Letter

Decision Support System Based on Indoor Location for Personnel Management

Néstor Álvarez-Díaz [1,*] and Pino Caballero-Gil [2]

1 Department of Statistics, Operations Research and Computing, University of La Laguna, 38200 San Cristóbal de La Laguna, Spain
2 Department of Computer Engineering, Faculty of Maths, University of La Laguna, 8200 San Cristóbal de La Laguna, Spain; pcaballe@ull.edu.es
* Correspondence: nalvared@ull.edu.es

Abstract: A wide variety of business areas organize their work based on the location of their employees because only by taking these locations into account, they can schedule activities properly. However, in a large number of cases, the requirement of immediacy, such as the need to help an injured person in a hospital or to dry up water in a busy hallway to prevent people from slipping, is a major constraint. This work is based on a proof of concept in which we used Bluetooth Low Energy devices to track the location of each employee in an indoor environment. Among other factors, the location of each individual is assigned a large percentage of the weight to assign a task. This proposal is intended to cover some scenarios of great interest, guaranteeing the correctness of measurement and the privacy of staff tracking.

Keywords: human resource management; IoT devices; indoor location; non-interactive zero knowledge range proof; privacy-preserving location

1. Introduction

Efficient and proper allocation of human resources is not an easy task, especially if the company has a high degree of uncertainty and requires quick responses at the same time. In many cases, different events need to be attended without prior scheduling, with a limited number of workers, and immediately. Huge facilities such as airports [1], docks [2] or hospitals [3] are examples of how important proper human resources scheduling is. A misallocation of resources could increase the risk of critical activities, increase the cost of an operation, or even block the smooth running of a particular service. These facilities have in common that their dimensions are enormous. For human resources scheduling, this factor must be taken into account if the distance between the workers and the place of the event can be an important restriction when assigning a task, since the travel time of the workers before starting the activity can be critical for its proper development. To improve the allocation of both human and non-human resources, the location of those resources in the work environment can become the cornerstone of a good scheduling.

Interest in location has not stopped growing in recent years due to the wide variety of its applications, from supply chain tracking [4] to blind people guidance [5]. However, an essential distinction must be kept in mind when the location is part of the information for further analysis, and the system considers the location of an outdoor or an indoor environment. A mature system, such as the Global Positioning System (GPS), provides good accuracy, yet not in closed environments like a building. Another kind of systems, normally based on Received Signal Strength Indicator (RSSI), continue to be a matter of study due to the improvement in accuracy in indoor environments [6]. In the analyzed scenario, where most of the resources are inside a building, the use of GPS, for example, is not the most convenient. For this reason, the proposal explained here uses a system not based on GPS, which provides good precision within the facilities.

For years, the RSSI-based systems have been supported by Wi-Fi access points as the best alternative because these types of elements are currently present in the facilities, in addition to having a wide range of coverage [7]. Besides, these elements are combined with Radio-Frequency Identification (RFID) or Bluetooth Low Energy (BLE) devices due to the improvements of the measures [8] and the extension of the range of action, as well as the lower cost of these devices compared to Wi-Fi access points. In the particular case of BLE beacons, their low cost, minimal battery consumption and small size allow us to conclude that they are a perfectly valid technology for use in indoor location.

Nowadays, the use of BLE-based systems for indoor location is quite common. Reflection, diffraction, or materials help decrease the accuracy of measurements. For that, a wide variety of systems are now using different techniques such as fingerprints, Kalman filters or even neural networks [9–11] in order to increase the precision of the measurements. Nonetheless, due to the workload of these methods, the resolution of the location problem is usually delegated to a centralized system, which is responsible for using all the individual measurements to provide a solution as accurately as possible without draining target's battery with an additional calculation of those heavy methods. This implies that each tracked location is sent directly to the central system, which records them for further analysis. Determining the location in this way poses a privacy issue in relation to the people who are being monitored [12,13].

Preserving the privacy of employees should be key, no matter how much location contributes to improving a scheduling system. The misuse of this system can cause that instead of improving the organization, it becomes a system that allows to infer habits in the routines of the employees, such as the time spent in the bathroom or meeting areas between employees. To avoid this potential malpractice, it may be more beneficial to reduce the location precision in order to ensure that privacy is preserved.

The case study analyzed here is based on a previous proof of concept [14] whose scenario is the management of a huge infrastructure such as an airport. The proposed application has two main parts: the categorization of the type of activities along with the ability to carry out some types of work by the staff and the addition of the location as part of the Decision Support System (DSS). This document presents a novel DSS that is endowed with the ability to add location as a key factor to a real DSS, paying special attention to preserving the privacy of each employee.

The paper is divided into three sections, as follows. Section 2 discusses the main issues related to location accuracy and describes some improvements to increase it. Section 3 addresses the privacy preservation issue by avoiding the use of the proposed DSS to track employees movements. Section 4 introduces an integration of the described tools in the DSS. Finally, Section 5 presents the conclusions and some future lines of research.

2. Discovering the Location

The proposed DSS takes into account the location of the employees as a key factor. In this case, BLE beacons have been chosen as the preferred technology to locate them as reference points [15], so that a receiver, usually a smartphone, can reference these points to locate employees within the facilities.

Employees must have the receiver for the entire working day to be located. Therefore, the used type of device must be portable to allow employee mobility, implying that it must have a battery. As mentioned above, draining the battery as little as possible is also a goal. For that, the proposed DSS uses a basic triangulation method without making large corrections to the received signals. Other methods can provide significant increases in precision by correcting the received signals, but in the proposed DSS, where privacy prevails, these calculations would be carried out in the receiver itself. A high precision system is not necessary in the current scenario because the arrival time of a person from 15 m is not much less than the time it takes a person to arrive if they are 20 m away.

To calculate the employee position in the facility, it is necessary to take into account several aspects:

- The employee's receiver is continuously searching for beacons placed as reference points.
- At least one beacon should be detected in each iteration, and a minimum of three beacons is recommended, for allowing to the receiver to perform the necessary calculations to determine the location.
- The RSSI associated to the discovered beacons must be converted to distance using $D = 10^{(A-RSSI)/K}$ [16].
- With that set of distances and the beacons identifiers, whenever possible, the receiver performs a triangulation to resolve its own position.
- The computed location is sent to the system in order to report the employee's position. Section 3 will show that the location is not sent in plain mode.

Unfortunately, a perfect setting is not always available for triangulation. In Figure 1, three different scenarios are shown where the resolution of the location has a variation of precision.
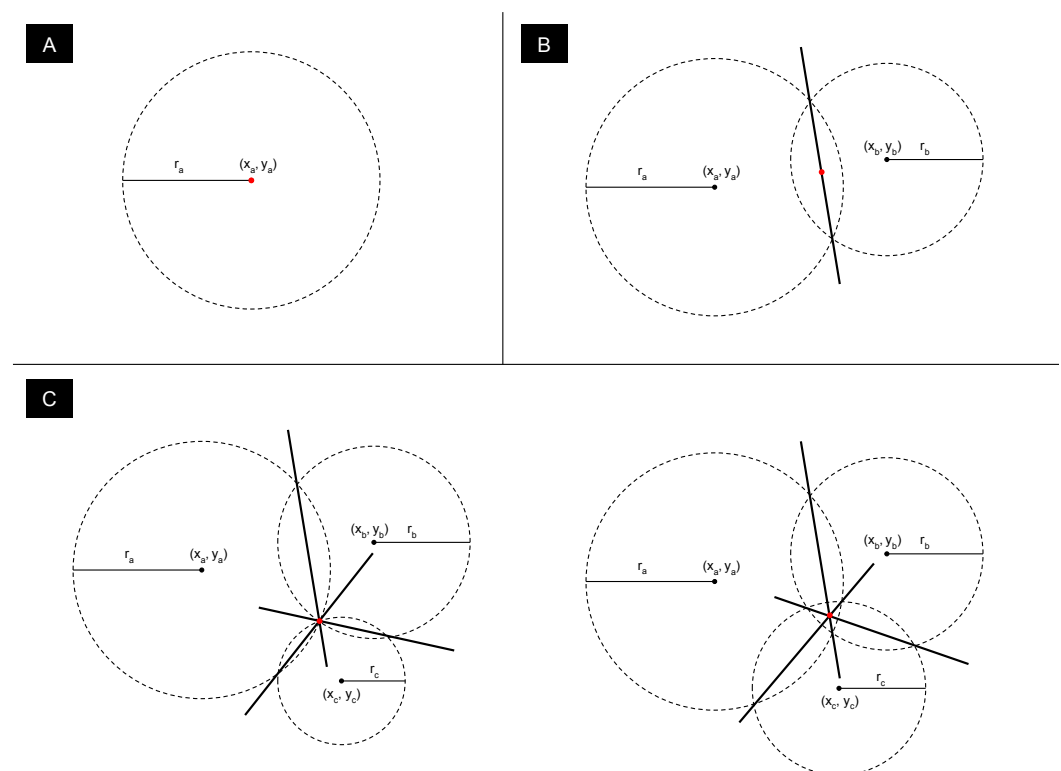
Figure 1. Case (**A**): 1 detected beacon; Case (**B**): 2 detected beacons; Case (**C**): 3 detected beacons.

In Figure 1, case A, where only one beacon is detected, is the worst if the absence of beacons is not considered. Logically, the geometric operations used in other cases will not fit in this case. Desirably, the probability of this event occurring is less than in other cases, but the employee's location is approximate to the location of the beacon, $(x, y) = (x_a, y_a)$.

In Figure 1, case B represents the situation where the receiver only detects two beacons. If a circle intersects another circle, they form a radical axis with two intersections that coincide with two possible points where the employee can be located. The midpoint of the segment formed with two intersection points is an approximate solution to provide homogeneity to subsequent calculations. So, it is necessary to solve the following system of equations to get the approximate location.

$$\begin{cases} \sqrt{(x - x_a)^2 + (y - y_a)^2} = r_a \\ \sqrt{(x - x_b)^2 + (y - y_b)^2} = r_b \end{cases}$$

In Figure 1, case C is the ideal scenario where three beacons are detected by applying geometric property that declares that three circles that cross each other only have one radical center that coincides with the employee's position. To calculate this value, it is necessary to solve an equation system with the equation of the circumference as the base, where (x, y) is the radical center.

$$\begin{cases} (x - x_a)^2 + (y - y_a)^2 - r_a^2 = (x - x_b)^2 + (y - y_b)^2 - r_b^2 \\ (x - x_a)^2 + (y - y_a)^2 - r_a^2 = (x - x_c)^2 + (y - y_c)^2 - r_c^2 \end{cases}$$

Using more beacons so that they are at a shorter distance from each other can prevent the situations in Figure 1A,B. However, this redundancy can provoke a different scenario where four or more beacons are detected, as shown in Figure 2.
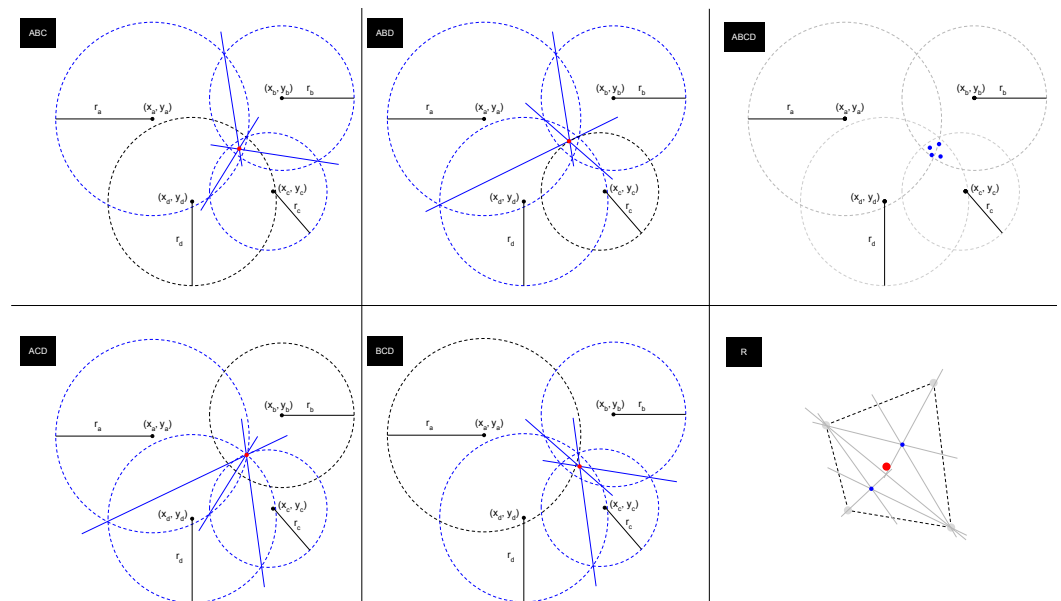

Figure 2. Case: 4 or more detected beacons.

In the case in which 4 or more beacons are detected in the same iteration, the approach proposed for this scenario is to solve all the combinations without repetition taken from 3 of 3 measurements to obtain each individual triangulation in the same way as in the case of 3 beacons. With all possible locations, the centroid of the closed polygon [17] formed by those points is taken as the result of this type of scenario. Figure 2 shows the scenario where 4 beacons are detected. Figure 2ABC,ABD,ACD,BCD are simple combinations, with their corresponding resolved triangulation. Figure 2ABCD shows only the computed results resolved in each individual case. Figure 2R is the closed polygon formed by each individual result and the centroid of this polygon. To compute the centroid of a closed polygon, the following formula is used, where $c = C_{n,3}$, n is the number of detected beacons and C is the number of combinations:

$$(x, y) = \frac{1}{3} \left(\frac{\sum_{i=1}^{c} (x_i + x_{i+1})(x_i y_{i+1} - x_{i+1} y_i)}{\sum_{i=1}^{c} (x_i y_{i+1} - x_{i+1} y_i)}, \frac{\sum_{i=1}^{c} (y_i + y_{i+1})(x_i y_{i+1} - x_{i+1} y_i)}{\sum_{i=1}^{c} (x_i y_{i+1} - x_{i+1} y_i)} \right)$$

3. Preservation of the Privacy

As mentioned in Section 1, the location of each employee is an important factor in determining the most suitable person to perform a particular activity, although the privacy of individuals using the proposed DSS is equally important. For that reason, neither each

individual measurement nor the calculated location is sent directly to the DSS. To guarantee the privacy of the employees, the system is based on the use of a specific type of Zero-Knowledge Proof that allows to convince that a number is within a defined range. In our case, this cryptographic evidence is sent to prove that a person is close to a desired location, without revealing their exact location.

A Zero-Knowledge Proof (ZKP) is a probabilistic cryptographic protocol that allows a prover (P) to convince a verifier (V) about the knowledge of some secret information without revealing anything about it [18]. ZKP is characterized by the following properties:

- Completeness. With a true statement, an honest V will be convinced with high probability by an honest P. Honesty implies that the scheme is followed correctly by both parties.
- Soundness. With an invalid statement, V is convinced of the contrary with very small probability.
- Zero-Knowledge. For a valid statement, V learns no information except that the statement is valid.

Essentially, this kind of proof are divided into two groups: Interactive Zero-Knowledge proofs, which involve synchronization between the prover and the verifier; and Non-Interactive Zero-Knowledge Proofs (NIZKP), which allow V to check the evidences generated by P without synchronous communications [19].

For the proposed DSS, a Non-Interactive Zero-Knowledge Range Proof (NIZKRP) is used to avoid knowing the location of each employee. This kind of proofs are characterized by giving V the ability to know if a certain value is within a defined range without knowledge of that value. Thus, the proposed DSS takes advantages of two main properties of NIZKRP:

- Non-Interactivity due to the need to reduce communications between P and V as well as to allow V to verify the suitability of a set of candidates by itself.
- Proof of Range due to the fact that the desired location cannot be compared to an exact point. This range is used to determine if a person is within a range of the desired location.

The proposed DSS takes advantage of a defined NIZKRP scheme [20] where, in our case, an employee wants to prove that he or she is within a distance range from a particular point. This kind of proofs are widely applied for economic purposes, particularly in the area of cryptocurrencies [21,22], to verify that a specific amount of money is within a known range without compromising the privacy of the transaction revealing the exact amount of money sent. The same mechanism has been applied here to prevent knowing the locations of the employees in a precise way.

Non-Interactive Zero-Knowledge Range Proof Scheme

The prover wants to show that it is m integer units away from the target location, i.e., m is in the $\{a, a+1, \cdots, b\}$ range, where a is the lower bound of defined range and b is the upper bound.

A secret integer m is committed at $c = g^m h^r \bmod N$, where r is a random integer, $N = PQ$ being P and Q large prime numbers, and $(P-1)/2$ is also a prime number. Then, the prover publishes:

$$c_1 = c/g^{a-1} \bmod N$$

$$c_2 = g^{b+1}/c \bmod N$$

$$c' = c_1^{b-m+1} h^{r'} \bmod N \text{ where } r' \text{ is a random integer}$$

$$c'' = c'^{w^2} h^{r''} \bmod N \text{ where } w \text{ and } r'' \text{ are a random integers}$$

The prover also publishes three random integers m_1, m_2, and m_3 such as $m_1 + m_2 + m_3 = w^2(m-a+1)(b-m+1)$ and m_3 is a square and thus non-negative $m_3 = m_4^2$.

Besides, the prover chooses three random integers r_1, r_2, and r_3 such as $r_1 + r_2 + r_3 = w^2((b - m + 1)r + r') + r''$, and publishes:

$$c_1' = g^{m_1} h^{r_1} \; mod \; N$$

$$c_2' = g^{m_2} h^{r_2} \; mod \; N$$

$$c_3' = c'' / c_1' c_2' \; mod \; N$$

The verifier publishes two random integers s and t.
The prover publishes:

$$x = sm_1 + m_2 + m_3$$

$$y = m_1 + tm_2 + m_3$$

$$u = sr_1 + r_2 + r_3$$

$$v = r_1 + tr_2 + r_3$$

The verification is performed by checking the following equations and that x and y are positive integers:

$$c'' = c_1' c_2' c_3' \; mod \; N$$

$$c_1'^s c_2' c_3' = g^x h^u \; mod \; N$$

$$c_1' c_2'^t c_3' = g^y h^v \; mod \; N$$

4. Decision Support System

The purpose of this section is to explain how to integrate the location mechanism described in Section 2 and the privacy preservation shown in Section 3 with a practical DSS. Each of these pieces add value to the system and has a functionality that can be used individually in other systems. However, they are presented here in combination, making a powerful DSS. It must be configured as follows:

1. Define the boundaries and the identifiers of each floor plan.
2. Place and configure beacons correctly, as shown with red dots in Figure 3. This means that each beacon will be registered with a unique identifier and the coordinates where it will be located, allowing the DSS to determine the relative location through triangulation. They should be placed trying to cover the floor in such a way that the receiver detects at least three signals at the same time to minimize the number cases where it only finds one or two beacons.
3. Define all control points within the boundaries of the floor plan, as shown with blue triangles in Figure 3. These points are used to calculate the distances to the receiver. The activities will be defined with some details and one of them is its location which will be located in one of those control points. In addition, a maximum distance is defined here to rule out people who are too far from the control point where the activity is required.
4. Enroll all employees in the system. They should be able to communicate with the system, preferably in a secure way, in order to publish the commitments of their location as well as be able to receive assignments.
5. Define factors and their weight to make decisions based on them, so that $\sum_{i=1}^{n} (f_i \cdot w_i)$ is the score associated to a particular employee, where f is a factor and w is its weight. The employee with the highest score will be selected to perform the activity.
6. Agree on the distance ranges as well as the common cryptographic parameters for the calculation of the NIZKR commitment and secure communications. As mentioned above, ranges should be an integer range such that $r_a^b = \{a, a + 1, \cdots, b\}$ where a is the lower bound and b is the upper bound. For example, the range $[0, 5]$ is represented by the range $\{0, 1, 2, 3, 4, 5\}$ where $a = 0$ and $b = 5$. More than one range could be defined and would be treated as independent factors. In Figure 3, the ranges

r_a^b, r_{b+1}^c, and r_{c+1}^d have been illustrated in order to define a possible scenario where the weight of being in the range r_a^b is greater than the weight of being in the range r_{b+1}^c. For example, the system can be configured to consider the ranges $r_0^5 = [0, 5]$, $r_6^{10} = [6, 10]$ and $r_{11}^{15} = [11, 15]$. In this situation, the employee e_a will be selected before the employee e_b if all other factors are considered equal.

Once the system is set up and employees have been enrolled, the employee receiver can begin detecting beacons. For each iteration, the receiver executes the following procedure:

1. Presumably, a set of beacons has been detected. With those signals, the receiver are able to compute its location using triangulation methods described above.
2. With the location computed, the receiver calculates its distance to nearby control points. For example, the employee e_b shown in Figure 3 should compute the distance to control points cp_a and cp_b but not with the control point cp_c if its distance is greater than the maximum distance defined in the system configuration.
3. In order to preserve privacy, the calculated distances will not be shared even in encrypted form. Instead, knowing distances to control points, the receiver calculates a NIZKR commitment for each nearby control point.
4. Each of the computed NIZKR commitment is sent to the DSS properly tagged. Figure 3 where red dots are beacons, blue triangles are control points and green squares are employees shows a possible scenario. There, the employee e_a will send the tuple $t_i = [e_a, cp_a, c_i]$ where e_a is the unique identifier of the employee, cp_a is the control point at which the proof was computed, and c_i is the NIZKR commitment. Also, this employee must submit all tuples calculated with the other nearby control points. These proofs allow the system to know that a particular employee is within a distance range of a certain control point, but without knowing the exact location of the employee.

At that point, the DSS has the ability to use the distance range as another factor in assigning activities by using the NIZKRP scheme described above to find out what range the employee is in. Table 1 includes information about other factors that the DSS could take into account for the assignment of an activity supported by the scenario illustrated in Figure 3. The score table is shown in Table 1 if the selected employee is calculated with

$$\max \left(\frac{1}{(k_P \cdot 0.4)} + \frac{1}{(t_C \cdot 0.4)} + (h_a^b \cdot 3 \cdot 0.2) + (h_{b+1}^c \cdot 2 \cdot 0.2) + (h_{c+1}^d \cdot 1 \cdot 0.2) \right).$$

Table 1. Variables table with computed score.

Employees	e_a	e_b	e_c
Number of assigned activities (k_P)	3	2	3
Time spent in completed activities (t_C)	5 h	4.5 h	4 h
Is in r_a^b range (h_a^b)	1	0	0
Is in r_{b+1}^c range (h_{b+1}^c)	0	1	0
Is in r_{c+1}^d range (h_{c+1}^d)	0	0	0
Score	1.7250	2.2055	1.4583

In this example, the selected employee is e_b even though employee e_a is closer because the distance is not the only factor that the system takes into account. However, it could be considered that the distance range contribute a higher percentage to the computation, which would imply that the employee e_a will be selected for his or her proximity. In any case, the employee e_c is not considered suitable due to his or her distance despite having worked less time than the others.
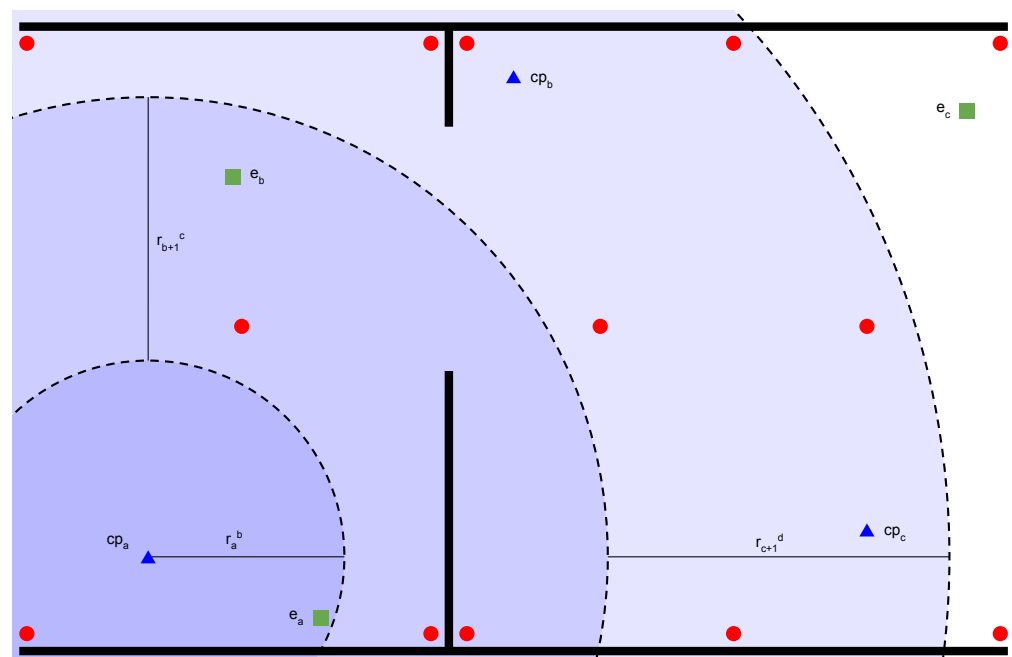
Figure 3. Example of possible scenario.

5. Conclusions

The proposed DSS is a practical solution for personnel management, focused on employee privacy thanks to the use of Non-Interactive Zero-Knowledge Range Proofs. Distance as a factor calculated by triangulating various Received Signal Strength Indicators emitted by Bluetooth Low Energy devices in combination with other influencing factors, such as completed or pending activities, priority or category, could help to correctly schedule daily activities.

From a privacy point of view, the system provides great power to avoid employee tracking even when defining small distance ranges. This is because the employee will be located in a radius around the control point and not at an exact point or a certain straight line distance from the control point. This makes it possible to prevent the system from knowing or inferring the location and therefore the employees from being monitored.

The main advantage of the proposed application is that it is able to record all activities and monitoring of the employees on a daily basis. It allows administrators to know the performance of employees, the level of success over the estimated time of routines, the control points with the highest flow of personnel, among other aspects. In addition, it is quite versatile since it is capable of adapting to various scenarios (airports, sports venues, universities ...) and situations (daily control of activities, specific events with a high number of participants ...).

As for future work, using the system in a real environment with enough staff could be useful to make corrections in the RSSI measurement as long as the errors are greater than the distance ranges defined in the system and to check the efficiency of the NIZKR proofs and its contribution as tool for privacy preserving.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Harris, H.; Brewster, C.; Sparrow, P. *International Human Resource Management*; CIPD Publishing: London, UK, 2003.
2. Legato, P.; Monaco, M.F. Human resources management at a marine container terminal. *Eur. J. Oper. Res.* **2004**, *156*, 769–781. [CrossRef]
3. Schneider, A.M.; Oppel, E.M.; Winter, V. Explaining variations in hospitals' use of strategic human resource management: How environmental and organizational factors matter. *Health Care Manag. Rev.* **2021**, *46*, 2–11. [CrossRef] [PubMed]
4. He, W.; Tan, E.L.; Lee, E.W.; Li, T.Y. A solution for integrated track and trace in supply chain based on RFID & GPS. In Proceedings of the IEEE Conference on Emerging Technologies & Factory Automation, Mallorca, Spain, 22–25 September 2009; pp. 1–6. [CrossRef]
5. Chumkamon, S.; Tuvaphanthaphiphat, P.; Keeratiwintakorn, P. A Blind Navigation System Using RFID for Indoor Environments. In Proceedings of the 5th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, Krabi, Thailand, 14–17 May 2008; pp. 765–768. [CrossRef]
6. Cantón Paterna, V.; Calveras Augé, A.; Paradells Aspas, J.; Pérez Bullones, M.A. A Bluetooth Low Energy Indoor Positioning System with Channel Diversity, Weighted Trilateration and Kalman Filtering. *Sensors* **2017**, *17*, 2927. [CrossRef] [PubMed]
7. Yang, C.; Shao, H. WiFi-based indoor positioning. *IEEE Commun. Mag.* **2015**, *53*, 150–157. [CrossRef]
8. Kriz, P.; Maly, F.; Kozel, T. Improving indoor localization using bluetooth low energy beacons. *Mob. Inf. Syst.* **2016**, *2016*, 2083094. [CrossRef]
9. Yoon, P.K.; Zihajehzadeh, S.; Kang, B.S.; Park, E.J. Adaptive Kalman filter for indoor localization using Bluetooth Low Energy and inertial measurement unit. In Proceedings of the 2015 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), Milan, Italy, 25–29 August 2015.
10. Iqbal, Z.; Luo, D.; Henry, P.; Kazemifar, S.; Rozario, T.; Yan, Y.; Westover, K.; Lu, W.; Nguyen, D.; Long, T.; et al. Accurate real time localization tracking in a clinical environment using Bluetooth Low Energy and deep learning. *PLoS ONE* **2018**, *13*, e0205392. [CrossRef] [PubMed]
11. Giuliano, R.; Cardarilli, G.C.; Cesarini, C.; Di Nunzio, L.; Fallucchi, F.; Fazzolari, R.; Mazzenga, F.; Re, M.; Vizzarri, A. Indoor localization system based on bluetooth low energy for museum applications. *Electronics* **2020**, *9*, 1055. [CrossRef]
12. Shen, H.; Bai, G.; Yang, M.; Wang, Z. Protecting trajectory privacy: A user-centric analysis. *J. Netw. Comput. Appl.* **2017**, *82*, 128–139. [CrossRef]
13. Michael, K.; McNamee, A.; Michael, M.G. The emerging ethics of humancentric GPS tracking and monitoring. In Proceedings of the IEEE International Conference on Mobile Business, Copenhagen, Denmark, 25–27 July 2006; p. 34. [CrossRef]
14. Álvarez-Díaz, N.; Caballero-Gil, P.; Reboso-Morales, H.; Martín-Fernández, F. Optimizing Resource Allocation and Indoor Location Using Bluetooth Low Energy. World Academy of Science, Engineering and Technology, Open Science Index 110. *Int. J. Comput. Inf. Eng.* **2016**, *10*, 333–336.
15. Scheerens, D. Practical indoor localization using Bluetooth. Master's Thesis, University of Twente, Enschede, The Netherlands, 2012.
16. Parameswaran, A.T.; Husain, M.I.; Upadhyaya, S. Is rssi a reliable parameter in sensor localization algorithms: An experimental study. In Proceedings of the Field Failure Data Analysis Workshop, New York, NY, USA, January 2009; Volume 5.
17. Bourke, P. Calculating the Area and Centroid of a Polygon. 1997. Available online: http://paulbourke.net/geometry/polygonmesh/ (accessed on 12 January 2021).
18. Goldwasser, S.; Micali, S.; Rackoff, C. The knowledge complexity of interactive proof systems. In Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing, Providence, RI, USA, 6–8 May 1985; pp. 291–304.
19. Blum, M.; Feldman, P.; Micali, S. Non-interactive zero-knowledge and its applications. In Proceedings of the 20th annual ACM Symposium on Theory of Computing, Chicago, IL, USA, 2–4 May 1988; pp. 103–112.
20. Peng, K.; Bao, F. An Efficient Range Proof Scheme. In Proceedings of the 2010 IEEE Second International Conference on Social Computing, Minneapolis, MN, USA, 20–22 August 2010; pp. 826–833. [CrossRef]
21. Koens, T.; Ramaekers, C.; Van Wijk, C. *Efficient Zero-Knowledge Range Proofs in Ethereum*; Technical Report; ING: Amsterdam, The Netherlands, 2018
22. Morais, E.; vanWijk, C.; Koens, T. *Zero Knowledge Set Membership*; Technical Report; ING Bank: Amsterdam, The Netherlands, 2018.