Abstract—Stationary low-power wireless networks are able to continuously monitor large areas for long periods of time. If densely deployed, they can accurately detect intruders and localise them. However, such density requires high installation and maintenance costs, and no identification of the intruders can be made. On the other side, mobile robots are able to precisely monitor areas and identify intruders when present in their field of view. Advances in multi-robot coordination allow them to cover large areas as patrolling guards. Nevertheless, they usually leave areas uncovered, and they can only work under battery-constrained time conditions. In this paper, we investigate the trade-offs in a practical hybrid surveillance system. A sparse low-power wireless network continuously monitors the environment and roughly estimates events locations, while robots resting on strategic positions wait for warning calls to survey specific areas and accurately observe the ongoing events. As a result, only a moderate accuracy is required from the stationary network, allowing a notable simplification with respect to similar localisation systems. At the same time, the robotic team size can be decreased and its coordination simplified. The on-demand activation drastically saves the energy and wear required by the continuous patrolling. In this paper, we provide an experimental analysis of such trade-offs and report on the lessons learned.

Index Terms—Surveillance, Low density wireless network, Patrolling robots, Long term monitoring

I. INTRODUCTION

The vision of the Internet of Things (IoT) is based on the embedding of intelligent monitoring in everyday scenario. The low cost of the devices and their extended lifetime allow deployments with high density of measurements and continuous availability. The resulting systems can then support long-term event detection with low response times. However, in order to provide high precision, the complexity of such systems quickly increases, making their configuration and maintenance difficult and ultimately affecting the achieved accuracy.

Complementary to low-power wireless systems, mobile robots allow to perform mobile sensing while exploring an area of interest. The sensors that they carry can also perform human identification and localisation in an accurate way, and even can differentiate between real intruders and authorized individuals. However, due to the restricted field of view, constant patrolling is required to search for events of interest, resulting in high response times. This can allow to an intruder to access a room in a short period of time without being detected. Also the constant mobility requires energy budgets that some sort of robots like drones cannot afford.

The collaboration between the two technologies creates an interesting design space where the individual strengths make it possible to outweigh the respective shortcomings. In this paper, we explore this design space with a concrete system that uses a low-power wireless network to detect the presence of an anomaly in the environment and provide a first estimate of its location. A set of robots wait for a warning call that triggers the movement of one of them. This robot then drives to the event area to identify the cause of the alarm. With respect to solutions based on an individual technology, our system requires less than half of the wireless sensor devices. Robots, on the other side, are released from their continuous patrolling duties, being used only when events are detected. This decreases drastically the size of the team while allowing the use of drones or fast robots with limited battery capacities.

In particular, our contributions are:

• The analysis of the trade-offs of the currently available solutions for indoor surveillance.
• The design of a practical hybrid system exploiting the strengths of the individual technologies.
• The identification of the challenges rising from the realization of such an hybrid solution.
• The discussion of lessons learned and research directions.

This report provides a practical, system-oriented perspective from the experimentation with a concrete prototype in a real-life scenario, demonstrating benefits and limitations.

In the rest of the paper, we discuss the literature related to surveillance systems (Section II) and present our system design (Section III). The details of the system components and some of the challenges encountered are presented in Section IV and V, followed by the report of our experimentation in an indoor scenario (Section VI). Section VII concludes the paper with a discussion of the limitations and benefits.

II. RELATED WORK

In the literature, it is possible to identify a variety of approaches related to surveillance employed in military as well as civil applications. Depending on the requirements and scenario, different technologies provide different trade-offs. In this work, we focus on the use of stationary low-power wireless networks performing localisation through the analysis of wireless signals and patrolling robots.

A. Stationary Low-Power Wireless Networks

The detection of the presence of persons in an environment is essential in a surveillance system. Among the different
possible approaches, passive localisation through wireless signals [1] has received particular attention. The underlying idea is to observe the variations in the Received Signal Strength (RSS) between two wireless devices. If the environment does not change, in fact, the feature of a wireless link should remain relatively stable. However, movements of obstacles in the Fresnel zone between sender and receiver typically cause a change in the observed RSS. As a result, by identifying such changes, it is possible to identify a movement in the environment and, with enough wireless links, localise it.

This basic technique has led to a variety of works and systems, e.g., for residential monitoring [2], outdoor surveillance [3] and waiting lines monitoring [4]. All the systems exploit the detection of RSS anomalies to realise solutions in which persons are not required to carry any device in order to be localised. A further advantage is that, e.g., with respect to camera systems, the privacy of the person is preserved as only localisation and tracking are possible, not identification.

All these approaches have the goal of increasing the accuracy to increase the reliability of the corresponding stand-alone systems. For this reason, they typically require more information to be collected, e.g., of the RSS measurements over multiple channels [5], in dense deployments. In this work, our goal is instead to minimise the system and algorithms complexity by reducing the number of required devices in the environment and the information collected from them.

B. Patrolling Robots

Due to their sensor capabilities, robots are required to perform patrolling tasks to detect intruders. The normal sizes of the areas to survey and the nominal speed of most of nowadays robots, have led to the use of multi-robots teams to accomplish this task. The coordination between robots while surveying is a challenge [6] [7]. Simple subdivisions of the area of interest can achieve optimal coverage, but can also be exposed if a single member of the team fails.

Solutions in that direction can base on graph-theory [8], where reachable places are discretised and introduced on a graph. Such a graph is analysed in order to cover it with the robots in a sequential, efficient way. The problem is that intruders can predict resulting movement patterns, giving the opportunity to perform short intrusions without being noticed.

Other solutions are achieved with direct negotiation mechanisms [9], indirect coordination [10] or other techniques based on artificial intelligence [11]. Those systems are harder to avoid, since movement pattern identification is not that simple. However, they tend to automatically split the area between the robots. When a robot fails or runs out of battery, re-adaptation times can expose whole areas for short periods of time.

In general, all the above solutions are exposed to the same weaknesses: robots have to constantly move, increasing the wear of their pieces and the requested size of their batteries; only huge teams leave no areas uncovered. The smaller is the budget, the larger is the gap between visits and the bigger is the opportunity for the intruder to access. In our system, we overcome those weaknesses by combining the detection capabilities of a stationary wireless network with a team of robots. As a result, no access remains undetected and the robots are released from the patrolling duty.

C. Hybrid Systems

The benefits of the combination of wireless low-power systems and mobile robots in hybrid systems were demonstrated in several works. In particular, mobile robots have been investigated as means to deploy sensor networks [12] or to complete them [13]. Closer to our scenario is the one of BorderSense [14], which exploits underground sensors in addition to stationary cameras to detect anomalies and dispatch unmanned vehicles to validate the alarms. Similarly [15] uses light sensors and microphones to identify deviations from the normal state and trigger the movements of a robot.

In our work, we explore a design independent of specific sensors, exploiting wireless signals already present in the environment. As a result, the detection services can use wireless devices already present in the environment, e.g., in common IoT scenarios and applications. This permits to avoid the installation of dedicated systems. Even in ad-hoc installations, our system allows for extending common sensors field of perception to the scope of wireless signals, e.g., crossing the typical limits of the walls. Finally, we experiment with a system prototype and report about our experience.

III. DESIGN

Visions such as the Internet of Things (IoT) and Cyber-Physical Systems (CPSs) are bringing a variety of devices in our everyday life to realise disparate application scenarios. At their basis, there is the possibility to exchange information and commands via wireless signals. Such signals are known to be affected by stationary as well as moving obstacles, such as persons, also if they are not carrying any signalling device. The proliferation of such devices as well as their ability to passively observe changes in their surroundings make them a good candidate to identify movements in an environment at a very low cost, also in terms of energy budget.

However, wireless signals are subject to significant variations also in case of changes not attributable to persons, e.g., as a consequence of changes in temperature [16] or interference from other devices. This can generate false triggers that cannot be verified by the system itself. A moving robot, instead, could provide extremely accurate information in its limited field of view, thanks to the rich set of sensors typically on-board. However, each operation of a robot incurs a high cost and offers a severely limited operation lifetime before recharging.

In a hybrid system, a rough localisation of undergoing events made by a stationary low-power wireless network, overlook the whole area of interest can overcome the limited scope of view of a robot. Even if the performed detection of events is inaccurate, it allows the system to avoid a continuous patrolling performed by robots and can direct them to a potential area of interest exclusively when likely needed. In this way, the number of robots required to overlook bigger
areas can be significantly decreased. Similarly, the problem of constrained operation time loses relevance.

The resulting system observes the ongoing wireless transmissions and monitors the corresponding Received Signal Strength (RSS). When a notable variation is detected, the information about the affected wireless links is used to identify the warning area in which such changes have been measured. The information is matched against a map of the environment and the information is sent in a warning call to a robot, which can then drive to the corresponding target and identify the actual cause of the change, if any. As a result, in contrast to other solutions, e.g., based on the exclusive use of cameras, we also obtain a system that can preserve the privacy of people moving in authorised spaces and times, while allowing a flexible configuration of which areas should trigger an alarm.

A. Approximate Localisation

The main task of the stationary wireless network is to monitor the features of the links that are known to be affected by the move of persons. In particular, several works have exploited the detection of RSS fluctuations to detect the presence of persons and localise them. As shown in [2], the density of devices and consequently links have a significant impact on the observed localisation accuracy. In the reported work, the system required 32 devices to achieve a root-mean-squared error of 0.23 m in a less than 60 m² environment. Such a density of nodes makes the system complex and hardly scalable. In addition, it requires a dedicated deployment as the number of wireless devices in an environment is nowadays smaller. Instead, we focus on a system that sacrifices accuracy by the move of persons. In particular, several works have exploited the detection of RSS fluctuations to detect the presence of persons and localise them. As shown in [2], the density of devices and consequently links have a significant impact on the observed localisation accuracy. In the reported work, the system required 32 devices to achieve a root-mean-squared error of 0.23 m in a less than 60 m² environment. Such a density of nodes makes the system complex and hardly scalable. In addition, it requires a dedicated deployment as the number of wireless devices in an environment is nowadays smaller. Instead, we focus on a system that sacrifices accuracy.

Considering that our first goal is only to detect where a person could be, the approach needs to essentially distinguish between the case in which a room is empty or when a person is present or moving. In particular, we are interested in detecting changes. If a person appears or moves, a warning area can be identified or updated and a robot will receive a warning call. If the person stops, the wireless network becomes blind, but the robot will still be able to catch the person. For these reasons, the variance is a more significant indicator to first identify a warning area and update it. This simplifies the computation and, considering the validation performed by the robot, allows to avoid complex learning phases, ultimately simplifying deployment, configuration and maintenance.

Once the set of links experiencing a change in RSS is identified, the information can be used to identify the warning area. In an environment with rooms, its best approximation is a room. This is, in fact, the unit that the robot can easily explore to identify possible intruders. Sending a robot to the wrong room would lead to false checks due to lack of visual contact and waste of energy in case of re-routing. For this reason, we include a majority voting scheme where nodes with multiple affected links weight more than other nodes observing fewer changes. The basic underlying idea is that links that are affected simultaneously and have one node in common define a restricted warning area where more information consistently support the indication of the presence.

B. Refined Intruder Identification

The team of robots is assumed to be waiting for warning calls. The surveillance area is subdivided according to the number of robots available. Each robot is positioned on a strategic place, with an automatic charging station that keeps it ready-to-go. With this distribution, robots are automatically in charge of responding to the warning events of their working areas. This solution avoids problems where multiple robots moving to a single target can obstruct themselves while navigating through doors or narrow corridors. The number of robots used on this application depends on the required responsiveness. The more are the robots, the smaller is the area to attend, shortening paths and response times.

Besides that, robots are still constrained by their navigation capabilities. This has to be taken into consideration when the deployment is designed. Areas can be partitioned not to just share the space with respect to the closest robot, but also to overcome natural obstacles like steps or closed doors. Once a warning call is triggered, the closest robot is automatically awakened and sent to the warning area. The main role of the robot is then to verify whether there is a false or real alarm. Considering the capabilities of nowadays robots, it is possible to foresee the use of cameras to perform such a verification.

Our configuration for the robot bases on the Robotic Operating System (ROS) [17] with its Navigation Stack [18], assuming the availability of a physical map of the environment. This map could have been created during the first deployment of the system; no big changes of furniture nor changes of the walls are assumed since then. We also assume the use of a laser ranger mounted on the robot. This device is capable of measuring obstacles, localise them on the map and, eventually, help while detecting the intruder. Finally, a camera is assumed to be part of the system, with enough resolution to allow for a visual recognition of an intruder in its field of view.

When a robot is moving, it is important to take into account that warning areas can be placed in unreachable areas for the robot (e.g., over a table) or in dangerous places (e.g., too close to a hole). In those cases the robot will never visit such areas. If that happens, the robot’s sensors should have sufficiently wide range to observe the warning area from a safe position.

C. Components Interaction

The robots exploit the stationary low-power wireless network to receive warning calls. Specifically, a dedicated device connected to a base station running ROS with a map of the environment is sufficient to bridge the two main system components. Our system considers the possibility of failing robots. This can happen due to broken power chargers or stalled processing services. In order to overcome such situations, once a robot receives a warning call, it automatically broadcasts an attendance message with the robot’s identification number and its distance to the centre of the warning area.

The wireless devices can broadcast this information in the whole network. If a device receives attendance messages from
multiple robots, it discards the ones with the largest distance. This automatically drops messages from robots far away from the warning area. If a robot receives an attendance message from a teammate with a lower distance, it automatically returns to its charging station. In this way, only the closest robot attends a warning call, hence reducing response times.

The procedure ends when an intruder is detected or the warning area is reached. If no intruder is found, a slow rotation to check the surroundings is performed. If still no intruder is detected, the warning call is identified as a false alarm. Robots are then commanded to return to their charging stations.

IV. Initial Intruder Detection

We turn now our attention to the practical realisation of the system, starting from the technical details of how the stationary wireless network detects the presence of an intruder.

To perform the RSS measurements, we employ a simple TDMA mechanism that schedules transmissions and avoids packet collisions. On the receiver side, RSS measurements are recorded and stored locally. At the next transmission, these values are reported inside the message so that any node listening can retrieve the history of RSS readings observed by the sender. This offers the flexibility to realise alternative system architectures, e.g., where all the RSS readings are collected at a central server or directly at a robot in communication range.

The RSS monitoring remains active continuously and the obtained measurements are processed based on the knowledge of which area, e.g., room, should be inspected. The selection defines which links should be kept active and triggers the identification of warning areas. The computation is performed at a coordinator in charge of gathering all the RSS measurements and performing the necessary processing to compute warning areas and send warning calls. In our current implementation, this service is programmed in Java, interacting with the stationary wireless network through standard TinyOS libraries [19] and with the robot through the ROSJava libraries [20].

To identify the affected links, we use a thresholding scheme that is adjusted based on the stability of each link in empty conditions. In particular, we identify threshold_{A→B} = k * mean_{RSS_{A→B}}, with k ∈ [0.1, 0.2] according to prior experiments. In case of frequent alarms that the robot identifies as false, this parameter can be conservatively adjusted. Furthermore, we reduce the frequency of RSS readings to a few per second in order to save energy and match the expected traffic of traditional, already deployed and operating networks.

As soon as a minimum number of links agree on a significant variation of RSS within a certain period of time, the intrusion is confirmed and a corresponding warning area is computed. Such an area is estimated by accounting for the sender and receiver positions of each involved link. The centre of that area is placed at equal distance from all the involved nodes. Then, the room where this centre is located is identified and compared against the room decided through the voting scheme described in Section III-A. If both estimations agree, then a warning call is transmitted to the robot team. Otherwise, depending on the voting, a move of the centre of the warning area is considered up to a maximum distance. If due to that update the warning area changes room, this is used as the new target. In all cases, a margin from walls and known objects is considered to avoid invalid targets for the robots.

Given that an intruder is likely to change position while a robot moves, the estimation of the actual warning area is repeated continuously. However, a new warning call is triggered exclusively if the warning area changes significantly, e.g., if there is a change of room. In fact, setting a new goal corresponds to the computation of a new path for the robot, involving significant processing power and time delays. When a new warning area is identified, this is treated as the current target but the older ones are preserved in a queue. In this way, the robot can visit rooms in reverse order of detection to search for the intruder if not found at the latest target.

V. Interaction between Network and Robots

The stationary wireless network is only capable of accurately localising intruders under dense deployments. Once that restriction is removed, the full architecture relies on the usage of robots to detect intruders or false alarms. In our case we take the chance to exploit the reliability of the multi-robot paradigm, generating a system capable of distributively determining the robot that should attend an event. Moreover, the full wireless network is used to share coordination messages between robots. This introduces the advantage of a hybrid system with double redundancy, where any of the members can fail without significantly compromising the reliability.

A. Distributed Coordinator

Any centralised solution working as a coordinator represents a strong weakness. Therefore, we placed a copy of the coordinator on each robot. This prevents our system from failing if a robot fails. Due to the characteristics of the propagation of the messages, coordinators closer to possible intrusions receive RSS updates first, being the first ones in identifying the warning area and thus dealing with the warning.

Once triggered, each coordinator commands its own robot to handle the warning call unless something prevents it. At the same time, it announces to the network its intention to check the warning area by sending a message with its robot’s id and its distance to the centre of the warning area. Any message received from the network, from another robot with a shorter path to the target, makes the coordinator cancel any action and command the robot to return to its base station.

B. Robot Manager

The robot manager deals with the information provided by the ROS Navigation Stack (in charge of the robot’s autonomous movements) and the coordinator. The system runs a state machine composed by four possible states:

1) Sleep: the robot waits for incoming events while resting and charging. Sensors and motors are off to prevent wear.
2) Preparing: if a warning area is identified, the robot computes a reachable goal close to it and returns the distance...
information to the coordinator to be broadcasted. Sensors and motors awakes to prepare for the movement.

3) Moving: after preparation, if no network information cancels the operation, the robot moves towards the selected goal while monitoring its surroundings.

4) Identifying: if during the movement a suspicious event occurs or the robot reaches the goal, the system decelerates or stops to analyse the environment. Slower movements and turns help algorithms to detect intruders. Laser rangers are more prone to detect movements and cameras are less exposed to blur effects.

5) Cancelling: if the area of interest is analysed without results, no new warning call occurs, or if the coordinator informs that another robot is handling the warning, the robot returns to its docking station to charge.

To avoid delays, the robot analyses the overlap between the warning area and its sensors’ field of view. When the latter contains the former, the robot changes to the identifying state. There are cases where the overlap is not possible due to a narrow field of view of the, e.g., camera, sensor or with a strange shape of the warning area due to corners or unusual corridors. In order to overtake them, the robot should drive until the centre of the area and perform a turn.

If the centre of the warning area is too close to a dangerous place or an unreachable one, the robot selects as a target the closest reachable position. Note that it is not necessary that the robot reaches the warning area, but only a position where the field of view of its sensors covers the target area. To perform the analysis of all situations, the maps provided by the Navigation Stack are analysed. Such maps are continuously updated with the ranger sensor information of the robot. From them it is easy to identify dangerous positions, not reachable positions or overlaps between sensors and target areas.

C. Robot Side Effects on RSS

The development and testing of the main functionalities were carried out in simulation. Despite convenient, the simulator hid the fact that the robot moving in the environment also affects the wireless links in a very similar way to the intruder. As a result, once the robot starts moving, a second warning area is identified. This not only bears the problem of creating ambiguity on which should be the target of the robot but can also decrease the accuracy of the localisation algorithm. Given that the position of the robot is known, from the links reporting a change the ones that could have been affected by the robot can be discarded. This ultimately reduces the links that can be used to localise the presence of the real intruder.

From our experimentation, we identified a clear case, depicted in Figure 1. While the intruder moves from position P1 to P2, the system correctly sets a corresponding sequence of goals (red crosses in the figure). When however the robot starts moving, the system falsely identifies that the intruder moved back, thus setting a new target goal 4 close to the first target. This effectively makes the robot move in circle.

In order to address this issue, we decided to exploit the knowledge of the current location of the robot to discard the links whose changes could be caused by the robot itself. This approach works reliably until the robot moves close to the warning area, where its movement interferes with the same links affected by the intruder. In case only an insufficient number of changed links remains, that can be attributed exclusively to the presence of the intruder, the robot stops and waits for an updated, reliable warning call.

VI. Evaluation

In this section, we evaluate the accuracy of the localisation performed with a sparse stationary wireless network and then the performance of the overall system with a moving robot.

A. Experimentation Setup

The experiments were conducted in an office environment. We focused our experiments on a section consisting of three rooms and one corridor. This is representative of one of the subsections that could be kept under surveillance by one single robot. Furthermore, the size of the area is already larger than other studies with a dedicated dense infrastructure [2] against which we can compare the achieved localisation accuracy. In comparison to the 60 m² of comparable works, our scenario, depicted in Figure 3, has an area of approximately 87 m².

In our experimentation campaign, we made use of TelosB [21] wireless sensors as reference of devices expected to be deployed in IoT scenarios. One of these devices was connected via USB to a PC to gather the RSS measurements from the network at a base station with enough resources to identify the warning area and transmit a warning call to the robot. The external usage of such a computer conveniently allowed
us to monitor and save all the information flowing through the system. As mobile robot, we employed the well-known TurtleBot 2, a state of the art robotic platform. The TurtleBot uses a Hokuyo UST-10LX laser ranger and a Microsoft Kinect RGB-D camera that in combination with its accurate odometry allows for locating itself and navigate. A second camera with a tilted angle was included for identification purposes. That camera was streamed at 1Hz and processed with a Deep Neuronal Network [22] (DNN) at a different computer (see Figure 2). TinyOS [19] and ROS Kinetic [17] with an appropriately tuned version of the Navigation Stack [18] were used to program the different functionalities of the system.

The experiments were run in the same scenario but with different configurations. As depicted in Figure 3a and Figure 3b, we tested the localisation accuracy with different subsets of nodes to understand the impact of a sparse network on the accuracy. In particular, we performed different tests with two, three, or four nodes per room. Based on the results of this initial study, we performed the final experiments involving a single robot in a scenario with three devices per room, shown in Figure 3c. The figures also indicate the tested positions of the intruder as well as the initial position of the robot $S_0$.

B. Preliminary Experimentation

We first investigate the impact of a low density of nodes on the achievable accuracy. The study in [2] reports about an ad-hoc installation made of 33 nodes in an indoor environment smaller than $60 \text{ m}^2$. With such a density, the authors were able to report a root-mean-square error of 0.23 m. A pure passive wireless localisation system needs, in fact, a high node density to achieve a good accuracy. The resulting system, however, is rather impractical and difficult to scale to bigger areas.

In our case, an estimated, inaccurate location is sufficient if it is within reasonable distance from the intruder. Furthermore, if we consider a reasonable IoT scenario, we can account for a few devices already present in indoor environments, e.g., light switches, lamps, heaters. For this reason, we experimented with scenarios involving two, three or four wireless devices per room and the deployment of devices was adapted to the room furniture at heights between 70 cm and 120 cm.

Initially, we focused on a rather simple scenario (Figure 3a) with a person standing close to one of the nodes and far away from walls dividing the rooms in the experimentation area. During the experiment, the person visited $P_1$, $P_2$, $P_3$ and $P_4$ in sequence, pausing at each of these positions for a few seconds. The experiment was repeated 10 times, producing the results shown in Figure 4. As expected, reducing the number of devices in general decreases accuracy and increases the observed variation of the results. An exception is $P_2$, where the configurations with three and four devices introduce links already overlapping with links triggered in the base case.

As a second scenario (Figure 3b), we tested the case in which the person was located farther away from individual nodes and also closer to the internal walls between rooms.
When the camera carried by the robot detects a person in its field of view, each intruder position was tested 5 times.

The results are reported in Table I. The first observation is that, even though the robot was driven directly to the right room in 80% of the cases, there are still a significant number of cases in which the final target was not reached. These cases correspond to situations in which the robot was driven to unreachable goals. By default, the coordinator uses the physical map of the environment, composed of mainly static walls, to compute the warning areas and the goals. While moving, the robot was expected to discover other obstacles like chairs or tables and report invalid goals before proceeding. In response, the coordinator was meant to compute a newer valid goal. However, it turned out that such a loop, with communication delays in between did not work fast enough, forcing the robot to enter in many cases a recovery state [23].

Moreover, the connectivity issues between the robot and the coordinator caused interruptions in the real-time tracking of the robot’s position. Therefore the coordinator could not always distinguish between the links affected by the robot and the ones affected by the intruder. This results in a poor localisation accuracy identifying a wrong warning area. This problem can be solved if the coordinator operates co-located with the robot. Aside of these, the localisation errors revealed no further differences with respect to the previous analysis.

The time to reach the final goal also highlights the problems rising from communications delays, as it is affected by the routes followed by the robot. In particular, there are several cases where the robot travels first to a wrong room and then is re-routed to the correct one. In these cases, the chances of the robot entering a safe, slow mode in order to avoid obstacles increase. Once the goal is reached, the intruder can still be at a significant distance from the robot. This depends on how the robot moves and the line of sight between the camera and the intruder, which ultimately depends on the path followed by the robot to reach the room and avoid obstacles.
VII. DISCUSSION AND CONCLUSION

We now discuss different aspects of our approach, highlighting benefits, limitations and open challenges.

Analysis of wireless signals. Despite the interference caused by the robot while moving, the overall results are promising. The method applied to recognise relevant links and ignore the ones possibly affected by the robot demonstrated to be effective in practice. Even if links are falsely considered or unnecessarily ignored, the robot can validate false alarms. This allowed us to employ 12 nodes to cover 87 m², employing a fourth of the devices needed in comparable studies [2]. This makes the system practical, scalable and allows to exploit wireless resources already present in the system.

It is also worth noting that localisation accuracy is not a primary goal as it is outweighed by the detection performed by the robot. In this sense, it is possible to avoid specific RSS monitoring schemes, e.g., to exploit channel diversity [5], and remove the need for a dedicated, potentially complex infrastructure. An interesting research direction is the analysis of the RSS measurements based on the knowledge of the environment structure and obstacles. Such information is, in fact, available (or collected while moving) at the robot and can be combined with, e.g., ray-tracing techniques to better localise a person with respect to walls and obstacles.

Coordination of robots. The experimentation confirms the feasibility of the approach and the consistent improvement in energy consumption, in particular, in comparison to a solution involving constant patrolling of robots. The operation lifetime of a robot like ours before recharging is in the order of 2-3 hours when large batteries are used, less than 20 minutes in the case of flying drones. Furthermore, while recharging, the specific drone cannot contribute to the detection. In our worst case, only 2:37 minutes were necessary for identification, after which the robot could return to the recharging station. This also offers a considerable advantage in detection delays with respect to a pure patrolling approach. Even if the placement of the coordinator on a external computer was convenient for our experimentation, the wireless communication with the robot demonstrated to be often unreliable. To overcome this problem, more computation power should be made available at the robot. Thus, not only the coordinator and the Navigation Stack but also the DNN could be executed on the robot itself.

Our first design focused on a modularised approach where the overall area to be monitored is divided in sections according to the number of available robots. Each robot is placed on a strategic position in order to easily supervise its assigned area. This offers a flexible solution with very low system, configuration and maintenance complexity that can easily scale. However, the availability of multiple robots offers a substantial opportunity for optimising the overall system efficiency and dependability. For example, while a robot moves towards a warning area, the other robots can relocate themselves in other to cover possible escaping routes. Similarly, in case of multiple warning areas and calls, the robots could plan routes and distribute the tasks to identify multiple persons moving in the same environment.

Conclusion and future work. In this work, we have demonstrated the possible synergies between mobile robots and stationary low-power wireless networks in a concrete scenario and experimented with the benefits. In particular, we studied to which extent passive localisation techniques based on wireless signals can be simplified when the presence of a person can be validated by one or multiple mobile robots. We also removed the need to have robots patrolling continuously with a significant improvement in energy savings as well as system availability and responsiveness. We currently focus on extending our experimentation to an area of around 300 m² with a density of 1 device every 10 m², further decreasing the node density and refining the analysis of wireless signal to perform the localisation. Finally, we intend to investigate the use of more robots to analyse the impact of different task assignment policies on the system responsiveness and robustness, e.g., in the case of multiple intruders.

REFERENCES