SecureIt

Luca Bonato, Marco Ziccardi

University of Padua

Sistemi Ipermediali

Table of contents

Obiettivi dell'applicazione

Un dispositivo per sicurezza ad ampio spettro

Avere in un solo dispositivo *molteplici* funzionalità per monitorare uno spazio privato ed il dispositivo stesso

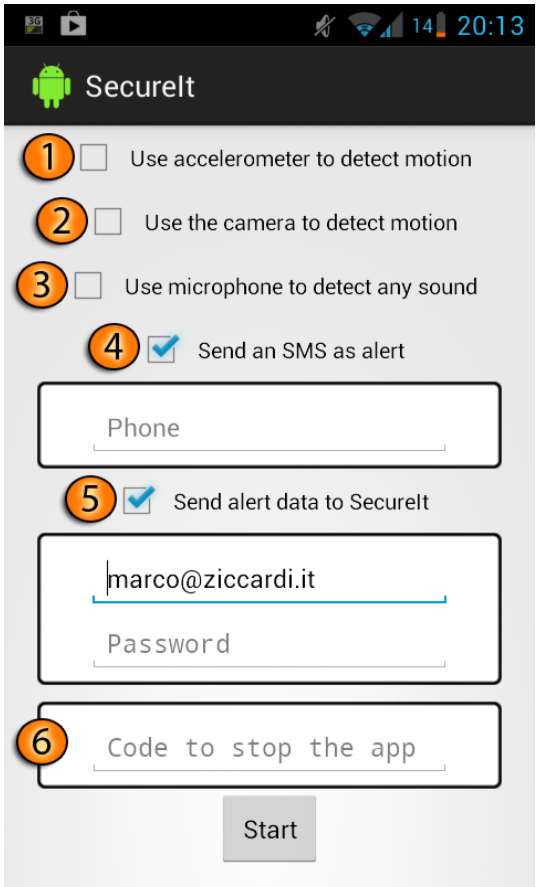
Altre applicazioni sul mercato offrono solo un monitoraggio parziale:

- **Motion Detector Pro**: solo motion detection
- **Sound Detector**: solo noise detection
- **Surveillance**: motion e sound detection. Non usa accelerometro e tracking

...si prova a sfruttare tutte le funzionalità del dispositivo per conoscerne i limiti

Funzionalità offerte

1. **Accelerometro**: determinare quando il dispositivo viene mosso
2. **Fotocamera**: determinare quando c'è movimento nell'ambiente
3. **Microfono**: determinare quando c'è rumore nell'ambiente
4. **SMS**: per avvisare l'utente di un'intrusione
5. **WiFi-3G-Bluetooth**: per fornire all'utente informazioni più accurate
6. **Codice sblocco**: per avere controllo sulla chiusura dell'applicazione
7. **Sito web**: in cui poter consultare le informazioni raccolte (audio, immagini, locazione dispositivo)



Accelerometro

Attraverso l'accelerometro è possibile determinare quando il dispositivo viene mosso

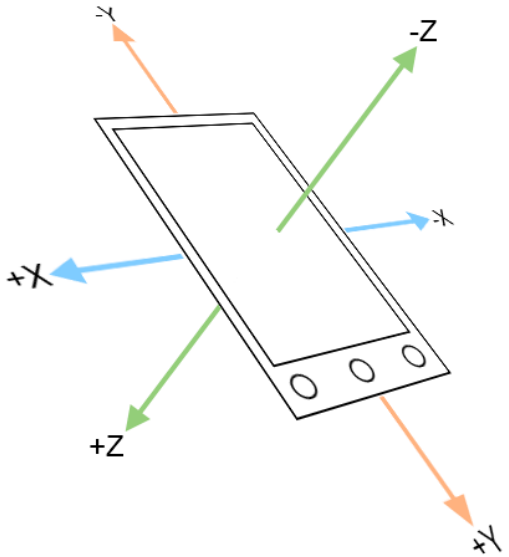
- Un intruso urta per sbaglio il dispositivo
- Un intruso prende volontariamente il dispositivo

Questa funzionalità viene utilizzata solamente per generare l'allarme

Come viene effettuato

- Possibile determinare la sensibilità (3 valori disponibili) con cui viene riconosciuto il movimento (`THRESHOLD`)
- Monitorare per un certo periodo le informazioni offerte dall'accelerometro (accelerazioni sui 3 assi)

$$\frac{(\Delta accel_X) + (\Delta accel_Y) + (\Delta accel_Z)}{\Delta t} > \texttt{THRESHOLD}$$



Cosa viene proposto all'utente

- Schermata in cui compare una superficie che rappresenta l'inclinazione del dispositivo
- Utilizzata OpenGL ES per non appesantire la CPU di calcoli grafici

Fotocamera

Attraverso la fotocamera è possibile determinare quando qualcosa all'interno del raggio visivo del dispositivo viene mosso o cambia posizione

- Un intruso passa all'interno del raggio visivo del dispositivo
- Un intruso muove qualche oggetto all'interno del raggio visivo del dispositivo
- ...ma non tutti i movimenti son causati da intrusi: vento, insetti, animali domestici...

Oltre a generare l'allarme, produce informazioni ausiliarie: scatta le foto di quel che si è mosso

Come viene effettuato

1. Monitoraggio:
   - Vengono catturate delle immagini ad intervalli regolari (1 immagine/1 sec)
   - Viene applicato un algoritmo di motion detection a due immagini consecutive
     - ★ Le immagini vengono convertite in scala di grigi: interessa solo la componente di luminosità per determinare movimento
     - ★ Si cercano le differenze tra le due immagini
     - ★ Vengono definiti 3 possibili valori per stabilire qualora le differenze riscontrate possano essere riconducibili a del movimento artificiale (ossia causato da un intruso)
   - Se si riconosce movimento viene generato l'allarme e si tenta di spedire le immagini catturate al server
2. Salvataggio: vengono sfruttate le funzionalità offerte dalle API Android per salvare le immagini in formato JPEG

Formati utilizzati e rappresentazione dell'informazione

Si lavora con immagini: si è cercato di utilizzare i formati più adatti

YUV N21 formato acquisizione nativo dispositivi Android. Separa informazione luma da crominanza: semplice ottenere le informazioni per convertire in scala di grigio le immagini

scala di grigi l'informazione su cui viene eseguito motion detection e base per costruire le immagini in RGB. Si sfruttano le relazioni tra spazi di colore YCbCr e RGB per ottenere questa informazione

RGB 565 formato per il display su dispositivo. Occupa poco spazio (2 byte per pixel) e non si spreca informazione (altri formati hanno canale alpha)

JPEG formato per memorizzare le immagini su dispositivo e per inviarle in rete. Si riduce lo spazio utilizzato su dispositivo e si riduce overhead per la trasmissione delle immagini su rete

Cosa viene proposto all'utente

- In alto viene fornito lo stream di immagini catturate dalla fotocamera (anche di quelle non processate)
- In basso a sinistra viene visualizzata la penultima immagine processata
- In basso a destra viene visualizzata l'ultima immagine processata in cui vengon evidenziate in rosso le zone in cui è stato determinato movimento

Microfono

Attraverso il microfono è possibile monitorare il livello di rumore presente nell'ambiente e di determinarne variazioni anomale

- Un intruso che parla
- Un intruso che produce rumori per entrare nell'abitazione
- ...ma non tutti i rumori sono causati da intrusi: tuoni, traffico, liti d'appartamento...

Oltre a generare allarme, il determinarsi di un livello di rumore anomalo causa la registrazione di 10 secondi di audio che saranno quindi trasmessi al server in rete

Come viene effettuato

1. Monitoraggio:
   - Viene riempito un buffer di valori campionati dal microfono
   - Viene eseguita una media dei valori campionati per ottenere un valore che possa riassumerli tutti
   - Si converte il valore ottenuto in decibel
   - Si confronta il valore in decibel con la soglia di sensibilità impostata dall'utente
   - Se si riscontra un valore anomalo viene generato l'allarme e si inizia ad acquisire l'audio da poi inviare al server predisposto
2. Registrazione: vengono sfruttate le strutture offerte dalle API Android per acquisire 10 secondi di audio in formato AAC

Formati utilizzati e rappresentazione dell'informazione

PCM 16 bit Acquisizione nativa Android. Queste informazioni vengono memorizzate temporaneamente su un buffer da 512 valori. Usare 8 bit diminuirebbe la qualità dell'audio

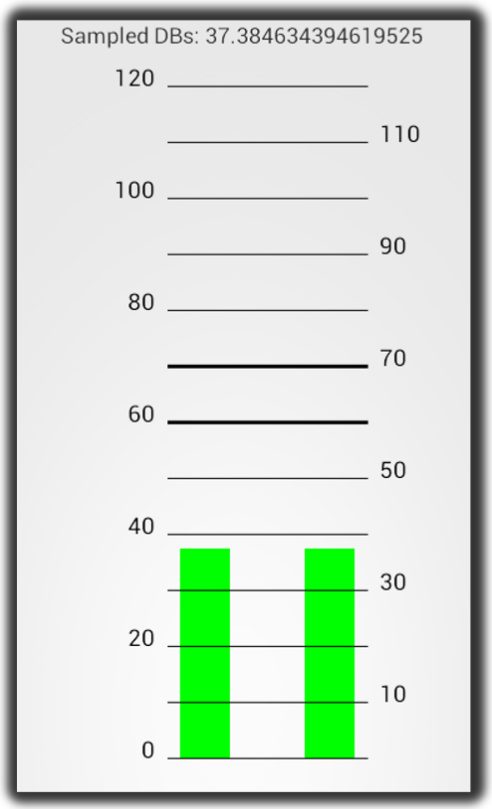
decibel l'ampiezza del segnale viene tradotto in decibels fornendo come soglia di riferimento il valore 1

$$dB_i = 10 \log_{10} \left(\frac{V_i}{V_o} \right)^2$$

AAC formato utilizzato per registrare i 10 secondi di audio. Permette di risparmiare spazio (in prospettiva di invio del file su rete) in quanto sfrutta modello psicoacustico per la compressione

Ogg Vorbis formato utilizzato per riprodurre l'audio acquisito qualora il browser utilizzato non supporti ACC

Cosa viene proposto all'utente



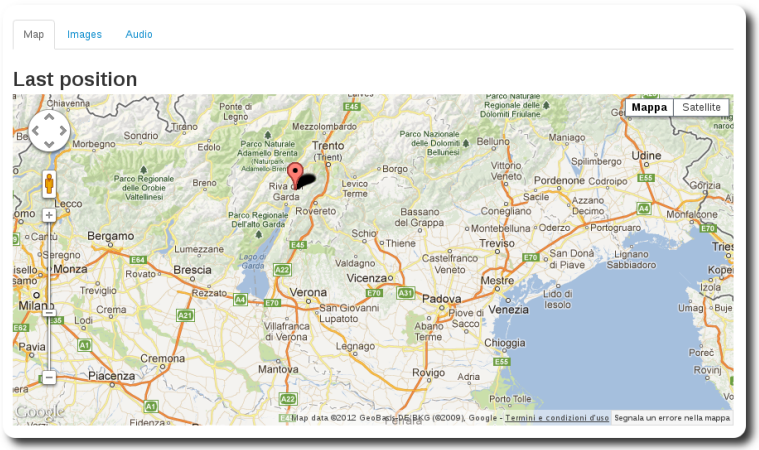
- Si fornisce graficamente la media del valore campionato su scala decibel
- Qualora il microfono riesca a campionare audio in modalità stereo verranno visualizzati i valori di entambi i canali (ciascuna barra sarà indipendente)
- Vengono evidenziati due valori di soglia:
  1. Il più basso rappresenta la sensibilità impostata dall'utente (è quindi il valore utilizzato per determinare un'intrusione)
  2. Il più alto è una soglia arbitraria di rumore

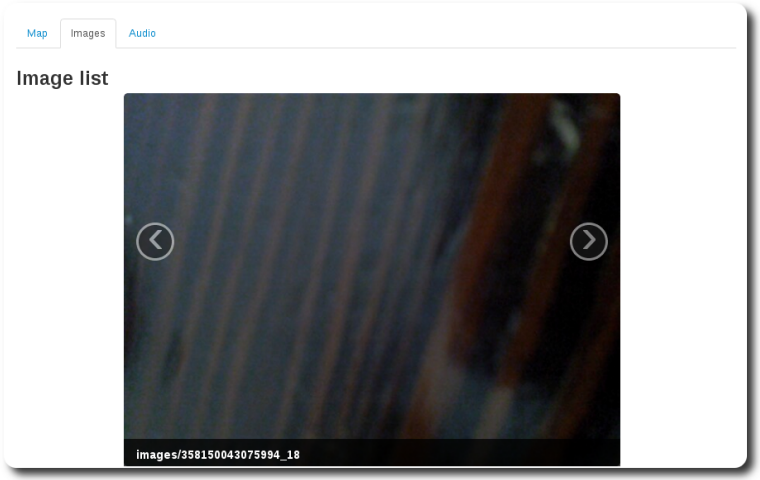
Server remoto

Si utilizza un applicazione web per poter memorizzare le informazioni raccolte dai vari dispositivi così da lasciarle sempre disponibili agli utenti

- Il sistema di allarme è utile. È più utile avere a disposizione anche le informazioni da cui è scattato l'allarme
- Il dispositivo può essere rubato. È bene salvare i dati in un luogo sicuro e sempre accessibile
- L'applicazione non è perfetta: può determinare una falsa intrusione. Poter accedere direttamente alla informazioni catturate può evitare attacchi di panico

Dati memorizzati





- Immagini: a seconda del tipo di connessione vengono inviate 5 (3G) o 10 (WiFi) delle immagini catturate
- Audio: inviati i 10 secondi registrati
- Locazione dispositivo: ottenuta tramite GPS se attivo o tramite servizi in rete. Informazione aggiornata periodicamente

API REST

Il server offre API REST per poter eseguire upload informazioni e per potersi autenticare: il server non accetta informazioni che potrebbero essere fasulle e si accerta che solo utenti/dispositivi autorizzati possano modificare le informazioni su server

- Necessario essere precedentemente registrati al server
- Necessario un access token per eseguire upload (access token ricevuto tramite login dell'applicazione)

```
[POST]/users/accesstoken
[POST]/api/phones/:phoneId/images
[POST]/api/phones/:phoneId/audio
[POST]/api/phones/:phoneId/positions
```

Sistema collaborativo Bluetooth

Qualora non vi sia a disposizione nessuna connessione di rete ma vi sia il bluetooth attivo, si tenta di instaurare connessioni opportunistiche con altri dispositivi e di delegare a loro il compito di notificare il server dell'attuale posizione del dispositivo

- Necessario assicurarsi che il dispositivo delegato non stia mentendo: utilizzo di un piccolo protocollo di firma digitale

Conclusioni

- I dispositivi riescono a sopportare il carico di lavoro
- Meccanismi di motion detection e noise detection sono naive (potrebbero essere uilizzati concetti di image/sound processing/recognition)
- Protocolli di sicurezza non sono perfetti (per questioni computazionali si è deciso di non utilizzare un protocollo a chiave pubblica)
- Per funzionamento efficace è necessario che tanti dispositivi adottino questa applicazione (vedesi comunicazione bluetooth)