Surveillance Tracking System

Intermediate Progress Report

Internet of Talents
Truong Xuan Nguyen
Fiona Lin
Christopher Beckett

Current Progress

Learnings
- Dividing the Work
- Moving away from a low power design
- Security

Changes from initial design
- Network
- Hardware

Planned next steps
- Complete localisation phase
- End to end testing
- Final demonstration

Current Progress

Overall, we have made excellent progress towards fulfilling the original project requirements. Currently we have a sensor module that can detect motion using a PIR sensor similar to the one used in the original paper, an end-user interface based on standard web application technologies that allows the use of any web capable device to report the status of the monitored space, and a RESTful API and persistence layer to co-ordinate messages flowing between the two.

The final outstanding phase is to display the specific location of the motion using the localisation algorithm used in the original paper. We currently have all of the required data for the actual sensor modules, and need only complete the drawing of the interface.

Learnings

Dividing the Work

Due to structuring our project around three main components, we were able to assign a team member to oversee the design and construction of each. We defined strong interface boundaries between each component, this allowed us to work more independently.

To ensure we were successful, we devised a RESTful API with a set of testing scripts to ensure interface compliance during the end to end testing phase.

Due to team member commitments, this independance allowed project progress to move forward smoothly, without the need to come together often.

Moving away from a low power design

Initially we wanted to create a low power, low maintenance design. However, it proved difficult and expensive to source the required hardware and meet the project deadlines.

Security

Securing IoT devices is the subject of much research, and we have looked into the various points where security risks might occur. While we have completed a threat modelling exercise, any of these vulnerabilities won’t be mitigated in the final design, but they are included for completeness.

Threat	Risk Statement	Possible Mitigation
Sensor module takeover	The sensor module may be forced to accept control instructions from unauthorised sources	Strong authentication and authorisation protocols should be implemented. These should include not using default passwords, and possibly implementing a two factor authentication system based on a hardware signal from the sensor device.
Sensor module transmission	Transmission of sensor data to the central server may be eavesdropped, or subject to a man in the middle attack. Leading to unauthorised data disclosure or loss of data integrity.	Strong encryption should be used between the sensor module and the central server, HTTPS with TLS v1.2 would be the suggestion.
UI data dissemination	Compromise of the application UI module would allow an attacker to view and possibly compromise the tracking system.	Care should be paid to ensure that the system meets OWASP web application security testing guidelines, and that strong access control and audit logging measures are in place.

Changes from initial design

Network

Due to the low power requirement of the initial design, we considered using a 6LoWPAN network for the local communication of the sensor nodes. We found it more cost effective to utilise WLAN technologies, and HTTPS as opposed to CoAP.
The change in the networking technologies, allowed for a faster development time using over the shelf components, and simple cloud based application hosting.

Hardware

We also switched our sensor modules from using a SensorTag microcontroller, to that of an arduino with built in WLAN.

These changes allowed us to use hardware that we happened to have on hand, and that we knew was compatible with the PIR sensors. Furthermore, the transition to WLAN removed the need for a Border Router and the Local Server, as the sensor nodes can report directly to the central cloud server via the internet.

Planned next steps

Complete localisation phase

Final work is being completed on the UI component to enable the processing of motion data to enable the localization of a subject moving through the monitored area. This will include a visualisation that is functionally similar to that in the original paper.

End to end testing

Now that we have the individual components of the system (i.e. the sensor module, the central server and the UI) up and running. Our next task is to connect the interfaces between these sub-systems and produce a complete prototype. Eventually, this prototype will be used in our final demo. This will include testing with multiple sensor modules, we are planning to use at least 4 in the final demonstration.
Also during this stage we will gather data to calibrate the sensor sensitivity in a varity of envrionments.

Final demonstration

Once the prototype has been proven to be working correctly, we will deploy our system to the final demo test environment. In particular, we will be scattering the sensor blocks around the room, adjusting their locations to obtain the optimum performance. Also, the central server will also be setup and verified in this environment. The UI and the main application will be used as our main tool to communicate and retrieve the information from our surveillance system.