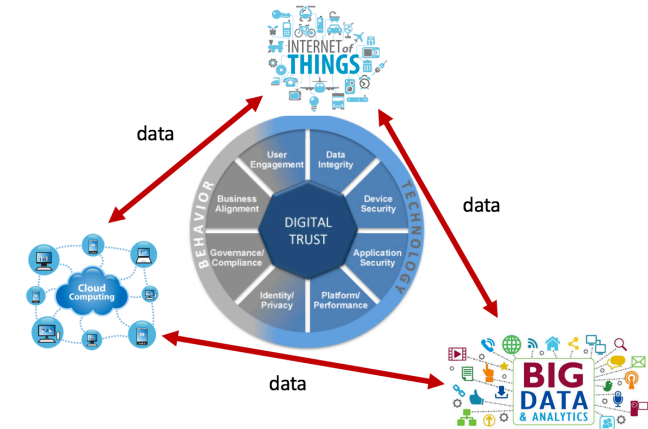


PCOG 2017

M. Brust

- **Programme title**
 - Technical Standardisation on Smart ICT with Digital Trust (Big Data, IoT, Cloud Computing)”
- **Duration**
 - 4 years research project
 - Co-funded by ILNAS-UL/SnT
 - Start date: 05/2017
- **Participants**
 - 3 PhD students, 1 postdoc, 1 professor dedicated to the project
 - 1 PhD student and 1 postdoc hired, 2 PhD students arriving
 - ILNAS/ANEC/UL personnel also participates
- **Research programme objective**
 - Creating an innovative environment on digital trust for smart-ICT and the related standardization efforts
 - Development of a new master program (Life-Long Learning) in collaboration with industry



PRESENTATIONS AND INVOLVEMENT

Mar 2017

- **The Crossfire Attack: A target-area link-flooding DDoS attack**
 - ILNAS/ANEC Digital Trust in Internet of Things Breakfast (Belval)



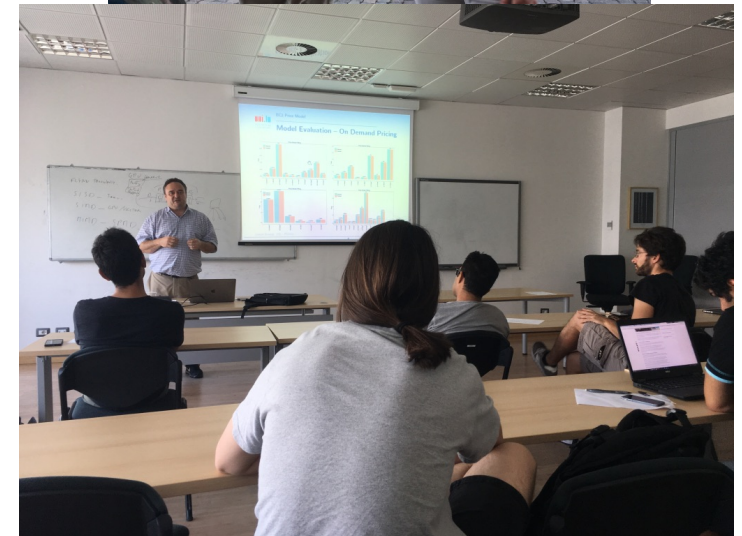
June 2017

- **IoT-UAV, Technical standardization and Digital Trust**
 - ICT Doctoral School (Trento)
 - Master Programme Entrepreneurship and Innovation (Limpertsberg)



Nov 2017

- **Participation**
 - UL HPC School (Belval)



Coverage Optimization with Connectivity Preservation for UAV Swarms applying Chaotic Dynamics

Martin Rosalie*, Matthias R. Brust*, Grégoire Danoy[†], Serge Chaumette[‡] and Pascal Bouvry[†]

*SnT, University of Luxembourg, Luxembourg

[†]SnT/FSTC-CSC, University of Luxembourg, Luxembourg

[‡]Univ. Bordeaux, LaBRI, UMR5800, Talence, France

Abstract—Cooperative usage of multiple UAVs as a swarm can deliver high-quality surveillance performance. However, the communication capabilities within the UAV swarm must be maintained for local data propagation to swarm members in favor of achieving an efficient global behavior. In this paper, we address the problem of optimizing two adversary criteria for such a UAV swarm: (a) maximizing the area coverage, while (b) preserving network connectivity. Our approach, called CACOC², solves the problem with a novel chaotic ant colony optimization approach, which combines an Ant Colony Optimization approach (ACO) with a chaotic dynamical system. CACOC² employs swarming behavior to obtain UAV clustering that result in maximized area coverage and preserved network connectivity. We show by extensive simulations how the size of the UAV swarm influences the coverage and connectivity. A metrics comparison chart shows the correlation of coverage and connectivity metrics.

Index Terms—cooperative UAV, multilevel swarm, mobility model, ant colony optimization, chaotic dynamics

I. INTRODUCTION

Advances in UAV technologies allow the development of new applications for both civilian and military domains. High-end UAVs are delivered with sophisticated on-board systems, extended flight autonomy, increased computing power, ad hoc networking capabilities, and with long-lasting batteries [1]. These improvements make UAVs capable of being deployed as a flying ad hoc network potentially forming a cooperative

stay in each other's proximity. Therefore, the potential for the UAV swarm to obtain the maximum coverage performance decreases considerably when considering the connectivity requirements. With the UAVs capacity to move freely in the three-dimensional space, an often applied technique on how to obtain superior results for this coverage-connectivity problem is the design of proper mobility models that aim to maximize both criteria (e.g., [4]). In this work, we propose CACOC² (Chaotic Ant Colony Optimization for Coverage with Connectivity), which extends the single criteria Chaotic Ant Colony Optimization for Coverage (CACOC) [3] with a swarming behavior to maintain more stable UAV clusters to deliver connectivity resilience within the swarm.

This work is organized as follows. In Section II, we report on related work and in Section III, we describe the original CACOC UAV mobility model and the novel extension for coverage and connectivity optimization, CACOC². Section IV, provides the experimental setup and settings as well as a description of the metrics used. In Section V we report on the results obtained in the experiments, and we finally conclude our work in Section VI.

II. RELATED WORK

Area coverage optimization with connectivity preservation

- **Background**
 - CACOC approach squared
 - CACOC²
- **Presentation**

Target Tracking Optimization of UAV Swarms based on Dual-Pheromone Clustering

Maciej Zurad*, Laurent Hentges*, Leandro Gomes*, Matthias R. Brust†, Grégoire Danoy*, Pascal Bouvry*

*FSTC-CSC, University of Luxembourg, Luxembourg

†Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg

Abstract—Unmanned Aerial Vehicles (UAVs) are autonomous aircraft that, when equipped with wireless communication interfaces, can share data among themselves when in communication range. Compared to single UAVs, using multiple UAVs as a collaborative swarm is considerably more effective for target tracking, reconnaissance, and surveillance missions because of their capacity to tackle complex problems synergistically. Success rates in target detection and tracking depend on map coverage performance, which in turn relies on network connectivity between UAVs to propagate surveillance results to avoid revisiting already observed areas. In this paper, we consider the problem of optimizing three objectives for a swarm of UAVs: (a) *target detection and tracking*, (b) *map coverage*, and (c) *network connectivity*. Our approach, Dual-Pheromone Clustering Hybrid Approach (DPCHA), incorporates a multi-hop clustering and a dual-pheromone ant-colony model to optimize these three objectives. Clustering keeps stable overlay networks, while attractive and repulsive pheromones mark areas of detected targets and visited areas. Additionally, DPCHA introduces a disappearing target model for dealing with temporarily invisible targets. Extensive simulations show that DPCHA produces significant improvements in the assessment of coverage fairness, cluster stability, and connection volatility. We compared our approach with a pure dual-pheromone approach and a no-base model, which removes the base station from the model. Results show an approximately 50% improvement in map coverage compared to the pure dual-pheromone approach.

I. INTRODUCTION

In the last decades, advancements in military research have lead to a tremendous increase in UAV usage, eventually earning UAVs a spot in the civil context [1]. Nowadays, airborne surveillance of moving targets is a common usage scenario for UAVs, in addition to search-and-rescue, fire detection and

the objective to maximize the total number of followed targets. But also the entire swarm can cover an area around the target to maximize the map coverage and cut short possible escape routes for the target.

Thus, we propose a hybrid solution, Dual-Pheromone Clustering Hybrid Approach (DPCHA), based on a dual-pheromone Ant Colony Optimization (ACO) [5] that includes a surveillance-oriented model [6] and a k -Hop Clustering Algorithm (KHOPCA) [7] for forming autonomous clusters among the UAV swarm. The clustering keeps stable network topologies, while attractive pheromones mark areas where targets have been recently found to improve overall tracking times, while repulsive pheromones indicate recently visited areas. Additionally, this paper introduces a disappearing target model that takes into account that targets might get lost or become temporarily invisible during the tracking process, for instance, after entering a tunnel or maneuvering around an area with restricted communication such as a dense forest [4].

The novelty of our approach is build a hybrid solution prioritizing the advantages from ACO and KHOPCA to gain a connectivity-stabilizing solution with communication capabilities and maximized coverage performance for high success rates in target tracking.

Extensive simulations show that DPCHA produces significant improvements in the assessment of coverage fairness, cluster stability, and connection volatility. A lower amount of total target have been detected in networks with sparser UAV coverage. Meanwhile, the target tracking times do not

- **Background**
 - Target detection and tracking
 - Optimizing map coverage and connectivity
 - Dual-Pheromone Clustering
- **Presentation**
 - Exeter, UK (May)
- **MICS (2016)**

Best Paper Award

Maciej Zurad, Laurent Hentges, Leandro Gomes, Matthias R. Brust, Grégoire Danoy, Pascal Bouvry

Target Tracking Optimization of UAV Swarms based on Dual-Pheromone Clustering

of the 3rd IEEE International Conference on Cybernetics (CYBCONF-2017) held on 21-23 June 2017, in Exeter, UK

CYBCONF-2017 General Chairs
Geyong Min, University of Exeter, UK
Jianhua Ma, Hosei University, Japan

IEEE Intern. Conference on Cybernetics (IEEE CYBCONF), 2017

Defending against Intrusion of Malicious UAVs with Networked UAV Defense Swarms

Matthias R. Brust¹, Grégoire Danoy², Pascal Bouvry¹, Dren Gashi², Himadri Pathak², Mike P. Gonçalves²

¹Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg

²Faculty of Science, Technology and Communication (FSTC), University of Luxembourg, Luxembourg

Abstract—Nowadays, companies such as Amazon, Alibaba, and even pizza chains are pushing forward to use drones, also called UAVs (Unmanned Aerial Vehicles), for service provision, such as package and food delivery. As governments intend to use these immense economic benefits that UAVs have to offer, urban planners are moving forward to incorporate so-called *UAV flight zones* and *UAV highways* in their smart city designs. However, the high-speed mobility and behavior dynamics of UAVs need to be monitored to detect and, subsequently, to deal with intruders, rogue drones, and UAVs with a malicious intent.

This paper proposes a UAV defense system for the purpose of intercepting and escorting a malicious UAV outside the flight zone. The proposed UAV defense system consists of a defense UAV swarm, which is capable to self-organize its defense formation in the event of intruder detection, and chase the malicious UAV as a networked swarm.

Modular design principles have been used for our fully localized approach. We developed an innovative auto-balanced clustering process to realize the intercept- and capture-formation. As it turned out, the resulting networked defense UAV swarm is resilient against communication losses. Finally, a prototype UAV simulator has been implemented. Through extensive simulations, we show the feasibility and performance of our approach.

I. INTRODUCTION

Governments, companies, third parties, or even individual citizens could permit UAV owners to use their designated air space during a given time and decide for how long, and so rent space and time to service providers using UAVs. They can then use the licensed flight zone (so-called *UAV flight*

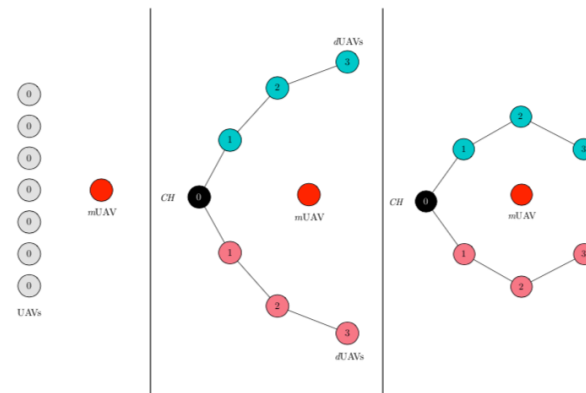


Fig. 1: An illustration of the escort mission phases.

are enforced by the dUAVs such that the mUAV surrounded by the dUAVs is moving outside the flight zone, thus escorting the mUAV (see Fig. 1).

A comprehensive UAV defense system is proposed, which is able to deploy auto-organized defense UAVs (dUAV) and create an intercept- and capture-formation to escort malicious UAVs (mUAV) outside the flight zone.

The most outstanding features and contributions of the presented approach are the balanced clustering to realize the intercept- and capture-formation. Additionally, the approach

- **Background**
 - UAV cybersecurity
 - How to defend against malicious UAVs?
 - Defense mechanism
 - Clustering
 - Formation control
 - Swarming
- **Presentation**
 - Singapore
- **MICS (2017)**

Detecting Target-Area Link-Flooding DDoS Attacks using Traffic Analysis and Supervised Learning

Mostafa Rezazad¹, Matthias R. Brust², Mohammad Akbari³, Pascal Bouvry², Ngai-Man Cheung¹

¹Singapore University of Technology and Design, {mostafa, ngaiman_cheung}@sutd.edu.sg

²SnT, University of Luxembourg, {matthias.brust, pascal.bouvry}@uni.lu

³SAP Innovation Center Singapore, mohammad.akbari@sap.com

Abstract—A novel class of extreme link-flooding DDoS (Distributed Denial of Service) attacks is designed to cut off entire geographical areas such as cities and even countries from the Internet by simultaneously targeting a selected set of network links. The Crossfire attack is a target-area link-flooding attack, which is orchestrated in three complex phases. The attack uses a massively distributed large-scale botnet to generate low-rate *benign* traffic aiming to congest selected network links, so-called *target links*. The adoption of benign traffic, while simultaneously targeting multiple network links, makes detecting the Crossfire attack a serious challenge. In this paper, we present analytical and emulated results showing hitherto unidentified vulnerabilities in the execution of the attack, such as a correlation between co-ordination of the botnet traffic and the quality of the attack, and a correlation between the attack distribution and detectability of the attack. Additionally, we identified a warm-up period due to the bot synchronization. For attack detection, we report results of using two supervised machine learning approaches: Support Vector Machine (SVM) and Random Forest (RF) for classification of network traffic to normal and abnormal traffic, i.e., attack traffic. These machine learning models have been trained in various scenarios using the link volume as the main feature set.

I. INTRODUCTION: THE CROSSFIRE ATTACK

A novel class of extreme link-flooding DDoS (Distributed Denial of Service) attacks [1] is the *Crossfire attack*, which is designed to cut off entire geographical areas such as cities and even countries from the Internet by simultaneously targeting a selected set of network links [2], [3]. The most intriguing

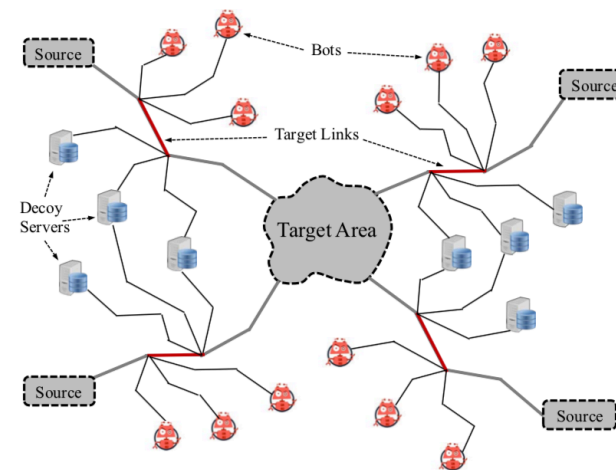


Figure 1. The Crossfire attack traffic flows congest a small set of selected network links using *benign* low-rate flows from bots to publicly accessible servers, while degrading connectivity to the target area.

reaching its destination. Reciprocally, access from the target area to Internet services outside the target area will be cut off. For the adversary to achieve its goal, it chooses public servers either inside of the target area or nearby the target area, which can be easily found due to their availability. The quality of

- **Background**
 - We care about security
 - Novel wave of sophisticated attacks
 - Distributed traffic analysis and supervised learning
 - Innovative attack detection
- **Collaboration**
 - SUTD
 - SnT
 - SAP Innovation Center

SERVICES (VALIDATED ON PUBLONS)

Peer Review Summary

Performed 30 reviews for journals including *IEEE Communications Magazine* and *IEEE International Conference on Communications (ICC)* between November 2016 and November 2017.

	8	IEEE Communications Magazine
	5	IEEE International Conference on Communications (ICC)
	3	Sensors
	2	Swarm and Evolutionary Computation
	2	IEEE Transactions on Cybernetics
	1	Information Sciences
	1	Computer Networks
	1	Computer Communications
	1	ISPRS International Journal of Geo-Information
	1	IEEE Global Communications Conference
	1	IEEE Consumer Communications and Networking Conference
	1	IEEE Transactions on Network Science and Engineering
	1	Information
	1	IEEE Conference on Local Computer Networks
	1	Workshop on Security Issues in Cyber Physical Systems (SecCPS)

FURTHER INVOLVEMENT

Since May 2017

- **Boonyarit Changaival**
 - Gregoire Danoy, Dzmitry Kliazovich, Frederic Guinand, Jędrzej Musiał, Kittichai Lavangnananda, Pascal Bouvry
- Optimal Fleet Placement in Station-based Round-trip Car Sharing Service



Since June 2017

- **Antonio Fiscarelli**
 - Community detection
 - Network probing

