Microgrid Protection and Control Through Reliable Smart Grid Communication Systems

Md Masud Rana, Li Li and Steven W. Su
Faculty of Engineering and Information Technology
University of Technology Sydney, Broadway, NSW 2007, Australia
Email: 11766084@student.uts.edu.au, Li.Li@uts.edu.au and Steven.Su@uts.edu.au

***Abstract*—Due to dramatically rising energy demand worldwide power system is often run near the operational and technical limits, where unexpected trivial disturbances can cause possibly massive blackouts. Cyber attacks on smart grid communication networks are one of the impending threats to cause large-scale cascading outage. In contrast to the traditional cyber attack protection techniques, this paper presents a recursive systematic convolutional code based defending technique from the signal processing perspective. This code introduces redundancy in the system for protecting the grid information. Furthermore, an optimal control law is designed to stabilize the power network. Specifically, the performance index for control is converted to a convex semidefinite programming problem. The proposed controller can work well for any initial values. The efficacy of the developed approach is verified through numerical simulations. Results show that the proposed strategy has stronger attack protection performance and the controller can stabilize the grid in a fairly short time. This approach provides a fundamental framework for the design of the smart grid energy management system and reliable communication infrastructure scheme with renewable integration applications.**

***Keywords*—Cyber attack, Kalman filter, renewable microgrid, smart grid, optimal feedback control.**

I. Introduction

Concerns associated with the growing costs of traditional energy with limited resources, greenhouse gas emissions, reliability, climate change, and security of the electric power system have forced toward the development of renewable distributed energy resources (DERs) all over the world [1]. These DERs such as solar panels, wind turbine, microturbine, and biomass are generally considered as environment-friendly, clean, and safe power sources. A microgrid with multiple DERs is a local energy network that integrates on-site electricity generation and storage with local loads. It can operate in parallel with the power systems or in an island mode. Unfortunately, the microgrid integration with distribution systems can have substantial negative impacts on grid operation and protection due to their intermittent power generation patterns [2]. That means under fault and unexpected conditions, the smart grid can experience severe monitoring and stabilization problems which can lead to blackouts and power quality problems [3].

To alleviate severe instability and monitoring of large-scale networks, one potential solution is to design a reliable and secure energy management system (EMS). EMS is highly dependent on measurements, and it has different signal processing modules including state estimation program, control functionalities, contingency analysis, forecasting, and optimal power flow [4]. Therefore, cyber attacks that change the system measurements can intrinsically cause wrong estimations within these modules which can lead to potential systematic problems and cascading failures [5]. In order to design an effective EMS, our first step is to design a suitable communication infrastructure incorporating state estimation algorithm and flexible control system. The state estimation can identify the system operating conditions and give alarm for utility engineers to take necessary actions if there is any faults or attacks. Therefore, the main function of state estimation is to estimate unmeasurable quantities, remove measurement errors and detect the existence of attacks. Following that the control algorithm is required to stabilize the power network.

Recently, the topic of information security is gaining interests in many research communities such as smart grid, control, signal processing and communication communities [6]. Indeed, a variety of state estimation methods has been proposed for estimating the system states under cyber attack conditions. Classic weighted least squares (WLS) method is widely used for bad data detection and state estimation [7], [8]. This method can estimate the system state accurately when the variances of the measurement errors are well known [9]. But the cyber-attacks such as false data injection can pass the bad data detection process, which can lead severe security and outage problems. The work presented in [10], [11] illustrates the least trimmed squares technique where the Jacobian matrix and measurements are attacked. Nowadays, a Bayesian and Neyman-Pearson based joint cyber attack detection and state estimation is explored in [12]. After defining the cost function, an optimal detection and estimation scheme is proposed under the Bayesian formulation. Based on the Neyman-Pearson theorem, the derived cost function is minimized under certain hypothesis conditions [13]. Moreover, a joint likelihood ratio test and maximum likelihood estimator is also widely used in the literature. Though some fundamental state estimation frameworks under attack conditions have been proposed but all the results have ignored a reliable communication and its corresponding dynamic state estimation algorithm.

It is not feasible for utility engineers to perform trial-and-error at controller points to find out cyber attacks, so a joint cyber attack protection and state estimation scheme is necessary to apply a control algorithm to stabilize the power network. Taking a scenario for example, an alteration in the system state information by attackers may deceive the control center with the fact that overloaded branches have secured voltage and vice versa (or attacker changes the breaker statuses of operational lines and marks them as open). Inspired by the fundamental requirement to design a secure EMS against attacks, this research considers the problem of estimating the dynamic system states when a set of sensors is arbitrarily corrupted by an adversary. The major contributions can be summarized as follows:

- Renewable microgrid is modelled to obtain state space equation where sensors are deployed to obtain measurements. For protecting the system information from attackers, recursive systematic convolutional (RSC) code defensive scheme is proposed for introducing redundancy into the system. This type of information/communication infrastructure is well suited to the needs of utilities with respect to cost, utility control, cyber security, and ability to provide near real-time two way communication.
- After estimating the system states together with the proposed reliable communication network, we design an optimal feedback control law to regulate the system. Particularly, the performance index for control is achieved by solving a convex semidefinite programming problem.
- The efficacy of the develop approach is verified through numerical simulations and it shows the proposed method can accurately estimate the system states after protecting impairments. Results also reveal that the controller needs only 0.03 seconds to stabilize the power network. By combing these approaches, a novel framework is constructed in the green energy and control engineering community which will shed the light to design a reliable communication and smart energy management system in future.

II. Microgrid Modelling and Cyber attacks

A microgrid is a subset of the smart grid extending from the substation to smart buildings and individual clients. The microgrid is interfaced to the infinite bus power network through inverters. Typically, there are N DERs connected to the main grid. For the sake of simplicity, we assume that $N = 4$ solar panels are connected through the IEEE-4 bus system as shown in Fig. 1 [1], [20]. Here $\mathbf{v}_p = (v_{p1}\ v_{p2}\ v_{p3}\ v_{p4})^T$ denotes input voltages where v_{pi} is the i-th DER input voltage. The four solar panels are connected to the point common Couplings (PCCs) whose voltages are denoted by $\mathbf{v}_s = (v_1\ v_2\ v_3\ v_4)^T$, where v_i is the i-th PCC voltage. Now the nodal voltage equation can be written as follows:

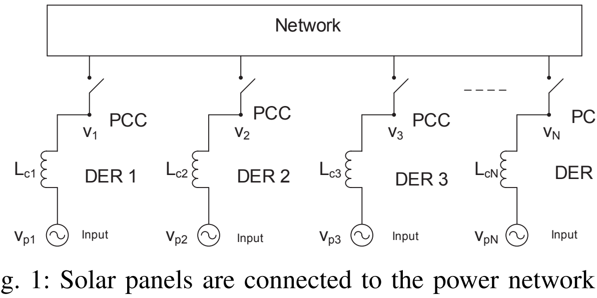

Fig. 1: Solar panels are connected to the power network [20]

$$\mathbf{Y}(s)\mathbf{v}_s(s) = \frac{1}{s}\mathbf{L}_c^{-1}\mathbf{v}_p(s), \tag{1}$$

where the coupling inductor $\mathbf{L}_c = diag(L_{c_1},\ L_{c_2},\ L_{c_3},\ L_{c_4})$ and $\mathbf{Y}(s)$ is the admittance matrix of the entire power network incorporating four mico-sources. Based on the typical specifications of the IEEE 4-bus distribution feeder [20], the admittance matrix is given in (2). The discrete-time linear state space system can be derived as follows:

$$\mathbf{x}(k+1) = \mathbf{A}_d\mathbf{x}(k) + \mathbf{B}_d\mathbf{u}(k) + \mathbf{n}_d(k), \tag{3}$$

where $\mathbf{x}(k) = \mathbf{v}_s - \mathbf{v}_{ref}$ is the PCC state voltage deviation, $\mathbf{v}_{ref}$ is the PCC reference voltage, $\mathbf{u}(k) = \mathbf{v}_p - \mathbf{v}_{pref}$ is the DER control input deviation, $\mathbf{v}_{pref}$ is the reference control effort, $\mathbf{n}_d(k)$ is the zero mean process noise and covariance matrix is $\mathbf{Q}_n$, the state matrix $\mathbf{A}_d = \mathbf{I} + \mathbf{A}\Delta t$ and input matrix $\mathbf{B}_d = \mathbf{B}\Delta t$ with

$$\mathbf{A} = \begin{bmatrix} 175.9 & 176.8 & 511 & 103.6 \\ -350 & 0 & 0 & 0 \\ -544.2 & -474.8 & -408.8 & -828.8 \\ -119.7 & -554.6 & -968.8 & -1077.5 \end{bmatrix}, \tag{4}$$

$$\mathbf{B} = \begin{bmatrix} 0.8 & 334.2 & 525.1 & -103.6 \\ -350 & 0 & 0 & 0 \\ -69.3 & -66.1 & -420.1 & -828.8 \\ -434.9 & -414.2 & -108.7 & -1077.5 \end{bmatrix}, \tag{5}$$

and Δt is the discretization parameter.

In order to monitor microgrids, the utility company has deployed a set of sensors around them. Thus, a linear relationship between the measurement and state variable can be obtained as follows:

$$\mathbf{z}(k) = \mathbf{C}\mathbf{x}(k) + \mathbf{w}(k), \tag{6}$$

where $\mathbf{z}(k)$ is the measurements, $\mathbf{C}$ is the measurement matrix, and $\mathbf{w}(t)$ is the measurement noise with zero mean and the covariance matrix $\mathbf{R}_w$.

Generally speaking, in smart grids the communication infrastructure is used to send information from sensors to EMS. However, vulnerabilities of the infrastructure make modern smart grids prone to cyber attacks. Typically, the aim of the attacker is to insert false data into the measurements as follows:

$$\mathbf{y}(k) = \mathbf{C}\mathbf{x}(k) + \mathbf{w}(k) + \mathbf{a}(k), \tag{7}$$

where $\mathbf{y}(k)$ is the measurements considering cyber attacks, and $\mathbf{a}(k)$ is the false data inserted by the attacker [21], [22], [23]. It assumes that attackers have complete accesses to the system information so that attackers can hijack, record and manipulate data according to their best interest [6]. Interestingly, our target is to secure the grid information from attackers so that the power system can operate properly.

III. Proposed Cyber attacks protection and communication systems

Normally, the smart grid is likely to combine communication infrastructure, control and computation to improve the efficiency, security and reliability [11]. Even though the communication infrastructure for supporting the monitoring and control of smart grid is secured, but it still can be vulnerable to

$$\mathbf{Y}(s) = (\mathbf{L}_c s)^{-1} + \begin{bmatrix} \frac{1}{0.1750+0.0005s} & \frac{-1}{0.1750+0.0005s} & 0 & 0 \\ \frac{-1}{0.1750+0.0005s} & \frac{1}{0.1750+0.0005s} + \frac{1}{0.1667+0.0004s} & \frac{-1}{0.1667+0.0004s} & 0 \\ 0 & \frac{-1}{0.1667+0.0004s} & \frac{1}{0.1667+0.0004s} + \frac{1}{0.2187+0.0006s} & \frac{-1}{0.2187+0.0006s} \\ 0 & 0 & \frac{-1}{0.2187+0.0006s} & \frac{1}{0.2187+0.0006s} + \frac{1}{12.3413+0.0148s} \end{bmatrix}. \tag{2}$$

the intended attacks. To design a reliable communication, the uniform quantizer performs quantization to obtain bit sequence $\mathbf{b}(k)$ from measurements. Then the RSC code is proposed to add parity bits in the bit sequence. Generally speaking, the RSC code is characterized by three parameters: the codeword length n, the message length l, and the constraint length m i.e., (n, l, m). The quantity l/n refers to the code rate which indicates the amount of parity bits added to the data stream. The constraint length specifies m-1 memory elements which represents the number of bits in the encoder memory that affects the RSC generation output bits. If the constraint length m increases, the encoding process intrinsically needs longer time to execute the logical operations. Other advantages of the RSC code compared with the convolutional and turbo encoder include its reduced computation complexity, systematic output features and no error floor [24]. From this point of view, this paper considers the (2, 1, 4) RSC code and (1 1 0 1, 1 1 1 1) code generator polynomial in the feedback process. The first generator polynomial is the lower row in the Fig. 2, while the second polynomial is the upper row in the diagram. So, the code rate is $1/2$ and there are three memories in the RSC process where the logical operations are performed. At the end, the codeword is obtained from the RSC process which goes to the modulation for transmission. The modulated signal $\mathbf{s}(k)$ is passed through a noisy channel.

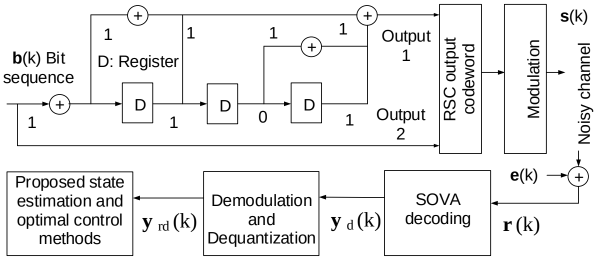

Fig. 2: RSC encoding process to protect the cyber attack.

At the EMS, the received signal is:

$$\mathbf{r}(k) = \mathbf{s}(k) + \mathbf{e}(k), \tag{8}$$

where $\mathbf{e}(k)$ is the additive white Gaussian noise. The $\mathbf{r}(k)$ is followed by the soft output Viterbi algorithm (SOVA) decoding process. The SOVA algorithm computes a maximum likelihood estimate on the code sequence from the received signals. This algorithm traverses the entire trellis and traces back along the maximum likelihood path with noting all path metrics [25], [26]. The decoded output $\mathbf{y}_d(k)$ is sent to the demodulation and de-quantization module and then finally used for the state estimation purpose.

IV. Proposed estimation and control framework

Smart grid state estimation plays a key role in controlling the performance of power networks. Typically, the predicted system state estimate for the system (3) and (6) is expressed as follows [27]:

$$\hat{\mathbf{x}}^-(k) = \mathbf{A}_d\hat{\mathbf{x}}(k-1) + \mathbf{B}_d\mathbf{u}(k-1), \tag{9}$$

where $\hat{\mathbf{x}}(k-1)$ is the estimated state of the previous step. Then the forecasted error covariance matrix is given by:

$$\mathbf{P}^-(k) = \mathbf{A}_d\mathbf{P}(k-1)\mathbf{A}_d^T + \mathbf{Q}_n(k-1), \tag{10}$$

where $\mathbf{P}(k-1)$ is the estimated error covariance matrix of the previous step. The observation innovation residual $\mathbf{d}(k)$ is given by:

$$\mathbf{d}(k) = \mathbf{y}_{rd}(k) - \mathbf{C}\hat{\mathbf{x}}^-(k), \tag{11}$$

where $\mathbf{y}_{rd}(k)$ is the dequantized and demodulated output sequence. The Kalman gain matrix can be written as:

$$\mathbf{K}(k) = \mathbf{P}^-(k)\mathbf{C}^T[\mathbf{C}\mathbf{P}^-(k)\mathbf{C}^T + \mathbf{R}_w(k)]^{-1}. \tag{12}$$

The updated state estimation is given by:

$$\hat{\mathbf{x}}(k) = \hat{\mathbf{x}}^-(k) + \mathbf{K}(k)\mathbf{d}(k). \tag{13}$$

Finally, the updated estimate error covariance matrix $\mathbf{P}(k)$ is expressed as follows:

$$\mathbf{P}(k) = \mathbf{P}^-(k) - \mathbf{K}(k)\mathbf{C}\mathbf{P}^-(k). \tag{14}$$

After estimating the system state, the proposed control strategy is applied for regulating the system states.

The simulation result in the next section shows that the proposed estimation technique is able to accurately estimate the system state. Thus, according to the separation principle [28, p. 427], we can implement the control law $\mathbf{u}(k) = \mathbf{F}\hat{\mathbf{x}}(k)$ [29], where $\mathbf{F}$ can be obtained from solving the following state feedback problem [29], [30], [31]:

$$\mathbf{u}(k) = \mathbf{F}\mathbf{x}(k), \tag{15}$$

by minimizing the following objective function:

$$J = \sum_{k=0}^{\infty}[\mathbf{x}'(k)\mathbf{Q}_z\mathbf{x}(k) + \mathbf{u}'(k)\mathbf{R}_z\mathbf{u}(k)]. \tag{16}$$

Here $\mathbf{F}$ is the state feedback gain matrix, $\mathbf{Q}_z$ and $\mathbf{R}_z$ are positive-definite state weighting matrix and control weighting matrix. By using (15) and the standard trace operator, (16) can be expressed as:

$$
\begin{aligned}
J =& \sum_{k=0}^{\infty} tr[\mathbf{Q}_z \mathbf{x}(k)\mathbf{x}'(k) + \mathbf{F}'\mathbf{R}_z\mathbf{F}\mathbf{x}(k)\mathbf{x}'(k)] \\
=& \sum_{k=0}^{\infty} tr[\mathbf{Q}_z + \mathbf{F}'\mathbf{R}_z\mathbf{F}]\mathbf{x}(k)\mathbf{x}'(k) \\
=& tr[\mathbf{Q}_z + \mathbf{F}'\mathbf{R}_z\mathbf{F}]\mathbf{P},
\end{aligned} \tag{17}
$$

where $\mathbf{P} = \sum_{k=0}^{\infty}[\mathbf{x}(k)\mathbf{x}'(k)]$ and it can be written as follows:

$$
\begin{aligned}
\mathbf{P} =& \sum_{k=0}^{\infty}[\mathbf{x}(k)\mathbf{x}'(k)] \\
=& \sum_{k=0}^{\infty} \mathbf{x}(k+1)\mathbf{x}'(k+1) + \mathbf{x}(0)\mathbf{x}'(0) \\
=& \sum_{k=0}^{\infty} (\mathbf{A}_d + \mathbf{B}_d\mathbf{F})\mathbf{x}(k)\mathbf{x}'(k)(\mathbf{A}_d + \mathbf{B}_d\mathbf{F})' + \mathbf{x}(0)\mathbf{x}'(0).
\end{aligned} \tag{18}
$$

Now (18) can be written as follows:

$$\mathbf{P} = (\mathbf{A}_d + \mathbf{B}_d\mathbf{F})\mathbf{P}(\mathbf{A}_d + \mathbf{B}_d\mathbf{F})' + \mathbf{x}(0)\mathbf{x}'(0), \tag{19}$$

whose feasibility is equivalent to

$$
\begin{aligned}
&(\mathbf{A}_d + \mathbf{B}_d\mathbf{F})\mathbf{P}(\mathbf{A}_d + \mathbf{B}_d\mathbf{F})' - \mathbf{P} + \mathbf{x}(0)\mathbf{x}'(0) \leq \mathbf{0}, \\
&(\mathbf{A}_d + \mathbf{B}_d\mathbf{F})\mathbf{P}\mathbf{P}^{-1}\mathbf{P}(\mathbf{A}_d + \mathbf{B}_d\mathbf{F})' - \mathbf{P} + \mathbf{x}(0)\mathbf{x}'(0) \leq \mathbf{0}.
\end{aligned} \tag{20}
$$

By introducing a new variable $\mathbf{H} = \mathbf{F}\mathbf{P}$, (20) can be rewritten as follows:

$$(\mathbf{A}_d\mathbf{P} + \mathbf{B}_d\mathbf{H})\mathbf{P}^{-1}(\mathbf{A}_d\mathbf{P} + \mathbf{B}_d\mathbf{H})' - \mathbf{P} + \mathbf{x}(0)\mathbf{x}'(0) \leq \mathbf{0}. \tag{21}$$

Now according to the Schur's complement, (21) can be transformed into the following form:

$$\begin{bmatrix} \mathbf{x}(0)\mathbf{x}'(0) - \mathbf{P} & \mathbf{A}_d\mathbf{P} + \mathbf{B}_d\mathbf{H} \\ (\mathbf{A}_d\mathbf{P} + \mathbf{B}_d\mathbf{H})' & -\mathbf{P} \end{bmatrix} \leq \mathbf{0}. \tag{22}$$

In order to avoid repeating the optimization procedure for every $\mathbf{x}(0)$, in the following, we attempt to find a mild condition which ensures the validity of (22) for any initial condition $\mathbf{x}(0)$.

Suppose $\mathbf{x}(0)\mathbf{x}'(0) \leq \alpha\mathbf{I}$, where α is a positive scalar number. Thus, (22) is sufficed if

$$(\mathbf{A}_d + \mathbf{B}_d\mathbf{F})\mathbf{P}(\mathbf{A}_d + \mathbf{B}_d\mathbf{F})' - \mathbf{P} + \alpha\mathbf{I} \leq \mathbf{0}. \tag{23}$$

For (23), if $\gamma > 0$ we have:

$$(\mathbf{A}_d + \mathbf{B}_d\mathbf{F})\gamma\mathbf{P}(\mathbf{A}_d + \mathbf{B}_d\mathbf{F})' - \gamma\mathbf{P} + \gamma\alpha\mathbf{I} \leq \mathbf{0}. \tag{24}$$

By defining $\tilde{\mathbf{P}} = \gamma\mathbf{P}$ and $\gamma = 1/\alpha$, we have:

$$(\mathbf{A}_d + \mathbf{B}_d\mathbf{F})\tilde{\mathbf{P}}(\mathbf{A}_d + \mathbf{B}_d\mathbf{F})' - \tilde{\mathbf{P}} + \mathbf{I} \leq \mathbf{0}. \tag{25}$$

Note that $\mathbf{F}$ will not be affected by the scaling parameter γ, thus independent of any initial value $\mathbf{x}(0)$. So, for any initial value, (22) can be sufficed by solving the following linear matrix inequality:

$$\begin{bmatrix} -\tilde{\mathbf{P}} + \mathbf{I} & \mathbf{A}_d\tilde{\mathbf{P}} + \mathbf{B}_d\tilde{\mathbf{H}} \\ (\mathbf{A}_d\tilde{\mathbf{P}} + \mathbf{B}_d\tilde{\mathbf{H}})' & -\tilde{\mathbf{P}} \end{bmatrix} \leq \mathbf{0}, \tag{26}$$

where $\tilde{\mathbf{H}} = \mathbf{F}\tilde{\mathbf{P}}$. From (17), $\mathbf{F}$ and $\tilde{\mathbf{P}}$ can be found by minimising the following:

$$
\begin{aligned}
\underset{\tilde{\mathbf{P}},\mathbf{F}}{\text{minimize}} \quad & tr[\mathbf{Q}_z + \mathbf{F}'\mathbf{R}_z\mathbf{F}]\tilde{\mathbf{P}} \\
\text{subject to} \quad & (26).
\end{aligned} \tag{27}
$$

Based on $\tilde{\mathbf{H}} = \mathbf{F}\tilde{\mathbf{P}}$, (27) can be transformed as follows:

$$\underset{\tilde{\mathbf{P}},\mathbf{S},\tilde{\mathbf{H}}}{\text{minimise}} \qquad tr[\mathbf{Q}_z\tilde{\mathbf{P}}] + tr[\mathbf{S}] \tag{28}$$

$$
\begin{aligned}
\text{subject to} \qquad & \mathbf{S} > \mathbf{R}_z^{1/2}\tilde{\mathbf{H}}\tilde{\mathbf{P}}^{-1}\tilde{\mathbf{H}}'\mathbf{R}_z^{1/2} \\
& Hold\ (26).
\end{aligned} \tag{29}
$$

According to the Schur's complement, we can rewrite (29) as follows:

$$\begin{bmatrix} \mathbf{S} & \mathbf{R}_z^{1/2}\tilde{\mathbf{H}} \\ \tilde{\mathbf{H}}'\mathbf{R}_z^{1/2} & \tilde{\mathbf{P}} \end{bmatrix} > \mathbf{0}. \tag{30}$$

Finally, the proposed optimization problem can be formulated as follows:

$$
\begin{aligned}
\underset{\tilde{\mathbf{P}},\mathbf{S},\tilde{\mathbf{H}}}{\text{minimise}} \quad & tr[\mathbf{Q}_z\tilde{\mathbf{P}}] + tr[\mathbf{S}] \\
\text{subject to} \quad & Hold\ (26)\ and\ (30).
\end{aligned} \tag{31}
$$

So, the proposed feedback gain matrix is calculated as follows:

$$\mathbf{F} = \tilde{\mathbf{H}}\tilde{\mathbf{P}}^{-1}. \tag{32}$$

V. RESULTS AND DISCUSSION

The system parameters are given in Table I. Moreover, the considered cyber attack pattern is similar to the model in [6], [21], [22].

TABLE I: System parameters for smart grid information security problem.

Parameters	Values	Parameters	Values
$\mathbf{Q}_z$	$diag(10^{-2}, 10^{-2}, 10^{1}, 10^{-3})$	$\mathbf{R}_z$	$0.01 * \mathbf{I}_4$
Codes generator	$(13/15)_{octal}$	Δt	0.0001
Quantization	Uniform 16 bits	Decoding	SOVA
Code rate	$1/2$	Channel	AWGN
$\mathbf{Q}_n$	$0.0001 * \mathbf{I}_4$	$\mathbf{R}_w$	$0.001 * \mathbf{I}_4$

The performance is compared based on the mean squared error (MSE) between the true and estimated states. First of all, MSE versus signal-to-noise ratio (SNR) is depicted in Fig. 3. It can be seen that the proposed estimator provides better performance in contrast with the existing approach in [21]. This is due to the fact that the RSC code is able to protect impairments. Moreover, SOVA can also eliminate noises from the received signal. Secondly, the system state versus time step results are shown in Figs. 4–7. It can be seen that the estimator provides satisfactory performance. It can also be seen that attacks can worsen the accuracy of the system state estimation. The inaccuracy of estimated system states by existing method can directly deceive the utility engineer for taking suitable corrective control actions and dispatch decisions, which can lead to series of outages. In other words, the proposed communication infrastructure and estimation algorithm is well suited to provide real-time two-way communication and defend cyber attacks. Thirdly, the design control law is applied to the

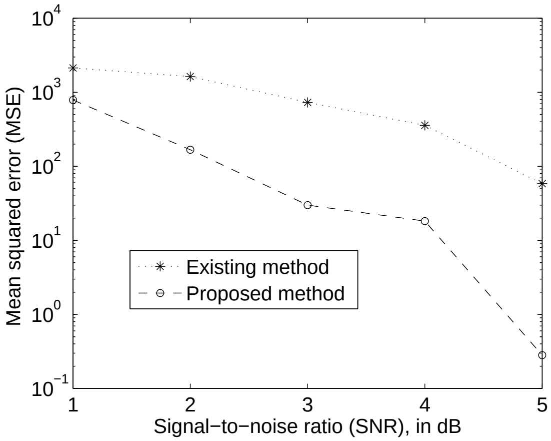

Fig. 3: MSE versus SNR comparison between proposed and existing method.

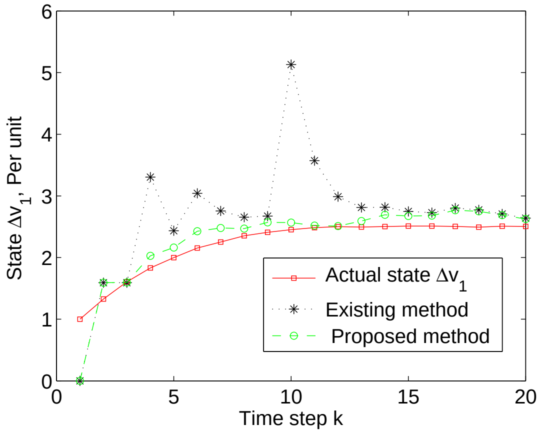

Fig. 4: Δv_1 comparison between true and estimate.

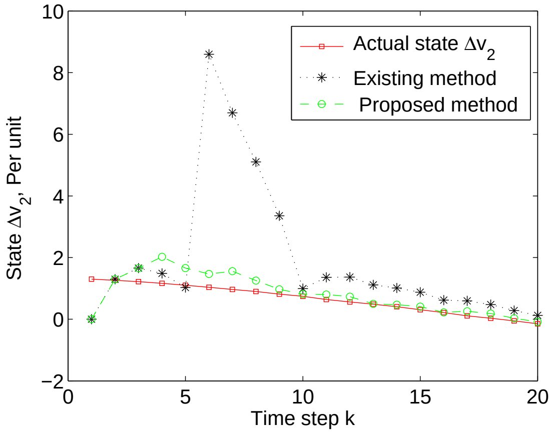

Fig. 5: Δv_2 comparison between true and estimate.

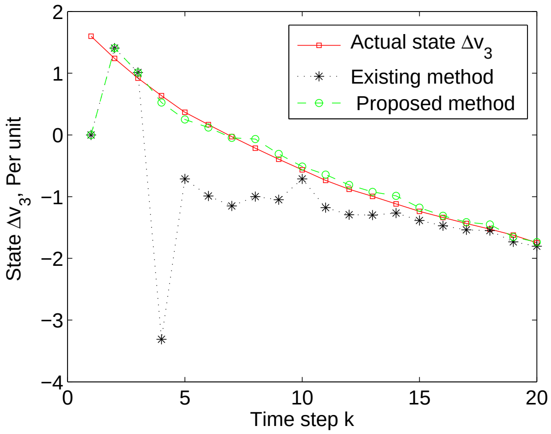

Fig. 6: Δv_3 comparison between true and estimate.

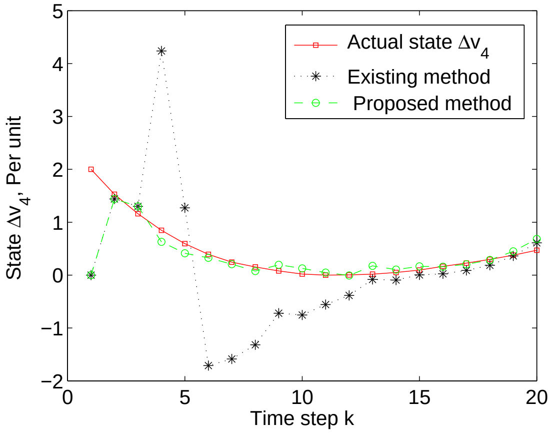

Fig. 7: Δv_4 comparison between true and estimate.

microgrid as its states dramatically increase over time. The outcome is illustrated in Fig. 8. It is observed that the controller needs about 0.03 seconds $(k \times \Delta t = 300 * 0.0001)$ to stabilize the system. Technically, it means that the developed approach requires much less time compared with the standard time $1-5$ seconds [32].

VI. Conclusion and Future Research

We have presented a centralized secure real-time monitoring infrastructure and control method that achieves the accurate state estimation and desired control performance. The numerical simulation results have shown that the proposed algorithm obtains better performance in contrast with the traditional method. In other words, adding redundancy in the system can mitigate the cyber attacks. Finally, the convex controller design is able to stabilize the system within only 0.03 seconds. Therefore, this framework will assist to design a green monitoring cyber physical system under the umbrella of smart grid communication systems. Developing an efficient and distributed state estimation to solve the cyber attack problem will be an interesting topic for the future smart grid research.

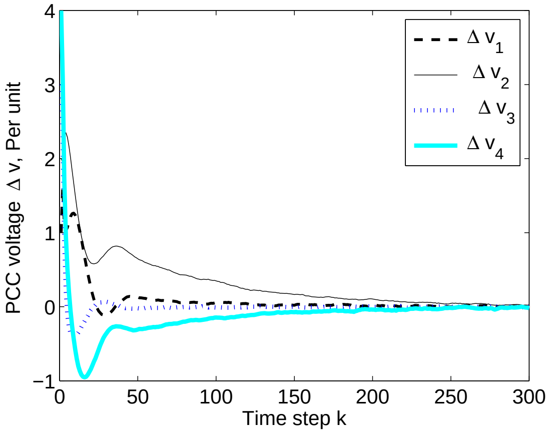

Fig. 8: Controlling the states trajectory.

References

[1] H. Li, F. Li, Y. Xu, D. T. Rizy, and J. D. Kueck, "Adaptive voltage control with distributed energy resources: Algorithm, theoretical analysis, simulation, and field test verification," *IEEE Transactions on Power Systems*, vol. 25, no. 3, pp. 1638–1647, 2010.

[2] A. Arefi, G. Ledwich, and B. Behi, "An efficient DSE using conditional multivariate complex Gaussian distribution," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 2147–2156, 2015.

[3] Y. Zhu, J. Yan, Y. Tang, Y. L. Sun, and H. He, "Joint substation-transmission line vulnerability assessment against the smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 5, pp. 1010–1024, 2015.

[4] K. C. Sou, H. Sandberg, and K. H. Johansson, "On the exact solution to a smart grid cyber-security analysis problem," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 856–865, 2013.

[5] J. Zhang and L. Sankar, "Implementation of unobservable state-preserving topology attacks," in *Proc. of the North American Power Symposium*. IEEE, 2015, pp. 1–6.

[6] S. Ntalampiras, "Detection of integrity attacks in cyber-physical critical infrastructures using ensemble modeling," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 1, pp. 104–111, 2015.

[7] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, 2012.

[8] A. Alimardani, F. Therrien, D. Atanackovic, J. Jatskevich, and E. Vaahedi, "Distribution system state estimation based on nonsynchronized smart meters," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 2919–2928, 2015.

[9] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in AC state estimation," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2476–2483, 2015.

[10] Y. Chakhchoukh and H. Ishii, "Cyber attacks scenarios on the measurement function of power state estimation," in *Proc. of the American Control Conference*. IEEE, 2015, pp. 3676–3681.

[11] ——, "Coordinated cyber-attacks on the measurement function in hybrid state estimation," *IEEE Transactions on Power Systems*, vol. 30, no. 5, pp. 2487–2487, 2015.

[12] A. Gaber, K. G. Seddik, and A. Y. Elezabi, "Joint estimation-detection of cyber attacks in smart grids: Bayesian and Non-Bayesian formulations," in *Proc. of the Wireless Communications and Networking Conference*, 2015, pp. 2245–2250.

[13] W. Cao, J. Lan, and X. R. Li, "Conditional joint decision and estimation with application to joint tracking and classification," *IEEE Transactions on Systems, Man, and Cybernetics: Systems, to appear in 2016*.

[14] J.-W. Jung, V. Q. Leu, T. D. Do, E.-K. Kim, and H. H. Choi, "Adaptive PID speed control design for permanent magnet synchronous motor drives," *IEEE Transactions on Power Electronics*, vol. 30, no. 2, pp. 900–908, 2015.

[15] R. Priewasser, M. Agostinelli, C. Unterrieder, S. Marsili, and M. Huemer, "Modeling, control, and implementation of DC-DC converters for variable frequency operation," *IEEE Transactions on Power Electronics*, vol. 29, no. 1, pp. 287–301, 2014.

[16] A. V. Sant and K. Rajagopal, "PM synchronous motor speed control using hybrid fuzzy-PI with novel switching functions," *IEEE Transactions on Magnetics*, vol. 45, no. 10, pp. 4672–4675, 2009.

[17] Y. Han, P. M. Young, A. Jain, and D. Zimmerle, "Robust control for microgrid frequency deviation reduction with attached storage system," *IEEE Transactions on Smart Grid*, vol. 6, no. 2, pp. 557–565, 2015.

[18] W.-M. Lin, C.-M. Hong, C.-H. Huang, and T.-C. Ou, "Hybrid control of a wind induction generator based on Grey–Elman neural network," *IEEE Transactions on Control Systems Technology*, vol. 21, no. 6, pp. 2367–2373, 2013.

[19] W.-M. Lin, K.-H. Lu, and T.-C. Ou, "Design of a novel intelligent damping controller for unified power flow controller in power system connected offshore power applications," *IET Generation, Transmission and Distribution*, vol. 9, no. 13, pp. 1708–1717, 2015.

[20] H. Li, L. Lai, and H. V. Poor, "Multicast routing for decentralized control of cyber physical systems with an application in smart grid," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 6, pp. 1097–1107, 2012.

[21] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Processing Letters*, vol. 22, no. 10, pp. 1652–1656, 2015.

[22] S. Li, Y. Yilmaz, and X. Wang, "Quickest detection of false data injection attack in wide-area smart grids," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 2725–2735, 2015.

[23] S. A. Salinas and P. Li, "Privacy-preserving energy theft detection in microgrids: A state estimation approach," *IEEE Transactions on Power Systems, to apper in 2016*.

[24] C. Vladeanu and S. El Assad, *Nonlinear Digital Encoders for Data Communications*. John Wiley and Sons, 2014.

[25] Y. Jing, *A practical guide to error control coding using Matlab*. Boston, London: Artech house, 2010.

[26] F.-h. Huang, "Evaluation of soft output decoding for turbo codes," Ph.D. dissertation, Virginia Polytechnic Institute and State University, 1997.

[27] D. Simon, *Optimal state estimation: Kalman, H infinity, and nonlinear approaches*. New Jersey: John Wiley and Sons, 2006.

[28] M. Gopal, *Digital Control and State Variable methods Conventional and Neural-Fuzzy Control System*. New Delhi, India: McGraw-Hill, 2003.

[29] A. K. Singh, R. Singh, and B. C. Pal, "Stability analysis of networked control in smart grids," *IEEE Transactions on Smart Grid*, vol. 6, no. 1, pp. 381–390, 2015.

[30] K. Zhou, J. C. Doyle, and K. Glover, *Robust and optimal control*. Prentice Hall, New Jersey, USA, 1996, vol. 40.

[31] M. Fardad and M. R. Jovanovic, "On the design of optimal structured and sparse feedback gains via sequential convex programming," in *Proc. of the American Control Conference*, 2014, pp. 2426–2431.

[32] Y. Wang, P. Yemula, and A. Bose, "Decentralized communication and control systems for power system operation," *IEEE Transactions on Smart Grid*, December 2014.