Reliable Security For Drones

Nidhi R Nayak[1], Goutam R[2]
[1,]Dept of Computer science & engineering
[2]Assistant professor, Dept of Computer science & engineering
[1, 2] Atria institute of technology, Bangalore, India.

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 behaviour, it is important to develop an autopilot system that is robust to potential cyber-attack.*

Keywords- UAV, xbee, EEG signal, encryption, advanced encryption standard (AES).

I. INTRODUCTION

UAV's are commonly called as drones,which is the aircraft system without human pilots. 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 [1], [2]. The increasing affordability of UAVs has broadened their use by hobbyists and enthusiasts, companies, and government agencies [3], [4]. This has subsequently led to the occurrence of severe incidents of different type of attacks on both military and civilian UAVs. Security laws 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", which has successfully tested its drones for food delivery, and Amazon's ``Prime Air'' service , which aims to provide same-day package delivery, would place several drones in commercial airspace, near population centres.

II. PROPOSED TECHNIQUE

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.

To enhance the security of the drone and base station communication, we need to perform the testing ona 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 have to 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.

III. WIRELESS COMMUNICATION WITH 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. 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 [5]. 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.

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. 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. 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. 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.

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 [6].

This element is utilized as a part of the product XCTU fora 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 [7], [6].

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 [6].

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 [6].

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 behaviour, 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 [5], [6].

IV. BLOCK DIAGRAM

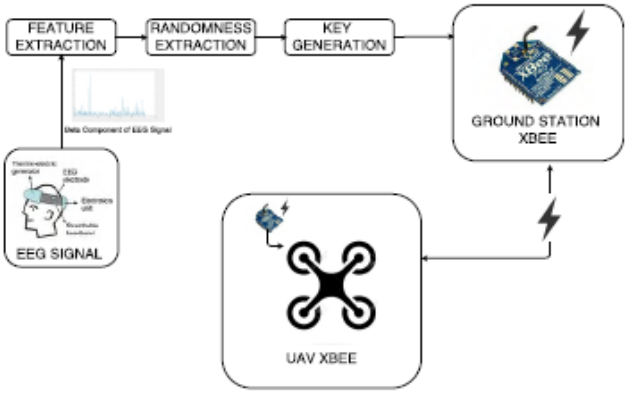

Figure: basic block diagram of the system

We record a user's EEG signal using the Mind wave EEG sensor for our evaluation. Then extract coefficients from Beta data using Legendre's polynomials. We perform encoding of the coefficient's 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.

A. EEG SIGNAL PROPERTIES

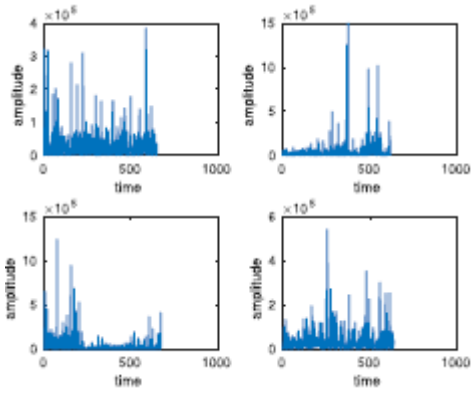

Figure 2: beta component of EEG waveform

We record a user's EEG signal using the Mind wave EEGsensor for our evaluation. 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 (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) are often classified into _1 (low Beta) and _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 beta activity when a person focuses on mental tasks such as resisting something or solving an analytical task [9] [10].

.

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:

$$\partial\partial x[(1-x2)\partial\partial xPn(x)]+n(n+1)Pn(x)=0\ldots\ldots\ldots 1$$

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 [11].
Legendre polynomials are computed using Rodrigues's formula, which is given by:

$$Pn(x) = 12n.n!\ 2n2[(x2-1)n] \text{ -------(2)}$$

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.

The randomness derived from each feature *ri* is computedas *ri =Hx* (*wi*). Here, *Hx* 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).

D. *KEY GENARATION*

The key generated based on the above features is used tosecure 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 [8]. The key generation technique is:

Randomly select *q* constants 1 ≤ j1 ≤ ……≤ jq < n to map several features to produce a feature vector *v* = {*wj*1 ; : : : ;*wjq}*

Most of the times the feature vectors are permuted. The key *K* is produced based on extracted randomnessrjiV *K:rj*1 ||:::: || *rjq;* where || denotes concatenation.

E. *CONFIGURING XBEE WITH KEY GENERATED*

We secured the XBee's communication using the generated AES encryption key. For this experiment, we used the Mind wave 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.

As a safety measure, we preconfigured the UAV's Xbeeto 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. The Lock GPS () function ensures that the sensor is not affected in any other way since it becomes completely independent of the rest of the communication process.

V. 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.

REFERENCES

[1] 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.

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

[3] 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 wild_retracking," in Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst. (IROS), Sep. 2017, pp. 6648_6653.

[4] 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.

[5] Digi. (2017). How XBee Devices Communicate: XBee/XBee-PRO S2C 802.15.4RF ModuleFeb.102018.[Online].Available:https://www.digi.com/resources/documentation/Digi.

[6] 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. 993994.

[7] 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.

[8] P. Huang, B. Li, L. Guo, Z. Jin, and Y. Chen, ``A robust and reusable ecgbasedauthentication and data encryption scheme for ehealth systems,"in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1_6.

[9] T. L. Huang and C. Charyton, ``A comprehensive review of the psychologicaleffects of brainwave entrainment," Alternative Therapies Health Med., vol. 14, no. 5, pp. 3850, 2008.

[10] T. Pham, W. Ma, D. Tran, P. Nguyen, and D. Phung, ``Eeg-based userauthentication in multilevel security systems," in Proc. Int. Conf. Adv. Data Mining Appl., 2013, pp. 512523.

[11] Khalil and F. Sue, ``Legendre polynomials based biometric authenticationusing QRS complex of ECG," in Proc. Int. Conf. Intell. Sensors,Sensor Netw. Inf. Process., Dec. 2008, pp. 297302.