Detection of Stealthy attacks on Electric Grids Using Transient Analysis

James Ranjith Kumar R. and Biplab Sikdar
Department of Electrical and Computer Engineering
National University of Singapore
Email: jamesranjithkumar@u.nus.edu, bsikdar@nus.edu.sg

***Abstract*—The information which is transferred over supervisory control and data acquisition (SCADA) and by phasor measurement units (PMUs) in an electric grid is vulnerable to a variety of cyber attacks. In this paper, a technique is proposed to detect stealthy attacks that were injected on SCADA and PMU measurements. This technique uses the principle that any state change will be accompanied by a respective transient as the electric grid has its own inherent dynamics. Since SCADA is unable able to pick up such transients, Thevenin based equivalent has been used to conduct the transient analysis and compared against the PMU measurements. The proposed method has been tested on the IEEE 14-bus system and the results have been presented. It is shown that the proposed technique is able to detect the presence of attack even if both SCADA and PMU measurements have been compromised.**

***Index Terms*—AC State Estimation, Bad Data Detection, False Data Injection Attack, Smart Grid, SCADA, Transients**

I. Introduction

Computer networks of a typical electric grid play a vital role as they transport the essential data that is necessary for power system operation and control. This computer network is a part of SCADA systems which also contains remote terminal units (RTUs) which act as field devices and the control center where the monitoring and operation procedures are carried out. The control center houses the energy management system (EMS) package which comprises of various tools that can assist the operator in decision making. These communication networks used in electric grids have recently become a target for cyber attackers. Such attack are typically aimed at creating a power outage or to overload a equipment in the electric grid.

In the EMS package, the state estimator plays a major role as it gives the values of voltage magnitudes and angles at various buses using the measurements that are obtained from RTUs. Hence, the attacker's aim is to manipulate the measurements sent by RTUs such that the state estimator gives incorrect manipulated values of voltage magnitudes and angles. These manipulated values will be utilized by other EMS functionalities which will lead to wrong decision making results and it may cause financial losses or equipment damage. The initial work which studied such an attack scheme was given in [1] which shows that if the attack vector is a linear combination of the system matrix, then the classical bad data detection scheme can be bypassed. After that, various studies have been made with respect to false data injection attacks in electric grids [2].

PMUs have become quite popular in modern electric grids in the past decade as it can measure both magnitude and angle of bus voltages and line currents which are the state variables in the electric grid. Apart from this, the most important difference is that PMUs have much higher sampling rate than SCADA RTUs. However, many control centers still carry out the monitoring, operation and control of the electric grid through SCADA. This is due to the fact that PMUs may not be available across all the buses in the electric grid. These PMU measurements are also as vulnerable as SCADA measurements for false data injection attacks since the state variables can be directly manipulated in the case of PMUs.

False injection attacks have been studied on various aspects over the past few years. However, most of the research has been done on attacks on the DC power flow model [2]. Since this model is a linear approximation of the power balance equations, it may not represent the actual electric grid. Also, the computation power has increased tremendously over the years and a modern EMS has the capability of solving non-linear power balance equations (AC state estimation). Some of the research has been carried out in the area of false data injection attacks on non-linear power balance equations. It can be categorized into two parts. One part of the research focuses on the analyzing the impact of a false data injection attack on electric grids [3]–[7]. This part of research also helps to estimate how much the electric grid is susceptible to such attacks. Another part of the research develops counter measures for false data injection to protect the electric grid against such threats [8]–[10].

The detection mechanisms which have been developed in the literature assume that few of the measurements should not be compromised and they should act as a reference for detecting the presence of attack. To the best of our knowledge, there are no detection techniques that consider both SCADA and PMU measurements under false data attack. In this paper, we take this into account for our detection technique. The proposed method uses the fact that due to system dynamics, a transient will be present during every state change. If it is a malicious change of state induced in the data, then there will not be any corresponding transient.

This research is supported by the National Research Foundation, Prime Minister's Office, Singapore under its Corporate Laboratory@University Scheme, National University of Singapore, and Singapore Telecommunications Ltd.

The rest of this paper is organized as follows: the next section gives a background of false data injection attacks which is followed by the detailed description of the proposed method. After that, the results obtained using the proposed method in IEEE 14-bus system has been presented. Finally we conclude this paper with the future direction of this work.

II. Background

In this section, the background on stealthy attacks has been presented. This section describes the AC model which is used in state estimation and the classical bad data detection scheme. It is further followed by the attack model of load redistribution attacks that can bypass the bad data detection scheme.

A. State Estimation and Bad Data Detection

In a typical electric grid, RTUs transmit the values of line flows, bus injections and bus voltage magnitudes. These data are sent once in 2 to 5 seconds [11] through the SCADA network to the control center where it is utilized by the EMS. On the other hand, PMUs send the voltage and current phasors (both magnitudes and angles) of the buses where they are present through a separate communication channel with a high sampling rate around 50 to 120 measurements per second. Due to the presence of noise content in the SCADA measurements, the state of the electric grid (which is the voltage phasors of all the buses) is estimated by the state estimator. Modern day EMS have more computational power and hence the non-linear form of power balance equations has been used in the state estimator instead of linearizing them with certain assumptions. It is popularly termed as AC state estimation and the measurement model for such estimator can be given as

$$z = h(x) + e \tag{1}$$

where z is the measurement vector, x is the state vector, and e is the noise content that is present in the measurement. The function that maps the state vector to the true value of the measurement is given by $h(\cdot)$. Usually, the dimension of z will be greater than the dimension of x and hence it would be an over-determined system. The observability analysis in the EMS software package will ensure that the solution to be found by the state estimator should be an over-determined system. Since the state estimator solves for the weighted least square of the measurement residuals, the non-linear function $h(\cdot)$ can be solved using Gauss-Newton method iteratively as

$$x^{k+1} = x^k - G^{-1}(x^k)g(x^k) \tag{2}$$

where

$$G(x^k) = H^T(x^k)R^{-1}H(x^k) \tag{3}$$

$$g(x^k) = -H^T(x^k)R^{-1}\left(z - h(x^k)\right). \tag{4}$$

The matrix $H(x)$ is the Jacobian of the function $h(x)$ and its values will change with every iteration with the updated value of x. In a conventional EMS package, the inaccuracies in the measurements are handled by bad data detection technique. For this technique, the converged value of the state x will be used to calculate the residuals using the following expression

$$J(x) = \|z - f(x)\|_2 . \tag{5}$$

This residual value $J(x)$ is compared against the threshold t_J to verify the presence of any bad data in the measurement. This threshold value has been obtained from chi-square testing and if $J(x)$ violates this threshold value then an alarm will be triggered indicating that bad data is present in the measurement.

B. Threat Model

If the attacker is able to change the measurements without triggering the bad data detector then it is known as a stealthy attack. For modeling such attacks, the following assumptions of the attacker's abilities are considered:

1) The attacker has the information of all the parameters of the network and the values of measurements from all the RTUs.
2) The attacker has the ability to manipulate the values of the measurements in the RTUs at the target bus and all the buses adjacent to it.
3) The attacker has enough computational power to carry out the state estimation process.

Let x_a be the manipulated state vector which is intended by the attacker to be injected in the EMS computation process. To obtain this state vector, the measurement vector is manipulated to z_a in the following manner:

$$z_a = z + a \tag{6}$$

where the attack vector a can be written as

$$a = f(x_a) - f(x). \tag{7}$$

As the bad data detector uses residual value for the detection process, the attacker will aim to keep the residual unchanged even if the measurements are changed. The residual under this manipulated measurement can be given as

$$J(x_a) = \|z_a - f(x_a)\|_2 \tag{8}$$

$$= \|z + a - f(x_a)\|_2 \tag{9}$$

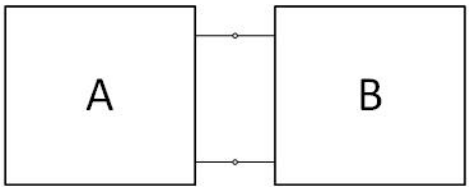
$$= \|z + f(x_a) - f(x) - f(x_a)\|_2 \tag{10}$$

$$= \|z - f(x)\|_2 = J(x). \tag{11}$$

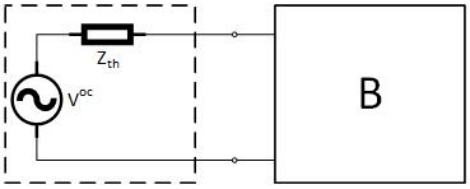
Thus, when the attacker uses the attack vector a for manipulating the measurements as given in (7), it will not change the residual value. Hence the threshold limit will not be violated and the bad data detector will not be able to detect this manipulation.

III. Proposed Detection Scheme

As shown in the previous section, stealthy attacks focus on manipulating each instance of measurement values. The proposed detection scheme considers a series of measurement values over a time span for detecting a stealthy attack. This section will explain the principle and the methodology of the detection scheme in detail.



(a) Original Network connection



(b) Network A transformed into its Thevenin equivalent

Fig. 1: Thevenin's Theorem

A. Transient Analysis using Thevenin's Model

A typical electric grid is composed of various elements among which the dominant ones are transmission lines, generators and loads. These elements, due to their inherent property, have significant amounts of resistance, inductance and capacitance. Due to these values, any change in the state will result in a transient which can be observed for a considerable duration before it reaches the steady state. The time domain specifications of such a transient will depend upon the initial condition, the amount of change imposed and the parameters of the elements that were present in the electric grid. Since the conventional electric grid are operated with AC supply, the initial condition of the system will depend upon the instance on the sine wave where the change of state was triggered.

In a false data injection attack, a different value of state is injected into a limited amount of RTUs in the SCADA measurement system. Any legitimate change in the measurement in a particular bus is a indication of change in state, and it will certainly induce transients across all the buses in the electric grid. Though RTUs cannot detect such transients, PMUs are able to pick them up as they have a sufficiently high sampling rate. However, it is difficult to correlate the PMU measurements with the state changes that are detected by the SCADA. The principle of the proposed detector is that if the attacker injects a stealthy attack, the transients cannot be observed in all the buses of the grid and with this (lack of) observation the presence of attack in the measurement can be detected. However, such an analysis is difficult since it is a computationally time consuming process and it requires highly sampled measurements in real time from all the buses which may not practically viable.

Thevenin's theorem is one of the most popular tools used in solving a variety circuit theory problems. Though this theorem is mostly attributed to Leon Charles Thevenin who postulated this theorem in 1883, it was basically first proposed by Hermann von Helmholtz in 1853. Thevenin's theorem is widely available in various circuit theory text books and the most common definition is available in [12]. For the purpose of revisiting this theorem, consider a linear network as shown in Figure 1. In this network, the voltage across element B has to be found and remaining part of the network is named as A. Thevenin's Theorem states that network A may be replaced with an equivalent circuit of a voltage source in series with the Thevenin's impedance. This voltage source is the open circuit voltage of network A with B disconnected and the Thevenin's impedance is the impedance looking back at the terminals of network A with all its independent sources being deactivated.

Though Thevenin's theorem is widely used in steady state analysis, it is shown in [13] that it can also be used to solve networks that involve transients. The only condition to be satisfied for solving such problems is that the open circuit voltage will not be dependent on the supply frequency. This condition will be satisfied in a typical electric grid as the time constants of automatic load frequency controllers in generators are much higher than the sampling time of PMUs. Hence by using Thevenin's theorem at the bus where a change in injection is detected, the transient response can be obtained by using the SCADA measurements which can be compared with the PMU measurements to detect the presence of an attack.

B. Methodology

Consider a n bus network where a state change is detected on bus i on the SCADA measurements. Let $Y \in \mathbb{C}^{n\times n}$ be the bus admittance matrix of the network including the reference bus. In order to find the Thevenin's impedance, the bus impedance matrix is found by

$$Z = (Y^{(j,j)})^{-1} \tag{12}$$

where $Y^{(j,j)}$ is part of Y in which the row and column corresponding to j were removed and j is the reference bus. The diagonal element in matrix Z that corresponds to the bus i is taken as the Thevenin's impedance Z_{th}. To find the open circuit voltage, the principle of superposition is used where the reference bus is considered as a voltage source and all the remaining buses are modeled as current sources. First, the voltage source at the reference bus is activated and the voltage at bus j needs to be calculated by keeping all other sources deactivated. Since transmission lines are modeled as π-sections, Y is invertible and the impedance matrix that includes the reference bus is calculated as

$$\hat{Z} = Y^{-1}. \tag{13}$$

Using the voltage divider rule, the voltage at bus j at this condition can be given as

$$V_1^{OC} = \frac{\hat{Z}(i,j)}{\hat{Z}(i,i)} v_j \tag{14}$$

where v_j is the value of voltage at the reference bus. In the next part, the voltage contribution due to the current sources are calculated. The bus impedance matrix Z can be expressed in the form of column vectors as

$$Z = \begin{bmatrix} z_1 & \cdots & z_{j-1} & z_{j+1} & \cdots & z_n \end{bmatrix}^T. \tag{15}$$

Let S_k and v_k be the complex power injection and the voltage phasor at bus k. The nodal power injections are modeled as current injections and it is given in the form of vector as

$$I = \begin{bmatrix} \mathbf{i}_1 & \cdots \mathbf{i}_{j-1} & \mathbf{i}_{j+1} & \cdots & \mathbf{i}_n \end{bmatrix}^T \tag{16}$$

where

$$\mathbf{i}_k = \begin{cases} 0 & \text{, for } k = i \\ \dfrac{S_k^*}{|v_k|^2} & \text{, otherwise} \end{cases}. \tag{17}$$

Finally, by the principle of superposition, the open circuit voltage at bus i for the Thevenin's equivalent can be given as

$$V^{OC} = V_1^{OC} + z_i I. \tag{18}$$

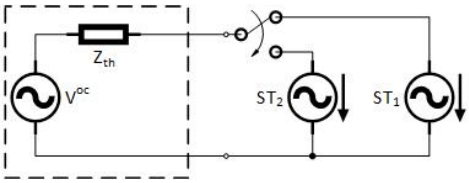


Fig. 2: Thevenin equivalent for Transient Analysis

With these calculated values of open circuit voltage and Thevenin's impedance, transient analysis can be carried out for the change in state which has been illustrated in Figure 2. Let ST_1 and ST_2 be the initial state and the final state that has been detected with the SCADA measurement. Considering that this change in state is a load change in bus i, both these states are modeled as current sources as

$$ST_1 = \frac{S1_i^*}{|v_i|^2} \tag{19}$$

$$ST_2 = \frac{S2_i^*}{|v_i|^2} \tag{20}$$

where $S1_i$ and $S2_i$ are the loads at bus i during initial state and final state, respectively. Since the circuit shown in Figure 2 is a simple network, electromagnetic transient program [14] has been used because it provides a simpler way for solving such transient problems. The results of this transient analysis are compared with the PMU measurements. If there is a significant difference between them, it indicates that a stealthy attack has been injected in the measurement.

IV. Results

The proposed detection technique is tested on IEEE 14-bus system as shown in Figure 3. The base solution of this 14-bus system has been obtained from MATPOWER [15]. In this test case, bus 9 is chosen as the target bus for the stealthy attack. Two scenarios have been created for testing the proposed detection scheme: no attack scenario and attack scenario. In both the scenarios, the load is changed from $0.1719 - 0.05528$i pu to $0.3135 - 0.1308$i pu from 0.2 to 0.4 seconds as shown in Figure 4.

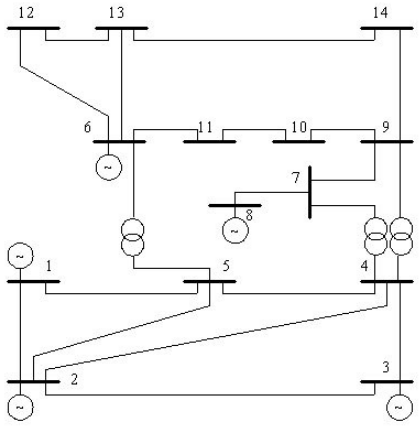


Fig. 3: IEEE 14-bus system.

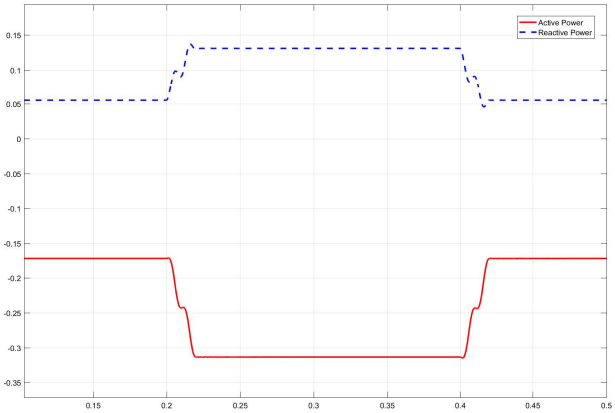


Fig. 4: Change in Power injection at Bus 9.

Since SCADA measurements have lower sampling rate, only the change in power injection is detected and it will not be able to capture the transients in the measurements. The test case is considered to be a 50 Hz electric grid and the PMU in bus 9 takes a sample once in every 0.02 seconds. The PMU measurements taken from bus 9 for attack and no attack scenarios are shown in Figure 5. It can be seen that in the no attack scenario, there are two ripples during the change in state. In the attack scenario, a trapezoidal shaped attack has been executed on the PMU measurements. In both the scenarios, it is difficult to correlate with the SCADA measurements to detect the presence of attack.

Using the proposed method, the Thevenin equivalent circuit is constructed and EMTP analysis is carried out on that circuit, and the results have been presented in Figure 6. It can be noticed that transient analysis from the Thevenin equivalent circuit provides a close approximation to the PMU measurement in the no attack scenario. As a part of detection mechanism, the error is calculated by taking the absolute value of the difference between the transient analysis results of the Thevenin's equivalent and the PMU measured values. The error under the no attack scenario and the attack scenario

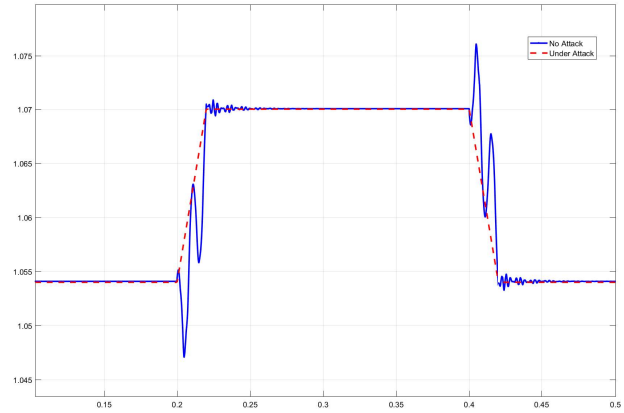


Fig. 5: PMU Voltage magnitude measurement at Bus 9 in attack and no attack scenarios.

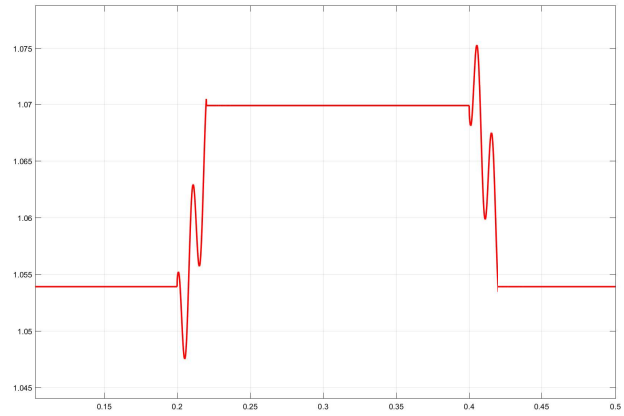


Fig. 6: RMS value of voltage from Thevenin's equivalent.

are shown in Figure 7. It is easy to see that the error in the no attack scenario is in the order of 10^{-4} whereas in the attack scenario it is in the order from 10^{-3} to 10^{-2}. Thus a clear threshold can be selected between these two ranges to detect any stealthy attack. It is to be noted that both SCADA and PMU measurements have been compromised and still the proposed method is able to detect the presence of stealthy attacks in the measurement.

V. Conclusion

In this paper, a new way of detecting stealthy attacks on SCADA and PMU measurements has been proposed. This method uses the system transients for detecting attacks and exploits the fact that transients will be absent for any state change resulting from data manipulation attacks. Instead of conducting transient analysis of the entire system, a Thevenin's equivalent was formed and EMTP is used to obtain the transients. These results are compared with the PMU measurements and if there is an attack present in the measurement, the error will cross the prescribed threshold limit. It has been shown that this technique can detect the presence of attacks even if both the SCADA and PMU measurements are compromised. This work will be further investigated in the future considering the

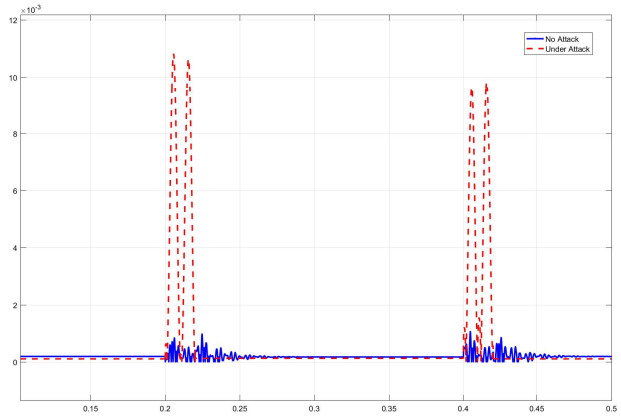


Fig. 7: Error under no attack and attack scenarios.

traveling wave effect in transmission lines and other control elements like automatic voltage regulators and automatic load frequency controllers.

References

[1] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 13:1–13:33, Jun. 2011.

[2] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems - attacks, impacts, and defense: A survey," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 411–423, April 2017.

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

[4] C. Konstantinou and M. Maniatakos, "A case study on implementing false data injection attacks against nonlinear state estimation," in *ACM Workshop on CPS Security and Privacy*, 2016, pp. 81–92.

[5] J. Zhao, G. Zhang, Z. Y. Dong, and K. P. Wong, "Forecasting-aided imperfect false data injection attacks against power system nonlinear state estimation," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 6–8, 2016.

[6] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 3864–3872, Sept 2016.

[7] X. Liu and Z. Li, "False data attacks against ac state estimation with incomplete network information," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2239–2248, Sept 2017.

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

[9] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1636–1646, May 2018.

[10] S. Pal, B. Sikdar, and J. Chow, "Classification and detection of pmu data manipulation attacks using transmission line parameters," *IEEE Trans. Smart Grid*, vol. PP, no. 99, pp. 1–1, 2017.

[11] C.-C. Sun, C.-C. Liu, and J. Xie, "Cyber-physical system security of a power grid: State-of-the-art," *Electronics*, vol. 5, no. 3, 2016.

[12] J. E. Brittain, "Thevenin's theorem," *IEEE Spectrum*, vol. 27, no. 3, pp. 42–, March 1990.

[13] W. Richter, "Applications of thevenin's theorem," *Electrical Engineering*, vol. 64, no. 3, pp. 103–105, March 1945.

[14] H. W. Dommel, "Digital computer solution of electromagnetic transients in single-and multiphase networks," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-88, no. 4, pp. 388–399, April 1969.

[15] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "Matpower: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb 2011.