基于身份的卫星网络密钥管理方案

周 星[1],刘 军[1],董春冻[2],张玉静[1]
(1. 解放军理工大学 指挥信息系统学院,江苏 南京 210007;
2. 解放军理工大学 通信工程学院,江苏 南京 210007)

摘 要:为进一步提高卫星网络密钥管理的效率,文中假设地面控制中心(Telluric Control Center,TCC)作为 PKG(Private Key Generation)是完全可信且性能强大的,由 TCC 为卫星计算私钥,并利用 Shamir 秘密共享方案将私钥分片传送给各卫星节点,在会话密钥协商过程中利用节点私钥加密时间戳和位置信息以保证新鲜性和认证性。文中利用串空间证明了该方案密钥传输过程的机密性和认证性以及会话密钥的认证性,并和现有的协议进行性能对比,结果表明在假设条件下,该方案是可行的,且性能消耗小。因此文中方案具有较强的实用性。

关键词:卫星网络;密钥管理;基于身份;串空间
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2013)11-0148-04
doi:10.3969/j.issn.1673-629X.2013.11.037

A Scheme of Identity-based Satellite Network Key Management

ZHOU Xing[1],LIU Jun[1],DONG Chun-dong[2],ZHANG Yu-jing[1]
(1. College of Command and Information System,PLA University of Technology,Nanjing 210007,China;
2. College of Communication Engineering,PLA University of Technology,Nanjing 210007,China)

Abstract:To further improve the efficiency of satellite network key management,assume TCC (Telluric Control Center) as PKG (Private Key Generation) is totally trustable and has a strong computing ability,using TCC to calculate private key for each satellite and Shamir secret sharing scheme to transfer private key to each satellite node in piece,it uses each node's private key to encrypt timestamp and location information of the node to guarantee freshness and authentication. In this paper,use strand space model to prove security and authentication in the key transfer process,and the authentication of session key. Compared with the current protocols,it turns out that,under the assuming condition,the scheme can be thought of as practical and has less efficiency consuming,thus it is practical in actual use.

Key words:satellite network;key management;identity-based;strand space

0 引 言

1984 年,Shamir 提出了基于身份的密码体制[1],在基于身份的密码体制中,用户的公钥能够根据代表用户身份的信息计算得出,省去了复杂的公钥管理机制,因此得到了广泛的应用。通常认为基于身份的密码体制存在密钥问题,即 PKG 知道用户的私钥,因而不诚实的 PKG 可以窃听用户的通信[2]。

在卫星网络密钥管理方案中,CCSDS 提出了基于 PKI 的密钥管理方案[3],然而它需要证书机制,将带来较大的额外开销。彭长艳等人在空间网络中利用基于身份的密码体制提供安全服务[4],但是没有考虑密钥更新问题。罗长远等人为解决集中式密钥管理困难以及公钥证书开销大的问题,提出了一种基于身份的空间物理分布式密钥管理方案[5],并给出了私钥更新、主密钥分量更新和会话协商等策略,实现了卫星节点间的身份认证。然而其无法抵御合法节点申请私钥时的拒绝服务攻击,且存在密钥托管问题。吴杨等人提出一种基于身份的分布式卫星网络私钥管理方案[6],它能够避免更新请求发送拥塞现象,它能够抵御多种外部攻击,且性能相对证书机制有较大提高,但在会话密钥协商过程中容易产生中间人攻击。

文中假定 TCC 性能强大,且绝对可信,可以作为安全的私钥生成中心(PKG: Private Key Generation),为解决密钥更新问题,将时间因子引入公钥计算公式,

收稿日期:2013-01-25 **修回日期**:2013-05-06 **网络出版时间**:2013-08-28
基金项目:江苏省自然科学基金(BK2008090)
作者简介:周 星(1988-),男,四川广安人,硕士研究生,CCF 会员,研究方向为安全协议、无线网络安全;刘 军,硕士,教授,研究方向为安全协议、无线网络安全、网络对抗。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20130828.0818.010.html

同时为解决私钥传输问题,文中还根据 Shamir 秘密共享机制,设计了基于 Shamir 秘密共享机制的私钥传输机制。TCC 仅需要在各节点的私钥更新前将节点的私钥安全完整地发送给私钥就能够完成密钥更新工作,不需要复杂的密钥更新步骤。为解决会话密钥传输过程中的中间人攻击和重放攻击,文中将时间戳和节点位置信息加密后引入 D-H[7] 密钥协商协议中。通过证明,该方案的私钥传输过程具备保密性和认证性,会话密钥协商过程具备认证性。

1　相关知识

1.1　双线性对

假设 G_1 是生成元为 P 阶为 q 的加法循环群,G_2 是生成元为 P 阶为 q 的乘法循环群,a,b 是 Z_q^* 的元素,假设群 G_1 和 G_2 都满足计算性难题,则满足下列性质的一个映射 $\hat{e}:G_1 \times G_2 \rightarrow G_2$ 是一个双线性对。

(1) 双线性:$\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}(a,b \in Z_q^*,P,Q \in G_1)$;

(2) 非退化:存在 $P,Q \in G_1,\hat{e}(P,Q) \neq 1$;

(3) 可计算:存在一个有效的算法,对任何 $P,Q \in G_1$ 都能够快速地计算出 $\hat{e}(P,Q)$。

椭圆曲线上的 Weit 对和 Tate 对可以用来计算双线性映射 $\hat{e}$。

1.2　计算难题

BDH(Bilinear Diffie-Hellman)问题:对于任意 $a,b,c \in Z_q^*$,由 $<P,aP,bP,cP>$ 计算 $\hat{e}(P,P)^{abc}$。

CDH(Computational Co-Diffie-Hellman)问题:对于任意 $<p_1,p_2,a\,p_1,b\,p_2>$,其中 $p_1,p_2 \in G_1,a,b \in Z_q^*$ 未知,计算 $abP_2 \in G_2$。

2　密钥管理方案

2.1　密钥初始化

在卫星发射之初,由地面控制中心(TCC:Telluric Control Center)为每颗卫星计算公私钥对。其中公钥包括卫星的 id 及位置信息,为了既能够方便地进行密钥更新又能够保留基于身份密码体制的优点,让节点方便地互相获知其他节点的公钥,在公钥中引入变化因子。具体为:$k_{\text{pub}}=H(i \| (n_i,m_i) \| [\frac{t-t_0}{w_i}])$,其中 i 表示卫星的身份标识,n_i 表示卫星处在第 n 个轨道平面,m_i 表示卫星在第 n 个轨道平面的第 m 个位置,w_i 是标识为 i 的卫星密钥更新周期,t 为当前时间,t_0 为地面控制中心统一设定的初始时间,各卫星都一致,$[\frac{t-t_0}{w_i}]$ 表示对 $\frac{t-t_0}{w_i}$ 向零取整,表示当前卫星已经过多少密钥更新周期。系统运行过程中,i,n_i,m_i,w_i 公开,t_0 全系统统一。各卫星的私钥由且仅由 TCC 计算。w_i 的大小应适当选取,太大,容易被攻击,太小,容易造成节点的公钥与其他节点计算得出的私钥不匹配,可以以一天或者几天作为更新周期。

2.2　密钥更新

由于 TCC 性能强大,且可以认为是绝对可信的,而在 LEO 卫星组成的单层网络中,各卫星节点功能相同、地位均衡,因此从安全及性能考虑,可以利用 TCC 为各节点计算私钥。TCC 为卫星计算私钥的另一个优点在于在大多数应用中,TCC 需要知道各卫星节点的私钥以解密网络中传输的机密消息,而如果用户要求保密性,可以在应用层再进行加密。

2.3　密钥分发

TCC 为各节点计算私钥后,为提高安全性和抗毁性,再利用 Shamir 秘密共享机制生成私钥分量,连接上时间戳和哈希函数生成一个消息进行传输。由于不是所有的卫星都可以直接覆盖地面控制中心,因此可以从卫星节点中选择 n 个能够直接覆盖 TCC 的 LEO 卫星作为密钥分配中心(KDC:Key Distribution Center),以帮助进行消息的传输。标识为 i 的卫星计算第 n 个私钥的具体流程为:

(1) 在 $t_0+n*w_i+t_a$(t_a 的值应该介于卫星 i 的密钥更新周期和向 n 个卫星传送消息需要的时间之间)时刻之前,TCC 为标识为 i 的卫星计算第 n 个私钥 $k_{i\_n}^{-1}$,为检验生成的私钥是否有效,验证 $\hat{e}(k_{i\_n}^{-1},P) \stackrel{?}{=} \hat{e}(k_{i\_n},k_{\text{TCC}})$,其中 P 是 G_1 上的生成元,$\hat{e}$ 是双线性映射,如果不成功,则再重新生成一次,如果成功,利用节点 i 的当前公钥(即第 $n-1$ 个公钥)加密得到 $(k_{i\_n}^{-1})_{k_{i\_(n-1)}}$,利用 Shamir 秘密共享方案,将 $(k_{i\_n}^{-1})_{k_{i\_(n-1)}}$ 分成 n 份私钥分量 s_i,再附上 TCC 的私钥加密的时间戳 TS_{TCC} 以及哈希值,最后生成消息 $s_i \| (\text{TS}_{\text{TCC}})_{k_{\text{TCC}}^{-1}} \| H(s_i \| (\text{TS}_{\text{TCC}})_{k_{\text{TCC}}^{-1}})$。

(2) TCC 在 n_i 卫星覆盖的时候,将该 $s_i \| (\text{TS}_{\text{TCC}})_{k_{\text{TCC}}^{-1}} \| H(s_i \| (\text{TS}_{\text{TCC}})_{k_{\text{TCC}}^{-1}})$ 消息以消息的形式经由 n_i 卫星发送给卫星 i,其中发送时按序发送,即 s_i 发送给卫星 n_i。

(3) 卫星 i 每当收到消息后,都首先验证完整性和新鲜性,如果验证成功,则缓存 s_i。对新鲜性有如下规定:s_{i_k} 晚于 $s_{i\_(k-1)}$ 被接收。

(4) 当卫星 i 完成接收来自 n 个 n_i 卫星的消息并得出 s_i 后,利用 Lagrange 多项式重构得出 $(k_{i\_n}^{-1})_{k_{i\_(n-1)}}$,再利用当前私钥(第 $n-1$ 个私钥)解密得出更新后的私

钥。

(5) 生成时间戳 TS_i 并用更新后的私钥加密后发给 TCC。

2.4 会话密钥协商

为解决会话密钥协商过程中可能出现的中间人攻击问题,将认证机制和时间戳引入 D - H 密钥交换协议中[8]。A 与 B 之间的密钥协商过程如下:

(1)A 选择随机数 r_A,并将时间戳和自身位置用自己的私钥加密后一起发送给 B。

$r_A, g^{r_A}(\mathrm{mod}p), (TS_1, n_A, m_A)_{k_A^{-1}}$

(2)B 检查时间戳 TS 的新鲜性,用 n_A, m_A 以及 A 的私钥共同验证 A 的身份,通过后,选择随机数 r_B,计算 $K_{xM} = (g^{r_A})^{r_M}(\mathrm{mod}p)$,并将 $g^{r_B}(\mathrm{mod}p), H_1(g^{r_B}\mathrm{mod}p, k_{AB})$ 与新的时间戳 TS_2 和 B 的位置用 B 的私钥加密后传送给 A。

$g^{r_B}(\mathrm{mod}p), H_1(g^{r_B}\mathrm{mod}p, k_{AB}), (TS_2, n_B, m_B)_{k_B^{-1}}$

(3)A 检查 TS_2 的新鲜性并同样利用 B 的位置和私钥以验证身份,验证成功后,计算 $k_{AB} = (g^{r_A})^{r_B}\mathrm{mod}p$,并计算 $H_2(k_{AB})$,将它与新的时间戳用 A 的私钥加密后传送给 B。

$H_2(k_{AB}), (TS_3)_{k_A^{-1}}$

3 安全性分析

文中利用串空间模型[9]中的认证测试理论[10]分析协议的机密性和认证性。

图 1 为密钥传输方案的形式化。

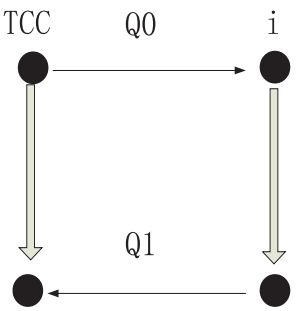

图 1 密钥传输方案的形式化

其中 $Q_0 = (k_{i\_n}^{-1})_{k_{i\_(n-1)}} \| (TS_{TCC})_{k_{TCC}^{-1}} \| H((k_{i\_n}^{-1})_{k_{i\_(n-1)}} \| (TS_{TCC})_{k_{TCC}^{-1}}))$

$Q_1 = (TS_i)_{k_i^{-1}}$

TCC 的串:$s_{TCC} \in TCC[(k_{i\_n}^{-1})_{k_{i\_(n-1)}} \| (TS_{TCC})_{k_{TCC}^{-1}} \| H((k_{i\_n}^{-1})_{k_{i\_(n-1)}} \| (TS_{TCC})_{k_{TCC}^{-1}})), (TS_i)_{k_i^{-1}}]$,其迹为:

$< +Q_0, -Q_1 >$

节点 i 的串:$s_i \in i[(k_{i\_n}^{-1})_{k_{i\_(n-1)}} \| (TS_{TCC})_{k_{TCC}^{-1}} \| H((k_{i\_n}^{-1})_{k_{i\_(n-1)}} \| (TS_{TCC})_{k_{TCC}^{-1}}), (TS_i)_{k_i^{-1}}]$,其迹为:

$< +Q_1, -Q_0 >$

3.1 私钥的机密性

由于私钥被加密后再分成 n 份,攻击者要获知节点私钥,必须能够监听到 n 份私钥分量以及暴力破解重构的私钥。

机密性证明:

命题1:假设 $\sum$ 为协议的串空间,C 为串空间中的一个束;$k_{TCC}^{-1}, k_{i-(n-1)}^{-1} \notin k_p$;$k_{TCC}^{-1}, k_{i\_n}^{-1}, k_{i-(n-1)}^{-1}$ 在 C 中唯一产生,令 $s = \{k_{TCC}^{-1}, k_{i\_n}^{-1}, k_{i-(n-1)}^{-1}\}$,$\underline{K} = (K/S)^{-1}$,则对于任何正常节点 $m \in C$,$\mathrm{term}(m) \notin I_{\underline{K}}[S]$。

证明:采用反证法。假设存在正常节点 $m \in C$ 令 $\mathrm{term}(m) \in I_{\underline{K}}[S]$,则 $k_{TCC}^{-1}, k_{i\_n}^{-1}, k_{i-(n-1)}^{-1}$ 中至少有一项为 $\mathrm{term}(m)$ 的子项。由定义可知,TCC、i 节点中不包含以 $k_{TCC}^{-1}, k_{i-(n-1)}^{-1}$ 为子项的项,因此 $k_{i\_n}^{-1}$ 一定为 $\mathrm{term}(m)$ 的子项。

若 m 符号为正,则 $k_{i\_n}^{-1}$? $\mathrm{term}(m)$ 意味着 $m = < s_{TCC}, 1 >$,由于 $k_{i\_n}^{-1}$ 在 $\sum$ 中唯一产生,因而 $\mathrm{term}(m) = (k_{i\_n}^{-1})_{k_{i\_(n-1)}} \| (TS_{TCC})_{k_{TCC}^{-1}} \| H((k_{i\_n}^{-1})_{k_{i\_(n-1)}} \| (TS_{TCC})_{k_{TCC}^{-1}}) \in I_{\underline{K}}[S]$,则 $k_{i-(n-1)}^{-1} \in \underline{K}$,该结论与前提条件 $\underline{K} = (K/S)^{-1}$ 矛盾。因而假设不成立,命题成立。

命题1 证明了在满足假设条件 $k_{TCC}^{-1}, k_{i-(n-1)}^{-1} \notin k_p$ 的前提下,该密钥协商协议能保证传输过程中 $k_{i\_n}^{-1}$ 的机密性。

3.2 认证性

文中仅验证端到端的认证性。由于私钥由目的卫星的当前公钥加密,仅可由当前私钥对其解密,保证了对目的卫星的认证性。该方案假定 TCC 是安全可信的,为防止非法冒充 TCC,还用 TCC 的私钥加密当前时间以抵御冒充和重放。

认证性证明:

命题2:假设 $\sum$ 为协议的串空间,C 为串空间中的一个束,包含 C - height 为 2 的串 $s_{TCC} \in TCC[(k_{i\_n}^{-1})_{k_{i\_(n-1)}} \| (TS_{TCC})_{k_{TCC}^{-1}} \| H((k_{i\_n}^{-1})_{k_{i\_(n-1)}} \| (TS_{TCC})_{k_{TCC}^{-1}})), (TS_i)_{k_i^{-1}}]$;$k_{TCC}^{-1} \notin k_p$;$TS_{TCC}$ 在 $\sum$ 中唯一产生,则 C 中一定存在一个正常的串 $s_i \in i[(k_{i\_n}^{-1})_{k_{i\_(n-1)}} \| (TS_{TCC})_{k_{TCC}^{-1}} \| H((k_{i\_n}^{-1})_{k_{i\_(n-1)}} \| (TS_{TCC})_{k_{TCC}^{-1}}), (TS_i)_{k_i^{-1}}]$,且 C - height 为 2。

证明:首先确定串对 TS_{TCC} 构成一个出测试,由于 $k_{TCC}^{-1} \notin k_p$,$(TS_{TCC})_{k_{TCC}^{-1}}$ 除了在节点 $< s_{TCC}, 1 >$ 中出现在 $(TS_{TCC})_{k_{TCC}^{-1}}$ 外,不以任何组元形式出现,且 TS_{TCC} 为节点 $< s_{TCC}, 1 >$ 处消息 $(TS_{TCC})_{k_{TCC}^{-1}}$ 的一个测试组元,所以边 $< s_{TCC}, 1 > \Rightarrow^+ < s_{TCC}, 2 >$ 为对于 $(TS_{TCC})_{k_{TCC}^{-1}}$ 中消息 $(TS_{TCC})_{k_{TCC}^{-1}}$ 的一个出测试。

由出测试可知,一定存在正常的节点 $n_0, n_1 \in C$ 使

得$(TS_{TCC})_{k_{TCC}^{-1}}$为节点$n_0$的一个组元,且边$n_0 \Rightarrow^+ n_1$为对于$TS_{TCC}$的一条变换边。

因为节点n_1为正的正常节点,且$(k_{i_n}^{-1})_{k_{i_(n-1)}} \| (TS_{TCC})_{k_{TCC}^{-1}} \| H((k_{i_n}^{-1})_{k_{i_(n-1)}} \| (TS_{TCC})_{k_{TCC}^{-1}}))$,$TS_{TCC}$在节点$< s_{TCC},1 >$处唯一产生,则一定存在正常的负节点$n_0$来接收$TS_{TCC}$。由于$n_0$为负节点,一定位于某些$i$的串$s_i \in i[(k_{i_n}^{-1})_{k_{i_(n-1)}} \| (TS_{TCC})_{k_{TCC}^{-1}} \| H((k_{i_n}^{-1})_{k_{i_(n-1)}} \| (TS_{TCC})_{k_{TCC}^{-1}}))$,$(TS_i)_{k_i^{-1}}]$的节点$< s_i,1 >$中。由$< s_i,1 > \Rightarrow^+ < s_i,2 >$及$\text{term}(< s_i,2 >) = (TS_i)_{k_i^{-1}}$可知,$k_i'^{-1} = k_i^{-1}$,$TS_i' = TS_i$,从而存在一个正常的串$s_i \in i[(k_{i_n}^{-1})_{k_{i_(n-1)}} \| (TS_{TCC})_{k_{TCC}^{-1}} \| H((k_{i_n}^{-1})_{k_{i_(n-1)}} \| (TS_{TCC})_{k_{TCC}^{-1}}))$,$(TS_i)_{k_i^{-1}}]$且$C-\text{height}$为$2^{[11-12]}$。

i实现了对TCC的认证,TCC对i的认证性证明类似。

此外,该方案包含了一个对TS_{TCC}的出测试,根据出测试的新鲜性质保证了协议中TS_{TCC}的新鲜性,可以防止恶意的重放攻击。

由于密钥更新过程并不需要各卫星节点主动发起,因此不存在拒绝服务攻击。

密钥协商过程的安全性证明与密钥分发过程类似。

4　计算复杂度分析

计算复杂度分析见表1。其中MG表示字符串到G_1上的点映射运算,MD表示G_1上的数乘运算,e表示双线性对运算,PA表示G_1上的点加运算,I表示插值运算,H表示哈希运算,DS表示私钥的解密运算,DP表示公钥的解密运算,EP表示公钥的加密运算,ES表示私钥的加密运算,S表示Shamir秘密共享方案所需运算,N表示节点数目,t表示多项式恢复的门限值,n表示选中的可以直接覆盖TCC的卫星数目,CL表示申请时刻合法性检查,/表示开销很小或无开销。

表1　方案计算复杂度对比

		申请节点开销	应答节点开销	地面控制中心开销
文献[5]方案	私钥更新	1MG+(2+t)MD+4te+(1+t)PA+1I	(Nt/n)(4MD+2e+2PA)	/
	会话密钥生成	1MG+2MD+2e	1MG+2MD+2e	/
文献[6]方案	私钥更新	1MG+(2+t)MD+4te+(1+t)PA+1I+hDS	(Nt/n)(4MD+2e+2PA)+1EP+1CL	/
	会话密钥生成	1MG+2MD+2e	1MG+2MD+2e	/
该方案	私钥更新	t(H+DP)+1I+2e+ES+DS	/	MD+EP+S+n(ES+H)+2e
	会话密钥生成	1MG+2MD+2e+2ES+1DS	1MG+2MD+2e+1ES+2DS	/

从表1可以看出,文中的申请节点的双线性对运算相比其他方案大幅减小,地面控制节点的开销也明显减小。即该方案用计算量相对较小的加解密操作和哈希操作代替了复杂的双线性运算。该方案总共增加了3次私钥加密运算和3次公钥解密运算,实现了密钥协商过程的身份认证和新鲜性保证。对于远距离通信中的密钥交换更有实用价值。

5　结束语

文中以TCC是安全可信的和性能强大为前提,提出了一种新的卫星网络密钥管理方案,它由TCC负责为各卫星计算私钥,并利用Shamir密钥共享方案将私钥机密完整地传送到卫星节点。针对密钥协商过程中可能的中间人攻击和重放攻击,文中将时间戳和位置用卫星的私钥加密实现对新鲜性和认证性的保护。文中最后利用串空间模型证明了密钥传输过程的机密性和认证性,以及会话密钥协商过程中的认证性。该方案中,卫星节点消耗较小,主要的性能消耗发生在TCC,在假设背景下,设计的方案是可行的,具有一定的实用价值。

参考文献:

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]//Proceedings of CRYPTO'84. Berlin, Germany: Springer-Verlag, 1984: 47-53.

[2] 张福泰,孙银霞,张　磊,等. 无证书公钥密码体制研究[J]. 软件学报,2011,22(6):1316-1332.

[3] Balasubramanian A, Mishra S, Sridhar R. Secure key management for NASA space communication[EB/OL]. 2005. http://gltrs.grc.nasa.gov/reports/2005/CP-2005-213878.

[4] 彭长艳,沈亚敏,王　剑,等. 基于身份的空间网络安全研究[J]. 飞行器测控学报,2008,27(3):56-62.

[5] 罗长远,李　伟,邢洪智,等. 空间网络中基于身份的分布式密钥管理研究[J]. 电子与信息学报,2010,32(1):183-188.

[6] 吴　杨,矫文成,潘艳辉,等. 基于身份的分布式卫星网络

(下转第 156 页)

4 系统测试

在开发完成后,为了测试系统是否具备投入正常使用的条件,对系统做了以下几个方面的测试。

功能测试:使用手机分别发送命令 102211067#y#0521#08、092212024#c#1352#16、112211065#s#0943#23 和 311#c#0432,以验证学生的预约实验、查询实验和删除实验的功能和教师的查询实验功能,在命令发送出去一段时间后,收到了来自系统的回复信息“欢迎使用中南大学物理实验中心实验室教学辅助系统,您已操作成功”;发送命令 139897789#y#0521#08(身份错误)、102211067#0521#y#08(命令格式错误)、102211067#y#2421#08(时间段超出范围)、102211067#y#0521#34(实验选择错误)后,收到系统回复“您的输入不正确,请重新输入”, 命令发送后,通过互联网访问系统,刷新信息,相关实验信息已经更新,证明操作已经成功。

性能测试:将系统开启,连续工作三天三夜后,重复上述的功能测试,系统依然工作正常;同时组织了 50 台手机同时向系统发送短消息,全部得到回复,且操作成功。

速度测试:该系统测试用的 GSM 模块,在信号良好的情况下每小时能发送或接收 500 至 700 条短信。而该系统启动后,从用户手机发送短消息瞬间开始计时,到接收到系统回复这一过程,平均耗时 11 秒,也就是说平均每小时接收或发送 654 条短信,在可接收范围内,在正式投入使用后,换用更先进的 GSM 模块,还可以进一步提高整个系统的响应速度。

5 结束语

基于 GSM 短信息的实验选课系统使用了手机短信作为通信手段,在 VS2008 平台上,结合 MFC、多线程技术以及数据库技术进行开发,各项功能指标均达到了要求,使用户能够通过操作手机即可完成各项功能,是对实验教学系统的有效补充。使用该系统,能使实验室管理更加人性化,给用户和系统管理员带来了很大的方便,因此,该系统在实验室开放中具有一定的应用前景。

参考文献:

[1] 刘华东,韩红江. 开放实验室,构建实验教学新体系[J]. 中国高等教育,2003(13):30-31.

[2] 佟 颖,白海会,吴晓荣. 实验室信息化管理系统的设计与实现[J]. 现代教育技术,2008,18(2):101-104.

[3] 马增良,牛俊省. 基于 GMS /SMS 的短信息应用平台设计与实现[J]. 仪表技术与传感器,2003(12):32-33.

[4] Yu D, Chen N. Design and implementation of secure SMS messaging system[J]. Advances in information sciences and service sciences,2012,4(23):72-78.

[5] 王晓娟,黄忠全,张根保. 短消息系统设计与实现[J]. 重庆大学学报,2004,27(5):96-98.

[6] 宣彩平,王 皓,邹国良. 利用 GSM 无线模块发送短消息[J]. 计算机应用,2004,24(5):148-150.

[7] 关 克,陈 阳,宋 柏. 基于 ARM 的传感器校验仪 GSM 数据传输的研究[J]. 制造业自动化,2012,34(3):34-36.

[8] 涂巧玲,戴宇航. 基于手机短信息的人体跌倒报自动报警研究[J]. 计算机工程与应用,2008,44(12):241-243.

[9] 孙丘伟,余 臻. 基于 GSM 的短信报警收发平台设计[J]. 福州大学学报(自然科学版),2008,36(Sup):44-48.

[10] Qian Z,Luo D,Wu S. Analysis and design of a mobile forensic software system based on AT commands[C]//Proc of 2008 IEEE international symposium on knowledge acquisition and modeling. Wuhan,China:[s. n.],2008.

[11] Jindal V. PC-to-PC communication via RS-232 serial port using C[J]. Electronics world,2006,112(1837):25-29.

[12] 石海杰,常 虹. 基于 VC 的多线程串口通信程序设计[J]. 可编程控制器与工厂自动化,2009(9):65-67.

(上接第 151 页)

私钥管理方案[J]. 计算机科学,2011,38(10):96-99.

[7] Shamir A. How to share a secret[J]. Communications of the ACM,1979,22(11):612-613.

[8] Diffie W. New directions in cryptography[J]. IEEE transactions on information theory,1976,22(6):644-654.

[9] Fabrega F J T,Herozog J C,Guttman J D. Strand space:why is a security protocol correct? [C]//Proc of 18th IEEE symposium on research in security and privacy. Los Alamitos:IEEE computer society press,1998:160-171.

[10] 刘家芬. 安全协议形式化分析中认证测试方法的研究[D]. 成都:电子科技大学,2008.

[11] Yuan Xing,Rui Jiang. MRST:multi routing based secure data communication in mobile Ad Hoc netwotks[C]//Proc of sixth international conference on innovative mobile and internet services in ubiquitous computing. Palermo,Italy:IEEE,2012.

[12] 邢 媛,蒋 睿. 基于串空间模型的 UMTS-AKA 协议安全分析与改进[J]. 东南大学学报(自然科学版),2010,40(6):1163-1168.

基于身份的卫星网络密钥管理方案

作者： 周星， 刘军， 董春冻， 张玉静， ZHOU Xing， LIU Jun， DONG Chun-dong， ZHANG Yu-jing

作者单位： 周星,刘军,张玉静,ZHOU Xing,LIU Jun,ZHANG Yu-jing(解放军理工大学 指挥信息系统学院,江苏 南京,210007)， 董春冻,DONG Chun-dong(解放军理工大学 通信工程学院,江苏 南京,210007)

刊名： 计算机技术与发展

ISTIC

英文刊名： Computer Technology and Development

年，卷(期)： 2013(11)