Hidden Level

LEGALITY OF AMS

Acquisition and Application of AMS

UAS detection and identification technology is a critical component of a comprehensive UAS security framework. Such technology can help address public safety and security concerns associated with unauthorized UAS by detecting rogue UAS whose operators may be engaged in nefarious behavior or seeking to intrude into sensitive or restricted airspace without permission. Therefore, legal considerations aside, there exists a strong public policy argument in favor of the ability to lawfully use UAS detection and identification technology.

In August of 2020, an interagency Advisory was issued from the Department of Justice, Department of Transportation, Federal Communication Commission, and Department of Homeland Security. The advisory outlines the questions and considerations for application and use of Counter UAS technologies. [1]

Hidden Level's Airspace Monitoring Service (AMS) operates by using multiple HL1000 sensors, which are passive RF sensors, to detect and track UAS. AMS does not record or attempt to analyze the information transmitted by the RF signals. However, by assessing the physical characteristics of RF signals transmitted by UAS and the direction from which RF signals are emitted, AMS can identify the type and location of a UAS. This analysis will focus only on issues relevant to passive RF technology and the interagency advisory.

[1] https://www.cisa.gov/publication/advisory-application-federal-laws-acquisition-and-use-technology-detect-and-mitigate

AMS Theory of Operation

An individual Hidden Level sensor (HL1000) sweeps its frequency range for characteristics of a signal of interest. Characteristics of a signal of interest include:

- Frequency, Bandwidth, Protocol, Altitude
- Video, Command and Control, and Telemetry RF links

In observing these characteristics, a single HL1000 sensor calculates a Line of Bearing (LoB)

- A LoB contains an estimated Azimuth and Elevation angle for a given signal of interest, which is a common technique called Direction Finding
- A LoB from two or more HL1000s produces an estimated 3D position location of a drone or operator

AMS detection methodology avoids collection of and reliance on Personally Identifiable Information (PII), breaking encrypted communications, and accessing underlying RF message content. Hidden Level's AMS system performs detection services only, no mitigation capabilities are built into the system.

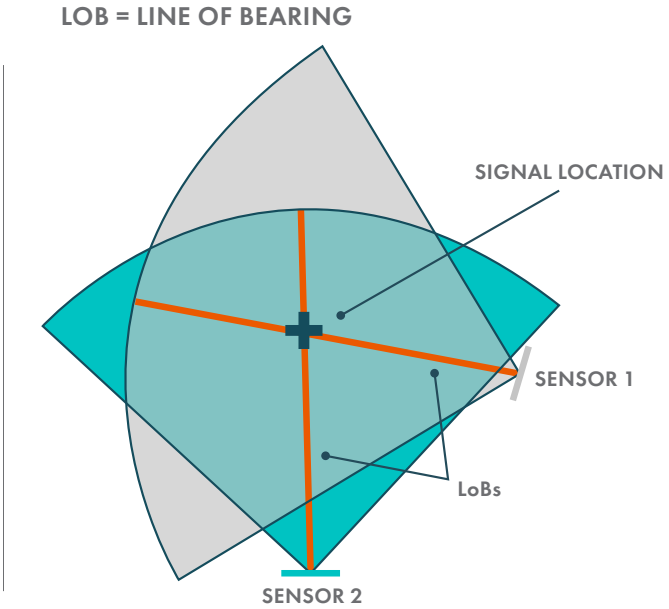
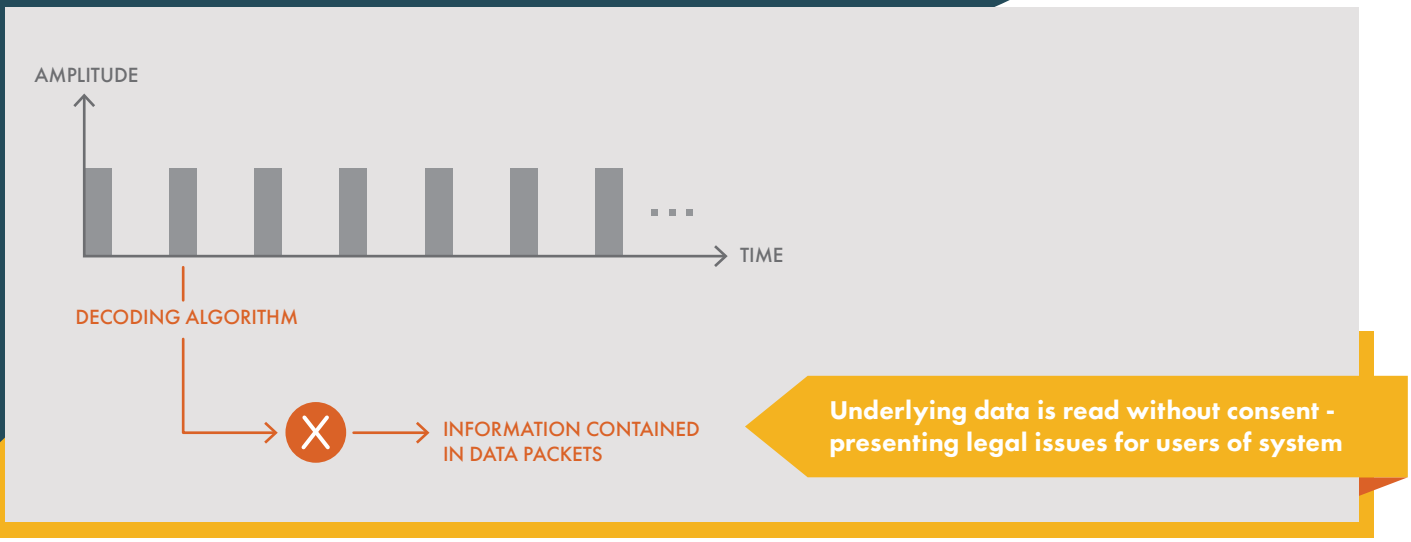


Figure 1. AMS Methodology for Determining Signal of Interest

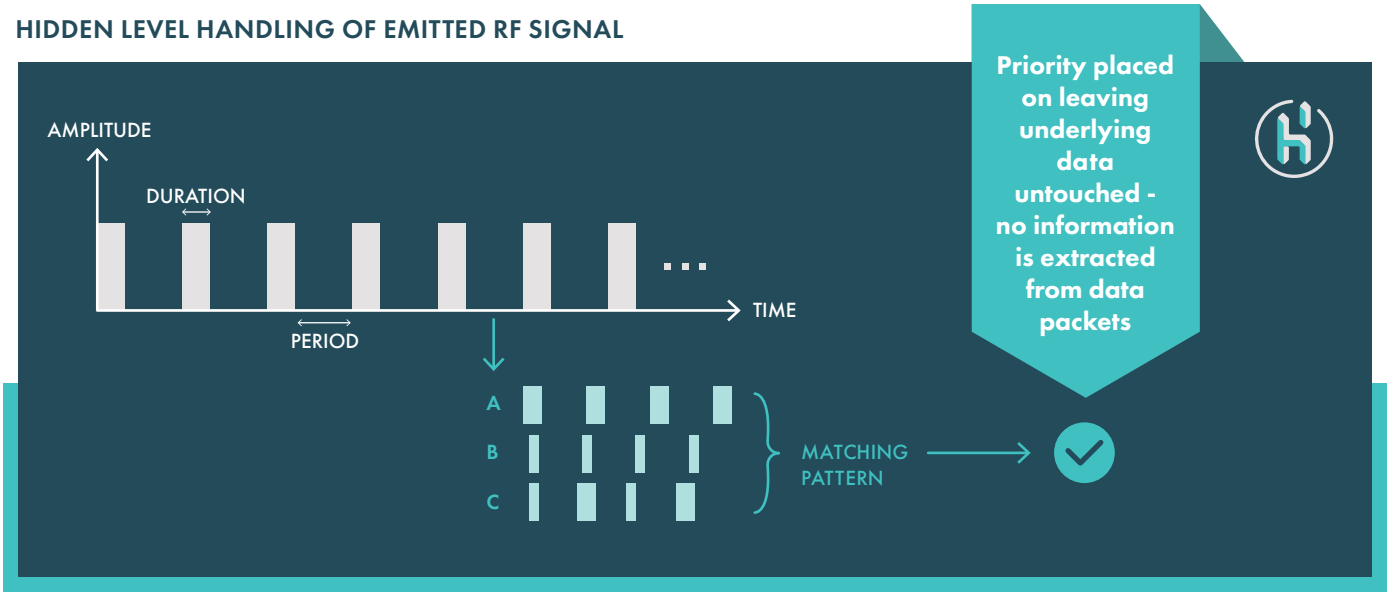
Detecting Drone Emissions

COMPETITOR HANDLING OF EMITTED RF SIGNAL



- Other systems demodulate (hack) the signal to read the information in the data packets
  - Includes craft identifier (serial number), location from GPS coordinates, and other information sent between craft and controller

HIDDEN LEVEL HANDLING OF EMITTED RF SIGNAL



- Hidden Level looks at the physical structure (packet duration, period between packets, etc) of the emitted signal and compares to a library of known drone links (A, B, & C)
  - If any match, Hidden Level knows that the RF signal is from a Drone
  - The Line of Bearing is calculated by comparing signal magnitude & phase between multiple channels on the HL1000

AMS Technology & Federal Statue Compliance

Since Hidden Level's AMS technology does not record or attempt to analyze the information transmitted by the RF signals, it is compliant with the three statues defined below. However, by assessing the physical characteristics of RF signals transmitted by UAS and the direction from which RF signals are emitted, the Technology can identify the type and location of a UAS.

1. WIRETAP ACT (18 U.S.C. §§ 2510)

The Wiretap Act prohibits the interception and disclosure of wire, oral and electronic communications, as well as the manufacture, distribution, and possession of such interception devices.

Hidden Level's AMS technology is compliant with the federal Wiretap Act as it does not record, capture, or otherwise acquire the contents of any electronic communication. Instead, AMS merely analyzes the physical characteristics of RF signals.

The Wiretap Act includes exceptions for radio communications that are transmitted "by any...aeronautical communications system". However, Hidden Level stays cautious of this potential carve out because the scope and exceptions intended by this statement are not well defined in the context of UAS and their RF communications from any existing case law.

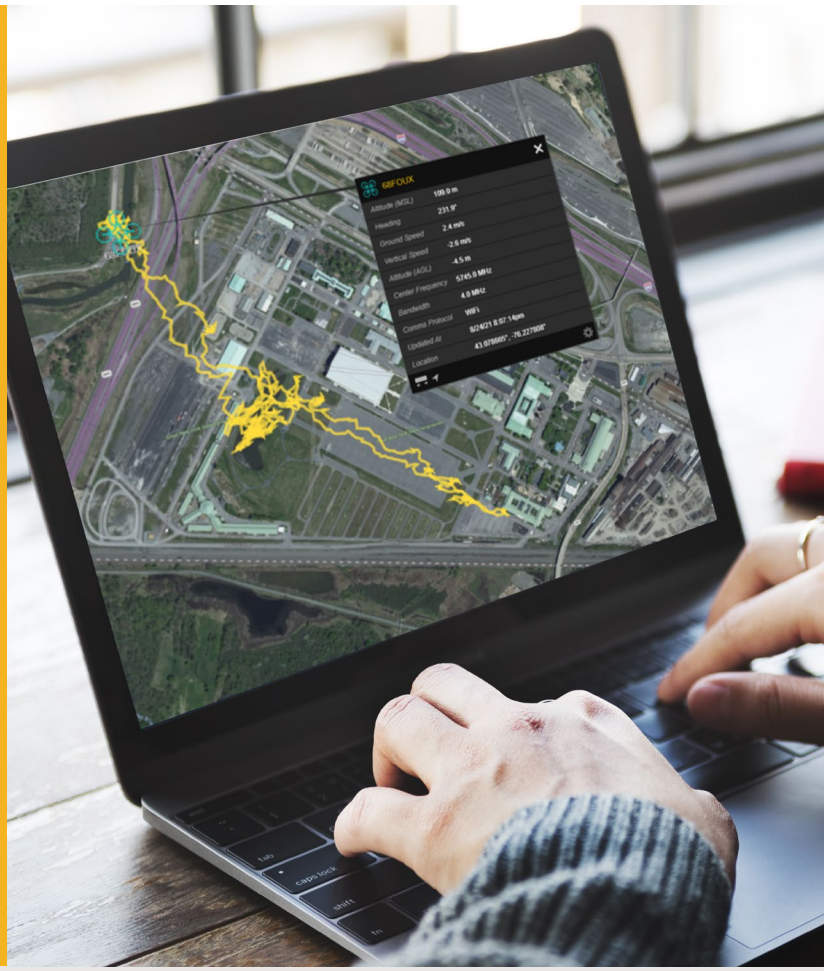


Figure 2. Example of Hidden Level AMS detection of a UAS using a WiFi based link. In this situation there are no other attributes to infer on the UAS because we are unable to extract information from the underlying communications

2. COMPUTER FRAUD AND ABUSE ACT (18 U.S.C §§ 1030)

The Computer Fraud and Abuse Act ("CFAA") is an anti-hacking statute primarily concerned with unauthorized intrusions into computers to steal information or to disrupt or harm computer functionality.[1] Under the CFAA, it is unlawful to "intentionally access a computer without authorization or exceed authorized access, and thereby obtain...information from any...computer [used in or affecting interstate or foreign commerce].[2]

AMS technology does not access the target UAS computer systems. Rather, it analyzes RF signals publicly transmitted by UAS. The Technology is therefore wholly outside of the scope of the CFAA.

[1] 18 U.S.C. § 1030.
[2] *Id.*

3. PEN/TRAP STATUTE (18 U.S.C. §§3121-3127)

The Pen Register Act prohibits any person from installing or using a pen register without first obtaining a court order. A pen register is a device or process that "records or decodes dialing, routing, addressing, or signaling information ***transmitted by an instrument or facility*** from which ... a[n] electronic communication is transmitted, provided . . . ."[3]

The Pen Register Act applies only to the capturing of information transmitted by instruments or facilities. AMS does not capture information transmitted by or contained in RF signals. Instead, it analyzes the physical characteristics of RF signals.

Despite being able to identify the signal type and estimate its location, AMS is unable to distinguish between different model of aircraft that use Ocusync (Mavic, Phantom 4 Pro). Additionally, Hidden Level AMS is unable to determine Serial Number/Unique ID or the UAS/ Operator exact coordinates, as these are inaccessible parts of the RF transmission underlying content without decoding or capturing content.

[3]18 U.S.C. § 3127(3) (emphasis added).

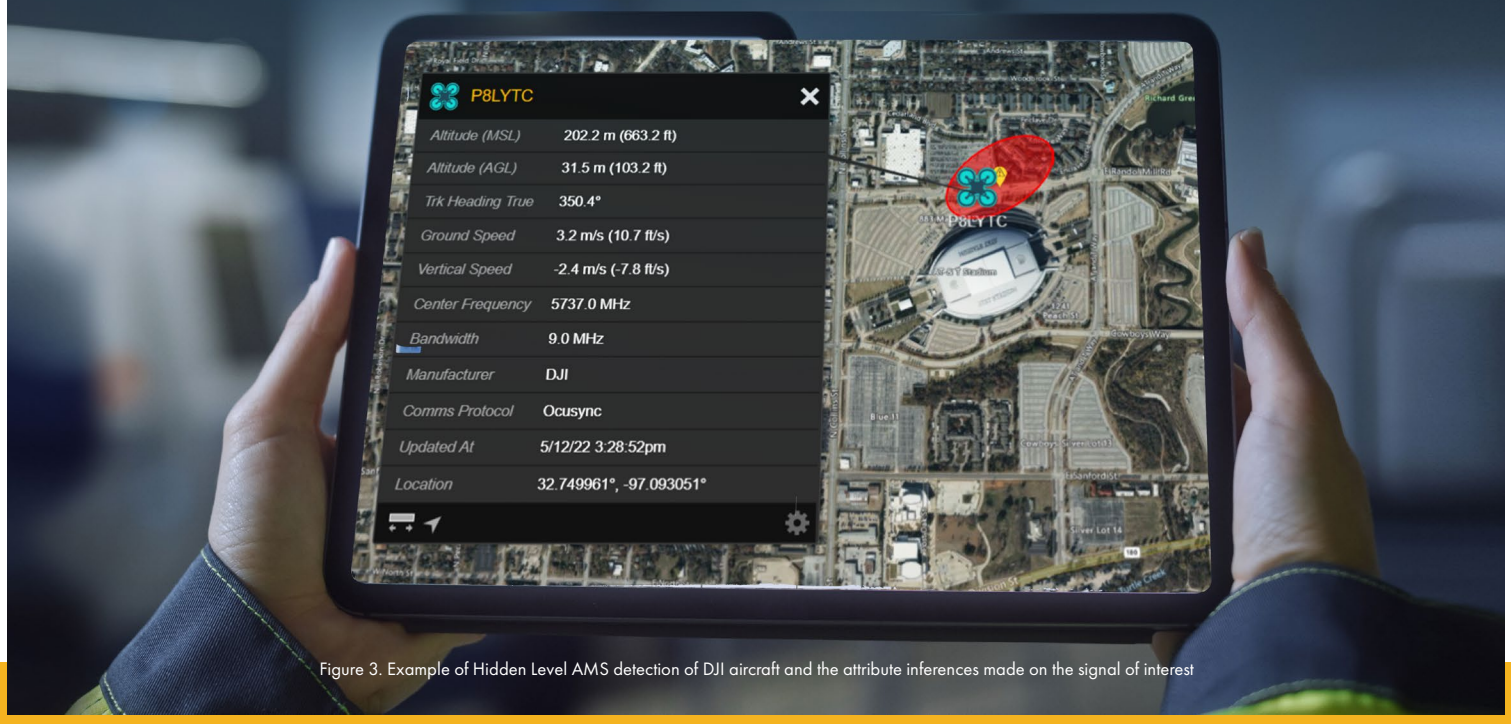


Figure 3. Example of Hidden Level AMS detection of DJI aircraft and the attribute inferences made on the signal of interest

Hidden Level, Inc | 1014 N Geddes Street | Syracuse, NY 13204 | info@hiddenlevel.com | hiddenlevel.com

Direct Contact: James Licata | james.licata@hiddenlevel.com