Communication Capacity Requirement for Reliable and Secure State Estimation in Smart Grid

Husheng Li†, Lifeng Lai‡ and Robert. C. Qiu§
† Department of Electrical Engineering and Computer Science, The University of Tennessee, Knoxville, TN
‡ Department of Systems Engineering, University of Arkansas, Little Rock, AR
§ Department of Electrical and Computer Engineering, Tennessee Technological University, Cookeville, TN

Abstract—Secure system state estimation is an important issue in smart grid to assure the reliability and security. In this paper, the case of a single observation station and Gaussian noise communication channel with an eavesdropper is considered. The channel capacity requirement is studied from the information theoretic perspective. The smart grid is modeled as a linear dynamic system. Then, the channel capacity requirement is studied for the state estimation of general linear dynamic systems and then applied in the system state estimation in smart grid. Numerical simulations are used to evaluate the capacity requirement in typical configurations of smart grid.

I. INTRODUCTION

In recent years, the smart grid technology has attracted much attention in the communities of power systems, communications, networking and control systems [5] [9] [7]. In a smart grid, modern information technologies are applied for power systems to report the instantaneous power load to the power market and feed back the time-varying power price to power consumers such that the power consumptions can be controlled using a price mechanism.

In smart grid, communications play a key role since the information about load and price needs to be delivered over the communication network. Two fundamental issues exist for the communication in smart grid:

- Capacity: The communication link should be able to convey the information of load and price to the destinations (the power market and the power consumer, respectively) with negligible error in a realtime manner.
- Security: It is important to preserve the privacy of the system state in smart grid. If the information is leaked, an eavesdropper could use this information to break the stability of the power market or steal personal private information.

The information leakage could occur during both the information transmission and information storage stages. In this paper, we address the above two issues during the information transmission stage. For simplicity, we consider the case of a single observation station and a control center. As illustrated in Fig. 1, the observation station encodes the observation on the system state into a bit string and then sends to the control center, which decodes the codeword and then uses the system state for further actions. The transmitted channel symbols are contaminated by Gaussian noise before the decoder at the power market. Meanwhile, an eavesdropper overhears the received signal at the control center and the signal is further contaminated by an independent Gaussian noise. Then, the goal of the communication in smart grid is to convey the system state to the control center reliably and without being intercepted by the eavesdropper. Note that the model considered in this paper is far simpler than the practical case, in which the system observations are collected from many distributed observers, e.g., the load information is obtained from the reports of smart meters and the power generation information is obtained from the power generation companies. However, the study on the simplified model can provide insights and tools for the study on more complicated systems. Moreover, it is the first study on the secured system state estimation via a communication channel in a dynamic system, to our best knowledge. In the near future, we will extend the study to the case of multiple observers.

We focus on the fundamental limit, i.e., how much channel capacity is needed to guarantee the secure and reliable system state estimation in smart grid, from the information theory perspective. The study on secure communications in the information theory community traces back to 1975 [10], when A. D. Wyner proposed the information theoretic study on wire-tap channels. Subsequently, the information theorists have studied the capacity requirement with security for different channels, like additive white Gaussian noise (AWGN) channel [2]. Recent years witnessed the resurrection of the information theoretic study on security issues, like channel capacity requirements for fading channels, multiple access channels, broadcast channels and interference channels. A survey on these studies can be found in [3].

However, the traditional information theoretic studies on communications with security usually focus on stationary and
ergodic information source. The smart grid is a dynamic system, which may not be stationary and ergodic. Moreover, the system state is continuously valued, instead of discrete information source. Therefore, these fundamental studies on secure communications must be revisited for the context of smart grid. We will first study the channel capacity requirement for secured communications for Gaussian wire-tap channels and general linear dynamic systems. As will be shown, under certain conditions, the channel capacity requirement could be zero or infinite. Then, we will study the special case of smart grid using practical parameters. The impacts of different factors of the power market on the communication requirement will be studied using numerical simulations.

The remainder of this paper is organized as follows. The system model of smart grid is given in Section II. Then the secured communication is studied for general dynamic systems in Section III, and is then applied in the context of smart grid in Section IV. Numerical results and conclusions are provided in Sections III and V, respectively.

II. SYSTEM MODEL

For simplicity, we consider a discrete time system, in which the time is divided into time slots. We consider the following general dynamics of smart grid, which is given by

\[ x(t + 1) = F(x(t), w(t)), \]

where \( x(t) \) is the state vector at time slot \( t \) (the alphabet of the state vector is denoted by \( X \)), \( w(t) \) is a random factor, \( F \) is a function mapping the previous state vector and the random factor to the next state vector.

We assume that the observation station can send a coded message about the state vector every \( T \) time slots, denoted by \( m(jT) \) at time slot \( jT \). When the control center receives a message at time slot \( jT \), it will decode it and then reconstruct the state vectors \( x(jT) \), \( x((j - 1)T + 1) \), ..., \( x(jT) \). We assume that the transmitter satisfies the average transmit power constraint and we denote by \( P \) the maximal average transmit power.

We assume that the channel between the observation station and the control center is an additive white Gaussian noise channel. The Gaussian noise is assumed to have a zero mean and a variance \( \sigma_0^2 \). We also assume that there is an eavesdropper monitoring the system state of smart grid by listening to the received signal at the power market, denoted by \( \{y(jT)\}_{j=1,2,...} \). The signal received at the eavesdropper, denoted by \( \{z(jT)\}_{j=1,2,...} \), is the sum of the signal received at the power market and an independent noise (with zero mean and variance \( \sigma_z^2 \)).

III. SECURED COMMUNICATION FOR DYNAMIC SYSTEMS

In this section, we first define the security metric in general dynamic systems. Then, we discuss the capacity requirement for secure communications for observable dynamic systems.

A. Security Metric

We need a metric to measure how secure the communication is in the smart grid. In the traditional communication systems, the transmitter satisfies the average transmit power constraint

\[ x(t + 1) = F(x(t), w(t)), \]

where \( x(t) \) is the state vector at time slot \( t \) (the alphabet of the state vector is denoted by \( X \)), \( w(t) \) is a random factor, \( F \) is a function mapping the previous state vector and the random factor to the next state vector.

We assume that the observation station can send a coded message about the state vector every \( T \) time slots, denoted by \( m(jT) \) at time slot \( jT \). When the control center receives a message at time slot \( jT \), it will decode it and then reconstruct the state vectors \( x(jT) \), \( x((j - 1)T + 1) \), ..., \( x(jT) \). We assume that the transmitter satisfies the average transmit power constraint and we denote by \( P \) the maximal average transmit power.

We assume that the channel between the observation station and the control center is an additive white Gaussian noise channel. The Gaussian noise is assumed to have a zero mean and a variance \( \sigma_0^2 \). We also assume that there is an eavesdropper monitoring the system state of smart grid by listening to the received signal at the power market, denoted by \( \{y(jT)\}_{j=1,2,...} \). The signal received at the eavesdropper, denoted by \( \{z(jT)\}_{j=1,2,...} \), is the sum of the signal received at the power market and an independent noise (with zero mean and variance \( \sigma_z^2 \)).

The set of all possible system realizations An element in the spanning set.

\[ H(F,X,\Omega) = \lim_{\epsilon \to 0} \lim_{k \to \infty} \frac{1}{k} \log_2 q(k,\epsilon). \]

We assume that the topological entropy in our considered dynamic system is finite. Obviously, the topological entropy represents the uncertainty of the dynamic system. For an arbitrary \( k \), \( \log_2 q(k,\epsilon) \) is the number of bits needed for describing an approximation (with precision \( \epsilon \)) of the system’s
dynamic behavior during the \(k\) time slots. Hence, we can replace the denominator of the equivocation in (2).

Now, we deal with the counterpart of the numerator, i.e., the conditional entropy, in (2) in the context of dynamic systems. Denote by \(\hat{Q}\) the \((k, \epsilon)\)-spanning set with the least cardinality. The elements can be denoted by 1, 2, ..., \(g\). We consider a random variable \(W_k\) taking values over these elements. Then, the value of \(W_k\) is determined by the randomness of the dynamic system: for a realization of the dynamic system, we define \(W_k\) as the label of the \(x\) in \(\hat{Q}\) that is the closest to the system realization. We assume that \(W_k\) is uniformly distributed. It is easy to observe that the topological entropy \(\Delta = 1\) is equal to the entropy of \(W_k\) as \(k \to \infty\). Now, considering a random vector \(Z\) dependent on the dynamic system’s behavior, we have the following definition.

Definition 3: The conditional topological entropy of the system in (1) is defined as

\[
H(F, X, \Omega | Z) = \lim_{k \to \infty} H(W_k | Z).
\]

On assuming that the conditional entropy in (4) exists, we define the equivocation of the dynamic system in (1) with respect to the overheard message \(Z\) as

\[
\Delta = \frac{H(F, X, \Omega | Z)}{H(F, X, \Omega)}.
\]

Then, we define reliable and secure communications between the system state sensor and the controller as follows.

Definition 4: If the communication between the sensor and the controller assures the observability of the system state and satisfies \(\Delta = 1\), we say that the communication is reliable and secure.

Note that the observability is defined as follows.

Definition 5: The system in (1) is called observable if for any \(\epsilon > 0\), there exist an \(T \geq 1\) and a coder-decoder pair such that

\[
\|x(t) - \hat{x}(t)\|_{\infty} < \epsilon, \quad \forall t = 1, 2, 3, ..., \]

where \(\hat{x}\) is the recovered system state at the controller.

B. Capacity Requirement

The following proposition discloses the requirement of the capacity for the reliable and secure communication in the dynamic system. The proof is given in Appendix I.

Proposition 1: When the following inequality holds,

\[
H(F, X, \Omega) \leq C_1 - C_2,
\]

in which

\[
C_1 = \log \left(1 + \frac{P}{\sigma_0^2}\right) \quad \text{and} \quad C_2 = \log \left(1 + \frac{P}{\sigma_0^2 + \sigma_c^2}\right),
\]

the reliable communication is guaranteed, however the security of the system is not guaranteed. Furthermore, when

\[
H(F, X, \Omega) > C_1,
\]

neither reliable communication nor the security of the system is guaranteed.

Remark 1: The physical meaning of the proposition is quite intuitive. The right hand sides of both (7) and (10) are the secrecy capacity of Gaussian wiretap channels [2]. For ergodic sources with entropy rate smaller than the secure capacity, the information can be reliably transmitted to the receiver without providing any information to the eavesdropper. The left hand sides of both (7) and (10) equal the minimal requirement of the channel capacity when there is no eavesdropper. However, since the source is a dynamic system, the conclusions for the ergodic information source does not apply directly.

IV. SECURED SYSTEM STATE ESTIMATION WITH LINEAR DYNAMICS

In this section, we apply the conclusion for general dynamic systems in the previous section to the Alvarado model of power grid [1] [6] and then discuss the secured system state estimation.

A. Alvarado Model

In this paper, we adopt the Alvarado model [1] [6] for the power system. In this model, there are four variables in the system state:

- \(P_g\): the amount of generated power;
- \(P_d\): the amount of consumed power;
- \(E\): the time integral of the difference in power supply and power demand;
- \(\lambda\): the price of a unit of power.

In the continuous time, the system state satisfies the following dynamics:

\[
\dot{P}_g = (\lambda - b_g - c_g P_g - kE)/\tau_g, \quad (12)
\]
\[
\dot{P}_d = (b_d + c_d P_d - \lambda)/\tau_d, \quad (13)
\]
\[
\dot{E} = P_g - P_d, \quad (14)
\]
\[
\dot{\lambda} = -E/\tau_\lambda, \quad (15)
\]

where \(\tau_g, \tau_d\) and \(\tau_\lambda\) are parameters controlling the rate at which the supply, demand and price change due to market changes, and \(b_g, b_d, c_d\) and \(c_g\) are also parameters, whose physical meanings can be found in [1] [6].

We can take a very small time interval \(\Delta t\) and convert the continuous time model into a discrete time one, which is given by

\[
x(t + 1) = Ax(t) + b,
\]

where

\[
A = \Delta t \begin{pmatrix}
-\frac{c_g}{\tau_g} & 0 & \frac{1}{\tau_g} & 0 \\
0 & -\frac{c_d}{\tau_d} & 0 & -\frac{1}{\tau_d} \\
1 & -1 & 0 & 0 \\
0 & 0 & -\frac{1}{\tau_\lambda} & 0
\end{pmatrix},
\]

\[
\dot{x}(t + 1) = \dot{x}(t) + \frac{\Delta t}{\tau} \begin{pmatrix}
-b_g & -c_g & -k & 0 \\
b_d & b_g & -c_d & 0 \\
E & -P_g & 0 & 0 \\
0 & 0 & 0 & -\lambda
\end{pmatrix} x(t) + \frac{\Delta t}{\tau} b(t),
\]

\[
\dot{x}(t + 1) = \dot{x}(t) + \Delta t \begin{pmatrix}
-k & 0 & 0 & 0 \\
0 & -\lambda & 0 & 0 \\
0 & 0 & -\frac{1}{\tau_\lambda} & 0 \\
0 & 0 & 0 & -\frac{1}{\tau_\lambda}
\end{pmatrix} x(t) + \Delta t \begin{pmatrix}
b_d & b_g & -c_d & 0 \\
b_g & b_g & -c_g & -k \\
0 & 0 & 0 & -\lambda \\
0 & 0 & 0 & -\lambda
\end{pmatrix} x(t) + \Delta t \begin{pmatrix}
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix} x(t) + \Delta t \begin{pmatrix}
b_d & b_g & -c_d & 0 \\
b_g & b_g & -c_g & -k \\
0 & 0 & 0 & -\lambda \\
0 & 0 & 0 & -\lambda
\end{pmatrix} x(t) + \Delta t b(t),
\]
and
\[
b = \Delta t \left( \frac{b_g}{\tau_g}, \frac{b_d}{\tau_d}, 0, 0 \right)^T ,
\]
and
\[
x = (P_g, P_d, E, \lambda)^T .
\]

B. Reliable and Secured State Estimation

The following proposition discloses the channel capacity requirement for the reliable and secured state estimation for the power system model discussed in this section. The proof is given in Appendix II.

Proposition 2: When \( b_d = b_g = 0 \), the reliable and secure system estimation requires zero channel capacity, when the system is stable, and requires non-zero channel capacity, when the system is unstable. When \( b \neq 0 \) and the matrix \( \mathbf{A} \) is reachable and stable, the reliable and secure system estimation can never be achieved with a communication channel with a finite capacity.

Remark 2: When the reliable and secured system estimation cannot be achieved, it does not mean that the system state can no longer be estimated in practice. It only means that the estimation error is not vanishing. However, when the estimation error is sufficiently small, it is still valid for practical systems. When then channel capacity requirement is 0, it does not mean that the communication system is trivial since an important issue, the delay, is omitted in the information theoretic analysis.

V. NUMERICAL SIMULATION

In this section, we use numerical simulations to study the impact of different factors on the channel capacity requirement for reliable and secure system state estimation. The default setup is \( \Delta t = 1, \tau_g = 0.2, c_g = 0.1, \tau_d = 0.1, c_d = -0.2, \tau_d = 100 \) and \( k = 0.1 \), unless stated otherwise, which is the same as those used in [6] except that we set \( b_d = b_g = 0 \). Note that the topological entropy is computed using (22) in Appendix II.

A. Impacts of \( c_g \) and \( c_d \)

Recall that the parameters \( c_g \) and \( c_d \) represent the increasing rates of the cost and benefit with respect to the generated power and consumed power, respectively. We plot the topological entropies in Figures 3 and 4 for large and small values, respectively. We observe that the topological entropy increases with the absolute values of \( c_g \) and \( c_d \). When the absolute values of \( c_g \) and \( c_d \) are sufficiently small, the topological entropy could be zero. This demonstrates that the communication requirement is improved when the rates of cost and benefit are increased.

B. Impacts of \( \tau_g \) and \( \tau_d \)

In the Avarado model, the parameters \( \tau_g \) and \( \tau_d \) represent the response times of the power generator and the power consumer, respectively. The topological entropy with various \( \tau_g \) and \( \tau_d \) is shown in Fig. 5. We observe that the topological entropy decreases with \( \tau_g \) and \( \tau_d \). An intuitive explanation is that an increasing response time makes the system less dynamical, thus facilitating the system state estimation.

C. Impacts of \( \tau_\lambda \) and \( k \)

In the Avarado model, the parameter \( \tau_\lambda \) means the market clearing time and \( k \) scales the additional cost when there is a history of supply excess. The corresponding topological entropy is shown in Fig. 6. We observe that the topological entropy decreases with \( \tau_\lambda \) since it makes the system less dynamical. Meanwhile, the topological entropy increases with \( k \), which adds more dynamical factors to the system.

D. Secrecy Capacity in Wireless Channels

For the default setup in the power system, we have obtained that the topological entropy is equal to 1.03 bits per channel use. If a binary phase shift keying (BPSK) modulation is used and the symbol rate is \( 1/W \), where \( W \) is the frequency bandwidth for communications, then the required spectral efficiency is 1.03 bits/sec/Hz.

Now, we assume that the observation station communicates to the control center using a wireless channel. We assume that
the frequency bandwidth is 10MHz. The path loss is given by

\[ L = 28.6 + 35 \log_{10}(d)(dB), \tag{20} \]

where \( d \) is the distance in meters. We also assume that the noise power spectral density (PSD) at the control center is -174dBm/Hz and the transmit power is 200mW. We assume that \( \sigma^2 = (G-1)\sigma_N^2 \), where \( G = 2, 3, 4, 5 \). The secrecy capacity\(^1\) is shown in Fig. 7. The requirement of 1.03bits/sec/Hz is also shown in the figure (the dashed horizontal line). We observe that, when \( G \) is small, the requirement cannot be achieved; when \( G \) is large, the reliable and secure system state estimation can be achieved if the observation station is close to the control center.

VI. CONCLUSIONS

We have studied the reliable and secured system estimation when the observation station and control center are separated. We have combined the theory of estimation over communication networks and the information theoretic study on secured communications, by assuming a Gaussian wiretap channel. Conditions, based on the concept of topological entropy, have been obtained. We have applied the conclusion for general dynamic systems to a simplified dynamic model of power systems. It has been found that, under certain conditions, the reliable and secure system state estimation may require zero or infinite channel secrecy capacity. For typical values of parameters of the power system model, numerical results have shown that the communication requirement increases with the increasing rates of cost and benefit, decreases with the response / clearance time and increases with the additional cost due to supply excess.

ACKNOWLEDGEMENT

The authors would like to thank Prof. Fangxing Li in the Dept. of EECS in the University of Tennessee, Knoxville, for the discussion on the dynamics of power market.

APPENDIX I

PROOF OF PROP. 1

Proof: The proof follows an argument similar to Theorem 2.3.6 in [4] and Theorem 1 in [2].

We first prove the conclusion from inequality (7), i.e., when the topological entropy of the system is smaller than the secrecy capacity of the Gaussian wiretap channel, we can always find a coding and decoding scheme such that the legitimate receiver can reliably obtain the system state while the eavesdropper can obtain no information about the system state.

The coding and decoding procedures are illustrated in Fig. 8. Fix a \( k > 0 \). Find the \((k, \epsilon)-\)spanning set \( Q \) having the least cardinality. Given the system realization \( x(1), \ldots, x(k) \), choose the closest element \( \tilde{x}_k = \{x(1), \ldots, \tilde{x}(k)\} \) such that

\[ \|x(t) - \tilde{x}(t)\|_\infty \leq \epsilon, \tag{21} \]

which is guaranteed by the definition of \((k, \epsilon)-\)spanning set.

Then, the label of the element in \( Q \) is converted into a binary sequence, which is the realization of the random variable \( W_k \). This sequence is then encoded into a codeword using a stochastic coding approach in the proof of Theorem 1 in [2]. Roughly speaking, in a stochastic coding scheme, each message \( W_k \) is associated with a group of codewords \( U \). To transmit \( W_k \), a codeword is randomly selected from its corresponding group. This additional randomness increases the

\(^1\)Although it is actually spectral efficiency, we call it capacity for simplicity.
transmission rate. However, as long as the sum of the message rate and the randomness rate is less than the capacity of the channel between the source and the receiver, the receiver can successfully decode the codeword $U$ and find its corresponding $W_k$. The receiver can then find the element $q$ in $Q$ that is associated with $W_k$, which will be used as the estimated state vector by the receiver. The property of the $(k, e)$-spanning set assures that the communication is reliable. Meanwhile, due to the conclusion of secrecy channel capacity in [2], the conditional entropy $H(W_k|Z)$ is very close to $H(W_k)$. Let $k \to \infty$, the conclusion of (7) is obtained.

Now, if $H(F, X, \Omega) > C_1$, according to the first part of Theorem 2.3.6 in [4], the transmission rate over the channel must be larger than or equal to $H(F, X, \Omega)$, which is larger than the capacity of the legitimate user. As the result, the legitimate user is not able to decode the message, which means that the reliability is not guaranteed. Hence, the claim in (11) is true.

When $C_1 > H(F, X, \Omega) > C_1 - C_2$, according to the first part of Theorem 2.3.6 in [4], the transmission rate over the channel must be larger than or equal to $H(F, X, \Omega)$. The receiver is still able to decode the message, i.e., the reliability requirement is satisfied. However, the transmission rate is larger than the secrecy capacity of the Gaussian wiretap channel, according to Theorem 1 in [2], which means that there exists a constant $c$ such that $\Delta < 1 - c$. And hence $H(W_k|Z) < H(W_k) < 1 - c$, meaning that $I(Z; W_k) > cH(W_k)$. Hence, from $Z$, the eavesdropper can infer information about $W_k$. Hence, the claim in (10) is valid.

**APPENDIX II**

**PROOF OF PROP. 2**

**Proof:** We discuss the secure state estimation for the following cases:

- $b = 0$: For this case, we have $b_y = b_d = 0$. According to the physical meaning $b_y$ and $b_d$, the marginal cost of the power generator is given by $c_g P_g$ and the marginal benefit of the power consumer is $c_d P_d$ for this situation. This means that the marginal cost and marginal benefit are both proportional to the amount of power generated or consumed, i.e., there is no constant cost or benefit. According to Theorem 2.4.2 in [4], the topological entropy of the system in (16) is given by

$$H(A) = \sum_{i=1}^{4} \log_2 \left( \max \{1, |\lambda_i|\} \right),$$

(22)

where $\{\lambda_i\}_{1,2,3,4}$ are the eigenvalues of the matrix $A$. Obviously, when the absolute values of all eigenvalues are smaller than 1 (i.e., the system is stable), the topological entropy is 0, thus requiring zero channel capacity. Otherwise, the topological entropy is non-zero.

- $b \neq 0$: In this case, there exist constant marginal cost and marginal benefit, which are independent of the power generated or consumed. According to Prop. 2.4.15 in [4], the topological entropy is infinite, when the matrix $A$ is reachable and stable. The topological entropy is still unknown for other cases.

**REFERENCES**


