2016 IEEE International Conference on Smart Grid Communications (SmartGridComm): Communications, Networks and Architectures to Enable the Smart Grid

Secure Compressive Random Access for Meter Reading in Smart Grid using Multi-Antenna Access Point

Jinho Choi, Kyungjun Lee, Yonggu Lee, and Nam Yul Yu
School of Electrical Engineering and Computer Science
Gwangju Institute of Science and Technology (GIST)
e-mail: {jchoi0114, leekj9001, yglee1096, nyyu}@gist.ac.kr

***Abstract*—In this paper, we study the advantages of multiple antennas at an access point (AP) for random access by smart meters in smart utility network (SUN) in terms of access delay and security. For random access with the capability of multiple signal recovery, we consider compressive random access and show that multiple antennas can help improve the access delay. In addition, we consider updating keys to generate spreading codes at smart meters using a physical layer security scheme that is available when the AP is equipped with multiple antennas. We show that the probability of successful attack by an eavesdropper can be low by updating keys. Consequently, in this paper, we demonstrate that multiple antennas at the AP in SUN is indispensable for random access with a low latency and security.**

***Index Terms*—smart meter; compressive sensing; security; smart grid**

I. Introduction

Smart grid is an intelligent power grid that includes sensing and communication technologies [1], [2]. While smart grid can offer efficient energy management based on sensing and communication technologies, there are various challenging issues including security issues [3], [4]. In particular, wireless communications for smart meters within smart utility networks (SUN) [5] not only need to support massive connections for a number of smart meters over fading, but also overcome security vulnerabilities due to broadcast nature.

In [6], [7], a multiple access approach to send meter readings from smart meters to an access point (AP), which is also a data concentrator unit (DCU) in smart grid, is proposed. In this approach, the AP can detect signals from multiple active smart meters based on the notion of compressive sensing (CS) [8], [9], which can exploit the sparsity of active smart meters. There are also similar random access approaches in [10], [11] which can exploit the sparsity of active transmitters to detect multiple signals using low-complexity algorithms such as the orthogonal matching pursuit (OMP) algorithm [12].

Note that for random access, each smart meter is to have a unique spreading code, which results in a code division multiple access (CDMA) system. In [13], CDMA based communications for smart grid are considered. Thus, the approach in [6] would be a reasonable choice for smart grid. Furthermore, as shown in [6], compressive random access can provide a shorter delay than other random multiple access schemes (e.g., carrier sensing multiple access (CSMA)). However, if the signals transmitted by some smart meters experience severe fading, those signals cannot be recovered by low-complexity CS algorithms, which results in a long access delay. According to [14], the required latency of meter reading is up to 15 seconds. In [2], however, the required latency can drop to 250 – 300 ms for critical and priority readings. As more frequent readings and data transmissions are required from a number of smart meters in the future, we can expect that the required latency can be shorter. Thus, a long access delay in compressive random access for SUN due to fading would be undesirable.

In [6], the encryption based on CS is also considered, which is similar to that in [15]. In [15], it is shown that CS based encryption can be computationally secure if a measurement matrix is generated by a key of long length (with each key, a unique measurement matrix is to be generated). For example, if each smart meter has a unique spreading sequence that can be generated by a key of length 20 bits, then there would be up to 2^{20} possible keys per smart meter. Thus, if there are 100 smart meters, there might be 2^{2000} combinations for keys in total. However, since there could be a few active smart meters at a time, the eavesdropper can take advantage of this in finding the keys of a small group of active smart meters with a relatively low computational complexity. Consequently, the encryption in compressive random access as in [6] may not be sufficiently secure in terms of computational secrecy. In order to overcome this shortcoming, it may be necessary to update keys to generate spreading codes frequently if possible.

In this paper, we consider an AP equipped with an array of multiple antennas and demonstrate that the array can play a crucial role in improving the reliability of multiple access over fading channels as well as security for transmissions from smart meters to the AP. Due to the improvement of the reliability of multiple access, smart meters can have a

This research was supported by Korea Electric Power Corporation through Korea Electrical Engineering & Science Research Institute. (grant number : R15XA03-60). and the GIST Research Institute (GRI) in 2016.

978-1-5090-4075-9/16/$31.00 ©2016 IEEE

shorter access delay over fading channels, which is important in smart grid where meter reading should be timely updated to avoid any instability of smart grid due to a long delay of load report. We also show that the security of compressive random access can be significantly improved by frequent updating of keys to generate spreading codes. To securely update keys, physical layer security [16] based on an antenna array at the AP is considered. From analysis and simulation results, we can demonstrate that multiple antennas should be considered for an AP in SUN not only to shorten the access delay, but also to improve the security for communications from smart meters.

Notation: Matrices and vectors are denoted by upper- and lower-case boldface letters, respectively. The superscripts T and H denote the transpose and complex conjugate, 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). The superscript † denotes the pseudo-inverse. $\mathbb{E}[\cdot]$ and $\mathrm{Var}(\cdot)$ denote the statistical expectation and variance, respectively. $\mathcal{CN}(\mathbf{a}, \mathbf{R})$ ($\mathcal{N}(\mathbf{a}, \mathbf{R})$) represents the distribution of circularly symmetric complex Gaussian (CSCG) (resp., real-valued Gaussian) random vectors with mean vector $\mathbf{a}$ and covariance matrix $\mathbf{R}$.

II. System Model

Suppose that there are K smart meters and one AP, which is also a DCU in SUN as illustrated in Fig. 1. Thus, we refer to AP as AP/DCU. Throughout the paper, we assume that the AP/DCU is equipped with N antennas. As in [6], we assume that each smart meter has a unique spreading code, which is denoted by $\{c_k(l)\}$ for smart meter k. Each spreading code is generated by a pseudo-random sequence generator with a key. At each time slot, a few active smart antennas transmit signals to the AP/DCU.

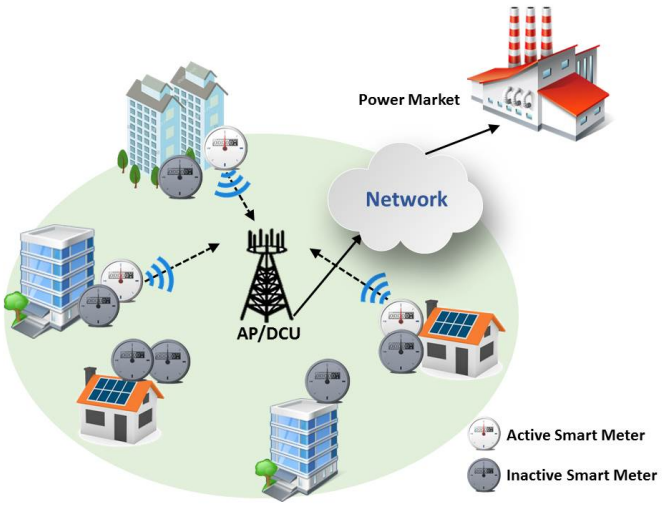

Fig. 1. An illustration of a wireless system with one AP/DCU and multiple smart meters.

Throughout the paper, we assume time division duplexing (TDD). For random access, we assume a frame that consists of two phases. In the first phase, the AP/DCU send a pilot signal to allow active smart meters to synchronize their transmissions. In the second phase, active smart meters send their signals to the AP/DCU. For convenience, the index of the mth active smart meter is denoted by $k(m)$. Suppose that there are M active smart meters. Denote by $h_{k,i;t}$ the channel coefficient from smart meter k to the ith antenna at AP/DCU and by $s_{k;t}$ the tth data symbol transmitted by smart meter k over time slot t. Then, the received signal vector at the AP/DCU through the ith antenna is given by

$$\mathbf{r}_{i;t} = \sum_{m=1}^{M} \mathbf{c}_{k(m);t} h_{k(m),i;t} s_{k(m);t} + \mathbf{n}_{i;t} = \mathbf{C}_t \mathbf{x}_{i;t} + \mathbf{n}_{i;t}, \tag{1}$$

where $\mathbf{x}_i$ is a M-sparse signal vector, $\mathbf{n}_i \sim \mathcal{CN}(0, N_0\mathbf{I})$ is the noise vector at antenna i, and $\mathbf{C}_t$ is the measurement matrix during time slot t, which is $\mathbf{C}_t = [\mathbf{c}_{1;t} \ \ldots \ \mathbf{c}_{K;t}]$. Here, $\mathbf{c}_{k;t} = [c_k((t-1)L+1) \ \ldots \ c_k(tL)]^{\mathrm{T}}$ is the spreading sequence of length L for the tth data symbol of smart meter k.

For secure transmissions, the spreading codes are assumed to be unknown to an eavesdropper, called Eve. However, Eve may attempt to estimate spreading codes. If spreading codes are based on pseudo-random sequences generated by a function of linear feedback shift registers (LFSRs), Eve can perform correlation attacks [17], [18] to find the initial vectors of LFSRs, which are regarded as keys. These attacks can be effective if the initial vectors are pre-stored and used without any updating. To mitigate such attacks, it is necessary to frequently update the initial vectors.

III. Signal Recovery with Multiple Antennas

In this section, we study signal recovery at the AP/DCU without knowing active smart meters using the notion of CS when multiple antennas are available at the AP/DCU. The approach is a generalization of that in [6] (where $N = 1$) and similar to that in [7]. However, unlike the approach in [7], we exploit the notion of multiple measurement vectors (MMVs) from multiple antennas to improve the delay performance. For convenience, we omit the time index t.

A. Signal Recovery with Multiple Antennas

In (1), the size of $\mathbf{C}$ is $L \times K$, where $L < K$ in general. To estimate $\mathbf{x}_i$ by solving the underdetermined problem, the signal recovery (of sparse signals) based on CS can be considered. Most CS algorithms can estimate $\mathbf{x}_i$ under certain conditions. In theory, $L = 2M$ measurements suffice to find a unique M-sparse vector $\mathbf{x}_i$ from the measurement $\mathbf{r}_i$. In practice, more measurements are required to estimate $\mathbf{x}_i$ by computationally tractable algorithms. Moreover, the magnitudes of the channel coefficients need to be sufficiently large for successful recovery in the presence of noise. However, the channel coefficients are random and their magnitudes can be small due to fading. To mitigate this problem, we can exploit the diversity gain from multiple antennas. Noting that the support sets of $\mathbf{x}_{i;t}$ are the same for all i, where $\mathbf{x}_i$'s are called *jointly sparse*, we can use a CS algorithm for MMVs [19] to exploit diversity gain. Precisely, if we define $\mathbf{R} = (\mathbf{r}_1 \cdots \mathbf{r}_N)$

and $\mathbf{X} = (\mathbf{x}_1 \cdots \mathbf{x}_N)$, the noiseless MMV problem $\mathbf{R} = \mathbf{C}\mathbf{X}$ can be solved by exploiting the jointly sparse structure of $\mathbf{X}$. In theory, if $\mathbf{C}$ has full spark and $\mathbf{X}$ has full rank, a unique solution can be found if and only if $M < \frac{\mathrm{spark}(\mathbf{C})-1+\mathrm{rank}(\mathbf{X})}{2}$ [19], where $\mathrm{spark}(\mathbf{C})$ is the smallest number of columns of $\mathbf{C}$ that are linearly dependent. Assuming that $\mathbf{C}$ has full spark, i.e., $\mathrm{spark}(\mathbf{C}) = L+1$, and $\mathbf{X}$ has full rank, a unique solution can be found from $\mathbf{R} = \mathbf{C}\mathbf{X}$ if and only if

$$M < \frac{L + \min(N, M)}{2} \tag{2}$$

In particular, if $N \geq M$, then $L \geq M+1$ measurements suffice to find unique channel estimates $\mathbf{x}_1, \cdots, \mathbf{x}_N$ from N antennas. Ideally, theoretical results imply that $L = M+1$ measurements and $N = M$ antennas are sufficient to guarantee unique recovery of $\mathbf{x}_i$'s in MMV settings with multiple antennas, which is a fundamental limit of the MMV approach. From the performance improvement by MMV, we can also show that the access delay is improved by multiple antennas.

B. Access Delay

In compressive random access, some smart meters may not be able to access the common channel if the AP/DCU cannot recover the transmitted signals from them. In this case, those smart meters[1] can perform fast retrials [20] in the next time slot.

We assume that each smart meter becomes active with access probability p_a that includes the re-transmission probability due to backlogged active smart meters from the previous slot. Then, M is a random variable with the following probability mass function:

$$\Pr(M = m) = \binom{K}{m} p_a^m (1 - p_a)^{K-m}.$$

In addition, denote by $P_k(M)$ the probability that smart meter k can successfully access the channel when M smart meters are active. Then, the probability that an active smart meter can access at the dth trial is given by

$$\Pr(D = d \,|\, M) = P_k(M)(1 - P_k(M))^{d-1}, \tag{3}$$

where D represents the number of retrials. With a stringent delay constraint for the transmissions from smart meters, we can consider the delay-outage probability as follows:

$$P_{\mathrm{out}}(D_{\max}) = \Pr(D \geq D_{\max} + 1), \tag{4}$$

where $D_{\max}$ denotes the maximum access delay or maximum number of retrials. From (3), we can show that

$$\begin{aligned} P_{\mathrm{out}}(D_{\max}) &= \mathbb{E}\left[\sum_{d=D_{\max}+1}^{\infty} P_k(M)(1 - P_k(M))^{d-1}\right] \\ &= \mathbb{E}\left[(1 - P_k(M))^{D_{\max}}\right] \\ &= \sum_{m=1}^{K} (1 - P_k(m))^{D_{\max}} \Pr(M = m). \end{aligned} \tag{5}$$

[1]At the end of each time slot, the AP/DCU broadcasts its recovery results so that the active smart meters can see whether or not their signals are successfully transmitted.

In CS, the probability of successful recovery can be bounded as

$$P_k(m) \geq \begin{cases} 1 - \epsilon, & \text{if } m \leq \bar{M}(\epsilon); \\ 0, & \text{if } m > \bar{M}(\epsilon), \end{cases} \tag{6}$$

where $\bar{M}(\epsilon)$ is the maximum sparsity that a CS algorithm can recover with a high probability, $1-\epsilon$. Finally, the delay-outage probability of (5) is bounded by

$$\begin{aligned} P_{\mathrm{out}}(D_{\max}) &\leq \epsilon^{D_{\max}} \Pr\left(1 \leq M \leq \bar{M}(\epsilon)\right) \\ &\quad + \Pr\left(M > \bar{M}(\epsilon)\right) \\ &= \epsilon^{D_{\max}} \sum_{m=1}^{\bar{M}(\epsilon)} \binom{K}{m} p_a^m (1 - p_a)^{K-m} \\ &\quad + \sum_{m=\bar{M}(\epsilon)+1}^{K} \binom{K}{m} p_a^m (1 - p_a)^{K-m}. \end{aligned} \tag{7}$$

With small ϵ, (7) implies that we need to have a sufficiently large $\bar{M}(\epsilon)$ to achieve low delay-outage probability. In particular, if we assume that $\mathbf{C}$ is full spark and $\mathbf{X}$ is full rank, we may set from (2)

$$\bar{M}(\epsilon) = \begin{cases} \left\lceil \frac{L+N}{2} \right\rceil - 1, & \text{if } N < \bar{M}(\epsilon), \\ L - 1, & \text{if } N \geq \bar{M}(\epsilon). \end{cases} \tag{8}$$

From this ideal case, it is obvious that having multiple antennas $N(\leq M)$ achieves the low delay-outage probability for a sufficient number of measurements L and high SNR.

IV. Secrecy Analysis

In this section, we address secrecy issues in compressive random access.

A. An Attack Model for Compressive Random Access

Suppose that there is an eavesdropper, called Eve, who wants to recover sparse signals from her received signals. To perform attacks, she needs to know the spreading codes used by smart meters or the measurement matrices, $\{\mathbf{C}_t\}$. In [15], it is shown that attacks to recover sparse signals without knowing the measurement matrix are computationally difficult. Thus, the signal compression using CS can be inherently secure (in terms of computational secrecy).

However, Eve may have sufficiently high computing power to perform attacks to find initial vectors of the spreading sequences of a certain target group of smart meters (in this attack, we assume that Eve knows the structure of the pseudo-random sequence generator used in smart meters, but not initial vectors). In particular, we may consider a known plain-text attack, where Eve knows the signals that are transmitted by the smart meters in a target group, but does not know their spreading codes (actually initial vectors). This kind of attack is possible if Eve can measure the power consumption of the smart meters in a target group. For convenience, the index set of the smart meters in this group is denoted by Ω.

Suppose that Eve is capable of suppressing the background noise and assume that $|\Omega| = M$. When all the smart meters in Ω become active, the received signal becomes

$$\mathbf{q}_t = \bar{\mathbf{C}}_t \mathbf{u}_t,$$

where $\mathbf{u}_t$ is the $M \times 1$ signal vector transmitted by the smart meters in Ω and $\bar{\mathbf{C}}_t$ represents the matrix consisting of M spreading codes of the smart meters in Ω used at time t. Eve needs to have some of pairs, $\{\mathbf{u}_t, \mathbf{q}_t\}$, for attacks to extract keys (e.g., correlation attacks if the pseudo-random sequence generator is a function of multiple LFSRs [17], [18]) to extract keys. We assume that Eve needs at least τ pairs of $\{\mathbf{u}_t, \mathbf{q}_t\}$ to carry out attacks with a reasonable size of Ω, M.

Note that τ depends on the structure and parameters of the pseudo-random sequence generator. For example, an LFSR is used, τ might be proportional to the period of the pseudo-random sequence, which depends on the order of the feedback polynomial of the LFSR.

B. Secret-Key Delivery to Smart Meters using ASM

In order to avoid the attack in Subsection IV-A, the keys or initial vectors of spreading sequences' generators can be frequently updated. To this end, it is essential to send new keys through secure transmission methods. It is important to note that the keys to generate spreading codes of inactive smart meters are not needed to be updated, while those of active smart meters are be updated as they could be estimated by Eve.

Note that in [21], making use of common random channels between a legitimate pair of transmitter and receiver is considered to extract secret keys for measurement matrices in CS based encryption. This approach can be employed to update a key of a smart meter. However, the key generation rate is limited by the variation of the channel. If the channel is static, it may not be possible to generate a key of a sufficiently long length. Thus, to mitigate this problem, we may consider the approaches in [22], [23] that require an antenna array. Those approaches can provide keys for both time-varying and time-invariant channels. In this subsection, we modify antenna subset modulation (ASM) in [23] to be used for communications over micro-wave[2] channels.

Suppose that the AP/DCU is to transmit signal, s, to a smart meter, which is called Bob, to update its key. Denote by $\mathbf{h}^{\mathrm{T}}$ and $\mathbf{g}^{\mathrm{T}}$ the channel vectors from the antenna array of the AP/DCU to Bob and Eve, respectively. We assume that the AP/DCU knows $\mathbf{h}$ (from the pilot signal transmitted by Bob). Then, the received signals at Bob and Eve, denoted by y_t and z_t, respectively, are given by

$$\begin{aligned} y_t &= \mathbf{h}^{\mathrm{T}}\mathbf{w}_t s + n_t \\ z_t &= \mathbf{g}^{\mathrm{T}}\mathbf{w}_t s + \bar{n}_t, \end{aligned} \tag{9}$$

where $\mathbf{w}_t$ is the beamforming vector and n_t and $\bar{n}_t$ are the zero-mean additive white Gaussian noise terms at Bob and Eve, respectively, at time t. For normalization purposes, we assume $\mathbb{E}[|n_t|^2] = \mathbb{E}[|\bar{n}_t|^2] = 1$. Unlike the channel vector in millimeter-wave channels [23], the elements of $\mathbf{h}$ are assumed to be independent random variables in micro-wave channels. In particular, for Rayleigh fading channels, the elements of $\mathbf{h}$ as well as $\mathbf{g}$ could be considered CSCG random variables. We assume that $h_l \sim \mathcal{CN}(0, \sigma_h^2)$ and $g_l \sim \mathcal{CN}(0, \sigma_g^2)$. Suppose that only few elements of $\mathbf{w}_t$, say V, are non-zero (the other elements are all zero) for ASM. Let $\mathcal{I}_t$ denote the index set of non-zero elements of $\mathbf{w}_t$ at time t. Then, it follows

$$\mathbf{h}^{\mathrm{T}}\mathbf{w}_t = \sum_{l \in \mathcal{I}_t} h_l w_l \text{ and } \mathbf{g}^{\mathrm{T}}\mathbf{w}_t = \sum_{l \in \mathcal{I}_t} g_l w_l.$$

Since the AP/DCU knows $\mathbf{h}$, it can decide $w_l \propto h_l^*$ or $w_l = \sqrt{\frac{P_{\mathrm{TX}}}{\sum_{l \in \mathcal{I}_t} |h_l|^2}} h_l^*$, $l \in \mathcal{I}_t$ to maximize the SNR at Bob with the transmission power $P_{\mathrm{TX}} = \mathbb{E}[||\mathbf{w}_t||^2]$ (under the assumption that the signal power is normalized, i.e., $\mathbb{E}[|s|^2] = 1$). Thus, it can be shown that

$$|\mathbf{h}^{\mathrm{T}}\mathbf{w}_t|^2 = P_{\mathrm{TX}} \sum_{l \in \mathcal{I}} |h_l|^2 \sim \frac{P_{\mathrm{TX}}\sigma_h^2}{2} \chi_{2V}^2,$$

where χ_n^2 represents a chi-squared random variable with n degrees of freedom. On the other hand, since w_l and g_l are independent, $\mathbf{g}^{\mathrm{T}}\mathbf{w}_t$ becomes a conditional Gaussian random variable with mean zero and variance $\sigma_g^2||\mathbf{w}_t||^2 = \sigma_g^2 P_{\mathrm{TX}}$ for given $\mathbf{w}_t$. Thus, we have

$$|\mathbf{g}^{\mathrm{T}}\mathbf{w}_t|^2 \sim \frac{P_{\mathrm{TX}}\sigma_g^2}{2} \chi_2^2.$$

From [24], the secrecy rate, which is the maximum data rate that can be securely transmitted in the presence of Eve, is given by

$$C_S = \left(\mathbb{E}[\log_2(1 + |\mathbf{h}^{\mathrm{T}}\mathbf{w}_t|^2)] - \mathbb{E}[\log_2(1 + |\mathbf{g}^{\mathrm{T}}\mathbf{w}_t|^2)]\right)^+, \tag{10}$$

where $(x)^+ = \max\{x, 0\}$. Then, from [25], we have

$$\begin{aligned} C_S = \frac{1}{\ln 2} \Bigg(& e^{\frac{1}{P_{\mathrm{TX}}\sigma_h^2}} \sum_{m=1}^{V} E_m\left(\frac{1}{P_{\mathrm{TX}}\sigma_h^2}\right) \\ & - e^{\frac{1}{P_{\mathrm{TX}}\sigma_g^2}} E_1\left(\frac{1}{P_{\mathrm{TX}}\sigma_g^2}\right) \Bigg)^+, \end{aligned} \tag{11}$$

where $E_m(x) = \int_1^\infty e^{-xt} t^{-m} dt$ is the exponential integral function of order m. From (11), we can see that the secrecy rate increases with V. Thus, although $\sigma_g^2 > \sigma_h^2$, the AP/DCU could transmit a key securely using ASM.

C. Impact of J on Probability of Successful Attack

Let J denote the maximum number of transmissions that an active smart meter can use the same key to generate a spreading sequence. The AP/DCU can send a new key to the active smart meter once the same key is used J times. For tractable analysis, we assume that the number of active smart meters for each time slot is fixed (i.e., M is deterministic), although M is a random variable. Since there are K smart meters, the probability that the smart meters in Ω become active is $p(K, M) = \frac{1}{\binom{K}{M}}$. Then, when a smart meter in Ω uses the same key to generate spreading codes J times, the probability that all the smart meters in Ω group become active n times is given by

$$P_n = \binom{J}{n} p^n(K, M)(1 - p(K, M))^{J-n}. \tag{12}$$

[2]For wireless communications in SUN, micro-wave frequency bands are considered [5] (e.g., 700MHz – 1 GHz and 2.4 GHz bands).

Then, the probability of successful attack (SA) is given by

$$P_{\mathrm{SA}} = \sum_{n=\tau}^{J} P_n = \sum_{n=\tau}^{J} \binom{J}{n} p^n(K,M)(1-p(K,M))^{J-n}. \tag{13}$$

Note that this probability is optimistic to the eavesdropper as it is based on the assumption that the smart meters in Ω do not change their keys to generate spreading codes when any smart meter in Ω uses the same key J times. If $\tau = 1$ (i.e., Eve just needs to have one observation of the pair of $(\mathbf{q}_t, \mathbf{u}_t)$), we have

$$P_{\mathrm{SA}} = 1 - (1 - p(K,M))^J.$$

Thus, in general, a small J and/or large K would be desirable for a low P_{SA}.

V. Simulation Results

For simulations, the total number of smart meters and the processing gain are set to $K = 64$ and $L = 32$, respectively. Also, there is one AP/DCU equipped with N antennas. We assume that the channel coefficients, $h_{k,i;t}$, are Rayleigh distributed and the QPSK modulated data symbols, $s_{k;t}$, are transmitted by smart meters. At the receiver, the OMPMMV algorithm [19] is used to recover the signal with multiple antennas.

Fig. 2 shows the delay-outage probability over N with $D_{\max} = 1$, 2, and 5. M smart meters of K are active and try to access with the access probability of $p_a = 0.1$. In simulations, the active nodes transmit symbols for 100 access slots during which some nodes perform fast retrials if they fail in access. From Fig. 2, we can see that the delay-outage probability decreases as N increases. In particular, if the number of antennas is sufficiently large, i.e. $N \geq 8$, the decreasing gets slow in actual P_{out} or even flat in the upper bounds. This observation is obvious from the ideal case of (8), where $\bar{M}(\epsilon)$ becomes constant for fixed L if N is large, which leads to the flat upper bound from (7). According to the results, we can claim that a low delay-outage probability can be obtained using multiple antennas at the receiver.

In order to send keys to smart meters over micro-wave channels, we consider ASM presented in Subsection IV-B. A high secrecy rate is desirable to transmit a long key to a smart meter within a short time period. Fig. 3 shows the secrecy rate that can be achieved by ASM for various values of N when $V = \lceil N/2 \rceil$. Clearly, we can see that a positive secrecy rate can be achieved for a large V, which demonstrates that the updating of smart meters' keys to generate spreading codes is possible using multiple antennas at the AP/DCU and more frequent updating is possible as N increases (since the secrecy rate increases with N).

Fig. 4 shows the probability of SA as a function of J for different numbers of K when $M = 5$ and $\tau = 1$. It is shown that P_{SA} increases with J. That is, it would be more secure if keys to generate spreading codes can be more frequently updated using physical layer security schemes with a large array. We can also confirm that a large K is desirable to decrease P_{SA}.

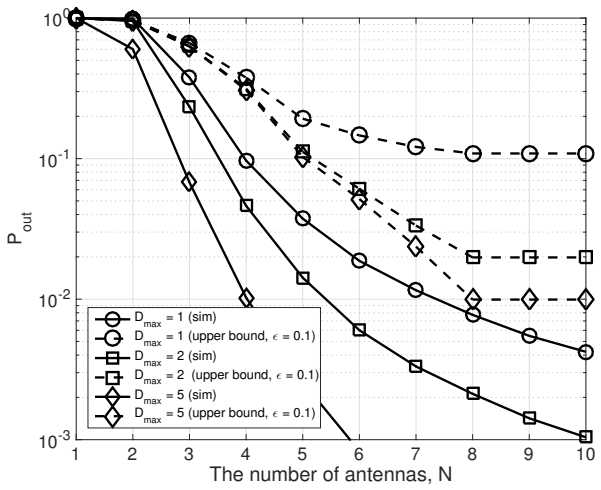

Fig. 2. Delay-outage probability versus N when $K = 64$, $L = 32$, and $p_a = 0.1$.

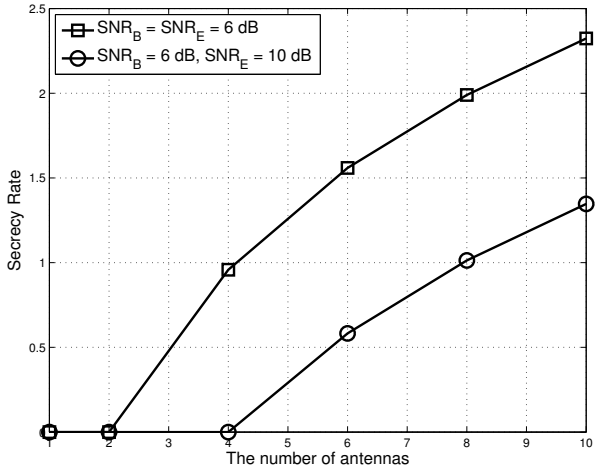

Fig. 3. Secrecy rate versus N when $V = \lceil N/2 \rceil$ antennas are active for ASM.

Fig. 5 shows the probability of SA as a function of J for different numbers of M when $K = 64$ and $\tau = 1$. If $M = 1$, Eve can perform a successful attack with a high probability (close to 1) when $J \geq 10^2$. From this, we can conclude that J has to be small (or frequent updating of key is required) for secure transmissions. Interestingly, we can also observe that a large M (a large sparsity) is desirable as the probability of SA is low. This demonstrates that although an eavesdropper is capable of estimating multiple initial vectors of spreading sequence generators simultaneously (for any M), her high computing power would not help to increase P_{SA} as the probability to observe the signals from the smart meters in a target group decreases with M. From this, we can see that for secure transmissions, it is better to have a large M or a large K (with a fixed access probability). While this results in some difficulty in detecting active smart meters at the AP/DCU, it could be mitigated by using multiple antennas. Consequently, we can claim that an antenna array at the AP/DCU plays

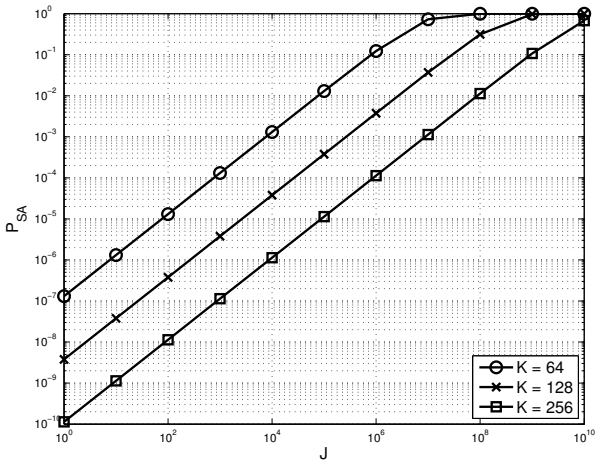

Fig. 4. P_{SA} versus J for different numbers of K when $M = 5$ and $\tau = 1$.

a critical role in providing both security and low latency transmissions.

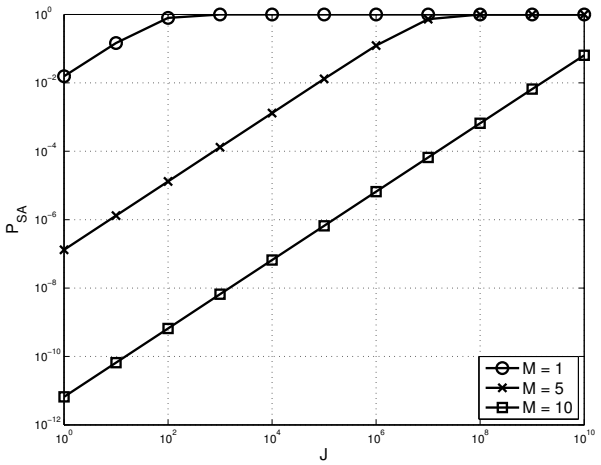

Fig. 5. P_{SA} versus J for different numbers of M when $K = 64$ and $\tau = 1$.

VI. Conclusions

In this paper, we studied random access for a number of smart meters in SUN, where active smart meters are to transmit their load reports with a stringent delay constraint to avoid instability of smart grid. Due to fading and noise, there might be some access delay. To lower access delay, we proposed to use multiple antennas with a CS algorithm for MMVs. From simulations, we showed that the delay-outage probability becomes lower as more antennas are used. In addition, we considered secret key updating in random access using a physical layer security technique, ASM, which is based on an antenna array, to mitigate a known plain-text attack that attempts to extract keys of some targeted smart meters. Consequently, in this paper, we demonstrated that multiple antennas are indispensable at an AP/DCU in SUN for random access with a low latency and security.

References

[1] A. Ipakchi and F. Albuyeh, "Grid of the future," *IEEE Power and Energy Magazine*, vol. 7, pp. 52–62, March 2009.

[2] Q.-D. Ho, Y. Gao, G. Rajalingham, and T. Le-Ngoc, *Wireless Communications Networks for the Smart Grid*. Springer, 2014.

[3] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Communications Surveys Tutorials*, vol. 14, pp. 998–1010, Fourth 2012.

[4] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344 – 1371, 2013.

[5] K.-H. Chang and B. Mason, "The ieee 802.15.4g standard for smart metering utility networks," in *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*, pp. 476–480, Nov 2012.

[6] H. Li, R. Mao, L. Lai, and R. C. Qiu, "Compressed meter reading for delay-sensitive and secure load report in smart grid," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pp. 114–119, Oct 2010.

[7] R. H. Y. Louie, W. Hardjawana, Y. Li, and B. Vucetic, "Distributed multiple-access for smart grid home area networks: Compressed sensing with multiple antennas," *IEEE Trans. on Smart Grid*, vol. 5, pp. 2938–2946, Nov 2014.

[8] E. Candes and T. Tao, "Decoding by linear programming," *IEEE Trans. Information Theory*, vol. 51, pp. 4203–4215, Dec 2005.

[9] D. Donoho, "Compressed sensing," *IEEE Trans. Inform. Theory*, vol. 52, pp. 1289–1306, April 2006.

[10] H. Zhu and G. Giannakis, "Exploiting sparse user activity in multiuser detection," *IEEE Trans. Communications*, vol. 59, pp. 454–465, February 2011.

[11] F. Fazel, M. Fazel, and M. Stojanovic, "Random access compressed sensing over fading and noisy communication channels," *IEEE Trans. Wireless Communications*, vol. 12, pp. 2114–2125, May 2013.

[12] G. M. Davis, S. G. Mallat, and Z. Zhang, "Adaptive time-frequency decompositions," *Optical Engineering*, vol. 33, no. 7, pp. 2183–2191, 1994.

[13] T. I. Choi, K. Y. Lee, D. R. Lee, and J. K. Ahn, "Communication system for distribution automation using cdma," *IEEE Transactions on Power Delivery*, vol. 23, pp. 650–656, April 2008.

[14] M. Kuzlu, M. Pipattanasomporn, and S. Rahman, "Communication network requirements for major smart grid applications in HAN, NAN and WAN," *Computer Networks*, vol. 67, pp. 74 – 88, 2014.

[15] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," in *Communication, Control, and Computing, 2008 46th Annual Allerton Conference on*, pp. 813–817, Sept 2008.

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

[17] W. Meier and O. Staffelbach, "Fast correlation attacks on certain stream ciphers," *Journal of Cryptology*, vol. 1, no. 3, pp. 159–176, 1989.

[18] T. Johansson and F. Jonsson, "Theoretical analysis of a correlation attack based on convolutional codes," *IEEE Transactions on Information Theory*, vol. 48, pp. 2173–2181, Aug 2002.

[19] J. Chen and X. Huo, "Theoretical results on sparse representations of multiple-measurement vectors," *IEEE Transactions on Signal Processing*, vol. 54, pp. 4634–4643, Dec 2006.

[20] Y.-J. Choi, S. Park, and S. Bahk, "Multichannel random access in ofdma wireless networks," *IEEE J. Selected Areas in Communications*, vol. 24, pp. 603–613, March 2006.

[21] R. Dautov and G. R. Tsouri, "Establishing secure measurement matrix for compressed sensing using wireless physical layer security," in *Computing, Networking and Communications (ICNC), 2013 International Conference on*, pp. 354–358, Jan 2013.

[22] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180–2189, June 2008.

[23] N. Valliappan, A. Lozano, and R. Heath, "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Trans. Communications*, vol. 61, pp. 3231–3245, August 2013.

[24] M. R. Bloch and J. N. Laneman, "Strong secrecy from channel resolvability," *IEEE Transactions on Information Theory*, vol. 59, pp. 8077–8098, Dec 2013.

[25] M.-S. Alouini and A. J. Goldsmith, "Capacity of rayleigh fading channels under different adaptive transmission and diversity-combining techniques," *IEEE Trans. Veh. Technol.*, vol. 48, pp. 1165–1181, July 1999.