Anti-Spoofing Capability in GPS by Signal Authentication

Dinesh Manandhar, Ryosuke Shibasaki
Center for Spatial Information Science, The University of Tokyo, Japan
Email:<dinesh@iis.u-tokyo.ac.jp>

(1) Motivation : GPS is widely used in many applications (LBS, ITS, Surveying, Mapping, Telecom etc) where position and time data are required due to its independent positioning capability with high-accuracy and global availability. However, GPS is also highly vulnerable to Jamming, Interference and Spoofing. There are many research and methodologies to detect and prevent against Jamming and Interference, but very little work has been done on Spoofing. Spoofing is an action to falsify a receiver's position data by broadcasting a special GPS like signal. It is possible to spoof a GPS receiver to show it's position data as in Osaka even if the receiver is in Tokyo. Thus, in order to detect and prevent such spoofing attacks on GPS devices, we have developed an anti-spoofing methodology by authenticating the GPS signals based on QZSS. This method can identify between true (signals from satellites) and false (signals locally generated) GPS signals

(2) Method : The general concept of authentication is to broadcast a digital signature data in a navigation message of one of the signals in QZSS (Japanese GPS). The digital signature data is a message generated from certain portions of the navigation message of GPS and QZSS satellites. These data are hashed, encrypted and broadcasted from QZSS L1S signal.

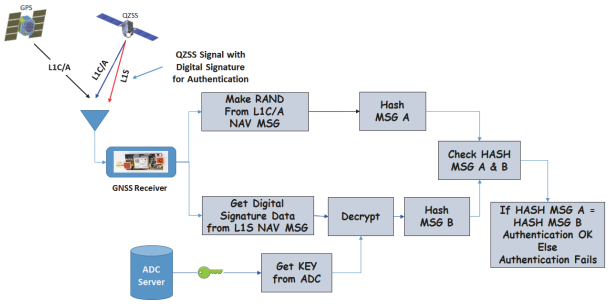

Figure 1: Digital signature generation method

At the user side, the receiver receives navigation data from L1S signal as well as from other L1C/A signals. The encrypted data in L1S signal is decrypted using the public key to generate the hashed message (A). The receiver creates a hashed message (B) from the incoming navigation data in L1C/A signal by using the same HASH algorithm at the authentication system side. Thus the generated hashed message (B) and received hash message (A) by decrypting the navigation data in L1S must be the same unless otherwise the navigation data bits in L1C/A signal are modified. This confirms that the signal in the receiver is authentic or not spoofed. **Figure 1** and **Figure 2** show methods of signal authentication.

(3) Result : We have conducted many tests by actually broadcasting the L1S signal from QZSS satellite with authentication capability for both GPS and QZSS. Tests were conducted in the lab in static mode as well as by driving a car at different times in a year.

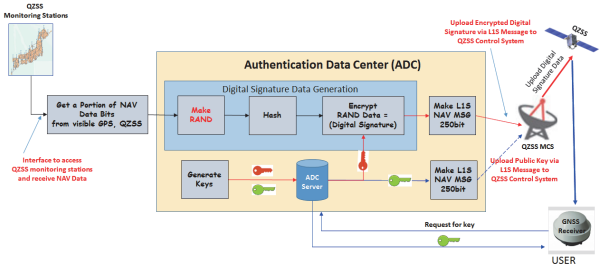

Figure 2: Signal authentication in the receiver

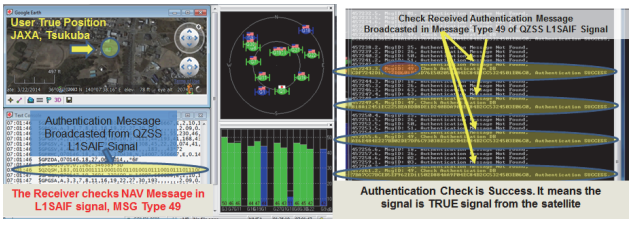

Figure 3: Result of signal authentication