UAV surveillance using multihop ad-hoc wireless networks: a demonstrator

Daniël Heimans, Maurits de Graaf and Gerard Hoekstra

Department of Electrical Engineering, University of Twente, Enschede, The Netherlands, e-mail: d.heimans@student.utwente.nl

Thales Nederland B.V., Huizen, The Netherlands and Department of Department of Stochastic Operations Research (SOR), University of Twente, The Netherlands, e.mail: maurits.degraaf@nl.thalesgroup.com

Thales Nederland B.V., Huizen, The Netherlands and CWI, Probability and Stochastic Networks, Amsterdam, The Netherlands, e-mail: gerard.hoekstra@nl.thalesgroup.com

Abstract

Festivals, public parades, and sports events are a common happening that attract a large amount of people to one location at the same time. To improve the safety at such crowded events, the event organization could use static and mobile sensors that sense and detect situations which require the attention of the security personnel. Camera surveillance of large areas is traditionally a costly endeavour, requiring either a large camera infrastructure or a lot of manpower. However, presently consumer electronics have evolved to the point where quadrotor toys with cameras and wireless connectivity have become affordable. In the meantime, the same has happened with consumer-grade wireless routers. In this paper, we describe a demonstration of a scalable aerial surveillance solution using consumer off the

shelf quadrotor drones and wireless routers to create an ad-hoc network based on optimized link state routing, extending the operational range of the drones.

1 Introduction

Critical infrastructures such as power plants, large industrial areas, harbours, railway emplacements, but also people-rich structures like railway stations, are essential enablers of our economy and way of living. The number of threats that may disrupt the normal functioning of these infrastructures is growing and it is not likely to diminish in the coming years. The aim of the COMMIT Sensafety project is (1) to offer real-time automatic analysis of potential hazardous situations and detection of important events and (2) give support in these situations to first responders to guarantee the safety of the general public as well as of the responding authorities. To improve safety, traditional surveillance methods are based on fixed camera systems or surveillance personnel on the ground. One of the main issues is that as the scale of the surveillance operation increases, more cameras and manpower are needed to cover greater areas, increasing costs.

In recent years, flying robots equipped with cameras, often referred to as drones, have been used to overcome the limitations associated to fixed camera systems. Drones are capable of flying over obstacles and provide a bird eye's view of the situation and can move easily while still being able to provide a stable video platform. An example use of this is seen at music festivals, where aerial footage is used for surveillance as well as for commercial purposes. Drones used are usually small and manoeuvrable, using four to eight rotors.

The downside of these drones is their limited range. Existing approaches are based on a single point of transmission, which automatically imposes limits to the scale to which they can be used. A solution to this problem can be found in the use of multihop ad-hoc networks: these are networks that consist of many transceivers sources, called nodes in the network. These nodes can enter and leave the network at any time while maintaining a connected, decentralized network via a routing protocol.

In this paper we propose a scalable aerial surveillance solution using consumer off the shelf quadrotor drones and wireless routers to create an ad-hoc network based on optimized link state routing, extending the operational range of these drones. An extended version of this paper, with a focus on the analysis of the scalability of ad-hoc networks and on the drone control framework appears as (Heimans et al., 2013).

2 Demonstration Overview

In our demonstration, we use a Parrot AR.Drone (http://ardrone.parrot.com/parrot-ar-drone/en/technologies) 2012 (see Figure 1). It provides wireless connectivity and video footage of up to 640 by 480 pixels. The demonstration shows a drone sending a video stream to the command centre. The drone is part of the ad-hoc network, which enables both the control of the drone as well as the video stream to be sent over an ad-hoc network. The drone runs low-level control firmware providing stable take-off, landing and hovering. The firmware takes high-level control commands and converts it to low-level control. An example of a high-level command is 'move forward at 50% speed'. The high-level control commands are sent over a wireless LAN connection. By default, the user connects to the access point the drone provides. In our experiments the drone is integrated in the OLSR network, so it can take commands from anywhere in the network.

Figure 1: The Parrot AR.Drone used for demonstrating camera surveillance over ad-hoc networks.

olsr.org OLSR daemon

Configuration | Routes | Links/Topology | All | About

OLSR Routes in Kernel

Destination	Gateway	Metric	Cost (ETT)	Interface
192.168.4.0/24	192.168.6.206	2	42455.000	wlan0
192.168.4.204	192.168.6.206	2	42455.000	wlan0
192.168.6.0/24	192.168.6.206	1	19573.000	wlan0
192.168.6.206	192.168.6.206	1	19573.000	wlan0
192.168.9.0/24	192.168.6.206	4	74092.000	wlan0
192.168.9.209	192.168.6.206	4	74092.000	wlan0
192.168.10.1	192.168.6.206	3	56521.000	wlan0

(C)2005 Andreas Tønnesen
http://www.olsr.org

Figure 2: The (linear) topology of the network consisting of nodes 192.168.6.206, *.204, *.9.209, and *.10.1, as seen by the command centre. The drone (with IP address 192.168.10.1) is 3 hops away from the command centre and functions as a router. The ETT values indicate the cost of the links based on delay and loss.

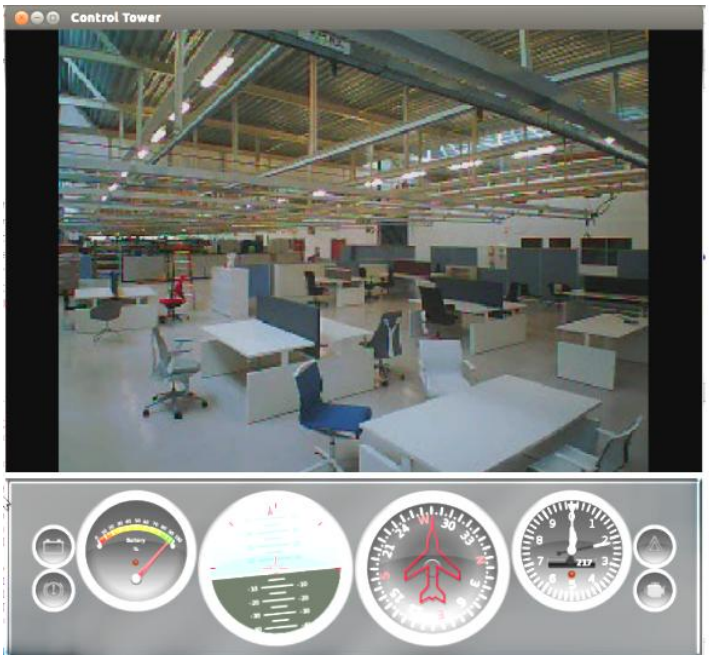

Figure 3: Impression of the AR.Drone Control Centre, to which the AR Drone streams the images over the multihop ad-hoc network.

By default, the drone is controlled using a smartphone which connects to the drone's wireless network. Once connected, the user can issue commands on the smartphone which are constantly being sent to the drone. For example, the user can tilt his phone forward, making the drone fly forward. During the time that the phone is tilted, it constantly sending commands to the drone, indicating it should move forward at the angle the user is holding the phone. In our demonstration we have replaced the phone with a laptop generating the same commands the phone would, using a gamepad (See Figure 3). We refer to this as the command centre. By default the drone is controlled by a steady stream of commands coming from the controlling device - be this a smartphone or the control centre application. The drone sends back two streams: one containing the video stream and one with navi-

gation data. Navigation data contains (amongst others) battery level, orientation, altitude, and speed.

Commands are sent every 30ms when controlling the drone as specified in the AR.Drone SDK (Piskorsi, Brusez, and Parrot, 2011). Commands are always smaller than 1024 bytes but are usually between 20 and 60 bytes. This constant sending of commands is called the control loop.

UAV surveillance applications are characterized by a continuous video stream from the drone to the command centre and an intermittent stream of time-critical control commands to the UAV. We use the Optimised Link State Routing protocol (OLSR) (Adjih et al., 2003) as topology control protocol. This protocol sends frequent network probing messages to keep an up to date routing table in every node. In addition, it has a mechanism to prevent broadcast messages from flooding the network called *multipoint relay* (Qayyum, L. Viennot, and A. Laouiti, 2000) Scalability issues of the OLSR, related to this specific application are investigated in (Heimans et al., 2013).

The hardware of the stationary nodes in our network are TP-link WR1043ND routers. They run a custom firmware called openWRT (https://openwrt.org/, 2012) which allows for the installation of non-default packages, such as OLSR. The network we are using is laid out linearly to allow experiments for different amount of hops. The maximum amount of hops between the drone and the command centre in our network is four (see Figure 2).

We have installed OLSR with link-cost extension (olsr-lc) (http://sourceforge.net/projects/olsr-lc, 2010) which is based on OLSR version 0.6.0 on the drone and the routers.

3 Conclusion

In this paper we describe a demonstrator for site surveillance using unmanned aerial vehicles in a multihop ad-hoc wireless networks. This provides a scalable solution using off-the-shelf consumer equipment. The paper describes a `lab test' with of the shelve means particularly because of the efficiency and low investments. The paper shows that, in potential, simple means could give good results. Besides adding to the surveillance capacities, the flying nodes-in-a-network could help with network coverage problems in larger areas.

Acknowledgement

This research has been partially funded by the SenSafety project in the Dutch COMMIT research programme.

References

References from Journals:

D. Heimans, G. Hoekstra, M. de Graaf, R. Carloni, Scaling UAV surveillance with ad-hoc wireless networks, submitted to IEEE Conference on Robotics and Automation 2013.

C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, and P. Minet, Optimized link state routing protocol, The Internet Engineering, pp. 176, 2003.

A. Qayyum, L. Viennot, and A. Laouiti, Multipoint relaying: An efficient technique for flooding in mobile wireless networks, no. 3898, 2000.

References from Other Literature:

S. Piskorsi, N. Brusez, and Parrot USA, AR.Drone SDK 1.6 Developer Guide, 2011.

References from websites:

P. USA, AR.Drone technical specifications website. http://ardrone.parrot.com/parrot-ar-drone/en/technologies, 2012.

OpenWRT, OpenWRT project website. https://openwrt.org/, 2012.

Thales Huizen, OLSR with Link Cost extensions webpage. http://sourceforge.net/projects/olsr-lc, 2010.