Secrecy Coding in the Integrated Network Enhanced Telemetry (iNET)

SECRECY CODING IN THE INTEGRATED NETWORK ENHANCED TELEMETRY (iNET)

Morteza Shoushtari
Department of Electrical and Computer Engineering
Brigham Young University
morteza.shoushtari@byu.edu

Faculty Advisor:
Dr. Willie Harrison

ABSTRACT

Data security plays a crucial role in all areas of data transmission, processing, and storage. This paper considers security in eavesdropping attacks over wireless communication links in aeronautical telemetry systems. Data streams in these systems are often encrypted by traditional encryption algorithms such as the Advanced Encryption Standard (AES). Here, we propose a secure coding technique for the integrated Network Enhanced Telemetry (iNET) communications system that can be coupled with modern encryption schemes. We consider a wiretap scenario where there are two telemetry links between a test article (TA) and a legitimate receiver, or ground station (GS). We show how these two links can be used to transmit both encrypted and unencrypted data streams while keeping both streams secure. A single eavesdropper is assumed who can tap into both links through its noisy channel. Since our scheme does not require encryption of the unencrypted data stream, the proposed scheme offers the ability to reduce the size of the required secret key while keeping the transmitted data secure.

INTRODUCTION

Consider a wireless communications system that consists of a test article (TA), a telemetry link, and a ground station (GS) receiver that collects and processes transmitted signals from the TA. In the world of aeronautical telemetry, such systems may require some real-time processing, and all links have strict reliability and security requirements. Due to the nature of wireless transmissions, aeronautical telemetry systems can be vulnerable to a number of factors that degrade reliability and/or security over telecommunications links. Performance over telemetry links may suffer, e.g., due to intersymbol interference from multi-path propagation [1, 2], or due to more sinister disturbances such as cyber-attacks [3].

To prevent system attackers from obtaining sensitive information, data security is typically guaranteed through the use of modern encryption protocols and algorithms. The last few decades, however, have given rise to a new area of inquiry called physical-layer security [4] that has been shown to be capable of enhancing security efforts at other layers through coding and signaling ef-

forts at the physical layer of communications systems [5]. In the original work on the subject [6], Wyner introduced the basic wiretap channel model, and showed how one could use coding techniques similar to error-control coding to devote coding overhead to secrecy rather than reliability.

This paper explores how physical-layer security may affect the level of achievable secure communications in modern telemetry links. We explore the possibility of adding physical-layer security components to the iNET system. The iNET is the telemetry networking approach that enhances reliability and security between TA and GS compared to older point-to-point links using network capabilities [7]. Traditional telemetry systems consist of only a one-way radio link from TA to GS, but iNET also adds another bidirectional link between the legitimate transmitter and receiver that leads to increased efficiency and effectiveness on data communication [8, 9]. In this paper, we propose a new scheme based on physical-layer security and network coding principles that maintains data security while reducing the size of the required secret key for the iNET communications system.

TRADITIONAL ENCRYPTION IN AERONAUTICAL TELEMETRY

AES is a formal encryption method adopted by the National Institute of Standard and Technology (NIST) of the US government [10] and is accepted in the telemetry industry [11]. The AES encryption algorithm is a block-based algorithm, which means that AES's encryption and decryption processes work on a single block of data at a time. Encryption and decryption of a block of data occur in several rounds using a key. The algorithm's use case depends on the length of the key. The term "rounds" refers to the way in which the encryption (or decryption) algorithm mixes the data, and then re-encrypts (or re-decrypts) it. These processes can be repeated in 10, 12, and 14 rounds with respective key sizes of 128-bits (16 bytes), 192-bits (24 bytes), and 256-bits (32 bytes). It is of note that AES's encryption and decryption functions are performed using the same key, which makes AES a symmetric encryption algorithm. At the first step of the procedure, data is arranged in blocks and then encryption (or decryption) operations are executed over multiple rounds, as previously stated. Each round consists of two main functions (1) substitution, and (2) permutation. The substitution function exchanges each byte of data based on a non-linear look-up table, while the permutation function shifts and mixes rows and columns of the blocked data respectively. Figure 1 describes the mathematical encryption and decryption process of the AES algorithm.

AES has superior security performance compared to previous encryption algorithms from the same family such as Data Encryption Standard (DES), and Triple-DES (3DES), but computational cost and energy consumption are excessive in each of these algorithms [8]. The performance of these cryptosystems depends on secure keys, and the sharing of secret keys is one of the biggest challenges in the application of cryptography today. This holds true for aeronautical telemetry applications, and designing good key management systems still remains an open problem in telemetry networks. This work provides a mechanism to reduce the length of the required key by one half.

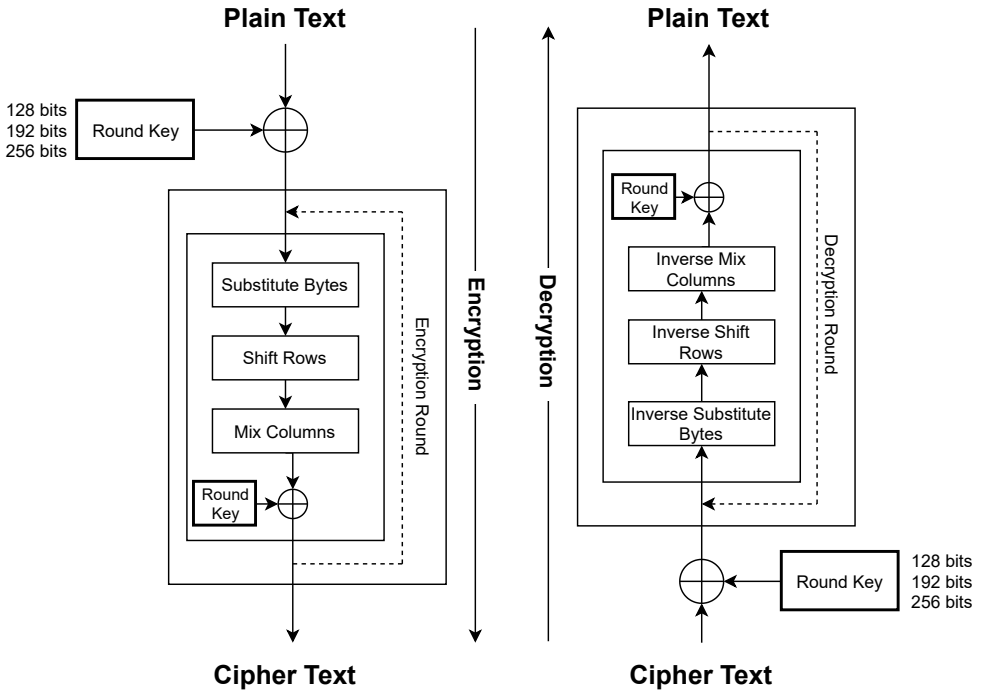

Figure 1: The AES mathematical encryption and decryption process.

SYSTEM SETUP

A. *Notation Clarification*

In this work, we indicate random variables (such as random vectors) and matrices as capital letters (e.g. X), and lower case letters denote realizations of their corresponding random variables (x). Calligraphic letters ($\mathcal{X}$) represent alphabets for their associated random variables, and the probability mass function (p.m.f) of a random variable is denoted by $p(x)$. Superscripts on variables indicate the length of vectors, and sets used as subscripts denote sub-vectors or sub-matrices that include only the columns indexed in the set. For instance, Z_X is a sub-vector of Z consisting of only columns with indices in the set X. Superscripts may be omitted when the length of vectors is clear. In this paper all codes are binary and vectors are row vectors. $\mathbb{H}(X)$ is the entropy of X, defined as

$$\mathbb{H}(X) = -\sum_{x\in\mathcal{X}} p(x)\log_2 p(x), \tag{1}$$

and $\mathbb{H}(X|Y)$ is the conditional entropy of X given Y that denotes how much entropy a random variable X has remaining if we already have perfect knowledge of Y. This is given by

$$\mathbb{H}(X|Y) = \sum_{y\in\mathcal{Y}} p(y)\mathbb{H}(X|Y=y) \tag{2}$$

$$= -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log_2 p(x|y). \tag{3}$$

Finally, mutual information $\mathbb{I}(X;Y)$ between two random variables measures the amount of information obtained about one random variable through observing the other random variable and is defined as

$$\mathbb{I}(X;Y) = \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log_2\frac{p(x|y)}{p(x)}. \tag{4}$$

B. Proposed Secrecy Coding

Consider the wiretap channel model for the iNET communication system in Figure 2. Here we see a TA is trying to send a secret message M^k to a GS in the presence of an eavesdropper. M^k is assumed to be a length-k binary vector with bits chosen independently, uniformly at random. There are two telemetry links between legitimate parties (TA and GS); one is encrypted and the other is unencrypted, and the TA wants to encrypt less data but keep data as secure as possible. For this purpose, first, the TA divides secret message M^k into two parts $M_1^{k/2}$ and $M_2^{k/2}$, then encrypts M_1 to produces ciphertext $S^{k/2}$. In practice, the encrypted link could use AES or any other cryptosystem. To simplify the security analysis, we will assume the crypto-layer is accomplished using the one-time pad (OTP) encryption technique with the secret key Λ, which is known to have perfect secrecy [12]; i.e.,

$$\mathbb{I}(M_1; S^{k/2}) = 0. \tag{5}$$

Then, $W^{k/2}$ be calculated as

$$W^{k/2} = M_1^{k/2} \oplus M_2^{k/2}, \tag{6}$$

where $\oplus$ is a bit-wise XOR operation. Then the TA encodes $W^{k/2}$ into an n-bit codeword X^n, and transmits the encrypted message $S^{k/2}$ through the encrypted link, and the codeword X^n over the unencrypted link to the GS. Again for simplicity, we assume the GS receives each of these signals error free. In practice, this may require forward error correction. Therefore, the GS is able to reconstruct M_1 and W error-free, and finally recover the secret message M.

Now consider the eavesdropper side. The eavesdropper's channel is a binary erasure channel (BEC), which means that the eavesdropper receives a bit of either data stream X^n or $S^{k/2}$ each independently with probability $(1-\epsilon_1)$, and $(1-\epsilon_2)$, respectively. The signals $Z_S^{k/2}$ and Z_X^n, respectively represent the eavesdropper's received versions of $S^{k/2}$ and X^n. We will consider the security implications of leaking information about M through the eavesdropper's observed signals. The symbol '?' indicates an erased bit in the eavesdropper's observed signals.

C. Coset Coding

The encoding of $W^{k/2}$ into the X^n is done using a secrecy (or wiretap) code. The secrecy coding we employ is based on a coset coding structure that maps the signal W, to one of secured codewords. It should be noted that these types of codes produce codewords without using any secret keys, and generally use the noise in the communications channel to keep the data secure. Let

$$Z = [Z_X^n \quad Z_S^{k/2}] \tag{7}$$

be the collection of all received signals at the eavesdropper. The best coding strategy in this scenario is to choose a code that maximizes the equivocation

$$E = \mathbb{H}(M|Z). \tag{8}$$

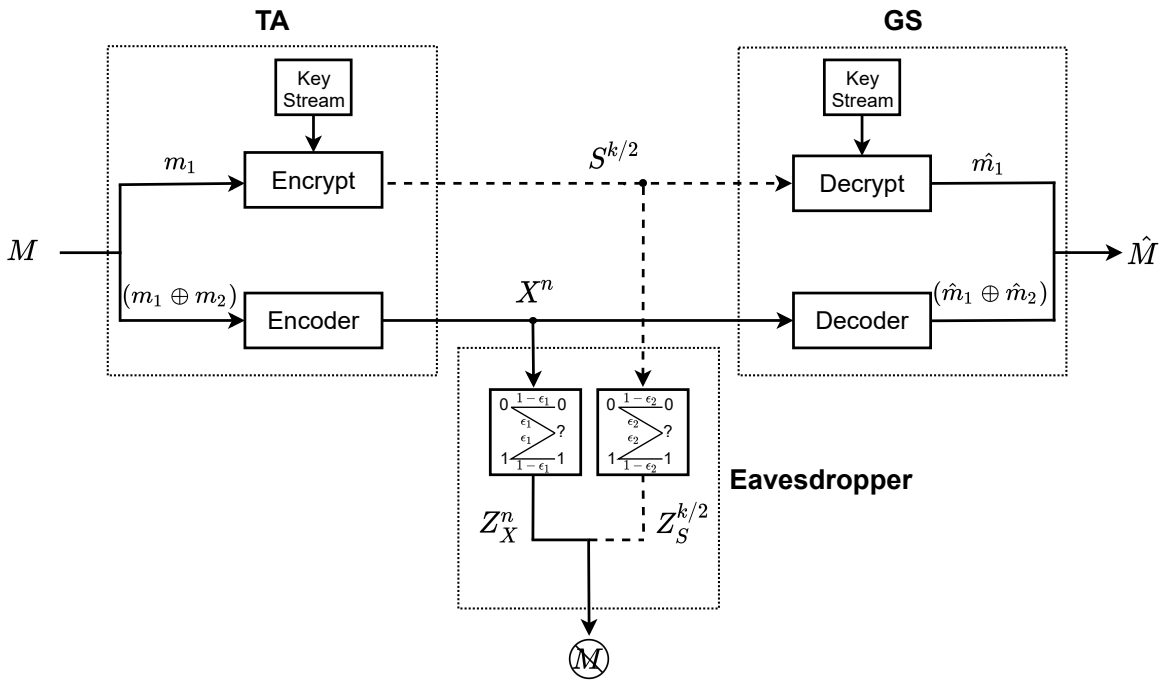

Figure 2: Wiretap channel model for the iNET.

Let $\mathcal{C}$ be an $(n, n-(k/2))$ binary linear block code, and $\mathcal{C} = C_0, C_1, C_2, ..., C_{2^{k/2}-1}$ be the cosets of $\mathcal{C}$. Also let G be an $(n-(k/2)) \times n$ generator matrix, and H be a $(k/2) \times n$ parity-check matrix for $\mathcal{C}$. Then define

$$G^* = \begin{bmatrix} G \\ G' \end{bmatrix}, \tag{9}$$

where G^* is the matrix used to encode W, and G' consists of $k/2$ linear independent row vectors from $\mathbb{F}_2^n$ that are not in $\mathcal{C}$. The TA encoder function also requires an $(n-(k/2))$-bit uniformly random binary auxiliary message W'. Then,

$$x^n = \begin{bmatrix} w' & w \end{bmatrix} G^* = \begin{bmatrix} w' & w \end{bmatrix} \begin{bmatrix} G \\ G' \end{bmatrix} = w'G \oplus wG', \tag{10}$$

where x^n represents the codeword of the corresponding binary message w. Note that, in coset coding, $w'G$ chooses the coset and wG' chooses a specific codeword from the coset uniformly at random.

On the decoding side, the decoder of GS attempts to decode codeword x^n by calculating the syndrome

$$\sigma = x^n H^T, \tag{11}$$

and because every codeword in a specific coset must have the same syndrome, consequently this syndrome can be map to the message w using a look up table.

	$w' = 00$	$w' = 01$	$w' = 10$	$w' = 11$
$w = 00$	0000	0110	1001	1111
$w = 01$	0111	0001	1110	1000
$w = 10$	1100	1010	0101	0011
$w = 11$	1011	1101	0010	0100

Table 1: A secrecy code table based on coset coding when $n = 4, k = 2$.

D. Numerical Example

Let us consider that the TA wants to send secret message $m = [1\ 0\ 0\ 1]$ to the GS, through both telemetry links as shown in Figure 2. The TA divides m into two parts $m_1 = [1\ 0]$ and $m_2 = [0\ 1]$, and produces binary vector w from m_1 and m_2 which is equal to $w = [1\ 1]$. The TA encrypts m_1 to generate ciphertext $s^{k/2}$. Let

$$G^* = \begin{bmatrix} G \\ \hdashline G' \end{bmatrix} = \left[\begin{array}{cccc} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ \hdashline 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{array}\right]. \tag{12}$$

The TA's encoder in (10) gives the secrecy code book as in Table 1. The TA selects w' at random, which then selects one of the codewords in the coset corresponding to binary message $w = [1\ 1]$ and sends ciphertext $s^{k/2}$ and codeword x^n to GS through encrypted and unencrypted telemetry links, respectively. Since we assume that both telemetry links are noise-free, therefore, the GS is able to receive $s^{k/2}$ and x^n without any error. For example, if GS receives $x^n = [1\ 1\ 0\ 1]$, then the syndrome can be calculated, or code Table 1 can simply be referenced to find that the binary message is equal to $w = [1\ 1]$. Also the GS decrypts $s^{k/2}$, and get $m_1 = [1\ 0]$, and finally can generate m_2 as follows

$$m_2 = m_1 \oplus w = [1\ 0] \oplus [1\ 1] = [0\ 1]. \tag{13}$$

Suppose the eavesdropper receives an erasure-prone version of transmitted codeword x^n and ciphertext $s^{k/2}$ due to its noisy channel. For example, if the eavesdropper's observation on the unencrypted link is $z_X = [1\ 1\ ?\ ?]$, the eavesdropper is unable to get any information about w, because according to our code table all four messages have a codeword that starts with $[1\ 1]$. Even if, however, the eavesdropper recovers w, there is still confusion about the message m due to the encrypted text and the network coding to produce W, as given in (6).

EQUIVOCATION EVALUATION

According to our wiretap channel model for the iNET in Figure 2, the eavesdropper has binary erasure channels with the erasure probabilities of ϵ_1 and ϵ_2 for unencrypted and encrypted links respectively. The ith bit of Z_X^n is then

$$Z_{X,i}^n = \begin{cases} ?, & \text{with probability } \epsilon_1, \\ X_i^n, & \text{with probability } (1 - \epsilon_1), \end{cases} \tag{14}$$

and the ith bit of $Z_S^{k/2}$ is given as

$$Z_{S,i}^{k/2} = \begin{cases} ?, & \text{with probability } \epsilon_2 \ , \\ S_i^{k/2}, & \text{with probability } (1-\epsilon_2), \end{cases} \tag{15}$$

where X_i^n and $S_i^{k/2}$ represent the i^{th}-bit of the transmitted codeword and ciphertext, respectively. Recall that $Z = [Z_X^n \quad Z_S^{k/2}]$ is the collection of received signals at the eavesdropper. Now we analyze the equivocation on the message given a specific observation $z \in \mathcal{Z}$

$$\mathbb{H}(M|Z) = \mathbb{H}(M|Z_X^n, Z_S^{k/2}). \tag{16}$$

We provide this analysis as a function of ϵ_1, ϵ_2, which yields the following four cases:

1. Noise-free case ($\epsilon_1 = 0$ and $\epsilon_2 = 0$).

   In this case the eavesdropper can get data from both telemetry links without any error. Hence, the eavesdropper can reconstruct W, and the equivocation decreases to the entropy of the key; i.e.,

   $$\mathbb{H}(M|Z_X^n, Z_S^{k/2}) = \mathbb{H}(M|X^n, S^{k/2}) = \mathbb{H}(M|W^{k/2}, S^{k/2}) = \mathbb{H}(\Lambda). \tag{17}$$

   This shows that when the eavesdropper receives all signals without errors the confusion to the eavesdropper is only a function of the unknown key, which is consistent with encrypted system. In the cases that follow we will see how our system adds confusion to the eavesdropper when the channels are noisy.

2. Noise on encrypted channel ($\epsilon_1 = 0$ and $\epsilon_2 > 0$).

   We now assume the eavesdropper has full access to the unencrypted text and can receive erasure-prone ciphertext $S^{k/2}$ through the encrypted link. The eavesdropper can again reconstruct message W and the equivocation becomes

   $$\mathbb{H}(M|Z_X^n, Z_S^{k/2}) = \mathbb{H}(M|X^n, Z_S^{k/2}) = \mathbb{H}(M|W^{k/2}, Z_S^{k/2}) = \mathbb{H}(\Lambda). \tag{18}$$

   Just as in case 1, every bit of key contributes to a unique bit of equivocation.

3. Noise on unencrypted channel ($\epsilon_1 > 0$ and $\epsilon_2 = 0$).

   Here the assumption is that the eavesdropper has error-free access to the encrypted link and has a noisy channel on the unencrypted link. The equivocation in this case is

   $$\mathbb{H}(M|Z_X^n, Z_S^{k/2}) = \mathbb{H}(M|Z_X^n, S^{k/2}) = \mathbb{H}(M|Z_X^n) + \mathbb{H}(\Lambda), \tag{19}$$

   because each bit of key and each bit of confusion brought on from the wiretap code yield independent bits of equivocation.

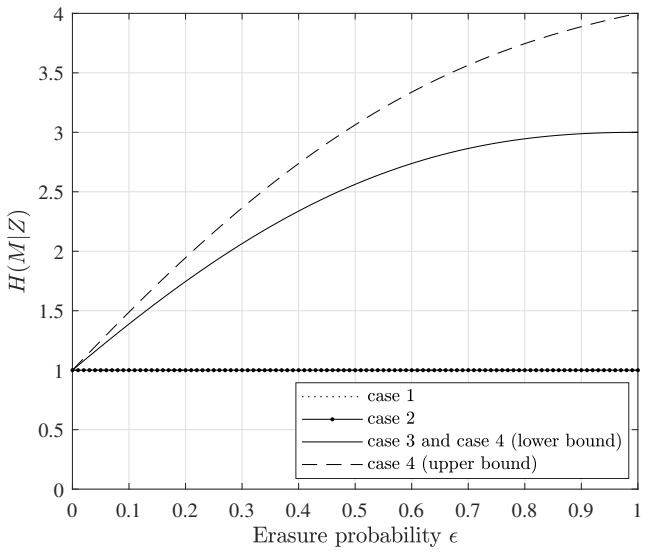

Figure 3: The equivocation $\mathbb{H}(M|Z)$ curves of proposed scheme with the secrecy code in Table 1.

4. Noise on both channels ($\epsilon_1 > 0$ and $\epsilon_2 > 0$).

   In this scenario, the presence of noise in the telemetry channels, which may be caused by natural disturbances, does not allow the eavesdropper to have perfect knowledge of either transmitted signal. Here the eavesdropper experiences erasure channels for both telemetry links. Thus, the equivocation of this case is lower bounded by the result from case 3 as

   $$\mathbb{H}(M|Z_X^n, Z_S^{k/2}) \geq \mathbb{H}(M|Z_X^n, S^{k/2}) = \mathbb{H}(M|Z_X^n) + \mathbb{H}(\Lambda). \tag{20}$$

   Moreover, $\epsilon(k/2) + \mathbb{H}(M|Z_X^n, S^{k/2})$ is an upper bound for $\mathbb{H}(M|Z_X^n, Z_S^{k/2})$, because each erased bit over the encrypted channel can add no more confusion than 1 bit in maximum case, i.e.,

   $$\mathbb{H}(M|Z_X^n, Z_S^{k/2}) \leq \epsilon(k/2) + \mathbb{H}(M|Z_X^n, S^{k/2}) = \epsilon(k/2) + \mathbb{H}(M|Z_X^n) + \mathbb{H}(\Lambda). \tag{21}$$

In all these cases, the proposed secrecy code does not rely on the eavesdropper's computing capability and it adds confusion to the eavesdropper as a function of the noise in the channel. The equivocation curves for all cases corresponding to the example of our scheme with the secrecy code in Table 1 are plotted in Fig 3. Note that as the eavesdropper's channels get noisier, the secrecy coding is able to add additional confusion beyond that supplied by the encrypted text.

CONCLUSIONS

Over the last few decades, information security in aeronautical telemetry systems has depended on cryptographic algorithms, which are deployed at the upper layers of network protocols. These algorithms require secret keys and proper key management. In this paper, we proposed a coding

approach for the iNET communication system with the presence of an eavesdropper who is able to tap into both telemetry links between the two legitimate parties. We showed that the TA can use the inherent noise of the telemetry channels to help keep the data provably secure. We demonstrated that our approach not only reduces the length of the key dramatically (by half), but also requires only low-complexity encoder/decoder operations to deploy. In the worst case (when the eavesdropper receives all signals error-free) the system retains its security from the encrypted text. As the quality of the eavesdropper's observed signals deteriorates, our system adds confusion to the eavesdropper above and beyond the level obtained using only cryptography.

REFERENCES

[1] F. Arabian and M. Rice, "On the performance of filter based equalizers for 16APSK in aeronautical telemetry environment," in *Proc. Int. Telemetering Conf. (ITC)*, Nov. 2018.

[2] F. Arabian and M. Rice, "Polarization diversity and equalization of frequency selective channels in telemetry environment for 16APSK," in *Proc. Int. Telemetering Conf. (ITC)*, Nov. 2019.

[3] R. Dukes, "Proposed iNET network security architecture," in *Proc. Int. Telemetering Conf. (ITC)*, Nov. 2009.

[4] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, UK: Cambridge University Press, 2011.

[5] W. K. Harrison and S. W. McLaughlin, "Physical-layer security: Combining error control coding and cryptography," in *Proc. IEEE Int. Conf. Communications (ICC)*, pp. 1–5, 2009.

[6] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[7] P. J. Noonan, T. A. Newton, G. C. Willden, T. B. Grace, and W. A. Malatesta, "iNET system manager," in *Proc. Int. Telemetering Conf. (ITC)*, Oct. 2014.

[8] H. Rifà-Pous and J. Herrera-Joancomartí, "Computational and energy costs of cryptographic algorithms on handheld devices," *Future Internet*, vol. 3, no. 1, pp. 31–48, 2011.

[9] M. Rice, K. Temple, T. Chalfant, D. Ernst, and C. Kahn, "Spectrum allocations: The aeronautical telemetry story in the USA," *IEEE Aerospace and Electronic Systems Magazine*, vol. 33, no. 12, pp. 50–58, 2018.

[10] M. Dworkin, E. Barker, J. Nechvatal, J. Foti, L. Bassham, E. Roback, and J. Dray, "Advanced encryption standard (AES)," 2001.

[11] M. Don and M. Ilg, "Advances in a low-cost software-defined telemetry system," in *Proc. Int. Telemetering Conf. (ITC)*, 2017.

[12] W. K. Harrison, K. Nelson, and S. Dye, "Physical-layer security for aeronautical telemetry," in *Proc. Int. Telemetering Conf. (ITC)*, Nov. 2018.