



(12) 发明专利申请

(10) 申请公布号 CN 101917712 A

(43) 申请公布日 2010. 12. 15

(21) 申请号 201010265297. 6

(22) 申请日 2010. 08. 25

(71) 申请人 中兴通讯股份有限公司

地址 518057 广东省深圳市南山区高新技术
产业园科技南路中兴通讯大厦法务部

(72) 发明人 张蓬勃 曹耀斌 薛宝林 薛涛
于松 邓方民 孙君生 杨玉林

(74) 专利代理机构 北京安信方达知识产权代理
有限公司 11262

代理人 解婷婷 龙洪

(51) Int. Cl.

H04W 12/02 (2009. 01)

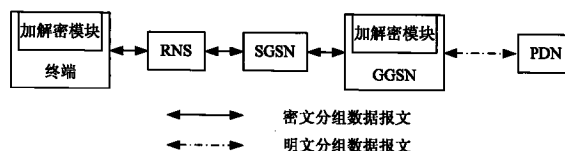
权利要求书 2 页 说明书 7 页 附图 1 页

(54) 发明名称

一种移动通讯网中数据加解密方法和系统

(57) 摘要

本发明公开了一种移动通讯网中数据加解密方法和系统,保证用户信息不通过明文传输,防止用户信息被非法监听,提高数据传输的安全性和保密性。所述方法包括:在分组数据传输之前,发送端将原始分组数据报文送入加密模块,由加密模块采用加密密钥(CK)对原始分组数据报文进行加密,对加密后的分组数据报文进行协议封装后发送至接收端;接收端收到加密的分组数据报文后,将其送入解密模块,由解密模块使用与发送端加密模块相同的CK对分组数据报文进行解密,将解密后的分组数据报文发往下一目的地。



1. 一种移动通讯网中数据加解密方法,包括:

在分组数据传输之前,发送端将原始分组数据报文送入加密模块,由加密模块采用加密密钥(CK)对原始分组数据报文进行加密,对加密后的分组数据报文进行协议封装后发送至接收端;

接收端收到加密的分组数据报文后,将其送入解密模块,由解密模块使用与发送端加密模块相同的CK对分组数据报文进行解密,将解密后的分组数据报文发往下一目的地。

2. 如权利要求1所述的方法,其特征在于:

所述发送端在分组数据传输之前,判断在分组数据通道建立时是否接收到加密标识,如果接收到,则将原始分组数据报文送入加密模块进行加密,否则封装后发送。

3. 如权利要求1或2所述的方法,其特征在于:

所述发送端为终端,所述接收端为GPRS网关支持节点(GGSN);或者,所述发送端为GGSN,所述接收端为终端。

4. 如权利要求3所述的方法,其特征在于:

所述发送端为终端,所述接收端为GGSN时,所述方法进一步包括:

终端在发送分组数据报文前,先通过终端中的加密模块使用CK对所述分组数据报文进行加密,终端对加密后的分组数据报文进行协议封装后发送至网络;所述GGSN收到终端发送的分组数据报文后,GGSN中的解密模块使用与所述终端相同的CK对所述分组数据报文进行解密,所述GGSN将解密后的分组数据报文发送至所述报文的目地址。

5. 如权利要求3所述的方法,其特征在于:

所述发送端为GGSN,所述接收端为终端时,所述方法进一步包括:

所述GGSN在接收到发送至终端的分组数据报文后,GGSN中的加密模块使用CK对所述分组数据报文进行加密,GGSN对加密后的分组数据报文进行协议封装后发送,通过网络发送至终端;所述终端接收到加密的分组数据报文后,由终端中的解密模块使用与所述GGSN相同的CK对所述分组数据报文进行解密,获取解密后的分组数据报文。

6. 如权利要求4所述的方法,其特征在于:

所述GGSN收到终端发送的分组数据报文后,GGSN中的解密模块使用与所述终端相同的CK对所述分组数据报文进行解密的步骤包括:所述GGSN收到终端发送的分组数据报文后,将所述终端的CK和所述分组数据报文发送给解密模块,由所述解密模块使用所述CK对所述分组数据报文进行解密;

所述GGSN在数据传输链路建立时,从归属位置存储器/鉴权中心(HLR/AUC)中获取所述终端的CK。

7. 如权利要求5所述的方法,其特征在于:

所述GGSN在接收到发送至终端的分组数据报文后,GGSN中的加密模块使用CK对所述分组数据报文进行加密的步骤包括:所述GGSN收到发送至终端的分组数据报文后,将所述终端的CK和所述分组数据报文发送给加密模块,由所述加密模块使用所述CK对所述分组数据报文进行加密;

所述GGSN在数据传输链路建立时,从归属位置存储器/鉴权中心(HLR/AUC)中获取所述终端的CK。

8. 一种移动通讯网中数据加解密系统,包括终端和GPRS网关支持节点(GGSN),其中:

所述终端包括加密模块、发送模块、接收模块和解密模块,其中:

所述加密模块,用于使用 CK 对所述分组数据报文进行加密;

所述发送模块,用于对加密后的分组数据报文进行协议封装后发送至网络侧;

所述接收模块,用于接收网络侧发送的加密的分组数据报文;

所述解密模块,用于使用与 GGSN 加密模块相同的 CK 对所述分组数据报文进行解密,获取解密后的分组数据报文;

所述 GGSN 包括接收模块、解密模块、加密模块和发送模块,其中:

所述接收模块,用于接收终端发送的加密的分组数据报文,以及用于接收发送至终端的分组数据报文;

所述解密模块,用于使用与终端加密模块相同的 CK 对所述接收的加密的分组数据报文进行解密;

所述发送模块,用于将解密后的分组数据报文发送至所述报文的地址,以及用于将加密后的分组数据报文进行协议封装后通过网络发送至终端;

所述加密模块,用于使用 CK 对所述接收的发送至终端的分组数据报文进行加密。

9. 如权利要求 8 所述的方法,其特征在于:

所述 GGSN,还用于在数据传输链路建立时,从归属位置存储器/鉴权中心(HLR/AUC)中获取的所述终端的 CK;以及:

在收到终端发送的分组数据报文后,将获取的所述终端的 CK 和所述分组数据报文发送给解密模块,由所述解密模块使用所述 CK 对所述分组数据报文进行解密;

在收到发送至终端的分组数据报文后,将获取的所述终端的 CK 和所述分组数据报文发送给加密模块,由所述加密模块使用所述 CK 对所述分组数据报文进行加密。

10. 如权利要求 8 所述的方法,其特征在于:

所述终端还包括判断模块,用于在发送分组数据报文前,判断是否有加密标识,如果有,则触发加密模块,否则触发发送模块;以及用于在接收到分组数据报文后,如果判断有加密标识,则触发解密模块。

11. 如权利要求 8 所述的方法,其特征在于:

所述 GGSN 还包括判断模块,用于在发送分组数据报文前,判断是否有加密标识,如果有,则触发加密模块,否则触发发送模块;以及用于在接收到分组数据报文后,如果判断有加密标识,则触发解密模块。

一种移动通讯网中数据加解密方法和系统

技术领域

[0001] 本发明属于移动通信领域,涉及在移动通信网中数据加解密方法和系统。

背景技术

[0002] 数据业务是第三代移动通讯技术发展的重点,也最受用户和运营商的关注,很多传统的业务(比如语音通话)也已经通过分组交互实现(VOIP),因此数据业务的保密性和安全性也越来越受到关注。

[0003] 移动网络本身有自身的通讯加密方法,在 3GPP(包括 UMTS 和 GSM)系统中,用户的 SIM 卡和归属网络的 HLR/AuC(归属位置存储器/鉴权中心,通用表示方式,表示集成了 AUC 的 HLR)共享一个安全密钥 Ki(128bit),基于该密钥,核心网和用户之间可以进行双向鉴权,同时基站和手机间也利用 Ki 对无线链路进行加密和完整性保护。

[0004] 3GPP 中定义的加密方法只是加密无线环境,在移动终端和 Node B 之间对传输的数据进行加/解密,数据在网络中都是通过明文传输的,很容易被监听,现有的网络监听技术大都在网络侧实现。图 1 为分组数据网络示意图,移动终端 A 和 B 分别通过各自的 RNS(Radio Network System 无线网络系统)、SGSN(Serving GPRS support node, GPRS 业务支持节点)、GGSN(Gateway GPRS support node, GPRS 网关支持节点)接入 PDN(Packet Data Network, 分组数据网络)。如附图 1,通常在 SGSN 和 GGSN 中进行监听。

[0005] 目前已有相关专利或者方案都是端到端的加密,这样的加密参数不能动态变化,很容易被破解。支持加密的用户和不支持加密的用户之间数据输出方式很难协调。

发明内容

[0006] 本发明要解决的技术问题是提供一种移动通讯网中数据加解密方法和系统,保证用户信息不通过明文传输,防止用户信息被非法监听,提高数据传输的安全性和保密性。

[0007] 为解决上述技术问题,本发明提供了一种移动通讯网中数据加解密方法,包括:

[0008] 在分组数据传输之前,发送端将原始分组数据报文送入加密模块,由加密模块采用加密密钥(CK)对原始分组数据报文进行加密,对加密后的分组数据报文进行协议封装后发送至接收端;

[0009] 接收端收到加密的分组数据报文后,将其送入解密模块,由解密模块使用与发送端加密模块相同的 CK 对分组数据报文进行解密,将解密后的分组数据报文发往下一目的地。

[0010] 进一步地,所述发送端在分组数据传输之前,判断在分组数据通道建立时是否接收到加密标识,如果接收到,则将原始分组数据报文送入加密模块进行加密,否则封装后发送。

[0011] 进一步地,所述发送端为终端,所述接收端为 GPRS 网关支持节点(GGSN);或者,所述发送端为 GGSN,所述接收端为终端。

[0012] 进一步地,所述发送端为终端,所述接收端为 GGSN 时,所述方法进一步包括:终端

在发送分组数据报文前,先通过终端中的加密模块使用 CK 对所述分组数据报文进行加密,终端对加密后的分组数据报文进行协议封装后发送至网络;所述 GGSN 收到终端发送的分组数据报文后,GGSN 中的解密模块使用与所述终端相同的 CK 对所述分组数据报文进行解密,所述 GGSN 将解密后的分组数据报文发送至所述报文的目的地址。

[0013] 进一步地,所述发送端为 GGSN,所述接收端为终端时,所述方法进一步包括:所述 GGSN 在接收到发送至终端的分组数据报文后,GGSN 中的加密模块使用 CK 对所述分组数据报文进行加密,GGSN 对加密后的分组数据报文进行协议封装后发送,通过网络发送至终端;所述终端接收到加密的分组数据报文后,由终端中的解密模块使用与所述 GGSN 相同的 CK 对所述分组数据报文进行解密,获取解密后的分组数据报文。

[0014] 进一步地,所述 GGSN 收到终端发送的分组数据报文后,GGSN 中的解密模块使用与所述终端相同的 CK 对所述分组数据报文进行解密的步骤包括:所述 GGSN 收到终端发送的分组数据报文后,将所述终端的 CK 和所述分组数据报文发送给解密模块,由所述解密模块使用所述 CK 对所述分组数据报文进行解密;所述 GGSN 在数据传输链路建立时,从归属位置存储器/鉴权中心(HLR/AUC)中获取所述终端的 CK。

[0015] 进一步地,所述 GGSN 在接收到发送至终端的分组数据报文后,GGSN 中的加密模块使用 CK 对所述分组数据报文进行加密的步骤包括:所述 GGSN 收到发送至终端的分组数据报文后,将所述终端的 CK 和所述分组数据报文发送给加密模块,由所述加密模块使用所述 CK 对所述分组数据报文进行加密;所述 GGSN 在数据传输链路建立时,从归属位置存储器/鉴权中心(HLR/AUC)中获取所述终端的 CK。

[0016] 为解决上述技术问题,本发明还提供了一种移动通讯网中数据加解密系统,包括终端和 GPRS 网关支持节点(GGSN),其中:

[0017] 所述终端包括加密模块、发送模块、接收模块和解密模块,其中:

[0018] 所述加密模块,用于使用 CK 对所述分组数据报文进行加密;

[0019] 所述发送模块,用于对加密后的分组数据报文进行协议封装后发送至网络侧;

[0020] 所述接收模块,用于接收网络侧发送的加密的分组数据报文;

[0021] 所述解密模块,用于使用与 GGSN 加密模块相同的 CK 对所述分组数据报文进行解密,获取解密后的分组数据报文;

[0022] 所述 GGSN 包括接收模块、解密模块、加密模块和发送模块,其中:

[0023] 所述接收模块,用于接收终端发送的加密的分组数据报文,以及用于接收发送至终端的分组数据报文;

[0024] 所述解密模块,用于使用与终端加密模块相同的 CK 对所述接收的加密的分组数据报文进行解密;

[0025] 所述发送模块,用于将解密后的分组数据报文发送至所述报文的目的地址,以及用于将加密后的分组数据报文进行协议封装后通过网络发送至终端;

[0026] 所述加密模块,用于使用 CK 对所述接收的发送至终端的分组数据报文进行加密。

[0027] 进一步地,所述 GGSN,还用于在数据传输链路建立时,从归属位置存储器/鉴权中心(HLR/AUC)中获取的所述终端的 CK;以及:在收到终端发送的分组数据报文后,将获取的所述终端的 CK 和所述分组数据报文发送给解密模块,由所述解密模块使用所述 CK 对所述分组数据报文进行解密;以及:在收到发送至终端的分组数据报文后,将获取的所述终端

的 CK 和所述分组数据报文发送给加密模块,由所述加密模块使用所述 CK 对所述分组数据报文进行加密。

[0028] 进一步地,所述终端还包括判断模块,用于在发送分组数据报文前,判断是否有加密标识,如果有,则触发加密模块,否则触发发送模块;以及用于在接收到分组数据报文后,如果判断有加密标识,则触发解密模块。

[0029] 进一步地,所述 GGSN 还包括判断模块,用于在发送分组数据报文前,判断是否有加密标识,如果有,则触发加密模块,否则触发发送模块;以及用于在接收到分组数据报文后,如果判断有加密标识,则触发解密模块。

[0030] 本发明通过在移动终端和 GGSN 中分别配置硬件加解密模块,硬件加解密模块通过 CK(Cipher Key,加密密钥)对上下行分组数据报文进行加解密,可以保证用户信息不通过明文传输。加密后的数据在网络侧无法监听,而且在无线环境传输还会进行加密,相当于双加密的,更加保密和安全。即使窃听方获得了被窃听方得安全密钥 Ki,也无法在无线传输环境中进行窃听,提高数据传输的安全性和保密性。

[0031] 本发明适用于政府敏感部门,情报机关,等等非常重视安全和保密的组织和个人。

附图说明

[0032] 图 1 为分组数据网络示意图;

[0033] 图 2 为加密后的分组网络及数据传输示意图;

[0034] 图 3 为终端和 GGSN 的具体结构示意图。

具体实施方式

[0035] 目前技术中端到端的加密由于没有传输网络参与,这样的加密参数不能动态变化,很容易被破解。本发明的发明构思是:

[0036] 在分组数据传输之前,发送端(用户终端或者 GGSN)将原始分组数据报文送入加密模块,由加密模块采用加密密钥(CK)作为加密运算因子对原始分组数据报文进行加密,得到加密后的分组数据报文,对加密后的分组数据报文进行协议封装后发送至接收端;

[0037] 接收端(发送端为用户终端时,接收端为 GGSN;发送端为 GGSN 时,接收端为用户终端)收到加密的分组数据报文后,将其送入解密模块,由解密模块使用与发送端加密模块相同的 CK 对分组数据报文进行解密,之后将解密后的分组数据报文发往下一目的地。

[0038] 具体地:

[0039] ●对于上行分组数据,终端在发送分组数据报文前,先通过终端中的加密模块使用加密密钥(CK)对所述分组数据报文进行加密,终端对加密后的分组数据报文进行协议封装后发送至网络;GGSN 收到终端发送的分组数据报文后,GGSN 中的解密模块使用与所述终端相同的 CK 对所述分组数据报文进行解密,所述 GGSN 将解密后的分组数据报文发送至所述报文的目的地。

[0040] 所述 GGSN 收到终端发送的分组数据报文后,GGSN 中的解密模块使用与所述终端相同的 CK 对所述分组数据报文进行解密的步骤包括:所述 GGSN 收到终端发送的分组数据报文后,将所述终端的 CK 和所述分组数据报文发送给解密模块,由所述解密模块使用所述 CK 对所述分组数据报文进行解密。

[0041] 所述 GGSN 中的终端的 CK 是在数据传输链路建立时,从归属位置存储器 / 鉴权中心 (HLR/AUC) 中获取的。

[0042] ●对于下行分组数据, GGSN 在接收到发送至终端的分组数据报文后, GGSN 中的加密模块使用 CK 对所述分组数据报文进行加密, GGSN 对加密后的分组数据报文进行协议封装后发送, 通过网络发送至终端; 所述终端接收到加密的分组数据报文后, 由终端中的解密模块使用与所述 GGSN 相同的 CK 对所述分组数据报文进行解密, 获取解密后的分组数据报文。

[0043] 所述 GGSN 在接收到发送至终端的分组数据报文后, GGSN 中的加密模块使用 CK 对所述分组数据报文进行加密的步骤包括: 所述 GGSN 收到发送至终端的分组数据报文后, 将所述终端的 CK 和所述分组数据报文发送给加密模块, 由所述加密模块使用所述 CK 对所述分组数据报文进行加密。

[0044] 本文的实现与移动网络自身加密无关, 直接对需要传输的原始数据进行加密和解密, 数据加密后在网络中传输, 以保证数据的保密性和安全性。

[0045] 硬件加密、解密模块使用 CK 作为加密因子对分组数据进行加解密。该 CK 是通过加密算法 (A3)、RAND (随机数) 和 Ki (根密钥) 计算出来的, 如 $CK = A3(RAND, Ki)$ 。Ki 由网络 (如网络单元 HLR/AUC) 与终端共享, 在终端 (如 USIM 卡中) 和 HLR/AUC 中存储, 不在网络中传输, 很难窃取。而 RAND 是随机序列, 在每次连接建立中都会变化, 具有很强的随机性。因此在本方案中加密因子每次都不同, 只在本次会话中有效, 所以又称为实时加密, 此举更加大了无线传输环境中对 CK 进行破解的难度, 从而保证数据传输私密性。

[0046] 另一方面, 本发明中使用数据业务的双方 (包括终端和 GGSN 服务器) 不需要知道对方的 CK。对终端而言, 网络侧负责在每次认证时将 RAND 传给终端, 终端可根据算法自己生成 CK; 对于 GGSN 而言, GGSN 可从 HLR/AUC 中获取 HLR/AUC 计算出的 CK。不会增加额外的损耗。

[0047] 上述硬件加密、解密模块可以由第三方提供, 嵌入终端及网络设备中, 负责对分组数据进行加解密运算。这样即使网络设备商、终端设备商和运营商都无法对加密分组数据进行窃听。

[0048] 分组数据都是基于 IP 传输, 本专利中, 对原始的数据进行加密, 密文作为 IP 包的原始数据, 通过 IP 相关协议封装, 不影响网关对分组数据的处理及路由选择。

[0049] 实现上述方法的系统如附图 2 和图 3 所示, 主要包括终端和 GGSN, 其中:

[0050] 所述终端包括加密模块、发送模块、接收模块和解密模块, 其中:

[0051] 所述加密模块, 用于使用 CK 对所述分组数据报文进行加密;

[0052] 所述发送模块, 用于对加密后的分组数据报文进行协议封装后发送至网络侧;

[0053] 所述接收模块, 用于接收网络侧发送的加密的分组数据报文;

[0054] 所述解密模块, 用于使用与 GGSN 加密模块相同的 CK 对所述分组数据报文进行解密, 获取解密后的分组数据报文。

[0055] 所述 GGSN 包括接收模块、解密模块、加密模块和发送模块, 其中:

[0056] 所述接收模块, 用于接收终端发送的加密的分组数据报文, 以及用于接收发送至终端的分组数据报文;

[0057] 所述解密模块, 用于使用与终端加密模块相同的 CK 对所述接收的加密的分组数

据报文进行解密；

[0058] 所述发送模块,用于将解密后的分组数据报文发送至所述报文的地址,以及用于将加密后的分组数据报文进行协议封装后通过网络发送至终端；

[0059] 所述加密模块,用于使用 CK 对所述接收的发送至终端的分组数据报文进行加密。

[0060] 上述终端中的加密模块和解密模块可以合一设置为加解密模块；同样地,所述 GGSN 中的加密和解密模块也可合一设置。发送模块和接收模块也可合一设置为收发模块。终端中如何设置与 GGSN 中如何设置无关, GGSN 中如何设置也与终端中如何设置无关。但 GGSN 和终端中加解密模块的运算规则相同,具体采用哪种加解密算法本发明不作限定。

[0061] 优选地,所述 GGSN,还用于在数据传输链路建立时,从 HLR/AUC 中获取的所述终端的 CK；以及：在收到终端发送的分组数据报文后,将获取的所述终端的 CK 和所述分组数据报文发送给解密模块,由所述解密模块使用所述 CK 对所述分组数据报文进行解密；以及：在收到发送至终端的分组数据报文后,将获取的所述终端的 CK 和所述分组数据报文发送给加密模块,由所述加密模块使用所述 CK 对所述分组数据报文进行加密。

[0062] 优选地,所述终端还包括判断模块,用于在发送分组数据报文前,判断是否有加密标识,如果有,则触发加密模块,否则触发发送模块；以及用于在接收到分组数据报文后,如果判断有加密标识,则触发解密模块。

[0063] 优选地,所述 GGSN 还包括判断模块,用于在发送分组数据报文前,判断是否有加密标识,如果有,则触发加密模块,否则触发发送模块；以及用于在接收到分组数据报文后,如果判断有加密标识,则触发解密模块。

[0064] 下面结合附图对技术方案的实施作进一步的详细描述：

[0065] 本发明所提出的实现方法需要网络参与,因此需要在终端和 GGSN(GPRS 网关支持节点)中嵌入硬件加密模块。选择把 GGSN 作为加密/解密的另一端,有几个好处：

[0066] 1) 分组业务包括很多种类, C/S(客户端/服务器)类的业务占了绝大多数,同时还有部分会话类业务,在 GGSN 中加密/解密,可以实现对各种类型的分组业务的加密。

[0067] 2) GGSN 是第三代移动通讯分组域网络的网关节点,是移动网络和公用 PDN 的分界点,用户数据在外部 PDN 传输时用户的 IP 地址都是动态分配的,根据 IP 很难获取到用户信息,而用户的标识信息(比如 IMSI 等)只在移动网络中传输,因此在 GGSN 中加密能够保证用户数据不被非法监听,所以在 GGSN 中加密能够保证用户信息的安全性和私密性。

[0068] 终端和 GGSN 中的硬件加密模块作用稍有差异,而运算规则完全相同。

[0069] 在本实施例中,可在分组数据通道建立过程中,通过参数控制终端和 GGSN 是否需要分组数据报文进行加密。下面分三个部分对具体实现流程进行介绍：

[0070] 第一部分：加密判断及 CK(密钥)的获得

[0071] 加密标识：

[0072] 在处理数据之前,移动终端和 GGSN 需要知道是否需要对用户数据进行加密解密。参照 3GPP 协议,在分组数据通道建立时,在终端和 GGSN 之间会共享传输相关的参数信息,如 IP 配置信息、DNS 配置信息等,终端通过在该参数中增加加密标识,通知 GGSN 是否需要进行加解密操作。

[0073] 终端和 GGSN 在数据发送之前,判断是否有该加密标识,如果有,则触发加密模块进行加密,如果没有,则按正常流程,对分组数据封装后发送。

[0074] CK(密钥)的获得：

[0075] 终端中：

[0076] 根据 3GPP 协议规定,在建立分组数据传输通道建立之前,首先要建立信令连接,在信令连接建立过程中需要对用户进行认证,在认证过程中网络侧将 RAND 发给终端,终端按照获得的 RAND,结合自身 Ki,通过 A3 算法,产生当前有效 CK,将 CK 传递给终端硬件加解密模块。

[0077] GGSN 中：

[0078] 按照 3GPP 的协议流程,GGSN 不参与信令链路的建立,因此在 GGSN 中无法根据现有流程获得 CK 值,因此需要增加额外的信令流程来实现。利用现有的 GGSN 和 HLR/AUC 之间的接口(Gc)口,在数据传输链路建立时,判断如果需要对数据进行加解密操作,从 HLR/Auc 中获取 CK,存储在 GGSN 中,在对应的用户终端需要传输数据时,发给硬件加解密模块。

[0079] 第二部分:终端中的加密解密处理

[0080] 加密：

[0081] 终端在发送数据前,先把分组数据报文发给硬件加解密模块,硬件加解密模块使用在链路建立时获得的 CK 对分组数据报文进行加密,终端加密后的分组数据报文进行相关的协议封装后发送给网络。

[0082] 解密：

[0083] 终端从网络收到分组数据报文后,把分组数据报文传给硬件加解密模块进行解密,硬件加解密模块使用 CK 对分组数据报文进行解密,终端把解密后明文数据报文传给对应的应用模块。

[0084] 第三部分:GGSN 中的加密解密处理

[0085] GGSN 从终端收到分组数据报文后,先进行解密,把分组数据报文以明文的形式发给外部 PDN(packet data network,分组数据网);GGSN 从外部 PDN 或者其他 GGSN 收到分组数据报文后,进行加密后,以密文形式发给终端。

[0086] 加密：

[0087] GGSN 从外部 PDN 或者其他 GGSN 收到分组数据报文后,根据目的地址获得用户信息,判断是否需要对当前用户的数据进行加密,需要加密时,获取当前用户的 CK,和原始分组数据报文一起传给硬件加解密模块,硬件加解密模块使用收到的 CK 对分组数据报文进行加密生成密文。GGSN 把密文按照 3GPP 规定的协议(和 SGSN(Serving GPRS support node,GPRS 业务支持节点)之间通过 GTP(GPRS Tunnelling Protocol GPRS 隧道协议)协议封装))封装后,发送终端。

[0088] 解密：

[0089] GGSN 根据从 MS 收到数据获得用户标识(按照 3GPP 协议规定,SGSN 和 GGSN 之间采用 GTP 协议进行数据传输,根据 GTP 的标识可以获得用户标识信息),根据获得的用户标识,从保存的 CK 中查出该 UE 的 CK,把分组数据报文和 CK 一起送给硬件加密模块进行解密,解密后获得明文形式的分组数据报文,按照报文中指定的目的地址发送报文。

[0090] 本领域普通技术人员可以理解上述方法中的全部或部分步骤可通过程序来指令相关硬件完成,所述程序可以存储于计算机可读存储介质中,如只读存储器、磁盘或光盘等。可选地,上述实施例的全部或部分步骤也可以使用一个或多个集成电路来实现。相应

地,上述实施例中的各模块可以采用硬件的形式实现,也可以采用软件功能模块的形式实现。本发明不限制于任何特定形式的硬件和软件的结合。

[0091] 当然,本发明还可有其他多种实施例,在不背离本发明精神及其实质的情况下,熟悉本领域的技术人员当可根据本发明作出各种相应的改变和变形,但这些相应的改变和变形都应属于本发明所附的权利要求的保护范围。

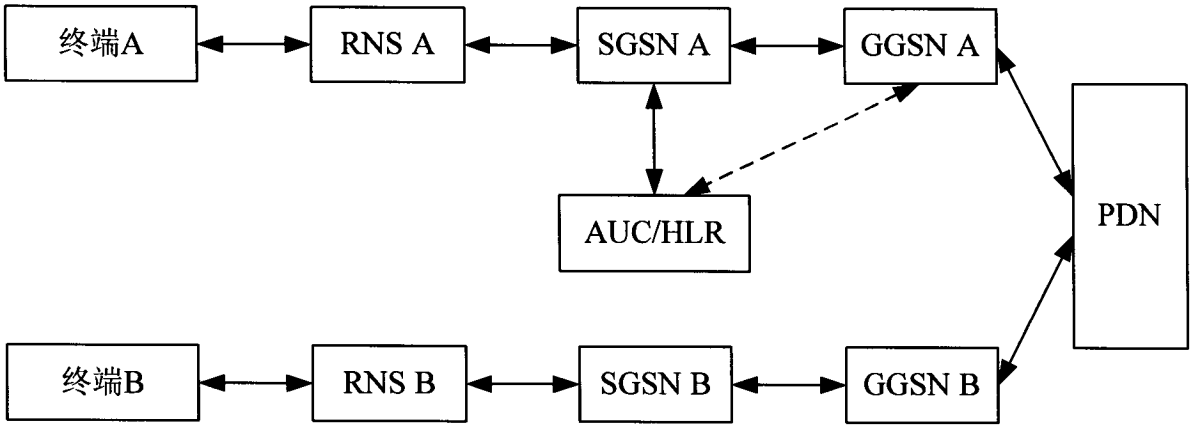


图 1

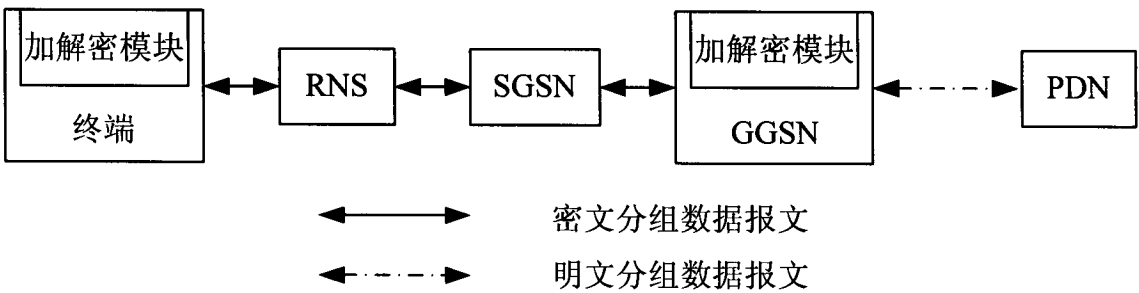


图 2

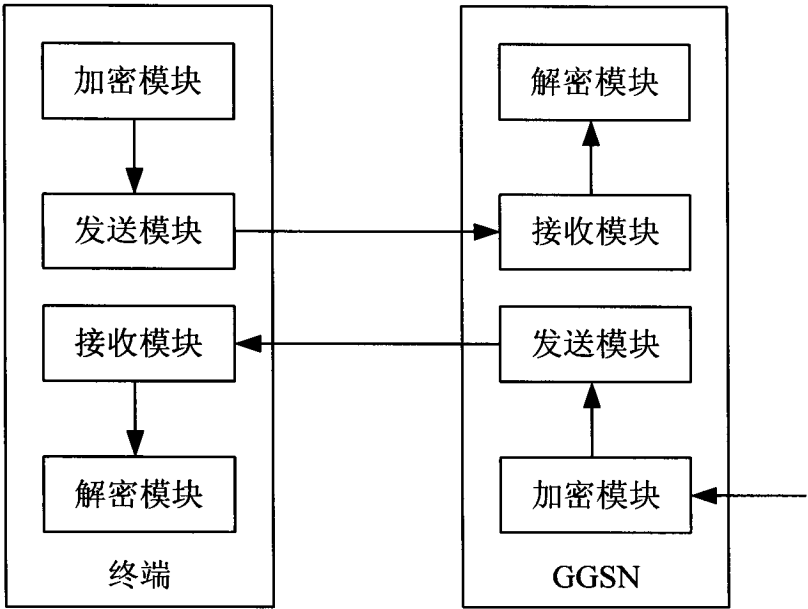


图 3