Techniques used to authenticate GPS signals

Institutional affiliation

Date:

It is indeed true that global navigation satellite systems (GNSS) play a key role in positioning vehicles on an accurate map. It is therefore quite important to protect against spoofing and the injection of fake messages. There are different techniques that are proposed to authenticate GPS signals for Intelligent Transportation System (ITS). This paper look at a number of them and discusses how they can be effectively applied to prevent such attacks.

Navigation Message Authentication (NMA)

This system addresses the GNSS vulnerabilities as evidenced in the last one decade. An authentic GNSS is critical underpinning that is considered a building block to help overcome the challenges of the system. There is a guaranteed accuracy, reception condition, and availability due to enhanced navigability of the Galileo OS. The Galileo signal design allows for proper authentication and higher bitrates as compared to GNSS. Its safety of life makes it possible to re-profile a significant amount of bandwidth for other uses (Kerns, Wesson, & Humphreys 2014).

Navigation Message Authentication seeks to authenticate the navigation data that is broadcasted by GNSS. A well designed and optimally functioning NMA should provide navigation accuracy while minimizing the difference of authentication time. An affordable system infrastructure in this decade can only arise when transmission and broadcast of generated Galileo occurs. This arrangement is often used by other systems which include services like the geostationary satellite. When generating NMA on-ground, only satellite with a ground connection are capable of delivering NMA in Galileo first generation which accounts for at most 24 Galileo Satellites among the available 24 satellites.

Usually, NMA is easy to implement than SSSC since its CNAV format is easier to extend due to its design. This allows for easy interpretation of messages sent in its framework. It is, however, less secure compared to SSSC. This is mainly due to its low rate security codes and its usual 5 minutes delay occurring in every signal.

Timed Efficient Stream Loss-Tolerant Authentication (TESLA)

Unlike other systems, TESLA requires no sophisticated time synchronization protocols as it works with loose synchronization between the users i.e. sender and receiver. This shows time synchronization between the sender and the receiver. Upon receiving the request, it is recorded as local time and replied to with a signed response.

A loss of synchronization time occurring between the sender and recipient is the basis upon which the use TESLA is hinged. It is introduced to solve a myriad of problems using group and ID which is based on schemes. A sender set up must have a robust packet and should be capable of scaling a large number of receivers. The bootstrapping receivers allow the senders to send a key disclosure schedule by transmitting information to receivers. This takes place in an authenticated channel.

TESLA works under the assumption of ability function F to provide a weak collision resistance that occurs when function F and F1 are secure. This makes it computably intractable for an attacker to forge TESLA. The system allows for city simulation scenario. Unlike privacy preservation protocol, it has a simulation time of 50 seconds. With a communication range of 300 m, TESLA has a channel bandwidth of 6 Mbps and a packet size of 301 bytes (Shiu, Chang, Huang, & Chen 2011).

Scott's Spread Spectrum Security Codes (SSSCs)

This involves a method by which a signal generated in a particular bandwidth spreads in a security domain giving rise to a signal with the wider bandwidth. Its variety of uses includes establishment of secure communication which leads to noise jamming, increased resistance to natural interference and limited power of flux density. Logan Scott in 2003 proposed this technique against spoofing. L1C is the most recent version that is used on GPS Block III satellites. It was proposed alongside data supporting infrastructure, a similar process to that proposed by M.G. Kuhn in 2004. This proposal from Logan has already been briefed in total cognisance of GPS Directorate. Scott's Spread Spectrum Security Codes represents high rate security code that offers an excellent defense against spoofing. Single frequency receivers can access authenticated signals when a coincidence of frequency is established between LIC and GPS LI.

This system has its limitations, an aspect that helps in modifying and incorporating the remaining changes. This is despite funds being availed to implement it. Keys required authenticating SSSC takes longer time which may stretch to 5 minutes after SSSC transmission. Where ten satellites are involved, it may mean that 30 seconds will be used between authentications which apply to any signal. This, however, is longer than expected time in aviation which is more accurate where the integrity of 2 seconds is required. A well-networked architecture will even simplify this time to 2 seconds.

Chips Robust Message Authentication (Chimera)

This technique combines cryptographic methods and physical layers in the bid to provide overall authentication of a GNSS system. Its symmetrical use is excluded since it must work for a vast group of people. It's basically used in the conversion of pseudo ranges that must be accurate to enable it to provide a navigation solution. This technique is flexible and allows for transmission and receipt platform which makes signal modification possible.

It applies and uses digital signatures authentication to authenticate data messages, a phenomenon that is rarely used in public key cryptography. The two methods used in this technique are bound together in a way that authenticates data and physical signal. The first idea of the technique proposed by Scott is expanded into a general structure which makes variations possible. The concept has attracted wide attention and advocacy due to the value of signal authentication. Its full proof security makes it hard for a spoofer to copy an aspect that enables it to provide a high degree of trust and assurance to its users.

It uses a digital signature to support navigation process which is based on the content of messages using the private key. The user is expected to validate his signature using a public key, a simple form of authentication because of interoperability. It defeats well-stocked attackers, but it is ineffective in the long run as a computing tool (Shokralla, Spall, Gibson, & Hajibabaei 2012).

In conclusion, the discussion helps in exploring the various authentication schemes and helps in listing the advantages and disadvantages of each. Time Efficient Stream Loss-Tolerant Authentication (TESLA) has been examined alongside Scotts Spread Spectrum Security Codes. This discussion help in comparing the newest concept of Chips Robust Message Authentication compared the other authentication methods. This presents the latest ideas and contributes to point the possible avenues of developing the idea.

References

Hofmann-Wellenhof, B., Lichtenegger, H., & Collins, J. (2012). *Global positioning system: theory and practice*. Springer Science & Business Media.

Kerns, A. J., Wesson, K. D., & Humphreys, T. E. (2014, May). A blueprint for civil GPS navigation message authentication. In *2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014* (pp. 262-269). IEEE.

Perrig, A., Song, D., Canetti, R., Tygar, J. D., & Briscoe, B. (2005). *Timed efficient stream loss-tolerant authentication (TESLA): Multicast source authentication transform introduction* (No. RFC 4082).

Shiu, Y. S., Chang, S. Y., Wu, H. C., Huang, S. C. H., & Chen, H. H. (2011). Physical layer security in wireless networks: a tutorial. *IEEE Wireless Communications*, *18*(2), 66-74.

Shokralla, S., Spall, J. L., Gibson, J. F., & Hajibabaei, M. (2012). Next-generation sequencing technologies for environmental DNA research. *Molecular ecology*, *21*(8), 1794-1805.