Secure Indoor Positioning System based on Inertial Measurements for Low Cost Devices

Iván Santos-González, Alexandra Rivero-García, Pino Caballero-Gil, Jezabel Molina-Gil

Department of Computer Engineering
University of La Laguna, Tenerife, Spain
Email: {jsantosg, ariverog, pcaballe, jmmolina}@ull.edu.es

***Abstract*—This work describes an alternative solution for the problem of indoor location in places where the use of GPS devices is either impossible or not precise enough. The new proposal is based on different methods that provide useful information about location in this type of places. In particular, the use of Near Field Communication (NFC) technology in combination with an Inertial Measurement Unit through mobile phones or smartphones allows solving the problem of indoor location without incrementing costs. In particular, an Android application has been implemented to show the applicability of the proposed solution, which adds a layer of security that it is very important to protect the positioning information and avoid the possibility of traceability of the users of the system. To do this, the FourQ elliptic curve has been selected to generate a shared key using the elliptic curve Diffie-Hellman protocol. Then, the generated key is used to encrypt all communications through the use of the SNOW 3G stream cipher. The developed system offers promising results.**

Keywords–Security; Positioning; IMU; Elliptic Curves; Low Cost.

I. INTRODUCTION

One of the places where location is not working well nowadays is indoors. It is well known that outdoors the use of GPS positioning system provides an accurate location, but its use indoor is not possible. The need of an indoor location system is essential in huge indoor places like malls or airports. The traditional way to solve this problem has been to place static maps in different points of the building indicating where you are inside the building map. The main disadvantage of this kind of information points is that they are not accessible in all building spaces.

It is known that smartphones are becoming more and more essential in our daily lives because we do not use the smartphone only to make phone calls or to send Short Message Service (SMS) messages, but also to do other tasks such as taking pictures, recording videos, reading mails, locating with Global Positioning System (GPS) or surfing the Internet. Due to this, different indoor location solutions based on smartphones have been proposed in the last years.

The proposal presented here is based on the use of two technologies: Near Field Communication (NFC) technology [1], which provides a short-range positioning, and an Inertial Measurement Unit (IMU) [2] settled on the user foot, which provides inertial changes to track the user's movement. The use of these technologies allows us to provide real-time position in a smartphone using an indoor map of the building. An aspect that is very important in this kind of systems and that is not usually studied is its security, and in particular, the untraceability of the users. To avoid this, the presented proposal adds the use of an elliptic curve Diffie-Hellman protocol [3] using the FourQ elliptic curve to generate a shared key and the Snow 3G stream cipher algorithm [4] to encrypt all communications between the IMU and the smartphone.

This work is structured as follows. Section 2 describes some preliminaries. The proposed system is defined in Section 3. Section 4 introduces some features of the system security. Finally, some conclusions and open issues close this paper.

II. PRELIMINARIES

During the last years, different proposals have been presented in the field of use of IMUs to track the movement and/or position of users in different situations. There are different IMU types, but traditionally, the ones used to track the movement and/or position have been the 6 Degrees of Freedom (DoF) or 9 DoF IMUs. A 6 DoF IMU usually has a 3 DoF accelerometer and a 3 DoF gyroscope. The accelerometer is used to measure the acceleration on IMU movements in the x, y and z coordinate systems, that can be easily transformed into speed through the first time integral of the acceleration, and to position through the second time integral of the acceleration. Thus, it can be used to measure changes in the speed and position respectively. A problem that usually appears when obtaining speed and position through the use of the integral is that if the intrinsic constant error is not removed from the original measurement, the acceleration, it becomes a lineal error in the speed and in a quadratic error in the position, fact that would do the system unusable. The gyroscope measures the orientation in the x, y and z coordinate systems. A 9 DoF IMU has the 3 DoF accelerometer and gyroscope and adds a 3 DoF magnetometer, a sensor that measures the magnetic field and that is usually used to get the global orientation due to the earth magnetic field. A complete guide of the most common error sources of the use of IMU for positioning systems and its effects on the navigation performance can be found in [5].

This kind of systems is widely used to track the movements in the space, so different proposals have been presented during the last years. A method that is usually used and that is based on the measurements of these aforementioned sensors is the Dead-Reckoning. This method consists on the use of different algorithms based on easy trigonometric equations to get the actual position of an object or person, through operations based on the course and navigation speed. There are multiple algorithms that implement the Dead-Reckoning [6]. In that paper, a comparative study of different Pedestrian Dead-Reckoning algorithms is presented. A Pedestrian Dead-Reckoning algorithm is basically an algorithm that estimates the movement of a person by detecting steps, estimating stride lengths and the directions of motion. The results obtained in

 ISBN: 978-1-61208-615-6

that work shows how this technique offers promising results with an average rate on the stride length estimation errors of about 1% and an estimation below 5% in the total travelled distance. Another method that is usually applied to improve the performance and to reduce the drift error on the sensors measurements is the use of static and adaptative filters, and one of the most used filters is the Kalman filter [7].

III. Proposed System

The developed system consists on an Android application that shows in an indoor map the current position of the user. This building indoor map must be previously provided by the building staff with its correct scale to be added to the system. The system uses two different technologies to perform this feature.

On the one hand, the NFC technology is used at the entrance and some specific points of the indoor places to set an initial position of the user in the map. The NFC technology was chosen for this purpose because it is a short range communication technology with no error in the initial position estimation. The selection of this technology instead of another cheaper like QR codes is because the NFC technology is easier to protect than the QR codes as shown in Section IV.

On the other hand, the use of an IMU located on the user foot supposes an static reference point. The use of an IMU located on the user foot is a more accurate way of collecting data than the smartphone because it is static and produces less noise than the use of smartphone sensors. The IMU is used to collect data about the accelerometer, gyroscope and magnetometer sensors, which are sent to the user smartphone through the use of Bluetooth Low Energy (BLE) [8] technology. The use of the IMU unit instead of the user smartphone is due to the smartphone movements could add some noise to the measurements and the measurements obtained through the IMU sensors are more precise than the smartphone measurements. In the user smartphone, the sensor data are processed through the use of the Madgwick algorithm. This algorithm provides an accurate orientation of the user in a quaternion form [9], which provides an absolute orientation from a relative one. Then, the quaternion is used to orientate the position in the indoor map.

Finally, a step length estimation has been used to perform an exhaustive study of different methods. As initial method, we decided to use a simple way to calculate the step length in centimetres, l, which can be shown in the equation 1, where h represents the height in centimetres of the user and k is a constant that is 0.415 for men and 0.413 for women [10].

$$l = hk \tag{1}$$

In future versions of the system, more efficient, precise and complex step length estimation methods will be implemented. Moreover, a comparative study of the accuracy of the different methods will be performed too. Some screenshots of the developed prototype can be shown in Figure 1.

The general system performance can be shown in Figure 2. The steps that a user of the system takes during its use are:

1) The initial step of the system consists of putting the user's height the first time that he/she uses the application to calculate the step length.

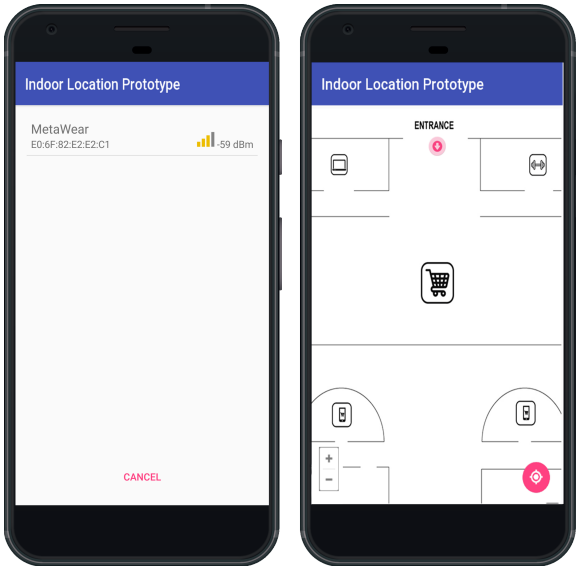

Figure 1. Prototype Aplication Screenshots

2) The user scans the NFC tag situated at the entrance. The NFC tag contains some identification numbers that represents the building, the entrance and the floor. The possibility of put more NFC tags around the building is open for some cases where the user forgot to do it at the entrance. This information is important to situate the user in the right place inside the building and floor.
3) Once the NFC tag has been read, the user can see her/his initial position over the floor map.
4) At this moment, the IMU unit starts to collect data and send them to the user smartphone, which is responsible for operating with it. The Madgwick algorithm is used to get the orientation in real time. With the quaternion obtained by algorithm and the step length, the user position for each step is shown in the smartphone.

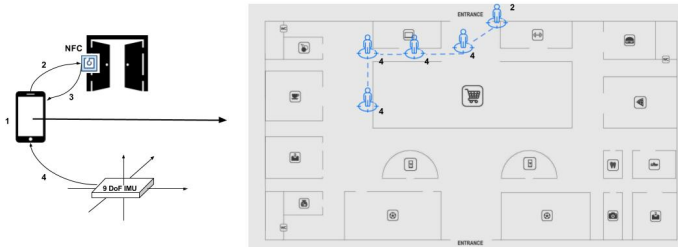

Figure 2. General System Performance

A. IMU Positioning System

The main part of the indoor positioning system is the part related to the IMU collected data and its treatment. In our positioning system a Metawear CPRO IMU that collect measures of the 3 sensors, accelerometer, gyroscope and magnetometer, obtaining g, $degrees/seconds$ and $Tesla$ units respectively, has been used. The complete specifications of the IMU unit can be shown in [11]. This IMU unit transmit the data through

BLE. The collected data is transmitted in real time to the smartphone where the treatment of the different variables is performed, including the conversion of accelerometer units, g, to m/s^2, and the gyroscope units, $degrees/seconds$, to rad/s. Then, the Madgwick filter is applied to obtain the quaternion that represents the pitch yaw and roll. With these data, the step detection and the step length, the user's position is shown over the map every time he/she takes a step. Different studies about the use of filters in IMU units data to improve the quality and reduce the noise in the data have been performed [12] [13] [14], showing that the Madgwick filter is the most appropriate in this kind of systems. In this paper, as complementary work, we decided to implement tests of three of the most used filters, a Kalman filter, a Mahony filter and the aforementioned Madgwick filter. The representation of the pitch, yaw and roll obtained in the tests are shown in Figure 3, Figure 4 and Figure 5, respectively. In all plots, the Kalman filter is represented in green color, the Mahony filter in blue and the Madgwick one in orange. During the different tests, the Magdwick filter shows a better accuracy by comparing the real position with the position shown in the Android application.

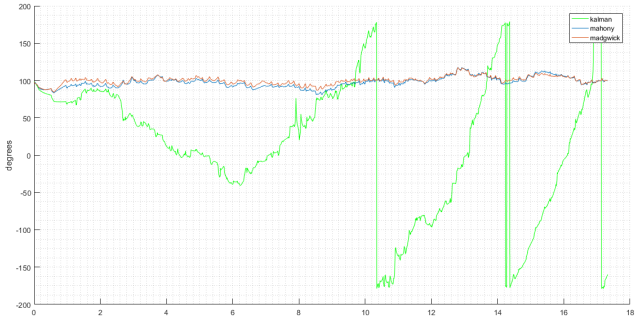

Figure 3. Filters Yaw

Figure 4. Filters Pitch

IV. System Security

In location systems, security is a very important aspect. A vulnerable application can involve a privacy problem, and in particular, traceability. The traceability of a user can imply a huge problem for the users of an application because an attacker could know where a user is in every moment and so perform derived attacks. For example, if the attacker knows that we are not at home, he/she could steal the house, or sell our data to different companies to allow that they send us, for example, food publicity if the user is in the kitchen, or shampoo publicity if the user is in the toilet, etc.

Figure 5. Filters roll

To protect the system, we decided to use two different methods. On the one hand, we used the Snow 3G stream cipher algorithm to encrypt all communications and an elliptic curve Diffie-Hellman (ECDH) protocol using the elliptic curve FourQ to generate a shared key. On the other hand, we decided to change the secret key every time the application is restarted to use it like a session protocol.

The trust model of the proposed system is based on using the FourQ elliptic curve through the ECDH protocol to generate a shared key each time a session starts. Then, this key is used to encrypt the communications between the IMU and the smartphone using the SNOW 3G stream cipher algorithm. The use of these two methods, ECDH and SNOW 3G, has been commonly used in different papers and its security is widely tested [15] [16].

A. Snow 3G

SNOW 3G is the stream cipher algorithm designated in 2006 as basis for the integrity protection and encryption of the UMTS technology. Thanks to the fact that the algorithm satisfies all the requirements imposed by the 3rd Generation Partnership Project (3GPP) with respect to time and memory resources, it was selected for the UMTS Encryption Algorithm 2 (UEA2) and UMTS Integrity Algorithm 2 (UIA2) [17] [18].

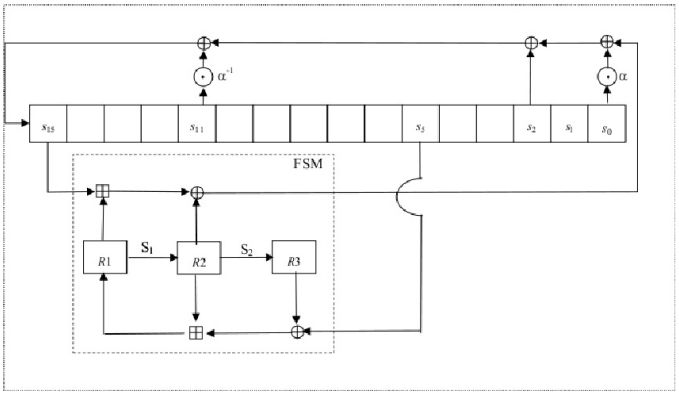

Figure 6. SNOW 3G scheme

The SNOW 3G algorithm derives from the SNOW 2 algorithm, and uses 128-bit keys and an initialization vector in order to generate in each iteration 32 bits of keystream. On the one hand, the LFSR used in this algorithm has 16 stages denoted s0, s1, s2... s15 with 32 bits each one. On the other hand, the used Finite State Machine (FSM) is based on three 32-bit records denoted R1, R2 and R3 and uses two Substitution-boxes called S1 and S2. The combination operation uses a XOR and an addition module 2^{32}, as we can see in Figure 6.

SNOW 3G has two execution modes: the initialization mode and the keystream mode. First, the initialization mode is executed without producing any keystream. Then, the keystream mode is executed. In particular, the number of iterations of such a mode depends on the number of 32-bit words that we want to generate.

B. FourQ ECDH

The use of elliptic curves in cryptography has been widely discussed during the last years and the advantages that they have with respect to the traditional cryptography both in key length and computational requirements are well known. The FourQ is a new elliptic curve developed by Microsoft Research [19], which accomplishes the NIST requirements for the selection of new generation elliptic curves. These requirements are that new curves must, at least, maintain the security level of the previous ones and be highly efficient in software and hardware implementations. This curve produces promising results, as shown in different studies presented by Microsoft Research, and offers improvements in the computing times in the tests done in traditional computers. To know if the improvements shown in the Microsoft Research tests are possible too in portable devices, where the processor architecture is totally different, because computers usually use an x32 or x64 architecture while the smartphones and portable devices usually use the arm architecture, we decided to port the implementation done by Microsoft Research to Java language to use it in Android devices. To do this, a java library was made and the FourQ computing time executing an elliptic curve Diffie-Hellman protocol was compared between FourQ, the NIST P-256 curve [20] and the Curve25519 curve [21]. The results of this comparison can be seen in Table I.

TABLE I. ELLIPTIC CURVES DIFFIE-HELLMAN EXECUTION TIME COMPARISON

Curve	Time
Curve25519	721 ms
Curve NIST P-256	1876 ms
Curve FourQ	417 ms

The computing times shown in Table I show that the FourQ elliptic curve offers interesting improvements in portable devices too. In particular, this curve is 2 times faster than the new generation Curve25519 curve and around 4-5 times faster than the NIST P-256 curve. The use of this curve can be an important advance in the IoT security due to the lower key length and higher efficiency, facts that are specially important in this kind of devices with low computing and storage capacities.

V. CONCLUSIONS

This work presents a new indoor location and positioning system that offers promising results. The combination of different technologies allow us to obtain the location indoors with a high level of precision. The use of a low cost IMU makes that the system could be used by a lot of people in a near future. During the simulations, an Android application prototype has been developed to collect the IMU information, proceed with the different calculations and show the path over the indoor map. The security of this kind of systems is essential, so different protocols and security algorithms have been implemented to avoid possible user's traceability by a malicious attacker. This is a work in progress, so several lines are still open. The first of them is the study of other sensor fusion algorithms that could fit the developed system better. Another improvement could be the use of sensors of the previously attached smartphone instead of the IMU to perform the positioning. On the other hand, security tests and controlled attacks to improve the system security are also necessary.

ACKNOWLEDGMENT

Research supported by TESIS2015010102, TESIS-2015010106 and by the Spanish Ministry of Economy and Competitiveness, the European FEDER Fund, and the CajaCanarias Foundation, under Projects TEC2014-54110-R, RTC-2014-1648-8, MTM2015-69138-REDT and DIG02-INSITU.

REFERENCES

[1] V. Coskun, K. Ok, and B. Ozdenizci, Near field communication (NFC): From theory to practice. John Wiley & Sons, 2011.

[2] M. M. Morrison, "Inertial measurement unit," Dec. 8 1987, uS Patent 4,711,125.

[3] N. Koblitz, "Elliptic curve cryptosystems," Mathematics of computation, vol. 48, no. 177, 1987, pp. 203–209.

[4] A. Kircanski and A. M. Youssef, "On the sliding property of snow 3g and snow 2.0," IET Information Security, vol. 5, no. 4, 2011, pp. 199–206.

[5] W. Flenniken, J. Wall, and D. Bevly, "Characterization of various imu error sources and the effect on navigation performance," in Ion Gnss, 2005, pp. 967–978.

[6] A. R. Jimenez, F. Seco, C. Prieto, and J. Guevara, "A comparison of pedestrian dead-reckoning algorithms using a low-cost mems imu," in Intelligent Signal Processing, 2009. WISP 2009. IEEE International Symposium on. IEEE, 2009, pp. 37–42.

[7] R. Van Der Merwe and E. A. Wan, "The square-root unscented kalman filter for state and parameter-estimation," in Acoustics, Speech, and Signal Processing, 2001. Proceedings.(ICASSP'01). 2001 IEEE International Conference on, vol. 6. IEEE, 2001, pp. 3461–3464.

[8] C. Gomez, J. Oller, and J. Paradells, "Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology," Sensors, vol. 12, no. 9, 2012, pp. 11 734–11 753.

[9] B. K. Horn, "Closed-form solution of absolute orientation using unit quaternions," JOSA A, vol. 4, no. 4, 1987, pp. 629–642.

[10] I. Bylemans, M. Weyn, and M. Klepal, "Mobile phone-based displacement estimation for opportunistic localisation systems," in Mobile Ubiquitous Computing, Systems, Services and Technologies, 2009. UBICOMM'09. Third International Conference on. IEEE, 2009, pp. 113–118.

[11] MambientLab, "Metawear specifications," https://mbientlab.com/docs/MetaWearCPSv0.5.pdf, accessed: 08/01/2017.

[12] S. O. Madgwick, A. J. Harrison, and R. Vaidyanathan, "Estimation of imu and marg orientation using a gradient descent algorithm," in Rehabilitation Robotics (ICORR), 2011 IEEE International Conference on. IEEE, 2011, pp. 1–7.

 ISBN: 978-1-61208-615-6

[13] S. Madgwick, “An efficient orientation filter for inertial and inertial/magnetic sensor arrays,” Report x-io and University of Bristol (UK), vol. 25, 2010, pp. 113–118.

[14] F. Alam, Z. ZhaiHe, and H. Jia, “A comparative analysis of orientation estimation filters using mems based imu,” in Proceedings of the International Conference on Research in Science, Engineering and Technology, Dubai, UAE, 2014, pp. 21–22.

[15] S. Kumar, M. Girimondo, A. Weimerskirch, C. Paar, A. Patel, and A. S. Wander, “Embedded end-to-end wireless security with ecdh key exchange,” in Circuits and Systems, 2003 IEEE 46th Midwest Symposium on, vol. 2. IEEE, 2003, pp. 786–789.

[16] J. Molina-Gil, P. Caballero-Gil, C. Caballero-Gil, and A. Fúster-Sabater, “Analysis and implementation of the snow 3g generator used in 4g/lte systems,” in International Joint Conference SOCO’13-CISIS’13-ICEUTE’13. Springer, 2014, pp. 499–508.

[17] P. Kitsos, G. Selimis, and O. Koufopavlou, “High performance asic implementation of the snow 3g stream cipher,” IFIP/IEEE VLSI-SOC, 2008, pp. 13–15.

[18] G. Orhanou, S. El Hajji, and Y. Bentaleb, “Snow 3g stream cipher operation and complexity study,” Contemporary Engineering Sciences-Hikari Ltd, vol. 3, no. 3, 2010, pp. 97–111.

[19] Z. Liu, P. Longa, G. Pereira, O. Reparaz, and H. Seo, “Fourq on embedded devices with strong countermeasures against side-channel attacks,” Cryptology ePrint Archive, Report 2017/434, 2017. 28, 29, Tech. Rep.

[20] M. Brown, D. Hankerson, J. López, and A. Menezes, “Software implementation of the nist elliptic curves over prime fields,” Topics in Cryptology—CT-RSA 2001, 2001, pp. 250–265.

[21] D. J. Bernstein, “Curve25519: new diffie-hellman speed records,” in International Workshop on Public Key Cryptography. Springer, 2006, pp. 207–228.

 ISBN: 978-1-61208-615-6