Surveillance Swarm: Gathering Resources for Finding Targets in a Distributed Global Network of Smart Devices

Laisa C. C. De Biase, Geovane Fedrecheski, Pablo C. Calcina-Ccori, Roseli de D. Lopes, Member, IEEE, Marcelo K. Zuffo, Member, IEEE
Centro Interdisciplinar de Tecnologias Interativas, Universidade de São Paulo, Brazil
{laisa,geovane,roseli,mkzuffo}@lsi.usp.br, pcalcina@ime.usp.br

Abstract—Missing people, animals or objects is a common problem. Many tracking systems are based on technologies that are expensive, demands large devices to be carried, or demands often battery charging. Approaches using cameras or RFID systems usually have the problem of requiring covering the search area with sensors. This work takes advantage of the Internet of Things proposing a system for finding targets using the Swarm, which enables to opportunistically gather heterogeneous resources of third parties. A use case was deployed and evaluated.

I. INTRODUCTION

Finding missing people, objects or animals is a common problem. Tracking techniques, such as embedded trackers are expensive and invasive. Although newer techniques have been used lately, including IoT technologies, no platform has offered the possibility to opportunistically recruit available resources to find targets. Also, current systems do not allow retribution to individuals that share resources, which could foster collaboration.

An example of resource that could be dynamically recruited to find targets is surveillance cameras, as they are widespread and non-invasive. The creation of a platform for resource gathering, however, faces some challenges.

First, it must allow opportunistic discovery of available resources. In addition, as devices may be built by different manufacturers, interoperability must be considered. Fairness is necessary to benefit owners that share their devices and well-behaved users. Another requirement is geolocation, needed to set the scope of interactions. Finally, a crucial requirement is security, since access to the cameras must be open but controlled, for example to exclude indoor cameras from an outsider access.

The SwarmOS, a framework for seamless cooperation among IoT devices [1], [2], satisfies these requirements. This paper describes a surveillance system that uses private cameras and other services built using the SwarmOS framework.

II. RELATED WORK

There are many proposals of surveillance systems exploring IoT technologies [3], [4], but few explore gathering resources from individuals to expand the surveillance coverage area.

Participatory sensing is the process whereby individuals and communities use mobile phones and cloud services to collect and to analyze systematic data for use in discovery [5]. Recent work has expanded this definition embracing other sensors [6]. It is similar to our approach, since individuals collaborate sensing data, leveraging a ubiquitous data capture system [7]. However, most works does not explore the heterogeneity of devices, the fairness of the system and an open and decentralized system.

III. SURVEILLANCE SWARM

SwarmOS [2] is a framework that offers all the required features: opportunistic discovery, interoperability, access control, fairness and geolocation. Based on a microservices architecture, device resources are widely available to be used through the network. The Swarm Broker is a distributed and heterogeneous agent that runs on each device offering a set of platform services that helps services to interact.

The Swarm Brokers form a dynamic network capable of working without centralized service registries that boosts interoperability by using semantics. Service discovery relevance is obtained using an ontology for geolocalization [8]. Fairness is achieved by a payment-reputation mechanism [9] that builds an economy for the resources sharing, i.e., devices that make their resources available, will receive a payment from devices that uses these resources. The reputation mechanism builds trust among participants, guaranteeing good behavior. Security is enforced by an access control system based on attributes [10]. Permissions may be issued by the payment-reputation mechanism, by an inference mechanism or by direct configuration of resource owners.

A. Surveillance Swarm based on computer vision

Figure 1 shows the Surveillance Swarm components:

- Consumer: a client application that sends find requests to the Swarm network. The find requests includes the type of object that it wants to discover and a geographical radius sets the scope of the query.
As a metric for developer effort, Table I (b) shows the number of Source Lines Of Code (SLOC) to program each software component.

Table I: Evaluation results.

<table>
<thead>
<tr>
<th>Step</th>
<th>Time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup</td>
<td>4263</td>
</tr>
<tr>
<td>Execution</td>
<td>626</td>
</tr>
<tr>
<td>Total</td>
<td>5889</td>
</tr>
</tbody>
</table>

of lines of each service of Figure 1, plus the SLOC of the Swarm Broker [2] and the SwarmLib

Results indicate that all software used in the system requires at most 110 SLOC. The Consumer, i.e. the application itself, uses only 25 SLOC. This is possible because the Swarm Broker and the SwarmLib abstract the complexities.

V. CONCLUSION

This work presented the Surveillance Swarm, a solution for finding targets using a system composed of resource sharing. The system enables gathering resources from individuals. A sample implementation based on computer vision was deployed. It was possible to verify the Swarm delay introduced for interaction setup was acceptable and that the Swarm Broker and the SwarmLib highly reduce the complexity in the application development. Furthermore, the Swarm abstractions give access to the global ecosystem that composes the Swarm.

REFERENCES