Paving the Way for New

ANTONIO PUJANTE CUADRUPANI
PANAMNAV

With the integration of payment systems in the smartphones, location information could be used as a key authentication factor, relating user location with purchase events and helping to reduce fraud.

Smartphone apps represent the most prominent market for GNSS. No other device or community of users has achieved a larger growth and market penetration in the period 2008–2013.

Apple introduced the first GPS capability on a smartphone in June 2008 with the iPhone3, and one year later Samsung introduced its Samsung Galaxy, incorporating the first GPS receiver for this brand.

Five years passed, and the number of position/location-related applications based on GPS data has boomed. A count on December 2013 showed about 250 apps for Android market, according to Google Play store information. Most of these applications offer tracking, real-time navigation, GPS receiver check, and GPS-supported sport activities.

According to figures cited in *Business Week* magazine, the number of smartphones in use reached one billion by the end of 2012 — a 47 percent increase from a year earlier and a number projected to double by 2015. That translates into one in every seven people on the planet owning a smartphone.

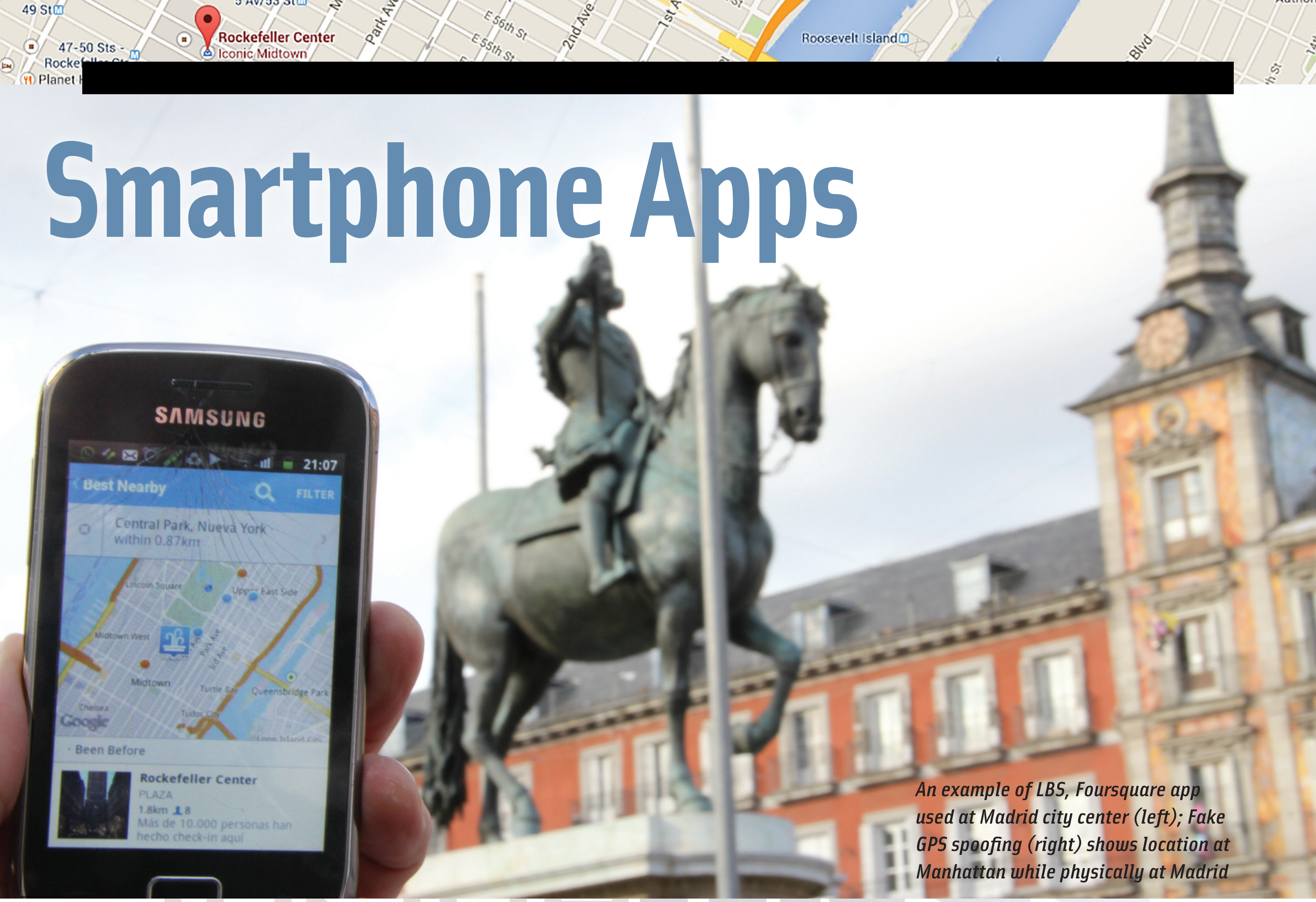
However, no other GNSS operating device is less protected and subject to degradation of the GNSS performance as smartphones are nowadays nor is the integrity of the associated information delivered by and to them as subject to question.

Not only can GNSS signals be corrupted by spoofing or radio-frequency interference and jamming, but even if these signals are properly received and the integrated GNSS receiver generates correct position information, a myriad of software-based applications (beneficial or not) can modify that position information.

Smartphones typically operate as an open environment that allows access to the instrument's physical and software layers. So, protecting the physical layer does not provide complete security because manipulation of the graphics layer (GL) engine or the location services modules can fake the final navigation position. This is a new situation that is not present in other devices where a closed environment protects the positioning, navigation, and time (PNT) solution.

All such apps are not necessarily malware, properly speaking, but a new class of software that is installed and/or activated with the concurrence of the user. This deserves attention, as a new

Smartphone Apps



An example of LBS, Foursquare app used at Madrid city center (left); Fake GPS spoofing (right) shows location at Manhattan while physically at Madrid

pattern of behavior appears where the figure of the user and the hacker merge in the same person.

To understand the distinction, let us compare the characteristics of malware and what we shall call GNSS faking software or GFS. Malware is introduced by a third party without the cooperation of or detection by the smartphone user; its operation is not initiated (at least voluntarily) by the user; and the benefits of malware operation are not for the user.

In contrast, GNSS faking software is installed by the smartphone user; its operation is initiated voluntarily by the user; the benefits of its use are obtained by the smartphone user directly.

The incentive to employ GFS arises in situations when the terminal user can gain an advantage or a benefit by falsifying his or her position/location. These can include such scenarios as safety and security (e.g., electronic monitoring of offenders), insurance (e.g., hiding traffic violations), labor (employee monitoring), cadastral surveys, transport (toll roads, travel distance–based tax schemes), banking, and any other activity that requires certainty about a reported location.

PanamNav has demonstrated how easy it is to fake an application such as FourSquare, a web and mobile application that allows registered users to post their location at a venue ("check-in") and connect with friends.

The opening images of this article illustrate an example of such an exercise using the app called FakeLocation for Android. The panel on the left shows a smartphone app displaying the actual location at which a photo was taken; the right-hand panel shows the same app with a faked location. A video demonstrating the test performed at Wayra facilities in May 2013 can be viewed at <http://www.youtube.com/watch?v=NL7Mrnioij4>.

Example: Improving Security for Banking Services

GPS is presently used in smartphones mostly for entertainment and sport. However, we can envisage a large new set of apps addressing safety and security problems that are encountered daily.

With the proliferation of smartphone-based payment systems, for instance, location information could be used as a key authentication factor, relating user location with purchase transactions and thereby helping to reduce fraud. Even the correlation of this information with credit card usage nowadays is already a feasible technique, as PanamNav has demonstrated in pilot studies with Visa and MasterCard.

Currently, credit card companies use a suspected discrepancy between the site of a transaction and the assumed location of the cardholder as a means for detecting fraud, but they usually do it in a very unrefined way. This accounts for the common practice by these companies of systematically blocking use of a credit card if, for example, a European cardholder tries to make a purchase in the United States shortly after landing at an airport. Use of a smartphone to authenticate the location of a cardhold-

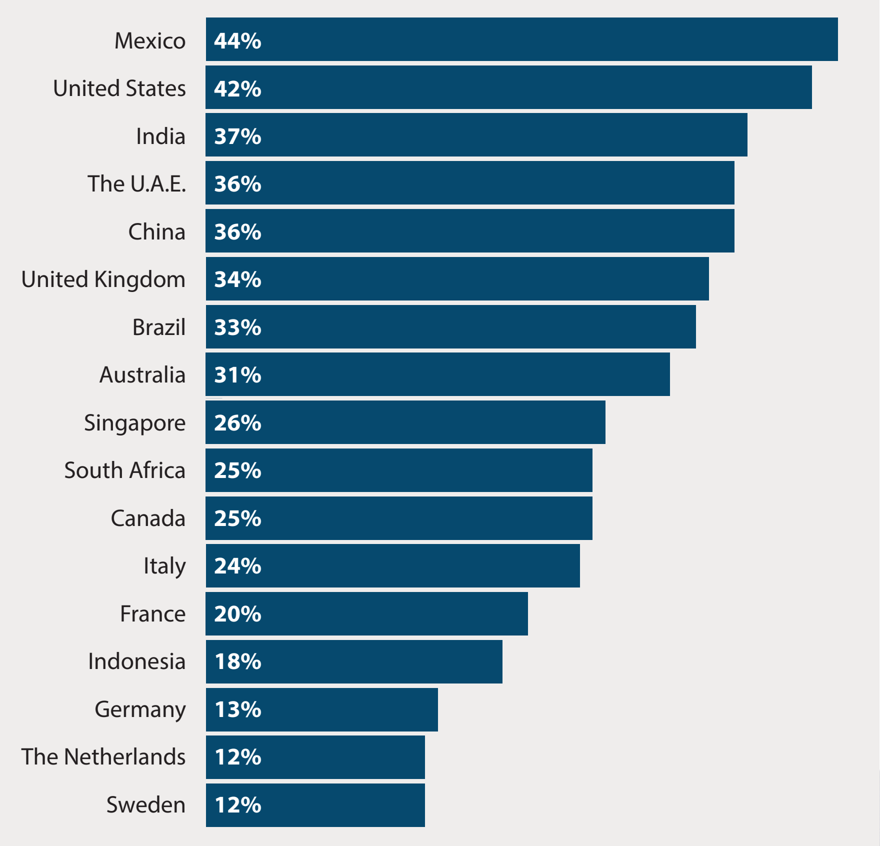
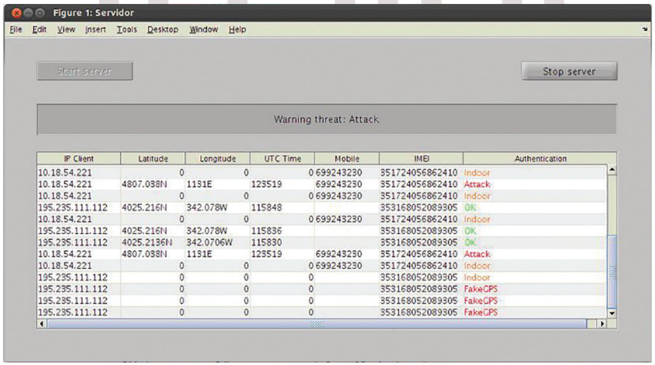


TABLE 1 Percentage of respondents who have experienced card fraud (N=5,114)



Warning threat: Attack

IP Client	Latitude	Longitude	UTC Time	Mobile	IMEI	Authentication
10.18.54.221	0	0	0	699243230	351724056862410	Indoor
10.18.54.221	4807.038N	1131E	123519	699243230	351724056862410	Attack
10.18.54.221	0	0	0	699243230	351724056862410	Indoor
195.235.111.112	4025.216N	342.078W	115848		353168052089305	OK
10.18.54.221	0	0	0	699243230	351724056862410	Indoor
195.235.111.112	4025.216N	342.078W	115836		353168052089305	OK
195.235.111.112	4025.2136N	342.0706W	115830		353168052089305	OK
10.18.54.221	4807.038N	1131E	123519	699243230	351724056862410	Attack
10.18.54.221	0	0	0	699243230	351724056862410	Indoor
195.235.111.112	0	0	0		353168052089305	Indoor
195.235.111.112	0	0	0		353168052089305	FakeGPS
195.235.111.112	0	0	0		353168052089305	FakeGPS
195.235.111.112	0	0	0		353168052089305	FakeGPS

FIGURE 1 GNSS events detection server developed by PanamNav in June 2013 for a mobile payments customer.

er in a credit transaction could alleviate such incidents.

According to a 2012 report by the Aite Group (**Table 1**), a financial services consultancy, a considerable difference has arisen between the United States and Europe in the number of people who have experienced credit card fraud: 42 percent of the U.S. population compared to 20 percent on average in Europe.

The primary factor for this difference is the prevalence in Europe of "chip and PIN" technology in credit cards, a combination of an embedded microchip and use of a personal identification number rather than a signature. The United States continues to rely on only magnetic strip containing relevant information due to the cost of technology migration.

This fact shows the promising effect of introducing a combined authentication factor strategy. The next natural step would be to integrate location information in the authentication process prior to payment authorization with the probable effect of a further substantial reduction in fraud.

With the widespread adoption of GNSS, location information is generally available nowadays and, what is even more important, it can be delivered in real time to react against fraud attempts. It can be applied also in indoor environments, because authentication is still useful with a time series of location traces.

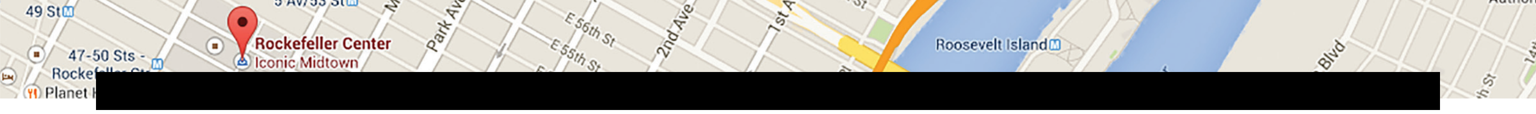
At this point, it might be helpful to clarify the difference between *authentication* and *integrity*. Integrity services are concerned primarily with present time information, and data from previous instants are not critical for, say, safety-of-life applications (although useful for computing continuity and availability figures).

In contrast, authentication is enriched by storing and analyzing the continuity and coherence of data in time series around the instants of interest. That is, the congruency of, say, the last 100 location points reported by a user can be used to validate the authenticity of the information provided. This technique — looking at the evolution over time of the locations reported and not just at the "present" location — is also called *vector tracking* by some authors.

At present, systems security is very much focused on answering the "who" question, and as a consequence we all have passwords, PIN numbers, or biometrics authentication methods in our daily tasks. However the "where" question is very much ignored despite the availability of technology to readily answer that question. A combination of both questions would provide a powerful synergy for increasing present security standards.

PanamNav has developed and demonstrated a platform with the technology for location authentication applied to mobile and credit card payments in mid-2012. **Figure 1** shows a view of the authentication server that was developed, which provides four types of status reports for location authentication: "OK," "Indoor" reception, "Fake GPS" use, and spoofing "Attack."

The system was able to differentiate between a situation in which a person was indoors and unable to provide a position fix and an incident of faked GPS location or a spoofing attack. A user who is indoors and unable to obtain a position fix is not necessarily showing an intentional behavior to block the infor-



mation. In such situations, the payment system relieved the user from responsibility for the lack of location information.

The "Authentication" column on the right-hand side of Figure 1 shows different events reflecting these four cases, and the associated IP address of each client device and its location, time, and identity, namely the phone number and International Mobile Equipment Identity (IMEI) number. Each type of event was identified by reading directly all the information available from the GPS chipset by means of a proprietary Android app developed by PanamNav that could be embedded or stand-alone. The server performed data correlation and issued the corresponding state report for each smartphone.

This tool proves the present feasibility of GNSS authentication based on mobile phones by correlating user location information directly with the physical protocol layer information provided by NMEA 0183 messages and bundled with other data available, for instance, from the mobile network, such as cell ID and location. Nevertheless, considerable improvements could be achieved with a richer variety of NMEA messages available from the embedded GNSS chips.

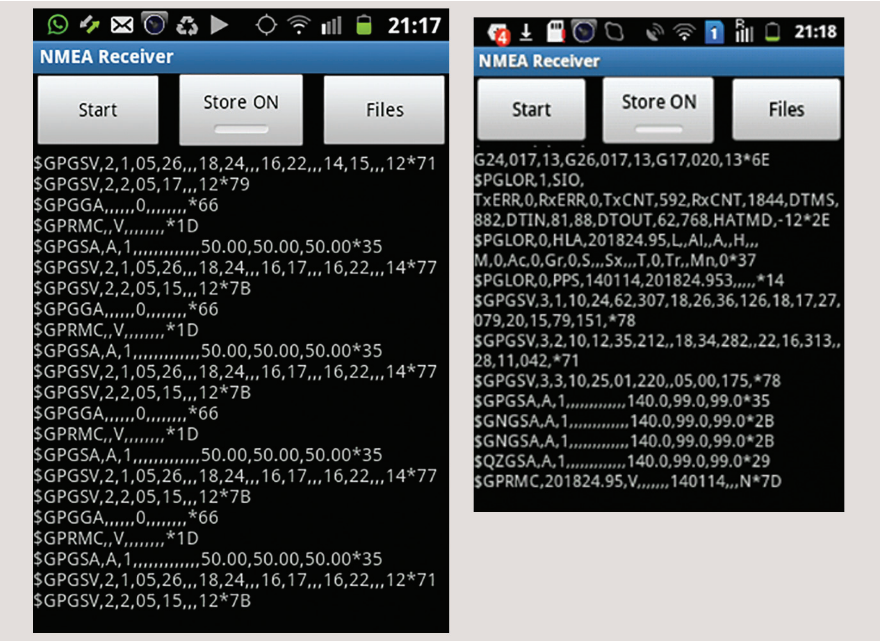
PanamNav encourages manufacturers to consider a wider view on the information to be provided by GNSS chips in the future in order to support more attractive services based on smartphones (as proposed in the conclusions to this paper).

Implementing Advanced GNSS Services on Smartphones

Apps based on GNSS information have shown an impressive growth in recent years.

One indicator of this trend is that not only companies but also institutions are contributing to the effort. In 2012, the EGNOS Office of the European Commission released a European Geostationary Navigation Overlay Service (EGNOS) Software Development Kit for the main mobile phone platforms.

However, for the time being applications are not able to exploit other information beyond time and position. Two main obstacles must be overcome in order to enable a new generation of services based on GNSS data.



```
$GPGSV,2,1,05,26,,,18,24,,,16,22,,,14,15,,,12*71
$GPGSV,2,2,05,17,,,12*79
$GPGGA,,,,,,0,,,,,,,,*66
$GPRMC,,V,,,,,,,,,*1D
$GPGSA,A,1,,,,,,,,,,,,,50.00,50.00,50.00*35
$GPGSV,2,1,05,26,,,18,24,,,16,17,,,16,22,,,14*77
$GPGSV,2,2,05,15,,,12*7B
$GPGGA,,,,,,0,,,,,,,,*66
$GPRMC,,V,,,,,,,,,*1D
$GPGSA,A,1,,,,,,,,,,,,,50.00,50.00,50.00*35
$GPGSV,2,1,05,26,,,18,24,,,16,17,,,16,22,,,14*77
$GPGSV,2,2,05,15,,,12*7B
$GPGGA,,,,,,0,,,,,,,,*66
$GPRMC,,V,,,,,,,,,*1D
$GPGSA,A,1,,,,,,,,,,,,,50.00,50.00,50.00*35
$GPGSV,2,1,05,26,,,18,24,,,16,17,,,16,22,,,14*77
$GPGSV,2,2,05,15,,,12*7B
$GPGGA,,,,,,0,,,,,,,,*66
$GPRMC,,V,,,,,,,,,*1D
$GPGSA,A,1,,,,,,,,,,,,,50.00,50.00,50.00*35
$GPGSV,2,1,05,26,,,18,24,,,16,17,,,16,22,,,12*71
$GPGSV,2,2,05,15,,,12*7B
```

```
G24,017,13,G26,017,13,G17,020,13*6E
$PGLOR,1,SIO,
TxERR,0,RxERR,0,TxCNT,592,RxCNT,1844,DTMS,
882,DTIN,81,88,DTOUT,62,768,HATMD,-12*2E
$PGLOR,0,HLA,201824.95,L,,AI,,A,,H,,,
M,0,Ac,0,Gr,0,S,,,Sx,,,T,0,Tr,,Mn,0*37
$PGLOR,0,PPS,140114,201824.953,,,,,*14
$GPGSV,3,1,10,24,62,307,18,26,36,126,18,17,27,
079,20,15,79,151,*78
$GPGSV,3,2,10,12,35,212,,18,34,282,,22,16,313,,
28,11,042,*71
$GPGSV,3,3,10,25,01,220,,05,00,175,*78
$GPGSA,A,1,,,,,,,,,,,,,140.0,99.0,99.0*35
$GNGSA,A,1,,,,,,,,,,,,,140.0,99.0,99.0*2B
$GNGSA,A,1,,,,,,,,,,,,,140.0,99.0,99.0*2B
$QZGSA,A,1,,,,,,,,,,,,,140.0,99.0,99.0*29
$GPRMC,201824.95,V,,,,,,,140114,,,N*7D
```

FIGURE 2 NMEA messages delivered by a Samsung Galaxy mini2 GT-6500D (left) and by a Samsung Yduos GT-S6102 (right)

Firstly, due to the low cost and power-consumption targets established in the design and selection of GNSS chips targeted for integration in smartphones, the information provided is limited to a subset of NMEA messages. Secondly, the subset of NMEA messages provided is not uniform among different types of smartphones — even among smartphones from the same manufacturer. For example, **Figure 2** shows a screen capture of the NMEA messages delivered by a Samsung Galaxy mini2 GT-6500D (left panel) and a Samsung Yduos GT-S6102 (right panel).

These two figures show the disparate landscape of the NMEA messages pool between two models of the same manufacturer. The only common baseline can be found in the messages GPRMC, GPGSA and GPGSV. GPRMC is well known as the minimum set of information to be delivered and is present in all smartphone devices. Depending on the model of smartphone, all other messages might be missing in practice, as no standard subset of NMEA messages exists.

The Yduos GT-S6102 shows a proprietary message called PGLOR that offers device-related information and is not a standardized NMEA message. This message is not present on the GT-6500D but is again available in Samsung Galaxy 3 and 4 smartphones.

PanamNav, in cooperation with Instituto Geográfico Nacional, has identified a wish list of GNSS data to be obtained from smartphones so that app developers can further expand the scope of services that can be provided on such devices. These services include anti-spoofing capabilities, advanced geodetic tools, improved accuracy, autonomous integrity, and location authentication.

As was shown in a previous *Inside GNSS* article, "Adding Intelligence to Receivers," (July/August 2013), signal-spoofing detection capabilities can be achieved by providing vector tracking through real-time measurements of Doppler effect, pseudorange, carrier phase, number of satellites providing NMEA data, frame data, lock and acquisition information, signal-to-noise ratio (SNR) and automatic gain control (AGC) behavior. This same set of data, used to evaluate the consistency of receiver performance, could also support autonomous integrity, location authentication,

and signal authentication rather than or in addition to using cryptographic solutions embedded in the GNSS signals themselves.

Smartphones could become very useful geodetic tools for use in the field if it were possible to have readings for pseudoranges and phase cycles provided along with the currently available NMEA data.

Coordinated use of uniform algorithms for integration and exploitation of multi-constellation information consistently among all chip models is also a must for achieving interoperability, data reliability, and universal exchange of information among smartphones and applications.

In order to support all these new possibilities, this brief list of suggested information is proposed for inclusion in new NMEA message formats: GNSS pseudoranges, frame data, Doppler measurements, SNR and AGC paired in real time, and carrier phase readings.

Additionally, agreement on a common set of NMEA messages for use in all models of smartphones would ease the task of the app developers who now have to write code with a considerable list of exceptions in order to cope with the disparate behavior of the various types of mobile devices.

Conclusions

This article has highlighted some key aspects to be considered for the embedding of GNSS chips in the next series of smartphones so as to enable advanced services beyond timing and positioning.

Higher accuracy, geodetic tools, autonomous integrity, and authentication capabilities could be added to smartphone capabilities with only minor and low-cost changes to the information delivered by GNSS chips.

Signal authentication is not sufficient for ensuring secure and reliable performance in smartphone software environments. Even for professional and commercial services, signal authentication would probably remain a question mark because positioning can be faked by software even after successful reception of authenticated signals.

We have emphasized the importance of focusing not only on the authentication of signal identity (the "who" question) but also to paying attention to the meaning of signal performance (the "where" question).

For this purpose two lines of actions are suggested:

- to create a forum for all relevant GNSS chip and smartphone manufacturers interested in introducing advanced features that will give them a competitive advantage in the market
- to propose a new set of NMEA data providing more details on signal information so that advanced services can be developed in smartphones.

These two lines of action have a natural convergence in corresponding standardization efforts. A successful standard for GNSS chips could have the same effect of GSM and DVB standards that have stimulated mass production, economies of scale, and deep penetration of the market. Hopefully GNSS technology, devices, and applications are the next successful worldwide market opportunity for sector growth and economy development in the 21st century.

Acknowledgments

The author expresses his appreciation for the support of Cesar Alierta, Jose Maria Alvarez-Pallete, Jesus Solana and Gonzalo Martin-Villa from Wayra/Telefonica; Miguel Angel Cano, Pedro Gonzalo, and Marcelino Valdés from Instituto Geográfico Nacional of Spain; Alberto Baeza, Pablo Pisonero, and Daniel Chung from PanamNav; and Leandro de Haro from Universidad Politecnica de Madrid. This work has been developed by PanamNav under sponsorship of Wayra/Telefónica in the period January/June 2013.

Additional Resources

[1] *Bloomberg Business Week*, "Smartphones in Use Surpass 1 Billion, Will Double by 2015," October 17, 2012, <http://www.businessweek.com/news/2012-10-17/smartphones-in-use-surpass-1-billion-will-double-by-2015>

[2] EGNOS SDK: <http://egnos-portal.gsa.europa.eu/developer-platform/egnos-toolkits/egnos-sdk>

[3] Fake GPS location app, Google Play – <https://play.google.com/store/apps/details?id=com.lexa.fakegps&hl=en>

[4] GPS apps in Google Play –<https://play.google.com/store/search?q=gps&c=apps>

[5] GPS - NMEA sentence information – <http://aprs.gids.nl/nmea>

[6] National Geographic Institute (Spain) geodetic data: <http://www.ign.es/ign/layout/datosGeodesicos.do>

[7] PanamNav at Wayra website – <http://wayra.org/en/startup/panamnav>

Author

Antonio Pujante Cuadrupani is responsible for the PanamNav project, a world reference in GNSS authentication solutions. He holds a Ph.D. and a M.Sc. in engineering from Universidad Politécnica de Madrid. He has been awarded two Galileo Masters Special Prizes (DLR and Gate/NavCert/IFEN) from the European Satellite Navigation Competition (ESNC) for his work on GNSS authentication. He was also a finalist in 2011 in North America and Bavaria regional competitions and first runner-up in 2012 in the Prague regional contest of the ESNC. PanamNav has also received in 2012 the IBM SmartCamp prize, the CeBit innovation prize, the StartEurope innovation prize and in 2013 the Wayra/Telefónica prize. Pujante has worked for Hispasat (1991–1994), Telefónica Sistemas (1994–1997), Eutelsat (1997–2005) and the European Space Agency (2005–2010). He has participated in the design and implementation of more than 25 satellites for Eutelsat and Hispasat and has been contributor to the development of the DVB-S, DVB-S2 and DVB-RCS standards. At ESA Pujante served as an officer for several activities related to advanced technology and GNSS studies. He has more than 20 international publications in satellite communications and GNSS and holds three patents on GNSS and communications. IG