

なりすまし攻撃とジャミング攻撃に対する重要インフラストラクチャの保護

GNSS 信号は、様々なジャミング攻撃およびなりすまし攻撃に対してますます脆弱化しています。ここでは、GNSS 受信の保護とセキュリティを強化するために信号可視性を提供する方法について解説します。

重要インフラストラクチャでは、GNSS ベース時刻同期の重要性が高まる一方、GNSS 信号のセキュリティは意図的あるいは偶発的なジャミングおよびなりすましの脅威に対してますます脆弱化しています。もともと脆弱な GNSS 信号の性質を考えると、リアルタイムで GNSS 信号特性の可視性を高める事により GNSS 信号の受信を保護する事が重要です。

ネットワーク セキュリティと同様に、新しい脅威が次から次に現れるため GNSS システムのセキュリティ強化に終わりはありません。軽微な障害が重大な機能停止へと進展する前に脆弱性の根本的原因を特定するには、「GNSS 信号の可視性」を高める事が重要です。

GNSS の脆弱性が検出された場合、BlueSky Performance Monitoring を使って GNSS 受信クオリティを調査し、ロケーションに固有の問題なのか、それとも広範な地理的範囲に影響が及ぶ問題なのかを判別できます。さらに、重要な性能指標を可視化する事で、迅速かつ対費用効果の高い対応を取る事ができます。GNSS アンテナには問題がないのにネットワーク担当者を高層ビルの屋上まで派遣して点検してもらうのはお金の無駄使いです。BlueSky Performance Monitoring を使って「GNSS の可視性」を高める事で、無駄な出費を防ぐ事ができます。

BlueSky™ Performance Monitoring は、Microchip 社の TimePictra®ソフトウェアに組み込まれた機能セットであり、実際の GNSS 信号を監視および評価するためのソリューションを提供します。これらの機能を使う事で、信号可視性を高めて GNSS 受信の保護とセキュリティを強化する事ができます。

詳細は **BlueSky™ Performance Monitoring 白書** をダウンロードしてご覧ください。

Greg Wolff, Jan 15, 2020