位置情報のハイジャック：GPS の新しい脆弱性

マナンダー　ディネス
東京大学

今日、コンピュータを購入する際には、ウイルス対策ソフトも同時に購入する。その理由は？それは、真新しいコンピュータがウイルスの攻撃にさらされては安全だと感じることができないし、考えられるウイルス攻撃から自身のコンピュータを保護し、安全な状態にしておきたいと思うからであろう。しかし、あなたは常に脅威にさらされており、ウイルス対策ソフトを定期的にアップデートし続けなければならない。そのようなウイルス攻撃は、命にかかわる問題ではないものの、データの損失によって様々な重大な問題が生じる。

近い将来、コンピュータに起きているのと同じようなことが、GPS 装置を使用して位置及び時刻情報を得ているシステムにも起きることが考えられる。現在、位置及び時刻の情報を必要としているシステムは、世界的に利用可能であることと、その精度と費用の安さからGPS に依存している。例えば、カーナビゲーション、自動運転、通信システムの同期、金融取引のタイミング、船舶の監視（船舶自動識別装置（AIS)、船舶監視システム（VMS))、航空機の誘導、車両の通行料徴収、位置情報サービス（LBS）及び多くの安全や安全保障に関わるシステムが GPS を使用して位置及び時刻情報を得ている。昨今のこれらのシステムは、GPS に大きく依存しており、我々の日々の生活を快適にするために必要不可欠なものとなっている。我々は、日常生活において、GPS 情報を意識的又は無意識的に利用しているのである。それはあなた自身が自ら行っている選択ではないかもしれないが、我々の日常生活に組み込まれたシステムになっている。それが法律、規則、法規によって求められている場合もある。例えば、すべての携帯電話には、緊急時に位置データを容易にわかりやすくするために GPS 受信機を備えていることが求められている。EU 及びロシアでは、車両に e-call や ERA-GLONASS といった車両緊急通報システムを搭載することが義務付けられている。

しかし、一方で、GPS 又は GNSS 信号には、干渉、ジャミング及びスプーフィング（なりすまし）に比較的脆弱であるという側面がある。干渉及びジャミングは、意図的又は非意図的に行われる場合がある。しかし、スプーフィングは、意図的に行われる行為であり、最も重大なものである。干渉やジャミングの場合、受信機が動作を中止するため、何か問題が生じたことをシステムが感知し、潜在的な危険を回避するために必要な対応をとることができる。スプーフィングの場合は、偽りの位置データと共に受信機が動作し続けるようにするのである。例えば、ユーザが東京にいたとしても、そのユーザの受信機に対してスプーフィングを行うことで、そのユーザが大阪にいるように見せかけることができる。あなたの位置

データは、簡単にある場所から別の場所へとハイジャックされてしまうのである。受信機もユーザも、この偽りの位置データの出力について、その正確性を確認する手段はない。現在の GPS 信号（民生用信号）の設計では、スプーフィング攻撃を確認することはできない。

GPS スプーフィングの問題は、2001 年には米国運輸省の Volpe Reports や 1997 年公開の映画、ジェームズ・ボンドシリーズ『007　トゥモロー・ネバー・ダイ』で取り上げられたものの、2010 年までに行われた研究の数は極めて少ない。2000 年から 2010 年の間及びそれ以降にも、多くの新しい GNSS 信号が設計されたが、これらの信号の中で、スプーフィングから保護するための機能を組み入れた民生用信号は一つもない。

スプーフィング攻撃は、ICD（Interface Control Document : インタフェース管理文書）にすべての必要な信号設計情報が公開されていることから、非常に容易に行うことができる。ICD は、サービスを提供している企業すべてに公開することが義務付けられた文書であり、これがあることにより、GPS 受信機の製造者が GPS 受信機の設計や製造を行うことが可能となる。スプーフィングを行うために GPS に似た信号を発生させることが可能なハードウェアは、数百ドルで入手可能であり、USB ポートを電源とすることができる。このような装置は、あらゆる種類の GNSS 信号を発生するようプログラミングすることも容易である。また、GPS 信号は、非常に微弱な信号（受電アンテナで-130dBm で、これは装置の熱雑音よりも低い）であり、例えば、-64dBm（送電アンテナでの EIRP）といった非常に低電力のスプーフィング信号でも、半径約 5-10 メートル付近の受信機にスプーフィングを行うのに十分な強度を持っていることになる。-64dBm は、日本の周波数 1-10GHz における送電アンテナ（EIRP）でのライセンスフリーの信号電力に相当する。このレベルの非常に弱い信号は、干渉やジャミングという観点からは問題にならない。なぜなら、1-3m を超える距離にある他の信号に、重大な影響を及ぼすことがないからである。しかし、スプーフィング攻撃を考えると、この電力レベルは、周辺半径 5-10m 以内のユーザを攻撃するのに十分なレベルである。多くの国の無線通信規則は、基本的にスプーフィングではなく、干渉やジャミングの脆弱性に重点を置いている。GNSS 又は RNSS 周波数に関連した無線通信規則も、スプーフィングの問題を考慮して改定されるべきである。例えば、米国政府は、（GPS/GNSS に使用される）RNSS 周波数帯域幅では、その他の信号の送信を認めてない。しかし、これはあくまでも、RNSS 帯域幅全体をその他の有害な信号から保護するための包括的なアプローチにすぎない。これによって干渉やジャミングからは防御できても、スプーフィングからは防御できない。もしも、何らかのシステムが、意図的若しくは非意図的に、GPS に似た信号を宇宙空間から送信し、GPS ユーザに対してスプーフィングを行ったら、どうなるだろうか？

2010 年以降、スプーフィングの問題を解決するための研究、論文及び暫定的な解決策が多く見られるようになった。しかし、これらの解決策は、すでに宇宙空間に存在する信号と互換性があり、他のシステムに組み込まれた既存の受信機のハードウェアに影響を及ぼすことのないようなものでなくてはならず、それを見出すのは簡単な作業ではない。我々は、この分野において、10 年以上の経験を有している。すでに数年前には試験システムを開発しており、これは QZSS 衛星から試験信号を送信し、リアルタイムで認証試験を実施することが可能である。我々のシステムは、QZSS（日本）の他に、GPS（米国)、GALILEO（欧州）及び BEIDOU（中国）の信号を認証することができる。GALILEO も、E1 信号周波数帯でのオープンシグナルに認証機能を備えることを発表している。

このように、GPS システムをスプーフィング攻撃から保護するという点においては、明るい側面も見られる。これは、あと数年後には、GPS 受信機あるいは GPS に基づいたシステムを購入する際に、GPS をスプーフィング攻撃から守るための「ウイルス対策パッケージ」も一緒に購入するようになるかもしれないということだ。我々は、このような「ウイルス対策パッケージ」を「信号認証サービス」と呼ぶ。このサービスが、あなたの受信機からの位置及び時刻データが、実際に宇宙空間にある GPS 衛星から算出されものかどうかを判断する。自動運転及び、その他多くの安全や安全保障に関連するアプリケーションの安全かつ確実な運用には、この種の認証サービスが必要不可欠である。

GNSS のさらに詳細な情報については、https://home.csis.u-tokyo.ac.jp/~dinesh/index.htm を参照いただきたい。