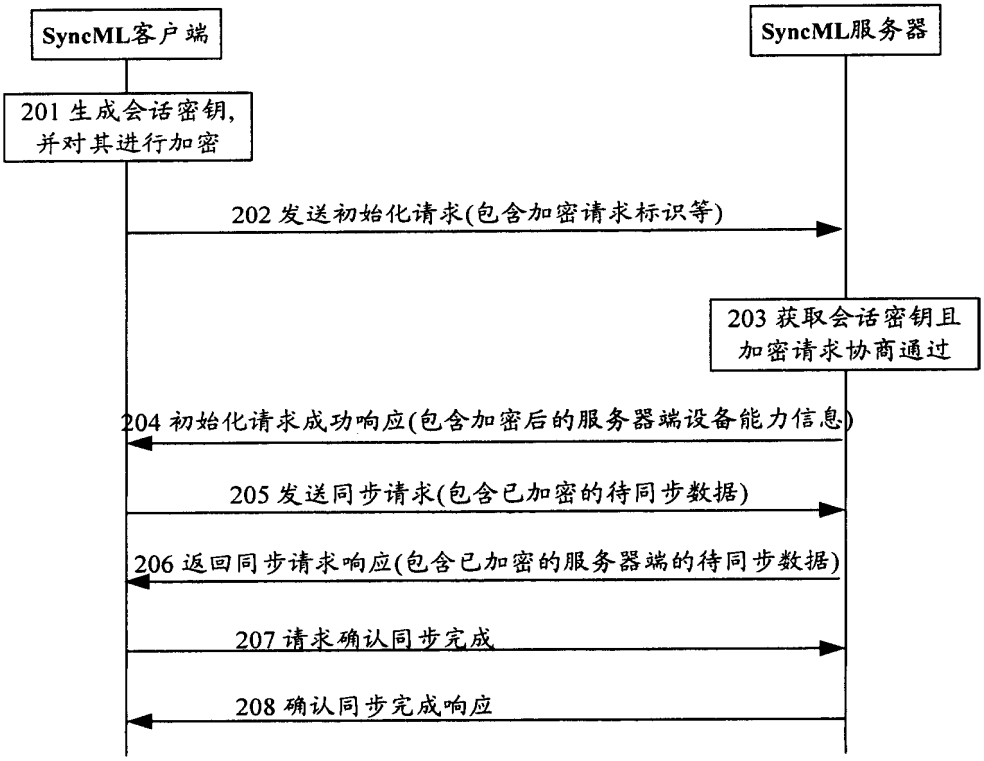

SyncML客户端
SyncML服务器
201 生成会话密钥，并对其进行加密
202 发送初始化请求(包含加密请求标识等)
203 获取会话密钥且加密请求协商通过
204 初始化请求成功响应(包含加密后的服务器端设备能力信息)
205 发送同步请求(包含已加密的待同步数据)
206 返回同步请求响应(包含已加密的服务器端的待同步数据)
207 请求确认同步完成
208 确认同步完成响应

图 2

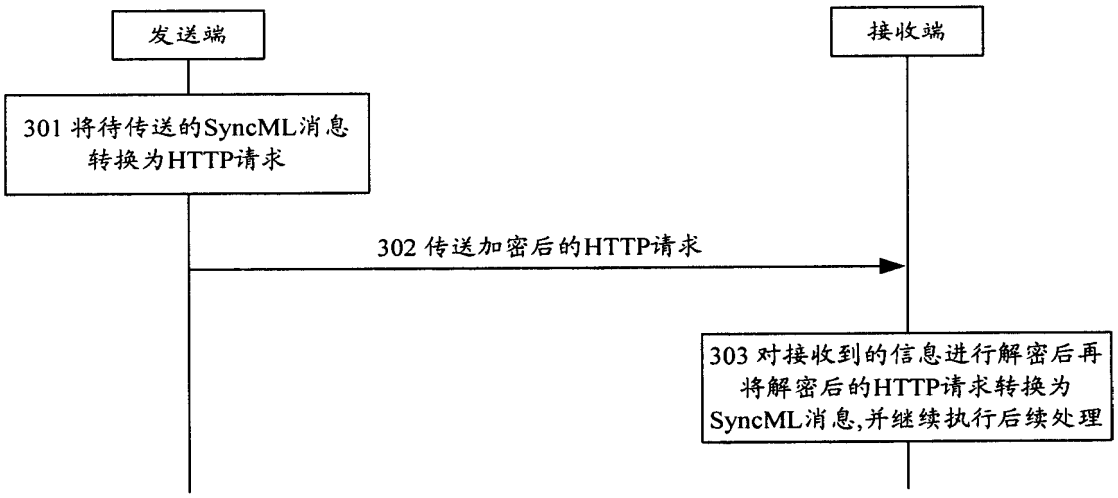

发送端
接收端
301 将待传送的SyncML消息转换为HTTP请求
302 传送加密后的HTTP请求
303 对接收到的信息进行解密后再将解密后的HTTP请求转换为SyncML消息,并继续执行后续处理

图 3