A Distortion-Theoretic Perspective for Redundant Metering Security in a Smart Grid

Mustafa El-Halabi, Abdallah K. Farraj, Hung D. Ly and Deepa Kundur
Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843
Email: {mustafa79, farraj, hungly, dkundur}@tamu.edu

***Abstract*—In a smart grid environment some customers employ third-party meters and terminals for integrity verification of the smart meter power measurements reported by the electric utility company. We address the security issues that may arise under the presence of a third-party wireless terminal. In this paper we consider a rate-distortion perspective that contrasts the Slepian-Wolf distortionless coding approach recently presented by Varodayan and Gao [1] for integrity verification through redundant metering. We show that through the use of a limited secret key, we can impose a certain minimum distortion on the eavesdropper, while enabling the wireless terminal to retrieve the measurements losslessly with high probability. We highlight the advantages of our approach.**

I. Introduction

A smart grid is a term used to describe an electricity network that employs advanced sensing, computation, and communications mechanisms to enable more efficient and flexible generation, transmission, and distribution of power through the grid. By facilitating bidirectional information and energy flow through the overall network, a smart grid promises energy savings, reduced operational and consumption costs, improved reliability, and great customer-centricity. One emerging service to consumers involves the availability of time-of-usage pricing. Here the electric power utility must install a *smart meter* at the physical location of a consumer. The meter provides real-time pricing information to the customer while tracking in quasi-real-time (typically once every 15 minutes) the customer's energy consumption. This higher granularity of information enables a customer to make more optimal decisions on energy usage, helps utilities in grid monitoring and planning through mechanisms such as *demand response*, and creates a culture of conservation.

This greater dependence on smart metering devices has recently resulted in cyber security concerns. One issue involves the *integrity* of the billing information a customer receives from the utility. Specifically, customers may question how accurate the energy usage information used for billing really is. Another issue relates to the *confidentiality* of the consumption data. Given the higher resolution of such acquired data that is communicated periodically to and stored by the utility, customer privacy issues arise. For example, specific types of activities such as charging a hybrid electric vehicle and running a clothes dryer have distinct energy signatures that can be employed by illegitimate parties to track the activities of an individual.

In this paper, we investigate the confidentiality of a third-party wireless device that is used to resolve billing data integrity issues between the utility company and the customers. We consider an information theoretic approach to addressing the integrity and privacy issues in a redundant metering framework employed for billing data integrity verification. Our goal is to, in part, shed light on fundamental paradigms and building blocks to enable a secure smart grid. We build upon the work of [1], and the information theoretic flavor provides fundamental insight into effective building blocks to secure system design. The proposed integrity verification scheme has more flexibility in transmission rate and integrity verification over that proposed in [1].

The rest of the paper is organized as follows: Section II introduces the concept of redundant metering and presents a recent case study demonstrating smart meter integrity verification. The smart meter integrity verification problem is then formally defined and the recent redundant metering work of Varodayan and Gao [1] is summarized. Section III presents a proposed solution to the smart meter verification problem based on a rate-distortion theory that promotes confidentiality of the consumer usage information. The system model and solution leverage information-theoretic notions of security and the details of a practical implementation are provided. Finally, concluding remarks are discussed in Section IV.

II. Redundant Metering

A. Media Attention

In 2009, a lawsuit was filed by nearly one thousand customers of *Pacific Gas & Electric* (PG&E) in Bakersfield, California. The plaintiffs claimed that PG&E's smart meters were resulting in overcharges to their utility bills [2], [3]. At that time, PG&E claimed that their smart meters were not the reason behind the rise in the bills. After successfully casting doubts on the integrity of the smart meter readings that were being used for billing, PG&E began to investigate further. In 2010, PG&E admitted that a few smart meters had accuracy and installation issues [2]–[4]. Although the faulted meters presented a very small percentage of the overall number of installed meters, the outcome was a substantial financial loss for the electric utility company.

In their attempt to check the integrity of the bills sent by PG&E, some customers had taken the initiative to install a

* Please note that the first three authors contributed equally to this article, and that their names are listed in alphabetical order.

2012 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)
978-1-4673-1433-6/12/$31.00 ©2012 IEEE

redundant, third-party, power meter [4] to validate the accuracy of the reported charges. In this scenario, the utility's smart meter measures the power usage and transmits the corresponding information to the electric utility company. Then, the utility relays the meter reading back to the customer as a *reported measurement*. A redundant meter installed by the customer also measures the power usage separately and it transmits this information as a *redundant measurement* wirelessly to a wireless terminal. Now the customer, equipped with the wireless terminal, can check the integrity of the power measurements taken by the utility meter. Although useful in checking the integrity of power measurements, this approach presents a substantial vulnerability; attackers can conceivably intercept the redundant meter data, jeopardizing the confidentiality of the customer consumption information.

B. Problem Setup

Specifically in this setting, the utility company installs a smart meter to measure the customer power usage, the smart meter sends the readings to the utility through a secure channel. The utility relays the smart meter readings back to the customer. In order to check the integrity of the readings, the customer installs an independent, redundant, power meter and a wireless terminal that will be used to view the power readings. The redundant meter measures the power usage and sends its readings, wirelessly, to the wireless terminal. As the reported and redundant measurements are available at the wireless terminal, the integrity of the utility smart meter can be verified. Fig. 1 elucidates this setup.

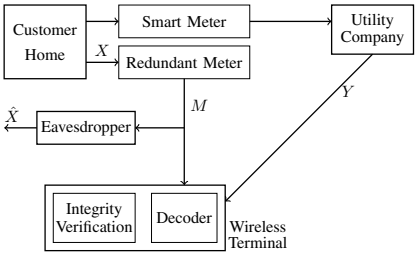

Figure 1. Power measurement integrity verification for a redundant metering setup in the presence of an eavesdropper: X, M, and Y represent the redundant meter measurement, the coded version of X, and the utility reported measurement respectively. The wireless terminal recovers X from M and compares with Y for integrity verification. The eavesdropper has access to M only.

A possible threat in this setup occurs because of the wireless nature of the communication link between the customer's redundant meter and the wireless terminal. An eavesdropper can exploit the wireless channel to intercept the power usage data reported by the redundant meter and violate the consumer privacy. Hence, the security issues addressed in this setting concern both data integrity and confidentiality. Data confidentiality can be provided through data encoding/decoding at the redundant meter and the wireless terminal. The encoder in the redundant meter will send its readings in a way that confuses the eavesdropper, and the decoder at the wireless terminal will be able to recover those readings back.

As illustrated in Fig. 1, X represents the power reading of the redundant meter (called the redundant measurement), Y represents the reading relayed by the utility company to the wireless terminal (known as the reported measurement), and M is the coded signal that is transmitted by the redundant meter to the wireless terminal. The eavesdropper has access to M only, he/she is assumed to be a passive listener that measures M but cannot change it.

C. Prior Art

Varodayan and Gao [1] addressed the confidentiality issue of the redundant metering paradigm used for integrity verification. They demonstrated how the inclusion of third party terminals and devices to enable specific types of protection may also introduce new forms of vulnerabilities not encountered before. The degree of dependence on these third party entities will influence the amount of risk they introduce to other smart grid components. Furthermore, they present a target for savvy attackers who will attempt to compromise those devices that are most "trusted" or depended upon.

The work of [1] enables both integrity and confidentiality for this problem by making effective use of source coding. Specifically, they integrate *Shannon* source coding theorem [5] with the results of Slepian and Wolf [6]. This provides a method of encoding the customer's redundant meter reading, that is sent wirelessly to the wireless terminal, such that it can only be decoded with the help of the readings relayed from the utility company. As shown in [1], integrity verification of the meter readings and confidentiality across the wireless link are simultaneously possible when the encoder at the redundant meter encodes the reading X into M at a rate R, such that $H(X|Y) \leq R < H(X)$, where $H(X)$ and $H(X|Y)$ represent the entropy and conditional entropy of X, respectively.

Since the decoder, located at the wireless terminal, receives both Y and M, i.e. an encoded version of X. Varodayan and Gao show that if X and Y are statistically dependent, the decoder can recover X from M and Y and accordingly check for the integrity of the reported measurement Y. If the two signals are significantly different, the coding rate R will be insufficient to recover X, and because of this decoding failure, a mismatch is reported and an integrity breach can be declared. This encoder-decoder setup is said to work well if the two meters are reasonably calibrated, but it would fail to work efficiently if the two meters are considerably uncalibrated [1].

D. A Rate-Distortion Perspective

In contrast to the distortionless coding scheme used in [1], we consider a rate-distortion perspective to secrecy [7]. Upon initial consideration, such an approach would have the following advantages:

1) Integrity checking will be independent of meter calibration. If the two meters are not calibrated, the Slepian-Wolf approach in [1] will not effectively work.
2) The data rate for transmitting M across the wireless link does not have to be as strictly bounded within a finite

range. The Slepian-Wolf approach limits the rate to be bounded between $H(X|Y)$ and $H(X)$.

3) The Slepian-Wolf approach requires X and Y to have a strong statistical dependence. The proposed scheme is independent of that condition.
4) Regardless of the computation power of the eavesdropper, security is guaranteed in this approach. In a coding scheme that utilizes classical cryptographic mechanisms, an eavesdropper with enough computation power can break the coding and successfully decrypt the redundant meter reading.

We adopt the coding scheme developed in [8], wherein the security is measured by the minimum distortion incurred by the eavesdropper. We show that adopting this perspective to the setting shown in Fig. 1 offers many improvements over the scheme proposed in [1]. We specifically adopt a rate distortion approach to achieve information-theoretic confidentiality. Through the use of a certain secret key at any positive rate, a certain distortion is induced on the eavesdropper that would prevent him/her from decoding the transmitted message. Accordingly, the minimum distortion that an eavesdropper incurs represents a security measure in such setting.

III. Rate-Distortion Solution

A. System Model

We consider the scenario of a customer that uses a redundant meter to make independent power measurements in order to verify the integrity of the utility company's consumption information. The independent and identically distributed (i.i.d.) sequence of the redundant measurements is denoted $\{X_1, X_2, ...\}$ and have a probability distribution $p(x)$. Each measurement X_i, at time index i, belongs to the alphabet $\mathcal{X}$. The redundant meter readings are encoded and transmitted to a wireless terminal. We assume the redundant meter and the wireless terminal, communicating through a lossless channel, share a secret key of rate R_k.

We assume that the passive eavesdropper intercepts the coded message M, and is capable of causally reconstructing the message X_i through performing a dynamic estimation. Specifically, we assume that the eavesdropper uses M, along with the past information in the measurement sequence $\{X_1, X_2, ..., X_{i-1}\}$, to perform an estimate of the measurement X_i as follows

$$z^{(i)}(M, X^{i-1}) = \hat{X}_i, \tag{1}$$

where $\hat{X}_i$ is the eavesdropper's estimate of X_i, X^{i-1} represents the sequence $\{X_1, X_2, ..., X_{i-1}\}$, and $z^{(i)}$ is the estimation function used by the eavesdropper to evaluate the decoded measurement. We consider the case of an eavesdropper who has perfect knowledge of X^{i-1} during estimation of X_i as it represents a worst-case scenario. We assert that the causality assumption on the eavesdropper's estimation is not restrictive and, in fact, makes the coding for secrecy more robust due to the dynamic capabilities of the eavesdropper. Developing a secure solution for this class of eavesdropper provides greater credibility and ensures robustness.

The encoder and decoder of an (n, R, R_k) block code are defined by the following mappings: $f : \mathcal{X}^n \times [2^{nR_k}] \to [2^{nR}]$ and $\phi : [2^{nR}] \times [2^{nR_k}] \to \mathcal{X}^n$, where R and R_k represent the transmission rate and the secret key rate, respectively.

B. Integrity Verification with Information-Theoretic Security

As previously mentioned, the distortion incurred by the eavesdropper in his/her attempt to reconstruct the redundant meter measurements is a key metric to evaluate the security of the encoded transmission. Hence, assuming we employ an (n, R, R_k) code, we require that for n sufficiently large, this code will induce enough distortion for the eavesdropper. This distortion prevents him/her from attaining a good reconstruction of the redundant meter reading. Furthermore, we simultaneously require that the wireless terminal successfully reconstructs the redundant meter reading X with high probability from M. To achieve the goal, we set out to design an (n, R, R_k) code such that for sufficiently large n, $\epsilon > 0$, and $D > 0$

$$P_r(\hat{X} \neq X) \leq \epsilon, \tag{2}$$

and

$$\frac{1}{n}\sum_{i=1}^{n} \min_{z^{(i)}(m, x^{i-1})} \mathbb{E}d(X_i, z^{(i)}(M, X^{i-1})) \geq D. \tag{3}$$

where $d(\cdot, \cdot)$ is the distortion function, the squared error distortion function $d(x, \hat{x}) = (x - \hat{x})^2$ represents one possibility, and $\mathbb{E}d(X_i, z^{(i)}(M, X^{i-1}))$ represents taking the expectation with respect to the joint distribution of X_i and $z^{(i)}(M, X^{i-1})$. Condition (2) ensures that the wireless terminal recovers the redundant measurement perfectly. Condition (3) guarantees that the eavesdropper is subject to at least a distortion D when he/she tries to recover that measurement.

It has recently been shown in [8], that the secret key rate R_k, the transmission rate R, and the induced distortion D tradeoff, is characterized by the following rate-distortion region:

$$\begin{aligned} R &\geq H(X) \\ R_k &\geq H(X|U) \\ D &\leq \min_{z(u)} \mathbb{E}d(X, z(U)), \end{aligned} \tag{4}$$

for some $p(x, u) = p(x)p(u|x)$ where U is an auxiliary random variable. We would like to review the achievability of region (4), and adapt it to perform the integrity checking. A main ingredient in coding for information-theoretic security is the notion of *binning*. As illustrated in Fig. 2, we begin by randomly generating a codebook of $2^{nH(X)}$ i.i.d codewords u^n. Then we randomly partition the codewords into $2^{nH(X|U)}$ bins. Hence, each bin contains $2^{nI(U;X)}$ codewords. Note that the number of bits to represent a codeword's index in a bin is $nI(U; X)$. The secret key is uniformly selected from the key space $\{1, \ldots, 2^{nR_k}\}$ and is used to encrypt the bin indices.

Given a measurement $\{X_i\}_{i=1}^{\infty}$, the redundant meter searches for the codeword that is the closest to (or jointly typical) to the measurement. As a result, the transmitted message, $\{M_i\}_{i=1}^{\infty}$, consists of the index of the typical codeword along with the encrypted bin index corresponding to the typical codeword. Since the key length is equal to the number of bits that is required to represent the bin index, the encrypted bin index is perfectly secure against the eavesdropper. Given

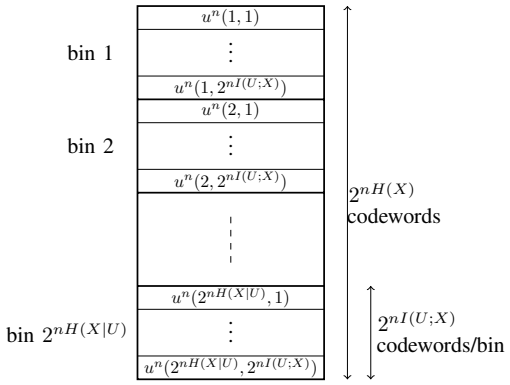

Figure 2. Codebook

access to the shared secret key, the wireless terminal is able to successfully decode the message and recover the measurement with high probability. On the other hand, without the secret key, the eavesdropper must either guess or solve an optimization problem to retrieve the measurement. It was shown in [8] that under this coding strategy the eavesdropper can only reconstruct a very noisy version of the measurement.

Returning to our billing integrity verification problem, we deduce that the proposed coding strategy enables the wireless terminal to successfully verify the integrity of the reported measurement. In particular, after receiving the measurement reported from the utility company, Y, the wireless terminal looks for the codeword which is jointly typical with the received M. If the index along with the corresponding bin index of the selected codeword, are identical to those of the decoded codeword, the wireless terminal reports that the measurement being sent (billing) is correct. Otherwise, a warning concerning the non-integrity of the billing will be flagged.

The advantage of the proposed integrity verification scheme over the Slepian-Wolf scheme proposed in [1] is two-fold. First, Slepian-Wolf scheme reports the non-integrity of the billing only when the reported measurement from the power utility Y is statistically independent of the redundant meter measurement X. However, this condition does not have to hold in practice, as the power utility can still report a measurement Y which is compatible with the measurement sent by the redundant meter X, while X and Y being mutually independent. Thus, our coding scheme being independent of the statistical dependence between X and Y, offers more flexibility. Second, the existing scheme only allows a secure transmission rate between $H(X|Y)$ and $H(X)$, while our scheme only requires a minimum transmission rate of $H(X)$, i.e., we can securely transmit the measurements at a higher rate.

C. Implementation

To implement the coding scheme proposed in this paper, we propose an approach inspired by the coset decoding in linear block codes. In particular, we randomly generate a codebook of 2^n codewords. Then, randomly partition the codebook into 2^k bins, where $k < n$. Here, each bin is referred to as a coset. Note that codewords in the same coset have identical syndromes.

The redundant meter measurement is converted into a bit sequence through a quantization scheme. Assume that each measurement sample is converted to q bits, then $n = lq$ is the number of bits for a group of l measurement samples. Note that the shared secret key consists of k bits. After computing the syndrome of the n-bit codeword representing the measurement, the redundant meter is now able to identify the codeword index and the corresponding bin index of the codeword.

D. Illustrative Example

To elucidate the basic approach we consider a practical low-order example. After measurement quantization and mapping the resulting samples into a bit sequence, we must construct a codebook that is used at the redundant meter and the wireless terminal. For instance, we demonstrate the implementation of a linear block code-based scheme. Here, we consider an $(5, 2)$ code [9] with the generator matrix $\mathbf{G}$ and the parity check matrix $\mathbf{H}$ given as follows

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix},$$

and

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Now we generate 32 codewords v and partition them into 8 bins. All codewords in the same bin have an identical syndrome s given by $s = v\mathbf{H}^t$.

The codebook is illustrated in the following table.

Codewords				Syndrome
00000	10111	01101	11010	000
00001	10110	01100	11011	001
00010	10101	01111	11000	010
00100	**10011**	01001	11110	**100**
01000	11111	00101	10010	101
10000	00111	11101	01010	111
00011	10100	01110	11001	011
00110	10001	01011	11100	110

In this example, each coset has four elements whose indices can be denoted by 00, 01, 10, and 11, respectively. Assume that the codeword 10011 is chosen to represent the measurement; the redundant meter may send a message consisting of the codeword index and the encrypted syndrome, i.e., $m = [01|100 \oplus K]$, where K is a secret key of 3 bits and $\oplus$ is the mod-2 sum. By using the secret key K, the wireless terminal can easily decode the received message and recover the redundant meter measurement. On the other hand, the eavesdropper only knows the codeword index 01 and has to guess to understand which coset can be the most possible one. Fortunately, since all codewords are equally probable, the eavesdropper still has the maximum uncertainty about the transmitted message.

The integrity verification can also be performed easily. After quantizing the reported measurement Y and mapping the samples into bit sequence, the wireless terminal can construct a checking message in the same way that the redundant meter generates the coded message M. It, then, compares the newly constructed message with the decoded message received from the redundant meter. If the newly constructed message is not $[01|100 \oplus K]$ in this example, the integrity invalidation is reported.

E. Encoder Algorithm

The block diagram for the encoder is illustrated in Fig. 3. The encoder in the redundant meter works as follows:

1) Quantize the redundant measurement
2) Map the quantized measurement into a bit sequence
3) Partition the bit sequence into blocks of n bits
4) For each block, conduct the following steps:
   a) Find the codeword index I_C from the lookup table
   b) Calculate the syndrome S
   c) Encrypt S using the secret key, K, as $I_S = S \oplus K$
   d) Using parallel-to-serial block, combine I_C and I_S into message M as $M = [I_C \quad I_S]$
   e) Transmit M over the wireless channel

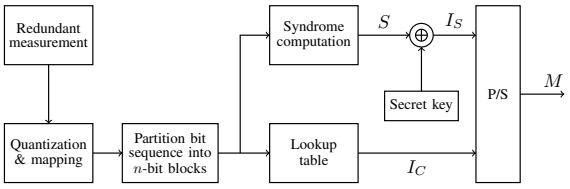

Figure 3. Encoder block diagram

F. Decoder Algorithm

The block diagram of the decoder is shown in Fig. 4. The decoder in the wireless terminal works as follows:

1) Quantize the reported measurement Y, map into bits, and partition into blocks of n bits
2) For each received coded message $\hat{M}$, conduct the following steps:
   a) Using serial-to-parallel block, separate $\hat{M}$ into $\hat{I}_S$ and $\hat{I}_C$
   b) Using the secret key, K, decrypt $\hat{I}_S$ into $\hat{S}$
   c) Using the lookup table, find the bit sequence that best matches $\hat{S}$ and $\hat{I}_C$
   d) Compare the decoded bit sequence with the corresponding bit sequence of Y: if not equal, abort the process; the reported measurement is not equal to the redundant measurement. Otherwise, continue to the next block of $\hat{M}$
3) If all bit blocks are equal, the reported measurement is equal to the redundant measurement

It is assumed that in order for this setup to work, the secret key K, which might change for each block of bits, has to be perfectly known at the encoder and decoder. A secure medium to share the key between the encoder and decoder is assumed as well.

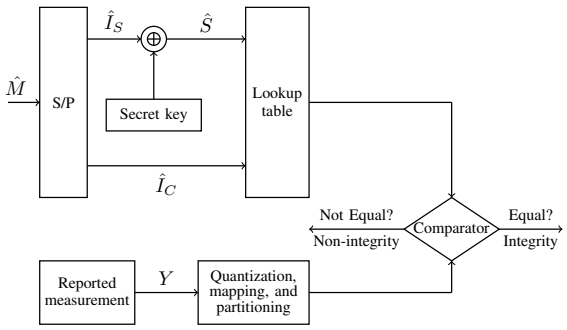

Figure 4. Decoder block diagram

IV. Conclusions

Redundant metering is an approach to verify the integrity of smart meter billing. The smart meter measures the power usage and sends the reading to the utility company, which relays that reading back to a wireless terminal that belongs to the customer. A redundant meter measures the power usage and transmits its reading wirelessly to the wireless terminal. In this way the customer can check the integrity of the power consumption measurements acquired by the utility's smart meter. A confidentiality vulnerability is imminent as an eavesdropper can access the wirelessly transmitted redundant measurement and figure out the customer power usage.

Inspired by the works of [7] and [8], we adopted a rate distortion approach to encode/decode the redundant meter measurements in order to achieve confidentiality. Through the use of a positive-rate secret key, a distortion is induced on the eavesdropper preventing him/her from decoding the transmitted message. This minimum distortion represents a security measure in such a setting. For practical implementations, we proposed a coding scheme inspired by the coset decoding in linear block codes. Future work involves implementation and application of the coding scheme to real metering data.

References

[1] D. P. Varodayan and G. X. Gao, "Redundant Metering for Integrity with Information- Theoretic Confidentiality," *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct. 2010.

[2] Greentech Media, "PG&E Sued Over Smart Meters, Slows Down Bakersfield Deployment," GreenTechMedia, Nov. 11, 2009. http://www.greentechmedia.com/articles/read/pge-sued-over-smart-meters-slows-down-bakersfield-deployment.

[3] San Jose Mercury News, "PG&E Details Technical Problems with SmartMeters," The Utility Reform Network, Apr. 26, 2010. http://www.turn.org/article.php?id=1194.

[4] KGO-TV, "Experiment Raises Questions About SmartMeters, May 05, 2010. http://abclocal.go.com/kgo/story?section=news/7 on your side&id=7424533.

[5] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell Systems Technical Journal*, vol. 28, pp. 656–715, Oct. 1949.

[6] D. Slepian and J. K. Wolf, "Noiseless Coding of Correlated Information Sources," *IEEE Transactions on Information Theory*, vol. 19, no. 4, pp. 471–480, Jul. 1973.

[7] H. Yamamoto, "Rate-Distortion Theory for the Shannon Cipher System," *IEEE Transactions on Information Theory*, vol. 43, no. 3, pp. 827–835, May 1997.

[8] P. Cuff, "A Framework for Partial Secrecy," *IEEE Global Telecommunications Conference (GLOBECOM)*, Dec. 2010.

[9] R. E. Blahut, *Algebraic Codes for Data Transmission*, 2nd edition, Cambridge University Press, 2002.