DRONE

New Design of Intrusion Prevention System for aerial fleets

Aircrafts as well as Unmanned Aerial Vehicles (UAV) are more and more organized as networks. Data exchange is becoming increasingly important with the need to perform complex functions: Traffic Management or Fleet Management (such as swarm applications). Maintaining the integrity of the aerial data network has become more and more crucial.

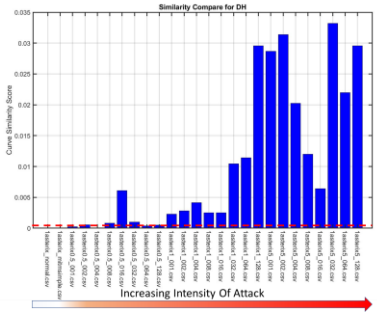
Wireless networks which topology can evolve randomly introduc[ing] additional security risks. To avoid undesirable consequences, it is necessary implement a security strategy. The technology presented herein is a new design of intrusion detection and prevention system which is efficient against various security threats including unknown types of attacks.

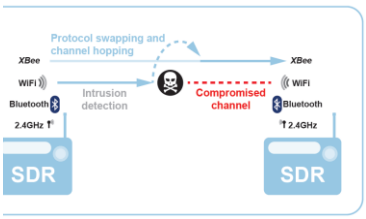
DESCRIPTION*

Our technology is a methodology for detecting and preventing intrusions which can operate in real complex environments (such as air transport or UAV fleets). It is composed of three stages: detection, decision making and prevention

- Intrusion detection is achieved through studying the signature of network. It is based on Wavelet Leader Multifractal Analysis and signature recognition
- Decisions are made to maximize the Quality of Service of the network under various types of attacks. Decisions are made upon the results from the signature recognition
- As patent application is pending, so far, no information can be given on the prevention system

This technology is efficient on wireless ad-hoc networks (i.e.: networks with evolutive topology) and enables the detection of 0-Day attacks





TECHNICAL SPECIFICATIONS

Key Technologies	- Wavelet Leader Multifractal Analysis - Network WLM signature analysis and recognition - Software Defined Radio to achieve evasive intrusion prevention
Advantages	- First IDS+IPS system proposed for aerial wireless network - Compact and efficient algorithmic design for aerial application and integration - Highly embedded physical design - Higher sensitivity to unusual traffic than classic IDS with increased ability to deal with network mobility

*Technology under license.

TOULOUSE TECH TRANSFER

COMPETITIVE ADVANTAGES

- Detection of 0-Day attacks
- In depth traffic analysis
- New generation prevention system
- Efficient on wireless ad-hoc networks
- Adaptable to different types of networks

APPLICATIONS

- Air Traffic Management (ATM) / ADS-C
- UAV Traffic Management (UTM)
- Drones/Robots Swarm
- Autonomous Vehicles
- IoT and Industry 4.0

INTELLECTUAL PROPERTY

- Patent application submitted
- Software protected by APP

DEVELOPMENT STAGE

- Experimental proof of concept

1	2	**3**	4	5	6	7	8	9

LABORATORY

ENAC
ECOLE NATIONALE DE L'AVIATION CIVILE

CONTACT

T. +33 (0)5 62 25 50 60
systemes@toulouse-tech-transfer.com
www.toulouse-tech-transfer.com