Acta Univ. Sapientiae, Informatica, **5,** 1 (2013) 63–76

DOI: 10.2478/ausi-2014-0005

Location-stamp for GPS coordinates

Éva ÁDÁMKÓ
University of Debrecen
Faculty of Informatics
email: adamko.eva@inf.unideb.hu

Attila PETHŐ
University of Debrecen
Faculty of Informatics
email: petho.attila@inf.unideb.hu

Abstract. Anybody can make a time information authentic easily nowadays with the help of a time-stamp by a Certification Authority. In this paper, we propose a similar service for mobile devices—which have GPS receiver–to authentication GPS coordinates. This service name is location-stamping, and we propose two protocols for this service.

1 Introduction

Nowadays the applications which based on the Global Positioning System (GPS) gain more and more place for themselves, like the locating, passenger guiding, traffic controlling, tracking or navigation system. These services became vital parts of our everyday life. A big percentage of the mobile devices have a GPS receiver too.

In 2001 Alf Zugenmaier and Matthias Kabatnik in [8] introduced a location-stamp service for mobile telephone network. Their solution authenticates cell information. The usage of the protocol mentioned in this article is impossible in the case of GPS because the Certification Authority and the Location Measurement System carry on two-way communication with each other. In our case the Location Measurement System is the GPS, where the communication is one-way, because the satellite only can send the information, but can't receive it. In this article we propose two solutions for the cryptographic authentication of GPS coordinates. The basic idea is that the data received and/or

Computing Classification System 1998: K.6.5
Mathematics Subject Classification 2010: 68P30
Key words and phrases: location authentication, GPS, location stamp

computed by the GPS device are sent to a trusted organization, which can be for example a certification authority. Of course the GPS device digitally signs the message. If this information is compatible with other information available by the organization, then it signs the GPS coordinates. The basic difference between the two solutions is that while in the first case we assume that we have access to the row data sent by the satellites and received by the GPS device, thus they can be signed; however in the second case we have access only to the computed GPS coordinates. Thus the first protocol is favorable, but the second is safe enough in most applications. This paper is the essentially revised and extended version of our publication [1].

The paper is organized as follows. In Section 2 we give a brief introduction to the basics of Global Positioning Systems (GPS). In Section 3 we compare the geodesic and cryptographic notion of authenticity. Furthermore we describe situations when cryptographic authentication of GPS data may be important. Finally in Section 4 we present two protocols, which are able to solve the basic problem of authentication of GPS coordinates.

2 Global Positioning System

"The Global Positioning System (GPS) is a space-based global navigation satellite system that provides location and time information anywhere on or near the Earth." [3] The position calculation is based on trilateration with satellites orbiting in space, and the measuring system is a receiver, which communicates with the satellites through radio-waves. This communication is one way because the satellites only can send the information, but cannot receive it. Several software exist which are able to calculate the GPS coordinates from the "raw" data which come from the satellites. For this reason, a GPS receiver calculates the actual coordinates with a special software, from the data received from the satellites through radio-waves. The Global Positioning System has three distinct segments. These segments are the space segment, the control segment and the user segment. The space segment formed from a constellation of 24 satellites. The control segment consists of the stations, which control the satellites from the Earth and last the user segment means anybody, who receives the data which come from the satellites. See more about the Global Positioning System in the following books [3, 2].

3 Authenticity

It is very important to define the differences between the geodesic and the cryptographic authenticity, to understand the aims of this paper.

3.1 Geodesic authenticity

If we measure the position of an object, we can do it accurate with the help of the Global Positioning System. But this accuracy can mean different measuring result for different people. “For example to a hiker or soldier in the desert, accurate means about 15m. To a ship in coastal waters, accurate means 5m. To a land surveyor, accurate means 1cm or less. GPS can be used to achieve all of these accuracies in all of these applications, the difference being the type of GPS receiver used and the technique employed.” [4] In some cases we need extremely high accuracy. For example in the OPERA project of CERN the distance of the source of the CNGS neutrino beams at CERN and the OPERA detector at Gran Sasso, which is about 730 km was measured with a precision of 20 cm. [3] It is possible to correct the calculations with a lot of different methods. So we may declare that the GPS coordinates of an object are more accurate from geodesy viewpoint when we can calculate them with much smaller difference. In other words, it means, we can calculate them more precisely. To improve the precision of GPS coordinates the mathematical methods must be made more accurate. The devices are validated regularly, which means that their results are compared with the results of authentic devices.

3.2 Cryptographic authenticity

In this paper we deal with the cryptographic authenticity of GPS coordinates. We use a lot of data while we work with the GPS system, for example the raw data arriving from a satellite, the time information or the calculated coordinates. The task of cryptography is to prevent these data from changing during the process of the calculations. The changes can be made by for example a malicious person, a virus, a modified device or modified software sometimes it may happen by chance.

The cryptographic authenticity—as any other prevention—costs time and money. Only such data should be prevented, which are worth enough. We should ask the question: is the authenticity of these data important? The answer depends on the application. It is true that for example in passenger guiding, or in navigation not really important the above-mentioned certainty because the calculation of GPS coordinates takes so little time and it happens so often that there is no chance to change them and there is no point in changing them too. At the topic of vehicle-tracking, certainty-problem also forced a little bit, but for example, if you would like to prove with GPS coordinates that the fences of your neighbor is on your place it is quite certain that you will need some kind of authentication before the official establishments to prove your truth. Until in an argument of a parcel the Land Register proceed, and make exact measurement, but it cannot do in any cases due to capacity problems.

For the foregoing case here is an example, and this will be our main example: A supervisor of the Land Registry finds a field where the ragweed had proliferated. He wants to fine the owner. To prove his truth he makes an official report:

- locates the area with a GPS device,
- signs the report digitally,
- and asks for an authentic time stamp.

After all these, he proves when the report was made and that he made it. If the aforesaid cases come on for trial, then neither the penalized driver nor the civil servant can prove that their GPS coordinates are match the place where they made it. Despite the fact that the supervisor certified the location information by his digital signature.

They cannot prove that the location information is correct because not a single people or device is fully trusted too. Electronically saved or transmitted data can be changed easily, thus without some kind of provable signature the authenticity of data is always questionable. That is why we need some kind of service, which helps us to certify our place authentically, by GPS coordinates.

In this article we suggest a solution to this problem. Our solution that is the location-stamp may be similar to the time-stamp for the above problems. The time stamp is provided by a Certification Authority. The plan with the location stamp is similar, we need an organization that is independent from the measurement and can guarantee that nobody modified the results we got. We think this location stamp service workable by a Certification Authority too. Actually, the aim is that we should make us independent from the person who makes the measurement and the device which makes it.

4 Problem formulation

As for the precision of the device, there are several options for the cryptographic authenticity:

- First we trust the person and the device in all cases. We accept the measured coordinates, and the time provided by the device.

- Second we trust the person and the device, but we do not trust the time information of the device. We accept the measured coordinates, but we do not accept the time provided by the device.

- Third we neither trust the person nor the device. We neither accept the measured coordinates nor the time provided by the device.

In this paper we only deal with this third option and we introduce two solutions for that option. First there is a higher safety solution, which is the driver-level solution, and then there is a lower safety solution that is the software-level solution. The differences between these two solutions are the following: in the first case the authentic software is built in the driver level of a mobile device. The data are signed immediately the device received them. Thus the provided security is as high as possible. On the other hand it is very hardware dependent. In the second case the authentic software is on the level of the operating system. Its security is a little bit less than in the other solution. Thus we complement this version with a trilateration for the mobile device for added security.

We use the following cryptographic primitives during the work of the protocols: digital signature, hash function and time stamp. We do not detail the working of these cryptographic primitives here, but we recommend the book [7] for the interested readers for the easier understanding.

5 Protocols

5.1 High-safety solution: Driver-level

In this solution our aim is to get the raw data before somebody could modify them. We try to build our authentic software in a very deep layer of the process, so we would like to build it in the driver level.

5.1.1 Participants and notations

GPS is the Global Positioning System. The satellites of this system provide the data from which the GPS receiver calculates the coordinates of the actual position.

MD is the Mobile Device. The device with a GPS receiver, we make the positioning and the authentication with the help of this device.

CA is the Certification Authority. It provides the authenticate time and

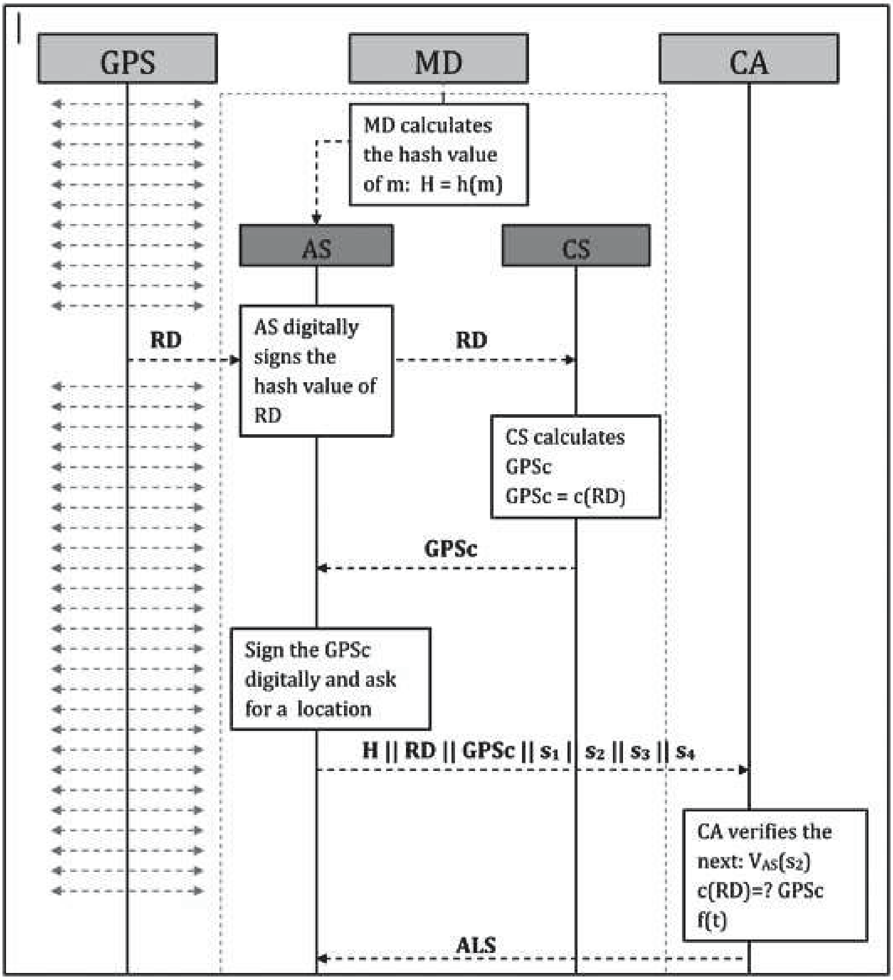
GPS
MD
CA
MD calculates the hash value of m: H = h(m)
AS
CS
RD
AS digitally signs the hash value of RD
RD
CS calculates GPSc GPSc = c(RD)
GPSc
Sign the GPSc digitally and ask for a location
H || RD || GPSc || s_1 || s_2 || s_3 || s_4
CA verifies the next: $V_{AS}(s_2)$ c(RD)=? GPSc f(t)
ALS

Figure 1: Driver-level protocol

location stamp, this is an organization, which is independent from the measurement and can guarantee that nobody modified the results we got.

AS is the Authentic Software. This software makes the authentication for the raw data (which come from the satellites) and for the calculated GPS coordinates.

CS is the Calculator Software. This software calculates the GPS coordinates of the actual position from the raw data come from the satellites.

M is the text or photo or some other data, that we want to authenticate with a location-stamp.

$h(\dots)$ is the hash function.

H is the hash value of the M.

$c(\dots)$ is the calculator function, which calculates the current position from the raw data that come from the satellites.

RD is the raw data come from one of the satellites of Global Positioning System.

GPSc is the GPS coordinate calculated by the calculator software.

$\mathsf{S}_{\mathsf{AS}}(\dots)$ is the signature of the data in parenthesis with the private key of the authentic software.

$\mathsf{S}_{\mathsf{CA}}(\dots)$ is the signature of the data in parenthesis with the private key of the certification authority.

$\mathsf{V}_{\mathsf{AS}}(\dots)$ is the verification of the data in parenthesis with the public key of the authentic software.

$\mathsf{V}_{\mathsf{CA}}(\dots)$ is the verification of the data in parenthesis with the public key of the certification authority.

s_{i} is the ith signed data.

TIME is the time information.

t is the time information of RD.

ALS is the authentic location stamp, generated by the certification authority.

$f(\dots)$ is the freshness checking function.

5.1.2 Protocol

1. MD calculates the hash value of $\mathsf{M} : \mathsf{H} = \mathsf{h}(\mathsf{M})$
2. $\mathsf{MD} \rightarrow \mathsf{AS} : \mathsf{H}||\mathsf{M}$
3. AS digitally signs H with its private key: $\mathsf{s}_1 = \mathsf{S}_{\mathsf{AS}}(\mathsf{H})$
4. $\mathsf{GPS} \rightarrow \mathsf{AS} : \mathsf{RD}$
5. AS digitally signs the hash value of RD with its private key: $\mathsf{s}_2 = \mathsf{S}_{\mathsf{AS}}(\mathsf{h}(\mathsf{RD}))$
6. $\mathsf{AS} \rightarrow \mathsf{CS} : \mathsf{RD}$
7. CS calculates the actual position from RD : $\mathsf{GPSc} = \mathsf{c}(\mathsf{RD})$
8. $\mathsf{AS} \leftarrow \mathsf{CS} : \mathsf{GPSC}$
9. AS digitally signs the hash value of GPSc with its private key: $\mathsf{s}_3 = \mathsf{S}_{\mathsf{AS}}(\mathsf{h}(\mathsf{GPSc}))$

10. AS concatenates H, s_1 , RD, s_2 , GPSc and s_3 and takes its hash value and then digitally signs this hash value with its private key:
    $s_4 = S_{AS}(h(H||RD||GPSc||s_1||s_2||s_3))$
11. $AS \rightarrow CA : H||RD||GPSc||s_1||s_2||s_3||s_4$
12. CA verifies that the raw data were signed by AS and CA verifies that GPSc can be computed from RD, and checks the freshness of the t.
    $V_{AS}(s_2)$
    $c(RD) = ?GPSc$
    $f(t)$

    12.1. if the answer is true for all questions, then CA makes the authentic location-stamp:
    $ALS = TIME||S_{CA}(h(H||RD||GPSc||s_1||s_2||s_3||s_4||TIME))$
    $AS \leftarrow CA : ALS$

    12.1.1. AS verifies that really the CA signed the location-stamp that it got:
    $V_{CA}(ALS)$

    12.1.1.1. if the answer is true, then AS accepts the authentic location-stamp

    12.1.1.2. if the answer is false, then AS starts a new location-stamp request with step 4.

    12.2. if the answer is false, then CA rejects to generate the authentic location-stamp
    $AS \leftarrow CA : rejection$

5.1.3 Protocol description

The protocol, described in the previous subsection, have three important participants, these are the satellites of the Global Positioning System, the mobile device and the certification authority. The mobile device generates a print of the data,—we want to stamp with an authentic location stamp—initially with an eligible hash function, this is necessary because of the digital signing. After this the authentic software, which is built in the driver of the mobile device, gets the data from the three GPS satellites, and then it digitally signs these data with its own private key presently. This signing is required in order that nobody is able to falsify during the computational process the raw data arriving from the satellites. The authentic software located in the driver of the mobile device so it can protect the data from the attack of any software installed on the operation system of the mobile device. Once the authentic software digitally signed and stored the raw data, sends it to the calculator software. The calculator software calculates the current GPS coordinates from the present raw data and sends back the result to the authentic software. The authentic software digitally signs these data too. Now we arrived at the point that the authentic software is able to ask for an authentic time stamp from the certification authority. So the authentic software sends a request to the certification authority, this request contains the data hash value, the raw data and the calculated coordinates concatenated and digitally signed with its own private key. Then the certification authority generates a nonce value in order to ensure the freshness of the protocol and gives it back to the software. The authentic software appends the nonce to the previous request and turns it back to the certification authority, which checks that really the authentic software sent the request. If the result of the verification is right then the certification authority checks that GPSc can be computed from the raw data, if the answer is true, then it generates the location stamp, which also includes a time stamp too.

5.2 Lower-safety solution: Software-level

The protocol of the previous section is hardware dependent. This is because we signed the raw data received by the GPS device from the satellites. Our aim in the sequel is to describe a less hardware dependent authentication. Thus we cannot assume to have access to the raw data, but only calculated GPS coordinates. Hence to authenticate the data of the GPS device, the trusted organization has to have own data which it can compare with received ones. The mobile phone services have cell information, but they are usually not accurate enough to fix the location the GPS device. By our knowledge this is possible in bigger cities where the mobile network coverage is broad enough. Then the mobile phone service has independent information on the location of the GPS device, which can be compared to the data it sends to the trusted organization. This second protocol is only applicable if the above assumption holds. After this preparation we present the details of the protocol.

5.2.1 Participants and notations

Here we mention only those symbols which differ from participants or notations in the previous protocol, other symbols denote the same as above. *MPSP* is the Mobile Phone Service Provider, this provides the cell information for a mobile identifier.

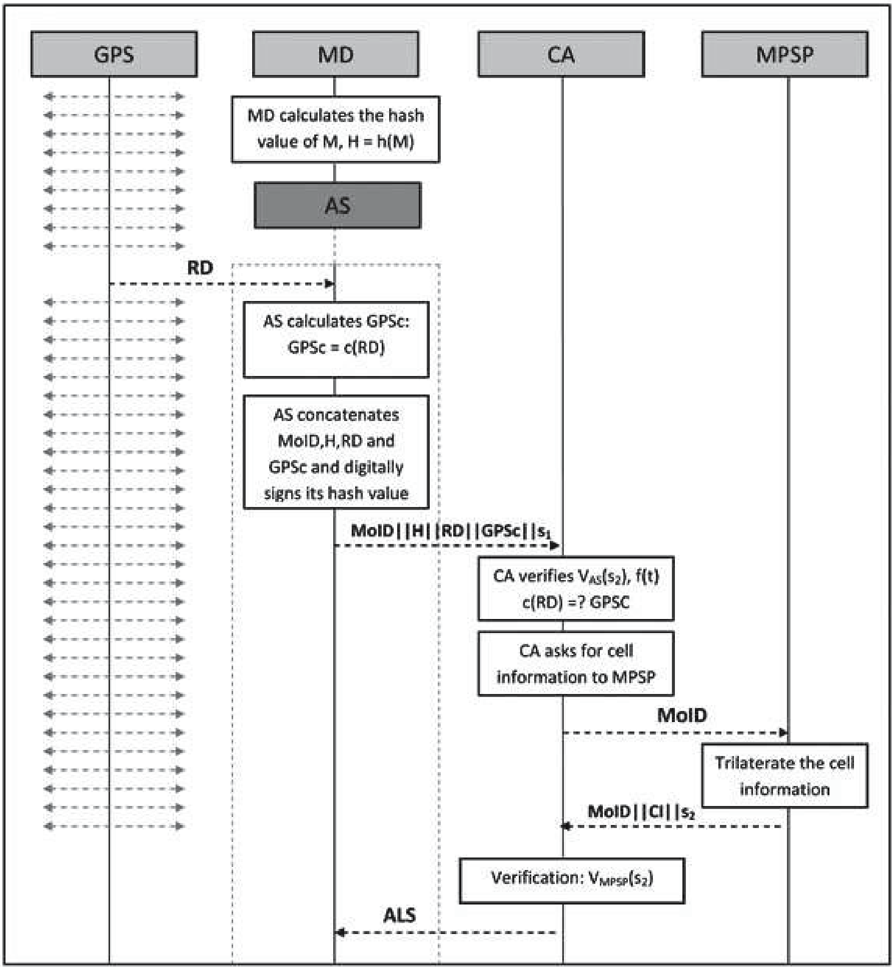
GPS
MD
CA
MPSP
MD calculates the hash value of M, H = h(M)
AS
RD
AS calculates GPSc: GPSc = c(RD)
AS concatenates MoID,H,RD and GPSc and digitally signs its hash value
MoID||H||RD||GPSc||s1
CA verifies VAS(s2), f(t) c(RD) =? GPSC
CA asks for cell information to MPSP
MoID
Trilaterate the cell information
MoID||CI||s2
Verification: VMPSP(s2)
ALS

Figure 2: Sotware-level protocol

AS is the Authentic Software. This software makes the authentication for the calculated GPS coordinates.

MoID is the Mobil identifier, a number from which the MPSP can identify the current mobile device.

$t(\dots)$ is the trilateration function, trilaterates the CI from the MoID.

CI is the cell information from the MPSP.

$ck(\dots)$ is the checking function, which checks if a GPS coordinates are in the area which is defined by the cell information.

$S_{MPSP}(\ldots)$ is the signature of the data in parenthesis with the private key of the mobile phone service provider.

$V_{MPSP}(\ldots)$ is the verification of the data in parenthesis with the public key of the mobile phone service provider.

5.2.2 Protocol

1. MD calculates the hash value of $M : H = h(M)$
2. $MD \rightarrow AS : H||M$
3. $GPS \rightarrow AS : RD$
4. AS calculates the actual position from RD : $GPSc = c(RD)$
5. AS concatenates MoID, H, RD and GPSc and digitally signs its hash value with its private key:
   $s_1 = S_{AS}(h(MoID||H||RD||GPSc))$
6. $AS \rightarrow CA : MoID||H||RD||GPSc||s_1$
7. CA verifies that the raw data were signed by AS and CA verifies that GPSc can be computed from RD and checks the freshness of the t.
   $V_{AS}(s_1)$
   $c(RD) = ?GPSc$
   $f(t)$

   7.1. if the answer is true then:
   $CA \rightarrow MPSP : MoID$ and asks for a cell information

   7.1.1. MPSP trilaterates CI from the MoID:
   $t(MoID) = CI$
   $s_2 = S_{MPSP}(MOID||CI)$
   $CA \leftarrow MPSP : MOID||CI||s_2$

   7.1.2. CA verifies that really the MPSP signed the data, which it got, and, that the GPSc matches to the CI:
   $V_{MPSP}(s_2)$
   $ck(GPSc, CI) = true$

   7.1.2.1. if the answer is true, then CA makes the authentic location-stamp:
   $ALS = TIME||SCA(h(MoID||H||RD||GPSc||s_1||s_2||CI||TIME))$
   $AS \leftarrow CA : ALS$

   7.1.2.1.1. AS verifies that really the CA signed the location-stamp that it got:
   $V_{CA}(ALS)$

7.1.2.1.1.1 if the answer is true, then AS accepts the authentic location-stamp

7.1.2.1.1.2 if the answer is false then AS starts a new location stamp request with the step 3.

7.1.2.2. if the answer it false then CA asks a new cell information with the step

7.2. if the answer is false, then CA rejects to generate the authentic location stamp
$\mathsf{AS} \leftarrow \mathsf{CA} : \mathsf{rejection}$

5.2.3 Protocol description

Against the protocol, described in the previous chapter, in this part the protocol has four important participants, the satellites of the Global Positioning System, the mobile device, the certification authority and the mobile phone service provider of the actual mobile device. There are some other differences between the two protocols, in the previous solution the authentic software is built in the driver level of the mobile device, in the actual case the software is installed on the operation system of the mobile device as it usually. The mobile device initially generates a print of the data with a hash function as same as the previous case. After this the authentic software, which is installed on the mobile device, gets the data from the three GPS satellites, and calculates the current GPS coordinates from the present raw data. Then it concatenates these two values, the document hash value and the mobile device identifier and digitally signs with its own private key. After this the authentic software asks for an authentic time stamp from the certification authority with the help of these digitally signed data. The certification authority generates a nonce value in order to ensure the freshness of the protocol and gives it back to the software. The authentic software appends the nonce to the previous request and turns it back to the certification authority, which checks that really the authentic software sent the request. Now the certification authority sends the identifier of the mobile device to the mobile phone service provider, which trilaterates the cell information for the device and gives it back. In this point only the verification remains behind. If the result of the verification is right, namely the calculated GPS coordinates matches to the cell information, and the private key belongs the authenticate software, then the certification authority generates the location stamp, which also includes a time stamp too.

6 Attacks

In the field of authentication of GPS information there are two main type of the possible attacks, these are jamming and spoofing.

- Jamming

In the course of jamming the attacker try to interrupt the connection between GPS satellites and GPS receivers. It is fairly an easy task, considering that the GPS satellites are orbiting in the space 20 000 km far from the Earth. This is the first reason why the broadcast signals are not too powerful and the other reason is that this communication happens over wireless connection. Therefore, the aim of the attacker is that make the satellites inaccessible for the receivers. In order to achieve the former goals the attacker produce an obstruction into the connection.

- Spoofing

In contrast with jamming, in the course of spoofing attack the connection between satellites and receivers is in good working order. Spoofing cause a much more dangerous situation. The attacker transmits a more powerful signal than the signal broadcast by the GPS satellites. From this point the receiver will think that this modified signal is the original which comes from the satellites. The fact that the receiver will receive this modified signal means that the attacker can fake the location information of the receiver, and this can mislead the user.

Compared to some other authentication method for GPS coordinates [5, 6] none of our protocols protects against jamming and only one of them protects against spoofing, but this was not the goal that we would have liked to achieve. Neither spoofing nor jamming is relevant to our case because this protocol is intended to use in the civil service. In the case that someone disrupts or terminates information flow - so the jamming occurred -, then there is simply no data that needs to be validated. There is a low-level security against spoofing in the second protocol, but this type of attack is not probable, because these data we would like to verify are not at the high classified level. So these data are not worth so much to make sense of spoofing—falsifying the GPS signals—. If you would like to verify a high classified data, then this can easily achieved by strengthen our protocol with another anti-spoofing solution, our make some changes on one of these protocols. Maybe in the future we will use some of these solutions to amplify the security of our protocol. In summary, our solution protects data from that point that they are in the mobile device.

7 Conclusion

In this article, we describe two protocols to authenticate GPS coordinates in a mobile device, and we did not give solutions to jamming or spoofing attack. So this service can only provide against for example the following type of attacks: modified software on the mobile device (which calculate false coordinates), direct adding a fake location information to the device (by hand, or by sms, or via email) or some analogue attacks. In a second article we would like to analyze the security and complexity of these protocols.

References

[1] É. Ádámkó, A. Pethő, Helyszín-bélyegzés, hitelesített GPS koordináták, in: *Az elmélet és a gyakorlat találkozása a térinformatikában, Ed.: Dr. Lóky József*, Debrecen, Hungary, 2011, pp. 381–388. ⇒64

[2] A. El-Rabbany, *Introduction to GPS: The Global Positioning System* (2nd edition), The Artech House Press, 2006. ⇒64

[3] B. Hofmann-Wellenhof, H. Lichtenegger, J. Collins, *Global Positioning System: Theory and Practice*, The Springer Press, 1993. ⇒64, 65

[4] C. Kennedy, GPS Basics, *GeoPlane Services.* (1999), `http://www.geoplane.com/gpsbasics.pdf` ⇒65

[5] M. G. Kuhn, An Asymmetric Security Mechanism for Navigation Signals, *Sixth Information Hiding Workshop*, Toronto, Canada, 2004, pp. 239–252. ⇒75

[6] S. Lo, D. De Lorenzo, P. Enge, D. Akos, P. Bradley, Signal Authentication, A Secure Civil GNSS for today, *InsideGNSS, Technical Article*, 2009 September-October, pp. 30–39. ⇒75

[7] A. J. Menezes, P. C.van Oorshot, S. A. Vanstone, *Handbook of applied cryptography*, The CRC Press, 1997. ⇒67

[8] A. Zugenmaier, M. Kabatnik, Location stamps for digital signatures: a new service for mobile telephone networks, *ICN'01 Proc. First International Conference on Networking, Part 2*, Colmar, France, 2001, pp. 20–30. ⇒63

Received: March 19, 2013 • Revised: June 1, 2013