Abstract—Wireless machine-to-machine (M2M) networks are becoming a relevant topic in the field of home automation and advanced security systems. A wireless network for indoor intrusion detection is based on several sensors that are deployed over the monitored area for detecting possible risky situations and triggering appropriate actions in response. The network needs to support traffic patterns with different characteristics and quality constraints. Namely, it should provide a periodic low-power monitoring service and, in case of intrusion detection, a real-time alarm propagation mechanism over inherently unreliable wireless links subject to fluctuations of the signal power. Following the guidelines introduced by recent standardization, this paper proposes the design of a wireless network prototype able to satisfy the specifics of the intrusion detection application. A proprietary medium access control is developed based on the low-power SimpliciTI radio stack. Network performance is assessed by experimental measurements using a test-bed operating at 868MHz in an indoor office environment with severe multipath and non line-of-sight propagation conditions.

I. INTRODUCTION

Wireless machine-to-machine (M2M) technologies are gaining the attention of companies operating in the field of home automation and advanced security systems. Although most solutions currently on the market are still based on power-line or wired communications, it is expected that cable replacing will eliminate time-consuming installations [1], opening the way to more flexible services for the end-user. The general requirements of wireless intrusion detection systems are evaluated at European level through the standard EN 5013-5-3 [2] that regulates several aspects such as immunity to the variations in the channel, collisions, intentional (or not) replacement of devices and interference. It also provides specifications for link monitoring, antennas, and test procedures for the verification of these properties. For each of these items the legislation defines four classes corresponding to different levels of security.

A wireless network for home automation is composed of a number of wireless-embedded sensors and actuators (e.g., infrared, motion sensors, light switches, safety sensors, accelerometers) that intelligently share their transmission resources and interconnect with each other according to a suitable wireless architecture. As depicted in Fig. 1, a network coordinator or Access Point (AP) is responsible for starting the network, choosing and monitoring the frequency for transmission and reception, joining new End Devices (ED). ED nodes can be spread over the area of interest (typically indoor and over different floors) while communication with the AP coordinator might be guaranteed by Range Extender (RE) devices serving as decode and forward relays.

In this paper, we consider the design and implementation of an indoor wireless network for indoor surveillance and intrusion detection. The system needs to periodically record activities in the environment and provide a highly reliable connection service for alarm message propagation. Several examples of Wireless Home Automation Networks (WHAN) have been discussed in the literature. A Bluetooth WHAN has been introduced in [3] using a primary network controller and a number of sub-controllers connected by star topology. However, the wireless architecture does not completely replace cabling and the use of the Bluetooth technology shows disadvantages in terms of access delay. A ZigBee-based WHAN has been proposed in [4]. Although ZigBee interface based on the IEEE 802.15.4-2006 standard [5] provides an effective network solution for low-power wireless sensing, the overall size of the radio stack (between 45 to 100 kbyte) limits its applications to a small subset of smart home automation scenarios.

Contribution of the paper. This paper focuses on new promising wireless technologies for next-generation smart surveillance systems and presents a network design validated by experimental tests. A proprietary Medium Access Control (MAC) link-layer protocol tailored for intrusion detection has been developed on top of the SimpliciTI compliant radio stack [6] based on the ultra-low-power CC430 microcontroller System-on-Chip (SoC) with integrated sub-GHz RF trans-

Fig. 1. Floor plan map and WHAN deployment with an AP controller and 8 EDs.
ceivers and low-power MSP430 controllers [7]. SimpliciTI wireless modules use a very basic core API compared to ZigBee and thus allow for a more flexible network design. The proposed MAC sub-layer has a smaller code size (8-16kbyte) compared to the ZigBee radio stack and it allows to efficiently manage the different traffic patterns generated by the intrusion detection system, jointly exploiting both synchronized and non-synchronized access schemes. The test-bed developed for this study uses radio devices operating at 868MHz ISM band; configuration and planning of the WHAN have been carried out in an indoor environment with severe multipath and non line-of-sight (NLOS) propagation.

II. NETWORK REQUIREMENTS FOR SMART SURVEILLANCE SYSTEMS

A WHAN designed for smart surveillance and intrusion detection has many peculiarities that are common to a broader class of automatic industrial control systems [8]. The physical (PHY) layer radio characteristics that are mostly common to all these systems are low data-rate (below 500kbps), carrier frequency at 2.4GHz or in the 915MHz/868MHz ISM bands, and receiver sensitivity above $-100\text{dBm}$ [9]. Most PHY layer access schemes are based on OQPSK or FSK combined with Direct-Sequence Spread Spectrum (DSSS) transmission, as proven technologies that reduce the network susceptibility to interference, providing a few dBs of coding gain and some improvements over harsh environments characterized by multi-path fading. Multi-channel radios are also adopted to efficiently manage co-channel interference and reject any external disturbance through dynamic scheduling and channel/frequency hopping.

Basic requirements that need to be considered for the WHAN protocol design are listed in the following:

Network services. A wireless network for smart surveillance must support different classes of traffic patterns with related quality constraints. The network should provide both a periodic low-power monitoring service and a real-time alarm propagation mechanism which must be robust enough to cope with inherently unreliable wireless links characterized by signal power fluctuations. Intrusion detection systems have stricter reliability and delay requirements compared to conventional home automation services. Reliable communication occurs only if both sensor observations and feedback from the AP controller are decoded by respective parties within specified deadlines defined by the controller policy. This hard constraint calls for an advanced wireless link-layer protocol management to provide an optimal trade-off between reliability and real-time communication.

Indoor radio planning. Indoor home environments are typically characterized by severe multipath due to the presence of reflective surfaces (e.g., walls, floor, furniture) [9]. Radio planning is a useful tool which relies on the prediction of wireless link quality. Prediction can be supported by independent radio measurement campaigns over typical indoor building and/or by empirical propagation models. A low accuracy in the radio planning design phase will turn into high logistic costs: adding new wireless range extenders to improve the coverage as well as moving them around the environment may become unacceptable and highly time-consuming in some cases. For this reason, it is crucial to develop design guidelines and tools that can allow to achieve a reasonable accuracy in the prediction of the wireless coverage.

Low duty-cycling operation. Wireless autonomous devices are battery-powered: EDs are usually deployed in predefined spots and must remain active for 3-5 years. This poses stringent constraints on the sensor and radio transceiver design for minimum energy consumption. The MAC layer protocol needs to be optimized to preserve the battery. Energy harvesting techniques also provide a powerful tool for lifetime maximization. Some of the techniques employed to reduce power consumption includes: i) dynamic sleep mode activation (with fast wake-up times) to shut-down devices when not transmitting or receiving; ii) low duty-cycling design to minimize ED activity cycles. Being the network almost static, the adoption of guaranteed (interference-free) time-division multiple access (TDMA) and beacon-enabled network designs [10] are to be preferred compared to random access strategies to minimize idle listening.

III. WHAN ARCHITECTURE AND MAC DESIGN

The proposed network architecture, depicted in Fig. 1, consists of an AP and a number of REs and EDs. The AP is the network coordinator which manages a low-power radio interface for two-way communications with the remote EDs and acts as a translator over any external network. From the application layer, the AP node should guarantee the

Fig. 2. Frame structure and keep-alive message passing.
interoperability of the wireless infrastructure with other end-user operator services, i.e., portable human machine interfaces (HMI), radio-frequency identification (RFID), video-cameras or thermocameras monitoring. As a consequence, the AP should perform the following tasks: i) adaptively choose the network resources (through channel hopping and dynamic power control); ii) register new EDs (joining phase) and synchronize them to guarantee low duty-cycle activity as prescribed by the standard [2]; iii) periodically monitor the device status through standard-compliant keep-alive messages; iv) guarantee real-time alarm message propagation with minimum latency.

The RE is the device responsible for multi-hop communications. Its basic function is to repeat the message from the ED under its control to the AP and viceversa. Finally, the ED is the low power input/output wireless instrument that interacts with the sensor hardware to monitor the indoor environment and detect intrusions. Any ED should perform two functions: i) periodic transmission of keep-alive messages containing basic information on radio device status (battery residual levels, receiver sensitivity, channel quality), sensor status and tampering; ii) transmission of alarm messages within a maximum latency of \(\sim 10\)s. Periodic retransmission of keep-alive messages conforms to the standard Grade 2 [2] that prescribes a minimum refresh rate of \(20\) min.

A. Network Configuration

The network configuration phase allows to register newcomer devices. Devices have to inform the AP about the role, the type and the number of their sensors in the network. A device can join the network either with direct or indirect (through a RE) connection. A RE can join the network only with a direct connection while an ED can exploit either direct or indirect connection. In case of indirect connection the ED communicates with a RE that forwards the message to/from the AP. Routing of packets is established at the time of network configuration.

B. Frame Structure and Traffic Management

The proposed MAC sub-layer defines a proprietary frame structure that jointly handles the periodic traffic needed for monitoring the status of the sensing devices and the potential bursty traffic generated by alarm messages in case of intrusion detection. The first task is implemented through a keep-alive message exchange with dedicated channel assignments; the second one by random slotted access through Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).

The frame structure is shown in Fig. 2. Time division duplex is employed to separate uplink and downlink. Logical frames have length \(T_{\text{frame}} = 208\)s and consist of 64 time-slots of \(T_{\text{slot}} = 3.25\)s separated by guard times. The frame duration depends on the number of EDs in the network, here 64.

Periodic keep-alive message exchange session (of duration \(T_{\text{frame}}\)) starts with the transmission of the first keep-alive message from ED #1 (time slot 1) and stops with the last from ED #64 (time slot #64). Each time-slot starts with the AP beacon message that contains the identifier (Turn Information or TI) of the device that has to update its status information. The beacon message is used for device synchronization following a similar approach as in [11] (see Sec. III-D). The time-slot is further subdivided into 65 mini-slots of duration \(T = 50\)ms, the first one being reserved for keep-alive message transmission (TI Answer) of the device indicated in the beacon message (holding the turn). A two-
way explicit acknowledgement policy (see Fig. 2, left-side and TI-ACK message) is adopted to guarantee reliable message delivery over fading links. The remaining 64 mini-slots are used for synchronization operations and for alarm propagation as indicated below.

For real-time alarm delivery, any ED detecting an intrusion cannot wait its reserved mini-slot, it has to propagate the alarm message immediately after the detection. The solution here proposed is to use a random access over the above-mentioned 64 mini-slots. The ED intending to give the alarm over-hears the beacon message (even if intended for another ED) to acquire synchronization, randomly chooses one of the 64 mini-slots and uses carrier sensing before any transmission attempt to avoid cross-tier interference from external devices operating on the same frequencies (e.g., WiFi, Bluetooth). In the worst-case the overall latency of alarm message propagation is thus limited to two times the slot duration $2T_{\text{slot}} = 6.5s$. If the first alarm transmission fails due to collision, the ED waits a random period (in number of mini-slots) before retransmission. If also the second-one fails the ED checks if the AP had change channel by performing two retransmissions for each available channel until an ACK is observed.

C. Interference-aware Channel Hopping

To avoid bursty errors over consecutive polling sessions, a channel frequency hopping (CH) phase can be adaptively initiated by the AP controller. CH is commonly adopted in industrial communication as it provides increased robustness against interference and some additional protection against eavesdroppers. In the proposed system the chosen carrier frequencies are 868 MHz and 869 MHz, respectively. As shown in the message exchange example of Fig. 3, the AP continuously monitors the background noise of the radio channel and it might decide to perform a channel hopping in case of severe interference. At the first beacon signal lost, the ED programs a timer at $2T_{\text{slot}}$. If after the timer interval the ED does not receive the next beacon signal, the ED changes its working frequency accordingly. This waiting period is necessary to be sure that beacon miss-detection is not caused by a temporary interferer.

D. Duty Cycling and Device Synchronization

Device synchronization is based on the approach in [10]. A drift error compensation algorithm is developed to minimize idle listening and thus maximize the device lifetime. Each ED sleeps during the beacon transmissions intended for other devices and, excluding the alarm transmissions, it wakes-up only to reply to its intended beacon message. The chosen interval $T_{\text{frame}}$ among successive beacon messages is large compared to typical re-synchronization intervals of $10 - 15s$ [10]. Time-synchronized duty cycling is thus guaranteed by correcting and updating the sleep time $T_{\text{sleep}}$ (the time elapsed between two consecutive wake-ups) on every beacon message reception to account for the timing error experienced with the AP local oscillator. The proposed synchronization algorithm allows the ED to turn on the radio $T_g = 50ms$ before the beacon message reception, being $T_g$ a pre-defined guard time. The residual timing uncertainty after drift correction makes the observed interval $\Delta t$ between the ED wake-up and the reception of the intended beacon message to be modeled as Gaussian distributed random variable with mean $T_g = 50ms$ and with maximum jitter of $4ms$. Observed probability function (pdf) is shown in Fig. 4 at bottom. Given that the k-th beacon message is received, the ED device updates the sleep time $T_{\text{sleep}}(k)$ before the next wake-up by following a Least Mean Square (LMS) approach as

$$T_{\text{sleep}}(k) = T_{\text{sleep}}(k-1) + \mu(\Delta t_k - T_g) \quad (1)$$

where $\Delta t_k = \Delta t(k-1)$ is the observed time between the ED wake-up and the reception of k-th beacon message. Initial value for $T_{\text{sleep}}$ assumes perfect synchronization as $T_{\text{sleep}}(0) = T_{\text{frame}} - T - T_g$, updating factor $\mu$ is chosen here as $\mu = 1/2$. As demonstrated in the experimental activity (see Sec. IV), a larger guard time ($T_g > 50ms$) would cause unnecessary idle listening and higher energy consumption.

The LMS tracking algorithm (1) can be applied when the intended k-th beacon message is correctly received: in Fig 4-top this scenario is referred to as Case 1. Case 2 refers instead to a scenario where the ED loses the beacon transmission due to a radio interference or a residual clock drift that delays its wake-up. In this case the LMS tracking is not applied while an ad-hoc re-synchronization policy is implemented. The ED stays awake to receive the next beacon transmission (intended for ED holding the next turn). Next, to avoid interference with the transmission of the ED indicated in the beacon, it sends the keep-alive message using a reserved mini-slot chosen among the available 64 mini-slots that follows the first mini-slot reserved for keep-alive message exchange\(^1\) (see framing structure in Fig. 2).

E. Dynamic Transmission Power Allocation

A dynamic transmission power control algorithm is implemented to minimize the energy expenditure during periodic keep-alive message transmission. For each ED the AP controller measures the received signal strength indicator (RSSI) from the received TI ACKnowledge message and thus sent back to the corresponding ED. The ED uses this information to adapt the transmit power level $P_T$ for the next keep alive message transmission. The goal of the power control algorithm is to adaptively adjust the power level $P_T$, so that the RSSI measurement $\Gamma$ can be kept below a maximum threshold $\Gamma_{\text{max}}$ and above a minimum threshold $\Gamma_{\text{min}}$. The threshold used during the experimental activity (Sect. IV) are $\Gamma_{\text{max}} = -20dBm$ and $\Gamma_{\text{min}} = -70dBm$.

F. Encryption

To improve the security level all the transmissions are coded with the XTEA encoding scheme [12]. It is composed by three main elements which are a 128-bit encryption key, a 32-bit initialization vector and a 32-bit counter. The initialization

\(^1\)Reserved mini-slot for re-synchronization is assigned during the network configuration phase.
vector and the encryption key are set at built-time while the counter value is determined at the time of the link creation between two or more devices. Devices that have formed the link preserve independent counters.

IV. EXPERIMENTAL ACTIVITY AND RESULTS

Wireless modules used for test-bed and experimental activity are part of the EM430F6137RF900 Texas Instrument kit with integrated System-On-Chip RF XCC430F6137IRGC. Key feature of the SOC are the follows: i) energy consumption from data-sheet is characterized by a RX absorbed current of 15mA, while TX current is 33 mA for \( P_T = 12 \text{dBm} \) (max. RF transmit power); ii) radio transceiver module is CC1101 with minimum sensitivity \(-111 \text{dBm}\), data-rate 500 kbit/s and 2-FSK as RF modulation; iii) microcontroller (MCU) core is MSP430 with AES compliant coprocessor, flash memory is 32 kB, RAM 4 kB, ADC 12bit. Experimental activity has been conducted in an indoor environment consisting of 8 adjacent rooms. A single wireless ED was deployed in each room to monitor the surrounding area. People were moving inside each room causing random fluctuations of radio signals. For all devices the antenna height from ground was below 1m. Propagation took place over an harsh radio environment with metallic objects (e.g., coaxial cabling, monitors/PCs, tubes for air conditioning, etc.) and furniture causing additional attenuation.

A. Analysis of network lifetime

Figure 5 shows the energy consumption profile of a battery-equipped ED during a normal cycle of remote control. Measurements were obtained through an oscilloscope connected in parallel with the node itself. The absorbed current has been observed during five different phases: the wake-up period (approx. 10mA), the beacon message reception (23mA), the state message transmission (40mA), the acknowledge reception (24mA) and the sleep mode (8μA). To avoid the high background noise of the oscilloscope, the absorbed current during the sleep period was measured by a precision ammeter. Values measured during reception and sleep mode differ from the declared power consumptions, respectively 15mA and 5μA. In sleep mode, the difference is due to the consumption of the wake-up timer not considered in the data-sheet.

In Fig. 5, the impact of the alarm transmission rate (expressed in average number of alarm messages per hour) and of the choice for the guard time on the expected lifetime of ED nodes are analyzed. We considered two cases: in the first one drift compensation is employed according to the specifics of the proposed MAC sub-layer with guaranteed guard-time of \( T_g = 50 \text{ms} \) can be estimated to 9 years using a commercial 1.4Ah lithium battery. In Fig. 5, the resulting values of RSSI average and standard deviation

\[
\begin{align*}
\text{RSSI average} & = \mu \\
\text{RSSI standard deviation} & = \sigma
\end{align*}
\]

for air conditioning, etc.) and furniture causing additional attenuation.

B. Channel measurements and network planning

In this section, we analyze the impact of radio propagation at 868 MHz on the wireless alarm message delivery. For the experimental activity we used 8 EDs deployed in different rooms and one AP controller. The effects of propagation in each office room has been characterized by calculating the average and the standard deviation of the RSSI samples measured over each AP-ED link. The radio environment has been observed over a period of 48 hours during which the position of the AP was fixed while the EDs were moved in two different locations in each room on every 24 hours of operation. To highlight the impact of channel fluctuations transmit power is here fixed to \( P_T = 12 \text{dBm} \) while dynamic power allocation is disabled.

The resulting values of RSSI average and standard deviation are shown in Fig. 6 and Fig. 7, respectively. From the comparison between daytime (top sub-figure) and night (bottom sub-
(figure) it is easy to notice that although the observed average RSSI does not change significantly from daytime to night, the standard deviation is strongly influenced by the presence of people in the propagation environment (during daytime [13]). The behavior of channel fluctuations is thus non-stationary as the standard deviation in some rooms is shown to increase from about 0dB during the night to more than 4dB during daytime. As also observed in [14], this suggests to dynamically increase transmit power during daytime by adding a 4dB constant fade margin to compensate for the random signal strength fluctuations. During night, transmit power can be instead decreased by 4dB on average.

V. CONCLUDING REMARKS

In this paper a proprietary MAC link-layer protocol tailored for smart surveillance and intrusion detection applications has been developed on top of the SimpliciTI compliant radio stack [6] using the ultra-low-power CC430 microcontroller [7]. The proposed protocol uses a very basic core API compared to ZigBee, allowing for a more flexible network design. The medium access scheme has been designed to jointly exploit both scheduled and random access to guarantee low-power periodic keep-alive message exchange and real-time alarm propagation with minimum latency, respectively. The analysis of battery consumption proved that low-power duty cycling can guarantee a lifetime of several years. Network planning in an indoor environment and power control are also discussed.

REFERENCES