基于身份签名的北斗二代民用D2导航电文认证协议

吴志军,杨一鸣,张 云
(中国民航大学电子信息与自动化学院,天津300300)

摘 要: 北斗二代民用D2导航电文(BeiDou-Civil Navigation Message-D2, B-CNAV-D2)信息在开放的信道中传输,缺乏完整性保护机制,面临信息被伪造和篡改的威胁,容易遭受欺骗攻击.为了保障B-CNAV-D2信息的完整、真实和可用,本文在分析B-CNAV-D2信息组成结构的基础上,设计了基于身份签名体制的北斗二代民用D2导航电文信息认证协议.该协议提供信息源认证和信息完整性保护,实现B-CNAV-D2信息防篡改和防伪冒的功能.B-CNAV-D2信息认证协议可以有效地减少传统签名认证方案中数字证书分发和更新等处理环节,提高认证协议的整体效率和认证效率,拥有较好的认证时效性与较低的计算成本和通信成本.

关键词: 北斗民用D2导航电文; 信息源认证; 完整性; 抗欺骗; 防篡改
中图分类号: TN915 **文献标识码:** A **文章编号:** 0372-2112(2021)09-1790-09
电子学报URL: http://www. ejournal. org. cn **DOI:** 10. 12263/DZXB. 20200428

The Authentication Protocol for Civil Navigation Message D2 of Beidou II Based on Identity Signature

WU Zhi-jun, YANG Yi-ming, ZHANG Yun
(*School of The Electronic Information and Automation, Civil Aviation University of China, Tianjin* 300300, *China*)

Abstract: The Beidou II civil navigation message D2(B-CNAV-D2) in Beidou navigation satellite system (BDS) are transmitted in an open channel without integrity protection, facing the threat of information being tampered and falsified, and vulnerable to spoofing attacks. In order to guarantee the integrity, authenticity and availability of B-CNAV-D2 information, based on the analysis of the composition structure of B-CNAV-D2, this paper presents an authentication protocol based on the identity signature to provide B-CNAV-D2 information source authentication and integrity protection. The authentication protocol is designed to achieve the functions of anti-tampering and anti-spoofing for B-CNAV-D2. The application of authentication protocol in B-CNAV-D2 can effectively reduce the processing steps of digital certificate distribution and update in traditional signature authentication schemes, improve the overall efficiency and authentication efficiency, and has better performance in authentication timeliness, and lower computing and communication costs.

Key words: Beidou II civil navigation message D2; information source authentication; integrity; anti-spoofing; tamper-proof

1 引言

北斗卫星导航系统BDS(BeiDou navigation Satellite system)中采用的民用导航电文信息B-CNAV(BDS Civil NAVigation)是北斗用户实现导航和定位的核心数据.这些数据内容向公众公开,并在未加密的信道中播发,具备开放的属性[1].另外,所有GNSS(Global Navigation Satellite Syslem)的民用导航电文信息都没有提供完整性保护措施.因此,B-CNAV信息很容易遭到信息篡改和伪造,导致欺骗(Spoofing)攻击[2,3].所以,B-CNAV的开放性和未认证的特点存在被恶意利用的风险,使得B-CNAV信息的安全性面临威胁,可能导致严重影响B-CNAV信息的真实性和可靠性的欺骗攻击发生.因此必须针对B-CNAV信息进行安全认证,保障其完整性、真实性和可用性,使其具有抵御欺骗攻击的能力.

本文针对北斗民用D2导航电文信息B-CNAV-D2

收稿日期:2020-05-08;修回日期:2021-05-27;责任编辑:梅志强
基金项目:国家自然基金委员会与中国民航局联合基金资助项目(No.U1933108);国家自然基金青年基金项目(No.61802276);天津市教委科研计划项目(No.2019KJ117);中央高校基本业务费项目资助(No.ZXH2012P004)

的抗欺骗攻击,提出一种基于国产SM系列密码的B-CNAV-D2的安全认证协议—基于身份签名的北斗二代民用D2导航电文认证协议(也称为基于身份签名的B-CNAV-D2认证协议). 该协议的设计与北斗二代系统的组成及其服务流程融合,根据B-CNAV-D2的具体特点,针对B-CNAV信息认证技术构造一种新型的认证信号结构,进而设计了基于身份签名的B-CNAV-D2认证协议,为B-CNAV-D2提供一种鲁棒性的抗欺骗攻击的方法,从信息完整性、真实性和可用性方面,保障北斗民用导航电文信息安全. 该协议的设计考虑了在认证过程中数据开销较大以及首次认证时间过长的问题,可以在一定程度上得到缓解,并且在结构设计上无须增加额外的硬件成本.

2　相关工作

国际上针对GNSS民用导航电文CNAV信息抗欺骗攻击的研究成果采用的方法可以分为加密认证和信号检测(非加密认证)技术两大类[2,3]:第一类,加密认证方法,主要包括:基于椭圆曲线数字签名算法ECDSA(Elliptic Curve Digital Signature Algorithm)的签名认证机制[1]、基于时间效应流丢失容错认证TESLA(Timed Efficient Stream Loss-tolerant Authentication)的机制和混合认证机制(ECDSA+TESLA)[2];第二类,信号检测技术,主要包含:信号功率监测方法[4]、信号质量监测方法[5]、到达方向区分[6]、多天线技术与接收机自主相关监视等方法. 由于本文主要针对加密认证技术进行研究,这里对信号检测(非加密认证)技术就不再进行研究.

2.1　椭圆曲线数字签名算法ECDSA

针对GNSS的CNAV信息进行抗欺骗的研究主要采用密码算法实现安全认证的方法,统称为导航电文消息认证NMA(Navigation Message Authentication). 该方法是由Kyle D. Wesson等人[7]针对全球定位系统GPS(Global Positioning System)的CNAV信息首先提出的. 他们采用ECDSA生成签名,设计了数字签名在GPS的CNAV信息中具体的编排方式. 该方案采用数字签名方法生成签名信息,接收机用户根据认证信息,验证民用用户接收电文的可靠性和真实性. 此外,该方案利用密码学方法实现欺骗干扰识别的同时,从另一个角度分析,也降低了恶意攻击者成功发起攻击的可行性. 吴志军等人[1]利用ECDSA签名算法,提出了面向北斗卫星导航电文的认证方案,利用数字证书和北斗卫星导航系统独特的短报文通信给出了密钥更新与传输整体流程,通过仿真实验结果展现了该方法的抗欺骗性能. 但是数字签名属于非对称的密码体制,针对大数据量的导航卫星系统,非对称加密相对于对称加密而言就是计算开销非常大.

2.2　时间效应流丢失容错认证TESLA

针对数据量庞大的导航卫星,为了解决计算开销问题, Perrig A等人[8]针对GNSS的CNAV首先提出并设计了基于时间效应流丢失容错认证TESLA机制. 他们研究了TESLA协议设计的核心理论,并给出了实现步骤;之后他们分析了基于TESLA认证机制的安全性. 但他们在TESLA协议密钥延迟分发和密钥认证所引入的通信开销方面的考虑较少. Fernández-Hernández I等人[9]针对伽利略Galileo系统公开服务的脆弱性,指出采取数据认证的措施对该系统的脆弱性可能起到缓解作用. 首次给出了交叉认证的新概念,并结合交叉认证与TESLA协议,提出了一个具体的伽利略公开服务导航电文认证方案.

基于TESLA的CNAV信息认证方案虽然可以大大减少使用非对称加密认证的计算和认证开销,但是还增加了方案的复杂度. 即使TESLA协议具有松散的同步,但仍可能造成接收方可以因为同步而产生认证困难等问题.

2.3　基于身份的认证

袁木子等人[10]针对北斗卫星导航系统BDS,结合ECDSA与TESLA协议,分别设计了超帧电文认证方案和北斗主帧组电文认证方案,并对认证方案中电文的具体编排方式进行了说明. 该方案设计巧妙之处在于针对数据量少的主帧组认证采用对称加密,针对数据量大的超帧认证采用TESLA认证. 其中,超帧认证方案中给出了当前使用密钥与备用公钥共同组成的密钥更新信息. TESLA协议不具备标准化的算法规范,加上ECDSA在计算开销方面较大. 因此,混合认证方法无论从复杂度还是实现难度都比较高. 目前,针对GNSS信息抗欺骗(anti-spoofing)的方法中大多集中在接收机层面进行欺骗攻击信号检测. 这类方法存在几个缺陷:(1)在信号检测方面,无法保证正确检测的有效性;(2)在信息属性方面,无法满足民用导航电文信息的完整性、真实性和可用性;(3)在民用导航信息安全认证方面,存在密钥安全管理、加密认证导致的数据开销较大和接收机首次认证时间较长的问题;(4)在成本开销方面,需要增加额外的接收机硬件[2,3].

赵东昊等人[11]提出一种基于北斗战场通信的身份认证方案,该方案引入时间戳和节点的位置信息加入到身份认证中来. 但是该方案存在两个问题:(1)基于BDS提供的高精度定时功能,高质量定位功能和安全可靠的短消息通信功能,过于理想化. 实际中,链路是开放的,民用导航电文完整性没有保护措施,容易遭受欺骗攻击;(2)认证对象是接收机,可能遭受实体伪装攻击,导致接收的信息可能是伪冒的;本文的研究对象是针对实际开放链路和接收的导航电文信息. 而未通

过认证的导航信息则不被使用,可以保证接收的导航电文信息的真实性.

本文采用一种鲁棒性的抗欺骗方式—基于密码的信息认证,结合B-CNAV-D2信息的具体特性,提出一种基于身份签名的B-CNAV-D2认证协议,从信息安全角度保障B-CNAV-D2的完整性和真实性两个信息安全属性;从信息传输的可靠性角度,保障B-CNAV-D2的可用性和有效性两个传输特性. 此外,由于导航电文加密认证方案从导航电文自身结构与可扩展性入手展开设计,相比较于其他需要增加额外基础设施的欺骗防护方法,对系统整体影响以及引入的附加硬件成本较小[12].

3 导航电文认证协议

为了更好地描述北斗D2导航电文认证协议的设计,将采用的符号及其含义定义如表1所示.

表1 B-CNAV-D2信息认证协议中相关的符号说明

符号	符号含义说明
G_1, G_2	q阶循环群
P,Q	生成元
P_0	公开的系统参数
H_1,H_2,H_3	单向的哈希函数
KGC	密钥生成中心
GCS	北斗卫星地面控制段
ID_{GCS}	北斗卫星地面段身份ID信息
ID_{BD}	北斗卫星身份ID信息
M_{D2}	待签名的D2导航电文
S_{D2}	签名认证信息
‖	位连接处理
e	双线性映射

3.1 B-CNAV-D2电文预留位设计

B-CNAV-D2信息进行信息格式编排时,预留了分布较为集中且数量较为充裕的预留信息位. 由于B-CNAV-D2各个子帧中的预留信息位的数量与分布不一致,分别将B-CNAV-D2各个子帧拥有的预留信息位统计在表2中[10,13].

根据表2中对B-CNAV-D2中预留信息位数量的统计数据,可以直观地看出B-CNAV-D2的预留信息位长度较长. 针对B-CNAV-D2的签名认证信息,提出的认证协议将其设计在B-CNAV-D2中大块连续的预留信息位区段上,以便对其进行集中高效地管理和维护[10,13].

3.2 设计思路

北斗民用导航电文拥有固定的结构和导航信息编排格式. 本文协议设计在现有导航信息帧结构上插入认证信息. 插入后的公开民用卫星导航电文需要结合兼容的设计理念,尽量不要影响当前广大接收机对导航信息的正常解算,以避免引入导航信息认证机制对现有接收机

表2 B-CNAV-D2子帧1~5的预留信息位

子帧编号	页面编号	预留信息位位数
1	1	166 bit
	2、4、5、6、7、9	162 bit
	3	198 bit
	8	160 bit
	10	207 bit
2	1~6	65 bit
3	1~6	156 bit
4	1~6	190 bit
5	1~12、61~72	14 bit
	13、73	65 bit
	14~34、74~94、103~120	183 bit
	35	12 bit
	36	68 bit
	37~60、95~100	7 bit
	101	93 bit
	102	95 bit

解算导航电文造成不必要的影响. 本文将导航信息相对应的认证信息设计在北斗导航电文中预留出来的且未进行实际含义定义的信息位区段上. 这样设计的目的是在安排认证信息到北斗导航电文的基础上,最大限度地减小对现有接收机正常解算定位过程的影响.

B-CNAV-D2认证协议设计主要侧重于考虑B-CNAV-D2信息速率较快和B-CNAV-D2的实际电文结构中预留信息位较充裕的特性. 传统的公钥密码体制需要数字认证证书为公钥提供可靠性保证. 无证书密码体制虽然摆脱了传统的公钥密码体制中公钥安全性依赖于数字认证证书的困扰,不过仍然不可避免地需要签署并分发验签公钥. B-CNAV-D2信息拥有电文速率较快且播发周期较短的自身属性,如果选用传统的公钥密码体制或无证书密码体制设计B-CNAV-D2认证协议,签名信息将随着B-CNAV-D2以较快的电文速率播发,可能导致较为频繁地签署、分发、更新数字认证证书或验签公钥的情况出现,额外引入较高的开销,影响协议的整体认证效率.

在基于身份的密码体制中,身份信息与公钥自然绑定,既不需要额外的公钥生成和分发,又不需要引入数字认证证书,相比较于传统的公钥密码体制与无证书密码体制,更适用于B-CNAV-D2应用场景. 因此,本文针对B-CNAV-D2信息,结合基于身份的签名,设计B-CNAV-D2认证协议[10,11,14].

3.3 协议设计

B-CNAV-D2认证协议整体包括五个部分:系统建立、获取北斗地面段密钥、提取北斗卫星密钥、生成签名信息与验证签名信息. 在B-CNAV-D2认证协议具体设计中,除参与认证导航信息过程的收方用户之外,引

入三个实体:密钥生成中心KGC、北斗卫星地面控制段、北斗卫星. 其中,密钥生成中心作为可信中心,负责密钥生成、公共系统参数的提取及全生命周期安全管理. 北斗卫星主要播发导航电文信息给用户,以便用户利用导航信息进行定位[11,14,15].

(1)系统建立

由北斗卫星地面控制段履行KGC的职责,负责执行系统建立阶段各步骤. 首先,选择一个大素数q,并输出两个q阶的循环群G_1和G_2,得到双线性映射$e: G_1 \times G_1 \to G_2$. 选取$P$、$Q$作为$G_1$的两个生成元. 然后,随机地选取一个$s \in Z_q^*$作为主密钥,并运算$P_{\text{pub}} = sP$和三个安全的单向哈希函数$H_1:\{0,1\}^* \to Z_q^*$、$H_2:\{0,1\}^* \to Z_q^*$和$H_3:\{0,1\}^* \to Z_q^*$. 最后,北斗卫星地面控制段生成B-CNAV-D2文认证协议所需的全部公共系统参数$P_0 = \{q, G_1, G_2, e, P, Q, P_{\text{pub}}, H_1, H_2, H_3\}$,并公开发布出去. 而主密钥$s$作为秘密信息,需要安全地保存在北斗卫星地面控制段中.

(2)获取北斗卫星地面段密钥

北斗卫星地面段随机选取$r_{\text{GCS}} \in Z_q^*$,系统输入参数P_0、身份信息ID_{GCS}、主密钥s与r_{GCS},并依次计算以下三者$R_{\text{GCS}} = r_{\text{GCS}} \cdot P$, $H_{\text{GCS}} = H_1(\text{ID}_{\text{GCS}}, R_{\text{GCS}})$和$S_{\text{GCS}} = (r_{\text{GCS}} + H_{\text{GCS}} \cdot s) \cdot Q$. 由北斗卫星地面段利用可靠信道,将$\{R_{\text{GCS}}, S_{\text{GCS}}\}$发送给北斗卫星.

(3) 生成北斗卫星密钥

这一步由北斗导航卫星完成,首先随机地产生$r_{\text{BD}} \in Z_q^*$,然后结合系统参数P_0、提取北斗地面段密钥步骤获取的数据$\{R_{\text{GCS}}, S_{\text{GCS}}\}$、北斗卫星的身份信息$\text{ID}_{\text{BD}}$、北斗地面段身份信息$\text{ID}_{\text{GCS}}$与$r_{\text{BD}}$,按顺序分别运算如下:$R_{\text{BD}} = r_{\text{BD}} \cdot P$, $H_{\text{BD}} = H_2(\text{ID}_{\text{GCS}}, R_{\text{GCS}}, ID_{\text{BD}}, R_{\text{BD}})$和$S_{\text{BD}} = S_{\text{GCS}} + H_{\text{BD}} \cdot r_{\text{BD}} \cdot Q$.

(4) 生成签名认证信息

签名认证信息生成阶段由签名者北斗卫星执行. 具体步骤如下:北斗卫星随机地选取$r_{\text{m}} \in Z_q^*$,结合系统参数P_0运算$R_{\text{m}} = r_{\text{m}} \cdot P$. 运算出的$R_{\text{m}}$是完整签名认证信息的部分信息. 需要结合北斗卫星的身份信息ID_{BD}、北斗卫星地面段身份信息ID_{GCS}、北斗地面段密钥提取阶段生成的R_{GCS}、提取北斗卫星密钥步骤中获得的结果数据$\{R_{\text{BD}}, S_{\text{BD}}\}$与公开的系统参数$P_0$,依次完成运算$H_{\text{m}} = H_3(M_{\text{D2}}, \text{ID}_{\text{GCS}}, R_{\text{GCS}}, \text{ID}_{\text{BD}}, R_{\text{BD}}, R_{\text{m}})$和$S_{\text{m}} = S_{\text{BD}} + H_{\text{m}} \cdot r_{\text{m}} \cdot Q$. 签名者北斗卫星生成B-CNAV-D2信息的签名认证信息$S_{\text{D2}} = \{R_{\text{GCS}}, R_{\text{BD}}, R_{\text{m}}, S_{\text{m}}\}$. 所提出的B-CNAV-D2认证协议将签名认证信息设计在较为集中分布的预留信息区域,以便对信息进行有效地管理、维护和更新. 分布较为连续和集中的B-CNAV-D2预留信息位分布情况统计如表3所示[10].

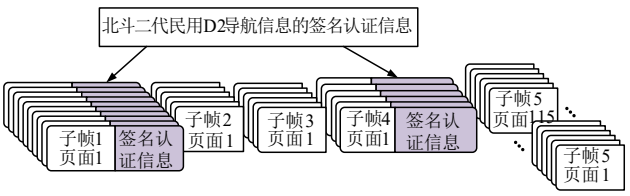
表3　分布较连续的北斗D2导航电文预留信息位分布情况

子帧编号	页面编号	起始位置	结束位置	预留信息位长度
1	1~10	151 bit	300 bit	150 bits
4	1~6	44 bit	228 bit	185 bits
5	14~34	51 bit	228 bit	178 bits
5	74~94	51 bit	228 bit	178 bits
5	103~120	51 bit	228 bit	178 bits

由表2与表3可知,B-CNAV-D2子帧1的全部页面与子帧4的全部页面都包含了连续分布的预留信息位. 子帧5虽然拥有120个电文页面,电文页面总数量最多,但是半数电文页面上的预留信息位并不充裕. 而且,子帧5的预留信息位分布较子帧1的预留信息位分布与子帧4的预留信息位分布更为分散[10].

再者,与子帧5的页面数量与电文播发周期相比,子帧1与子帧4的页面数量较少且导航电文的播发周期较短. 也就是说,如果把认证信息设计在子帧1与子帧4中,将有助于更好地保证信息实时性.

因此,子帧5并不是B-CNAV-D2的认证信息编排位置的设计首选. 针对B-CNAV-D2的认证信息编排设计侧重于考虑子帧1与子帧4. B-CNAV-D2子帧1所有页面的低150比特与子帧4所有页面的185比特预留信息位,将被用于编排签名认证信息. 本认证协议针对B-CNAV-D2设计的签名认证信息编排格式示意图如图1所示[12].



(5)认证

图1　B-CNAV-D2认证协议中签名认证信息编排格式示意图

基于身份签名的B-CNAV-D2认证协议中导航信息有效签名的正确性验证如下[11,14,15]:

$$
\begin{aligned}
&e(R_{\text{GCS}} + H_{\text{GCS}} \cdot P_{\text{pub}} + H_{\text{BD}} \cdot R_{\text{BD}} + H_{\text{m}} \cdot R_{\text{m}}, Q)\\
&= e(r_{\text{GCS}} \cdot P + H_{\text{GCS}} \cdot s \cdot P + H_{\text{BD}} \cdot r_{\text{BD}} \cdot P + H_{\text{m}} \cdot r_{\text{m}} \cdot P, Q)\\
&= e((r_{\text{GCS}} + H_{\text{GCS}} \cdot s + H_{\text{BD}} \cdot r_{\text{BD}} + H_{\text{m}} \cdot r_{\text{m}}) \cdot P, Q)\\
&\because\ e(nP, Q) = e(P, nQ) = e(nQ, P)\\
&\therefore\ e((r_{\text{GCS}} + H_{\text{GCS}} \cdot s + H_{\text{BD}} \cdot r_{\text{BD}} + H_{\text{m}} \cdot r_{\text{m}}) \cdot P, Q)\\
&= e((r_{\text{GCS}} + H_{\text{GCS}} \cdot s + H_{\text{BD}} \cdot r_{\text{BD}} + H_{\text{m}} \cdot r_{\text{m}}) \cdot Q, P)\\
&= e(((r_{\text{GCS}} + H_{\text{GCS}} \cdot s) + H_{\text{BD}} \cdot r_{\text{BD}} + H_{\text{m}} \cdot r_{\text{m}}) \cdot Q, P)\\
&= e((r_{\text{GCS}} + H_{\text{GCS}} \cdot s) \cdot Q + H_{\text{BD}} \cdot r_{\text{BD}} \cdot Q + H_{\text{m}} \cdot r_{\text{m}} \cdot Q, P)\\
&= e(S_{\text{GCS}} + H_{\text{BD}} \cdot r_{\text{BD}} \cdot Q + H_{\text{m}} \cdot r_{\text{m}} \cdot Q, P)\\
&= e(S_{\text{BD}} + H_{\text{m}} \cdot r_{\text{m}} \cdot Q, P)\\
&= e(S_{\text{m}}, P)
\end{aligned}
$$

B-CNAV-D2 认证协议的整体认证流程如图 2 所示[11,14,15].

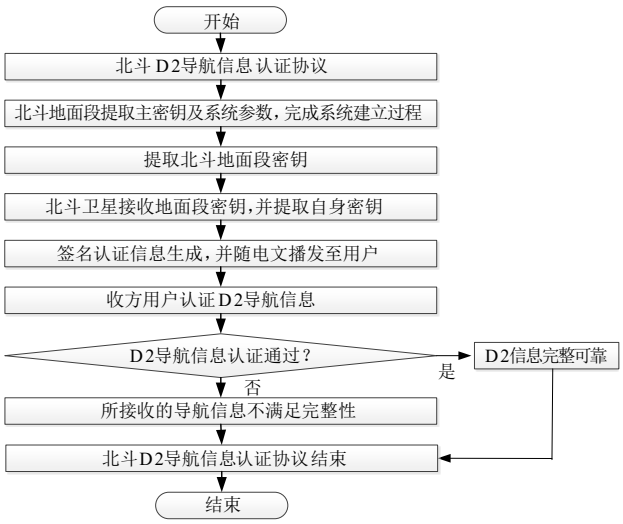


图 2 B-CNAV-D2 认证协议整体认证流程

收方用户作为签名验证者，通过确认签名认证信息 S_{D2} 的可靠性，鉴别所接收的 D2 导航电文来源是否为真实的信息发送实体北斗卫星. 首先，由作为协议认证端的收方用户按顺序分别运算出 $H_{GCS}=H_1(\mathrm{ID}_{GCS},R_{GCS})$，$H_{BD}=H_2(\mathrm{ID}_{GCS},R_{GCS},\mathrm{ID}_{BD},R_{BD})$ 和 $H_m=H_3(M_{D2},\mathrm{ID}_{GCS},R_{GCS},\mathrm{ID}_{BD},R_{BD},R_m)$. 然后，协议认证者核验 $e(R_{GCS}+H_{GCS}\cdot P_{pub}+H_{BD}\cdot R_{BD}+H_m\cdot R_m,Q)$ 与 $e(S_m,P)$ 是否一致. 最后，对接收到的 D2 导航电文信息是否通过信息认证过程做出判断. 如果，$e(S_m,P)$ 与 $e(R_{GCS}+H_{GCS}\cdot P_{pub}+H_{BD}\cdot R_{BD}+H_m\cdot R_m,Q)$ 二者是一致的，那么签名验证者认定签名有效，导航信息通过了信息认证过程，可以确认所接收的 B-CNAV-D2 是合法而且完整的；反之，用户认定签名无效，导航信息未通过信息认证过程，需要对接收的导航信息发出警告，并结合实际应用情况对 B-CNAV-D2 做进一步处理.

4 分析与证明

为了验证 B-CNAV-D2 认证协议的有效性，具体从计算成本、通信成本与执行协议各阶段所用时间三个角度对认证协议进行性能分析[11,15]，并对认证协议各执行阶段进行了仿真，并对实验结果进行了分析.

仿真实验采用的开发工具是 Visual Studio Community 2019；仿真实验程序运行在安装了 64 位 Windows8.1 操作系统和配置了 12.0 GB 内存的计算机上，以验证该认证协议的实用性. 利用 PBC 密码库，在多种可选的配对参数类型中，选用椭圆曲线 $y^2=x^3+x$ 定义的类型 A 对称配对，采用 C 语言库实现基于身份签名的 B-CNAV-D2 认证协议.

通过调用配对初始化函数配置好椭圆曲线相关参数. 由于双线性对有对称配对与非对称配对两种，因此在程序运行之初，需要判断采用的双线性对是否为对称的双线性对. 如果程序判断出所使用的双线性对是非对称的，那么不再继续执行协议，终止执行算法并安全退出程序. 通过对称配对验证之后，才可实现认证协议具体算法. 认证协议核心程序运行完毕，待程序执行到最后的时候，需要分别调用函数 element_clear() 和函数 pairing_clear() 实现元素变量和配对类型变量的清除和释放，避免内存泄露.

B-CNAV-D2 认证协议实现的流程图如图 3 所示.

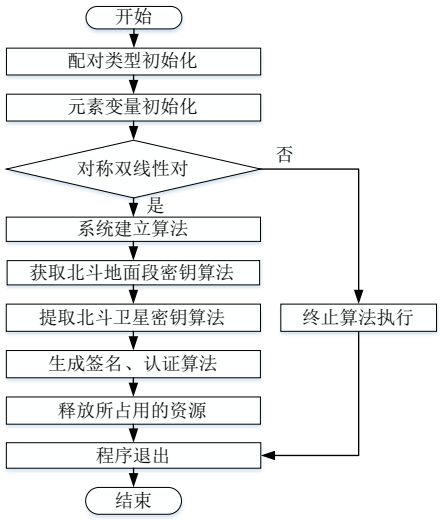


图 3 程序设计流程图

基于身份签名的 B-CNAV-D2 认证协议具体分为：系统建立阶段、获取北斗地面段密钥及获取北斗卫星密钥、生成签名及认证阶段.

首先，运行系统建立算法，提取相应的系统参数与主密钥. 图 4 给出了生成的主密钥 s 与系统参数 P_0 的程序运行结果.

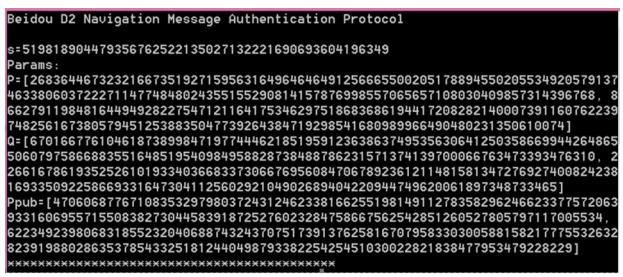


图 4 系统建立阶段运行结果

由图 4 的程序运行结果，可以看到认证协议在系统建立阶段运算出的部分系统参数. P 和 Q 分别是两个生成元. 通过运算 $P_{pub}=sP$，可以得到 P_{pub} 的结果. 系统参数在后续各部分程序中都会作为输入，参与程序运

行,因此系统参数的准确生成对于认证协议有序执行是至关重要的. 系统参数生成完毕后,进入到提取方案所需密钥阶段,依次提取北斗地面段密钥和北斗卫星密钥.

北斗地面控制段密钥提取流程是根据输入的系统参数、北斗地面段身份信息$\mathrm{ID}_{\mathrm{GCS}}$、上一阶段已提取的主密钥$s$与$r_{\mathrm{GCS}}$,依次完成运算$R_{\mathrm{GCS}}=r_{\mathrm{GCS}}\cdot P$,$H_{\mathrm{GCS}}=H_1(\mathrm{ID}_{\mathrm{GCS}},R_{\mathrm{GCS}})$和$S_{\mathrm{GCS}}=(r_{\mathrm{GCS}}+H_{\mathrm{GCS}}\cdot s)\cdot Q$. 其中,$r_{\mathrm{GCS}}$是随机选取得到的数据. 该步骤生成的$\{R_{\mathrm{GCS}},S_{\mathrm{GCS}}\}$在北斗卫星密钥提取步骤与生成签名认证信息阶段是需要作为输入信息的. 图5给出了$\{R_{\mathrm{GCS}},S_{\mathrm{GCS}}\}$的运行结果数据.

图5　北斗卫星地面段密钥提取结果

进入到提取北斗卫星密钥阶段后,执行北斗卫星密钥提取算法. 首先,随机地产生r_{BD};然后,利用系统参数P_0、北斗地面段密钥提取步骤生成的结果数据$\{R_{\mathrm{GCS}},S_{\mathrm{GCS}}\}$、北斗卫星地面段的身份信息$\mathrm{ID}_{\mathrm{GCS}}$、北斗卫星的身份信息$\mathrm{ID}_{\mathrm{BD}}$及$r_{\mathrm{BD}}$,按顺序进行如下运算$R_{\mathrm{BD}}=r_{\mathrm{BD}}\cdot P$,$H_{\mathrm{BD}}=H_2(\mathrm{ID}_{\mathrm{GCS}},R_{\mathrm{GCS}},\mathrm{ID}_{\mathrm{BD}},R_{\mathrm{BD}})$和$S_{\mathrm{BD}}=S_{\mathrm{GCS}}+H_{\mathrm{BD}}\cdot r_{\mathrm{BD}}\cdot Q$. 北斗卫星密钥提取阶段生成的$R_{\mathrm{BD}}$和$S_{\mathrm{BD}}$如图6所示.

图6　北斗卫星密钥提取结果

结合系统参数与随机选取的r_{m},运算$R_{\mathrm{m}}=r_{\mathrm{m}}\cdot P$. 利用上述算法已经生成的结果数据$R_{\mathrm{GCS}}$、$R_{\mathrm{BD}}$、$S_{\mathrm{BD}}$,身份信息$\mathrm{ID}_{\mathrm{BD}}$和$\mathrm{ID}_{\mathrm{GCS}}$,分别运算以下两种信息它们的计算方法是$H_{\mathrm{m}}=H_3(M_{\mathrm{D2}},\mathrm{ID}_{\mathrm{GCS}},R_{\mathrm{GCS}},\mathrm{ID}_{\mathrm{BD}},R_{\mathrm{BD}},R_{\mathrm{m}})$和$S_{\mathrm{m}}=S_{\mathrm{BD}}+H_{\mathrm{m}}\cdot r_{\mathrm{m}}\cdot Q$的结果数据,对待签名的B-CNAV-D2信息生成签名认证信息$S_{\mathrm{D2}}=\{R_{\mathrm{GCS}},R_{\mathrm{BD}},R_{\mathrm{m}},S_{\mathrm{m}}\}$. 签名认证信息生成阶段的程序运行结果如图7所示.

协议认证端的主要工作是认证导航信息的可靠性,首先,运算出H_{GCS},H_{BD}及H_{m}. 完成上述运算后,核验$e(R_{\mathrm{GCS}}+H_{\mathrm{GCS}}\cdot P_{\mathrm{pub}}+H_{\mathrm{BD}}\cdot R_{\mathrm{BD}}+H_{\mathrm{m}}\cdot R_{\mathrm{m}},Q)$与$e(S_{\mathrm{m}},P)$二者是否一致,进而对签名认证信息是否有效做出相

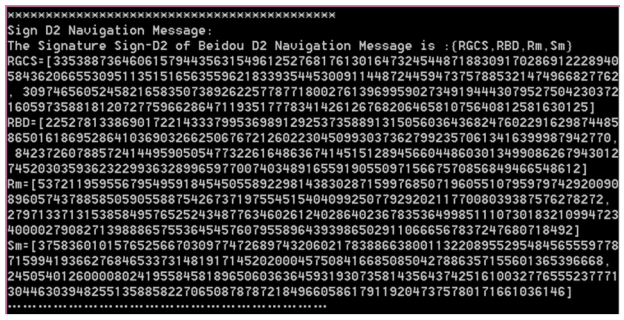


图7　签名认证信息生成阶段的程序运行结果

应的判断. 如果二者一致,说明收到的导航信息通过了信息认证过程,拥有真实性和完整性,输出"The Signature is Valid!",如图8所示.

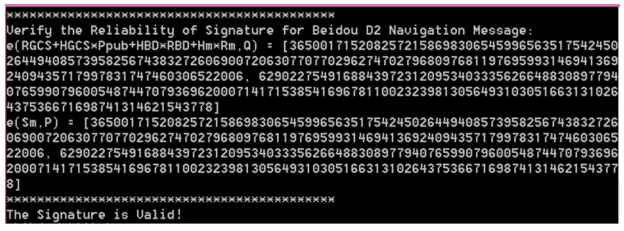


图8　通过信息认证阶段的程序运行结果

在具体仿真实验中,为了消除外部环境引入的干扰,直观、简明地反映仿真实验数据的一般水平,进行30组仿真实验,每组实验中设置1000次仿真,以对基于身份签名的B-CNAV-D2认证协议的实用性进行验证分析;并对这30000次实验结果求取算术平均值,以得到更具代表性的实验结果数据. 结合B-CNAV-D2认证协议的具体实现步骤,对系统建立阶段、提取北斗地面段密钥阶段、提取北斗卫星密钥阶段、生成签名认证信息阶段和认证阶段所用时间进行统计,便于比较协议各阶段具体耗费时间,分析该协议的时间效率. 具体的仿真实验结果如图9所示.

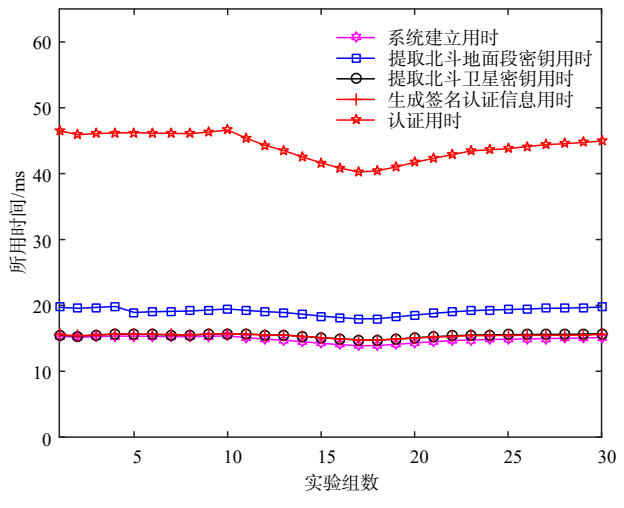


图9　B-CNAV-D2认证协议各阶段计算成本

图9显示认证协议在其他各执行阶段算法运行时间较为平稳,但在系统建立阶段所用时间上下波动幅度较大. 这是因为在系统建立阶段需要完成系统初始化过程,包含生成公共系统参数和主密钥的操作,产生在该认证协议全生命周期内都有效可用的系统参数,该算法运行时间变化幅度较大.

通过30000次仿真实验,得到协议中的五个阶段所消耗时间的平均统计值,如表4所示.

表4 B-CNAV-D2认证协议各阶段运行时间

认证协议各阶段	运行时间(单位:ms)
系统建立阶段	15.1167
提取北斗地面段密钥阶段	19.7534
提取北斗卫星密钥阶段	15.7094
生成签名认证信息阶段	15.5638
认证阶段	44.9409

为了较为直观地比较协议不同阶段的时间效率,执行认证协议每个步骤的平均计算成本如图10所示;执行所设计的认证协议各步骤所需的平均时间占总运行时间的比例如图11所示.

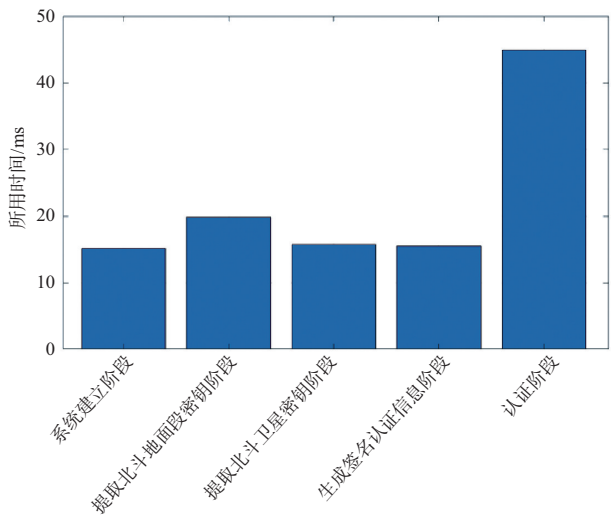


图10 认证协议每个步骤平均计算成本

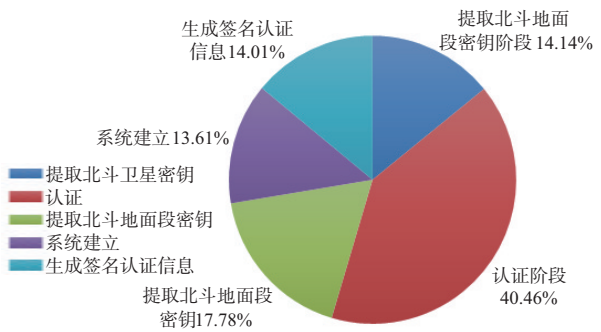


图11 认证协议执行各阶段所用时间比例图

由图11可知,执行该协议的过程中,由北斗卫星导航系统端完成的协议前四个算法运行时间较为一致. 与上述北斗系统端执行的四个算法运行时间相比,需要用户完成的信息认证过程所用的时间较长一些. 从运算量方面进行分析,协议中提取北斗卫星密钥阶段与生成签名信息阶段,所需要进行的运算均为两次点乘运算、一次点加运算和一次哈希运算. 用户对接收的导航信息进行认证的过程中,需要执行两次配对运算、三次点乘运算、三次点加运算及三次哈希运算. 与协议中另外两个步骤的运算量相比,认证导航信息阶段需要多进行两次配对运算、一次点乘运算、两次点加运算及两次哈希运算. 配对运算的复杂度较点乘、点加和哈希这三种运算的复杂度更高,执行该运算需要耗费更多的时间. 因此,认证导航信息阶段的运算量更大,花费的时间相对更长,认证导航信息阶段运行时间占方案整体运行时间的比例更大.

经过上述分析可以得出图11中各步骤平均运行时间占总运行时间的比例与方案理论运算量相符合.

针对认证协议所需要的通信成本,主要从生成的签名认证信息所占据的信息存储空间进行分析. B-CNAV-D2认证协议中签名认证信息长度为4096比特,因此引入的信息认证协议将为现有北斗卫星导航系统带来额外的4096比特的通信开销.

本认证协议与其他认证方案在通信成本和计算成本方面的协议性能比较见表5.

表5 认证协议性能比较

认证协议	通信成本	计算成本	
		发送信息者签名阶段	接收信息者认证信息阶段
文献[16]	1024 bits	MP	2MP+HMTP +2PP
文献[17]	3072 bits	3EXP	EXP+5PP
文献[18]	320 bits	2MP+EXP	3MP+4EXP
文献[19]	1024 bits	EXP+ HMTP	EXP+HMTP+PP
D2协议	4096 bits	2MP	3MP+2PP

由于配对运算、点乘运算、指数运算及映射到点哈希运算这四类运算的计算开销相比于其他运算的计算开销是较大的,也是比较耗时的,因此其他运算所带来的计算开销在分析计算成本的过程中,可以不做重点考虑. 表5中,采用PP表示运算量较大的配对运算;MP是指循环群中的点乘运算;EXP表示循环群中的指数运算;HMTP指示一种低效的映射到点哈希运算. 本文认证协议与文献[11]的区别有三点:(1)文献[11]的前提条件理想化(准确的定位、精确的定时和可靠的通信),而本文的假设前提是基于真实的卫星传播环境(开放信道和未认证信息);(2)文献[11]的认证对象是

面向北斗接收机,而本文的认证对象是民用导航电文信息,属于深度认证;(3)认证方法的不同,文献[11]是身份认证,而本文是基于身份签名的认证.

为了直观地对本认证协议与其他四个认证方案的通信成本大小进行比较和分析,将五个认证方案的通信成本统计如图12所示. 从表5和图12中的统计数据可以分析出来,各认证方案性能上各有优劣,其中,文献[18]方案在通信成本方面优势明显,文献[16]和文献[19]方案的通信成本优于本认证协议与文献[17]方案所需的通信成本.

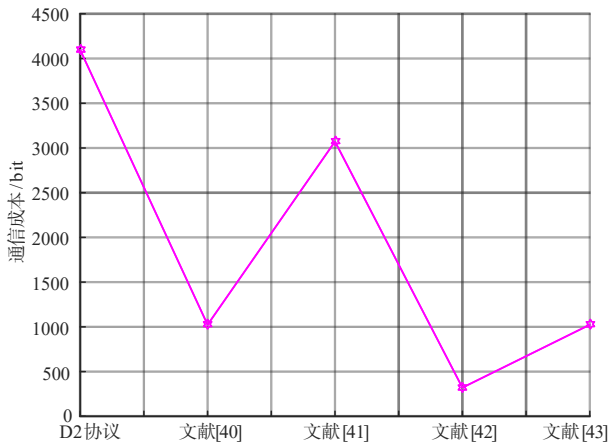


图12　认证方案通信成本比较直观图

在协议计算成本的方面,需要执行两次点乘运算来完成B-CNAV-D2认证协议中的签名过程;需要执行三次点乘操作和两个配对运算来完成相对应的认证过程. 虽然该协议在通信成本方面,与文献[16]及文献[19]所提方案相比未体现出优势,不过该协议整体不涉及较低效率的映射到点哈希操作,在计算复杂度方面优于两个方案,说明本协议所消耗的计算成本较低. 从计算复杂度方面考量,配对运算高于指数运算和点乘运算. 因此,本文提出的方案与相关方案[16,19]在计算成本方面相比拥有的优势,主要体现在签名阶段所需的运算数量较少且运算复杂度更低,可以在较低的计算开销和较高的整体效率下保证导航信息的安全性,满足北斗导航信息认证需求. 综合评估B-CNAV-D2认证协议具备可行性和正确性,在未引入证书且不依赖于公钥基础设施PKI(Public Key Infrastructure)的情况下,利用身份信息获得了公钥,实现了实体身份与公钥的自然绑定,节省了认证方案整体的通信开销和公钥维护管理负担. 该协议在计算成本方面拥有较好的性能,通信成本在合理可接受的范围内,适合在北斗卫星导航系统领域应用.

5　结论与未来工作

目前北斗卫星与用户通信使用开放无线信道,导航电文信息作为通信内容,很容易被篡改或被伪造. 面对信息安全威胁时,如何保障民用导航信息的真实可靠是一个亟需解决的问题. 本文在分析B-CNAV-D2具体特性的基础上,结合基于身份的签名技术,设计了一种适用于B-CNAV-D2的安全认证协议,并给出了认证协议的性能分析,从理论上分析了协议的安全性. 本文提出的北斗民用导航电文认证技术是一种从信息层面为民用导航电文信息提供信息安全保护的方法,以提供安全、可靠、标准的信息认证机制为目标. 运用密码认证技术,采用附加签名认证信息到现有导航电文的方式,在保留北斗系统开放性的基础上,提供了有效识别出虚假导航信息的方法. 从计算成本、通信成本和执行协议各阶段所用时间三个方面对认证协议进行了性能分析. 评估结果表明设计的认证协议在保障较好的认证时效性,合适的计算成本与通信成本的同时,实现了导航信息的完整性保护和信息源认证目标.

在未来的研究中,计划将本文认证协议应用到真实的北斗导航环境中,开展相关的实验和测试.

参考文献

[1] Wu Z J, Liu R S, Cao H J. ECDSA-based message authentication scheme for BeiDou-II navigation satellite system [J]. IEEE Transactions on Aerospace and Electronic Systems, 2019, 55(4): 1666 – 1682.

[2] Schmidt D, Radke K, Camtepe S, et al. A survey and analysis of the GNSS spoofing threat and countermeasures[J]. ACM Computing Surveys, 2016, 48(4): 1 – 31.

[3] Wu Z J, Zhang Y, Yang Y M, et al. Spoofing and anti-spoofing technologies of global navigation satellite system: A survey[J]. IEEE Access, 2020, 8: 165444 – 165496.

[4] 贾琼琼, 吴仁彪, 王文益, 等. 满足高精度测量的GNSS自适干扰抑制算法[J]. 电子学报, 2018, 46(11): 2753 – 2760.
Jia Q Q, Wu R B, Wang W Y, et al. GNSS adaptive interference suppression algorithm for high accuracy measurement[J]. Acta Electronica Sinica, 2018, 46(11): 2753 – 2760.(in Chinese)

[5] 康立, 王雪, 熊定喜, 等. 北斗系统导航信号标称失真研究[J]. 电子学报, 2018, 46(12): 2848 – 2853.
Kang L, Wang X, Xiong D X, et al. Nominal deformations analysis of BDS navigation signal[J]. Acta Electronica Sinica, 2018, 46(12): 2848 – 2853.(in Chinese)

[6] 房晓丽, 吴礼杰, 张金菊. 有限测试距离对GNSS抗干扰天线阵远场测试的影响[J]. 电子学报, 2020, 48(5): 1030 – 1035.
Fang X L, Wu L J, Zhang J J. Influence of limited test distance on far-field measurement for GNSS anti-jamming ar-

ray[J]. Acta Electronica Sinica, 2020, 48(5): 1030 – 1035. (in Chinese)

[7] Wesson K, Rothlisberger M, Humphreys T. Practical cryptographic civil GPS signal authentication[J]. Navigation, 2012, 59(3): 177 – 193.

[8] Perrig A, Canetti R, Tygar J D, et al. The TESLA broadcast authentication protocol[J]. RSA CryptoBytes Technical Newsletter, 2002, 5(2): 2 – 13.

[9] Fernández-Hernández I, Rijmen V, Seco-Granados G, et al. A navigation message authentication proposal for the Galileo open service[J]. Navigation, 2016, 63(1): 85 – 102.

[10] Yuan M Z, Lv Z, Chen H M, et al. An implementation of navigation message authentication with reserved bits for civil BDS anti-spoofing[A]. China Satellite Navigation Conference (CSNC) 2017 Proceedings: Volume II[C]. Singapore: Springer, 2017. 69 – 80.

[11] 赵东昊, 卢昱, 王增光. 北斗战场通信网络身份认证方法[J]. 现代防御技术, 2019, 47(3): 99 – 105.
Zhao D H, Lu Y, Wang Z G. Identity authentication method of "BeiDou" battlefield communication network[J]. Modern Defence Technology, 2019, 47(3): 99 – 105. (in Chinese)

[12] Wu Z J, Zhang Y, Liu R S. BD-II NMA&SSI: An scheme of anti-spoofing and open BeiDou II D2 navigation message authentication[J]. IEEE Access, 2020, 8: 23759 – 23775.

[13] BDS-SIS-ICD-2.1,北斗卫星导航系统空间信号接口控制文件(2.1版)[S].

[14] He D B, Kumar N, Choo K K R, et al. Efficient hierarchical identity-based signature with batch verification for automatic dependent surveillance-broadcast system[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(2): 454 – 464.

[15] Wu Z J, Zhang Y, Liu L, et al. TESLA-based authentication for BeiDou civil navigation message[J]. China Communications, 2020, 17(11): 194 – 218.

[16] Chen Y C, Horng G, Liu C L. Strong non-repudiation based on certificateless short signatures[J]. IET Information Security, 2013, 7(3): 253 – 263.

[17] 杨小东, 王美丁, 裴喜祯, 等. 一种标准模型下无证书签名方案的安全性分析与改进[J]. 电子学报, 2019, 47(9): 1972 – 1978.
Yang X D, Wang M D, Pei X Z, et al. Security analysis and improvement of a certificateless signature scheme in the standard model[J]. Acta Electronica Sinica, 2019, 47 (9): 1972 – 1978.(in Chinese)

[18] Li J G, Wang Z W, Zhang Y C. Provably secure certificate-based signature scheme without pairings[J]. Information Sciences, 2013, 233: 313 – 320.

[19] Li J G, Huang X Y, Zhang Y C, et al. An efficient short certificate-based signature scheme[J]. Journal of Systems and Software, 2012, 85(2): 314 – 322.

作者简介

吴志军 男, 1965 年 5 月生, 新疆库尔勒人. 现为中国民航大学教授, 博士生导师, 密码学会高级会员. 主要研究方向为航空电信网及信息安全、大数据和云计算的安全.
E-mail:zjwu@cauc.edu.cn

杨一鸣 女, 1994 年 6 月生, 辽宁抚顺人. 现为中国民航大学电子信息与自动化学院研究生. 研究方向为北斗导航信息安全.
E-mail:13654137311@163.com

张 云 男, 1996 年 2 月生, 山东烟台人. 现为中国民航大学电子信息与自动化学院研究生. 研究方向为北斗导航信息安全.
E-mail:chunyyzhang@163.com