2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)
Banff Center, Banff, Canada, October 5-8, 2017

Securing a UAV Using Individual Characteristics From an EEG Signal

Ashutosh Singandhupe, Hung Manh La, David Feil-Seifer, Pei Huang, Linke Guo, and Ming Li

***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 work, 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 the Beta component of a user's EEG. 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. The increasing affordability of UAVs have broadened their use by hobbyists and enthusiasts, companies, and government agencies. This have subsequently led to the occurrence of several 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" [17], has successfully tested its drones for food delivery, and Amazon's "Prime Air" service [1], that 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, potential cyberattacks on those UAVs. These potential 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 which secures the UAV communication to the ground control station using an encryption key generated using features of a person's Electroencephalogram (EEG) signal. UAVs communicate using small mobile modules called XBee. XBee's secures communication using the Advanced Encryption Standard (AES). We have developed a system to generate an AES encryption key, which is derived from an operator's EEG signal. We have also demonstrated a safety mechanism activated in the case of a third-party attack which secures the UAV. This entire system was validated on a commercially available UAV.

We performed the testing on a UAV, where we encrypt 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 robots have been remotely compromised, taking control of the UAV or making it crash-land. It is well shown that the first known attack was started by the Iraqi militants in 2009, when they gained access on a Predator Drone (UAV) [6]. 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 [19].

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 [8]. 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 [5], [8]. An example of this type of attack was demonstrated using relatively inexpensive equipment, spoofing the GPS and taking complete control of the UAV [9], [20], [21].

UAV infrastructure is moving towards more network-centric command and control, where components are interconnected through mesh networks [3]. Some military UAV systems, more specifically the Global Hawk, already

Ashutosh Singandhupe and Dr. Hung La are with the Advanced Robotics and Automation (ARA) Lab, Department of Computer Science and Engineering, University of Nevada, Reno, NV, 89557, USA

Dr. David Feil-Seifer and Dr. Ming Li are with the Department of Computer Science and Engineering, University of Nevada, Reno, NV, 89557, USA

Pei Huang and Dr. Linke Guo are with Department of Electrical and Computer Engineering Binghamton University, State University of New York, Binghamton, NY, 13902, USA.

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

978-1-5386-1644-4/17/$31.00 ©2017 IEEE

has infrastructure of this type. Public safety and disaster management UAVs are also moving to a similar network architecture for planning and communication [11]. 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 and 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 been examined which evaluates 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 [9].

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 it's 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 LP's would give the expected delivery time under different conditions [23].

To the best of our knowledge, biometric UAV authentication has 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 [2]. In this way, a more secure biometric feature is needed. We propose to use EEG signal characteristics to secure communication between an operator and a UAV.

III. Wireless Communication With a UAV

Communication between a ground station and a civilian UAV is typically done through Zigbee or XBee, based on international standard IEEE 802.15.4. For enhanced transmission range, ZigBee has been incorporated with mesh networking capability along with 802.15.4 standard, where single packets are transmitted to the destination node along the network. Transmission rates vary depending on the frequency band used, ranging from 20kbit/s to 250kbit/s [4].

For encrypting the transmitted data, IEEE 82.15.4 protocol uses AES encryption algorithm.The AES encryption algorithm has a key length of 128b (16 bytes). The AES algorithm also checks the transmitted data along with the encryption of the information [16]. Another component called Message Integrity Code (MIC) enables data integrity. A component called Message Authentication Code (MAC) is added to the message. If a message is received from an unknown source, the MAC estimated from the sent message will not equate to the MAC generated using that message with the current key. This concludes that the message source is unknown or cannot be trusted, so it is discarded. The size of the MAC are varied: 32, 64 and 128 bits, but it is generated using the 128 bits AES algorithm. ZigBee also incorporates 2 additional security layers along with the standard IEEE 802.15.4 layer. These are the Network layer and the Application Security layer. Every layer relies on AES 128b encryption algorithm. The generated keys are generally classified into 3 types:

Master key: Every device or node in a network are preprogrammed with this key. The primary purpose is to maintain the confidentiality of the link keys exchange between 2 devices [24].

Link Keys: This is generally handled at the application layer. These are also unique among each pair of devices or nodes. These are used to encrypt the information transfer between devices or nodes, but at the same time consumes memory resources in each device [24].

Network Keys: Just like the other keys these are very unique keys which are shared among all the devices or nodes in a network. Among these devices or nodes in the network, there is one device which is responsible to check which other nodes or devices can join the network. This primary device is called a Trust Center (TC). The TC generates the network key and also regenerates it at different intervals of time to enhance the security. Enabling the TC allows validation of every router or an end device that intends to join the network. It also sends a proper notification to the trust center in case the end device is allowed to join the network through a router. Accordingly the trust center manages the router by either authenticating the newly joined device or discarding and forcing the device to leave the network. So in conclusion, every node or device requires the network key to join the network.

IV. Approach

An EEG signal is unique; to a person and values overtime. It is possible to generate a key unique to a particular user. Since EEG behavior is activity-dependant, a user's EEG signal is unique to that user at a particular time. This unique signal changes every few hours meaning that it cannot be permanently "stolen." This unique key can be used for encrypting AES data like what is used in Zigbee 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 implement a safety backtrack path procedure in case the communication is attacked.

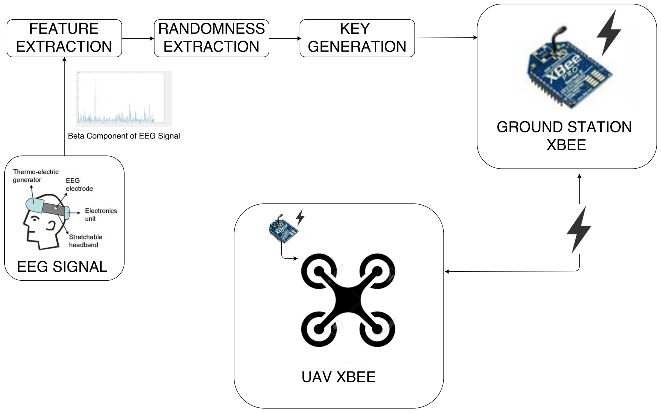


Fig. 1. Basic block diagram of the system overview.

A. EEG Signal Properties

We obtain a user's EEG signal using Mindwave EEG sensor and record it for our evaluation [22]. The device consists of ear-clip, 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. 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), 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.

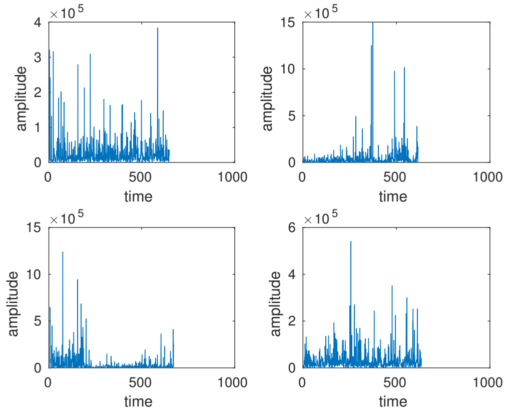


Fig. 2. Beta component of EEG waveform of 4 different people. The patterns in the β waves are unique to each individual, making them ideal for biometric encryption.

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:

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

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 $a_0, a_1, ...a_n$ are merged together along with a time window of size T. We then use the amplitude multiplier A to generate a raw feature vector $z := \{ca_0, ca_1, ca_2, ...ca_n, A, T\}$ 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 $[2^{-\theta}, 2^{\theta}]$. 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 [10].

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 [10].

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

$$S_{c_i} = w_i(x) \text{mod} g(x) = \left\{w_i(\alpha^1), w_i(\alpha^2), ..., w_i(\alpha^{2t})\right\}. \tag{4}$$

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

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-board UAV, thereby ensuring security of the communication channel. The key K is generated based on chosen extracted randomness from the previous step [10]. The key generation technique is:

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

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

E. Configuring XBee with the Key Generated

We secured the XBee's communication with the generated AES encryption key. For this experiment, we used the Mindwave sensor and an Intel i7 laptop to create the EEG-based security. We utilized a commercially available UAV with Pixhawk controller and an AnDroid embedded computer for the XBee communication connection with the ground control station. The UAV and the base station were wirelessly connected using Xbee transmitter and receivers.

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 of the UAV. We introduced a scenario where an attacker was trying to intercept the communication between the UAV and ground control station to override operator control. For simplicity, we have assumed that the attacker already knows the key generated and has configured its own device with that key and to maliciously communicate with the UAV.

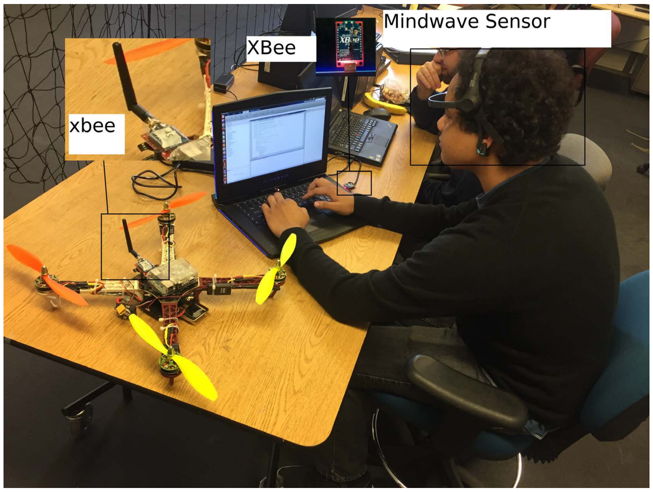


Fig. 3. Experimental Setup.

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 tries to send the control signals from it's device then from the attacker's packet address we verify that a third party is intervening and we activate the Return-To-Launch 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 (Return-To-Launch 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. The algorithm is described below as Algorithm 1.

```
Algorithm 1: RTL mode activation in UAV
  $getAddress \leftarrow xbeedata.getAddress()$
  if $getAddress \neq groundcontrolstation.getAdress()$ then
    $LockGPS()$
    $ReturnToLaunch()$
  else
    $Continue$;
  end if
```

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

We also propose another methodology where, in case an attack is attempted, the Xbee sends predefined signal to the ground control station which signals the station to configure the XBees (both the ground control station and the UAV) with a new key. 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.

We describe the algorithm below:

```
Algorithm 2: Key Change request in UAV
  $getAddress \leftarrow xbeedata.getAddress()$
  if $getAddress \neq groundcontrolstation.getAdress()$ then
    $LockGPS()$
    $SendKeyChangeToGroundControlStation()$
    $WaitForKey()$
  else
    $Continue()$;
  end if
```

An alternative method to ensure a secure communication is to regularly change the key generated and configure the Xbees at regular intervals of time. This way we achieve quite robust and secure way of communication in the UAVs.

V. Results

In the initial setup we collected the EEG data and for the developed key generation pipeline. The data were collected from a user performing a specific task which involves activating 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. A normal EEG waveform of a single person is shown in Figure 4.

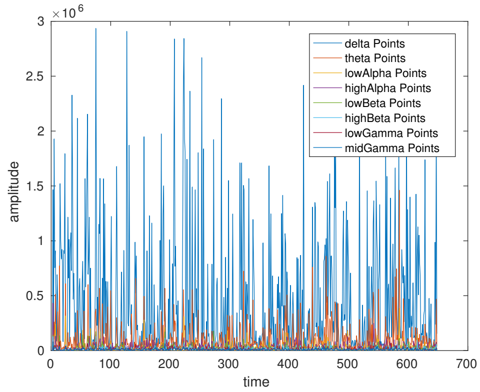


Fig. 4. Sample EEG waveform(with all the components) of a user performing a specific mental task.

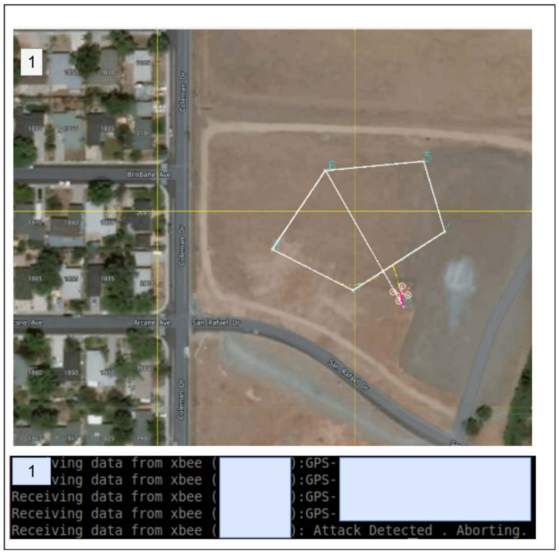
Xbee has two modes of interaction: AT and AP2 mode. AT mode is also referred as "Transparent" mode. In AT mode, the data sent to the XBee module is immediately sent to the remote module, whose destination address is already defined in its memory. This mode is useful when the destination address is same for a particular setting or generally referred as point to point communication. Since Xbee's can be configured only in AT mode we had to stop the ongoing communication operation which was going on in AP2 mode. In AT mode no communication takes place so even a potential attack would fail to communicate. Xbee's inbuild encryption is also disabled in AT mode.

We configure the XBees in AT mode to ensure that XBee's AES encryption mode is enabled and uses the EEG-based key. 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 set up an ordered set of waypoints for the UAV using mission planner software. For our experiment we set up different waypoints at different configurations and tested our methods at different times (Figures 5-8).

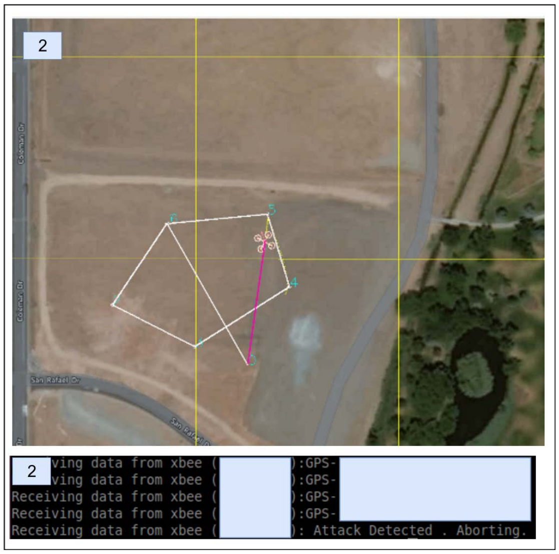
The *a priori* goal was to travel these way-points and return to a base location if an attack was detected. We introduced a third party attacking mechanism. As the third party started attacking and maliciously sending control signals to the UAV, our algorithm successfully detected the intervention (since 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.



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

Fig. 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.

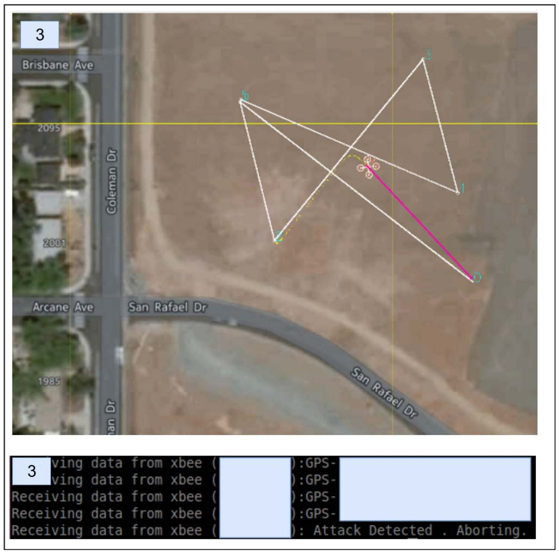


```
ving data from xbee ([redacted]):GPS-[redacted]
ving data from xbee ([redacted]):GPS-
Receiving data from xbee ([redacted]):GPS-
Receiving data from xbee ([redacted]):GPS-
Receiving data from xbee ([redacted]): Attack Detected . Aborting.
```

Fig. 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.

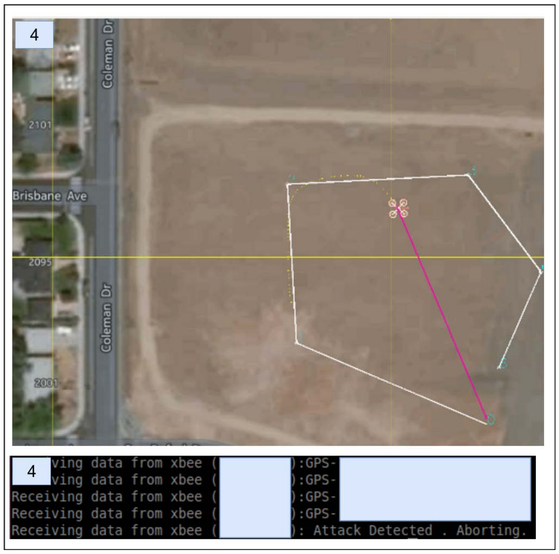
VI. Conclusion

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



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

Fig. 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.



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

Fig. 8. Way points 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.

with low-cost resources.

In the future work, we plan to further extend our authentication scheme to multi-UAV scenarios [12], [13], [18], where a cluster of UAVs aim to authenticate their controller. A possible approach is to have each member in the all UAVs (a 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 [7], [14], [15].

ACKNOWLEDGEMENTS

This material is based upon work supported by the National Aeronautics and Space Administration (NASA) under Grant No. NNX10AN23H issued through the Nevada NASA Space Grant, and Grant No. NNX15AI02H issued through the Nevada NASA Research Infrastructure Development Seed Grant and the National Science Foundation (IIS-1528137).

REFERENCES

[1] Amazon. Amazon prime air, 2016.

[2] A. Anjos and S. Marcel. Counter-measures to photo attacks in face recognition: a public database and a baseline. In *Biometrics (IJCB), 2011 international joint conference on*, pages 1–7. IEEE, 2011.

[3] S. M. Diamond and M. G. Ceruti. Application of wireless sensor network to military information integration. In *Industrial Informatics, 2007 5th IEEE International Conference on*, volume 1, pages 317–322. IEEE, 2007.

[4] C. Evans-Pughe. Bzzzz zzz [zigbee wireless standard]. *IEE review*, 49(3):28–31, 2003.

[5] L. Franceschi-Bicchierai. Drone hijacking? thats just the start of gps troubles, July 2012.

[6] S. Gorman, J. Y. Dreazen, and A. C. Insurgents hack u.s. drones. *The Wall Street Journal*, Dec. 2009.

[7] T. T. Han, H. M. La, and B. H. Dinh. Flocking of mobile robots by bounded feedback. In *2016 IEEE International Conf. on Automation Science and Engineering (CASE)*, pages 689–694, Aug 2016.

[8] K. Hartmann and C. Steup. The vulnerability of uavs to cyber attacks-an approach to the risk assessment. In *Cyber Conflict (CyCon), 2013 5th International Conference on*, pages 1–23. IEEE, 2013.

[9] B. M. Horowitz. Cybersecurity for unmanned aerial vehicle missions., April 2016.

[10] 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 *Global Communications Conference (GLOBECOM), 2016 IEEE*, pages 1–6. IEEE, 2016.

[11] H.-B. Kuntze, C. W. Frey, I. Tchouchenkov, B. Staehle, E. Rome, K. Pfeiffer, A. Wenzel, and J. Wöllenstein. Seneka-sensor network with mobile robots for disaster management. In *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, pages 406–410. IEEE, 2012.

[12] H. M. La, R. Lim, and W. Sheng. Multirobot cooperative learning for predator avoidance. *IEEE Transactions on Control Systems Technology*, 23(1):52–63, Jan 2015.

[13] H. M. La and W. Sheng. Dynamic target tracking and observing in a mobile sensor network. *Robotics and Autonomous Systems*, 60(7):996 – 1009, 2012.

[14] H. M. La and W. Sheng. Distributed sensor fusion for scalar field mapping using mobile sensor networks. *IEEE Transactions on Cybernetics*, 43(2):766–778, April 2013.

[15] H. M. La, W. Sheng, and J. Chen. Cooperative and active sensing in mobile sensor networks for scalar field mapping. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 45(1):1–12, Jan 2015.

[16] C.-C. Lu and S.-Y. Tseng. Integrated design of aes (advanced encryption standard) encrypter and decrypter. In *Application-Specific Systems, Architectures and Processors, 2002. Proceedings. The IEEE International Conference on*, pages 277–285. IEEE, 2002.

[17] M. McFarland. Google drones will deliver Chipotle burritos at Virginia Tech, September 2016.

[18] T. Nguyen, T. T. Han, and H. M. La. Distributed flocking control of mobile robots by bounded feedback. In *2016 54th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 563–568, Sept 2016.

[19] T. C. Nguyen. Virus attacks military drones, exposes vulnerabilities, October 2011. Retrieved 6/7/13.

[20] T. C. Nguyen. How college students hijacked a government spy drone., 2012. Retrieved 6/7/13.

[21] P. Paganini. Hacking drones ... overview of the main threats. retrieved 6/7/13. 2013.

[22] W. Sałabun. Processing and spectral analysis of the raw eeg signal from the mindwave. *Przeglad Elektrotechniczny*, 90(2):169–174, 2014.

[23] A. Sanjab, W. Saad, and T. Basar. Prospect theory for enhanced cyber-physical security of drone delivery systems: A network interdiction game. In *Proc. of the IEEE International Conference on Communications (ICC), Communication and Information Systems Security Symposium, Paris, France,*, 2017.

[24] E. Yüksel, H. R. Nielson, and F. Nielson. Zigbee-2007 security essentials. In *Proc. 13th Nordic Workshop on Secure IT-systems*, pages 65–82, 2008.