

# 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 gained much attention in recent years for both commercial and military applications. The progress in this field has gained much popularity and the research has encompassed various fields of scientific domain. Cyber securing a UAV communication has been one of the active research field since the attack on Predator UAV video stream hijacking in 2009. Since UAVs rely heavily on on-board autopilot to function, it is important to develop an autopilot system that is robust to possible cyber attacks. In this work, we present a biometric system to encrypt the UAV communication by generating a key which is derived from Beta component of the EEG signal of a user. We have developed a safety mechanism that would be activated in case the communication of the UAV from the ground control station gets attacked. This system has been validated on a commercial UAV under malicious attack conditions during which we implement a procedure where the UAV return safely to a ‘home’ position.

## 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. It could be well explained by the increasing affordability of the technology by hobbyists and enthusiasts, which allows them for the creation of innovative applications for the UAV’s. This have subsequently led to the occurrence of several severe incidents of different type of attacks on both military and civil UAVs. Several security issues have been demonstrated in recent investigations of cheap consumer UAVs, revealing these systems to be vulnerable to attack.

Commercial activities such as Google’s “Project Wing” [18], 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 with 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 in modern times communicate with each other using small mobile modules called XBee. XBee’s provides the functionality of securing the communication using AES encryption standard. We generate an AES encryption key derived from the an EEG signal. We have developed a demonstration safety mechanism which becomes activated in case there is a detection of potential

attack from a third party. This secures UAV communication using a biometric signal. This entire system is 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 Xbees, we create a simple attack scenario hack, in which 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 known incidents where civilian and military robots have been remotely compromised for the purposes of taking control of the UAV or making it crash-land. The first most popular known attack on a UAV occurred in 2009, where the Iraqi militants used “SkyGabbler” software to intercept live video feeds from an unsecured communication link used by a Predator Drone [8]. In October 2011, a key-logging malware was found in the Predator and Reaper ground control stations, likely installed using a removable hard drive. The virus got spreaded to both classified and unclassified computers [19].

A more troubling incident that grabbed international attention was the claimed theft of a Sentinel RQ-170 UAV by Iranian forces in December 2012. Hostile agents were able to compromise the control system of the craft and remotely land the UAV, obtaining sensitive data including mission and maintenance data. There are competing theories regarding how the RQ-170 Sentinel may have been lost. The simplest theory is that the loss of the UAV was a result of a technical malfunction, causing the UAV to mistakenly land in Iranian territory [9].

However, a more nefarious possibility is that through a vulnerability in a sensor system, the UAV’s GPS could have been intentionally fooled into landing to a location where a hostile agent intended. This type of attack is generally referred to as a “GPS-Spoofing” attack [7], [9]. An example of this type of attack was demonstrated by a University of Texas at Austin research team, partnered with the Department of Homeland Security to demonstrate the ability to hijack a military UAV. Using relatively inexpensive equipment, these researchers were able to spoof the global position system (GPS) and take complete control of the UAV [20] [1].

Interesting research regarding control security for UAVs is being pursued. A team from the University of Virginia (UVA)

and the Georgia Tech Research Institute, operating with the Federal Aviation Administration (FAA), conducted flight tests that evaluated a new class of cyber security solutions on a UAV performing a video surveillance mission. Their goal was to protect computer-controlled remote systems from cyber attacks. It included a new cybersecurity layer called as System-Aware which represents a class of solutions that depends on detailed knowledge of the design of the system being protected. This layer of security provides both complement network and perimeter security solutions and protects against supply chain and insider attacks that may be embedded within a system [10].

Most UAV systems are moving their infrastructure towards more network-centric command and control, where all of the components are interconnected through sophisticated mesh networks [5]. This enables fast communication and constant environmental and asset awareness, but introduces security drawbacks. Some military UAV systems, such as the Global Hawk, already employ this type of infrastructure. Public safety and disaster management UAVs are also moving to a similar network architecture for planning and communication [12]. When the components of the system are interconnected through such a network, a compromise of one component can cause a propagation of failures or malicious behavior can occur throughout the whole system.

Other research from UVA and the MITRE Corporation at Creech Air Force Base in Nevada designed and conducted a set of tabletop simulation-based experiments with active military UAV pilots. The purpose of these simulations was to determine the best course of action if a cyberattack was detected and if autonomous behavior could provide a secure and safe solution to a potential attack. The pilots presumed that a System-Aware solution could automatically detect cyber attacks. The pilots were asked to suggest how to control the UAV to restore normal operations. Possibilities included navigating to an earlier waypoint or switching from GPS-based navigation to less accurate, but more trusted, inertial navigation [10].

An interesting perspective which attempts to solve the cyber-security aspect of UAVs considers the whole scenario of vendor and an attacker as a zero-sum network interdiction game. It is represented as a game where the vendor, also assumed an evader, seeks to choose the optimal path strategy for its UAV, from a source location to a destination location, to evade attacks along the way and minimize its expected delivery time. On the other hand, the attacker or interdictor, aims at choosing the optimal attack locations along the paths traversed by the UAV to interdict the UAV, causing cyber or physical damage, with the goal of maximizing the travel time. Later on it is shown that this network interdiction game is equivalent to a zero-sum matrix game whose Nash equilibrium (NE) can be derived by solving two linear programming (LP) problems. Solving the LP's would give the expected delivery time under different conditions [3].

One potential solution is to use biometric information to secure communication between a UAV and its command and control station. This would allow the UAV to verify that its

stated operator is issuing the commands to the UAV. 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 of the actual operator [4]. 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. ZigBee is based on the international standard 802.15.4. To extend the transmission range, ZigBee is adding mesh networking functionality on top of the 802.15.4 standard, in which single messages are forwarded through the network to its destination node. Depending on the frequency band used, transmission rates can vary. Typically it ranges from 20kbit/s to 250kbit/s [6].

Zigbee uses IEEE 802.15.4 protocol as its MAC layer. IEEE 802.15.4 sets the encryption algorithm to use when cyphering the data to transmit. However, the standard does not specify how the keys have to be managed or what kind of authentication policies have to be applied. These issues are treated in the upper layers which are managed by ZigBee. The encryption algorithm used is AES (Advanced Encryption Standard) with a 128b key length (16 Bytes). The AES algorithm is not only used to encrypt the information but also validates the data which is sent [17]. This Data Integrity is achieved using a Message Integrity Code (MIC) also named as Message Authentication Code (MAC) which is added to the message. So, a message is received from a non-trusted node we will see that the MAC generated for the sent message does not correspond to the one what would be generated using the message with the current secret Key, so we can discard this message. The MAC can have different sizes: 32, 64, 128 bits, however it is always created using the 128b AES algorithm. The MAC's size is just the bit length which is attached to each frame. Data security is accomplished by encrypting the data payload field with the 128b Key. ZigBee implements two extra security layers on top of the 802.15.4 layer: Network and Application security layers. All three security policies rely on the AES 128b encryption algorithm. There are three kinds of keys:

**Master key:** These are pre-installed in each node. Their function is to keep confidential the Link Keys exchange between two nodes in the Key Establishment Procedure (SKKE) [22].

**Link Keys:** These are unique between each pair of nodes. These keys are managed by the Application level. They are used to encrypt all the information between each two devices, for this reason more memory resources are needed in each device [22].

**Network Keys:** These are a unique 128b key shared among all the devices in the network. It is generated by the Trust Center and regenerated at different intervals. Each node has to get the Network Key in order to join the network. Once

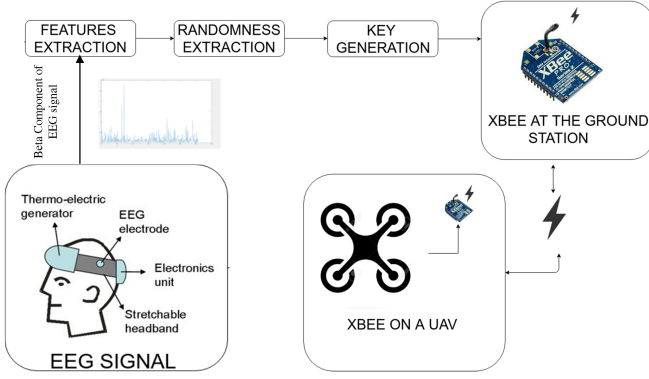


Fig. 1. Basic block diagram of the system overview.

the trust center decides to change the Network Key, the new one is spread through the network using the old Network Key (see image above about “ZigBee Residential Mode”). Once this new key is updated in a device, its Frame Counter (see in the previous sections) is initialized to zero. This Trust Center is normally the Coordinator, however it can be a dedicated device. It has to authenticate and validate each device which attempts to join the network.

#### IV. APPROACH

The EEG signal is unique; to a person and values overtime. It is possible to generate a key unique to a particular user. Also, based on different user activity and different state of mind, the EEG signal of even a same person will be different. Moreover, this unique signal changes every few hours at different state of mind, which means 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 robust 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 of both the UAV and the ground control station with the Key generated from the above procedure. We also implement a safety backtrack path procedure in case the communication is attacked.

##### A. EEG Signal Properties

We obtain a user’s EEG signal recorded using the Mind-wave EEG sensor [21]. This device safely measures and outputs the EEG power spectra (alpha waves, beta waves, etc), NeuroSky eSense meters (attention and meditation), and eye blinks. The device consists of a headset, an ear-clip, and a sensor arm. The headsets reference and ground electrodes are on the ear clip and the EEG electrode is on the sensor arm, resting on the forehead above the eye (see Figure 1). It operates using battery power.

We chose to use Beta waves from the EEG signal as the basis for our analysis. Beta waves are in the frequency range of 12 and 30 Hz, but are often divided into  $\beta_1$  (low Beta) and  $\beta_2$  (high Beta) to get a more specific range. The waves are small and fast, associated with focused concentration and

best defined in central and frontal areas. There is an increase of  $\beta$  activity when a person concentrates on tasks such as resisting or suppressing movement or solving a math task.

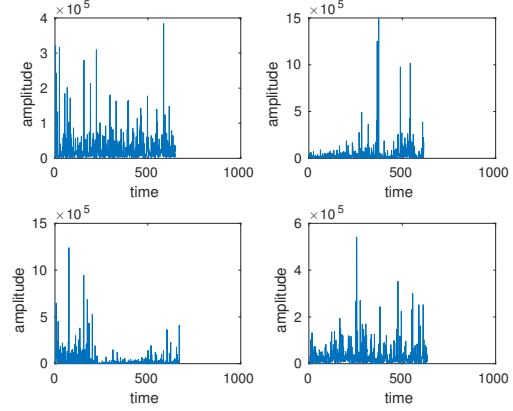


Fig. 2. Beta component of EEG waveform of 4 different people. The patterns in the  $\beta$  waves are unique to each individual, making them ideal for biometric encryption.

##### B. Feature Extraction

We record a EEG signal (Beta waves) from a specific user for time period  $T$ . The Beta waves are amplified by amplifier value  $A$  and matched via high order Legendre Polynomials, where Legendre Differential equation is given by:

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

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

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

The  $n$ -degree equation used for fitting data is given by:

$$y(x) = a_0 + \sum_1^n a_i p_{i(x)}. \quad (3)$$

The polynomial coefficients  $a_0, a_1, \dots, a_n$  are combined together with the time window of size  $T$  and the amplitude multiplier  $A$  to form the raw feature vector  $z := \{ca_0, ca_1, ca_2, \dots, ca_n, A, T\}$  where  $c$  is a constant to magnify the difference between coefficients. We map  $z$  to  $w$  such that  $w = z \times M + \gamma$  where  $M$  is an  $n \times n$  invertible matrix which satisfies  $\sum_i m_{i,j} = 1$ ;  $\gamma$  is a random vector whose elements are within the range  $[2^{-\theta}, 2^{\theta}]$ .

The polynomial coefficients are combined together with the time window size  $T$  and the amplitude multiplier  $A$  to form the raw feature vector. Since attackers can reconstruct the original EEG waveform given the feature vector, we map the feature vector with some random vector using Linear transformation. This results as a random feature vector  $w$  [11].

### C. Randomness Extraction

After obtaining feature vector  $w$ , we use a reusable fuzzy extractor constructed from  $(n, k)$ -BCH codes (The BCH codes form a class of cyclic error-correcting codes to correct errors occurred [11].) with generator function to extract enough randomness from it. Randomness provides the functionality of representing the feature vector in different form so that attacker cannot reconstruct the original signal.

The randomness extracted from each feature  $r_i$  is computed as  $r_i = H_x(w_i)$ , where  $H_x$  is a hash function in a universal hash family. The universal hash family  $H$  is a class of hash functions.  $H$  is defined to be universal if the possibility of a pair of distinct keys being mapped into the same index is less than  $1/l$  ( $l$  is the length of the randomness string). The hashing operation is performed after making a random choice of hash function from the universal class  $H$ . The universal hash function already gives the optimal length of extracted randomness [11].

We also compute the syndrome  $S_c$  of feature values for future authentication. If the feature element is viewed as  $w_i(x) = w_{i_0} + w_{i_1}x + \dots + w_{i_{n-1}}x^{n-1}$ , every element  $w_i$  has a corresponding syndrome  $S_{c_i}$  for  $(n, k)$ -BCH codes:

$$S_{c_i} = w_i(x) \bmod g(x) = \{w_i(\alpha^1), w_i(\alpha^2), \dots, w_i(\alpha^{2^r})\}. \quad (4)$$

### D. Key Generation

Next, we generate the key based on the features and pre-program the specific UAV with that key to secure the communication channel. This is a practical way to ensure that both the ground control station Xbee and the XBee on-board UAV obtain exactly the same key for encryption and decryption. The key  $K$  is generated based on chosen extracted randomness from the previous step [11]. The key generation technique is given below.

We randomly choose  $q$  constants  $1 \leq j_1 \leq \dots \leq j_q \leq n$  to pick up several features and produces a permuted feature vector  $v := \{w_{j_1}, \dots, w_{j_q}\}$ .

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

### E. Configuring XBee with the Key Generated

After generating the key using the above procedure we configure the XBee's AES encryption key parameter to use the generated key for communication. For this experiment, we used the Mindwave sensor and Alienware 15' with i7 6820 HK processor to create the EEG system. The architecture of the EEG system is described in Figure 1.

We utilized a commercially available UAV to conduct this experiment. The UAV uses the Pixhawk as its controller and had android as the CPU which had the XBee connected to in order to communicate with the ground control station. The UAV and the base station were wirelessly connected using Xbee transmitter and receivers.

After configuring the AES encryption key of the XBee with the generated encryption key, we tested the communication of UAV with the Xbee connected to the ground

control station. The AES key configuration ensured secured communication of the UAV to the ground control station. However, we have also introduced a scenario where an attacker is trying to intercept the communication between the UAV and ground control station for the primary purpose of controlling the UAV for its own purpose. 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.

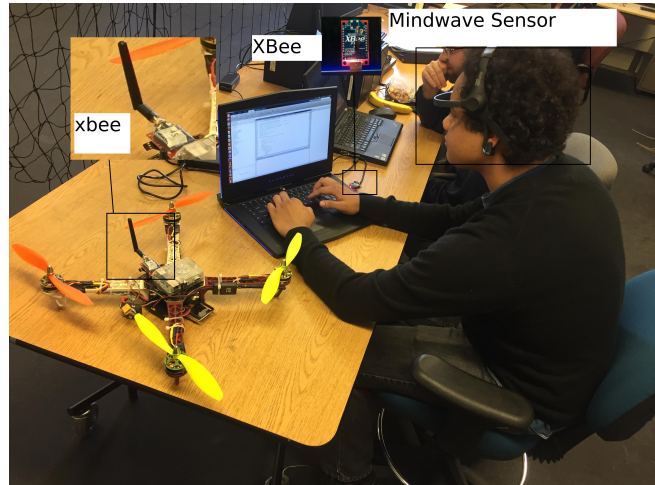


Fig. 3. Experimental Setup.

As a safety measure, we have 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 its 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 ← xbeedata.getAddress()
if getAddress ≠ groundcontrolstation.getAddress() 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 a hack is attempted, the Xbee sends predefined signal to the ground control station which signals the station to configure



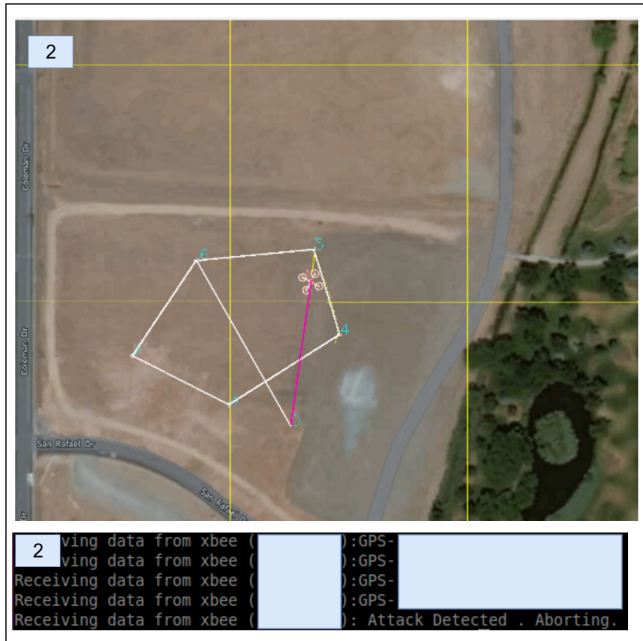


Fig. 6. Waypoints set for the experiment in the second configuration. The attack was discovered after the UAV navigated from waypoint 5 and Return-to-Launch (RTL) was enabled.

sending control signals to the UAV, our algorithm successfully detects the intervention (since the received packets at the UAV's XBee has different source address). After detection of the intervention, the UAV initiates its RTL mechanism and return 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 setup 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 is restricted to the ground control station and it hovers at a specified location where the attack was attempted. After the Xbee is configured to a new AES key, the navigation is resumed to the destined location.

## 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 intervention is detected along the way. 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.

In the future work, we plan to further extend our authentication scheme to multi-UAV scenarios [13], [14], 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 [15], [16].

## 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.

## REFERENCES

- [1] Hacking drones ... overview of the main threats.
- [2] Amazon. Amazon prime air, 2016.
- [3] W. S. Anibal Sanjab 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*.
- [4] 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.
- [5] 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.
- [6] C. Evans-Pughe. Bzzzz zzz [zigbee wireless standard]. *IEE review*, 49(3):28–31, 2003.
- [7] L. Franceschi-Bicchierai. Drone hijacking? thats just the start of gps troubles, July 2012.
- [8] S. Gorman. Insurgents hack u.s. drones, 2009.
- [9] 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.
- [10] B. M. Horowitz. Cybersecurity for unmanned aerial vehicle missions., April 2016.
- [11] P. Huang, B. Li, L. Guo, Z. Jin, and Y. Chen. A robust and reusable eeg-based authentication and data encryption scheme for ehealth systems. In *Global Communications Conference (GLOBECOM), 2016 IEEE*, pages 1–6. IEEE, 2016.
- [12] 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.
- [13] 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.
- [14] 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.
- [15] 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.
- [16] 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.
- [17] 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.
- [18] M. McFarland. Google drones will deliver Chipotle burritos at Virginia Tech, September 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] W. Sařabun. Processing and spectral analysis of the raw eeg signal from the mindwave. *Przeglad Elektrotechniczny*, 90(2):169–174, 2014.
- [22] 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.