



(12) 发明专利申请

(10) 申请公布号 CN 104301111 A

(43) 申请公布日 2015. 01. 21

(21) 申请号 201410535665. 2

(22) 申请日 2014. 10. 11

(71) 申请人 中国科学院国家授时中心

地址 710600 陕西省西安市临潼区书院东路
3号

(72) 发明人 洪浩 卢晓春

(74) 专利代理机构 西北工业大学专利中心

61204

代理人 顾潮琪

(51) Int. Cl.

H04L 9/32(2006. 01)

H04L 9/06(2006. 01)

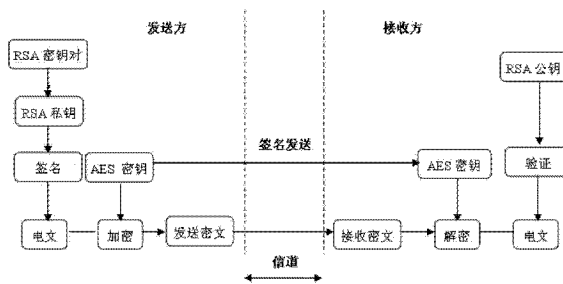
权利要求书1页 说明书4页 附图2页

(54) 发明名称

北斗高精度差分信息安全传输方法

(57) 摘要

本发明提供了一种北斗高精度差分信息安全传输方法,针对普通用户采用 RSA 密钥对对电文信息中的指定区段添加签名,接收方利用 RSA 的公钥验证签名的正确性,若签名验证无效则丢弃电文信息;针对特殊用户依照 AES 标准流程对电文信息进行加密,再利用 RSA 的私钥对指定区段添加签名,接收方利用 AES 加密密钥进行解密,再利用 RSA 的公钥验证签名的正确性。本发明可以有效地抵制外界的欺骗性攻击方法,从而进一步提高系统的通信可靠性。



1. 一种北斗高精度差分信息安全传输方法,其特征在于包括下述步骤:

(1) 根据信息帧头区分普通用户和特权用户,普通用户进入步骤(2),特权用户进入步骤(3);

(2) 普通用户执行以下步骤:

(a) 发送方编辑电文信息的同时,产生 RSA 密钥对;

(b) 对电文信息中的指定区段添加签名;

(c) 将签名后的电文信息上注给卫星;

(d) 接收方收到卫星转发过来的电文信息,利用 RSA 的公钥验证签名的正确性,若签名验证无效则丢弃该电文信息;反之,则接受电文信息进行后期定位解算;

(3) 特权用户执行以下步骤:

(a) 发送方编辑电文信息的同时,产生 RSA 密钥对;

(b) 依照 AES 标准流程对电文信息进行加密,再利用 RSA 的私钥对指定区段添加签名;

(c) 将签名、加密后的电文信息上注给卫星;

(d) 接收方收到卫星转发过来的电文信息,利用发送方提供的 AES 加密密钥进行解密;

(e) 利用 RSA 的公钥验证签名的正确性,若签名验证无效则丢弃该电文信息;反之,则接受电文信息进行后期定位解算。

2. 根据权利要求 1 所述的北斗高精度差分信息安全传输方法,其特征在于所述的 RSA 密钥对采用以下步骤产生:

Step1:随机产生两个大质数 p 和 q , p 和 q 的取值范围为 96-1024;

Step2:计算 $n = p \times q$, $\phi(n) = (p-1) \times (q-1)$, mod 代表同余符号;

Step3:随机选取一个与 $\phi(n)$ 互素的整数 e 作为公开密钥,即 $\text{gcd}(e, \phi(n)) = 1$;

Step4:计算私有密钥 $d = e^{-1} \text{mod}(\phi(n))$ 。

3. 根据权利要求 1 所述的北斗高精度差分信息安全传输方法,其特征在于:所述的添加签名包括以下步骤:将电文信息 M 分解成为若干消息比特串分组,分组长度 L 保证 $2^L \leq n$,用 m 表示某一分组后的十进制消息的表示,则 $0 \leq m \leq n$;采用私有密钥 d 执行分组模指数运算,得到分组信息 $c = m^d \text{mod}n$,将分组信息组合成签名 C ,将签名 C 及电文信息 M 一起发送。

4. 根据权利要求 1 所述的北斗高精度差分信息安全传输方法,其特征在于:所述的验证签名包括以下步骤:接收方从公布的公钥簿上获得公钥 e ,然后执行分组模指数运算 $m' = c'^e \text{mod}n$,然后将解算出的 m' 组合成 M' ;比较 M 和 M' ,如果相同则认为签名有效,反之则认为此次签名不是真实的,拒绝接受信息。

5. 根据权利要求 1 所述的北斗高精度差分信息安全传输方法,其特征在于:所述的加密过程中,将分组长度等于原电文信息帧长度的分组用 AES 进行数据加密,将分组长度小于原电文信息帧长度的分组用前一组加密后的密文的后部数据补足,得到分组长度等于原电文信息帧长度的分组然后再进行加密,最后将得到的密文按次序重新填充到原有帧长度中。

北斗高精度差分信息安全传输方法

技术领域

[0001] 本发明涉及一种北斗高精度差分信息安全传输实现方法。

背景技术

[0002] 我国的北斗卫星导航系统是继美国 GPS、俄罗斯 GLONASS 之后,全球第三大卫星导航系统。2003 年“北斗一号”卫星导航系统的建成,标志着我国成为世界上第三个拥有独立自主卫星导航系统的国家。北斗卫星导航系统 2012 年将覆盖亚太区域,2020 年将形成由 35 颗卫星组网具有覆盖全球的卫星导航系统。但由于通信卫星星体长时间暴露在其覆盖区域的上空;通信卫星的服务对象多且分散,卫星的天线覆盖范围大,电文导航信号比较微弱,而且信号频率和带宽固定,因此电文信号很容易受到干扰。从技术角度出发,电子干扰可以分为两类:一是压制性干扰,二是欺骗性干扰。压制式干扰容易被发现,而欺骗性干扰,是指将接收到的电文卫星信号重新广播出去,从而构成一个虚假的电文卫星信号(称为转发式干扰欺骗)或由干扰机发射与电文卫星信号相同的无线信号来欺骗接收机(称为产生式干扰欺骗),因此是电文信息安全领域亟待解决的问题。

[0003] 对于以密码体制为基础的信息安全策略如果以密钥为基准,它们都可以分为双钥密码体制和单钥密码体制。前者,每个用户都有一对密钥,即公钥和私钥;后者的加密过程和解密过程相同,而且在这两个过程中所用的密钥也相同。RSA 算法是公开密钥系统的代表,其安全性建立在具有大素数因子的合数,其因子分解困难这一法则之上的。Rijndael 算法作为新一代的高级加密标准(AES),其属于单钥密码体制范畴,运行时不需要芯片有非常高的处理能力和大的内存,操作可以很容易的抵御时间和空间的攻击,在不同的运行环境下始终能保持良好的性能。这使 AES 将安全,高效,性能,方便,灵活性集于一体,理应成为大数据量加密的首选。相比较,因为目前 AES 密钥的长度最长只有 256 比特,可以利用软件和硬件实现高速处理,而 RSA 算法需要进行大整数的乘幂和求模等多倍字长处理,处理速度明显慢于 AES;所以 AES 算法加解密处理效率明显高于 RSA 算法。在密钥管理方面,因为 AES 算法要求在通信前对密钥进行秘密分配,解密的私钥必须通过网络传送至加密数据接收方,而 RSA 采用公钥加密,私钥解密(或私钥加密,公钥解密),加解密过程中不必网络传输保密的密钥;所以 RSA 算法密钥管理和签名机制上要明显优于 AES 算法。综上所述,RSA 加解密速度慢,不适合大量数据文件加密,因此在通信中完全用公开密码体制传输机密信息是没有必要,也是不太现实的。AES 加密速度很快,但是在网络传输过程中如何安全管理 AES 密钥是保证 AES 加密安全的重要环节。这样在传送机密信息的双方,如果使用 AES 对称密码体制对传输数据加密,同时使用 RSA 不对称密码体制来作为签名验证机制,就可以综合发挥 AES 和 RSA 的优点同时避免它们缺点。

发明内容

[0004] 为了克服现有技术的不足,本发明提供一种基于 RSA 和 AES 相结合的综合加密体制对北斗高精度差分系统进行信息处理,可以有效地抵制外界的欺骗性攻击方法,从而进

一步提高系统的通信可靠性。

[0005] 本发明解决其技术问题所采用的技术方案包括以下步骤：

[0006] (1) 根据信息帧头区分普通用户和特权用户,普通用户进入步骤 (2),特权用户进入步骤 (3)；

[0007] (2) 普通用户执行以下步骤：

[0008] (a) 发送方编辑电文信息的同时,产生 RSA 密钥对；

[0009] (b) 对电文信息中的指定区段添加签名；

[0010] (c) 将签名后的电文信息上注给卫星；

[0011] (d) 接收方收到卫星转发过来的电文信息,利用 RSA 的公钥验证签名的正确性,若签名验证无效则丢弃该电文信息;反之,则接受电文信息进行后期定位解算；

[0012] (3) 特权用户执行以下步骤：

[0013] (a) 发送方编辑电文信息的同时,产生 RSA 密钥对；

[0014] (b) 依照 AES 标准流程对电文信息进行加密,再利用 RSA 的私钥对指定区段添加签名；

[0015] (c) 将签名、加密后的电文信息上注给卫星；

[0016] (d) 接收方收到卫星转发过来的电文信息,利用发送方提供的 AES 加密密钥进行解密；

[0017] (e) 利用 RSA 的公钥验证签名的正确性,若签名验证无效则丢弃该电文信息;反之,则接受电文信息进行后期定位解算。

[0018] 所述的 RSA 密钥对采用以下步骤产生：

[0019] Step1:随机产生两个大质数 p 和 q , p 和 q 的取值范围为 96-1024；

[0020] Step2:计算 $n = p \times q$, $\phi(n) = (p-1) \times (q-1)$, mod 代表同余符号；

[0021] Step3:随机选取一个与 $\phi(n)$ 互素的整数 e 作为公开密钥,即 $\text{gcd}(e, \phi(n)) = 1$ ；

[0022] Step4:计算私有密钥 $d = e^{-1} \text{mod}(\phi(n))$ 。

[0023] 所述的添加签名包括以下步骤:将电文信息 M 分解成为若干消息比特串分组,分组长度 L 保证 $2^L \leq n$,用 m 表示某一分组后的十进制消息的表示,则 $0 \leq m \leq n$;采用私有密钥 d 执行分组模指数运算,得到分组信息 $c = m^d \text{mod}n$,将分组信息组合成签名 C ,将签名 C 及电文信息 M 一起发送。

[0024] 所述的验证签名包括以下步骤:接收方从公布的公钥簿上获得公钥 e ,然后执行分组模指数运算 $m_i = c_i^e \text{mod}n$,然后将解算出的 m_i 组合成 M' ;比较 M 和 M' ,如果相同则认为签名有效,反之则认为此次签名不是真实的,拒绝接受信息。

[0025] 所述的加密过程中,将分组长度等于原电文信息帧长度的分组用 AES 进行数据加密,将分组长度小于原电文信息帧长度的分组用前一组加密后的密文的后部数据补足,得到分组长度等于原电文信息帧长度的分组然后再进行加密,最后将得到的密文按次序重新填充到原有帧长度中。

[0026] 本发明的有益效果是:针对北斗高精度差分信息的不同用户将单钥密码体制与公钥密码体制有机结合,在安全性、时效性以及实用性中找出最佳的平衡点,使北斗高精度差分系统在满足现有需求的同时,其自身安全性得以保障。采用本发明,可以有效地遏制差分

信息传递过程中的欺骗性干扰问题。

附图说明

[0027] 图 1 是本发明针对普通用户的方法流程图；

[0028] 图 2 是本发明针对特权用户的方法流程图；

[0029] 图 3 是本发明针对特权用户分组密码二次加密的方法流程图

具体实施方式

[0030] 下面结合附图和实施例对本发明进一步说明,本发明包括但不限于下述实施例。

[0031] 北斗高精度差分信息有两类用户——普通用户、特权用户(根据信息帧头进行区分),针对每一类用户,电文方面将采用不同的信息安全方案。

[0032] 普通用户的信息安全机制

[0033] 定义:普通用户是指可以获得非加密通道的导航电文,电文信息只具有检错能力,基本保证信号的完整性,只可以完成粗略的定位导航功能的用户。

[0034] 安全机制:发送方只对电文信息采用签名保护,对于电文数据本身并不加密。在定期更换密钥对的情况下可以防止前文所提到的产生式干扰欺骗。具体操作见图 1,包括以下步骤:

[0035] (1) 发送方编辑电文信息的同时,产生 RSA 密钥对;

[0036] (2) 对特定信息(例:子帧中 100 ~ 300 区间的电文信息)进行签名;

[0037] (3) 将签名后的电文信息上注给卫星;

[0038] (4) 接收方(接收机)收到通过卫星转发器发射过来的签名电文,利用 RSA 的公钥验证签名的正确性,若签名验证无效则丢弃导航电文;反之,则接受电文进行后期定位解算。

[0039] 特权用户(商用和军用)的信息安全机制

[0040] 定义:特权用户是指通过特定通道获得导航电文,电文不仅具有检错能力,而且具有较高信号的完整性,以及附加信息(例如差分信息等),以满足较高精度的导航定位要求需要。

[0041] 安全机制:发送方不仅对电文采用签名保护,而且对于电文数据本身进行加密。在定期更换密钥对的情况下,不仅可以防止前文所提到的产生式干扰欺骗,而且由于电文数据本身被加密亦可以应对转发式干扰。从商业运作角度考虑,加密电文还可以防止未授权的第三方擅自使用,从而可以达到便于管理的目的。具体操作见图 2,包括以下步骤:

[0042] (1) 发送方编辑电文信息的同时,产生 RSA 密钥对;

[0043] (2) 依照 AES 标准流程对电文信息进行加密,再利用 RSA 的私钥对特定信息进行签名(例:子帧中 100 ~ 300 区间的电文信息);

[0044] (3) 将签名、加密后的电文信息上注给卫星;

[0045] (4) 当接收方(接收机)收到通过卫星转发器发射过来的密文后,利用发送方 AES 的加密密钥(加密密钥可以通过运控中心颁发给授权用户的电子卡获得)进行解密;

[0046] (5) 进行 RSA 的公钥解密验证签名的正确性(公钥可以通过地面运控中心或官网

上获得),若签名验证无效则丢弃导航电文;反之,则利用所接收到电文进行解算。

[0047] 进行所述的签名时,包括以下步骤:

[0048] RSA 算法初始化的时候一般要填入密钥长度,在 96-1024bits 间。鉴于卫星通信效率和实时性考虑,本实施例选用密钥长度为 155bit。

[0049] RSA 密钥产生算法

[0050] Step1:随机产生两个大质数(155bit 长度) p, q ;

[0051] Step2:计算 $n = p \times q, d = e^{-1} \bmod(\phi(n))$ $\phi(n) = (p-1) \times (q-1)$ (mod 代表同余符号);

[0052] Step3:随机选取一个与 $\phi(n)$ 互素的整数 e 作为公开密钥,即 $\gcd(e, \phi(n)) = 1$;

[0053] Step4:计算私有密钥 $d = e^{-1} \bmod(\phi(n))$;

[0054] 公开 n, e , 保密 p, q, d , 就可以使用它们进行签名验证工作了。

[0055] 签名验证过程

[0056] Step1:对签名的原始数据 M 进行加密前,首先将消息 M 分解成为消息比特串分组,分组长度 L 保证 $2^L \leq n$,若用 m 表示某一分组后的消息的十进制表示,则 $0 \leq m \leq n$;然后取得用自己的私钥 d ,执行分组模指数运算: $c = m^d \bmod n$,将运算后的分组信息组合成签名 C ,最后通过信道将签名 C 及文本 M 一起发送;

[0057] Step2:接收方从网上公布的公钥簿上获得公钥 e ,然后按照和签名相同的分组方式执行下面的模指数运算: $m = c^e \bmod n$,然后将解算出的 m , 组合成 M' ;

[0058] Step3:比较 M 和 M' ,如果相同则认为签名有效,反之则认为此次签名不是真实的,拒绝接受信息。

[0059] 外层数据加密

[0060] 利用 AES 的加密算法,加密前后数据长度一致,所以经其加密后的密文不会对帧长度产生影响。本实施例采用 128bit 密钥,对于原始数据也是采用每 128bit 为一组进行加密,所得密文长度也是 128bit 为一组,然后重新填充至原始帧结构中进行播发。若子帧结构的长度不是 128bit 的倍数,则先将分组长度满足 128bit 的分组用 AES 进行数据加密,剩下的不足 128bit 的数据和前一组加密后的密文重组凑成 128bit 然后再进行加密,最后将密文按次序重新填充到原有帧长度中。具体操作见附图 3。

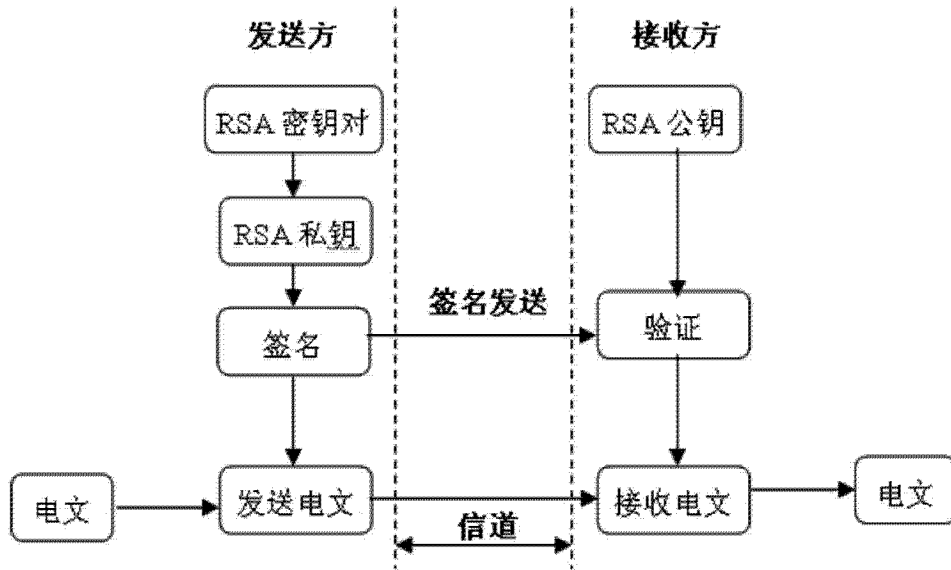


图 1

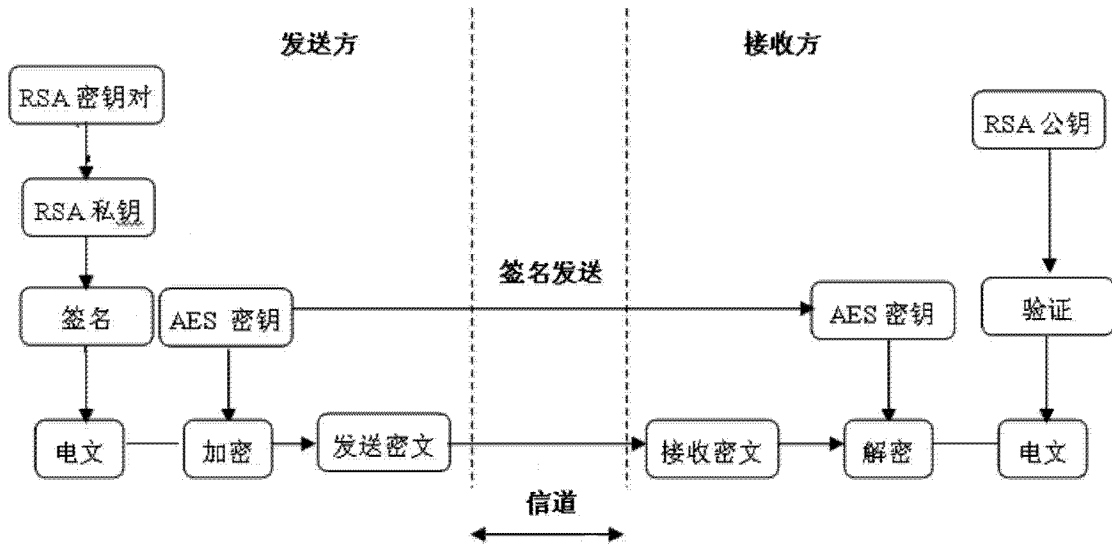


图 2

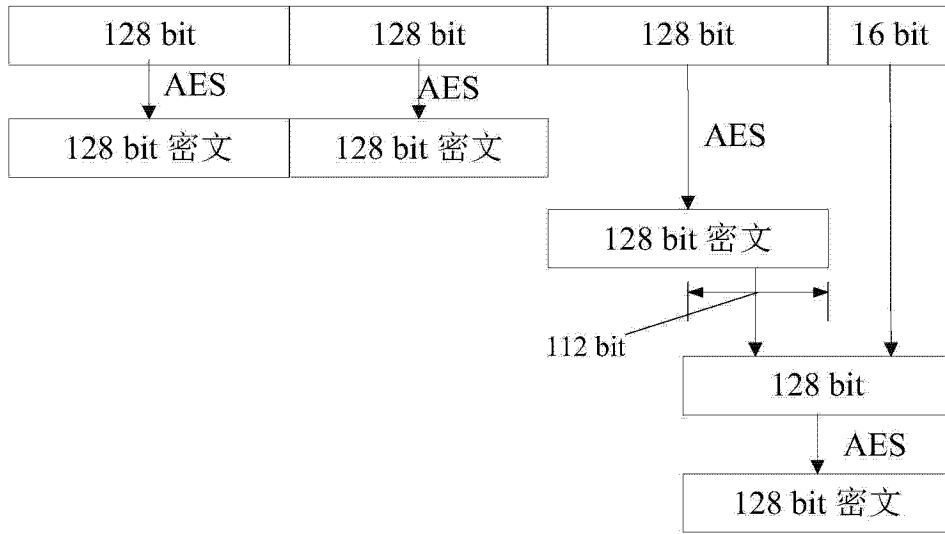


图 3