IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 19, 2018, accepted April 3, 2018, date of publication April 17, 2018, date of current version May 16, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2827362

Reliable Security Algorithm for Drones Using Individual Characteristics From an EEG Signal

ASHUTOSH SINGANDHUPE[1], HUNG MANH LA[1], (Senior Member, IEEE), AND DAVID FEIL-SEIFER[2], (Member, IEEE)

[1]Advanced Robotics and Automation Laboratory, Department of Computer Science and Engineering, University of Nevada, Reno, NV 89557, USA
[2]Robotics Research Laboratory, Department of Computer Science and Engineering, University of Nevada, Reno, NV 89557, USA

Corresponding author: Hung Manh La (hla@unr.edu)

This work was supported in part by the National Aeronautics and Space Administration (NASA) issued through the Nevada NASA Space Grant under Grant NNX10AN23H, in part by the Nevada NASA Research Infrastructure Development Seed Grant issued through under Grant NNX15AI02H, and in part by the National Science Foundation under Grant IIS-1528137.

ABSTRACT Unmanned aerial vehicles (UAVs) have been applied for both civilian and military applications; scientific research involving UAVs has encompassed a wide range of scientific study. However, communication with unmanned vehicles are subject to attack and compromise. Such attacks have been reported as early as 2009, when a Predator UAV's video stream was compromised. Since UAVs extensively utilize autonomous behavior, it is important to develop an autopilot system that is robust to potential cyber-attack. In this paper, we present a biometric system to encrypt communication between a UAV and a computerized base station. This is accomplished by generating a key derived from a user's EEG Beta component. We first extract coefficients from Beta data using Legendre's polynomials. We perform encoding of the coefficients using Bose-Chaudhuri-Hocquenghem encoding and then generate a key from a hash function. The key is used to encrypt the communication between XBees. Also we have introduced scenarios where the communication is attacked. When communication with a UAV is attacked, a safety mechanism directs the UAV to a safe home location. This system has been validated on a commercial UAV under malicious attack conditions.

INDEX TERMS UAV, xbee, EEG signal, encryption, advanced encryption standard (AES).

I. INTRODUCTION

The role of Unmanned Aerial Vehicles (UAVs) in civilian airspace has been growing, ranging from public safety applications, to commercial use, to personal use by hobbyists [42], [43]. The increasing affordability of UAVs has broadened their use by hobbyists and enthusiasts, companies, and government agencies [34], [35]. This has subsequently led to the occurrence of severe incidents of different type of attacks on both military and civilian UAVs. Security flaws have been demonstrated in recent investigations of inexpensive consumer UAVs, revealing these systems to be vulnerable to attack.

Commercial activities such as Google's "Project Wing" [25], which has successfully tested its drones for food delivery, and Amazon's "Prime Air" service [2], which aims to provide same-day package delivery, would place several drones in commercial airspace, near population centers. This increases the number of UAVs in civilian airspace and their proximity to people. This increases the potential for, and interest in, cyberattacks on those UAVs. These threats need to be addressed in order to ensure that a UAV completes its mission and is not used for a malicious purpose.

In this work, we propose a technique that secures the UAV communication to the ground control station. The proposed technique can generate an Advanced Encryption Standard (AES) encryption key, which is derived from an operator's Electroencephalogram (EEG) signal. We have also demonstrated a safety mechanism, which is activated in the case of a third-party attack, to secure the UAV. This entire system was validated on a commercially available UAV.

Most current commercial UAVs (e.g., Parrot, DYI, DJI, Dragonfly, PlexiDrone, DreamQii Robotics, etc.) are equipped with XBee modules [8] and Bluetooth, which run the IEEE 802.15.4 protocol, for enabling the control message exchange between drones and the controller. To secure the exchanged information, the IEEE 802.15.4 protocol provides authentication and encryption to prevents unauthorized parties from participating in the network and protect data confidentiality. These security goals are achieved by incorporating a message authentication code (MAC) generated by authorized senders and receivers with a shared secret cryptographic key and the AES block cipher. However, the open nature of wireless medium brings severe threats to drone communication resulting from unauthorized access and data leakage [4]. To enhance the security of the drone and base station communication, we have performed the testing on a UAV, encrypting its communication to the ground control station by configuring the XBee's AES encryption key using an EEG biometric key. After configuring the Xbee, we create a simple attack scenario where the third party or attacker is aware of the key and tries to attack the communication from the UAV to the ground control station. We test our proposed safety solution that enables the UAV to detect that an attack has been attempted and should return back to the ''home'' station.

II. RELATED WORK

There have been several incidents where the UAVs have been remotely compromised, taking control of the UAV or making it crash-land. The first known attack was initiated by the Iraqi militants in 2009, when they gained access on a Predator Drone (UAV) [12]. Later in October 2011, a key-logging malware was detected on a Predator and a Reaper ground control station, which propagate to both classified and unclassified computers [31].

The claimed theft of a Sentinel RQ-170 UAV by Iranian forces in December 2012 was a troubling incident. Hostile agents were able to compromise the control system of the craft and remotely land the UAV, obtaining crucial information which includes mission plan and maintenance data. There are competing theories regarding how the RQ-170 Sentinel may have been lost. The simplest theory is that a technical malfunction caused the UAV to mistakenly land in Iranian territory [14]. A more nefarious possibility is that, through a vulnerability in a sensor system, the UAV's global position system (GPS) could have been intentionally fooled into landing to a location where the hostile agent intended. This type of attack is generally referred to as a ''GPS-Spoofing'' attack [11], [14]. An example of this type of attack was demonstrated using relatively inexpensive equipment, spoofing the GPS and taking complete control of the UAV [15], [32], [33].

UAV infrastructure is moving towards more network-centric command and control, where components are interconnected through mesh networks [6]. Some military UAV systems, specifically the Global Hawk, have infrastructure of this type already. Public safety and disaster management UAVs are also moving to a similar network architecture for planning and communication [19]. This enables fast communication and constant environmental and asset awareness, but introduces security drawbacks. Most elements of the UAV system are interconnected through a network, so if one component fails, it would affect the other components which might result in malicious behavior throughout the system.

Certain simulation-based testing with active military UAV pilots have examined whether the autonomous behavior could provide a secure and safe solution to an attack. They determined that the best course of action includes navigating to an earlier way point or switching from GPS-guided navigation to less precise, but more reliable navigation [15].

An interesting perspective considers a scenario of vendor and an attacker as a zero-sum network interdiction game. From vendor's perspective, the aim is to determine an optimal strategy that evades attacks along the way during its travel from source location to a destination point. It also takes the expected delivery time into consideration, thereby maximizing the security of the UAV's communication. Similarly, from attacker's perspective, the aim is to choose the optimal attack locations along the path. This could result in potential physical or cyber damage which would eventually maximize delivery time. Mathematically it was shown that this ''network interdiction'' game is similar to a ''zero-sum matrix game''. This results in two linear programming (LP) equations whose solutions attains the Nash Equilibrium (NE). Solving the LPs would give the expected delivery time under different conditions [41].

Biometric UAV authentication has largely been limited to facial recognition alone. Facial authentication is problematic, since it can be easily deceived by an attacker if they have a picture or significant visual cues of the actual operator [3]. Various research has been done in implementing EEG-based encryption on different security systems. For example, in multilevel security systems a technique is proposed to authenticate users using information from the EEG data by performing motor imagery tasks [36]. Another approach proposes to use rich information like gender and age carried out by EEG signals to perform user authentication [37]. However, its application to UAV systems are yet to be implemented, which motivated us to pursue this research. We propose to use EEG signal characteristics to secure communication between an operator and a UAV.

III. WIRELESS COMMUNICATION WITH A UAV

In wireless communication, the transmitter role is to feed a signal to an antenna for transmission. The radio transmitter encodes the data into RF waves, which are projected to a receiver. The receiver decodes data that comes from the receiving antenna. The receiver also performs the task of accepting and decoding specific RF signals while rejecting unwanted or redundant data. The space between the transmitter and receiver is called the environment. Xbee is one of the mobile communicating devices that can be mounted on a UAV for its communication with the ground control station. Xbees only communicate with other Xbees (Fig. 1). Xbees operate on the Zigbee protocol, following the IEEE 802.15.4 international standard. XBee is a product line and a brand name developed by Digi International [8]. XBees have the IEEE 802.15.4 standard in the bottom layer, but also they have their own suite of protocols layered on top. The IEEE 802.15.4 standard is a suite of protocols that allows communication through low cost and low powered devices [8].

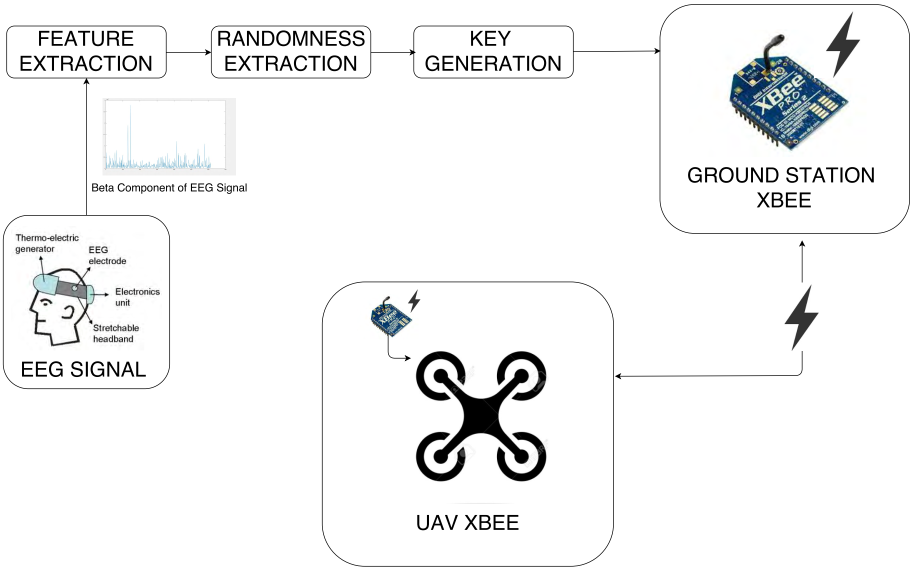


FIGURE 1. **Basic block diagram of the system overview.**

To achieve greater transmission range, Zigbee also allows mesh networking functionality in addition to the IEEE 802.15.4 standard. Mesh networking forwards messages from one node to another to reach the destination node through the network. The frequency band used for transmission determines the transmission speed. XBee devices can also run Zigbee compliant software, but need to be flashed with the Zigbee firmware. This results in losing the XBee implementation advantages, but allows for full connectivity with other Zigbee compliant devices. The manufacturer of XBee 868LP devices, which use proprietary multi point protocols, specifies the device's range to be 40 km. XBee devices do not require the coordinator and end-device to be configured in the network. In addition, the XBee 868LP chip uses Listen Before Talk (LBT) and Adaptive Frequency Agility (AFA) to check whether the channel is independent, and the data can be sent. This potential allows multiple varied networks to coexist, which allows dynamic data transfer [10].

Another framework, Killerbee [45], has both Zigbee and the IEEE 802.15.4 based networks. Killerbee prevents Denial of Service (DoS) attacks on nodes by setting repeated connections, replay previously recorded, sniffing and dumping traffic, etc. However, to run the framework specific hardware is required. It runs with three different USB dongles with 2.4 GHz radio device, which makes it incompatible with 868 Mhz band. Killerbee can also be integrated with GoodFET hardware debug tool. Other research has indicated that GoodFET mentions a common issue in Texas Instruments and Ember chips to extract RAM (Random access memory) even on a locked chip. It allows the user of both devices to look in an encrypted packet and then apply the correct key to decrypt the packet by trying all possible combinations in the RAM.

To test the experiment, 2 XBee modules are required. The below-mentioned data are needed to transfer the data from one XBee to another XBee (Point-to-Point) data. It could be changed if the user had physical access to the device.

- PAN ID
- Channel
- Baud Rate
- Device High (DH) address
- Device Low (DL) address

The device comes with the default values for Channel, PAN ID, and Baud Rate [7]. It allows the change of Device High (DH) and Device Low (DL) address for the customer to test the device quickly. The user needs to only change the DH and DL address of the other device so that it can communicate [7]. The UAV manufacturer does not change any parameters except for the DH and DL parameters. It uses default values for the rest of the parameters. There are different possibilities to get information about the DH and DL values:

- Physical access: Reading them from the cover of the chip;
- Physical access: Reading from the storage of the chip;
- Software Defined Radio;
- Brute-Force.

Once the parameters are known by the attacker, fake data can be sent, and different types of attacks can be performed. However, this simple scenario is not fairly possible, since the chips are hidden in the hardware of the user, and the attacker is unaware of the physical address.

A. XBEE MODES

There are two different working modules of XBee. The initial setup for basic communication is called the transparent mode. In transparent mode, all the data received by the chip through a serial interface is interpreted as payload and wrapped in a packet. The chip adds the DH and DL values with the preamble and network ID from memory. To communicate with another chip, the DH and DL values needs to be changed [9].

Another mode that exists in XBee is the Application Programming Interface (API) mode. In this mode, the receiver expects payload plus API-frame which includes payload. In the API-frame, the destination address can also be specified along with other parameters. This provides a benefit of not changing the DH and DL address every time the destination needs to be changed for the payload. Simply the API-frame can be sent to the device with the destination address specified in the frame itself.

B. BROADCAST MODE

The XBee chip disposes of all packets that are received. However, it contains another address than its own in the destination address field. There is another alternative, which was found; the utilized XBee gadgets take into consideration sending and receiving of communication packets. Also, each received packet, which is viewed as legitimate by the chip autonomous of the sender's address, will be recognized by the accepting chip. Regardless of the possibility that the receiving chip has an alternate destination address put away in its memory, it will return an acknowledgment [38].

This element is utilized as a part of the product XCTU for a device called "Node Discovery." This permits the client of one XBee chip to find different devices in a range, which are utilizing a similar preamble and network ID. This usefulness can be effectively manhandled for pernicious purposes as the acknowledgment uncovers the address of the reacting chip.

The main measure to confound discovery of the utilized network is to change preamble and network ID. The parameters are checked in the firmware of the chip upon supply of a packet. On the off chance that the estimations of the preamble or network ID are not coordinating to the ones present on the chip, the frame is not sent to the serial connection, but rather specifically disposed of. This was initially actualized to keep from interfering with other network in range and over-burdening the serial output of the chip with information from different networks. Since the chip is restrictive, and just proprietary firmware can be introduced, it is impractical to compel the chip to forward such packets. If this were possible, the preamble and network ID would likewise not contribute extra haziness [10], [38].

XBee gives a probability of changing the parameters remotely. By sending the correct API frame having the DH (or DL) parameter with another value, the remote chip will briefly utilize the recently received address. To persevere the change, another API frame with the Write (WR) command is required. As no integrity checks are played out, an attacker is additionally ready to remotely change the DH and DL address of an any given XBee chip and can along these lines divert the entire information exchange. When this is done, the attacker has the whole control over the channel.

C. XBEE ON-BOARD ENCRYPTION

Encrypting the channel would ensure the confidentiality of the information. XBee provides such a feature as mentioned earlier. This would be a convenient method to use since it do not take much to implement. It avoids the attacker to modify the internally stored data remotely without knowing the correct encryption key. XCTU software can be used to store the encryption key. Any user can use the XCTU software to store an encryption key in the XBee chip to allow encrypted communication. Of course, the key should be the same on both sides, else the packets will be easily discarded. As both sides use the same key, the encryption and decryption are completed using AES-128. The encryption occurs symmetrically. The performance may be affected since the chip requires time to encrypt and decrypt the payload. Link layer encryption seems to be the most practical approach to the problem, but cannot be applied to the above case [38].

D. ADDITIONAL APPROACH

If the on-board encryption as mentioned earlier is not used, a man-in-the-middle attack [1] is still possible, the attacker would not be able to read the content. Since a change of address is still possible, the DoS attack might be performed when the XBee encryption is disabled. Since there is no way around it, and the encryption needs to be setup, which is not possible in DoS attacks, an alternative needs to be found out that provides the same bandwidth and functionality as the XBee but does not allow changes of the internal parameters. An option that might work is using duplicate channels by using two Xbee communication channels with enabled encryption on both of them. It only gives an additional logic to split up the communication and reassemble [38].

Since encryption ensures confidentiality and not integrity, the attacker could still read packets and replay them to understand the consistent pattern. By any chance, if we know that the attacker recorded the whole data stream and re-transmits all split packets, then the application would not know the data pattern that are valid and would act accordingly. To get rid of such behavior, cryptographic nonces can be used. If the packet is received twice, it should be discarded by the application. The XBee chip cannot provide this functionality, as the chip cannot make a decision whether the payload is allowed to be sent again or not, so this is managed by the application protocol [8], [38].

IV. APPROACH

An EEG signal is unique to a person at a particular time. It is possible to generate a key unique to a particular user. Since EEG behavior is activity-dependent, a user's EEG signal is unique to that user at that particular time [36]. This unique signal changes every few hours meaning that it cannot be permanently "stolen". This unique key can be used for encrypting the data using AES, which is used in XBee communication. We have developed a method for utilizing brain EEG signal characteristics to generate the cryptographic key for AES data encryption and decryption.

In this section, we describe our method for securing a UAV communication using this EEG signal. We configure the AES encryption key of the XBee device present on the UAV and at the ground control station with the key generated from the above procedure (see Fig. 1). We also provide an approach to a safety backtrack path procedure in case the communication is attacked [36].

A. EEG SIGNAL PROPERTIES

We record a user's EEG signal using the Mindwave EEG sensor for our evaluation [40]. The device consists of earclip, headsets and a resting arm. This device outputs different components of the EEG signal such as alpha, beta, gamma, theta and delta waves every second (1 Hz). The device is easy and comfortable to wear and also checks the person's attention and meditation levels. It is powered by a battery. We opted to use Beta waves from the EEG signal as the basis for our analysis. Beta waves (12-30 Hz) as shown in Figure 2, are often classified into $\beta 1$ (low Beta) and $\beta 2$ (high Beta) to gain a more specific range. The waves are generated in the central and frontal areas of the brain. It determines the concentration of the person doing a task. There is an increase of β activity when a person focuses on mental tasks such as resisting something or solving an analytical task [17] [36].

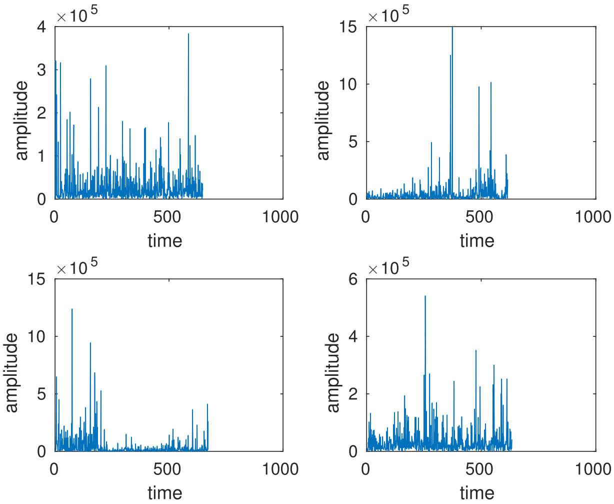


FIGURE 2. Beta component of EEG waveform of 4 different people. The patterns in the β waves are unique to each individual, making them ideal for biometric encryption. The amplitude is the EEG power units. Normally, the power spectrum band powers have units Volts-squared per Hz, but since the values have undergone a number of complicated transforms (Internally from the NeuroSky device) and rescale operations from the original voltage measurements, there is no longer a simple linear correlation to units of Volts and the values are simply referred as EEG power units.

Among the waveforms present in the EEG signal, Beta waves are used since these waves are related to performing a mental task like drawing, solving analytical problems etc. For simplicity we asked the subjects (users) to draw a random picture on a piece of paper while the EEG sensor is connected to the users and thus recording their Beta EEG data. It is also a way to ensure that while the data were collected, the users were consciously aware that the data are being collected for key generation.

B. FEATURE EXTRACTION

We record an EEG signal (Beta waves) from a specific user for time period T. Since the Beta waves are of less amplitude, they are amplified by a certain value A. Later on, the data is mapped through higher order Legendre Polynomials derived from a Legendre Differential equation which is given by:

$$\frac{\partial}{\partial x}[(1-x^2)\frac{\partial}{\partial x}p_n(x)] + n(n+1)p_n(x) = 0 \tag{1}$$

Higher order Legendre's polynomials has the property of carrying unique signatures. In more precise terms, the coefficients derived from various degrees of polynomials matchings are unique for different individuals. It has been proven a significant feature for QRS signals for ECG [18].

Legendre polynomials are computed using Rodrigues's formula, which is given by:

$$p_n(x) = \frac{1}{2^n n!}\frac{\partial^n}{\partial x^n}[(x^2-1)^n]. \tag{2}$$

For data fitting we use an n-degree equation:

$$y(x) = a_0 + \sum_{1}^{n} a_i p_{i(x)}. \tag{3}$$

The polynomial coefficients $a_0, a_1, \ldots a_n$ are merged together along with a time window of size T. We then use the amplitude multiplier A to generate a raw feature vector $z := \{ca_0, ca_1, ca_2, \ldots ca_n, A, T\}$ where c is a constant to boost the difference between coefficients. We map z to w such that $w = z \times M + \gamma$. Here, M is an $n \times n$ invertible matrix which meets the criterion: $\sum_i m_{i,j} = 1$; where γ is a random vector whose elements lie in the range $\left[2^{-\theta}, 2^{\theta}\right]$. To conclude, the polynomial coefficients are merged together along time window of size T and uses amplitude amplifier A to generate a raw feature vector.

C. RANDOMNESS EXTRACTION

Given the potential of the attackers to reconstruct the original EEG signal from the feature vector, we attempt to map the feature vector with some random vector using linear transformation. So, after getting the feature vector w, we utilize a reusable fuzzy extractor generated from (n, k)-BCH (Bose-Chaudhuri-Hocquenghem) codes. These codes form a class of cyclic error-correcting codes. It evidently corrects the error occurred, along with the generator function to get sufficient randomness from it [16].

The randomness derived from each feature r_i is computed as $r_i = H_x(w_i)$. Here, H_x is a hash function which belongs to a universal hash family. The universal hash family H is a class of hash functions. Mathematically, H is defined to be universal if the probability of mapping of distinct keys to the same index is less than $1/l$ (l is the length of the randomness string). Hashing is implemented after making a random choice of hash function extracted from the universal class H.

The universal hash function ensures the optimality in the length of the extracted randomness [16].

For future authentication of feature values, we compute the syndrome S_c. If the feature element is interpreted as $w_i(x) = w_{i_0} + w_{i_1}x + \ldots + w_{i_{n-1}}x^{n-1}$, then every element w_i should have a matching syndrome S_{c_i} for (n, k)-BCH codes:

$$S_{c_i} = w_i(x) \bmod g(x) = \left\{ w_i(\alpha^1), w_i(\alpha^2), \ldots, w_i(\alpha^{2t}) \right\}. \quad (4)$$

This randomness represents the feature vector in a different form, so that attacker cannot reconstruct the original signal.

Advantages of using BCH codes:

- It can be easily decoded with the syndrome decoding method;
- It requires simple hardware to function, so it obviates the use of complex systems to perform the decoding procedure making it easy to implement on a low powered device;
- It is highly flexible, allowing control of block length and acceptable error thresholds. This allows for custom code to be designed for a given specification;
- BCH are useful in theoretical computer science;
- Easy to implement in hardware;
- Widely used encoding and decoding technique.

D. KEY GENERATION

The key generated based on the above features is used to secure the UAV communication channel. This key is used to configure both the ground control station Xbee and the XBee on-the UAV, thereby ensuring security of the communication channel. The key K is generated based on chosen extracted randomness from the previous step [16]. The key generation technique is:

Randomly select q constants $1 \leq j_1 \leq \ldots \leq j_q \leq n$ to map several features to produce a feature vector $v := \{w_{j_1}, \ldots, w_{j_q}\}$. Most of the times the feature vectors are permuted.

The key K is produced based on extracted randomness r_{j_i} : $K := r_{j_1}|| \ldots ||r_{j_q}$, where || denotes concatenation.

E. CONFIGURING XBEE WITH THE KEY GENERATED

We secured the XBee's communication using the generated AES encryption key. For this experiment, we used the Mindwave sensor and an Intel i7 laptop to create the EEG-based encryption. We assembled a UAV with a Pixhawk controller connected to an XBee used to communicate with the ground station's XBee. The Pixhawk is connected to the XBee using a serial port. After configuring the XBee with the generated AES encryption key, we tested the communication of UAV with the XBee present at the ground control station. The AES key configuration ensured secured communication with the UAV.

We validated the system using a scenario where an attacker was trying to intercept the communication between the UAV and ground control station in order to override operator control. For simplicity, we assumed that the attacker already knew the key generated and configured his/her own device with that key, intending to maliciously communicate with the UAV.

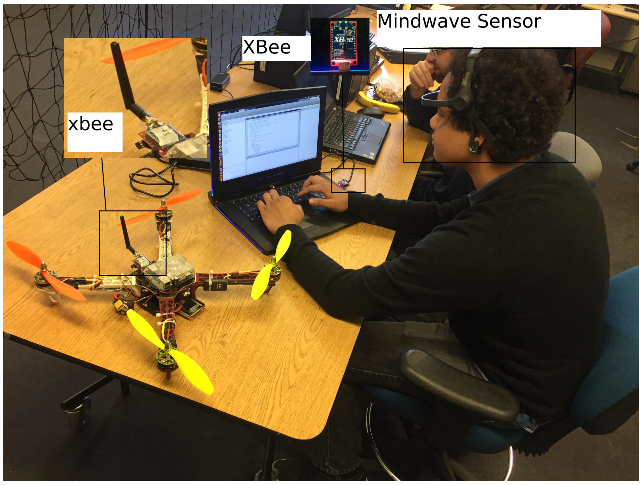


FIGURE 3. Experimental Setup.

As a safety measure, we preconfigured the UAV's Xbee to receive the commands from the ground control station Xbee's address. If the attacker tried to send the control signals from its device then from the attacker's packet address we verified that a third party was intervening, and we activated the Return-To-Launch (RTL) control signal in the UAV. This would mean that the UAV identified that an attack was attempted and should return to its starting location. The RTL mode aids the UAV navigation from its current position to hover above the home position. RTL is a GPS-dependent move, so it is essential that GPS lock is enabled before attempting to use this mode (Algorithm 1).

Algorithm 1 RTL Mode Activation in UAV

```
getAddress ← xbeedata.getAddress()
if getAddress ≠ groundcontrolstation.getAdress() then
    LockGPS()
    ReturnToLaunch()
else
    Continue;
end if
```

The LockGPS() function ensures that the sensor is not affected in any other way since it becomes completely independent of the rest of the communication process.

Another proposed methodology would send a predefined signal to the ground control station to configure the XBees (both the ground control station and the UAV) with a new key if an attack is attempted. We then run key generation from the EEG signal on the ground control station and generate an new key to ensure the communication is secure (Algorithm 2).

An alternative method to ensure secure communication is to regularly change the key generated and configure the

Algorithm 2 Key Change Request in UAV

```
getAddress ← xbeedata.getAddress()
if getAddress ≠ groundcontrolstation.getAdress() then
    LockGPS()
    SendKeyChangeToGroundControlStation()
    WaitForKey()
else
    Continue();
end if
```

Xbees at regular time intervals, achieving quite robust and secure communication with the UAVs.

V. RESULTS

In the initial setup we collected the EEG data to be used for the developed key generation pipeline. The data was collected from a user performing a specific task that activates the Beta component of the EEG signal. The collected data (around 1000 data points), were fed to the key generation pipeline described in the prior section. We extracted the Beta components of different people, monitored doing similar tasks (e.g., drawing). A normal EEG waveform of a single person is shown in Figure 4.

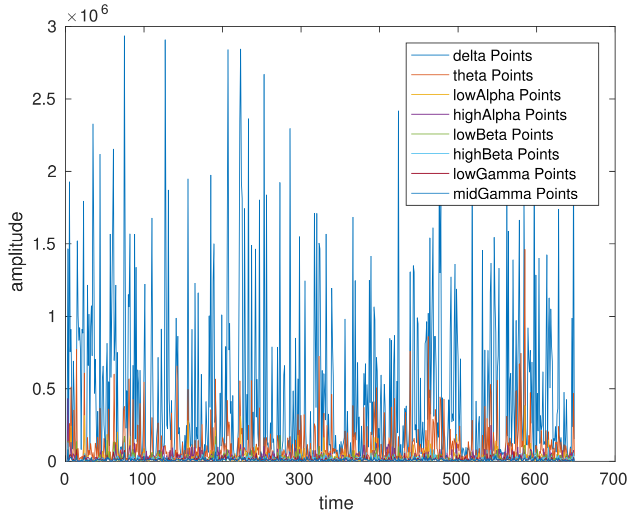
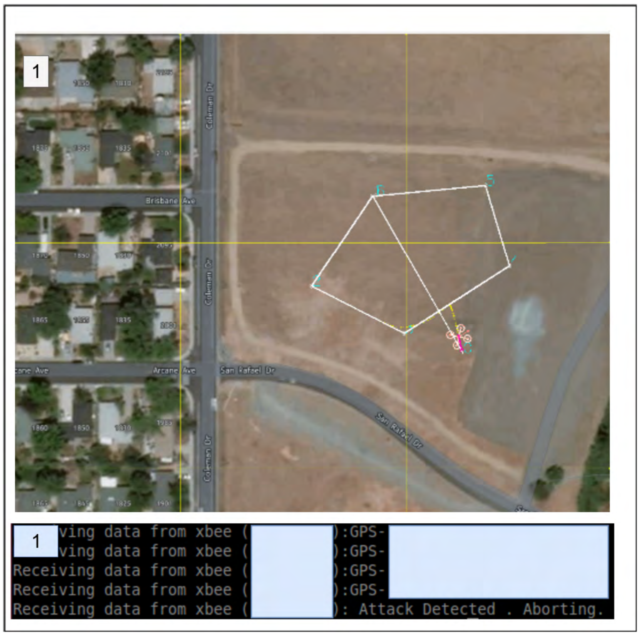


FIGURE 4. Sample EEG waveform (with all the components) of a user performing a specific mental task.

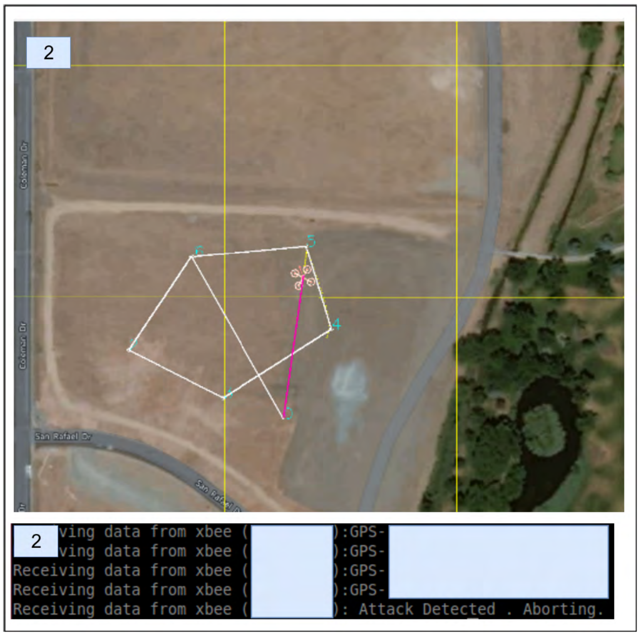
Xbee has two modes of interaction: AT and API mode. AT mode is also referred as "Transparent" mode. In transparent mode, all the data received by the chip through a serial interface is interpreted as payload and wrapped in a packet. Another mode that exists in XBee is the Application Programming Interface (API) mode. In this mode, the receiver expects payload plus API-frame which includes payload. In the API-frame, the destination address can also be specified along with other parameters. This provides a benefit of not changing the DH and DL addresses

We configure the XBees in AT mode to ensure that XBee's AES encryption mode is enabled and uses the EEG-based key.



```
ving data from xbee ([redacted]):GPS-[redacted]
ving data from xbee ():GPS-
Receiving data from xbee ():GPS-
Receiving data from xbee ():GPS-
Receiving data from xbee (): Attack Detected . Aborting.
```

FIGURE 5. Waypoints set for the experiment in the first configuration. The attack was discovered after the UAV navigated from waypoint 3 and Return-to-Launch (RTL) was enabled. The drone was able to travel back the originally deployed position.



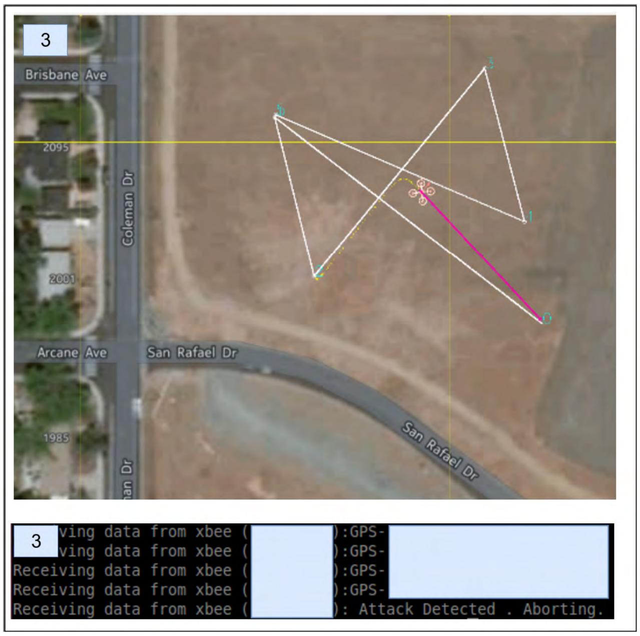
```
ving data from xbee ([redacted]):GPS-[redacted]
ving data from xbee ():GPS-
Receiving data from xbee ():GPS-
Receiving data from xbee ():GPS-
Receiving data from xbee (): Attack Detected . Aborting.
```

FIGURE 6. Waypoints set for the experiment in the second configuration. The attack was discovered after the UAV navigated from waypoint 5 and Return-to-Launch (RTL) was enabled. The drone was able to travel back the originally deployed position.

Since the EEG data changes for the same user over time, the generated key from our pipeline would be different, thus ensuring uniqueness of the key generated. This enables users to configure the XBee's AES key to different values (see Figure 3).

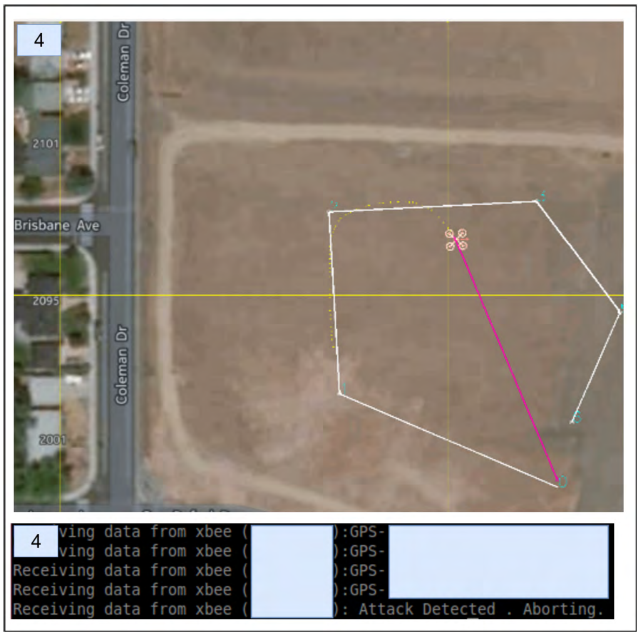
We performed our proposed fail-safe mechanism using a commercially-available quadcopter with an on-board autopilot using Xbees to communicate with the secured ground control station. We setup an ordered set of waypoints for the UAV using mission planner software. For our experiment we setup different waypoints at different configurations and tested our methods at different times (Figures 5-8).

In all of the experimental results, we can see that the drone was able to detect attacks at different locations (waypoints) and activated the RTL function to navigate back to originally deployed "home" location. For instance, Fig. 9 shows



```
3  ving data from xbee ([redacted]):GPS-[redacted]
   ving data from xbee (         ):GPS-
Receiving data from xbee (       ):GPS-
Receiving data from xbee (       ):GPS-
Receiving data from xbee (       ): Attack Detected . Aborting.
```

FIGURE 7. Waypoints set for the experiment in third configuration. The attack was discovered after the UAV navigated from waypoint 2 and Return-to-Launch (RTL) was enabled. The drone was able to travel back the originally deployed position.



```
4  ving data from xbee ([redacted]):GPS-[redacted]
   ving data from xbee (         ):GPS-
Receiving data from xbee (       ):GPS-
Receiving data from xbee (       ):GPS-
Receiving data from xbee (       ): Attack Detected . Aborting.
```

FIGURE 8. Waypoints set for the experiment in fourth configuration. The attack was discovered after the UAV navigated from waypoint 2 and Return-to-Launch (RTL) was enabled. The drone was able to travel back the originally deployed position.

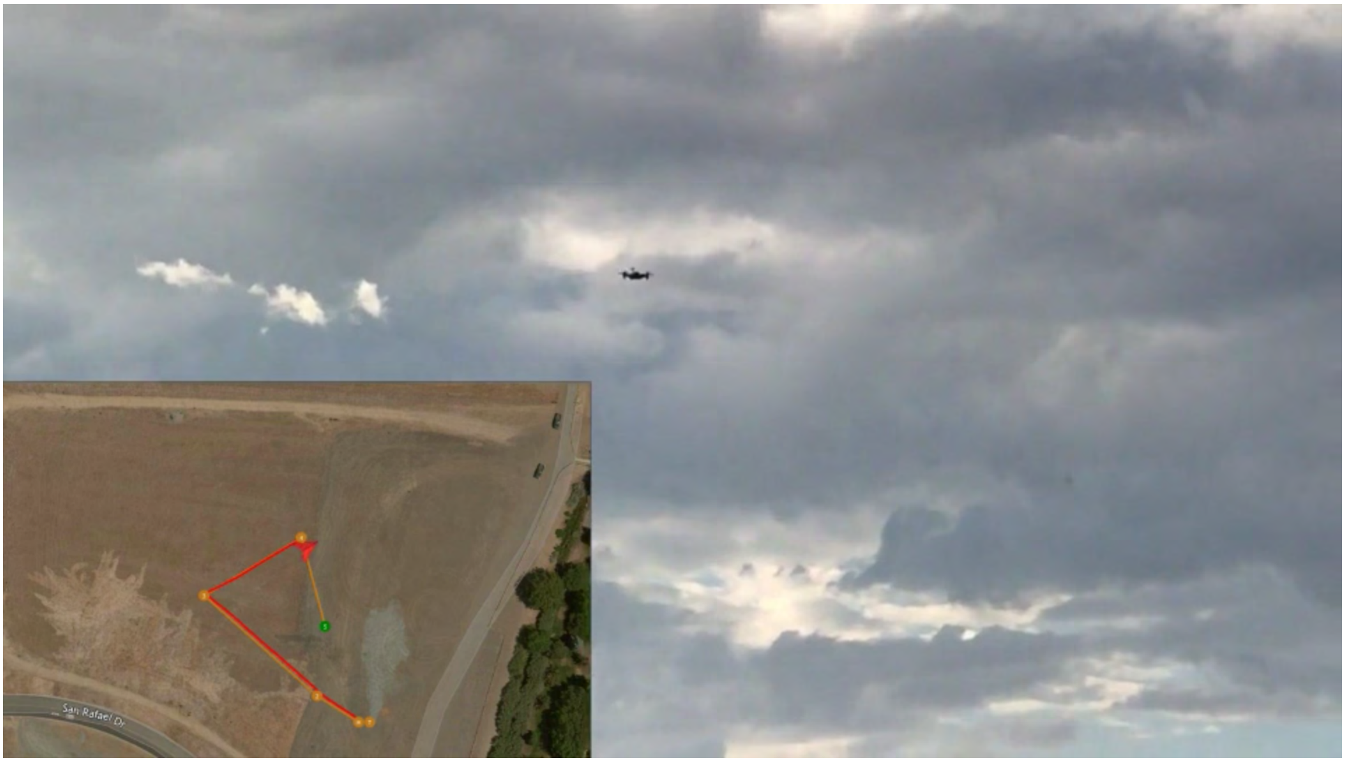


FIGURE 9. Waypoints set for the experiment on the physical drone in real time. The attack was discovered after the UAV navigated after waypoint 4 and Return-to-Launch (RTL) was enabled. The drone was able to travel back the originally deployed position. Video link: https://www.youtube.com/watch?v=TXwQiGoNsjw&feature=youtu.be

the results in real-time deployment on the field (Rancho San Rafael Regional Park, near University of Nevada, Reno campus). The attack was detected after waypoint 4 and Return-to-Launch (RTL) was enabled to allow the drone to travel back "home".

The *a priori* goal was to travel these way-points and return to a base location if an attack was detected. We introduced a third party attacking mechanism, maliciously sending control signals to the UAV. Our algorithm successfully detected the intervention (since the received packets at the UAV's XBee had a different source address). After detection of the intervention, the UAV initiated its RTL mechanism and returned to the base GPS location without completing the directed trajectory.

We tested our other approach of changing the key when an attack is detected. During this test we set up the same waypoints and introduced a similar type of attack along the way. After successful detection of the intervention, the algorithm sent a key change request to the ground control station, during which, the UAV's communication was restricted to the ground control station and it hovered at a specified location where the attack was attempted. After the Xbee was configured to a new AES key, navigation resumed to the destined location.

For more information of the implementation demonstration, the reader can watch this video link:

https://www.youtube.com/watch?v=TXwQiGoNsjw&feature=youtu.be

VI. CONCLUSION

We have provided an approach for biometric encryption of a UAV communicating with the ground control station. We have also provided a safety mechanism for the UAV in case a third-party attack is detected along the way. We have demonstrated this fail-safe mechanism on a commercially-available UAV. This approach can be used for any UAV scenario where cyberattacks are a particular concern. Our approach not only adds a layer of additional security to the UAV but also provides a unique way for securing the UAV with low-cost resources.

VII. DISCUSSION

Our proposed algorithm can be further extended for authentication scheme of multi-UAV scenarios [20], [21], [23], [30], where a cluster of UAVs aim to authenticate their controller [44]. A possible approach is to have each member of a UAV cluster sequentially verify the controller one by one utilizing the proposed authentication scheme. Formation control and cooperative learning in multi-robot systems can be utilized to enhance the safety security mechanism [5], [13], [22], [24] through cooperative sensing [28], [29].

The EEG key generation technique can be enhanced from extracting polynomial coefficients to perform a statistical analysis of the EEG data. One potential approach could use the averaged event-related potential (ERP) [39], which has the potential to provide more accurate biometric identification. It describes the Cognitive Event-Related Biometric Recognition (CEREBRE) protocol [39], an ERP bio metric protocol designed to express individual's unique responses coming from multiple functional brain systems (e.g., the primary visual, facial recognition, and gustatory/appetitive systems). The results based on their approach indicate 100 percent identification accuracy in a pool of 50 users.

The idea for statistical analysis for EEG is to extract consistent parameters in an EEG signal of a particular user. This consistency ensures a single key or a single type of key with a known variance. Identifying other consistent parameters of brain EEG signals that highlight the task in which a particular user is performing like sleeping, doing a different mental tasks, etc., would not only help identifying a state of mind (which is important for generating a key from sleeping person would defeat our purpose), but also identify the intensity of state of mind of different individuals performing a different task. This requires different volunteers performing different tasks. This requires active data collection for a longer period.

Another idea is to use only the three dimensional (3D) data acquired over time as the UAV travels in a specified path. Assume a scenario, where the ground control station specifies a path for a UAV to travel from Point A to Point B. Since the UAV is equipped with 3D sensors (i.e., Velodyne LiDAR) we attempt to store the 3D data in memory and perform the alignment of 3D point clouds to reconstruct the scene [26], [27] as the UAV acquires through time along the way. Assume that at a certain point, X, an attack was detected. Our approach is to cut/disable all the communication of the UAV to the ground control station and use only the previously reconstructed scene to navigate and find its way back to "home". It essentially simplifies as follows: understand the environment, detect the key features, find a path to return to the "home" position based on the reconstructed 3D scene until the attack was detected.

REFERENCES

[1] (Oct. 2017). *Man-in-the-Middle Attack*. Accessed: Feb. 18, 2018. [Online]. Available: https://www.ssh.com/attack/man-in-the-middle

[2] Amazon. (2016). *Amazon Prime Air*. Accessed: Jul. 30, 2017. [Online]. Available: https://www.amazon.com/b?node=8037720011

[3] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," in *Proc. Int. Joint Conf. Biometrics (IJCB)*, Oct. 2011, pp. 1–7.

[4] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: The insecurity of 802.11," in *Proc. 7th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, New York, NY, USA, 2001, pp. 180–189.

[5] A. D. Dang, H. M. La, and J. Horn, "Distributed formation control for autonomous robots following desired shapes in noisy environment," in *Proc. IEEE Int. Conf. Multisensor Fusion Integr. Intell. Syst. (MFI)*, Sep. 2016, pp. 285–290.

[6] S. M. Diamond and M. G. Ceruti, "Application of wireless sensor network to military information integration," in *Proc. 5th IEEE Int. Conf. Ind. Inform.*, vol. 1. Jun. 2007, pp. 317–322.

[7] Digi. (2017). *Addressing Modes: XBee/XBee-PRO S2C 802.15.4 RF Module User Guide*. Accessed: Feb. 10, 2018. [Online]. Available: https://www.digi.com/resources/documentation/Digidocs/90001500/Default.htm#Reference/r_addressing%20modes.htm%3FTocPath%3DOperation%7CAddressing%7C_____2

[8] Digi. (2017). *How XBee Devices Communicate: XBee/XBee-PRO S2C 802.15.4 RF Module User Guide*. Accessed: Feb. 10, 2018. [Online]. Available: https://www.digi.com/resources/documentation/Digidocs/90001456-13/Default.htm#concepts/c_how_xbees_communicate.htm%3FTocPath%3DHow%2520XBee%2520devices%2520work%7C_____1

[9] Digi. (2017). *Serial Modes: XBee/XBee-PRO S2C 802.15.4 RF Module User Guide*. Accessed: Feb. 10, 2018. [Online]. Available: https://www.digi.com/resources/documentation/Digidocs/90001500/Default.htm#Containers/cont_serial_modes.htm%3FTocPath%3DModes%7CSerial%2520modes%7C_____0

[10] Digi. (2017). *XBee/XBee-PRO S2C 802.15.4 RF Module User Guide*. Accessed: Feb. 10, 2018. [Online]. Available: https://www.digi.com/resources/documentation/Digidocs/90001500/Default.htm#Concepts/c_90001500_start.htm%3FTocPath%3DXBee%252FXBee-PRO%2520S2C%2520802.15.4%2520RF%2520Module%2520User%2520Guide%7C_____0

[11] L. Franceschi-Bicchierai, "Drone hijacking? That's just the start of GPS troubles," Univ. Texas, Austin, TX, USA, Tech. Rep., Jul. 2012, accessed: Feb. 10, 2018. [Online]. Available: https://www.wired.com/2012/07/drone-hijacking/

[12] S. Gorman, J. Y. Dreazen, and A. Cole, "Insurgents hack U.S. drones," *Wall Street J.*, Dec. 2009. [Online]. Available: https://www.wsj.com/articles/SB126102247889095011

[13] T.-T. Han, H. M. La, and B. H. Dinh, "Flocking of mobile robots by bounded feedback," in *Proc. IEEE Int. Conf. Autom. Sci. Eng. (CASE)*, Aug. 2016, pp. 689–694.

[14] K. Hartmann and C. Steup, "The vulnerability of UAVs to cyber attacks—An approach to the risk assessment," in *Proc. 5th Int. Conf. Cyber Conflict (CyCon)*, Jun. 2013, pp. 1–23.

[15] B. M. Horowitz, "Cybersecurity for unmanned aerial vehicle missions," *Cyberedge*, Apr. 2016, accessed: Feb. 10, 2018. [Online]. Available: https://www.afcea.org/content/Article-cybersecurity-unmanned-aerial-vehicle-missions

[16] P. Huang, B. Li, L. Guo, Z. Jin, and Y. Chen, "A robust and reusable ecg-based authentication and data encryption scheme for ehealth systems," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–6.

[17] T. L. Huang and C. Charyton, "A comprehensive review of the psychological effects of brainwave entrainment," *Alternative Therapies Health Med.*, vol. 14, no. 5, pp. 38–50, 2008.

[18] I. Khalil and F. Sufi, "Legendre polynomials based biometric authentication using QRS complex of ECG," in *Proc. Int. Conf. Intell. Sensors, Sensor Netw. Inf. Process.*, Dec. 2008, pp. 297–302.

[19] H.-B. Kuntze *et al.*, "SENEKA-sensor network with mobile robots for disaster management," in *Proc. IEEE Conf. Technol. Homeland Secur. (HST)*, Nov. 2012, pp. 406–410.

[20] H. M. La, R. Lim, and W. Sheng, "Multirobot cooperative learning for predator avoidance," *IEEE Trans. Control Syst. Technol.*, vol. 23, no. 1, pp. 52–63, Jan. 2015.

[21] H. M. La and W. Sheng, "Dynamic target tracking and observing in a mobile sensor network," *Robot. Auto. Syst.*, vol. 60, no. 7, pp. 996–1009, 2012.

[22] H. M. La and W. Sheng, "Distributed sensor fusion for scalar field mapping using mobile sensor networks," *IEEE Trans. Cybern.*, vol. 43, no. 2, pp. 766–778, Apr. 2013.

[23] H. La and W. Sheng, "Multi-agent motion control in cluttered and noisy environments," *J. Commun.*, vol. 8, no. 1, pp. 32–46, 2013.

[24] H. M. La, W. Sheng, and J. Chen, "Cooperative and active sensing in mobile sensor networks for scalar field mapping," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 45, no. 1, pp. 1–12, Jan. 2015.

[25] M. McFarland, "Google drones will deliver Chipotle burritos at Virginia Tech," Virginia Tech, Blacksburg, VA, USA, Tech. Rep., Sep. 2016, accessed: Jul. 30, 2017. [Online]. Available: http://money.cnn.com/2016/09/08/technology/google-drone-chipotle-burrito/index.html

[26] L. V. Nguyen and H. M. La, "Development of a smart shoe for building a real-time 3D map," in *Proc. 32nd Int. Symp. Autom. Robot. Construction Mining (ISARC)*, Jan. 2015, pp. 1–8.

[27] L. V. Nguyen, H. M. La, J. Sanchez, and T. Vu, "A smart shoe for building a real-time 3D map," *Autom. Construction*, vol. 71, pp. 2–12, Nov. 2016.

[28] M. T. Nguyen, H. M. La, and K. A. Teague, "Compressive and collaborative mobile sensing for scalar field mapping in robotic networks," in *Proc. 53rd Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Sep. 2015, pp. 873–880.

[29] M. T. Nguyen, H. M. La, and K. A. Teague, "Collaborative and compressed mobile sensing for data collection in distributed robotic networks," *IEEE Trans. Control Netw. Syst.*, to be published. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8046067&isnumber=6730648, doi: 10.1109/TCNS.2017.2754364.

[30] T. Nguyen, T.-T. Han, and H. M. La, "Distributed flocking control of mobile robots by bounded feedback," in *Proc. 54th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Sep. 2016, pp. 563–568.

[31] T. C. Nguyen, "Virus attacks military drones, exposes vulnerabilities," Tech. Rep., Oct. 2011, accessed: Jun. 7, 2013. [Online]. Available: https://www.zdnet.com/article/virus-attacks-military-drones-exposes-vulnerabilities/

[32] T. C. Nguyen. (2012). *How College Students Hijacked a Government SPY Drone*. Accessed: Jun. 7, 2013. [Online]. Available: https://www.zdnet.com/article/how-college-students-hijacked-a-government-spy-drone/

[33] P. Paganini. (2013). *Hacking Drones … Overview of the Main Threats*. Accessed: Jun. 7, 2013. [Online]. Available: http://resources.infosecinstitute.com/hacking-drones-overview-of-the-main-threats/

[34] H. X. Pham, H. M. La, D. Feil-Seifer, and M. Deans, "A distributed control framework for a team of unmanned aerial vehicles for dynamic wildfire tracking," in *Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst. (IROS)*, Sep. 2017, pp. 6648–6653.

[35] H. X. Pham, H. M. La, D. Feil-Seifer, and L. V. Nguyen. (Jan. 2018). "Autonomous UAV navigation using reinforcement learning." [Online]. Available: https://arxiv.org/abs/1801.05086

[36] T. Pham, W. Ma, D. Tran, P. Nguyen, and D. Phung, "Eeg-based user authentication in multilevel security systems," in *Proc. Int. Conf. Adv. Data Mining Appl.*, 2013, pp. 512–523.

[37] T. Pham, W. Ma, D. Tran, P. Nguyen, and D. Phung, "Multi-factor EEG-based user authentication," in *Proc. Neural Netw. (IJCNN)*, Jul. 2014, pp. 4029–4034.

[38] N. M. Rodday, R. D. O. Schmidt, and A. Pras, "Exploring security vulnerabilities of unmanned aerial vehicles," in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp. (NOMS)*, Apr. 2016, pp. 993–994.

[39] M. V. Ruiz-Blondet, Z. Jin, and S. Laszlo, "CEREBRE: A novel method for very high accuracy event-related potential biometric identification," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 7, pp. 1618–1629, Jul. 2016.

[40] W. Sałabun, "Processing and spectral analysis of the raw eeg signal from the mindwave," *Przeglad Elektrotechn.*, vol. 90, no. 2, pp. 169–174, 2014.

[41] A. Sanjab, W. Saad, and T. Başar, "Prospect theory for enhanced cyber-physical security of drone delivery systems: A network interdiction game," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, May 2017, pp. 1–6.

[42] A. C. Woods and H. M. La, "Dynamic target tracking obstacle avoidance using a drone," in *Advances in Visual Computing*. Cham, Switzerland: Springer, 2015, pp. 857–866.

[43] A. C. Woods and H. M. La, "A novel potential field controller for use on aerial robots," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7932539&isnumber=6376248, doi: 10.1109/TSMC.2017.2702701.

[44] A. C. Woods, H. M. Lay, and Q. P. Ha, "A novel extended potential field controller for use on aerial robots," in *Proc. IEEE Int. Conf. Autom. Sci. Eng. (CASE)*, Aug. 2016, pp. 286–291.

[45] J. Wright. (2016). *Killerbee: Practical ZigBee Exploitation Framework or Wireless Hacking and the Kinetic World*. Accessed: 2018-02-10. [Online]. Available: http://www.willhackforsushi.com/presentations/toorcon11-wright.pdf

ASHUTOSH SINGANDHUPE received the B.E. degree in electronics and communication engineering from Karunya University, Coimbatore, India, in 2011, and the M.S. degree in computer science and engineering from the University of Nevada, Reno, NV, USA, in 2017. He was a Graduate Research Assistant of the Advanced Robotics and Automations Laboratory, Department of Computer Science and Engineering, University of Nevada, Reno, NV, USA. He is currently with ScadaTEC Inc., as a Software Research Engineer. His research interest includes unmanned aerial vehicles, autonomous navigation, computer vision, and artificial intelligence.

HUNG MANH LA (M'09–SM'14) received the B.S. and M.S. degrees in electrical engineering from the Thai Nguyen University of Technology, Thai Nguyen, Vietnam, in 2001 and 2003, respectively, and the Ph.D. degree in electrical and computer engineering from Oklahoma State University, Stillwater, OK, USA, in 2011. From 2011 to 2014, he was a Post-Doctoral Research Fellow and then a Research Faculty Member with the Center for Advanced Infrastructure and Transportation, Rutgers University, Piscataway, NJ, USA. He is currently the Director of the Advanced Robotics and Automation Laboratory, and also an Assistant Professor with the Department of Computer Science and Engineering, University of Nevada, Reno, NV, USA.

He has been actively involved in research projects with the National Science Foundation, Department of Transportation and National Aeronautics and Space Administration. He has authored over 80 papers published in major journals, book chapters, and international conference proceedings. His current research interests include robotic systems and mobile sensor networks. He was a recipient of the 2014 ASCE Charles Pankow Award for the Robotics Assisted Bridge Inspection Tool, three best paper awards, and a best presentation award in international conferences. He was a Guest Editor of the *International Journal of Robust and Nonlinear Control* from 2016 to 2017. He is currently an Associate Editor of the IEEE TRANSACTIONS ON HUMAN-MACHINE SYSTEMS.

DAVID FEIL-SEIFER (M'06) received the B.S. degree in computer science from the University of Rochester, Rochester, NY, USA, in 2003, and the M.S. and Ph.D. degrees in computer science from the University of Southern California, Los Angeles, CA, USA, in 2007 and 2012, respectively. From 2011 to 2013, he was a Post-Doctoral Associate with the Computer Science Department, Yale University, New Haven, CT, USA. He has been an Assistant Professor and the Director of the Socially Assistive Robotics Group with the Department of Computer Science and Engineering, University of Nevada, Reno, NV, USA, since 2013.

He has been involved in research projects with the Nevada Department of Wildlife, U.S. Office of Naval Research, National Science Foundation, and the National Institutes of Health. He has authored over 50 papers published in major journals, book chapters, and international conference proceedings. His current research interests include human-robot interaction, socially assistive robotics, and intelligent user interfaces for multi-robot control. He is a member of the HRI Steering Committee. He was a recipient of the USC Mellon Award for Excellence in Mentoring, the USC Order of Arete', a best poster award, and the USC College of Engineering Best Dissertation Award. He is a Co-Chair of the IEEE Robotics and Automation Society Technical Committee on Human-Robot Interaction and Communication. He is a Managing Editor of the ACM *Transactions on Human-Robot Interaction*.