Fuzzy-Logic-Based Application to Combat Gender Violence

José Á. Concepción-Sánchez, Pino Caballero-Gil, Jezabel Molina-Gil

Department of Computer Engineering and Systems, University of La Laguna,
La Laguna, 38206, Tenerife, Spain
E-mail: {jaconcep, pcaballe, jmmolina}@ull.edu.es

Abstract

Gender violence is one of the most serious and widespread problems in our society. In dangerous cases, the use of special devices for GPS tracing is recommended in some countries. However, these devices are used only in extreme cases and have many drawbacks. This work describes a new system to combat gender violence that tries to improve the existing system. It combines different location schemes based on distinct technologies to determine the distance between victim and aggressor. Besides, the application is enriched with a fuzzy-logic-based approach as a way to avoid false alarms. If an offender gets close to a victim, even if the established set distance has not been broken yet, the victim is warned thanks to the application. Moreover, if the fuzzy logic based approach confirms that the pre-set distance has been broken, an automatic streaming of a real-time video starts to be sent to the police, and some stored contacts are warned so that they can try to protect the victim until the police arrive. A beta-version has been implemented and the obtained results are promising.

Keywords: Security, Fuzzy Logic, Mobile Application, Gender Violence

1. Introduction

Nowadays, one of the most difficult problems affecting society is gender violence. This claim is supported by many statistical data, such as, for example, the fact that, in Spain in 2015 the gender violence rate was 1.3 per thousand women aged 14 or over, increasing two percent more than the previous year[1]. Similar data can be found for many other countries so it is clear that today's solutions to this problem are not being effective.

This work proposes a set of mobile and web applications to help people who suffer this problem by providing them prompt and proven information. In order to reach this purpose, the mobile application installed on the victim's smartphone sends continuously its position to the server so that the server can check whether the set distance has not been broken. If the set distance has not been respected, the system uses fuzzy logic[2] to determine if the warning is true or false. This latter mechanism is helpful because it is possible that the location system returns incorrect values. If the fuzzy logic mechanism concludes that the warning is true, the system will not only notify the victim but also will send this information to the chosen contact numbers and to the control centre. Throughout the paper, these operation and functionalities are described in more depth.

This work is structured as follows. Section 2 mentions several related works. Section 3 describes the operations of the proposed Android and web applications. Section 4 explains the used technologies and the architecture of the system, while Section 5 describes the used fuzzy-logic-based approach. Finally, a brief conclusion closes the paper.

2. Related Works

In Europe, each country has its own initiatives to tackle the serious problem of gender violence. For example, in Germany, where approximately 100,000 women suffer gender violence[3] nowadays, the Government has adopted two measures[4]. On the one hand, they focused on prevention and legislation, based on cooperation among institutions as well as nationwide networking of assistance services. On the other hand, the second Federal Government's action plan focused on deficiencies that had been unveiled in a comprehensive study of health, well-being and personal safety of women.

Other countries, like Portugal, France or Spain[5], decided to introduce a monitoring device that allows controlling that the aggressor does not approach the victim. This system consists in a system based on a GPS monitoring device in the form of a bracelet worn by the aggressor[6] [7], either on the wrist or ankle, and a device carried by the victim, which notifies them and a police station in case the aggressor has breached the set distance[8].

According to its definition, this system provides up-to-date and permanent information on incidents that affect compliance or non-compliance, with measures or penalties, as well as possible incidents, whether accidental or caused, in the operation of the monitoring elements, with three basic consequences: to make effective a restricting order, to document the possible breach of the measure of restricting order, and to dissuade the aggressor.

Regarding the features of the system, the devices carried by an aggressor can be only associated to one victim, and it is recommended that the minimum pre-set distance is 500 meters. This can be a disadvantage, since in small towns or villages, 500 meters radius can be very easy to break as they can live relatively close to each other so, as a consequence, false alarms can arise that affect their day-to-day. In order to overcome this problem, the system proposed here combines different location systems and fuzzy logic for more effective decision-making. In fact, the idea of using fuzzy aggregation in trust models has been proposed by several authors [9] [10].

In addition, many victims refuse to use the current system because they are forced to wear, in their day-to-day life, a device that does not go unnoticed as people around them become aware of the situation they are suffering.

This work aims not only at preventing unwanted situations between victims and aggressors, but also in conveying a sense of security to victims in their everyday life, so that they can go outside without being worried that their aggressors can appear suddenly. The proposed system is continuously checking the distance between them. If it gets shorter and it is determined by fuzzy logic that the alarm is real, a danger notification is sent to the victim, the emergency services and a list of contacts.

Due to the fact that most people have smartphones, we propose a mobile-based system in charge of checking if the aggressor is close to the victim. Thus, the cost of this system is lower than that of other proposals[11] [12]. Besides, victims do not have to worry about carrying any other device. With only the victim's smartphone, and a Bluetooth bracelet with GPS for the aggressor, we can have the system running, since the data connection for sending streaming video that exists today (4G) allows the operation of the proposed system.

3. System Operation

In this section, the operations of the mobile application and the web application are described.

3.1. Android Application

The proposed mobile application[13] in the smartphones of the victims has two main features.

On the one hand, the use of Bluetooth Low Energy (BLE) [14] and Global Positioning System (GPS) allows detecting the presence of the aggressor. On the other hand, the use of Long Term Evolution (LTE)[15] allows sending streaming of a real-time video to the police.

The mobile application described in this work has been developed for the Android operating system, but it is possible to develop it for iOS and Windows Phone. It uses different location systems to check that the aggressor is not close to the victim. To make this possible, the mobile application running in the victim's smartphone is continuously sending the victim's position to the server, and the bracelet of the aggressor is sending the aggressor's location too. When the server receives this information, it calculates the distance between victim and aggressor. If the distance is close enough, it takes into consideration a fuzzy logic approach to determine if the alarm is really true, and in this case it notifies the control centre and the victim.

In addition, BLE will also be making searches from the mobile application. Therefore, victims will be safe if they enter a closed space where no GPS-based location system can function properly. Hence, when the aggressor is detected near the victim, the application can notify the victim with one of the following two notifications, which also include the vibration and sound functionalities.

- Warning level (caution): The aggressor is detected in the vicinity of the victim thanks to the calculation that the server has done through the positions of the victim and aggressor. In this case, the victims will receive a push notification informing them about the incident, as well as the control centre, so that they can contact the aggressor.
- High level (hazard): The server has detected that the aggressor has exceeded the limit distance or the BLE itself has detected it.

In the high level of hazard warning, besides notifying the victim and the control centre, the application will start a video recording that will be sent in real time using 4G mobile or Wi-Fi technologies to the receiver station of the police. If the victim does not have her smartphone at hand, the audio of the video can still be used by the control centre to analyse the situation and proceed accordingly.

Regarding video recording and sending to the server in live when the aggressor exceeds the limit distance, victims are also able to activate it by only pushing on a button. Thus, whenever they want to notify an incident, they will be able to do so. In addition, when the aggressor is detected via BLE, the video recording starts automatically, without the need for the mobile to be unlocked or the application to be in the foreground. To allow this, *libstreaming* library[16] was modified to start a video recording on Android without the need to have a video preview.

Another feature of the application, is that if the Bluetooth is turned off on the device, a push notification will notify the victim, as this will not allow the application to function in short distances. This means that the victim will not know in closed spaces when there is not GPS coverage if the aggressor is getting closer. Besides, this warning cannot be removed from the Android notification until Bluetooth is activated. Also, the application will notify it to the control centre so that the police can contact the victim and warn her in case of danger. Likewise, we have another similar notification for when the victim's mobile device fails to obtain its location. Thus, victims will be always informed.

Finally, to close the application, the Android back button functionality has been modified so that the application stays running in the background while victims use the smartphone or block it. If victims wish to close the application, they will have to do it from the menu, and accept a dialogue that informs them that they will be in danger if the aggressors are near because they will not be detected by the application. As in the previous case, if the victim is closing the application, before closing it, a notification is send to the control centre.

3.2. Web Application

The web application[17] is used by the control centre, which is in charge of managing all the incidents sent from the mobile applications of the victims. This application is divided into three parts.

First, the *Live* tab is where all the videos that are being sent from mobile applications are played. Along with the videos, the police will be able to access the victim's contact information, their GPS position or the distance with the aggressor for instance. If there is more than one live broadcast, the interface is progressively adapted so that the police can see all the content. Then, if they want to make special emphasis on one in particular, just with one click, they have access to that particular content.

Second, a history of incidents is recorded with all types of received notifications. Within these notifications are all the connections that have been made with the control centre from the mobile application, like low battery notifications, disabled Bluetooth or

GPS, or when application has been closed either by the application itself or because the mobile run out of battery. Thus, the police can manage all the incidents and contact the victims if necessary. In addition, if the web application detects that the aggressor is close to the victim, it shows a notification to the control centre, informing the police that the aggressor is approaching the victim so that they can contact and notify the aggressor. For that, the web application performs the tasks of calculating distances between victim and aggressor. If the result of the distance is an estimated alarm, through a fuzzy logic approach it is checked whether it is true or not.

Third, the control centre also registers all the devices that have been used, thus keeping the date of the last connection. To distinguish the devices stored in the database, we use MAC address, with which we also generate the video links where the control centre has to access to obtain the video and play it. In addition, we have decided to save the devices that have been using the system so that we do not have to send to the control centre the link of the video every time the streaming video is sent from the mobile application. In this way, the mobile application only notifies that the video is available or not when it starts sending it and when it ends, so that the web application only has to enable or disable the link.

Finally, the web application has also a tab where all the related information can be found. Thus, from the control centre, the police will be able to monitor locations of victims and aggressors, the alerts that may have arisen, and also thanks to the streaming video, they will also have the possibility to see or hear what is happening of what has happened.

4. System Architecture

The used communication scheme shown in Fig. 1 is composed of the three elements: Smartphones, Wowza Server and Web application. As can be seen there, different flows of the system are differentiated with colours.

First, yellow arrows indicate video streaming sent from the victims' mobile applications to the server. These videos can be activated automatically once the BLE detects the aggressor or if the victim wants to notify something to the control centre. The mobile starts sending streaming video to the Wowza server while the mobile application also notifies the web application that the video is being sent (blue arrow), so that it can connect to the Wowza server and get the video to play it. Besides, with this notification, the victim's contact information (name, phone number and location) is also sent so that the police can get in touch if necessary. Finally, when the video playback is finished, the application stops sending the video to the Wowza server and notifies to the web application that the transmission has ended.

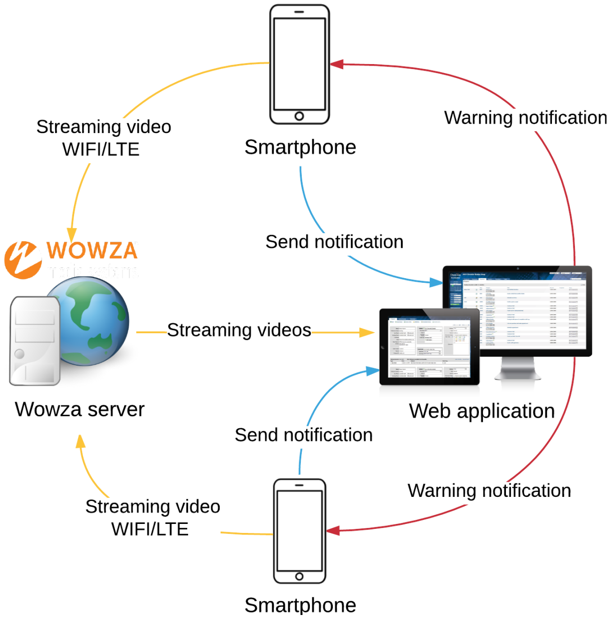


Fig. 1. Communication scheme

Second, it is not only when the video is streamed that the application notifies the server. There are also two other circumstances in which notifications are sent (blue arrow): on the one hand, when the phone is running with low battery or it cannot get the current position for a while. It is required to monitor the victim's device to have total control of the situations; and on the other hand, when the application is to be closed on the mobile device or when the mobile phone is turned off. To the previous notifications, it has been also added the current position that is sent periodically so that the server can calculate the distance between victim and aggressor.

Third, the red arrows indicate the notifications sent from the web application to the mobile application in case the server detects the aggressor close to the victim. Note that the distance for this notification could be configurable in each case.

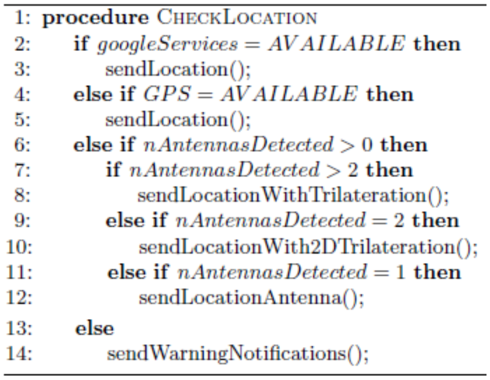
In addition, the protocols RTMP and RTSP, which are responsible for establishing the connection and the reception of video through streaming respectively, are used for sending the video in streaming. In terms of security, both protocols are safe since they use security mechanisms for Transport Layer and within the protocol. Due to this the encryption of the video, sent by streaming, is not necessary since the protocols themselves take care of it.

5. Fuzzy-Based Location

Location systems that use only GPS can fail because in some cases such as GPS initialization or GPS synchronisation, it is possible that the system returns incorrect values. Thus, making decisions only based on GPS information is not recommended in this application because that approach is susceptible of many errors. This proposal analyses the received pieces of information in order to determine whether the received information is similar enough to get the real position. Such decisions take into account possible inaccuracies or approximations regarding space and time data to define an event. Therefore, our proposal for applying fuzzy logic is focused especially on the description of the decision criteria of the user application position. In this section, the operation of the fuzzy-logic-based approach to determine the location is described in detail.

5.1. Deterministic Approach

The proper operation of this proposal is mainly based on the location, for this reason, the location of victims and aggressors is a fundamental parameter. As we mentioned before, the system is based on two measurements, GPS location and Google service information to determine proximity between them. As we can see in Fig. 2, the algorithm has a series of IF-ELSE IF conditions where it is checked if both locations are available. The proposal has into account the values from greater to lesser precision and finally picks the best option. In addition to the position obtained with some of these systems, BLE will be verified to detect the aggressor in the vicinity, thus avoiding that the victims are unprotected if they are inside an area without coverage (see Fig. 2).



```
procedure CheckLocation
    if $googleServices = AVAILABLE$ then
        sendLocation();
    else if $GPS = AVAILABLE$ then
        sendLocation();
    else if $nAntennasDetected > 0$ then
        if $nAntennasDetected > 2$ then
            sendLocationWithTrilateration();
        else if $nAntennasDetected = 2$ then
            sendLocationWith2DTrilateration();
        else if $nAntennasDetected = 1$ then
            sendLocationAntenna();
    else
        sendWarningNotifications();
```

Fig. 2. Location algorithm

The location system operation works as follows:

First, the mobile app will try to use Google's highly accurate services to get the location (latitude and longitude) of the victim. This positioning system is most accurate one because it not only uses the GPS but also the data and Wi-Fi signals that can be found around. It system provides a low margin of error in the location of the device.

Secondly, in case Google services are not available, the mobile application will attempt to obtain the location of the victim using GPS.

As third option, we have the trilateration, which is intended in case both Google services and GPS cannot obtain a location, which could happen in closed environments such as buildings. To obtain the location through this mechanism, it will be needed to obtain the signals from the coverage antennas closest to the victim's device. To do this, it is used a series of libraries that Android provides. Once detected the antennas closest to the victim, we proceed to calculate, using the intensity of the signal and the location of each of them, the location of the victim. To obtain the location through the trilateration we will need to detect at least three antennas to obtain a reliable location. For the two other possible cases, when two or one antenna is detected, we choose the intermediate point between the two antennas or the location of the antenna respectively.

Then, once the location of the victim is obtained, it is sent it to the server so that together with the location of the aggressor, it can calculate the distance to which they are. For this, we make use of the Haversine's formula, whose mathematical expression is shown in Fig. 3, where:

- *R*: Earth's radius.
- *lat1* and *lat2*: Latitude of the coordinates of victim and aggressor.
- *long1* and *long2*: Longitude of the coordinates of victim and aggressor.

$$a = \sin^2\left(\frac{lat2 - lat1}{2}\right) + \cos(lat1) * \cos(lat2) * \sin^2\left(\frac{long2 - long1}{2}\right)$$
$$c = 2 * \tan^{-1}(\sqrt{a}, \sqrt{(1-a)})$$
$$d = R * c$$

Fig. 3. Haversine's formula

Thus, once established the distance between victim and aggressor, the server will be forced to make a decision depending on the results obtained. In case the result is that the aggressor is close to the victim, the server will use fuzzy logic to determine if it is really a true alarm.

Also BLE will be checking, on the mobile application, that the aggressor is not detected. For this, we use the algorithm shown in Fig. 4.

```
procedure CheckLocation Ble
    if $stateBle = UNABLED$ then
        sendWarningNotifications();
    else if $stateBle = ENABLED$ AND $check() = aggressorDetected$ then
        sendNotifications();
        sendVideoStreaming();
        sendSmsToContacts();
    else
        noDanger;
```

Fig. 4. Detection algorithm using BLE

To do this, the signal strength between the two devices is used so that if the aggressor's bracelet is not detected, it means that he is not in the closest radius of the victim. Otherwise, if the aggressor's device is detected, the signal strength received by the victim's application is transformed into meters by the mathematical formula:

$$10^{(PX-rssi)/(10*df)} \tag{1}$$

where:

- *px*: Signal strength value between the two devices at 1-meter distance (smartphone of the victim and bracelet of the aggressor).
- *rssi*: Current signal intensity between the two devices. Mobile application gets the signal intensity.
- *df*: Constant value computed from average.

The detection via BLE of the aggressor is deterministic, since we only need to detect the signal of the device to know that the alarm is true, so in this case, the system does not use fuzzy logic to determine if the alarm is real.

Finally, note that if the aggressor were detected with BLE, the danger level would be automatically activated and, therefore, the streaming video would automatically start and the application notifies the victim, the contacts and to the control centre. This is because BLE is a short-range technology, which would mean that, in this case, the aggressor is already very close to the victim.

5.2. Fuzzy-Logic-Based Approach

In the process of initializing GPS or Google's own services of maximum precision, while trying to get the exact location, the mobile application can return erroneous location values. This can happen when victims leave a place where they did not have coverage previously. That is why the localization system cannot be deterministic, since then the system could not control these cases. To avoid this false alarm, we have decided to use fuzzy logic[2], which will allow the web application to decide if the alarm is true or not.

To do this, if the application detects a possible alarm with a packet, the following ones packets will be sent quickly from the devices to be able to compare the initial packet with the following ones using fuzzy logic and determine if it is really an alarm.

In this way, two linguistic variables[18] are used to compare the packets. These linguistic variables are denoted as Space-Difference (SD) and Time-Difference (TD). On the one hand, SD measures the difference between the current distance between victim and aggressor, and the distance that triggered the alarm. TD, for its part, measures the difference between the current time and the time indicated for the received alarm. Fig. 5 shows the graph where the values taken by the different membership functions[18] are represented.

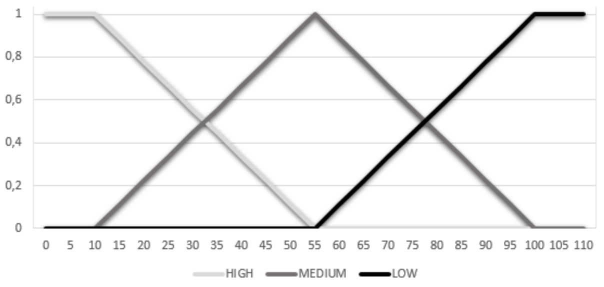


Fig. 5. Fuzzification functions of SD and TD

Both linguistic variables represent the influence taking into account that the X coordinate represents respectively SD in meters and TD in seconds, and the Y coordinate is the probability corresponding to the following linguistic terms:

- *High*: This linguistic term takes its maximum probability value when SD and TD are between values equal to or less than 10 meters or seconds. We have established these values because we consider that a packet within the time interval or with such a close distance is a clear indication that the alarm is real. From 10 meters or seconds, the probability of this linguistic term will decrease.
- *Medium*: This gets its maximum probability when SD or TD are equals to 55, increasing and decreasing its probability before and after this value. This linguistic term has been introduced between the other two because that way the system achieves a greater capacity of decision making.
- *Low*: It indicates that the possibility to confirm the alarm is low, but it does not discard it. For this, this linguistic term obtains its greater probability to the 100 meters or seconds, since it is considered that, with a difference of so many seconds o meters, the packet might not belong to the alarm.

Each linguistic term is described by a membership function that associates the actual input value of the influence factor with a degree of membership corresponding to the linguistic term described by the function. These membership functions[18] are as shown in Fig. 6. Thus, the output of the function for an SD of about 30 meters will be classified at the same time as HIGH and MEDIUM with a degree of 0.56 and 0.44 respectively. The same is considered in TD in seconds, considering that in general the same alarm can be detected for at least 10 seconds and that from the second 100 could be a different alarm.

$$f_{HIGH}(x) = \begin{cases} 1, & x \leq 10 \\ \dfrac{55 - x}{55 - 10}, & 10 < x \leq 55 \\ 0, & x > 55 \end{cases}$$

$$f_{MEDIUM}(x) = \begin{cases} 0, & x \leq 10 \\ \dfrac{x - 10}{55 - 10}, & 10 < x \leq 55 \\ \dfrac{100 - x}{100 - 55}, & 55 < x \leq 100 \\ 0, & x > 100 \end{cases}$$

$$f_{LOW}(x) = \begin{cases} 0, & x \leq 55 \\ \dfrac{X - 55}{100 - 55}, & 55 < x < 100 \\ 1, & x \geq 100 \end{cases}$$

Fig. 6. Membership functions

The next step after fusifying is the formulation of specific rules to express the combination of influences. As an example, a possible simple structure of such fuzzy logic rules would be as in Fig. 7, where REAL_ALARM is a linguistic variable defined by two linguistic terms, YES and NO. These linguistic terms are associated with their respective membership functions, where the output will depend what linguistic term has the maximum probability using the max-membership defuzzification method.

```
if $(SD = HIGH)$ OR $((SD = MEDIUM)$ AND $(TD = MEDIUM))$ then
    REAL_ALARM is YES ;
```

Fig. 7. Fuzzy rules

There may be more than one value assignment rule for the aggregation decision. In this case, the assignments to the aggregation decision are combined by an implicit AND, so the probability corresponding to the aggregation decision corresponds to the minimum value between the SD and TD input probabilities.

In an illustrative example, SD is 40 meters and is fused as HIGH with degree 0,33 and as MEDIUM with grade 0.67, and for the same pair of packets TD is 60 seconds and it is fused as MEDIUM with grade 0.89 and as LOW with grade 0.11. The result will be YES with grade 0.67 and NO with degree of 0.33. Since YES has the highest probability, the package would be added, because the system concludes that the alarm is true. In Table 1, other possible cases are evaluated. While rows 1 and 2 return that the alarm is true, the output in the third row is false because of there is a high SD in a short TD.

Table 1. Example input cases with their outputs

INPUT SD	INPUT TD	FINAL OUTPUT
50	30	ALARM is TRUE
15	5	ALARM is TRUE
200	5	ALARM is FALSE

6. Conclusions

The measures taken till now to combat gender violence are not having the desired effect, as their use has hardly been extended due to several drawbacks. This work describes the implementation of a new alert system to protect the people who suffer this problem. The main goal of this work is to make the victim feel safer because the proposed application guarantees that if the offender gets close to the victim, even if the set distance has not been broken yet, the victim is warned so that protection measures can be taken. If the set distance is broken and fuzzy logic determines that the alarm is true, an automatic streaming of a recording in real time is sent to the police while a list of stored contacts are warned.

This is part of a work in progress where new improvements are being developed. For instance, incident information shown in the control centre is being organized so that the police in charge of carrying out the task of monitoring the web application, can focus better on this task. Besides, the mobile application is being developed for the other mobile operating systems iOS and Windows Phone, so that the system can be accessible to all victims, independently of the operating system of their smartphones.

7. Acknowledgments

Research supported 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. Estadística de Violencia Doméstica y Violencia de Género Año 2015, http://www.ine.es/prensa/np972.pdf (accessed on 17 July 2016)
2. L.A.Zadeh. Fuzzy Set. Information and Control. 8(3): 338-353. 1965.
3. Domestic violence affects over 100,000 women in Germany, http://www.dw.com/en/domestic-violence-affects-over-100000-women-in-germany/a-36482282 (accessed on 12 December 2016)
4. Citizens' rights and constitutional affairs, http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/510025/IPOL_IDA(2015)510025_EN.pdf (accessed on 11 November 2016)
5. A.G. Lorea. The efficacy of electronic monitoring in gender violence: criminological analysis, http://www.ehu.eus/ojs/index.php/inecs/article/view/17240/15020 (accessed on 20 November 2016)
6. M. Ellsberg, D.J. Arango, M. Morton, F. Gennari, S. Kiplesund, M. Contreras and C. Watts. Prevention of violence against women and girls: what does the evidence say? The Lancet, 385(9977) (2015) 1555-1566.
7. D. Whitfield. The Magic Bracelet: technology and offender supervision. Waterside Press (2001).
8. España, protocolo de actuación, http://www.violencia genero.msssi.gob.es (accessed on 9 May 2016)
9. K.M. Lee, K. Hwang, J.H. Lee and H.J. Kim. A Fuzzy Trust Model Using Multiple Evaluation Criteria. Fuzzy Systems and Knowledge Discovery. Lecture Notes in Computer Science, vol 4223. Springer (2006).
10. C. Castelfranchi and R. Falcone. Trust is much more than subjective probability: mental components and sources of trust, Annual Hawaii International Conference on System Sciences, vol.1 (2000) 10.
11. D. Chand, S. Nayak, K.S. Bhat, S. Parikh, Y. Singh and A.A. Kamath, A mobile application for Women's Safety. IEEE Region 10 Conference (2015) 1-5.
12. D.G.Monisha, M. Monisha, G. Pavithra and R. Subhashini. Women Safety Device and Application-FEMME. Indian Journal of Science and Technology, 9(10) (2016)
13. Proposed mobile application, https://github.com/alu0100697414/MobileApp (accessed on 14 April 2017).
14. C.Gomez, J. Oller and J. Paradells. Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. Sensors, 12(9) (2012) 11734-11753.
15. B.Furht and S.A. Ahson. Long Term Evolution: 3GPP LTE radio and cellular technology. Crc Press (2016).
16. Libstreaming library, https://github.com/fyhertz/lib streaming (accessed on 4 May 2016).
17. Proposed web application, https://github.com/alu0100697414/WebApp (accessed on 14 April 2017).
18. L.A. Zadeh. The concept of a linguistic variable and its application to approximate reasoning. Information Sciences. Part I,II,III, 8,8,9: 199-249.301-357,43-80. 1975.