

Access provided by:
Universidad Nacional de Colombia
(UNAL)
Sign Out

Browse

My Settings

Get Help

Advertisement

Browse Journals & Magazines > IEEE Transactions on Mobile C... > Volume: 16 Issue: 5

An RFID Based Smartphone Proximity Absence Alert System

<< Results | Next >

3

Muhammad Jawad Hussain ; Li Lu ; Shan Gao

Author(s)

View All Authors

1

Paper

Citation

898

Full

Text Views

Export

to

Print

Collabratec

Alerts

Manage

Content

Alerts

Add to

Citation

Alerts

Related Articles

Batteries for low power electronics
Proceedings of the IEEE
Published: 1995

A Healthcare Integration System for Disease Assessment and Safety Monitoring of Dementia Patients
IEEE Transactions on Information Technology in Biomedicine
Published: 2008

View All View More

See the top organizations patenting in technologies mentioned in this article

ORGANIZATION 4

ORGANIZATION 3

ORGANIZATION 2

ORGANIZATION 1

Click to Expand

Provided by: InnovationQ PLUS
POWERED BY IEEE AND IP.COM
A PATENT SEARCH AND ANALYTICS TOOL

Related Articles

Batteries for low power electronics
Proceedings of the IEEE
Published: 1995

A Healthcare Integration System for Disease Assessment and Safety Monitoring of Dementia Patients
IEEE Transactions on Information Technology in Biomedicine
Published: 2008

View All View More

See the top organizations patenting in technologies mentioned in this article

ORGANIZATION 4

ORGANIZATION 3

ORGANIZATION 2

ORGANIZATION 1

Click to Expand

Provided by: InnovationQ PLUS
POWERED BY IEEE AND IP.COM
A PATENT SEARCH AND ANALYTICS TOOL

Advertisement

See the top organizations patenting in technologies mentioned in this article

ORGANIZATION 4

ORGANIZATION 3

ORGANIZATION 2

ORGANIZATION 1

Click to Expand

Provided by: InnovationQ PLUS
POWERED BY IEEE AND IP.COM
A PATENT SEARCH AND ANALYTICS TOOL

Advertisement

Abstract

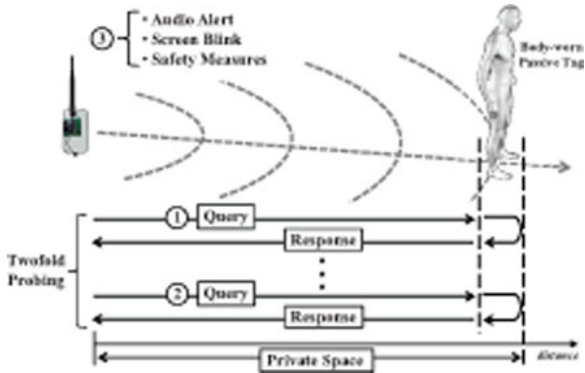
Document Sections

1 Introduction

Loading web-font TeX/Main/Regular

2 Related Work
3 System Design
4 System Evaluation
5 Proposed Embedded Reader Modules

Show Full Outline	☐
Authors	
Figures	
References	
Citations	
Keywords	
Metrics	
Related Articles	



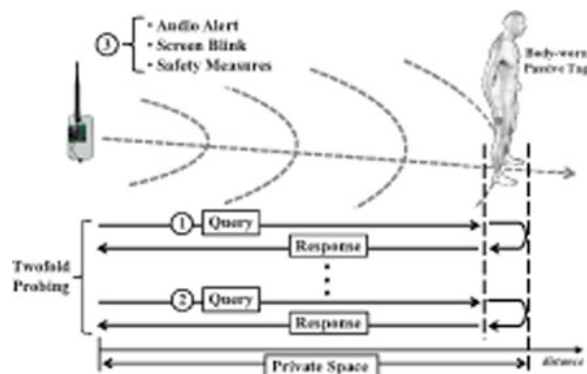
Abstract: We present the design, implementation, and evaluation of an RFID-based cellphone anti-lost and anti-theft measure. The cellphone owner is given an audio-visual alert at t... [View more](#)

Metadata

Abstract: We present the design, implementation, and evaluation of an RFID-based cellphone anti-lost and anti-theft measure. The cellphone owner is given an audio-visual alert at the very instant of the lost event, and the cellphone deduces the fact that it is away from its owner and executes the safety measures. This is realized by equipping the cellphone with a low-power RFID Reader and tagging the owner with a passive RFID token to determine a private space around him, which spans within 2-10 feet. We prototype an RFID Reader from discrete components under \$60 which can transmit 30 dBm with -78 dBm sensitivity, and can also serve as an educational tool for academic learning. Our system works on automatic, timed, or accelerometer based thresholds. We interface our system with Samsung Galaxy Note2 and develop an Android User Interface. We carry out extensive indoor and outdoor experiments under static and dynamic scenarios to ascertain the Frontal and Angular ranges, energy and power consumption, and memory and computational overheads. Our salient contribution is a twofold probing scheme-a duty cycle approach that economizes battery overhead, mitigates false alarms and scans the tag for multiple times by leveraging the interrogation time and power. We argue that though our design is costly in power budget, it is highly economical on battery energy because of short interrogation cycles. We show that for 17 tag interrogations from 20-24 dBm, our scheme consumes 72.1 to 52.4 percent lower energy than a single Bluetooth device scan. For a fully embedded design, we propose System-on-Chip RFID solutions. We foresee our endeavor as a viable proximity absence detection scheme for short range applications and scenarios.

Published in: IEEE Transactions on Mobile Computing (Volume: 16 , Issue: 5 , May 1 2017)

Page(s): 1246 - 1257	INSPEC Accession Number: 16824221
Date of Publication: 14 July 2016	DOI: 10.1109/TMC.2016.2591524
ISSN Information:	Publisher: IEEE
	Sponsored by: IEEE Computer Society
	Funding Agency:


[Hide Full Abstract](#)

Advertisement

Contents

SECTION 1 Introduction

In recent past, the smartphone lost and theft cases have emerged as a serious concern not only to individuals but also at official echelons, notably the Secure-our-Smartphones (S.O.S) initiative and the term “Apple Picking” introduced by US officials for theft cases of iDevices [1], [2]. During 2014 alone, the lost and stolen cellphones amount to 30\$ billion whereby 1.6 million people lost their cellphones and roughly 113 smartphones were lost or stolen each minute [2]. To circumvent, we observe two surfacing solutions in shape of Activation Lock by Apple Inc. [3] and Kill Switch by Samsung Electronics [4]. Both make it hard to use or re-sell the cellphone by requiring the owner’s ID and password for its operation, and device can be remotely erased and locked if it has active data connection (e.g., Wi-Fi, 3G/4G). However, the owner becomes aware of the lost or theft incident only once he intends to use the phone, i.e., no indication is rendered at the very occurrence of the lost event. Moreover, the cellphone can be remotely locked or erased only if it is connected to wireless network.

Our research relies on an endeavor to take the security measures at the very instance a cellphone is lost. Since, a cellphone can be housed inside pocket, bag, table, car dashboard and else, therefore, we deem it more appropriate to devise a proximity based absence alert mechanism which monitors the presence of cellphone in close proximity of the user and generates an alert once it falls outside this vicinity, which we term as *private space*. Such security mechanism offers three benefits: 1) The owner is notified at the instant he loses the cellphone rather than he learns the fact and takes measures afterwards. 2) The cellphone also gets an indication that it is outside the private space of the owner, and automatically adopts the protection measures. 3) A self-sustained solution which does not depend upon active data connection or third party support.

This brings us to the next question: how to formulate such mechanism in present-day smartphones? At one side, we observe plethora of anti-lost measures based upon GPS, GSM, Wi-Fi, Bluetooth and else; which involve Triangulation, Trilateration, Multilateration, Angle of Arrival and Signal Strength [5], [6], [7]. However, such solutions are not widely practiced because of limited coverage or stringent requirements like third party support, pre-mapped data, multiple base stations, specialized beacons, or the data connection. Though Bluetooth offers complete communication autonomy, we argue that our RFID-based

system is more economical in energy budget and used tags are fully passive unlike battery assisted Bluetooth tokens. We observe that a security measure should be host-independent, i.e., works indoors and outdoors without data connectivity constraints and third party support; it should be budget friendly and should not drain the memory, computational as well as energy resources of the cellphone.

We employ the key principle of short range off-body communication whereby cellphone estimates its position with reference to human body. Our system consists of a low-power RFID Reader interfaced with smartphone and a passive RFID tag attached to the user. The RFID protocol is executed in embedded hardware for computational liberty. The user can control its operation through an Android Interface and can select the profiles, transmission power, and various functions related to passive tag like managing, activating and disabling the tag IDs. The tag can be interfaced to user in variety of ways, like pasted on the name-tag, bracelet or watch, tied to key-chain or kept in the pocket. The Reader searches for tagged owner on various profiles depending upon automatic, time or accelerometer based thresholds. Beyond private space, the Reader cannot interrogate the tag and cellphone moves into protection mode to perform pre-programmed measures (Fig. 1).

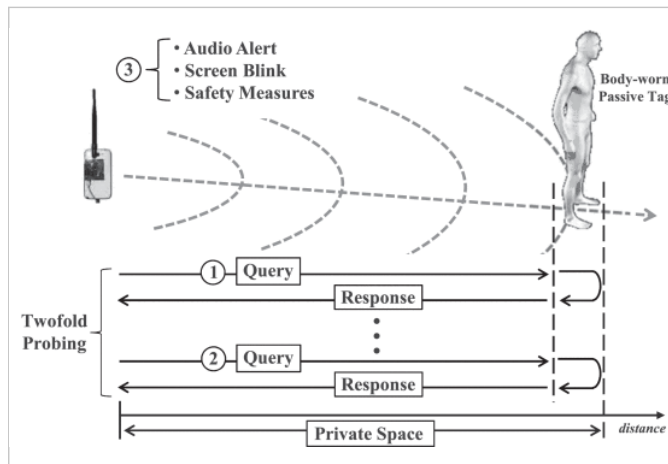


Fig. 1.

Proposed scheme. Step-1: Reader queries the tag for three consecutive times upon time or accelerometer thresholds. Step-2: if the tag is not found, the Reader leverages its transmission power to scan the tag for 14-79 times within 4.5-7 sec. Step-3: if the tag is still not found, the cellphone adopts two kinds of pre-programmed safety measures: 1) Alerting the owner through specific audio or blinking its screen. 2) Sending specific SMS, locking the phone, erasing specific contents, etc.

We perform extensive indoor/outdoor evaluation for following parameters: Frontal and Angular ranges under static evaluation; response time, average detection rate and false negatives under dynamic uncontrolled experiments; transmission power versus maximum read distance; multiple tags scenario; and overhead to smartphone's computational, memory and energy resources. We leverage transmission power from 20-24 dBm which results to a private space of 2-10 feet. We simulate Pickpocketing and Cellphone Fall scenarios for Solo evaluation (tagged owner with the cellphone) and Accompanied evaluation (both surrounded by five people). We follow an experimental approach to devise a duty cycle approach, twofold probing scheme, that mitigates the intermittent tag responses due to multipath, shadowing, body postures and non-coherent receiver. It also economizes the overall energy budget while benefitting from short interrogation operations of EPC protocol. An in-depth analysis shows that our system is light-weight on cellphone battery once compared with onboard sensors like accelerometer

battery, and compared with onboard sensors like accelerometer, camera, microphone and communication interfaces like GPS, Wi-Fi and Bluetooth.

Our system has four salient attributes: communication autonomy; energy efficiency; fully passive wearable tags; low-cost. Besides anti-lost solution, we envision our design to be a good reference for academic learning and experimentation. We implement RFID protocol in a microcontroller and design the Reader from commercial-off-the-shelf (COTS) components within a budget of \$60, excluding the PCB and the antenna cost. It can deliver +30 dBm power with -78 dBm receiver sensitivity, and covers the global UHF RFID band from 860-960 MHz. Therefore, it can also be used as a low-cost mobile RFID terminal.

Followings are major limitations of our design: 1) For energy, cost and processing simplicity, the Reader is designed on the topology of a homodyne receiver which can only interrogate ASK backscatter tags. 2) Tag is not read once the backscattered phase is orthogonal to the Reader's phase, which we overcome by twofold probing scheme. Lastly, as the smartphones lack the RFID interface, we propose System-on-Chip (SoC) solutions for an embedded design. Also, some users may not remember to wear the tag therefore we propose the tag to be coupled with wrist watch or bracelet, wallet or the ID card.

Rest of the paper is organized as follows: Related works are discussed in Section 2. We explain our design in Section 3 followed by evaluation results in Section 4 with relation to various performance parameters. We propose low-power Reader modules for an embedded smartphone-based solution in Section 5 followed by the Conclusion.

SECTION 2 Related Work

2.1 Anti-Lost Solutions via Short Range Wireless Communications

Though Near Field Communication (NFC) is an integral part of smartphones and NFC tags are fully passive tokens, it covers up to 20 cm with 4-5 cm being the typical distance [8]. Anti-theft solutions based upon Zigbee are also available [9], but present-day cellphones lack this interface and Zigbee tokens are battery operated devices [10]. Amongst WPANs, we find plenty of Bluetooth based anti-lost solutions ranging from 5 to \$30 [11], [12]. The typical range extends to 10 m which can be decreased by low-cost attenuator [13], [14]. Such solutions are also coupled with smartwatches [15]. However, it uses battery assisted tokens with higher energy overhead as compared to our system.

The fully passive Electronic Article Surveillance (EAS) tags are widely used in supermarkets for anti-shoplifting. It uses one-bit tags [16] which will result in false alarms. Also, the smartphones do not have the integrated EAS Readers. Lastly, we do not consider cellular (GSM/CDMA etc.) and WLAN technologies because the communication autonomy is not available in cellular solutions, and power budget for compatible tags is too high in both cases.

2.2 RFID Schemes as Anti-Lost Solution

We find only few relevant UHF RFID systems because of small

we find only few relevant UHF RFID systems because of small interrogation range and tag's dependence upon host for communication and power [17], [18], [19]. In [20], tags are attached to valuables like documents, pets etc. which can be located by third party tracking units. In [21], the RFID Reader gives an alert if a dental fixture retrofitted with RFID tag is missing. A campus security system is demonstrated in [22] based upon RFID and Zigbee. The Libera RFID Library System uses UHF RFID tags [23]. Within Wireless Body Area Network (WBAN), the off-body communication can be used to locate people inside the buildings equipped with fixed Readers [24] or disseminated tags [25]. TagMobile uses active and passive tags for location and tracking [26].

2.3 Reader Design and Integration with Smartphone

To best of our knowledge, we find only one smartphone based Reader design as an integrated solution which is developed as a low-cost and low-power mobile RFID terminal [27]. The Reader is integrated inside smartphone housing as a "functional cover", transmission power is up to 20 dBm, read range extends till 50 cm and design does not offer any flexibility in customizing the Reader operation [28]. Another microcontroller based design is presented in [29] which costs under \$40. However, its read range is limited to 15 cm.

SECTION 3 System Design

The design challenges include: 1) Reader Design: hardware design for a computational and energy efficient solution, and the bare-metal firmware design for EPC-C1G2 protocol in MCU. 2) Practical Realization: mitigating false alarms through a two-fold probing scheme. Since, this paper primarily relates to an application scenario, therefore, we will briefly present the Reader design and mainly focus on our anti-lost scheme in two aspects: 1) Mitigating false alarms by multipath, body shadowing and non-coherent receiver design. 2) Realizing an optimized Android system in terms of computation, memory, power consumption and cost. Our prototyped system is shown in Fig. 2 and explained next.

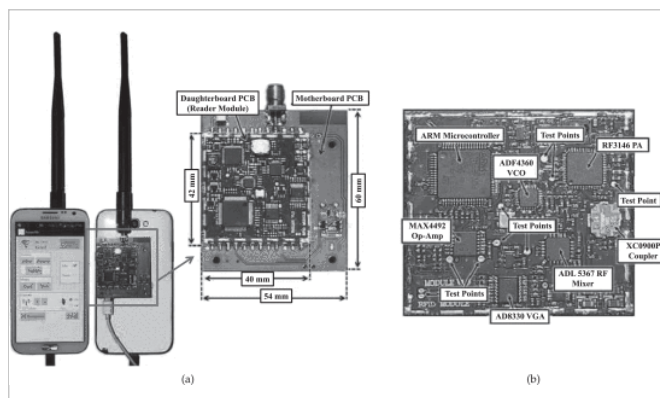


Fig. 2. Prototype consists of a low-power RFID Reader interfaced with smartphone through USB interface. It is equipped with an omni-directional antenna and attached at back side of the cellphone for evaluation. (a) Reader interfaced with Smartphone. (b) Reader Module.

3.1 Android Interface

The main panel of Android User Interface, SecureMe, is shown in

Fig. 3a from where the user can select the Profiles, leverage the transmission power and enable or disable the accelerometer support for a quick operation. The user can customize the overall operation through three sub-panels. The user can add new tag IDs to scan list, delete specific IDs in case a tag is lost or damaged, or can disable a tag under *Tag ID* Panel. The Reader's scan operation can be set according to time or accelerometer based thresholds (or combination of both) under *Threshold Selection* Panel. System can also be configured for automatic threshold operation. Under *Actions* Panel, the user can define measures taken by the smartphone in case the tag is not identified. As overall, the system works in Check and Track Modes. The Track Mode is used for rapid scanning while the Check Mode operates on Office, Outdoor and Custom Profiles.

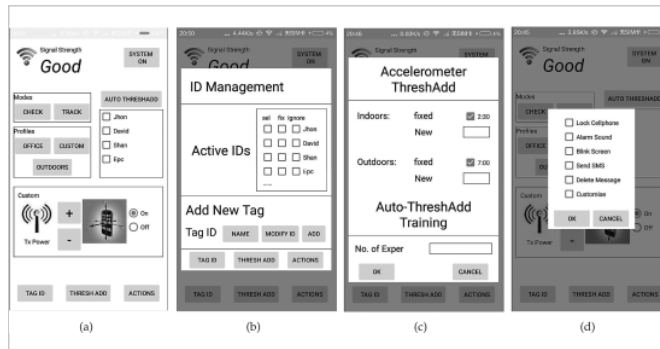


Fig. 3. Android User Interface. (a) GUI main Panel. (b) Tag ID Panel. (c) Threshold Panel. (d) Actions panel.

3.2 Operational Modes

The Check Mode is the routine mode in which a single tag search consists of three consecutive interrogations. A tag is declared to be identified if its unique Tag-ID (TID) is read. For *Outdoor Profile*, accelerometer threshold is set to 7.0 and time threshold is 10 sec. For *Office Profile*, the default time and accelerometer thresholds are set to 60 sec and 2.30. In both modes, the default transmission power is set to 22 dBm which can be leveraged between 20-24 dBm. A user can define the *Custom Profile* within 20-24 dBm transmission power, and 5 sec to 10 min of scan time.

The Track Mode can be thought of a rapid scan mode. The system enters into Track Mode upon any of two conditions: 1) If Reader cannot identify the tag under any Profile in Check Mode. 2) The user intentionally wants to have a rapid scan against viable theft or lost threat. Importantly, this mode is independent of Profile and threshold settings.

Track Mode uses a *twofold probing* scheme, which is a duty cycle approach. The main idea is to scan the tag multiple times in conjunction with overall energy budget as well as to mitigate the false alarms against shadowing, multipath, body gestures and “nulls” at the Mixer because of backscatter phase rotation. In first segment (Segment-1), the Reader scans the tag at 1.25, 2.5, and 3.75 sec intervals, whereby each scan comprises of three consecutive tag searches. If not identified, it switches to Segment-2 which is a rapid search for next 0.5-7 sec (user selectable) at intervals of 500 msec. The transmission power is swept from 20-24 dBm. So, there are 10 tag searches per second. As per our Reader settings (Q value set to 5), an interrogation cycle in EPC protocol takes about 7-26 msec which

results the Reader to search the tag within 130 msec and then go in idle mode for next 370 msec. In essence, for $t=0.5-7$ sec, a tag is searched for $14-79$ times: 3×3 times in Segment-1 (fixed intervals) and $10 \times t$ in Segment-2 (user selectable intervals). If the tag is still not identified, the cellphone adopts the pre-defined security measures.

3.3 Design of Reader Module

3.3.1 Microcontroller Unit (MCU)

The microcontroller (STM32F103RC by STMicroelectronics) implements the complete RFID protocol. We use a single ADC in the receiver and a DAC in the transmitter chain. The MCU receives the user specified parameters from Android application and executes them in hardware. At transmitter's end, it generates frequency tuning word (FTW) to tune the oscillator and outputs the precise voltage from on-chip DAC to control the gain of power amplifier (PA) from 20-24 dBm. At receiver's end, the baseband signal is fed to internal ADC for digitization and decoding the tag's reply.

3.3.2 Transmitter Unit

The UHF RFID signals are generated by ADF4360-3 which is an integrated synthesizer and Voltage Controlled Oscillator (VCO) by Analog Devices for GSM band frequencies. We use VCO in divide-by-two option to generate 800-975 MHz signals which covers the global UHF RFID frequency band from 860-960 MHz. The VCO receives FTWs from the MCU through a three-wire SPI interface and outputs the synthesized signal at -3 dBm. We directly modulate VCO to generate the RFID signals. We follow the timings of *Tari* (pulse widths of logical one and zero under EPC protocol) and switch the VCO to ON and OFF to perform On-Off-Keying (OOK modulation) to generate the RFID signals [30], [31]. This way, we perform encoding and modulation through a VCO. Another advantage of ADF4360-3 is that it outputs an identical copy of the synthesized signal as "Secondary RF" which is fed to RF Mixer in receiver. Fig. 4a shows the modulated signals at VCO output.

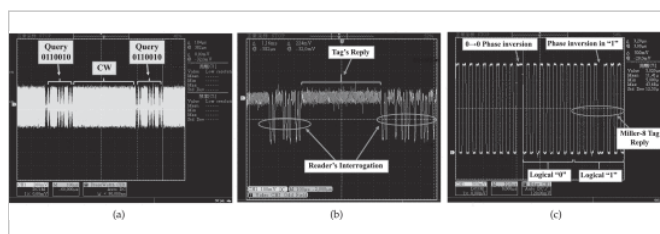


Fig. 4. RFID signals in Reader Module. (a) Query command at VCO output. (b) Received tag reply. (c) Miller-8 tag's reply at mixer output.

The passband signals are amplified by RF3146 by RF MicroDevices (RFMD) which is a GSM power amplifier for portable battery devices and integrates three cascaded amplifiers on the chip. The precise voltage from MCU's DAC feeds the gain control pin of PA which tailors the gain from 0 to 30 dBs in 1 dB steps. The internal power control circuitry ensures that output is continuously calibrated which liberates us from implementing the external transmit signal strength indication (TSSI) circuit. The PA is internally matched to 50Ω and its load VSWR is 10:1 which offers high sustainability in case the output stage is mismatched like antenna held in hand, broken RF cable or no antenna attached. The output of PA is fed to antenna through a 10 dB directional Coupler, XCO900P by Anaren.

3.3.3 Receiver Unit

The received signals are passed to double-balanced Mixer ADI 5267

The received signals are passed to double balanced mixer, AD8330 by Analog Devices. The Mixer takes its LO input from the VCO and works like a demodulator to output the FMO or Miller encoded tag's reply. The use of double-balanced topology offers high isolation between RF, LO and IF ports and its IF response extends down to DC. We also check the sensitivity of our system by introducing a variable attenuator at the Mixer's input and varying the RF input, which comes out to be -78 dBm. For coherent down-conversion with only one channel, the tag signal will fade in and out due to changes in the carrier phase because of tag's motion or dynamic multipath [32]. At worst, it will result to nulls at Mixer's output. The commercial Readers use I/Q demodulators to avoid losing the tag under such scenarios. We address this issue by twofold probing scheme as explained earlier. Fig. 4 shows the RF and baseband tag's data at the input and output of the Mixer.

The baseband signals are amplified through a Variable Gain Amplifier (VGA, AD8330 by Analog Devices) which is used for pre-ADC signal conditioning and can offer a maximum gain of 50 dBs. The output of VGA is further amplified and converted to fine-grained digital waveforms by an Operational Amplifier (Op-Amp, MAX4492 by Maxim) which can deliver up to 60 dB gain. Finally, the signals are fed to ADC in MCU for decoding the tag's reply.

3.4 Tag Considerations and Implementation

Within WBAN, our scenario comes under *Off-body Communication* in which a tag is pasted on human body and its performance is evaluated through external Reader [33], [34]. As human body is lossy and conducting in nature, electromagnetic emissions are scattered, diffracted and absorbed depending upon body properties and postures [35], [36]. Resultantly, the performance of RFID tags is seriously degraded and antenna's impedance, radiation pattern and realized gain are changed. As user can move around the cellphone in any direction or can adopt various postures (like standing, sitting, bending etc.), an antenna with omnidirectional pattern is required. We use a commercial body wearable tag with dipole antenna that costs \$0.94 [37].

The tag can be pasted at various locations of human body like chest, arm, belt, back, shoulders, ankle etc. In [35], it is shown that chest, belt and hand placements give 5.7, 5.3 and 3 m ranges, respectively. For chest placement, the tag would only provide the coverage at front side which can be mitigated by putting another tag at the back. We benefit from the findings of these evaluations and test our system by pasting a body-wearable tag at chest location (for scenarios like tag placed on chest pocket, attached to ID card, hung around the neck), and, at wrist position (like pasted on smartwatch, bracelet etc.).

3.5 Accelerometer Threshold

A user can choose predefined and fixed, or automatic accelerometer threshold. For fixed threshold for Office Profile, Fig. 5a shows the readings once the cellphone is picked up from the table, held and operated in hand and placed back. We perform ten experiments involving five volunteers. At each sampling time t , we use the accelerometer readings to measure the euclidean Norm or euclidean length, $d_t = (x_t, y_t, z_t)$. The threshold P is given by averaging d_t from all five volunteers for ten experiments ($N=10$) as

$$\begin{equation} D_{\text{avg}}(t) = \frac{1}{N} \sum_{i=1}^N ||d_t|| = \frac{1}{N} \sum_{i=1}^N \sum_{t=1}^T \left(\sqrt{x_t^2 + y_t^2 + z_t^2} \right). \end{equation}$$

The threshold for Office Profile comes out to be 2.30. Similarly, for Outdoor Profile, we consider the event once the cellphone is taken out from the pocket while each of the five volunteers follow the course shown in Fig. 5b. Since accelerometer readings are diverse and higher, we find the best suited threshold of 7.00 for Outdoor Profile.

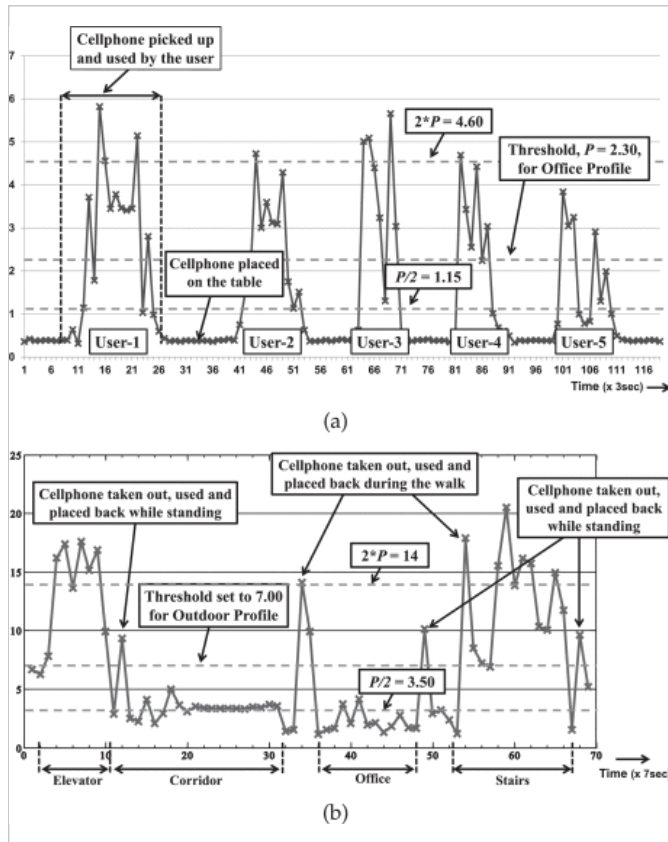


Fig. 5. Accelerometer threshold. (a) Office Profile. (b) Outdoor Profile.

For Automatic Threshold, the new accelerometer values are recorded and threshold is calculated in a following manner: if new threshold N_1 falls within $P/2 \leq N_1 \leq 2^*P$ (Fig. 5), then new threshold $P^{\prime}$ is calculated as the mean of P and N_1 . If N_1 falls outside these bounds, the user is asked to run at least three more tests. The new threshold will be the mean of N_1 and next three values, N_2 , N_3 and N_4 which fall within $N_1/2 \leq N_i \leq 2^*N_1$. For such case, user can choose to perform 5 to 15 new experiments. In case the user selects the Automatic Threshold option in the main Panel, the system will keep updating the threshold in intervals of 3 minutes whenever accelerometer values are detected.

3.6 Limitations

We conceive our system as an *application specific design* which has following limitations:

- Reader can only interrogate ASK backscatter tags because of non-coherent receiver.
- We do not implement RSSI functionality. For calibration of output power, TSSI is employed through internal power control circuitry of PA.
- The receiver does not perform I/Q processing which results to “nulls” at Mixer’s output once the phase of backscatter signal becomes orthogonal to VCO’s output, which is the key limitation of all non-coherent receivers. We circumvent this through a twofold probing scheme whereby our system scans the tag at least 17 times before declaring it absent.
- The Reader will have varying degree of sensitivity based upon mutual Reader-tag distance, multipath and relative motion. We overcome this shortcoming by twofold probing scheme which scans the tag multiple times within few seconds.
- The hardware debugging and signal analysis cannot be performed through the firmware. We use lab equipment like Oscilloscope and Spectrum Analyzer for this purpose.
- As present-day smartphones lack the RFID interface, we recommend fully embedded SoC RFID solutions for an embedded design in Section 5.

SECTION 4

System Evaluation

The evaluation aims for the following: 1) Frontal and Angular interrogation ranges for *static* environment. 2) Maximum read range for *dynamic* uncontrolled environment. We also calculate average response time, tag detection rate and False Negatives. 3) Interrogation range over varying transmission power. 4) System performance under multiple tag scenario. 5) Computation, runtime memory and energy overhead.

We rigorously check our system at open place, corridor and office locations. The system is tested against *Pickpocketing* which is simulated by a second volunteer holding the cellphone in hand, and *Cellphone Fall Scenario* which is simulated by the cellphone placed on the ground for corridor and open places, and on table for office location. Above two scenarios are evaluated for *Solo* and *Accompanied* cases, as shown in Fig. 6.

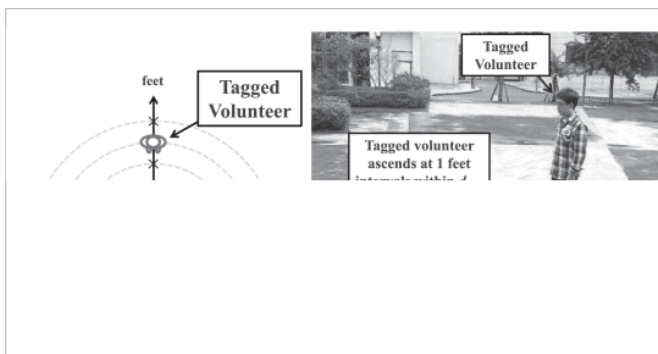




Fig. 6. Chest Evaluation. (a) Solo case. (b) Evaluation scenario. (c) Accompanied case. (d) Evaluation scenario.

4.1 Static Environment

Figs. 7 and 8 show the evaluation results for 24 dBm. During Frontal evaluation, the tagged volunteer directly faces the smartphone ($\theta = 0^\circ$) while he turns at specific angles, $\theta = \pm 30^\circ, \pm 45^\circ, \pm 60^\circ, \pm 90^\circ$, during Angular trials. The successful readings are shown by a filled circle while fault interrogations are shown by a crossed point.

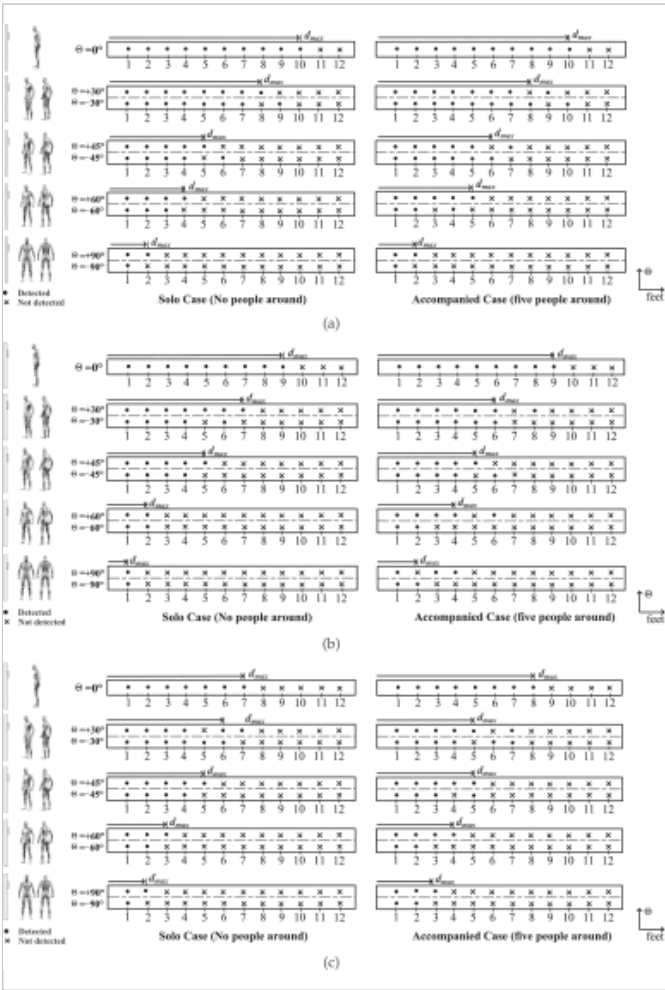


Fig. 7. Evaluation results for volunteer tagged at Wrist location. (a) Office. (b) Corridor. (c) Open.

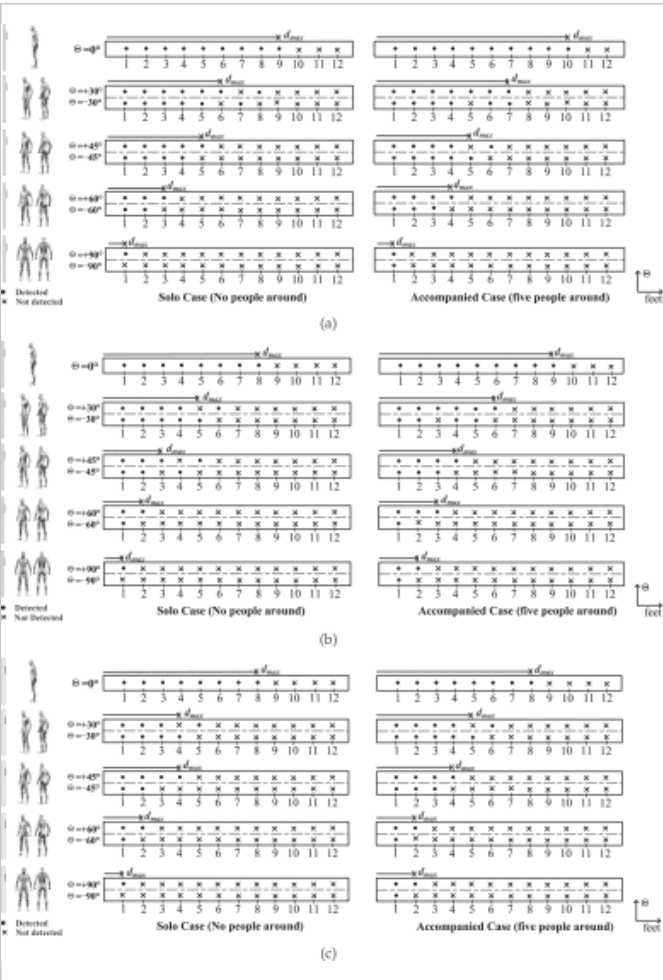


Fig. 8. Evaluation results for volunteer tagged at Chest location. (a) Office. (b) Corridor. (c) Open.

For Frontal distance, the results of wrist evaluation (Fig. 7) show a maximum range of 10, 09 and 07 feet for office, corridor and open place for Solo case, and, 10, 09 and 08 feet respectively for Accompanied case. Similarly, during chest evaluation, the Frontal range comes out to be 09, 08 and 08 feet for Solo case and 10, 09 and 08 feet for Accompanied case (Fig. 8). The range is higher in office environment and Accompanied evaluation because of adequate multipath and resultant constructive interference.

severe manner. Like, for $\pm 30^\circ$ in Fig. 7c in Accompanied case, a fault interrogation at 6 feet is followed by a successful read while at -30° degree, a fault value at 5 feet is followed by two successful readings. We also observe that the tag response is mostly identical for Solo and Accompanied cases for small angles, normally till $\pm 30^\circ$ degree because of low multipath. For higher values, the multipath due to surrounding five people plays its role and we observe slightly irregular tag responses. Besides, it also increments the range by 1 to 2 feet for $\pm 60^\circ$ degree and $\pm 90^\circ$ degree in Accompanied case. We note that by coincidence, the volunteer wears the tag on left side of the chest and left wrist in our evaluations, and there are two surrounding people at right side (Fig. 6c) compared to one on the left. As a result, the ranges for $+\theta^\circ$ are mostly higher than $-\theta^\circ$.

The address intermittent tag responses, we follow a criterion of maximum successful read distance, $d_{\max}$. It is the distance to the point of last successful interrogation in case of consecutive success readings. In case, the success and fault readings are sporadic, $d_{\max}$ is given by first observation of fault interrogation followed by at least two consecutive success readings [38]. In case the fault interrogation is followed by only one success reading, $d_{\max}$ is given by the last successive true reading. This way, we assign a positive weight even to very isolated failure point.

4.2 Dynamic Environment

For dynamic uncontrolled environment, we simulate a scenario in which the volunteer is tagged at the wrist and moves in a specific direction, pickpocket remains within $d_{\max}$ in any direction, and surrounding five people are allowed to move around both in a random fashion. We perform a total of 75 trials with each consisting of 150 tag search rounds by the Reader in Track Mode.

Regarding response time, the Reader will notify the user about a lost event *always* towards the end of Segment-2. It will first execute Check Mode and upon failure, Segment-1 of Track Mode will search the tag for 9 times within 4 sec. If not identified, Segment-2 will scan the tag over user selectable 0.5-7 sec. So, the response time will vary between 4.5-11 sec for which our duty cycle scheme interrogates the tag for 17-82 times. Fig. 9 shows the results of a single trial for office location, for which the tag was successfully interrogated for all 150 Reader search rounds. We consider the overall detection time including all interrogations of a segment, i.e., 129 (86 percent) for Segment-1 and 21 (14 percent) for Segment-2 in Fig. 9. Similarly, the results for Corridor are 111 (74 percent) in Segment-1 and 39 (26 percent) for Segment-2, and 95 (63 percent) for Segment-1 and 55 (37 percent) for Segment-2 in Office.

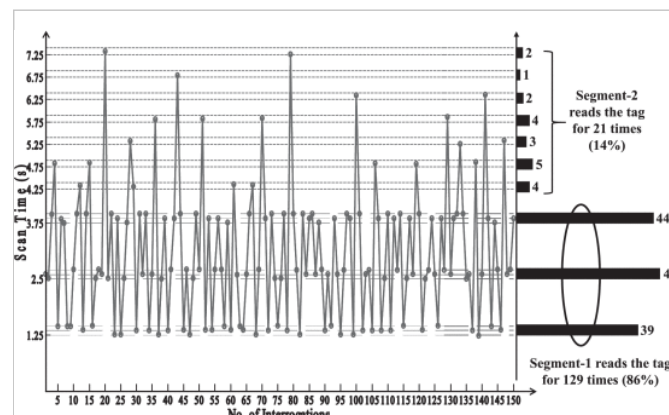
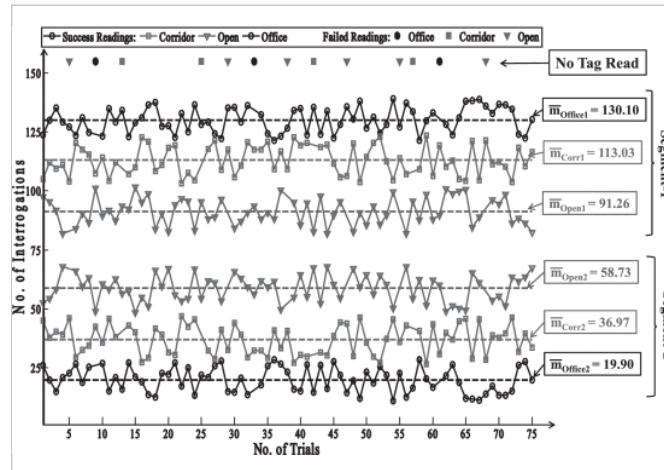


Fig. 9.

Detection and response time for office location.

For *Average Response Time*, we show the histogram of scan time for both Segments which is also useful to estimate the energy and power consumption of the system (Section 4.5.2). In Fig. 9, $t = 3.5$ sec for Segment-2 and the Reader interrogates the tag for 44 times: three search rounds in Segment-1 shown by dotted red lines and seven rounds in Segment-2 shown by dotted gray lines. From 150 Reader scans at all three locations, we observe that Segment-1 reads the tag in higher proportion, i.e., 86 percent for office, 74 percent for corridor and 63 percent for open place. Within Segment-2, we observe that initial 2-4 scans read the tag in higher numbers as compared to last intervals. The results also show that as the multipath increases, the chances to read the tag quickly also increase as Segment-1 at office location reads the tag in higher numbers than Segment-1 in corridor and open place.

Regarding *Tag Detection Rate*, Fig. 10 shows the results of 75 trials. The overall results show that for office location, Segment-1 reads the tag for 130.10 times (denoted by $\bar{m}_{\text{Office1}}$) while Segment-2 reads the tag for 19.90 times ($\bar{m}_{\text{Office2}}$). The detection rates for corridor and outdoor locations are shown by $\bar{m}_{\text{Corridor}}$ and $\bar{m}_{\text{Outdoor}}$ respectively. It is also observed that as multipath increases, Segment-1 has more probability of reading the tag.

**Fig. 10.**

Average scan time of Segment-1 and Segment-2 shown for 75 experiments at office, corridor, and open locations.

Lastly, *False Negatives* are shown by individual markers at the top, i.e., system did not read the tag at trial No 9, 33 and 61 in office. Like d_{max} , we assign a positive weight to even a single false negative point and consider a complete trial as failure if any of the 150 search rounds cannot interrogate the tag. In total, there are three false negatives for office (4 percent of 75 trials), 4 (5.3 percent) for corridor and 6 (8 percent) for open location. For such event, the system adopts the security measures and moves to protection mode.

4.3 Transmission Power versus Max Read Range

The maximum read range, $\max(d_{\text{max}})$, is shown in Fig. 11 for wrist and chest evaluations. For 24 dBm, the chest evaluation results to 09 and 10 feet for office location for Solo and Accompanied cases; 08 and

09 feet for corridor; and 08 feet for open place. We observe that range is higher for tag placed at wrist compared to chest location. The interrogation range is noticeably increased from 21-23 dBm whereas a slight increment is observed between power levels from 20-21 dBm and 23-24 dBm. Since our system searches a tag for tens of times, we observe that 20 and 23 dBm offers an appealing trade-off between the power versus range, than 21 and 24 dBm. Furthermore, 22 dBm can be observed as a point that keeps the interrogation range and transmission power in conjunction. Motivated by the same observation, we keep 22 dBm as the default transmission power for Check Mode and Segment-1 of Track Mode.

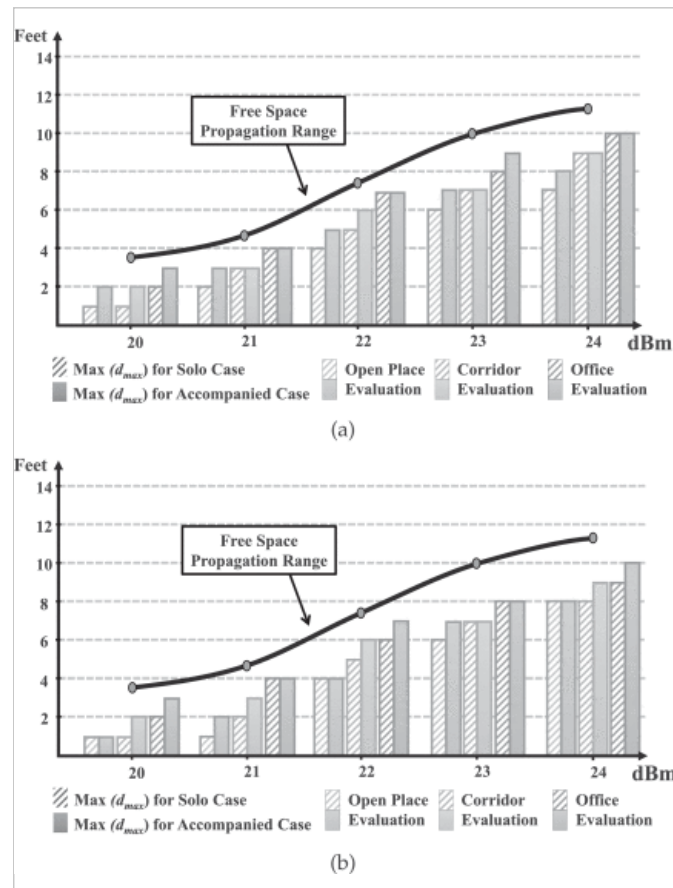


Fig. 11. Transmission power versus $\max(d_{max})$. (a) Wrist. (b) Chest.

4.4 Multiple Tag Scenario

The Reader will encounter tag-tag collisions from EPC-C1G2 compatible tags in private space. To this end, we first analyze the time overhead for various numbers of body wearable tags for 500 trials. For brevity, the results for the interrogations of 10 tags show a mean time of 153.76 msec with max/min values of 163/91 msec. Similarly, the results for 07 tags are 102.48 (109/76) msec, 05 tags are 78.03 (83/52) msec, 03 tags are 46.31 (64/29) msec, 02 tags are 17.28 (27/19) msec, and 01 tag are 10.37 (18/11) msec.

In Android Interface, a user can register multiple tags and we assume that 2 to 5 registered tags can be present in the Reader's zone. In this case, the interrogation time will reside within 80 msec, which is quite handful for duty cycle algorithm. The user also has the option to "fix"

and “ignore” the tag-IDs in Android Interface whereby the Reader will only look for specific tags while ignoring the others.

4.5 Cellphone Resources

4.5.1 Memory and Computational Overhead

The overhead of Android Interface is 28.10 and 20.38 Mbytes with and without accelerometer support. The application occupies 3.52 Mbytes of system memory. The memory usage increases to 37.42 Mbytes if user intends to train the system for Automatic Threshold operation. The computational overhead is 9.78 percent with accelerometer and 6.24 percent without accelerometer support for Samsung Galaxy Note2. In essence, our User Interface is quite handy and resource friendly once compared with specifications of present day smartphones.

4.5.2 Energy and Power Overhead

We argue that interfacing a low-power Reader with a smartphone incurs lower energy consumption once compared with onboard sensors like GPS, Wi-Fi, Bluetooth, camera, speaker etc. The underlying reason is the short time operation of EPC protocol, i.e., a complete inventory round amounts to couple of msec. Since Check Mode is analogous to a single scan of Segment-1 in Track Mode, it is annotated in Fig. 12a which consumes 33.96 to 160.8 millijoule of energy for 20-24 dBm power. In Segment-1, the Reader repetitively moves between sleep and active modes before and after each interrogation cycle to conserve power. Since Segment-2 is a rapid scanning of the tag, the Reader moves between idle and active modes within each 500 msec period (Fig. 12b). It scans the tag for five times while sweeping the transmission power from 20-24 dBm. We have followed an experimental approach to devise this duty cycle scheme which offers two advantages: First, duty cycle is not too high to drain the cellphone battery. Second, it is not too low to indicate the lost event after substantial delay.



Fig. 12.
Energy consumption for Track Mode. (a) Segment-1. (b) Segment-2.

Next, we answer a key question: what is the power and energy overhead of our anti-lost solution once compared with sensing and communication interfaces of a smartphone. In this context, we find an appealing study on energy and power overhead of an RFID Reader on the battery of HTC Magic Android phone in [39]. The authors investigated the power utilization of three low-power commercial UHF RFID Readers and compared them with smartphone's camera, microphone, accelerometer, Wi-Fi, Bluetooth and GPS interfaces. For each sensor, a typical operation is considered, i.e., 5 sec of continuous sampling for microphone and accelerometer, taking a picture from the camera, AP and device scan for Wi-Fi and Bluetooth, and getting a location fixed on the GPS. We benefit from findings of this study and compare our results which show that our anti-lost scheme incurs no more battery overhead than onboard sensors in both Check and Track Modes.

In Fig. 13a, we observe that Segment-1 consumes very less power for a total of nine tag interrogations over 4 sec because of duty cycle approach and short interrogation cycles of EPC protocol. Segment-2 consumes higher power because the Reader is continuously powered-on between 20-24 dBm, and the interrogation cycle is repeated ten times per sec. The key figure of merit, the energy overhead, is shown

in Fig. 13b. The results show that taking a single picture from camera consumes nearly the same energy as 4.5 sec of Reader's operation at full power (Check Mode at 24 dBm; Segment-1 at 24 dBm; Segment-2 with $t=0.5$; 17 tag interrogations in total). If operated at 22 dBm, our scheme consumes energy comparable to a single AP scan in Wi-Fi and around three times lower than a single device scan in Bluetooth. For 20-24 dBm power in both Check Mode and Segment-1, and $t=0.5$ sec in Segment-2, our system scans the tag for 17 times under 4.5 sec while offers 72.1 to 52.4 percent lower energy budget than a single Bluetooth device scan. The energy consumption of GPS is quite high as it takes several seconds to get a location fix. In line with the findings in Figs. 11 and 13, we configure our default Profile settings to 22 dBm which offers us adequate range while optimizing the energy budget.

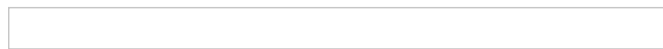


Fig. 13.

Power and energy comparison with onboard smartphone sensors. (a) Power consumption. (b) Energy consumption.

SECTION 5

Proposed Embedded Reader Modules

Our prototype is a proof-of-concept model that demonstrates the viability of an RFID-based anti-lost solution. For an envisaged practical design, we propose the following:

In [40], a fully integrated SoC UHF RFID Reader is specifically designed, fabricated and evaluated for smartphones. It delivers 22 dBm at 600 mW, with -79 dBm sensitivity. In [41], the single-chip Reader offers 22.4 dBm power with -75 dBm sensitivity. However, power consumption of 1.1 W is considerably high. An on-chip Reader is proposed in [42] that consumes 980 mW for 20 dBm, with a higher sensitivity value of -88 dBm. Within commercial solutions, a low-power RFID Reader in a SoC package is available from AustriaMicrosystems (AMS AG) [43] which can transmit 20 dBm with high receiver sensitivity of -86 dBm. Moreover, system-in-package (SIP) modules, like Indy-series by Impinj Inc. [44] and Red-series by PhyChips Inc. [45] can also be considered as viable alternatives.

SECTION 6

Conclusion

We articulate the viability and efficacy of an RFID-based system as a cellphone anti-lost and anti-theft measure. The system comprises of a smartphone equipped with a low-power RFID Reader that interrogates a body-worn passive tag to determine a private space which resides within 10 feet of the tagged owner. We focus our discussion on practical modalities and analyze the variability of the received power reflected by the tag, in presence of obstacles and other people under various factors like multipath, body shadowing and non-coherent receiver design. Motivated by our current investigation, we propose that low power SoC RFID chips may be incorporated in the smartphones for a proximity absence scheme as a viable anti-lost and anti-theft solution. Besides, the cellphone can also function like a low-cost mobile RFID terminal

COST MODELS FOR RFID COMMUN.

In future, we want to implement I/Q signal processing in MCU to support all kinds of RFID tags. Moreover, the appealing results of current design show that our system can be referenced for academic learning and further experimentations on RFID-based communication.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (Grant No. 61472068), China Postdoctoral Science Foundation (Grant No. 2014M550466), and PAPD and CICAEEET fundings.

Authors
Figures
References
Citations
Keywords
Metrics

IEEE Account

Profile Information

Purchase Details

Need Help?

Other

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.
© Copyright 2018 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

US & Canada: +1 800 678 4333
Worldwide: +1 732 981 0060

IEEE Account	Purchase Details	Profile Information	Need Help?
» Change Username/Password	» Payment Options	» Communications Preferences	» US & Canada: +1 800 678 4333
» Update Address	» Order History	» Profession and Education	» Worldwide: +1 732 981 0060
	» View Purchased Documents	» Technical Interests	» Contact & Support

| About IEEE Xplore | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | Sitemap | Privacy & Opting Out of Cookies

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.
© Copyright 2018 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

Loading web-font TeX/Main/Regular