Journal of Reliable Intelligent Environments
https://doi.org/10.1007/s40860-024-00227-x

ORIGINAL ARTICLE

Secure electronic monitoring of sex offenders

Francesco Buccafurri[1] · Vincenzo De Angelis[2] · Maria Francesca Idone[1] · Cecilia Labrini[1]

Received: 16 April 2024 / Accepted: 2 July 2024

Abstract

Electronic monitoring is a viable approach to controlling sex offenders and making the environment safe for victims. Two technologies are currently being adopted: RFID and GPS. Both technologies aim to detect the proximity between the offender and the victim and alert the relevant authorities in real time. However, the security of the system adopted is a key issue, given the risk to the victim's safety. In this paper, we analyze the existing approaches from the perspective of security, in case of possible misbehavior of the offender. The theoretical analysis shows that GPS is the best choice when high security requirements are desired. In fact, radio frequency attacks are possible for RFID, endangering the victim. However, when GPS is adopted, privacy issues become critical. In particular, when considering a victim moving around the territory, it is unacceptable to track them even with the goal of offering protection. To overcome this drawback, we propose a GPS-based solution that does not allow the victim's location to be revealed unless the offender is nearby, thus finding a solution that advances the state of the art.

Keywords Electronic monitoring · Privacy · GPS · Crime fighting

1 Introduction

In recent years, due to the increasing number of crimes committed and prison overcrowding, many efforts have been made to identify appropriate legal measures to address the above problems. In the case of crimes in which the safety of a victim is threatened by a sex offender, if for the offender imprisonment is not applied, alternative measures are applied, such as restraining orders. According to a restraining order, the sex offender cannot get closer to the victim (or areas of potential victims) beyond a given distance.

These alternative measures can profitably exploit technology [1, 2] in order to make the environment safe for the victim. In particular, electronic monitoring (EM) is used to monitor the movements of the offender according to the order issued by the court, thanks to the use of a device worn by the offender (and the victim) [3]. Obviously, the use of a monitoring tool leads to great advantages [4–6], as the police can constantly check whether the offender is complying with the restraining order imposed by law.

Two different types of restrictions can be imposed: *inclusion* or *exclusion* zones. An inclusion-zone order defines the area in which the offender must be located. For example, this order may be applied in combination with the house arrest measure. Exclusion zones define the zones in which the offender should not enter. A typical exclusion zone is the victim's home. We refer, in cases like this, to *static* exclusion zones. There can also be a *dynamic* exclusion zone when the restraining order prohibits the offender from approaching the victim beyond a certain distance.

Observe that, in the context of location tracking technologies, we refer to the two main technologies, namely Radio Frequency (RF) [7] and Global Positioning System (GPS) [8]. They can also be used in combination. In both cases, mon-

Francesco Buccafurri, Vincenzo De Angelis, Maria Francesca Idone and Cecilia Labrini contributed equally to this work.

✉ Francesco Buccafurri
bucca@unirc.it

Vincenzo De Angelis
vincenzo.deangelis@dimes.unical.it

Maria Francesca Idone
mariafrancesca.idone@unirc.it

Cecilia Labrini
cecilia.labrini@unirc.it

[1] Department DIIES, University Mediterranea of Reggio Calabria, Via dell'Universitá 25, 89122 Reggio Calabria, Italy

[2] Department DIMES, University of Calabria, Via P.Bucci, 87036 Arcavacata di Rende, Cosenza, Italy

Published online: 11 July 2024

itoring is under observation by the law enforcement agency (LEA). This means that the LEA can verify that the offender complies with the area indicated by the restraining order.

However, the security of the system adopted is a key issue, given the risk to the victim's safety. Only if the victim can rely on a reliable EM system, they can effectively lead a life free from the compression of their basic rights. Apart from hardware or software failures, which are beyond the scope of this paper, the EM system can be considered reliable in a broad sense if the functional requirements are achieved even in the case of of dishonest offender's behavior.

In this paper, we analyze EM from the perspective of security, identifying a gap in existing techniques in the case of of dynamic exclusion zones, which is the most critical case from the point of view of victim privacy.

The general analysis is done by defining a theoretical framework (see Sects. 3 and 4) in which functional, security, and privacy requirements are jointly considered. From the analysis, it emerges that for all types of EM but in the case of dynamic exclusion zones, current approaches are appropriate. In contrast, for dynamic exclusion zones, functional requirements would be securely achieved only with GPS-based approaches. However, unlike the case of static exclusion zones, serious privacy problems arise regarding the victim. Indeed, the traditional GPS-based approaches require tracking their movements to detect proximity with the offender. This is unacceptable from the point of view of privacy.

The fact that GPS should be used for dynamic exclusion zones but cannot be used for privacy reasons is a shortcoming of current systems that we want to overcome in this paper. Indeed, we propose a privacy-preserving GPS-based solution that does not allow the victim's location to be revealed unless the offender is nearby, thus finding a solution that advances the state of the art.

The structure of the paper is the following. In Sects. 2, we describe the literature related to our work. Some basic notions useful for the comprehension of the paper are given in Sect. 3 in which we highlight several security requirements according to the different technologies used for electronic monitoring. Then, given these notions, in Sect. 4, we compare RF and GPS-based approaches under the security and privacy lens. In Sect. 5, we describe our electronic Monitoring system of Sex Offenders overcoming the privacy issues related to the victim. The security of the solution is analyzed in Sect. 6. In Sect. 7, we consider implementation issues for real-world adoption. Finally, in Sect. 8, we draw our conclusions.

2 Related work

In recent years, the increase in cases of domestic violence or stalking has led to finding new strategies to protect victims. Among the various adopted measures, many states have approved the use of electronic monitoring (EM) technologies to supervise sex offenders. Electronic monitoring is a term that refers to various location control technologies that allow the management of offenders or prisoners awaiting trial [9]. Indeed, EM has always been used primarily to remove criminals from detention, either as an alternative to incarceration or a means of post-release supervision.

The use of technology to supervise is not new. It is in the US that this practice has been initiated [10]. In [11], the authors show the evolution of electronic offender-tracking systems, whose origin dates back to the 1960s, thanks to the study conducted by Ralph Kirkland Gable and William S. Hurd at the University of Harvard [12]. In the mid-1960s, early technologies were tested on groups of parolees, released mentally ill patients, and research volunteers. However, these devices were large, difficult to hide, and impractical to wear on a daily basis [13]. In 1987, about 900 people participated in nationwide electronic monitoring programs in more than US 21 states [14]. In 1998, that number increased to over 95,000 [15]. By the end of the 2000s, EM was being used for violent offenders [16]. In 2006, 22 states passed legislation requiring or authorizing the use of Global Positioning Satellite (GPS) technology to track sex offenders. In 2009, there were more than 200,000 GPS and radio frequency (RF) monitoring devices in use across the United States and the State court system [17].

Europe has also accumulated a body of experience in the field of EM of sex offenders [18–21]. For an overview of EM use around the world, see [3].

Wearable devices are typically used to track people, especially in the context of e-health [22–24]. In the context of Electronic Monitoring of sex offenders, two technologies are currently being used, namely Radio Frequency (RF) systems and Global Positioning Systems (GPS) systems. The latter, from a qualitative analysis conducted by the authors of [25], has shown to be more effective. In this paper, we provide a formal validation of the above claim.

RF-based technology allows checking if an offender is located in a specific place (typically the offender's home) through signals at a reasonable frequency. Differently, GPS-based systems allow the collection of the actual location data of offenders thanks to a device worn by the offender. This way, the monitoring center can in real-time track the movements of the offender.

In the literature, GPS technology is used in three different ways: *active GPS tracking*, *passive GPS tracking*, and *hybrid systems*. Active systems are those systems that transmit real-time information about the offender's location to an almost real-time monitoring center. Differently, passive systems collect location information at a specific time interval and are sent in an aggregated way to the monitoring center. Finally, hybrid systems combine both passive and active monitoring capabilities, where data is sent after a longer interval of time with respect to the active system.

The current technologies aim to allow an alternative to imprisonment, reduce non-compliance and violations of supervisory conditions, assist offenders in reintegration into society, prevent future and repeated sexual offenses by convicted offenders, and increase public safety. The EM technology used today has greatly improved compared to the past and allows for an increasingly sophisticated use as a tool for the management, punishment, and public protection of the offender. Furthermore, current devices are generally smaller and can be hidden. However, there are still limitations [26]. A first limitation is represented by the battery life that some providers have tried to solve by developing a portable charging pack that can be clipped onto the electronic anklet. A problem that has not yet found a solution is that of jammers that can be used to block or interfere with both the RF and the GPS signals. Although it could be possible to identify when a jammer was used, there is a risk that a crime will be committed before the jammer is identified, or that the offender has escaped at that time. In addition, even the hardware can be damaged or removed, although there are mechanisms that allow notifying the competent authority in the event of tampering. This does not prevent offenders who have successfully removed their label from offending or fleeing.

In the context of Electronic Monitoring of sex offenders, a new problem has emerged. The offender is strictly prohibited from approaching the places usually frequented by the victim. If the offender approaches the victim or the pawn in places where there is no prohibition, the electronic bracelet would be of no use. The device is used exclusively to monitor the movements of an individual within one or more predefined places, generating an alarm only when the offender accesses the areas that are excluded. Therefore, some countries, such as Spain and Italy [27, 28], are adopting a new approach based on *proximity tracking*, and it is the scenario in which the victim is also equipped with an electronic bracelet to detect the presence of the offender in the immediate proximity. As a matter of fact, the above problem can be related to the issue of *proximity-based services*, in which the proximity of two users or the proximity of a user to a given target should be detected in order to provide a given service [29–36].

Our paper focuses on this kind of monitoring, which we call *dynamic exclusion zones*, as the exclusion zone is virtually defined as an interdiction zone around the victim, thus moving with them. We improve the state of the art by enabling GPS in this kind of monitoring yet preserving the privacy of the victim. This way, we obtain the increased robustness of the GPS solution with respect to the RFID, without paying the intolerable price of continuous victim tracking.

3 Background, threat model, and research questions

Electronic Monitoring is a tool widely used for more than a decade to enforce restrictions on the movements of offenders, according to the order of a court. The order may regard *inclusion* or *exclusion* zones. When an inclusion zone is imposed on the offender, they are enforced not to leave this zone. In the case of exclusion zones, the offender is not allowed to enter these zones. Examples of restrictions of the first type are the house arrest measure, or the restriction limiting the movements of the offender within the area of a given city. Examples of the second type are the denial for the offender to approach certain places, such as schools or sport-clubs for pedophiles, or to approach the house of the victim (and other places attended by them too) for general sex offenders. In the latter case, also the denial to approach the victim, independently of the place in which they are placed, is also possible.

Therefore, we can identify three different *security requirements*, which we denote as:

1. **SIZ**: inclusion zones, which are necessarily static;
2. **SEZ**: static exclusion zones;
3. **DEZ**: dynamic exclusion zones.

The technologies used to implement EM are basically two (possibly used in combination):

- **Radio frequency (RF)** The offender is equipped with a tamper-proof tag worn on an arm or on an ankle, which plays as a radio frequency transmitter. The tag is active and the signal has an action range of the magnitude of 100 ms.
- **Global positioning system (GPS)** GPS is the geostationary satellite system allowing GPS devices to detect continuously the position coordinates and, thanks to an on-board SIM card, to communicate them to a server. In this case, the GPS device is a tamper-proof tag worn on an arm or on an ankle of the offender. The coordinates are sent to the provider of the service, which we assume to be a telephone service provider (TSP)—as it happens in Italy, and/or the law enforcement agency (LEA).

Let us see how the two technologies can be used to achieve the above security requirements. For each security requirement, we consider the two technologies.

- **SIZ** (static inclusion zones)
  - **SIZ with adoption of RF**. In the case of RF, the inclusion zones should be tagged with non-tamperable and non-removable RF receivers equipped with a SIM

card. The restriction imposed on the offender is verified if the signal is received. In the absence of a signal, the restriction is considered violated. RF is suitable for SIZ only for limited areas. In practice, this system is adopted for house arrests.
  - **SIZ with adoption of GPS**. In the case of GPS, the inclusion zones are trivially identified by TSP/LEA and, then, the respect of the restriction can be checked by computing the distance between the tracked coordinates of the offender and the borders of the zones.

- **SEZ** (static exclusion zones)
  - **SEZ with adoption of RF**. In the case of RF, the exclusion zones should be tagged with non-tamperable and non-removable RF receivers equipped with a SIM card too. The restriction imposed on the offender is verified if the signal is not received. If the signal is received, then, the restriction is considered violated. RF is suitable for SEZ only for limited areas. In practice, this system is adopted to guarantee that the offender keeps far from the house of the victim or their office.
  - **SEZ with adoption of GPS**. In the case of GPS, the exclusion zones are trivially identified by TSP/LEA. Similar to the case of SIZ, the respect for the restriction can be checked by computing the distance between the tracked coordinates of the offender and the borders of the zones.

- **DEZ** (dynamic exclusion zones)
  - **DEZ with adoption of RF**. In the case of RF, the only difference with respect to SEZ, is that the receiver is a portable removable device kept by the victim.
  - **DEZ with adoption of GPS**. In the case of GPS, the system could be implemented by equipping also the victim with a GPS tracker, and, then, by continuously computing the distance between the coordinates of the victim and the coordinates of the offender. However, in most countries, a similar measure would be unacceptable from a privacy point of view [37, 38].

In the context above, we study the security issues arising from the possible malicious behavior of involved actors. Specifically, we consider the following *threat model*. We can assume that *spoofing* and *impersonation* are not possible. Therefore, messages sent by the offender can be assumed to come from the legal device and cannot be tampered with. Moreover, we can assume that the offender-side device and the RF receivers (except for DEZ) are not removable. However, we cannot assume that the offender (playing as an attacker) is not able to inhibit the transmission of the RF/GPS-coordinates messages. Indeed, a *jamming attack* [39–41] is always possible. Consider that, the absence of a GPS signal could also derive from physical obstacles (thus not from malicious behavior of the offender).

Under the above threat model, these are the possible attacks/anomalies to consider:

- RAT: an attack performed by the offender on the RF transmission;
- GAT: an attack performed by the offender on the GPS transmission;
- GFA: the case in which the GPS signal is obscured by an accidental physical obstacle.

The research problems we study in this paper is the following.

- **RQ1.** How RF and GPS can be compared in terms of security and privacy in the considered threat model?
- **RQ2.** Can we find a new solution that overcomes the state of the art?

4 RF and GPS under the security and privacy lens

In this section, we study the first research question (**RQ1**) introduced in the previous section.

We start by formalizing the security policies that should be adhered to by the electronic monitoring system. We schematize the policies by defining the following predicates.

- SI is the predicate stating that an RF signal is received by the receiver.
- GP is the predicate representing the reception of the GPS coordinates TSP/LEA-side.
- DI is the predicate stating that the tracked position of the offender is inside the inclusion zones in the case of GPS.
- DO is the predicate stating that the tracked position of the offender is outside the exclusion zones in the case of GPS.
- AL is the predicate representing the alarm state, which results in some intervention from the side of the LEA (e.g., call to the offender, call to the victim, the arrival of the police at the victim and at the offender).
- OK means that no violation is detected so that the state of the victim is assumed to be safe.

From a logical point of view (as it will be clear later), it can be realized that the closed world assumption can be adopted, so that $\neg AL$ cannot be considered in general equivalent to OK, and vice versa.

The security policies are the following. We distinguish the security policies per adopted technology (RF and GPS).

- **SIZ with RF technology**

$$\begin{aligned} \neg SI &\rightarrow AL \\ SI &\rightarrow OK \end{aligned} \tag{1}$$

Indeed, if the RF signal is not received by the receiver, then the alarm is generated because the offender is assumed to be outside the inclusion zone. Conversely, no anomaly is detected if the signal is received.

- **SEZ and DEZ with RF technology**

$$\begin{aligned} SI &\rightarrow AL \\ \neg SI &\rightarrow OK \end{aligned} \tag{2}$$

Indeed, if the RF signal is received by the receiver, then the transmitter is close to it (close to the victim, in the case of **DEZ**), thus within the exclusion zone. Therefore, the alarm is generated. Conversely, if no signal is received, the offender is assumed to be outside the exclusion zone. Therefore, no anomaly is detected.

- **SIZ with GPS technology**

$$\begin{aligned} \neg DI &\rightarrow AL \\ DI &\rightarrow OK \\ \neg GP &\rightarrow AL \end{aligned} \tag{3}$$

The first implication just states that when the GPS coordinates of the offender are received, the alarm is generated if those coordinates are not within the inclusion zone. Conversely (second implication), no alarm is generated if the detected location of the offender is within the inclusion zone. The last implication refers to the case in which the offender's device does not transmit any coordinate. In this case, the alarm is raised.

- **SEZ and DEZ with GPS technology**

$$\begin{aligned} \neg DO &\rightarrow AL \\ DO &\rightarrow OK \\ \neg GP &\rightarrow AL \end{aligned} \tag{4}$$

The first implication just states that when the GPS coordinates of the offender are received, the alarm is generated if those coordinates are within the exclusion zone. Conversely (second implication), no alarm is generated if the detected location of the offender is outside the inclusion zone. The last implication refers to the case in which the offender's device does not transmit any coordinate. In this case, the alarm is raised.

Now, we study the security of the two systems in the threat model defined in the previous section.

We can write the following implications to formalize the above attacks/anomalies.

$$\begin{aligned} RAT &\rightarrow \neg SI \\ GAT &\rightarrow \neg GP \\ GFA &\rightarrow \neg GP \end{aligned}$$

First, consider the case of RF, and, then, the RAT attack. According to (1), for **SIZ**, $\neg SI \rightarrow AL$. Then $RAT \rightarrow AL$. This is a good behavior of the model.

Instead, for **SEZ, DEZ**, from (2), we have that $\neg SI \rightarrow OK$. Then, $RAT \rightarrow OK$. This represents a serious vulnerability of the security policy in the considered threat model because the general objective of the protocol (the safety of the victim) is not reached. Indeed, the case of RAT can reasonably coincide with a physical attack of the offender on the victim.

Now, we test whether the security policies stated below in the considered threat model guarantee the safety requirement in the case of GPS.

Here, the attacker can perform a GAT attack. In this case, $GAT \rightarrow \neg GP$, but, according to (3) and (4), for all the requirements (i.e., **SIZ**, **SEZ** and **DEZ**), it holds that $\neg GP \rightarrow AL$. Therefore, $GAT \rightarrow AL$. Similar reasoning can be done in the case of GFA, and for GFA we have the same implication as GAT (i.e., $GFA \rightarrow AL$).

Therefore, the security policy is then safe, because no safety failure occurs, even though some false alarms are possible (i.e., in the case of GFA).

From the analysis above, we should conclude that, in the case of sex offenders, in which the security requirements are **SEZ** and **DEZ**, RF is not adequate and we should adopt GPS.

However, also privacy requirements should be considered. In particular, GPS can be certainly adopted for **SEZ** because the GPS coordinates of the exclusion zones are static, but for **DEZ**, it would require victim tracking, which is not acceptable from the privacy point of view and not compliant with the most legal systems [37, 42, 43].

On the other hand, **DEZ** is much more effective than **SEZ**, since it allows permanent protection of the victim, also when they move from predetermined locations (such as home and office).

As a conclusion of the analysis, we can observe that GPS is, in general, better than RF under the security lens. Conversely, when privacy is taken into account, the superiority of GPS cannot be exploited in the most challenging case (i.e., **DEZ**) because leads to intolerable privacy problems.

5 How to improve the state of the art

In this section, starting from the analysis provided in the previous section, we study the research question **RQ2**, as defined in Sect. 3. Specifically, the aim of this section is to understand how we can adopt a GPS-based solution without facing the privacy and legal issues identified earlier. Obviously, any privacy-preserving GPS-based solution can be combined with an RF solution to have a backup system, but, from a logical point of view, it does not increase the security of the electronic monitoring solution. Indeed, if the attacker is performing simultaneously RAT and GAT, RF cannot help us to distinguish the case of GAT with exclusion violation on the victim from the case of GAT without exclusion violation (that could drastically change the urgency of the police intervention). Similarly, RF cannot help us to distinguish the case of GFA with exclusion violation from the case of GFA without exclusion violation for the same reason.

As a first step, we describe a mechanism that we use for mapping the territory according to a grid-based approach. Our solution relies on this mechanism.

5.1 Grid-based approach

The solution proposed in this work is grid-based [44–46]. This requires that the territory is organized as a grid composed of *cells* of a certain shape (squares, hexagons, circles, etc.). In our approach, we consider squares cells overlapping each other covering the entire territory in which the victim and offender move. This structure is at the basis of the mechanism allowing the detection of the proximity between offender and victim at a distance less than that allowed by the restraining order.

Furthermore, since different restraining orders may require different distances, we implement a hierarchical grid organization including different levels, to allow distance modulation. Higher levels correspond to higher distances. Through this organization, the law enforcement agency may set the distance in the electronic monitoring system to be compliant with the restraining order. This is done by selecting the proper level in the hierarchy.

More formally, we design a hierarchical spatial index based on the concept of *quad tree* [47] and partially resumed in [48], in which also overlapping is enabled at each level. We call this structure *shifted quad tree* (SQT). A quad tree is a tree in which each internal node has exactly four children. It can be used to partition a 2-dimensional area into regions of different sizes. Specifically, the entire area is associated with the root of the tree and it is partitioned into four regions, each associated with a child of the root. Recursively, each region is partitioned into four regions and so on. The smallest indexed regions are associated with the leaves of the tree.

We denote by 0 the level corresponding to the leaves of the SQT and by k the level corresponding to the root (i.e., k is the maximum level).

We start by describing the level 0, by referring to Fig. 1.

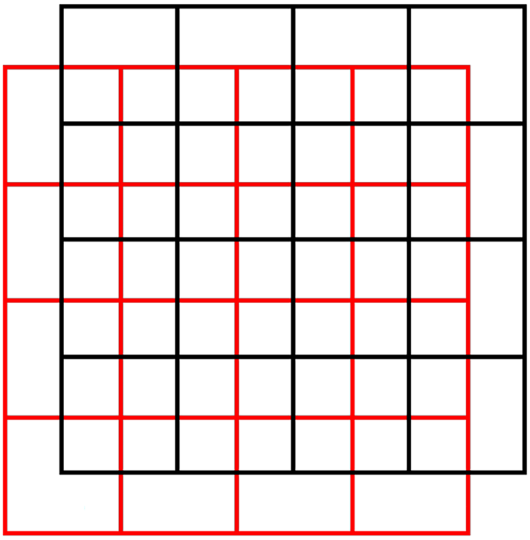

Fig. 1 Level 0 of the SQT

Consider two grids (one black and the other red) composed of square cells, initially coinciding and shifting the red one across the left-bottom diagonal by the half diagonal of the square. The result is depicted in Fig. 1. Each cell (black or red) corresponds to a leaf of the SQT and it is identified by the coordinates of its center. We denote such a pair of coordinates as *centroid*.

It is easy to see that this structure satisfies two properties: (1) the victim/offender is always simultaneously within two cells and (2) if the distance between the victim and the offender is less than half of the length of the side of the cell, then they have at least one cell in common. Therefore, the level 0 corresponds to the minimum safety distance equal to half of the side of a cell.

To enable greater distances, we leverage the same shifted structure at higher levels. To understand the mechanism, we show as the level 1 of the SQT is implemented.

Consider just the black grid of level 0, reported for clarity in Fig. 2. The four adjacent black cells α, β, γ, δ are aggregated into a cell blue of level 1, say A. At this point, we take the four black cells ϵ, γ, ζ, η of level 0 and aggregate them into a green cell of level 1, say B. Observe that B can be viewed as the cell A shifted across the left-bottom diagonal by the half diagonal of the square (similarly to level 0). The above procedure is applied to the entire level 0, by taking (four by four) the other adjacent cells, thus completing the level 1.

At the end, we obtain two grids, one blue, and the other green shifted in the same way as the black and red grids, but with greater size of the cells (twice the size of the cells of level 0).

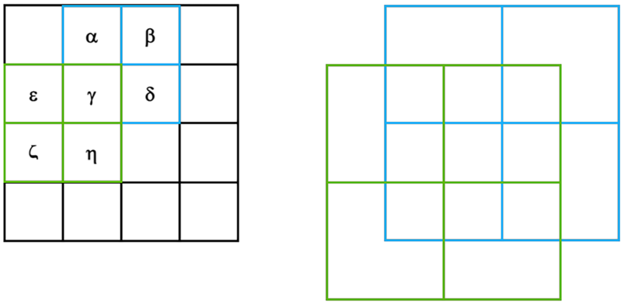

Fig. 2 Level 1 construction of the SQT

At this point, the same procedure can be iterated to build the level 2 starting from the blue grid, and so on, until the desired roots (to have a forest of SQTs).

The SQT-based grid organization of the territory will be exploited in our protocol to identify the proximity of the victim and offender. This is done by enabling the periodical sending from them of the centroids of the cells they belong to (once the level of the SQT is set). The server will detect the proximity in the case of common centroids.

However, allowing the sending of centroids as plaintext would disclose the position of the victim. This would be intolerable from a privacy point of view. Even sending a cryptographic hash of the centroid is not resolutive, because the size of the domain of centroids is not enough large to prevent the reverse of the digests. To avoid this, we combine our grid-based approach with a tag-based (see Sect. 2) mechanism, to make available an unpredictable value, associated with a point in space and over time used as a *salt* when digests are generated. This way, reversing is prevented.

In the literature [49], by tag, we can refer to Bluetooth IDs, Wifi IDs, military codes in GPS, audio signals, LTE, and atmospheric gases.

In our protocol, we choose to implement the salt mechanism by relying on the collaboration of a telephone service provider (TSP), which transmits the salts through the cellular network. In this approach, we exploit cellular cells to identify a region of the space in which, for a given time interval, a random salt, with a suitable rounding protocol, is periodically sent in broadcast to all the devices belonging to this cell. We organize the tag mechanism in a hierarchical way, where level 0 is represented by the physical TSP cells and, at higher levels, we set suitable cells (by aggregating underlying cells) that we call *virtual* TSP cells. With the term *tag-cell*, we generically denote either physical or virtual TSP cells. Specifically, tag-cells of level k are obtained by aggregating tag-cells of level $k - 1$, as described in the following.

Before discussing it, we deal with the problem of possible misalignment, at each level of the hierarchy, between the grid and the tag-cell structure.

Indeed, it may happen that a grid cell is cut from a tag-cell. In this case, two users belonging to the same grid cell could receive two different salts, thus compromising proximity detection.

To avoid this, we implement a mechanism to obtain tag-cells that include entirely grid cells of the same level, thus preventing the above drawback. This is obtained with levels greater than 0 by construction, just by aggregating tag-cells of a lower level to obtain tag-cells of the successive level that include entirely grid cells of the same level.

At level 0, we have to face the problem that physical TSP cells have a fixed size that cannot modulate to adapt to our solution. To solve this problem, at level 0, we introduce a tailored mechanism.

We assume that the grid cells of level 0 have a size of the same order of magnitude as the physical TSP cells or they are smaller. This is not an abstraction since TSP cells currently deployed on the territory have at least a coverage area of at least 200 ms (picocells).

At level 0, our mechanism works as follows. Each TSP antenna broadcasts:

1. A *primary salt* in its coverage area (physical TSP cell), and
2. the primary salts of the adjacent TSP antennas. These salts are called *secondary salts*.

Then, each user receives a set of salts of level 0. It is easy to realize that, two users in the same grid cell of level 0 receive at least one salt of level 0 in common.

For a generic level l, we require that the same salt be provided in the entire tag cell of level l. To do this, the TSP broadcasts the same salt of level l in all the physical TSP cells forming the tag cell of level l.

To conclude this section, we summarize the information captured by the users and exploited in the protocol presented in Sect. 5.2.

Consider the offender S and the victim V at a distance less than half of the length of the side of the cells of level l.

1. S detects two centroids C_1^S and C_2^S and V detects two centroids C_1^V and C_2^V such that at least one between C_1^S and C_2^S coincides to one between C_1^V and C_2^V.
2. S detects a set of salts of level l R_S and V detects a set of salts of level l R_V such that $R_S \cap R_V \neq \emptyset$.

The importance of the above information will be clear in Sect. 5.2.

5.2 The proposed protocol

In this section, we propose our solution that gives an answer to research question **RQ2** defined in Sect. 3. First, we define all the involved actors, and then we describe the protocol on which the solution is based.

The actors are:

- *Victim* V: the person who is under the threat of a sex offender.
- *Sex Offender* S: the person who threatens the safety of the victim and who is, therefore, under police surveillance.
- *Law Enforcement Agency* L: a central entity that monitors S and is authorized to collect and handle data and information about them. No monitoring threatening privacy is allowed to L regarding the victim, except in case of emergency.

As discussed in Sect. 5.1, in addition to the above actors, also the *Telephone Service Provider* (TSP, for short) has a role in the solution, consisting of the periodical sending of salts in the territory.

To implement our solution, we leverage the SQT structure introduced in Sect. 5.1. Suppose L received a court restraining order specifying d as the minimum distance that the S must maintain with respect to V. According to this distance, L sets the proper level l of the SQT. Specifically, l is selected as the minimum level such that, denoting by x the length of the side of its cells, it holds that $x \geq 2d$.

Now, we describe how the solution is implemented by considering separately the offender-side equipment and actions and the victim-side equipment and actions.

Offender. The sex offender will be equipped with a special portable GPS tracking device running our application and embedding also a SIM card. The device is tamper-evident and includes non-accessible memory areas. As already happens in adopted electronic monitoring systems, the device is worn on the ankle (or on the arm) of the offender and is equipped with a battery unit.

We want to observe that standard GPS localization may present some flaws in terms of accuracy in the case of indoor positioning. However, as reported in [50], it can be used in combination with other already available technologies. For example, the combination of GPS and PDR (Pedestrian Dead Reckoning) [51] enables localization for both indoor and outdoor environments.

The following information is inserted by L at the set-up phase into the non-accessible memory area:

- ID_S: An ephemeral identifier of the sex offender.
- ID_V: An ephemeral identifier of the victim.
- l: The level of the SQT selected by L.

Furthermore, some information is periodically received by the SIM card and the GPS receiver, and allows the application to compute further information to send to L via cellular communication, leveraging a cryptographic hash function h.

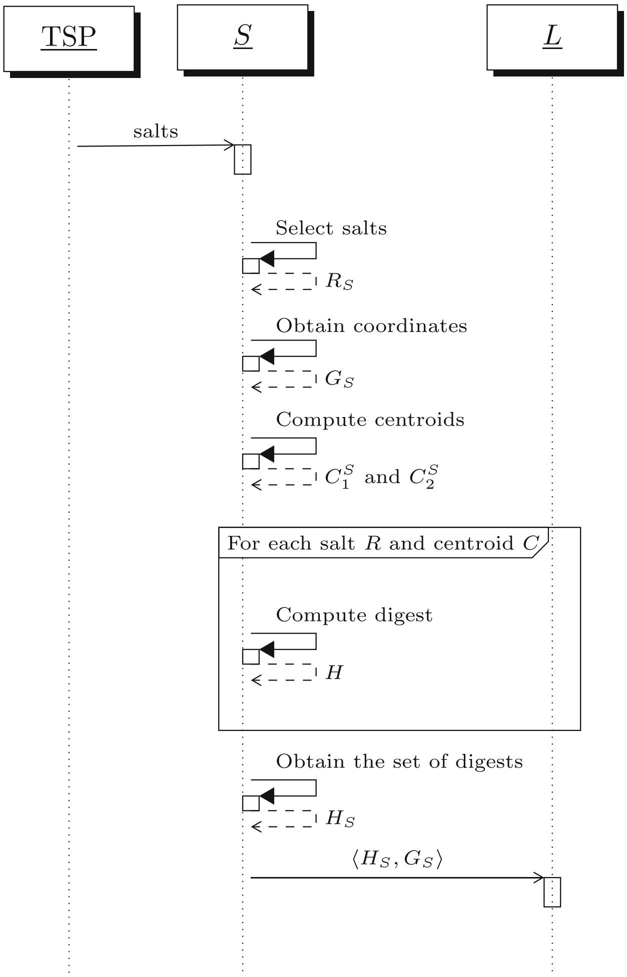

Fig. 3 Sequence diagram of the offender-side actions

Specifically:

- The SIM card receives all the salts transmitted by TSP in that location.
- The application selects the salts associated with level l. Denote by R_S the set of these salts.
- The GPS receiver obtains the coordinates G_S identifying the position of S.
- The application computes, starting from G_S, the centroids C_1^S and C_2^S of the cells of level l which S belongs to.
- For each salt R and for each centroid C, the application computes a digest $H = h(R||C||ID_V||ID_S)$. We denote by H_S the set of the thus computed digests.
- Finally, S sends $\langle H_S, G_S \rangle$ to L.

The sequence of the actions performed offender-side is summarized in the sequence diagram of Fig. 3.

Victim. The victim should not be provided with dedicated devices. They can use their personal smartphone equipped with our specific application.

The same information stored in the offender's device is inserted by L at the set-up phase into the smartphone of the victim:

- ID_S: An ephemeral identifier of the sex offender.
- ID_V: An ephemeral identifier of the victim.
- l: The level of the SQT selected by L.

The application runs a sequence of actions very similar to those executed offender-side:

- The SIM card receives all the salts transmitted by TSP in that location.
- The application selects the salts associated with level l. Denote by R_V the set of these salts.
- The GPS receiver obtains the coordinates G_V identifying the position of V.
- The application computes, starting from G_V, the centroids C_1^V and C_2^V of the cells of level l to which V belongs.
- For each salt R and for each centroid C, the application computes a digest $H = h(R||C||ID_V||ID_S)$. We denote by H_V the set of the thus computed digests.
- Finally, V sends $\langle H_V \rangle$ to L.

The sequence of the actions performed victim-side is summarized in the sequence diagram of Fig. 4.

Observe that V does not send the GPS coordinates G_V to L, but only the non-reversible digests. This preserves their privacy.

At this point, some actions are performed server-side by L.

Law Enforcement Agency. L receives $\langle H_S, G_S \rangle$ from S and $\langle H_V \rangle$ from V.

Then, it performs as follows:

- L computes $H_{SV} = H_S \cap H_V$.
- If $H_{SV} = \emptyset$, then no action is needed and L waits for the next tuples from S and V.
- Otherwise (i.e., $H_{SV} \neq \emptyset$), the proximity between V and S is detected. Therefore, the following actions are performed:
  - L, who knows V's mobile number, sends the alarm to V and also communicates the exact location of S so that V can move away in the opposite direction.
  - Once the alarm is received, the app of V will respond with an acknowledgment and provide its exact G_V location to facilitate the possible intervention of the police that can reach both V and S.

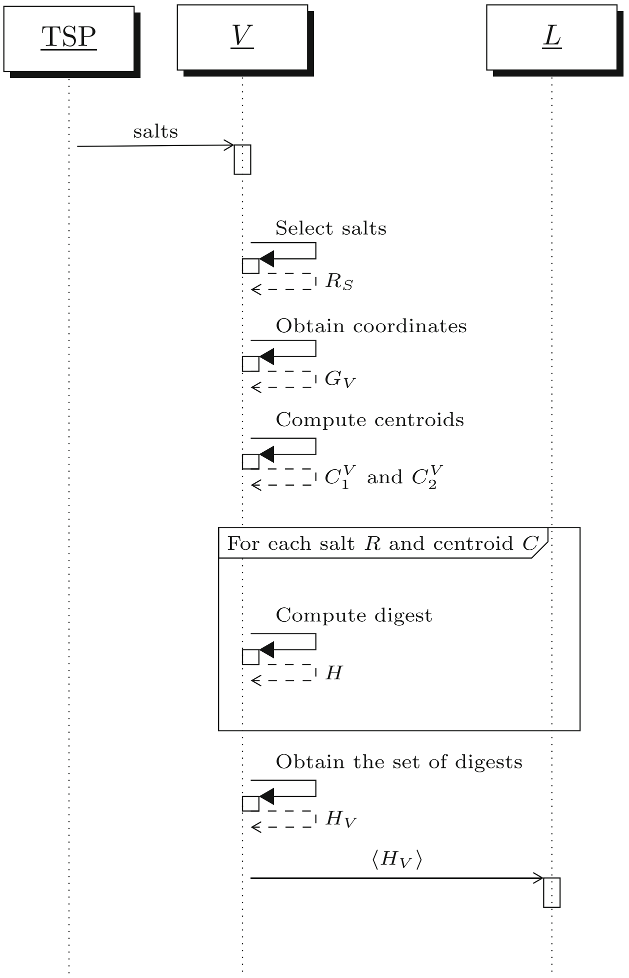

Fig. 4 Sequence diagram of the victim-side actions

The sequence of the actions performed by the Law Enforcement Agency is summarized in the sequence diagram of Fig. 5.

6 Security analysis

Through this section, we discuss the security guarantees offered by our proposal.

We refer to the notation introduced in Sect. 5.2.

Our analysis is performed in terms of *Security Properties*.

SP1: If V and S are at distance less than d, an alarm is triggered by L.

This property refers to the *correctness* of the protocol.

We show that this property is guaranteed by our solution.

Indeed, regardless of the distance between V and S, V sends L the tuple $\langle H_S, G_S \rangle$. Since S is equipped with a non-tamperable device, such a tuple may not be correctly provided only if the GPS receiver is not able to detect the GPS signal. We observe that, as discussed in Sect. 3, the absence of a GPS

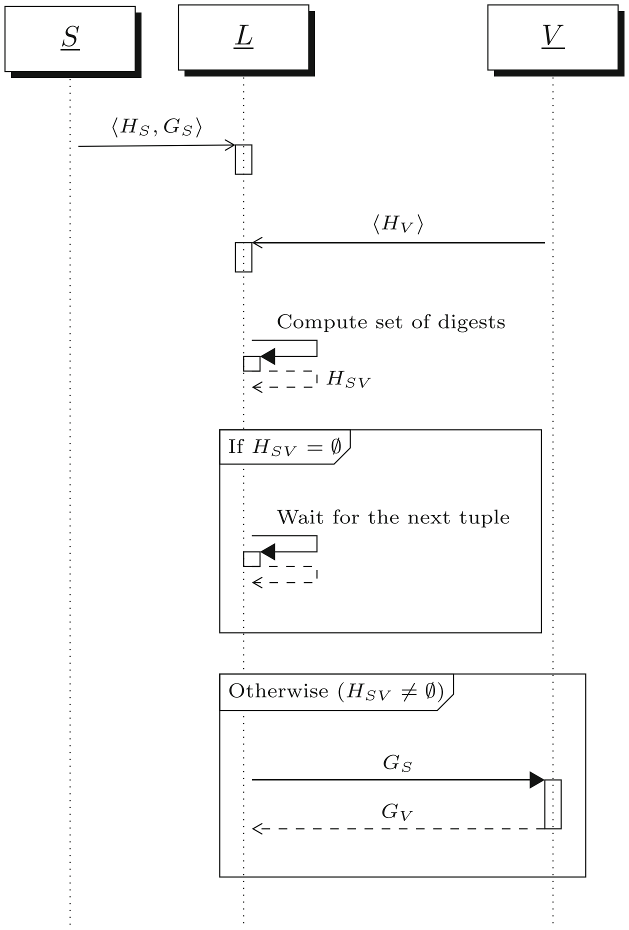

Fig. 5 Sequence diagram of the Law Enforcement Agency-side actions

signal can occur in two cases. Either the offender performs a jamming attack on the GPS signal or the GPS signal is obscured accidentally by obstacles. However, in both cases, if L does not have the information from S, the alarm is triggered.

Now, consider the case in which the tuple $\langle H_S, G_S \rangle$ is correctly provided by S to L. We recall that d is the distance selected by the court order. Moreover, L selects a level l of the SQT corresponding to cells of size x, such that $x > 2d$. As illustrated in Sect. 5.1, this implies that two users at a distance less than $\frac{x}{2}$ share at least a cell. Therefore, if V and S are at a distance less than d, then they share at least a centroid, say C.

Furthermore, the introduction of the tag-cells ensures that V and S receive at least one common salt, say R, since they share a cell. Then, they compute the same digest $H = h(R||C||ID_V||ID_S)$. Therefore, the set $H_{SV} = H_S \cap H_V$ includes at least H. This condition triggers the alarm.

SP2: L knows the position G_V of V if and only if their proximity with S is detected.

This property refers to the *privacy* feature offered to V. In our threat model, we assume L is honest-but-curious, in the sense that it performs legally the step of the protocol, but attempts to leak the privacy of V.

We show that this property is guaranteed by our solution.

Concerning the **if-part**, by definition of the protocol, when the proximity between V and S is detected, V voluntarily provides their coordinates G_V to L.

Consider now the **only if-part**. According to the assumption, L is honest-but-curious. Therefore, we assume L attempts to discover the position of V from the information provided by them. The only information V sends L is the set of digest H_S. Each element $H \in H_S$ is in the form $H = h(R||C||ID_V||ID_S)$. From H, L may attempt to discover C, as it represents approximate information about the location of V.

Even though L knows ID_V and ID_S, the presence of the salt R prevents dictionary attacks performed on the domain of the centroids. Therefore, L is not able to reverse the hash function and detect C.

7 Implementation issues for real-world adoption

In this section, we discuss some possible hardware and software technologies to adopt for a real-life implementation of our proposal.

7.1 Hardware components

The offender tracking device should include:

- **Microcontroller:** A microcontroller (e.g., STM32) to run some operations of the protocol written in the flash memory.
- **GPS module**: A high-sensitivity GPS receiver to ensure accurate outdoor positioning. For example, the u-blox M8 receiver may reach an accuracy of about 2 m. We observe that distances of restrictive orders vary from country to country and from case to case. However, typical distances are above 100 m.[1], [2], [3], [4], [5] Therefore, 2 ms of accuracy are sufficient to minimize false positives (where the system incorrectly identifies the offender as being

[1] https://www.courts.ca.gov/1260.htm.

[2] https://lisagelman.com/domestic/domestic-violence-restraining-orders-legal-principles/.

[3] http://poems-project.com/wp-content/uploads/2015/02/Spain.pdf.

[4] https://www.avvocatoflash.it/blog/diritto-penale/cosa-vuol-dire-ordinanza-restrittiva.

[5] http://poems-project.com/wp-content/uploads/2015/02/Estonia.pdf.

Table 1 Examples of distances for restrictive orders in different countries

State	Distance (m)
United States (California)	100
Canada (Ontario)	500
Spain	500
Italy	500
Estonia	100

nearby) and false negatives (where the system fails to detect the offender's proximity). In Table 1, we report some examples of distances for restrictive orders in different countries.

- **PDR system**: An inertial measurement unit (IMU) such as the MPU-9250 to complement GPS data for accurate indoor positioning. It can achieve accuracy for indoor positioning in the order of centimeters [52, 53].
- **Communication module**: A GSM/3 G/4 G LTE module (e.g., Quectel EC25) for data transmission.
- **Tamper detection hardware**: Examples include co conductive traces or pressure sensors.
- **Power supply**: A rechargeable battery with a capacity of at least 2000 mAh to ensure a day's operation, with low-battery alerts.

The victim should have:

- **A portable device**: Concretely, a smartphone with GPS enabled.

The Law-Enforcement Agency should have:

- **Backend server**: A robust server infrastructure to handle data reception, detect proximity, and alert generation. This infrastructure can be implemented through cloud platforms such as AWS or Azure.

7.2 Software components

The software running in the offender hardware is directly written in the flash memory and performs the following operations:

- Retrieve the offender position through the GPS Module and PDR System.
- Retrieve the salt through the Communication Module.
- Compute the digests through a secure cryptographic hash function (e.g., SHA-256)
- Encrypt the digests before sending them to the backend server. A robust encryption function such as AES-256 should be adopted.
- Transmit the (encrypted) digest to the backend server through the Communication Module.

The software running on the victim's portable device performs the same operations as the software of the offender. However, it is not written in the flash memory of a microcontroller.

Realistically, the software is an application running both on Android and IOS systems.

7.3 Salt distribution

One of the aspects to cover in more detail is the technology adopted by the TSP to transmit the salt. In this section, we propose two possible alternatives leveraging standard protocols.

Cell broadcast service (CBS) CBS is a method of GSM/3 G/LTE networks designed for simultaneously sending messages to multiple users in a specific area. It's often used for emergency alerts.

In this case, the salt can be embedded in a CBS message and broadcasted to all devices in a specified area. The advantage of this approach is that minimal modifications are required to the standard.

Dedicated network signaling Another possibility is to use an existing signaling protocol (e.g., System Information Block (SIB)) to include the salt.

In this case, the SIB messages should include an additional field for the salt. The base stations broadcast them to all devices within a cell.

If the frequency of transmission of SIB messages is compatible with that of the salts, the advantage of this approach is that it does not require additional messages to transmit the salt.

For both the approaches, the salts should be encrypted to prevent tampering.

7.4 Scalability issues

One of the aspects to consider is whether scalability may be a concern for our protocol. We preliminarily observe that in [50], a grid-based solution based on the transmission of digests to detect proximity is adopted in the context of digital contact tracing. Therein, the authors show that a simple personal computer, equipped with a 1.8 GHz Intel i7-8850 CPU and 16 GB of RAM, can manage an area including up to 300,000 users.

Clearly, the domain considered in this paper (sex offender) includes (hopefully) a much smaller number of users than the contact tracing domain.

For example, according to[6], in the US, Texas has the largest list of registered sex offenders in 2023, with over 100,000 individuals. Therefore, a simple server with no particular computation capability is sufficient to implement our solution in an entire State.

We can conclude that scalability problems cannot affect our proposal.

8 Conclusion

In this paper, we propose a GPS-based solution for electronic monitoring preserving the victim's privacy. The choice of GPS in place of (or in combination with) other alternatives as RFID, arises from a detailed analysis of the security requirements that have to be achieved. The result of this analysis shows that GPS represents the better choice when high security is required. However, current solutions involving GPS are not adequate since they present serious privacy issues. To solve this, we implement a more complex solution involving a hierarchical grid-based approach and the collaboration of a telephone service provider. Through our approach, the victim does not send in clear GPS coordinates, but just an obfuscated form of them. The disclosure of the position of the victim is allowed only in the case the offender is in their proximity. This shows that our solution allows both to preserve the privacy of the victim and the effectiveness of electronic monitoring to safeguard the victim. As future work, we plan to implement the solution and test it in a real environment.

Funding Open access funding provided by Università degli Studi Mediterranea di Reggio Calabria within the CRUI-CARE Agreement.

Data availability Not applicable.

References

1. Anderez DO, Kanjo E, Amnwar A, Johnson S, Lucy D (2021) The rise of technology in crime prevention: opportunities, challenges and practitioners perspectives. arXiv preprint arXiv:2102.04204
2. Weber RH (2010) Internet of things—new security and privacy challenges. Comput Law Secur Rev 26(1):23–30. https://doi.org/10.1016/j.clsr.2009.11.008
3. Nellis M (2021) Electronic monitoring around the world. Oxford University Press, Oxford. https://doi.org/10.1093/acrefore/9780190264079.013.642
4. Williams J, Weatherburn D (2022) Can electronic monitoring reduce reoffending? Rev Econ Stat 104(2):232–245
5. Fitzalan Howard F (2020) The experience of electronic monitoring and the implications for effective use. Howard J Crime Justice 59(1):17–43
6. Belur J, Thornton A, Tompson L, Manning M, Sidebottom A, Bowers K (2020) A systematic review of the effectiveness of the electronic monitoring of offenders. J Crim Justice 68:101686. https://doi.org/10.1016/j.jcrimjus.2020.101686
7. Abudalfa S, Bouchard K (2023) Two-stage RFID approach for localizing objects in smart homes based on gradient boosted decision trees with under-and over-sampling. J. Reliab. Intell. Environ. 10:45–54
8. Padgett KG, Bales WD, Blomberg TG (2006) Under surveillance: an empirical test of the effectiveness and consequences of electronic monitoring. Criminol. Public Policy 5(1):61–91
9. Haverkamp R, Mayer M, Levy R (2004) Electronic monitoring in Europe. In: Encyclopedia of criminology and criminal justice, vol. 12, p 36
10. Renzema M, Skelton DT (1990) Use of electronic monitoring in the united states: 1989 update. National Institute of Justice, Washington, DC
11. Taylor SR, Kandaswamy S, Evans T, Mahaffey D (2016) Market-survey of location-based offender tracking technologies
12. Schwitzgebel R, Schwitzgebel R, Pahnke WN, Hurd WS (1964) A program of research in behavioral electronics. Behav Sci 9(3):233–238
13. Police IA (2008) Tracking sex offenders with electronic monitoring technology: implications and practical uses for law enforcement. International Association of Chiefs of Police, Alexandria
14. Schmidt AK (1988) The use of electronic monitoring by criminal justice agencies, 1988. US Department of Justice, National Institute of Justice, Washington, DC
15. Kilgore J (2013) Progress or more of the same? Electronic monitoring and parole in the age of mass incarceration. Crit Criminol 21(1):123–139
16. Demichele M, Payne BK, Button DM (2008) Electronic monitoring of sex offenders: identifying unanticipated consequences and implications. J Offend Rehabil 46(3–4):119–135
17. Button DM, DeMichele M, Payne BK (2009) Using electronic monitoring to supervise sex offenders: legislative patterns and implications for community corrections officers. Crim Justice Policy Rev 20(4):414–436
18. Nellis M (2014) Understanding the electronic monitoring of offenders in Europe: expansion, regulation and prospects. Crime Law Soc Change 62(4):489–510
19. Nellis M (1991) The electronic monitoring of offenders in England and wales: recent developments and future prospects. Br J Criminol 31(2):165–185
20. Nellis M (2006) Electronic monitoring in Scotland 1998–2006. Scott J Crim Justice Stud 12:74–96
21. Sarzała D (2016) Electronic monitoring in the polish legal system as a form of social readaptation. American Historical, 1916
22. Paganelli AI, Velmovitsky PE, Miranda P, Branco A, Alencar P, Cowan D, Endler M, Morita PP (2022) A conceptual IoT-based early-warning architecture for remote monitoring of COVID-19 patients in wards and at home. Internet Things 18:100399. https://doi.org/10.1016/j.iot.2021.100399
23. Hyysalo J, Dasanayake S, Hannu J, Schuss C, Rajanen M, Leppänen T, Doermann D, Sauvola J (2022) Smart mask-wearable

[6] https://www.safehome.org/data/registered-sex-offender-stats/.

IoT solution for improved protection and personal health. Internet Things 18:100511. https://doi.org/10.1016/j.iot.2022.100511

24. Schmidtke HR (2020) Location-aware systems or location-based services: a survey with applications to COVID-19 contact tracking. J Reliab Intell Environ 6(4):191–214
25. Bulman P (2010) Electronic monitoring reduces recidivism. Correct Today 72(6)
26. Lockhart-Mirams G, Pickles C, Crowhurst E (2015) Cutting crime: the role of tagging in offender management. Reform, London
27. Marzena Kordaczuk-Was MP (2012) Integrated system of monitoring cases of domestic violence—Spanish experience (2011/2012). https://www.policja.pl/download/1/186464/PublikacjaENGLISH.pdf
28. Albrecht H-J (1995) Electronic monitoring in Europe. Bulletin d information penologique 19 20:8–9
29. Ramtohul AM, Khedo KK (2021) In: Paiva S (ed) Proximity based social networking in urban environments: applications, architectures and frameworks. Springer, Cham, pp. 71–107. https://doi.org/10.1007/978-3-030-71288-4_4
30. Buccafurri F, De Angelis V, Idone MF, Labrini C, Lazzaro S (2022) Achieving sender anonymity in tor against the global passive adversary. Appl Sci 12(1):137. https://doi.org/10.3390/app12010137
31. Mascetti S, Bettini C, Freni D, Wang XS, Jajodia S (2009) Privacy-aware proximity based services. In: 2009 Tenth international conference on mobile data management: systems, services and middleware. IEEE, pp 31–40
32. Oleynikov I, Pagnin E, Sabelfeld A (2020) Where are you bob? Privacy-preserving proximity testing with a napping party. In: European symposium on research in computer security. Springer, pp. 677–697
33. Buccafurri F, De Angelis V, Francesca Idone M, Labrini C (2021) A privacy-preserving protocol for proximity-based services in social networks. In: 2021 IEEE global communications conference (GLOBECOM), pp 1–6 . https://doi.org/10.1109/GLOBECOM46510.2021.9685284
34. He Y, Chen J (2021) User location privacy protection mechanism for location-based services. Digit Commun Netw 7(2):264–276. https://doi.org/10.1016/j.dcan.2020.07.012
35. Bostanipour B, Garbinato B (2015) Effective and efficient neighbor detection for proximity-based mobile applications. Comput Netw 79:216–235. https://doi.org/10.1016/j.comnet.2014.12.013
36. Buccafurri F, De Angelis V, Labrini C (2020) A privacy-preserving solution for proximity tracing avoiding identifier exchanging. In: 2020 International conference on cyberworlds (CW), pp 235–242. https://doi.org/10.1109/CW49994.2020.00045
37. Weisburd K (2019) Sentenced to surveillance: fourth amendment limits on electronic monitoring. NCL Rev 98:717
38. Wekesa M, Muendo M, Mikinyango A (2020) The use of electronic tracking and monitoring systems and the right to privacy. Int J Soc Sci Technol 5(4):1–35
39. Li M, Koutsopoulos I, Poovendran R (2010) Optimal jamming attack strategies and network defense policies in wireless sensor networks. IEEE Trans Mob Comput 9(8):1119–1133
40. Muraleedharan R, Osadciw LA (2006) Jamming attack detection and countermeasures in wireless sensor network using ant system. In: Wireless sensing and processing, vol 6248. International Society for Optics and Photonics, p 62480
41. Singh J, Woungang I, Dhurandher SK, Khalid K (2022) A jamming attack detection technique for opportunistic networks. Internet Things 17:100464. https://doi.org/10.1016/j.iot.2021.100464
42. Hunt-Grubbe H (2020) In: Igoumenou A (ed) The many faces of surveillance: ethical considerations that encompass the use of electronic monitoring in criminal and clinical populations. Springer, Cham, , pp 115–134. https://doi.org/10.1007/978-3-030-37301-6_7
43. Owens K (2022) Electronic monitoring smartphone apps: an analysis of risks from technical, human-centered, and legal perspectives. In: 31st USENIX security symposium (USENIX Security 22). USENIX Association, Boston, MA. https://www.usenix.org/conference/usenixsecurity22/presentation/owens
44. Li HP, Hu H, Xu J (2012) Nearby friend alert: location anonymity in mobile geosocial networks. IEEE Pervasive Comput 12(4):62–70
45. Šikšnys L, Thomsen JR, Šaltenis S, Yiu ML, Andersen O (2009) A location privacy aware friend locator. In: International symposium on spatial and temporal databases. Springer, pp 405–410
46. Šikšnys L, Thomsen JR, Šaltenis S, Yiu ML (2010) Private and flexible proximity detection in mobile social networks. In: 2010 Eleventh international conference on mobile data management. IEEE, pp 75–84
47. Buccafurri F, Furfaro F, Mazzeo GM, Saccà D (2011) A quad-tree based multiresolution approach for two-dimensional summary data. Inf Syst 36(7):1082–1103. https://doi.org/10.1016/j.is.2011.03.007. (**Special Issue: Advanced Information Systems Engineering (CAiSE&apos;10)**)
48. Buccafurri F, De Angelis V, Idone MF, Labrini C (2022) A protocol for anonymous short communications in social networks and its application to proximity-based services. Online Soc Netw Media 31:100221. https://doi.org/10.1016/j.osnem.2022.100221
49. Narayanan A, Thiagarajan N, Lakhani M, Hamburg M, Boneh D et al (2011) Location privacy via private proximity testing. In: NDSS, vol 11
50. Buccafurri F, De Angelis V, Labrini C (2022) A centralized contact-tracing protocol for the COVID-19 pandemic. Inf Sci 617:103–132. https://doi.org/10.1016/j.ins.2022.10.101
51. Li X, Wei D, Lai Q, Xu Y, Yuan H (2017) Smartphone-based integrated PDR/GPS/Bluetooth pedestrian location. Adv Space Res 59(3):877–887
52. Zhang H, Zhang Z, Gao N, Xiao Y, Meng Z, Li Z (2020) Cost-effective wearable indoor localization and motion analysis via the integration of UWB and IMU. Sensors. https://doi.org/10.3390/s20020344
53. Yao L, Yao L, Wu Y-W (2021) Analysis and improvement of indoor positioning accuracy for UWB sensors. Sensors. https://doi.org/10.3390/s21175731