**Phuc Nguyen, Hoang Truong, Mahesh Ravindranathan,
Anh Nguyen, Richard Han and Tam Vu**
University of Colorado Boulder

Editors: Nic Lane and Xia Zhou

COST-EFFECTIVE AND PASSIVE RF-BASED DRONE PRESENCE DETECTION AND CHARACTERIZATION

Excerpted from "Matthan: Drone Presence Detection by Identifying Physical Signatures in the Drone's RF Communication," from MobiSys 2017, *Proceedings of the 15th Annual ACM International Conference on Mobile Systems, Applications, and Services*, with permission. https://dl.acm.org/citation.cfm?id=3081354

The rapidly increasing attention regarding drone privacy and security issues requires a robust solution in both detecting and characterizing unauthorized drones. We have designed a RF-based, cost-effective and passive drone detection system, named *Matthan*, based on two key physical signatures of the drones, i.e., body shifting and body vibration, in the drone's wireless communication channel. In realizing Matthan, there are many open challenges in wireless sensing and networking, software-defined radio deployment, network synchronization to passively and accurately detect, localize, and characterize drones.

Drones have been rapidly rising in popularity as a host of a wide class of applications including commercial delivery, photography, environment monitoring, and fire-fighting due to the advent of inexpensive commercially available unmanned aerial vehicles. However, unauthorized drones are increasingly flying in sensitive airspace, where their presence may cause harm, such as crowded events, airport areas, forest fires, and even jails. For example, Dubai airport, the third busiest airport in the world, had to shut down three times in 2016 to avoid unauthorized drone activities [2]. A quadcopter crashed on the White House lawn [3], raising concerns about the safety of buildings and political leaders. The presence of drones interfered with and grounded aircraft fighting forest fires [4].

A variety of approaches have been explored to take down the drones. These include shooting nets at the drones to tamper with their propellers to bring them down [5], using lasers to shoot down drones [6], spoofing GPS to confuse a drone's localization system [7], hijacking the software of drones by hacking into them [8], using other drones to hunt down unauthorized drones [2], and even training eagles/hawks to attack and disable drones [9]. However, these interdiction strategies typically presume that the presence of the drone has already been detected. Recent work has sought to develop drone detection systems using microphone, camera, or radar to sense the presence of drones. Each of these approaches has its own limitations of detection range, environmental condition dependence and interference with surrounding wireless environment.

We have proposed a passive sensing approach, named Matthan, to detect the presence of a drone by listening on the RF communication between a drone and its controller [1]. Such communication mode often happens over standard unlicensed spectrum for which a low-cost COTS hardware can be utilized for observation. We have studied the fundamental aerodynamic and motion control mechanisms of drones

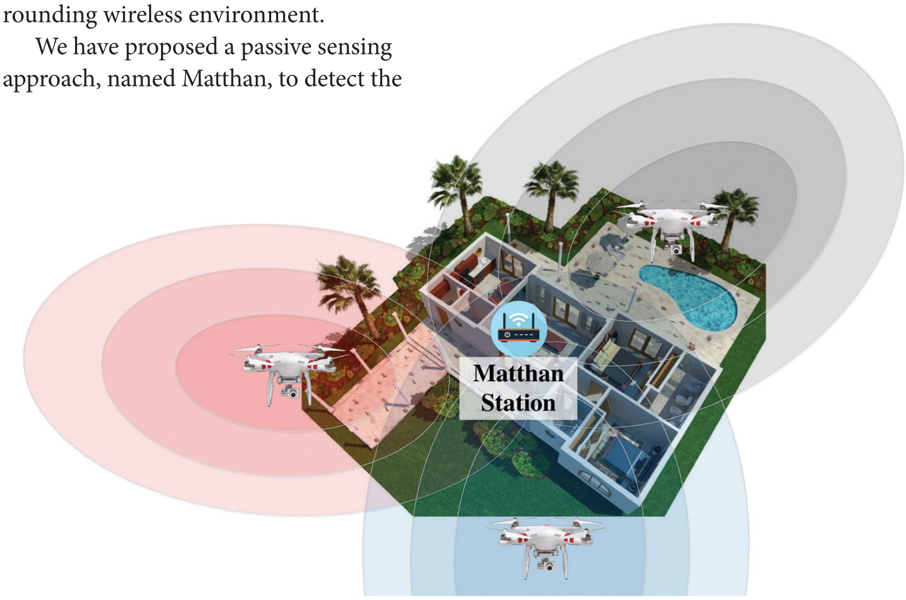


FIGURE 1. Passive RF-based drone detection system.

to identify two key inherent types of movement of the drone's body, namely "body shifting" caused by the spinning propellers and "body vibration," due to navigation/communication and environmental impact corrections. The proposed system employs low-cost software-defined radios (SDRs) to eavesdrop on wireless channels used in drone-to-controller communication. We envision a passive and cost-effective drone defense system as shown in Figure 1, in which a passive RF receiving station can detect the presence of nearby drones.

DRONE DETECTION

Multiple sensing modalities have been employed for drone detection, including audio, video and RF. Acoustic signatures from different drones have been collected to build a database which is later used to give a decision on drone presence. This approach has drawbacks of low-detection accuracy in a noisy urban environment, complexity in maintaining the database and ineffectiveness with drone models with noise-canceling techniques. Visual and thermal signatures have been utilized to detect the drone in video-based solutions. These techniques have limited coverage, and suffer from low-light condition and line-of-sight blockage due to building [1].

In addition, various RF-based solutions for drone detection also attract the attention of researchers. Geofencing is useful to prevent drones from flying into fixed areas known a priori as sensitive [10], but requires manufacturers to install such software and is less useful to prohibit drones from flying around temporary event venues. Radar-based techniques are the most popular approaches, in which active radars transmit RF waves and capture the reflection to determine the presence of the drone; or passive bistatic radar processes a received signal from a known source of transmission and reflected signals from the moving target. In conjunction with the usage of abundant Wi-Fi sources as reference transmitters, multiple algorithms have been proposed for signal processing in passive biostatic radar systems, such as MTI and LS adaptive filters or compressive sensing. However, there are many disadvantages of using this approach due to the limitation of the radar angle, lack of high precision and expensive system deployment. Moreover, radar in general introduces interference due to active transmissions, which is especially problematic when there is a large amount of legitimate packet traffic over RF bands, such as Wi-Fi, especially in crowded environments.

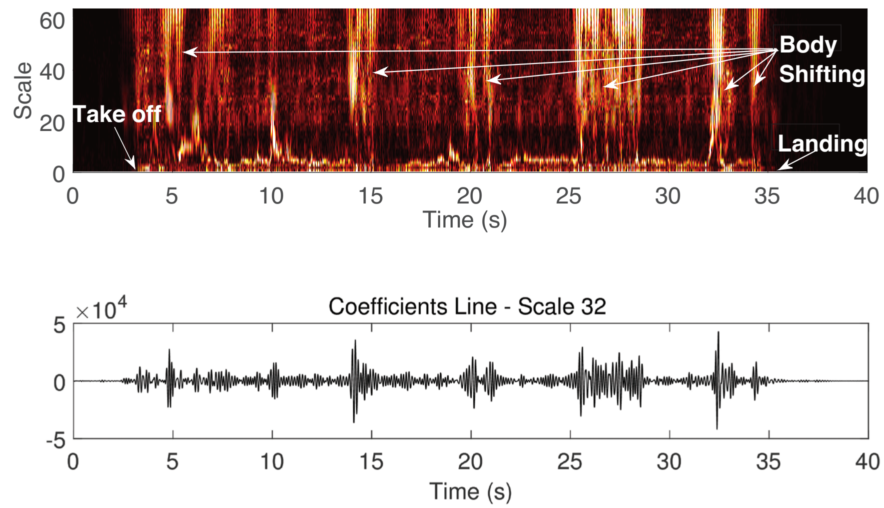


FIGURE 2. An example wavelet analysis of body-shifting detection.

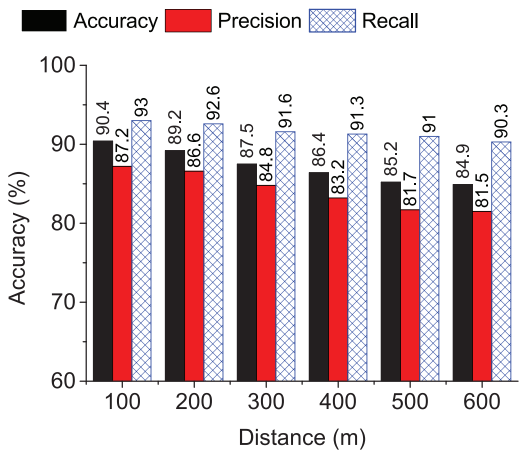
BUILDING A COST-EFFECTIVE AND PASSIVE DRONE DETECTION SYSTEM

Matthan detects the drone by recognizing the drone body shifting and drone body vibration from the drone's RF communication channel. Building Matthan is difficult because of the following reasons:

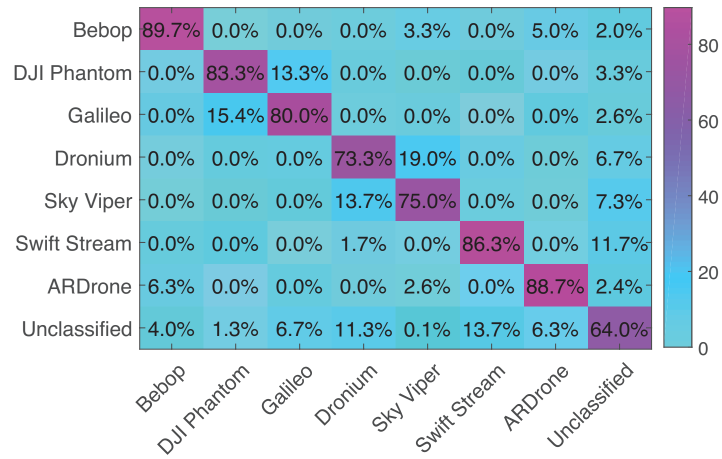
- *Identifying the drone's unique signatures.* Finding the signatures that uniquely represent the drone presence, by which the system could detect the drone at a long distance and at different weather conditions, is challenging. These criteria make active radar, acoustic signature-based and vision-based techniques unusable.
- *Drone movement to RF translation.* The drone body movement information are buried in the wireless signal. This limits the maximum detection range that can be obtained from the system at different environments.
- *The drone physical signatures can happen at different scales.* Different drones create different signatures of body shifting according to their controlling mechanism and accuracy, as well as their physical characteristics (weight, structures, etc.). The signal can be detected at different magnitudes as well as frequencies.
- *Interference from other wireless sources.* A mobile access point (AP) carried by a human walking or an embedded AP on a moving vehicle (e.g., bus) could create similar wireless signals to the drone, which could affect the detection results. The detection algorithm should be able to distinguish between the signals from the static/mobile APs and the signal from the drone.
- *Variety of drones.* There are many different type of drones having different numbers of propellers, weights, sizes, speeds, and communication mechanisms.

To overcome these challenges, Matthan has employed an evidence-based algorithm taking the input from Wavelet and Fourier analysis to make the final decision for detecting the two key physical characteristics of the drones, i.e., the body shifting and body vibration.

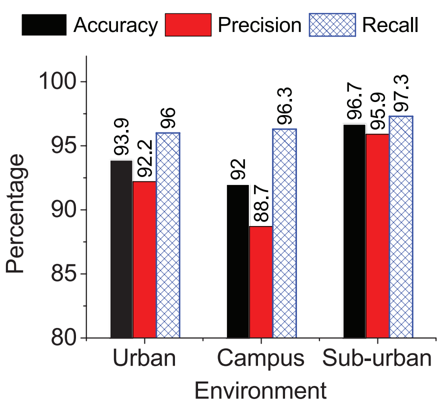
- *Drone Body-Shifting Detection.* A wavelet is a wave-like oscillation with an amplitude that begins at zero, increases, and then decreases back to zero. Wavelets are especially good at capturing brief oscillations. From the results of our experiments, we found that the behavior of the drone body shifting is similar to the form of a wavelet. This characteristic



(a) Matthan is able to detect the drone at a distance of hundreds of meters with high accuracy.



(b) Matthan is able to classify 7 different types of drones based on their body vibration signature.



(c) Matthan is also able to detect the drone at different environments.

FIGURE 3. Matthan's performance in detecting a drone at different distances (a), classifying different drones (b), and detecting the drones at different environments (c).

will result in high coefficients when multiplying the wireless signal with scaled versions of the mother wavelet. As the discontinuity (generated by body shifting) is considered to be an event and happens quickly in time, the result of correlation with high-frequency wavelet will be readily captured. Figure 2 illustrates the results of wavelet analysis on the captured RF signal emitting from the drone's RF antenna. The coefficients are used to identify the shifting body events.

- *Drone Body Vibration.* The drone's vibration creates a periodic signal that is well-reflected in the FFT-based spectrogram. Conversely, a wavelet transform that is better suited for capturing transitory phenomena, such as a body shifting event, is not well-suited for drone vibration detection. Consequently, we employ a frequency domain approach to identifying the presence of the drone's vibration signal. From the received wireless samples, an efficient approximation of the drone's vibration frequency is used to identify the dominant frequency component that has maximum power density through the Short-Time Fast Fourier Transform (STFT). The STFT analysis will result in the central frequency of the vibration. That frequency is used to infer the phase and the amplitude of the signal.
- *Evidence-Based Drone Detection Algorithm.* We design an algorithm to determine a drone's presence by first gathering evidence from multiple sources that relate to drone body shifting and vibration, then combine these sources of evidence to form a binary classifier. The different forms of evidence are collected at each time window. The decision is made based on the number of forms of evidence that are confirmed on each window. We sort the evidence based on its uniqueness as the signature for drones. All the evidence is combined linearly for the final decision of detection. That is, Matthan concludes that a drone is present only when all the forms of evidence are confirmed [1].

PERFORMANCE EVALUATION

Matthan was prototyped and evaluated using SDRs in three different real-world environments (urban, campus, suburban). We implement Matthan using the USRP B200 mini. The USRP board is sampled at 100 kHz to collect wireless samples from the drone's communication channel. The USRP board is configured as a receiver connecting to a 2.4GHz 20dBi gain directional antenna. The experiment is conducted in three different environments, including a soccer field inside our university (campus), a parking lot in the downtown of a city (urban), and an open field (suburban). In each environment, the data are collected when the drone is flying at a different distance with respect to our receiver. The drone is controlled to take off and hover within the coverage area of the antenna receiver's beam during all experiments.

We showed that Matthan is capable of differentiating drone signals from other mobile wireless devices by achieving high accuracy, precision and recall, all above 90% at 50 meters. Matthan's accuracy, precision and recall varies with distance, dropping to 90% accuracy and 80 to 85% precision and recall at a distance of 600 meters (Figure 3a). Matthan's performance was studied across seven different drones (Protocol Dronium, Sky Viper, Swift Stream, Parrot Bebop, Parrot ARDrone, Protocol Galileo Stealth, and DJI Phantom) as illustrated in Figure 3b. Matthan was also tested across three different environments, including urban, campus, and suburban. As shown in Figure 3c, Matthan obtains 93.9%, 92%, and 96.7% accuracy at urban, campus, and suburban environments, respectively.

REMAINING CHALLENGES

While Matthan has contributed to the first milestone on detecting the presence of the drone based on its body shifting and body vibration, the challenges in making Matthan work in real-time, characterizing the drone structure and detecting multiple drones at the same time are unsolved. These challenges are as following:

- *Automated antenna steering/beamforming.* Currently, Matthan can only detect the drone when it is flying inside the coverage area of Matthan's directional antenna. Matthan should also be enhanced to integrate automated antenna steering to continuously tracking the drone and reduce the delay of detecting and characterizing the drone signatures.
- *Extending the detection range.* Matthan is currently evaluated using seven different types of Wi-Fi drones with a maximum distance of 600 meters. We wish to expand our experiments to consider a wider variety of drones, which use different wireless standards for communication, and at kilometer distances.
- *Localizing the drones.* Even though localizing the drone is not the focus of the current design of Matthan, it is definitely a next logical step. In that, Matthan needs to accurately localize the drone after detecting it.
- *Characterizing the drones.* While Matthan illustrates a first step of classifying different drones utilizing drone's body vibration signature, this signature is not sufficient for a large-scale scenario. We propose to classify the drones by characterizing them in detail, such as cargo load, number of propellers, manufacturers' features, and so on. Such information requires a novel wireless architecture and method to realize the idea.
- *Detect multiple drones at the same time.* Matthan is currently not capable of detecting multiple drones in the same vicinity at the same time. We believe that a multimodality approach of combining an RF-based, acoustic-based, and video-based solution in a cost-effective manner may become a neat solution to make the system ready for massive deployment to detect multiple drones at the same time.

SUMMARY

In this article, we have introduced Matthan, a cost-effective and passive RF-based drone detection system. Our system detects the presence of drones by identifying the unique signatures of its body vibration and body shifting in the transmitted wireless signals. The joint detector integrates evidence from both a frequency-based detector that indicates drone body vibration as well as a wavelet-based detector that captures the sudden shifts of the drone's body by computing wavelets at different scales from the temporal RF signal. We also envision that a future drone-defense system could detect and localize single or multiple drones at the same time. ■

Phuc "VP" Nguyen is a PhD student at the Department of Computer Science, University of Colorado Boulder. He received a BS from Vietnam National University in 2010 and a MS from Sungkyunkwan University (SKKU), Seoul, South Korea in 2014. His research interests include mobile computing, wireless short-range communication, wireless sensing, and wireless security.

Hoang Truong received a BS in Electrical & Electronic and MS in Computer Science from KAIST, South Korea, in 2012 and 2014 respectively. He is pursuing a PhD in Computer Science at the University of Colorado Boulder. His research interests include mobile security, wearable sensing and wireless communication.

Mahesh Kumar Ravindranathan received a BE in Electronics and Communication Engineering from Bangalore Institute of Technology, Bangalore, Karnataka, India in 2012, and a MS in Computer Science from the University of Colorado Boulder in 2016. He is currently working as a Data Streaming Engineer at Oracle.

Anh Nguyen is a PhD candidate in the Department of Computer Science at the University of Colorado Boulder. She received her MS at Chonnam National University in 2012 and BE at the University of Science in 2009. Her primary research interests are in mobile systems, with emphasis on applying sensing techniques for mobile health care.

Richard Han is an Associate Professor of Computer Science at the University of Colorado Boulder. He received his BS in Electrical Engineering with Distinction from Stanford University in 1989, and his PhD in Electrical Engineering from the University of California at Berkeley. His research interests include mobile and cloud systems, wireless sensor networks, cyber-safety, and cyber-physical systems.

Tam Vu received a BS in Computer Science from Hanoi University of Technology, Vietnam in 2006, and a PhD in Computer Science from WINLAB, Rutgers University in 2013. He is currently an Assistant Professor and Director of the Mobile and Networked Systems Lab at the Department of Computer Science, University of Colorado Boulder. His research interests are wireless sensing, mobile healthcare, mobile centric network, mobile communication, and mobile security.

REFERENCES

[1] Phuc Nguyen, Hoang Truong, Mahesh Ravindranathan, Anh Nguyen, Richard Han, and Tam Vu, "Matthan: Drone presence detection by identifying physical signatures in the drone's RF communication." Proceedings of ACM MobiSys '17, pages 211-224.

[2] CNN. "Dubai deploys a 'drone hunter' to keep its airport open." https://goo.gl/iXJMu3, 2017.

[3] B. Jansen. "Drone crash at White House reveals security risks." *USA Today*, Jan. 26, 2015.

[4] P. McGreevy, "Private drones are putting firefighters in 'immediate danger,' " California fire official says. *LA Times*, Aug. 18, 2015.

[5] A. Rozantsev, V. Lepetit, and P. Fua, "Detecting flying objects using a single moving camera." IEEE Transactions on Pattern Analysis and Machine Intelligence, pages 879 – 892, 2017.

[6] R. Vander Schaaf. "What technologies or integrating concepts are needed for the US military to counter future missile threats looking out to 2040?" PhD thesis, US Army, 2014.

[7] T. Humphreys, "Statement on the security threat posed by unmanned aerial systems and possible countermeasures," Submitted to the Subcommittee on Oversight and Management Efficiency of the House Committee on Homeland Security, 2015.

[8] J.-S. Pleban et al. Hacking and securing the AR Drone 2.0 quadcopter: investigations for improving the security of a toy. *SPIE Electronic Imaging*, 2014.

[9] BBC. "Dutch police fight drones with eagles." https://goo.gl/PnJCcd, Nov. 07, 2017.

[10] Samantha Masunaga. "To keep drones out of high-risk areas, companies try hijacking them and shooting them down." https://goo.gl/MqDag5, *LA Times*, Nov. 07, 2017.