Compressive Sensing based Physical Layer Authentication for Wireless Energy Auditing Networks

Yonggu Lee, Hanseong Jo, Jinho Choi
School of Electrical Engineering and Computer Science
Gwangju Institute of Science and Technology (GIST), Korea
Email: {yglee1096, kaiser825, jchoi0114}@gist.ac.kr

***Abstract*—In this paper, we study joint physical layer compression and authentication based on compressive sensing (CS) for multicarrier transmissions in wireless energy auditing networks. For real-time power signal transmissions, we consider transmissions for compressed power signals by using the notion of CS without an analog-to-digital conversion in a multicarrier system. In addition, the notion of CS is exploited to distinguish between a legitimate power signal and a intrusion power signal. Through simulation results with a data set of power consumptions, we can see that the power signals can be differentiated by using a hypothesis testing based on empirical distributions for power of residual errors.**

***Index Terms*—Authentication, compressive sensing, signal compression, wireless energy auditing networks**

I. Introduction

Wireless energy auditing networks (WEAN) consisting of power meters and an access point (AP) provide basic services such as demand response, usage disaggregation and power quality monitoring in smart grid [1], [2]. However, there are a number of challenges in WEAN caused by the limited abilities of the power meters (e.g., low battery, limited computing power). Especially, assuming the presence of active malicious power meters which perform intelligent attacks (e.g., impersonation attack, jamming attack), WEAN become vulnerable to the attacks due to the nature of wireless broadcast [3]. It may cause serious economic loss and instability of the power system by manipulating power signals.

High sampling rates of the power signals make an accurate power analysis for appliances by capturing more characteristics of power signals in WEAN. However, high sampling rates induce a burden of increasing computational complexity and transmission power for the power meter which has limitations of hardware resources. To solve the problem, compression techniques for power signals have been extensively studied in smart grid [4]–[6]. Wavelet transform methods can be used to compress power signals in smart grid [4]. In [5], a compression technique based on high-order delta modulation is proposed. In addition, compressive sensing (CS) has been considered for the compression of power signals in [6]. In this paper, we also use the notion of CS to compress power signals.

In smart grid, authentication techniques have been studied mostly in network and application layers [7], [8]. But there are some challenges for the authentication such as key management, high complexity and so on. To address the challenges, physical layer authentication methods which are based on the exploitation of the dynamic physical characteristics (e.g., channel, analog front-end (AFE)) have been considered. Channel based physical layer authentication [9] uses the time-variant channel state information (CSI) which makes a receiver differentiate the received signals. The hardware imperfection of AFE which causes input and output (I/O) imbalance, phase offset error, carrier frequency offset error can be used for the physical layer authentication [10]. However, if the characteristics of AFE and channel for an intrusion node are close to those of a legitimate transmitter, the authentication techniques may result in relatively poor authentication performance. In [11], a tag signal is concurrently transmitted for a stealth authentication with a message signal.

In this paper, we present a new physical layer authentication method using CS in WEAN. It enables a power signal to be compressed and authenticated simultaneously. As mentioned in [6], a power signal can be compressed by the notion of CS. Then, we can directly transmit the compressed power signals without an analog-to-digital conversion in a multicarrier system. It simplifies the procedures for the power signal transmission and reduces a burden of the signal processing of the power meter. Then, at an AP which collects the power data from the power meter, the power signal can be authenticated in physical layer under the assumption that an authentication matrix is shared between the legitimate meter and the AP as a secret key. It means that the AP can discard a intrusion signal in physical layer directly without upper layer processing, which can effectively reduce the burden of network due to unnecessary traffics caused by intrusion meters. A data set of real-time power consumptions [12] for electrical appliances is used for simulations. Through simulation results, we can see that it is possible to authenticate the power signals in the physical layer by using hypothesis testing with empirical distributions at the AP.

Notation: Upper-case and lower-case boldface letters are used for matrices and vectors, respectively. $\mathbf{A}^{\mathrm{H}}$ and $\mathbf{A}^{\mathrm{T}}$ denote the Hermitian and transpose of $\mathbf{A}$, respectively. The p-norm of a vector $\mathbf{a}$ is denoted by $\|\mathbf{a}\|_p$ (If $p = 2$, the norm is denoted by $\|\mathbf{a}\|$ without the subscript). $\mathcal{CN}(\mathbf{a}, \mathbf{R})$

represents the distribution of circularly symmetric complex Gaussian (CSCG) random vectors with mean vector $\mathbf{a}$ and covariance matrix $\mathbf{R}$.

II. System Model

In this section, we consider a power metering system consisting of an AP, which is connected to a data concentrator unit (DCU) and multiple power meters. Among power meters, it is assumed that some power meters are used for intrusion, which are called intrusion meters, as shown in Fig. 1. For simplicity, we only consider one legitimate meter and one intrusion meter in this paper.

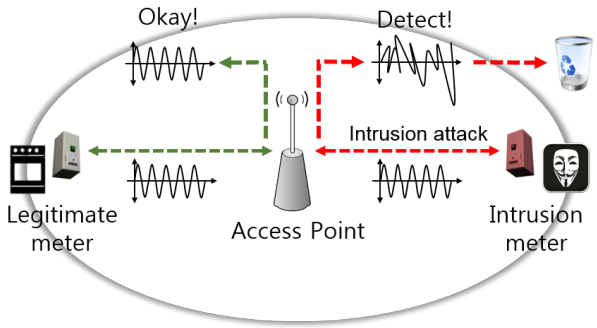

Fig. 1. System model for CS based authentication in WEAN

We consider a multicarrier system for transmissions from the legitimate meter to the AP with L subcarriers. Throughout the paper, the legitimate meter sends a block of signal denoted by $\mathbf{x}_B \in \mathbb{C}^{L\times 1}$ over L subcarriers, where $\mathbf{x}_B$ contains a message of meter reading. Furthermore, the intrusion meter also transmits a forged signal denoted by $\mathbf{x}_E \in \mathbb{C}^{L\times 1}$ over L subcarriers with the aim of impersonating the legitimate meter. Then, the received signals from the legitimate meter and the intrusion meter, respectively, are given by

$$\mathbf{y} = \mathbf{H}\mathbf{x}_B + \mathbf{n} \tag{1}$$

and

$$\mathbf{z} = \mathbf{G}\mathbf{x}_E + \mathbf{e}, \tag{2}$$

where $\mathbf{n} \sim \mathcal{CN}(0, \sigma_n^2\mathbf{I})$ and $\mathbf{e} \sim \mathcal{CN}(0, \sigma_e^2\mathbf{I})$ are the background noise terms associated with the legitimate signal and the intrusion signal, respectively. We assume that each signal is separately (in time or frequency) received at the AP. In addition, $\mathbf{H} = diag(H_0, ..., H_{L-1})$ and $\mathbf{G} = diag(G_0, ..., G_{L-1})$ are the diagonal channel matrices from the legitimate meter and the intrusion meter to the AP, respectively. Here, H_l and G_l are the l-th frequency-domain channel coefficients, which are assumed to be circularly symmetric complex Gaussian (CSCG) variables with $H_l \sim \mathcal{CN}(0, \sigma_h^2)$ and $G_l \sim \mathcal{CN}(0, \sigma_g^2)$.

III. CS based Joint Compression and Authentication

In this section, we consider a joint compression and authentication scheme using CS in WEAN.

A. Compression of Power Signal

To apply the notion of CS to the compression of power signals, power signals which are measured by power meters should be sparse. If the power signal can be transformed to a sparse signal, the power meter can compress the power signal by using the notion of CS without complex signal processing. Thus, it is possible to transmit real-time power signals with a simplified transmission scheme by using the CS based compression.

For the sparse transform, we need to know the characteristics of power signals. For each electrical appliance (e.g., computer, refrigerator and water heater), the power signals may have different characteristics. The power signals can be classified into five categories: *duty-cycled*, *periodic*, *fluctuating*, *spiky*, and *silent* [6]. The most home appliances which have duty cycle operations (e.g., water heater, hair dryer, washing machine) belong to the $duty-cycled$ group. The power consumptions of a CD-player and projector have periodic characteristic. Computers generate $fluctuating$ power consumption patterns. The $spiky$ group contains a server which causes a bursty workload. Finally, the ceil lights and lamps are classified into the $silent$ group.

To obtain high sparsity, we have to design a proper representation matrix for power signals. A power signal can be represented by

$$\mathbf{p} = \mathbf{\Psi}\mathbf{s}, \tag{3}$$

where $\mathbf{\Psi}$ is a representation matrix. Here, $\mathbf{s}$ contains Q large coefficients and $N-Q$ small coefficients which are close to zero. For tractable analysis, a common approach is to approximate $\mathbf{s}$ by $\mathbf{s}_{(Q)}$ which is obtained by setting the $N-Q$ small coefficients to zero. There exists a trade-off between sparsity and the accuracy of approximation. In this paper, Q is the minimum q subject to the energy of $\mathbf{s}_{(q)}$ contains more than $\epsilon(\%)$ of energy of $\mathbf{s}$ (i.e., $\|\mathbf{s}_{(q)}\|^2 \geq \epsilon\|\mathbf{s}\|^2$), where ϵ is a certain threshold.

In [6], the authors studied to find $\mathbf{\Psi}$ that is the best in terms of the sparsity, according to the characteristics of the power signals. Through the empirical experiments, [6] showed that the discrete cosine transform (DCT) [13] can efficiently compress power signals in $periodic$ group. In addition, the adjacent difference transform (ADT) [14] is suitable to power signals with duty-cycled property. Haar wavelet transform (HWT) [15] is the best default basis without prior knowledge of the signal structure of power readings. In this paper, we use a data set of real-time power consumptions and HWT known as a best representation matrix in [6] for the transformation.

B. CS based Physical Layer Authentication

This section presents a CS based physical layer authentication in WEAN. As mentioned in Subsection III.A, power signals can be transformed to sparse signals with HWT. It means that the power signals can be compressed by the notion of CS. For the CS based authentication, we design an authentication matrix, $\mathbf{\Phi}$ which has to be shared between the legitimate meter and the AP as a secret key for the authentication. The authentication matrix is unknown to the intrusion meter, while the representation matrix, $\mathbf{\Psi}$, is known. Throughout the paper, we consider a Gaussian matrix whose element is drawn from the complex Gaussian distribution, as the authentication matrix. Then, the received signals from the legitimate meter and the intrusion meter at the AP, respectively, are given by

$$\mathbf{y} = \mathbf{H}\mathbf{\Phi}_B\mathbf{\Psi}\mathbf{s}_B + \mathbf{n} \tag{4}$$

and

$$\mathbf{z} = \mathbf{G}\mathbf{\Phi}_E\mathbf{\Psi}\mathbf{s}_E + \mathbf{e}, \tag{5}$$

where $\mathbf{\Phi}_B$, $\mathbf{\Phi}_E \in \mathbb{C}^{L\times N}$ are the authentication matrices for the legitimate meter and the intrusion meter, respectively. As mentioned earilier, the elements of the matrices follow a Gaussian distribution, $\mathcal{CN}(0, \frac{1}{L})$. Meanwhile, the AP should know the channels to detect the transmitted signals. To this end, the power meters transmit pilot signals before the power signals. Throughout the paper, we assume the channels for the legitimate meter and the intrusion meter are perfectly estimated. Then, for the CS recovery, the measurement matrix for the legitimate signal becomes $\mathbf{\Theta}_B = \mathbf{H}\mathbf{\Phi}_B\mathbf{\Psi}$. On the other hands, the measurement matrix for the intrusion signal is $\mathbf{\Theta}_E = \mathbf{G}\mathbf{\Phi}_B\mathbf{\Psi}$ which is different from that of the intrusion signal. Noting that $\mathbf{s}_B$ and $\mathbf{s}_E$ are Q-sparse signals with $N \times 1$ size, we use the orthogonal matching pursuit (OMP) algorithm [16] which is a low-complexity greedy algorithm for the CS recovery. In most CS recovery algorithms, the sufficient number of measurements is an important parameter for the successful recovery. At a high SNR, the required number of measurements, L, for the successful recovery is bounded as follows:

$$L \geq CQ\ln\left(\frac{N}{\delta}\right), \tag{6}$$

where C is a constant and $\delta \in (0, 0.36)$ [16]. Then, OMP can reconstruct the signal with probability exceeding $1-\delta$.

For the CS based authentication, the power of residual error plays a crucial role in distinguishing whether the received signal is the legitimate signal or the intrusion signal. So, we have to know the probability density functions of the power of residual error for the legitimate and intrusion signals for a decision rule. Let $\alpha = \| \mathbf{r} \|^2$ denote the power of residual error for the received signal, where $\mathbf{r}$ is a residual error vector. The authentication is cast as a binary hypothesis testing problem. Then, the decision rule using the maximum a posterior probability (MAP) is given by

$$P(\mathcal{H}_1|\alpha) \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} P(\mathcal{H}_0|\alpha), \tag{7}$$

where $\mathcal{H}_1$ is the hypothesis that the signal is the legitimate signal and $\mathcal{H}_0$ is the other hypothesis that the signal is the intrusion signal. After Q iterations in the OMP algorithm, the powers of the residual errors for the legitimate and intrusion signals, respectively, are given by

$$\alpha_B = \|\mathbf{y} - \hat{\mathbf{\Theta}}_B\hat{\mathbf{s}}_B\|^2, \tag{8}$$

$$\alpha_E = \|\mathbf{z} - \hat{\mathbf{\Theta}}_E\hat{\mathbf{s}}_E\|^2, \tag{9}$$

where $\hat{\mathbf{s}}_B = (\hat{\mathbf{\Theta}}_B^{\mathrm{H}}\hat{\mathbf{\Theta}}_B)^{-1}\hat{\mathbf{\Theta}}_B^{\mathrm{H}}\mathbf{y}$ and $\hat{\mathbf{s}}_E = (\hat{\mathbf{\Theta}}_E^{\mathrm{H}}\hat{\mathbf{\Theta}}_E)^{-1}\hat{\mathbf{\Theta}}_E^{\mathrm{H}}\mathbf{z}$. At the AP, for the authentication, $\alpha \in \{\alpha_B, \alpha_E\}$ becomes the test statistics, in (7), which is obtained from the received signals in the physical layer. Thus, the authentication can be performed in the physical layer. In this paper, we draw empirical probability density functions of the power of residual error for the power signals through the empirical simulation. The empirical distributions are used for the hypothesis testing in order to see the performance of the proposed CS based authentication scheme.

IV. Simulation Results

In this section, we present simulation results for the proposed authentication scheme with the real-time power consumption data. For simulations, we assume $N = 128$, $\sigma_h^2 = \sigma_g^2 = 1$ and $\epsilon = 99\%$. As we mentioned earlier, $Q = \min q$ subject to $\|\mathbf{s}_{(q)}\|^2 \geq \epsilon\|\mathbf{s}\|^2$. So, according to a data set of power consumptions, the sparsity becomes different.

Fig. 2 shows the simulation results for the empirical probability density functions of the power of residual errors for the legitimate power signal and the intrusion power signal, when $L = 64$ and SNR $= 20$dB. We can find that the distribution of the legitimate signal is different from the distribution of the intrusion signal. It means that if we set a proper threshold for the hypothesis testing, we can detect the intrusion signal with a high probability. Because the authentication matrix (i.e., key of the authentication) is unknown to the intrusion meter, the power of the residual error is relatively high than that of the legitimate meter. In summary, the empirical results of Fig. 2 demonstrate that it is possible to apply the hypothesis testing to the proposed authentication scheme using the notion of CS.

In Fig. 3, we show the simulation results of the authentication error probability which is the probability of an incorrect authentication decision over SNR. For the simulation, we collected a data set of power consumption of the computer for 10 hours with a smart plug. From the data, we obtain a threshold for the hypothesis testing by using the empirical distributions. In this figure, we can find that as the SNR decreases, the authentication error probability also decreases. If the SNR is close to 0dB, the authentication error probability approaches to 0.5. It means that if the SNR is 0dB, the

distribution of power of the residual error for the legitimate signal is almost equal to that of the intrusion signal.

Fig. 4 depicts the authentication error probability for the number of subcarriers when SNR $= 20$dB. In the simulation, we use a data set of power consumptions for several appliances which have different characteristics (television: $fluctuating$, washing machine: $duty-cycled$, projector: $periodic$) [12]. The figure shows that as the number of subcarriers increases, the authentication error probability decreases. As shown in (6), the sufficient number of measurements are required to perfectly recover the signal. It means that under the high CS recovery condition, the proposed CS based authentication scheme has a good performance because the residual error for the legitimate signal is distinguished from that of the intrusion signal with a good signal reconstruction performance.

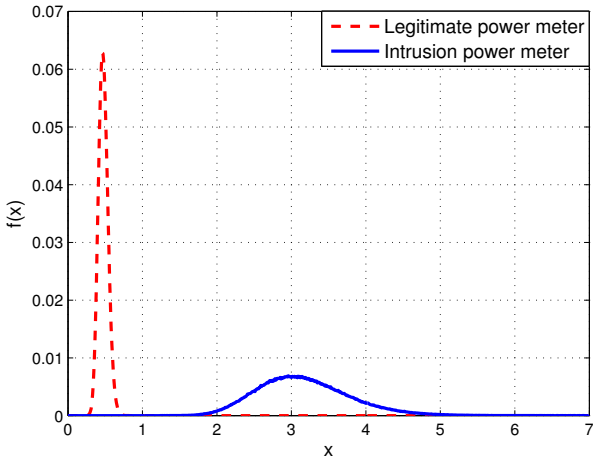

Fig. 2. Comparison of the empirical probability density functions between the legitimate meter and the intrusion meter, where $L = 64$ and SNR $= 20$dB

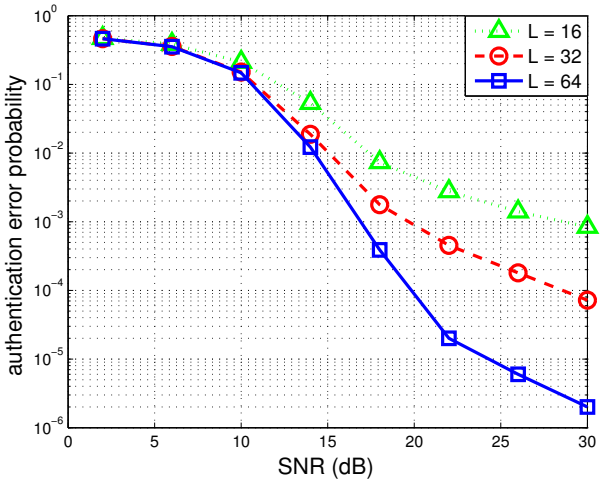

Fig. 3. Authentication error probability for SNRs with various L

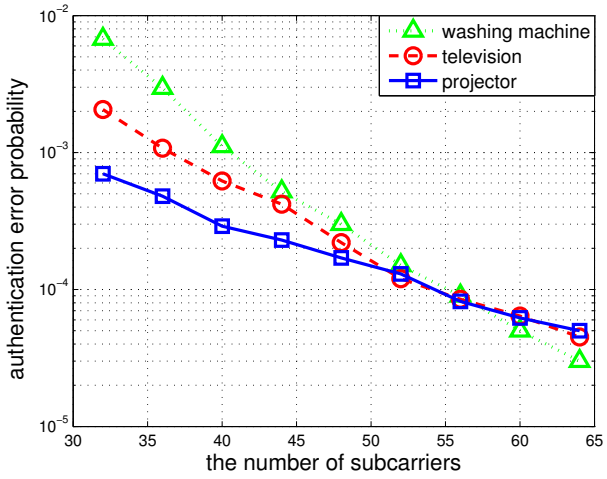

Fig. 4. Authentication error probability for the number of subcarriers, L, where SNR $= 20$dB

V. Conclusion

In this paper, we introduced a CS based physical layer authentication scheme in WEAN. We considered a multicarrier system for transmissions from a power meter to an AP. Based on the sparse signal which is transformed from the power signal, the CS based joint compression and authentication scheme in physical layer was applied to WEAN. Through simulation results, we found that it is possible to discriminate the intrusion signal from the received signal by using hypothesis testing with empirical distributions for power of residual errors.

Acknowledgment

This work was supported by Agency for Defense Development (the title of the project is PHY/MAC-NETWORK Technologies Against Jamming Attack and Eavesdropping).

References

[1] X. Jiang, M. Van Ly, J. Taneja, P. Dutta, and D. Culler, "Experiences with a high-fidelity wireless building energy auditing network," in *Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems*, pp. 113–126, ACM, 2009.

[2] X. Jiang, S. Dawson-Haggerty, P. Dutta, and D. Culler, "Design and implementation of a high-fidelity ac metering network," in *Information Processing in Sensor Networks, 2009. IPSN 2009. International Conference on*, pp. 253–264, IEEE, 2009.

[3] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security & Privacy*, vol. 7, no. 3, 2009.

[4] J. Ning, J. Wang, W. Gao, and C. Liu, "A wavelet-based data compression technique for smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 1, pp. 212–218, 2011.

[5] D. Zhang, Y. Bi, and J. Zhao, "A new data compression algorithm for power quality online monitoring," in *Sustainable Power Generation and Supply, 2009. SUPERGEN'09. International Conference on*, pp. 1–4, IEEE, 2009.

[6] S.-Y. Chiu, H. H. Nguyen, R. Tan, D. K. Yau, and D. Jung, "JICE: Joint data compression and encryption for wireless energy auditing networks," in *Sensing, Communication, and Networking (SECON), 2015 12th Annual IEEE International Conference on*, pp. 453–461, IEEE, 2015.

[7] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. S. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 675–685, 2011.

[8] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, "An efficient merkle-tree-based authentication scheme for smart grid," *IEEE Systems Journal*, vol. 8, no. 2, pp. 655–663, 2014.

[9] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Transactions on Wireless Communications*, vol. 7, no. 7, 2008.

[10] W. Hou, X. Wang, J.-Y. Chouinard, and A. Refaey, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," *IEEE Transactions on Communications*, vol. 62, no. 5, pp. 1658–1667, 2014.

[11] L. Y. Paul, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 38–51, 2008.

[12] A. Reinhardt, P. Baumann, D. Burgstahler, M. Hollick, H. Chonov, M. Werner, and R. Steinmetz, "On the accuracy of appliance identification based on distributed load metering data," in *Sustainable Internet and ICT for Sustainability (SustainIT), 2012*, pp. 1–9, IEEE, 2012.

[13] N. Ahmed, T. Natarajan, and K. R. Rao, "Discrete cosine transform," *IEEE transactions on Computers*, vol. 100, no. 1, pp. 90–93, 1974.

[14] X. Wu and M. Liu, "In-situ soil moisture sensing: measurement scheduling and estimation using compressive sensing," in *Proceedings of the 11th international conference on Information Processing in Sensor Networks*, pp. 1–12, ACM, 2012.

[15] R. S. Stanković and B. J. Falkowski, "The haar wavelet transform: its status and achievements," *Computers & Electrical Engineering*, vol. 29, no. 1, pp. 25–44, 2003.

[16] J. A. Tropp and A. C. Gilbert, "Signal recovery from random measurements via orthogonal matching pursuit," *IEEE Transactions on information theory*, vol. 53, no. 12, pp. 4655–4666, 2007.