第十三届中国卫星导航年会 候选年会最佳论文公示表

姓　　名	袁木子	出生年月	1993.9	论文编号	CSNC-2022-0293
论文题目	民用卫星导航信号的互相关扩频码认证 Cross-correlation based Spreading Code Authentication Scheme for GNSS Civilian Signals				

论 文 概 要

一、研究目的和方法

民用卫星导航服务的信号结构细节公开、由卫星单向广播，在开放使用且用户容量无限的同时存在欺骗攻击的风险。如果接收机无法有效检测信号是否遭到伪造，其输出的定位、导航与授时结果将被欺骗攻击误导。

导航信号防伪认证可以可靠检测欺骗信号，是各大导航系统的重要发展方向。这其中，导航电文认证计算和存储复杂度低，但是面临安全码估计与再生攻击的威胁；主流扩频码认证设计一部分要求长时间缓存导航信号采样，另一部分需要进行授权密钥的分发，对接收机的存储能力和通信保障能力造成较大压力。

本文通过提出导航信号认证方案，实现对生成式和再生式欺骗的可靠检测。

二、主要结果与结论

本文提出了基于不同卫星信号之间互相关结果进行导航信号认证的设计原理，并为北斗 B1C 民用信号分量选择了设计参数。

根据性能评估结果以及与 GPS Chimera 和 Galileo OSNMA 两大主流导航信号认证方案的对比，发现本文提出方案在北斗 B1C 信号分量中，在检测概率与 OSNMA 以及 Chimera 相当的前提下，相比 OSNMA 额外具备了对安全码估计与再生攻击的防护能力，相比 Chimera 节省了大量存储空间，同时认证效率高于 OSNMA 和 Chimera 的慢通道认证。

三、主要创新点

1. 通过将民用周期扩频码中的一部分序列替换为相同且保密的认证扩频码，实现任意两路卫星信号互相关即可检测认证特征；

2. 通过对认证扩频码初始相位添加受到安全码驱动的偏移实现认证信息的调制；

3. 相比现有的被动导航信号扩频码认证方案，对安全码估计与再生攻击不敏感、避免了对导航信号采样进行长时间存储。

四、科学意义和应用前景

本文提出的方案和设计原理可以应用在包括北斗 B1C 在内的各类导航信号的认证设计中，用于实现高安全性低开销的导航信号认证以及欺骗检测。

五、解决的实际问题

相比目前已公开的导航信号认证手段，本文方案解决了 GPS 方案需要较大存储开销的问题，同时在一定程度上缓解了 Galileo 方案对再生式欺骗的敏感性。本文方案如果应用在民用卫星导航信号中，可以解决民用卫星导航信号易受生成式和再生式欺骗威胁的问题。

填表说明：请论文作者如实填写表格，字体采用“楷体 小四”，总字数控制在 600 至 800 字。