MESMER™ COUNTER UAS SYSTEM

In response to the
The Joint Improvised-Threat Defeat Organization Counter UAS Hard Kill Challenge

Submitted by: Department 13, Inc.
7021 Columbia Gateway Drive, Suite 175
Columbia, MD, 21046
www.department13.com

CAGE Code: 4QC83

Company POC: Roshni Sherbondy
Tel: (443) 510-3155
roshni.sherbondy@department13.com

Date: December 1, 2016

DEPARTMENT 13 SUBMISSION TO THE JIDO COUNTER-UNMANNED AERIAL SYSTEM (C-UAS) HARD KILL CHALLENGE

a. Business Name

Department 13, Inc.

b. Business Address

7021 Columbia Gateway Drive, Suite 175, Columbia, MD, 21046

c. Business Webpage

www.department13.com

d. CAGE Code

4QC83

e. Company POC and Contact Information

Roshni Sherbondy, roshni.sherbondy@department13.com, Tel: (443) 510-3155

f. Detailed System/ Subsystem Description

Name of system: Mesmer™

Team overview

Department 13 (D13) was formed in 2010 with a mix of scientists, engineers, security professionals, and former military operators whose goal was to transform how people use technology. D13 has been granted 13 patents and has 22 patent applications pending in the fields of drone defense, electronic warfare, communications, networking, and wireless security. Currently D13 is developing a commercial counter drone platform called Mesmer™. Mesmer uses sophisticated and novel methods to manipulate drones allowing users to automatically detect drones and stop, kill, redirect, or safely land them. Our solution is ideal for both commercial and defense/security organizations to deal with the emerging threat of ubiquitous autonomous systems. The D13 team successfully completed the Joint Integrated Air and Missile Defense Organization Black Dart exercise, and Mesmer was a finalist at the MITRE C-UAS Challenge.

Solution Overview

The emergence of small, lightweight, low cost Unmanned Aerial Systems (UAS) offers many applications in the theatre of conflict, but their ubiquitous nature and ease of use make UAS as much a threat as they are an asset. The use of UAS by conventional, non-state and irregular forces has added another dimension of threat on the asymmetric battlefield, enabling adversaries to observe military dispositions and capabilities. The Joint Improvised-Threat Defeat Organization (JIDO) needs a capability to neutralize this potential threat and inhibit the situational awareness of enemies and antagonists.

Mesmer is a counter UAS (C-UAS) system with key benefits that include:

- Mesmer detects, identifies, tracks, and mitigates UAS threats.
- Mesmer identifies and takes control of commercial drones. It can defend points, perimeters, or areas against one or multiple drones (swarm).
- Mesmer lands drones safely and does not cause uncontrollable crashes. It does not require an operator to visually spot a drone.

- Unlike traditional electronic warfare (EW) systems Mesmer does not affect other communications.
- Mesmer is inherently low-power and has low interference with existing signals in the environment.
- Mesmer can be operated below 1 Watt and within most regulatory constraints.
- Mesmer's radio frequency (RF) systems gain is tuneable to operate below or above 1 Watt depending on requirements and regulations.
- Mesmer can easily scale and adapt to different needs and integrate with existing security installations, enabling quick deployment for a wide range of concept of operations (CONOPS).
- Mesmer's software defined architecture enables deployment flexibility, able to adapt to threats, constraints and user needs that will constantly change and evolve.

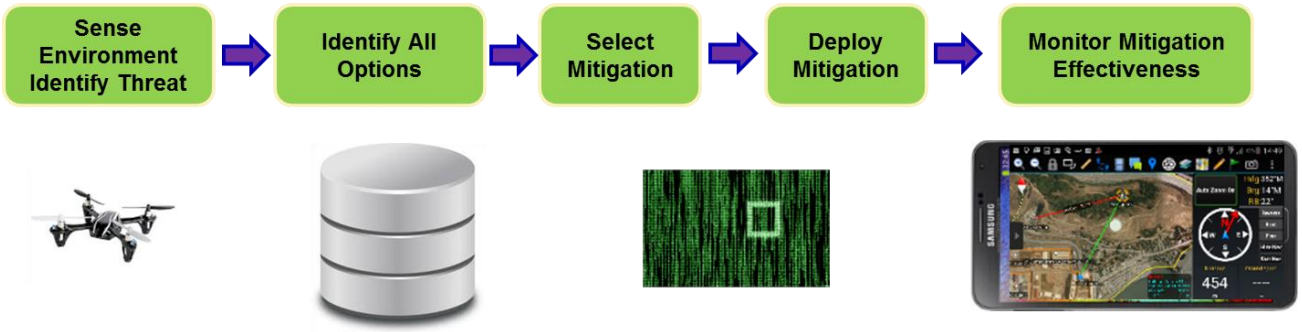

Figure 1: Mesmer C-UAS process to detect, identify, track, mitigate and monitor a UAS

Figure 1 represents Mesmer's end-to-end process. On the left, an environmental trigger (e.g. a UAS intruder) is present and sending RF signals between itself and its corresponding transmitter. Mesmer detects the RF transmission within this environment, assesses the environmental triggers and determines whether what was observed is a drone. Based on the location of the drone and its path, Mesmer performs an analysis to identify its best mitigation options (step two). From its mitigation options, Mesmer chooses the best option for the specific conditions and available resources (step three). In the fourth step, "deploy mitigation", Mesmer evaluates internal logic and rules against the collection of resources available to Mesmer, and Mesmer assembles these resources to disrupt the drone. The operator can define mitigation strategies by defining "rules" on the Mesmer user interface. For example, rules can be applied based on drone whitelist/ blacklist, or as a redirect for all incoming targets within the first layer of the defense perimeter; if an intruder does not respond to protocol manipulation within 30 seconds of attempts, Mesmer should switch to the next most aggressive approach.

System Description

Detection

Mesmer detects by sensing RF emissions from commercial off-the-shelf (COTS) drones, either flown by the operator using a controller or autonomously using way points to fly by GPS. Compared to existing methodologies that use various techniques to demodulate or characterize a signal, Mesmer has a much lower rate of false positives because Mesmer directly interrogates the device RF front end. Mesmer uses methods to detect potential signals of interest including the traditional approaches to signal identification as well as more novel approaches including machine learning and "Deep Learning" to categorize, identify, and demodulate unknown signals. The advantage against systems that only look for standard physical features of a signal such as frequency or waveform characteristics, Mesmer utilizes other parameters such as chip rate, duty cycle, modulation type, and other attributes.

Once Mesmer has extracted enough features, it can determine the radio protocol and often the UAS make, model, and version. This identification is accomplished by correlating the features in the encrypted data to known radios.

In other cases, when Mesmer can collect and demodulate the data, a deeper analysis can capture telemetry information and provide a higher confidence level in identifying the drone. Without additional sensor information, Mesmer can provide all telemetry data that originates from the drone or the controller, e.g., GPS location, altitude, bearing, battery life, point of origin, and destination. The UAS sensor data may also be accessible, such as video, accelerometer, magnetometer data. If the device is unknown, Mesmer can extract enough features from the data to provide Mesmer's mitigation engine the details to mitigate and disrupt the drone.

Mesmer has been tested against many COTS drones with a focus on specific vendors DJI, 3D Robotics, and Parrot. D13 will soon add mitigations for drone manufacturers Horizon Hobby, Hubsan, Yuneec, Autel and custom built drones. D13 is deliberately concentrating on the consumer drones with the most significant market share at this stage of product development.

Mesmer can use off the shelf antennas, i.e., omnidirectional, directional, or sophisticated steerable antenna arrays. However, detection and tracking will be impacted by the type of antenna. Currently Mesmer uses standard low cost omnidirectional antennas and a tuneable RF frontend running below 1 Watt. Drone acquisition can occur as soon as 2s within operational range of the system. At the MITRE C-UAS Challenge, Mesmer detected and mitigated drone signals of interest beyond 1 km. Mesmer's RF detection can be enhanced via positioning of antennas, types of antennas, and tuning power/gain to increase range as needed. Depending on the installation site and CONOPS, Mesmer can make use of simple directional finding for tracking or a 360 degree antennae array for more precise RF spatial tracking.

UAS "Hard Kill"

To disrupt the UAS, Mesmer uses a technique called protocol manipulation that uses signal features and metadata to select and apply strategies to physically interrupt the drone's ability to maintain lift and continue its mission. These mitigation strategies may include the direct capture of the UAS by taking control of the drone, flying it and landing it safely at a position of choice, cause a drone software malfunction to reset the drone flight control system or simply crash land the drone. The Mesmer platform offers significant benefits over traditional approaches. Since protocol manipulation does not attempt to overpower signals like jammers, protocol manipulation is inherently low-power and has minimal interference with existing signals in the environment. Therefore, it can operate within the regulatory restrictions of the US and other countries.

Protocol manipulation takes advantage of the radio protocols hierarchal structure to control the radio's behaviour. By speaking the same language of the drone, Mesmer utilizes the drone's control protocols to silence the drone's controller or by abusing the protocol to lead the control logic to a failure state. These RF signals look legitimate but exploit the drone's internal logic to achieve the desired results. Most COTS and military drones use a RF platform, or just GPS receivers. Hence manipulating the drone data and taking control of a system via its RF front end becomes very attractive and a practical approach to mitigation. Protocol manipulation is effective, especially against modern digital communications, because most digital radio protocols have major weaknesses related to beaconing, announcements, authentication, pairing, key exchange, and other data attributes. Further, protocol based exploitation is much harder for adversaries to defend; while they may change the frequency and/or waveform on a threat platform, it is difficult to change even the fundamental and well known major vulnerabilities in the protocols.

Protocol exploitation also allows for "positive control"; positive control is the ability to affect a deterministic outcome of the targeted device by maintaining continuous control over the device. This is different than traditional EW or kinetic effects that often have unintended and highly stochastic outcomes. Lastly, protocol manipulation can be used either surgically or to target numerous devices simultaneously, thus allowing the system to target a specific device out of a group of devices or a whole swarm.

D13 designed Mesmer to target any digital RF platform. It has been tested, in a limited manner, against various Internet of Things (IoT) targets including Bluetooth headsets, Bluetooth LE sensors, ZigBee based home sensors, alarm systems, and remote controlled car control links. Mesmer has been also tested on TCP/IP based direct wired

platforms. While Mesmer currently focuses on COTS drone threats, D13 plans to build out the capabilities of the system to create a more generic capability to mitigate any network reachable device. D13 sees Mesmer and similar systems soon becoming common place on EW platforms and at the tactical level, e.g., wearable Electronic Attack systems for Infantry.

Subsystem Description

The key components of the Mesmer system include the following:

- General purpose server. Mesmer uses a general-purpose computer running Linux OS. Multiple PCI slots are utilized for accommodating multiple Ethernet and Wi-Fi interface cards that are used for intra-system communication and Wi-Fi-based drone detection, identification, tracking, and mitigation. Current configuration has multiple Network cards to integrate other systems via RJ45 cable and standard IP based networking.
- Software Defined Radios (SDR). Mesmer utilizes commercially available SDRs for RF signal detection and identification. These radios are also used for mitigating drones that employ proprietary radio protocols within the frequency bands commonly used by drones. Mesmer currently operates in the 2.4GHz and 5.8GHz unlicensed bands but will expand to include 433MHz and 915MHz bands in future versions.
- RF Front End (optional). The RF front end is an optional component that provides filtering and amplification on the receive and transmit channels of the SDR. Many commercially available SDRs do not have adequate filtering on the receive channels and are susceptible to saturation outside of a lab environment. In addition, the SDR may also not have enough transmit power. The RF front end provides external filtering and amplification that allows Mesmer to perform optimally in a real-world environment.
- Operator console (Android-based device). The operator console is based on the Android Tactical Assault Kit (ATAK). ATAK runs on the latest version of the Android operating system. Mesmer comes with an integrated LCD screen, keyboard, and separate platform that runs the ATAK. The Mesmer operator console can run on a tablet, smartphone, and desktop-based Android devices. The console only requires a network connection to the Mesmer general purpose computer, allowing it to be remotely or co-located with the Mesmer hardware. However, Mesmer is designed to be integrated easily via an open application program interface (API) with other third part command and control systems if there is a desire to use another tool system instead of ATAK. The API can be accessed via a secure public key infrastructure built into the system. Mesmer supports Cursor on Target via MQ messaging, JSON, or RESTful services.
- Antenna. Mesmer can operate with many antenna types and configurations. Mesmer can work with omnidirectional and directional antennas. Antenna choice and configuration is largely driven by the site survey and perimeter protection requirements.
- Uninterruptable Power Supply (UPS) (optional). The UPS is an optional component that is highly recommended for installations where power may be unreliable or poorly conditioned.

System Configuration

The Mesmer system is packaged in a ruggedized rackmount enclosure. This configuration allows for maximum flexibility for deployment allowing for fixed site (indoor/outdoor) or mobile installation. Figure 2 depicts the system in the ruggedized enclosure.

The Mesmer system hardware includes:

- High performance general purpose computer with all necessary Ethernet and Wi-Fi interfaces running Mesmer software
- Rackmount packaged, commercially available software defined radios
- Rackmount packaged, Android device running ATAK-based Mesmer operator console
- Rackmount RF front end and Antenna interface box
- Rackmount Keyboard, Video, Mouse (KVM) console
- Rackmount UPS and power distribution
- Nine omnidirectional antennae and RF cabling

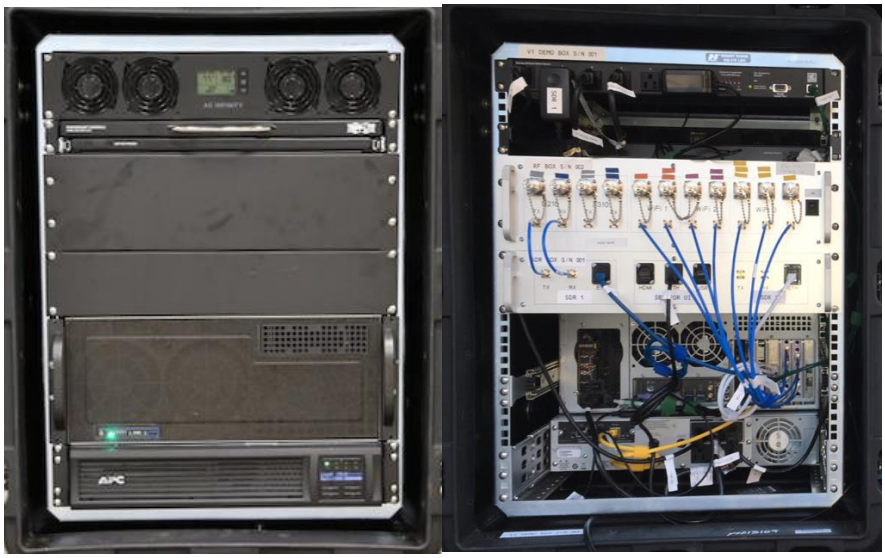

Figure 2: Mesmer configuration (front/back) installed in a ruggedized rackmount enclosure

Mesmer Technical Specification

The following table lists the specifications of the Mesmer system.

GENERAL	
Frequency Range	2.4 – 2.5 GHz, 5.18 – 5.825 GHz
Transmit Power *	< 1W. Configurable upon request.
Antenna	An array of 9 antennas
EFFECTIVE RANGE	
	1 km nominal at 1W transmit power using omnidirectional antenna. Range may vary depending on antenna type, transmit power, and terrain.
OPERATION MODES	
	Detection Only Mode
	Auto-Mitigation Mode
	Manual Mitigation Mode
SUPPORTED DRONE MODELS	
	Multiple models and manufacturers of commercial drones. Please contact for updated list.
EXTERNAL SENSORS	
	Open architecture and standardized interface for ease of integration with external sensors (e.g. acoustic, radar, electro-optical sensors).
PHYSICAL (STAND-ALONE SYSTEM)	
Dimensions (Rack)	19 W x 10.5 H x 20 D in (48.3 W x 26.7 H x 50.8 D cm)
Volume (Rack)	2.3 ft^3 (0.07 m^3)
Dimensions (External)	28 W x 19.5 H x 28.5 D in (71.1 W x 49.5 H x 72.4 D cm)
Volume (External)	9 ft^3 (0.25 m^3)
Weight	90 lbs. (41 kg) (not including antenna assembly)
POWER	
Power Consumption (Avg.)	220 W (110V/2A, or 240V/1A)
ENVIRONMENTAL	
Temperature (Indoor Ver.)	32°F to 100°F (0°C to 38°C)
Temperature (Outdoor Ver.)	-40°F to 131°F (-40°C to 55°C), with additional air conditioned enclosure

Table 1: Mesmer System Specifications

Mesmer Open Architecture

The Mesmer software platform is designed with General Purpose Processors running a Linux operating system. Mesmer provides abstracted services to control RF hardware, specifically SDRs, for the detection and mitigation of threats. This allows Mesmer to run with minimal modification across many hardware platforms using a variety of different sensors and RF hardware for mitigating UAS. External, multimodal sensors and client applications, such as command and control platforms, can communicate with Mesmer by sending messages via a well-defined API over a standard network interface. Other applications or systems can either pull data from Mesmer or push data to it allowing for easy integration but also a wealth of flexible CONOPS.

g. System TRL Level and Justification

The D13 Mesmer technology is currently between TRL 6 and 7. D13 is planning the Mesmer product launch in 1QCY17. D13 has a clear product development strategy and plan to get to an initial TRL 9 product offering, and a strategic path for product enhancements.

D13 are currently engaged in a detailed and comprehensive product development for Mesmer. This has involved much laboratory experimentation and some scenario specific testing. D13 current testing is as follows:

1: Automated testing suite that checks new mitigations and confirms performance assertions

2: Bench testing in the lab against targets that are tethered or have had their propellers removed

3: Live testing against targets that are flying and being controlled by human controller or in a waypoint autonomous mode in a controlled environment

4: Live tests against targets on a test range

D13 is currently moving to implement RF simulators to simulate contested or denied RF environments as well as simulate scenarios such as implementations at an airport. D13 is also planning for the use of Government and other ranges to allow for more sophisticated testing and measuring of performance of the system. D13 has demonstrated Mesmer's capabilities to detect and mitigate drones at the MITRE C-UAS Challenge and Black Dart Demonstration.

h. Brief Concept of Operations

Mesmer was specifically designed to maximize flexibility and portability to allow users to adopt or integrate into multiple situations including existing perimeter defense systems, airborne platforms, sea borne platforms, or even mobile VIP protection. While Mesmer fits into many CONOPS, D13 will introduce two initial use cases: Basic Site Protection and Military Perimeter Defense.

Basic Site Protection: D13 will provide a Mesmer system in a portable case containing all necessary components and an operator interface. This configuration will support deployment to a range of sites to support a C-UAS security operation. The operator interface will use a flexible and feature-rich Android Tactical Assault Kit (ATAK) client for perimeter defense management; Mesmer can also be operated through a MAFIA based interface.

Military Perimeter Defense: D13 will provide a Mesmer to military bases, naval assets, and/or Forward Operating Bases. Military grade solutions will detect incoming drones, trigger defense notifications, and redirect drones to predefined landing areas or disrupt drones in place. Additionally, Mesmer can be configured to utilize existing installed military hardware, e.g., antennas.

In the near future, Mesmer may be used in the following use-case scenarios:

Mobile detection and defense: A Mesmer system can be deployed in a vehicle to provide a mobile drone defense system. Incoming drones are detected and vectored away from the convoy. Convoy personnel are alerted and provided situational awareness on their tablets or handsets.

Human Portable: A Mesmer system can be carried in knapsack or bag to provide localized detection and defense. Operators can use Mesmer, for example in a conflict zone, to provide protection from detection, from drone threats, or to passively tap into opposition elements drone sensors to collect data such as raw video feeds without opposition being aware. In civilian setting a portable version of Mesmer could be used to provide ad-hoc defense for public speakers and VIP's.

Civilian Air Defense: Multiple Mesmer nodes could be setup around an airport and connect to the airport tracking systems. If drones penetrate a restricted area the drones can be stopped, redirected, or forced to

land at a safe zone. Since Mesmer can operate using low power modes, under a watt in many cases, or in a very surgical manner Mesmer will not interfere with critical ground based and ground to aircraft communication traffic.

Hard Kill Options

Protocol manipulation facilitates Mesmer's versatility and adaptability to unforeseen threats by enabling the operator to not only redirect drones to a specified location but also disable drones completely. Options to "hard kill" the drone include:

Flight Controller attacks: The Mesmer operator can choose to stop or crash the drone flight controller, resulting in the drone crashing into the ground or landing safely in place depending on the existence of a backup flight controller. Both results leave the drone disabled and unable to fly.

Severing the control link: A drone that has had its control link severed by Mesmer will either land in place or return to where it came. In some cases, the drone must be manually rebound to its controller before it can be flown again. This Mesmer mitigation enables the operator to "kill" but not physically destroy the drone, hence permitting forensic inspection.

Seizing complete control of the drone: By taking advantage of the same control mechanisms used by the drone's controllers", Mesmer can take complete control of the drone. The Mesmer operator can land the drone in place, land the drone at a user designated location, or completely lock the drone out from its controller and leave the drone hovering in midair.

Low level Software flaws: Due to the use of open source software in many Group 1 drones, Mesmer is also able to utilize a drone's control channel to effect services on the drone that are needed for its control. This results in a drone that can no longer be controlled; the drone will hover in mid-air till it crashes, land safely due to low battery, or the drone will be unable to take off.

i. Operational View (OV-1)

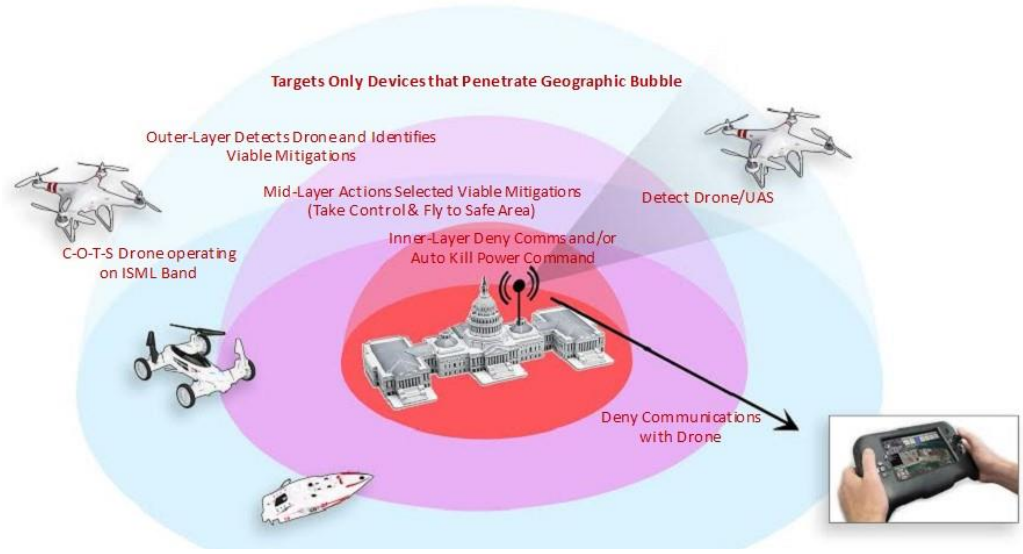

Figure 5: Operational view of how Mesmer protects assets against a variety of autonomous threats

j. Narrative of what it would take to be deployable and ready to use in an austere environment within 12 months.

D13 will launch the Mesmer product in 1QCY17. The Mesmer system will withstand environmental conditions in accordance with its specifications, in Table 1. The Mesmer system is designed to withstand wind gusts of up to 100mph. The enclosure is NEMA 4/4X compliant; however, if additional requirements such as increased temperature range or dust or shock exceed existing specifications, D13 will source a new enclosure to meet those operational requirements. For mobile applications, D13 will source a different enclosure for additional requirements for shock, active cooling and vehicle mounts.

k. Program, Product or System Security

Mesmer was built by computer security professionals to be secure from the ground up. Using mutually-authenticated SSL encryption and encryption certificates, all communications over any network are both confidential and secured using industry standard software. Mesmer also employs memory-safe programming languages and robust, mature software when decoding and analyzing drone communications, ensuring that drones can't attack Mesmer. In addition, internal network segments and firewalls contained within Mesmer ensure that any Wi-Fi connections established with target drones can't connect with any part of Mesmer that isn't designed to specifically handle that drone.

l. Information Exchange Requirements (IERs/ Interface Control)

Mesmer uses a custom API utilizing JSON and MQTT. Though the use of software gateways Mesmer can be adapted to interface with many systems. Interfacing to Mesmer can be facilitated using various formats, e.g., Ethernet utilizing TCP/IP protocol.