Cyber Attack Protection and Control in Microgrids Using Channel Code and Semidefinite Programming

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*—The smart grid has been considered as a next-generation power system to modernize the traditional grid to improve its security, connectivity and sustainability. Unfortunately, the grid is susceptible to malicious cyber attacks, which can create serious technical, economical and control problems in power network operations. In contrast to the traditional cyber attack minimization techniques, this paper proposes a recursive systematic convolutional (RSC) code and Kalman filter based method in the context of microgrids. Specifically, the proposed RSC code is used to add redundancy in the microgrid states, and the log maximum a posterior is used to recover the state information which is affected by random noises and cyber attacks. Once the estimated states are obtained, a semidefinite programming based optimal feedback controller is proposed to regulate the system states. Test results show that the proposed approach can accurately mitigate the cyber attacks and properly estimate and control the system states.**

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

I. Introduction

The smart grid can provide an efficient way of supplying and consuming energy by providing two-way energy flow and communication [1]. It can integrate multiple renewable distributed energy resources (DERs) which are environment friendly, low green house emission and effective to alleviate transmission power losses. The associated connectivity and advanced information/communication infrastructure make the smart grid susceptible to cyber attacks [1], [2]. Statistics in the energy sector show that more than 150 cyber attacks happened in 2013 and 79 in 2014 [1]. As a result, the power outage cost is about 80 billion per year in the USA. Usually, the utility operators amortize it by increasing the energy tariff, which is unfortunately transferred to consumer expenses [3]. The renewable microgrid incorporating DERs can be a potential solution, but it needs to be properly monitored as its generation pattern depends on the weather and surrounding conditions. One of the smart grid features is that it can integrate multiple microgrids and monitor them using reliable communication networks.

Since the generation pattern of a microgrid varies on the time-place basis so its operating condition should be closely monitored. Therefore, the microgrid state estimation is an important function in the smart grid energy management system (EMS). As shown in Fig. 1 system state estimation is an essential task for the monitoring and control of the power network. In order to monitor the grid information, the utility company is deployed a set of sensors around them. The communication infrastructure is used to send grid information from sensors to EMS. The accurately estimated states can also be used in other functions of EMS such as contingency analysis, bad data detection, energy theft detection, stability analysis, and optimal power dispatch [4].

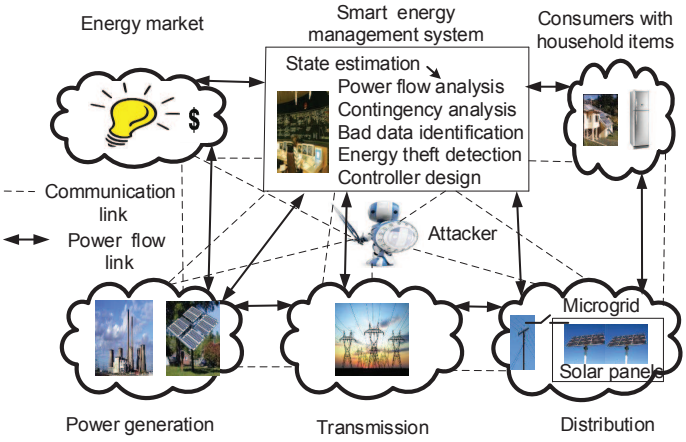

Fig. 1: Flow of electricity and information between different sections of smart grids [5].

Many studies have been carried out to investigate the cyber attacks in smart grid state estimations. To begin with, most of the state estimation methods use the weighted least squared (WLS) technique under cyber attacks [6], [7], [8]. Chi-Square detector is also used to detect those attacks. Even though this approach is easy to be implemented for non-linear systems, it is computationally intensive and it can not eliminate the attacks properly [6], [5]. To this end, the WLS based l_1 optimization method is explored in [4]. Furthermore, a new detection scheme to detect the false data injection attack is proposed in [9]. It employs a Kullback-Leibler method to calculate the distance between the probability distributions derived from the observation variations. A sequential detection of false data injection in smart grids is investigated in [2]. It adopts a centralized detector based on the generalized likelihood ratio and cumulative sum algorithm. Note that this detector usually depends on the parametric inferences so is inapplicable to the nonparametric inferences [9]. Thereafter, a Kalman filter (KF) based microgrid energy theft detection algorithm is presented in [3].

Many feedback control algorithms have been proposed to regulate the system states. The most established approach is

the linear quadratic regulator (LQR) method [10], [11], [12]. It is shown in [13], [14] that designing a state feedback controller framework for a general case of polynomial discrete-time system is quite challenging because the solution is nonconvex. Thus, the convex method based controller design has gained growing interest in the research communality. Driven by the aforementioned motivations, this paper proposes a recursive systematic convolutional (RSC) code and KF based cyber attack minimization technique in the context of microgrids. The key contributions of this paper are summarized as follows:

- A microgrid incorporating multiple DERs is modelled as a discrete time linear state-space equation considering the uncertainty and cyber attack in the measurement.
- An RSC code is proposed to mitigate the impairments and introduce redundancy in the system states. The log maximum a posterior is adopted to recover the state information which is affected by random noises and cyber attacks.
- After estimating the system states, a feedback control strategy for voltage regulation of the microgrid is proposed based on semidefinite programming. This proposed control scheme acts as a precursors in term of network stability and the operation of DERs.

II. Microgrid system model

A microgrid is a small-scale power network that can operate independently or be connected to the main grid. The considered N micro-sources in this study are connected to the main grid. For simplicity, we assume that N=4 solar panels are connected through the IEEE-4 bus test feeder as shown in Fig. 2 [15], [16]. Here the input voltages are denoted by

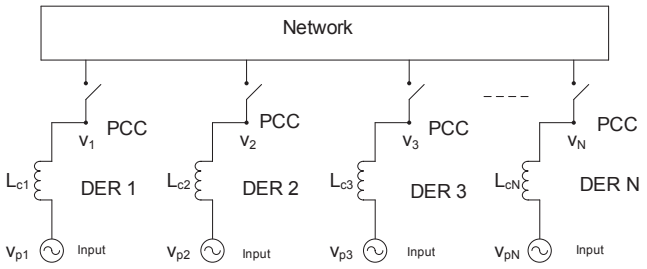

Fig. 2: Micro-sources are connected to the network [16].

the $\mathbf{v}_p = (v_{p1}\ v_{p2}\ v_{p3}\ v_{p4})^T$, where v_{pi} is the i-th DER input voltage. The four micro-sources are connected to the power network at the corresponding Points of Common Coupling (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 by applying Laplace transformation, the nodal voltage equation can be obtained:

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

where $\mathbf{L}_c = diag(L_{c_1},\ L_{c_2},\ L_{c_3},\ L_{c_4})$ 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 [16], the admittance matrix is given in (2). Now we can convert the transfer function form into the linear state-space model [16]. The discrete-time linear dynamic 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 whose 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.

III. Observation model and cyber attack

The measurements of the microgrid states are obtained by a set of sensors and can be modelled 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 $\mathbf{w}(k)$ is the zero mean sensor measurement noise whose covariance matrix is $\mathbf{R}_w$. Generally, the objective of attackers is to insert false data into the observations 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 [1], [2], [3]. The attackers have complete accesses to the system infrastructure so that they can hijack, record and manipulate data according to their best interest. In this paper, the cyber attack pattern is similar to those illustrated in [1], [2], [17]. Figure 3 shows the observation model and cyber attack process in the context of microgrid state estimations.

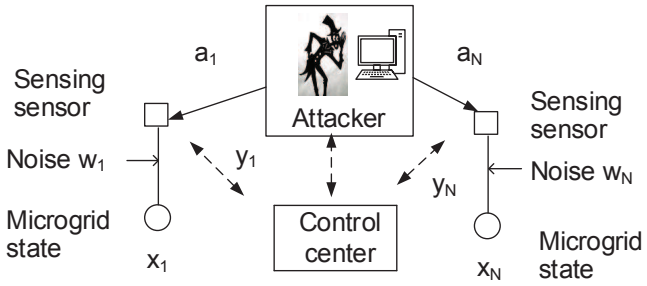

Fig. 3: Observation model with cyber attack in the microgrid.

To secure the system states, in the signal processing research community, the channel code is used. Motivated by the convolutional coding concept [18], [19], the microgrid state-space and observation models are regarded as the outer code.

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

Then the standard uniform quantizer performs quantization to get the sequence of bits $\mathbf{b}(k)$. $\mathbf{b}(k)$ is encoded by RSC channel code which is regarded as the inner code. Generally speaking, 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. This paper considers a (2, 1, 3) RSC code and (1 0 1, 1 1 1) code generator polynomial in the feedback process. As shown in Fig. 4, this RSC code produces two outputs and can convert an entire data stream into one single codeword. The codeword is then passed through the binary phase shift keying (BPSK) to obtain $\mathbf{s}(k)$. $\mathbf{s}(k)$ is passed through the additive white Gaussian noisy (AWGN) channel with some noise. To illustrate, Fig. 4 shows the proposed cyber attack protection procedure in the context of microgrids. At the

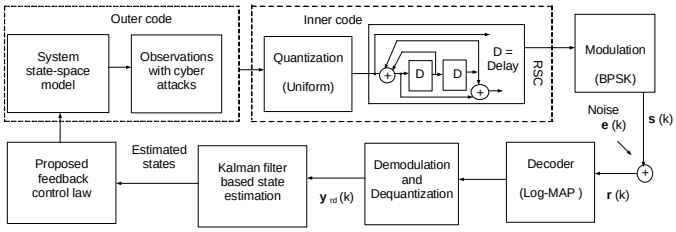

Fig. 4: An illustration of the cyber attack protection in microgrids.

end, the received signal is:

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

where $\mathbf{e}(k)$ is the AWGN noise. The received signal is followed by the log-maximum a posteriori (Log-MAP) decoding for this dynamic system. The Log-MAP works recursively from the forward path to the backward path to recover the state information [18]. The Log-MAP output is sent to demodulation and de-quantization and then finally used by the state estimation method.

IV. Proposed framework for cyber attack minimization in microgrids

Generally, the forecasted system state estimate is expressed as follows [20]:

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

where $\hat{\mathbf{x}}(k-1)$ is the estimated state of the last 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 last 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 bit 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 estimated 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 microgrid states. In order to regulate the microgrid states, define the following feedback control law [10], [11], [12]:

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

by minimizing the following cost 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 standard trace operator $(m'Dn = tr[Dnm'])$, (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:

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

whose feasibility is equivalent to

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

It can be observed that the (20) is nonlinear because it involves the multiplication of variables $\mathbf{P}$ and $\mathbf{F}$. This prevents a straightforward application of linear matrix inequality. Fortunately, one can introduce a new variable $\mathbf{H} = \mathbf{F}\mathbf{P}$ and rewrite the (20) as follows:

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

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

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

From (17), $\mathbf{F}$ and $\mathbf{P}$ can be found by minimising the following expression:

$$\begin{aligned}&\underset{\mathbf{P},\mathbf{F}}{\text{minimize}} \quad tr[\mathbf{Q}_z + \mathbf{F}'\mathbf{R}_z\mathbf{F}]\mathbf{P}\\ &\text{subject to} \quad (22).\end{aligned} \quad (23)$$

Based on the $\mathbf{H} = \mathbf{F}\mathbf{P}$, (23) can be transformed as follows:

$$\underset{\mathbf{P},\mathbf{S},\mathbf{H}}{\text{minimise}} \quad tr[\mathbf{Q}_z\mathbf{P}] + tr[\mathbf{S}] \quad (24)$$

$$\text{subject to} \quad \mathbf{S} > \mathbf{R}_z^{1/2}\mathbf{H}\mathbf{P}^{-1}\mathbf{H}'\mathbf{R}_z^{1/2} \quad (25)$$
$$Hold\ Eq.\ (22).$$

According to the Schur's complement, we can rewrite (25) as follows:

$$\begin{bmatrix}\mathbf{S} & \mathbf{R}_z^{1/2}\mathbf{H}\\ \mathbf{H}'\mathbf{R}_z^{1/2} & \mathbf{P}\end{bmatrix} > \mathbf{0}. \quad (26)$$

We can finally formulate the proposed optimization problem as follows:

$$\begin{aligned}&\underset{\mathbf{P},\mathbf{S},\mathbf{H}}{\text{minimise}} \quad tr[\mathbf{Q}_z\mathbf{P}] + tr[\mathbf{S}]\\ &\text{subject to} \quad Hold\ Eq.\ (22), Hold\ Eq.\ (26).\end{aligned} \quad (27)$$

Finally, the feedback gain matrix is computed as:

$$\mathbf{F} = \mathbf{H}\mathbf{P}^{-1}. \quad (28)$$

The performance of the proposed method is analysed in the next section.

V. Performance evaluation

The simulation parameters are summarized in Table I. The mean squared error (MSE) versus signal-to-noise ratio (SNR) is presented in Fig. 5. It can be observed that the proposed method significantly outperforms the existing KF method [1]. For better visualization of the cyber attack, the state (Δv_1 and Δv_2) versus time step results are illustrated in Figs. 6–7[1]. It can be observed and expected that the cyber attack enormously affects the system states when KF filter is used to estimate system states [1]. In other words, there is a significant fluctuation due to the random noises and cyber attacks. Interestingly, the proposed RSC based cyber attack protection technique can regulate the system impairments by introducing redundancy and protection in the system states. As a result, the proposed method can estimate microgrid states accurately even if there is cyber attacks and noises.

[1]Other states have similar estimation performance.

TABLE I: The parameters for the simulation using Matlab.

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	$5/7$	Δt	0.0001
Quantization	Uniform 16 bits	Decoding	Log-MAP
Code rate	$1/2$	Channel	AWGN
$\mathbf{Q}_n$	$0.005 * \mathbf{I}_4$	$\mathbf{R}_w$	$0.05 * \mathbf{I}_4$

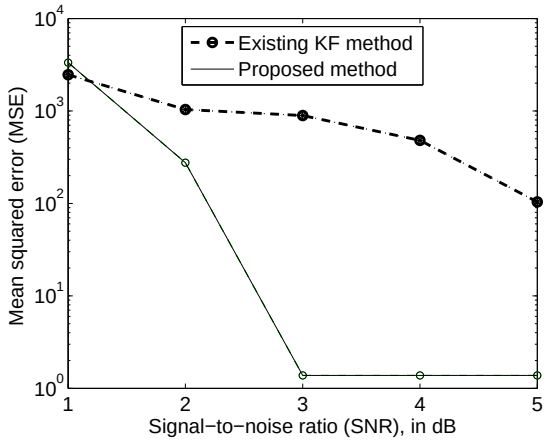

Fig. 5: MSE versus SNR performance comparison.

Unfortunately, it is noticed that the actual PCC state deviations increase dramatically, which is very dangerous in terms of network stability and microgrid operation. Thus, it is necessary to apply a suitable control technique, so that the PCC voltage deviations are driven to zero. After applying the proposed control method to the microgrid connected to the IEEE 4-bus distribution system, it can be seen from Fig. 8 that the proposed controller is able to keep the voltage deviations to zero by the time k=100, which acts as a precursor in terms of network stability and proper operation of microgrids.

VI. Conclusion

This paper proposes a cyber attack minimization based dynamic state estimation technique and feedback control algorithm in microgrids. An RSC coded cyber attack protection technique is proposed to add redundancy in the system states. Then a Log-MAP decoding can assist to extract the system states from the received signal which is polluted by random noises and cyber attacks. In order to regulate the voltage deviation, this study proposes an semidefinite programming based optimal feedback control method. The effectiveness of the developed approaches is verified by numerical simulations. These findings can help to design the future smart control center under cyber attacks. Consequently, it is encouraged to use environment-friendly renewable microgrid and the utility

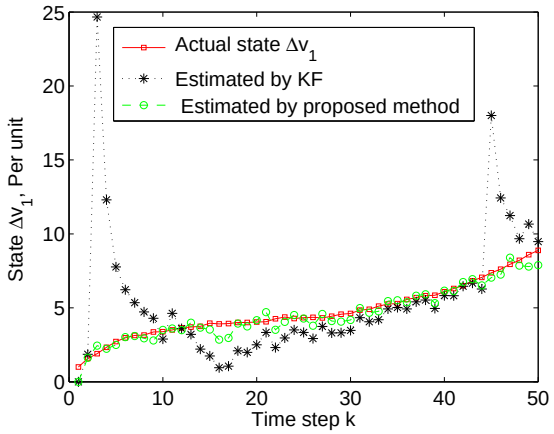

Fig. 6: State trajectory of Δv_1 and its estimate.

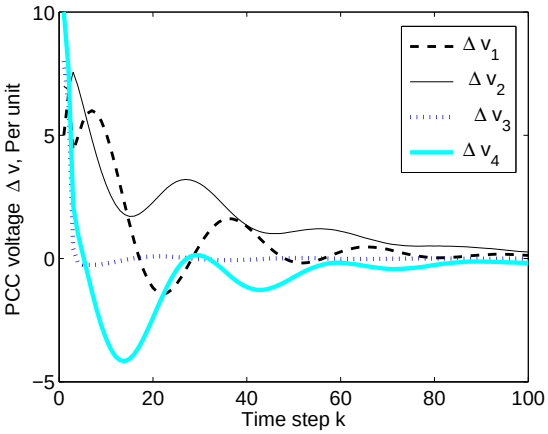

Fig. 8: Controlling the states trajectory.

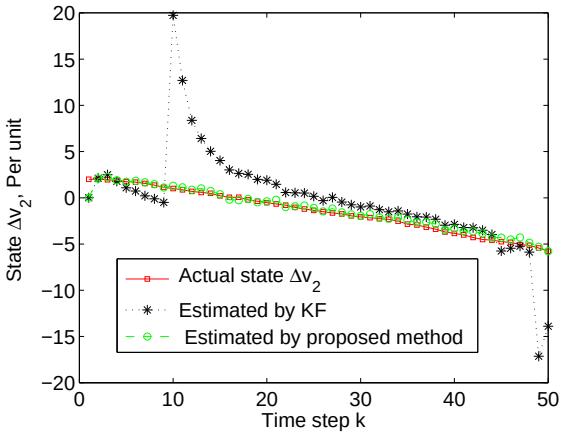

Fig. 7: State trajectory of Δv_2 and its estimate.

operator can monitor and control the power network properly. In the future work, packet losses and delay will be investigated in terms of system performance.

REFERENCES

[1] 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.

[2] 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.

[3] 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*.

[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] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 160–169, 2013.

[6] 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.

[7] 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.

[8] S. Meliopoulos, R. Huang, E. Polymeneas, and G. Cokkinides, "Distributed dynamic state estimation: Fundamental building block for the smart grid," in *Proc. of the Power and Energy Society General Meeting*, 2015, pp. 1–6.

[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] 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.

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

[12] 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.

[13] S. Saat, S. K. Nguang, J. Wu, and G. Zeng, "Disturbance attenuation for a class of uncertain polynomial discrete-time systems: an integrator approach," in *Proc. of the International Conference on Control Automation Robotics and Vision*, 2012, pp. 787–792.

[14] N. Azman, S. Saat, and S. K. Nguang, "Nonlinear observer design with integrator for a class of polynomial discrete-time systems," in *Proc. of the International Conference on Computer, Communications, and Control Technology*, 2015, pp. 422–426.

[15] 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.

[16] 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.

[17] 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.

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

[19] S. Gong, H. Li, L. Lai, and R. C. Qiu, "Decoding the nature encoded messages for distributed energy generation control in microgrid," in *Proc. of the International Conference on Communications*, 2011, pp. 1–5.

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