民生用衛星測位システムの脆弱性軽減方法の開発

The development of decrease of vulnerabilities for Civilian GNSS

千野孝一* Dinesh Manandhar** 柴崎亮介**
Koichi Chino Dinesh Manandhar Ryosuke Shibasaki

*㈱日立情報制御ソリューションズ、**東京大学
Hitachi Information &Control Solutions, Ltd. , The University of Tokyo

１．まえがき

民生用途 GPS 信号は広く社会生活のインフラ分野に利用されているが，容易に成りすましされやすく，脆弱性(スプーフィングとミーコニング）を内在している．本研究では，まずスプーフィングのデモから如何に GPS 信号が脆弱であるかを示し，その対応策をナビゲーションメッセージにエラー訂正の秘匿化演算を施すことにより実現できることを示した．次に準天頂衛星システムの地上システム・衛星システム・受信機に秘匿化演算したナビゲーションメッセージを実装する方法を示した．最後に秘匿化演算したナビゲーションメッセージが既存の GPS 信号の脆弱性を解決する有望な手段であることをシミュレーションと実験により示した．

２．スプーフィングのデモ

衛星システムでは潜在的な脆弱性（スプーフィングとミーコニング）が問題になる可能性がある．なぜなら、GPS シミュレータとリピータの出現で，スプーフィングとミーコニング信号は意図的に生成することが可能である．さらに，GPS 民生信号の仕様は，ICD- GPS ドキュメントに公開されているので誰でも偽装した信号を生成、送信することができる．図1にスプーフィングの例を示す．GPS シミュレータから１分毎に異なる地点（東京タワー、大阪城、富士山）の位置情報を PND(Personal Navigation Device)へ送信する．すると PND はエラーを表示せずに素直に異なる３地点の地図を表示した．いかに簡単に位置のスプーフィングが可能であるかが判明した．ここで、スプーフィングの定義は衛星から送信された位置情報と同じ位置情報をシミュレータ等から送信してなりすます技術である．

図１　スプーフィングの例

３．ナビゲーションメッセージへの秘匿化

GPS 信号のナビゲーションメッセージを認証することによって GPS 信号のスプーフィングの問題を解決する方法論を提案する．ナビゲーションメッセージの認証は，QZSS L1C/A 信号または L1SAIF（L1 Submeterclass Augmentation with Integrity Function）信号を使用して実現される．位置データを認証したいユーザは準天頂衛星モニタリングステーションで観測された GPS のナビゲーションメッセージの特定ビット RAND(Reference Authentication Navigation Data)に対し秘匿化データを計算し，その結果を L1SAIF 信号で送信することで認証が実現できる．この提案手法は，認証のために受信機のソフトウェア/ファームウェアの変更が小修正であるので既存の GPS 受信機から容易にアップグレードでき，位置情報認証機能を追加できる．

４．準天頂衛星システムへの実装提案

準天頂衛星システムの宇宙セグメント、地上セグメントには手を加えずに新たに認証局（仮想）を設けて GPS/QZSS 民生用信号 L1C/A に秘匿化演算を行う．受信機では秘匿化された L1C/A 信号を認証できる仕組みを設ける．現行の GPS へ最適な認証方法の概念を提案する．図 2 に信号の送信方法における認証データ生成の概念を示す．4 つのステップがある．

- RAND メッセージ生成
- SEED 値生成
- LDPC 演算
- QZSS ナビゲーションメッセージの加工

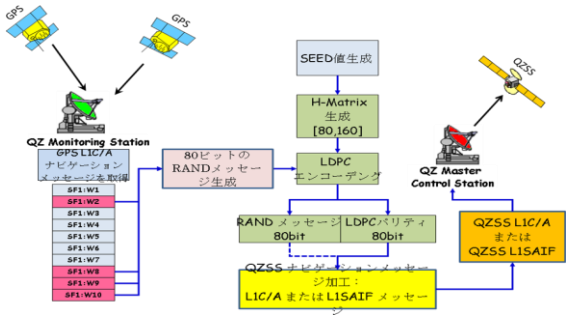

図２　認証データ生成の概念

５．シミュレーション結果

図３に認証データベースの例を示す．データベースは TOW と PRN ID をインデックスにして RAND,LDPC Parity bit(A),SEED 値,H-Matrix 等で構成される．受信機では TOW と PRN ID をキーにして受信した信号の RAND から H-Matrix を認証データベースから引き出し、LDPC 演算を実施する．得られた LDPC Parity bit(B)が認証データベースの LDPC Parity bit(A)と比較して同一ならば認証成功と判断する．複数のデータベースで認証成功がシミュレーションより得られたことで本方式が GPS/QZSS 民生信号脆弱性を解決する有望な手段であることが証明された．

TOW	PRN ID	RAND MSG	PARITY DATA	SEED VALUE	H-Matrix Data	RSA KEYS
272726	8	58B1A1660000007BC708	73DBEA93E7961A5FB2E3	653012443	HMAT_DAT_1	RSAKEY_DATA_1
272816	10	58B1A1667FFBFBA6C50A	0D2E53CCA0D967C248A8	653015706	HMAT_DAT_2	RSAKEY_DATA_2
272846	13	58B1A1667FFA127FD30D	AD5EB63397267847FCC3	653018415	HMAT_DAT_3	RSAKEY_DATA_3
272877	26	58B1A1667FD5F7F9731A	E73E9799583AC510FD58	653020857	HMAT_DAT_4	RSAKEY_DATA_4

図３認証データベース例