Error Propagation after Reordering Attacks on Hierarchical State Estimation

Ammara Gul, Stephen Wolthusen

Chapter 4

ERROR PROPAGATION AFTER REORDERING ATTACKS ON HIERARCHICAL STATE ESTIMATION

Ammara Gul and Stephen Wolthusen

Abstract State estimation is vital to the stability of control systems, especially in power systems, which rely heavily on measurement devices installed throughout wide-area power networks. Several researchers have analyzed the problems arising from bad data injection and topology errors, and have proposed protection and mitigation schemes. This chapter employs hierarchical state estimation based on the common weighted-least-squares formulation to study the propagation of faults in intermediate and top-level state estimates as a result of measurement reordering attacks on a single region in the bottom level. Although power grids are equipped with modern defense mechanisms such as those recommended by the ISO/IEC 62351 standard, reordering attacks are still possible. This chapter concentrates on how an inexpensive data swapping attack in one region in the lower level can influence the accuracy of other regions in the same level and upper levels, and force the system towards undesirable states. The results are validated using the IEEE 118-bus test case.

Keywords: Power systems, hierarchical state estimation, reordering attacks

1. Introduction

Efficient and reliable supervisory control and data acquisition (SCADA) systems along with energy management systems (EMSs) contribute to the safe and efficient operation of power grids. A SCADA system located at a control center collects data from remote substations in order to manage the power grid. An energy management system at the control center processes the collected data using an on-line application called state estimation. State estimation enables an operator to obtain accurate estimates of the system state despite noisy or faulty measurement data using a steady state flow model of the physical system [1, 13].

Many energy management system applications (e.g., for contingency analysis) use the estimated system state, which makes accurate state estimation vital to safe and efficient power grid operations.

Modern power systems are becoming more interconnected and less likely to be dependent on a single control center for operations. Positioning operators throughout the system in a hierarchical or distributed structure improves operational efficiency. Each operator located at his/her own control center uses SCADA and emergency management systems to manage a certain region of the overall system. Examples of such interconnected systems are the ENTSO-E in Europe and Western Interconnect (WECC) in the United States. Future power systems are expected to be even more interconnected than before and, thus, systems without any central coordinators should be anticipated. The timely exchange of accurate information between regional operators is essential to maintaining the safety of a large interconnected power network. At the same time, data exchange is limited for reasons of sensitivity. This complicates the tasks of operators who use local state estimates for command and control in their regions, which, in turn, contribute to the estimated state of the entire system.

Hierarchical state estimation requires control centers at each level to exchange data regularly. The Inter-Control Center Communications Protocol (ICCP) is widely used to transmit information from one level to another during hierarchical state estimation. This protocol supports access control, but it does not provide key-based authentication for the exchanged data. Therefore standard protocols such as TLS as mandated by IEC 62351 are used to implement authentication for ICCP associations [6]. As a result, ICCP messages may be passed in the clear to the protocol stack to provide authentication. An adversary who installs a Trojan could compromise all incoming and outgoing ICCP messages [19]. The vulnerability of control systems to such attacks is exacerbated by the fact that ICCP relations are often formed between hosts in the various regions.

This chapter examines the conditions under which a compromised region in a lower level can have undesirable impacts on other regions in the same hierarchical level as a result of the propagation of faults to the top level and then back down to each level. Although an attacker can impact other regions by manipulating a single region, in reality, the magnitudes of the changes that can be induced are limited. This chapter determines a necessary condition that enables the formulation of a minimum cost attack to realize a maximum (negative) impact.

2. Related Work

The effects of bad data on state estimation in power systems have been studied extensively [14–16]. Typically, a bad data detection algorithm is executed during state estimation; this algorithm removes outliers based on simple statistical thresholds.

When the measurement data collected by a SCADA system is compromised, the resulting incorrect state estimation can force the system into an undesirable state. Without further constraints on data and data correlations, Liu et al. [12] have relied on DC power flows. Other studies have attempted to determine the minimal undetectable attacks that require the least manipulation of data [5, 10].

Van Cutsem and Ribbens-Pavella [18] were among the earliest researchers to focus on hierarchical state estimation; their seminal survey paper is still used to construct models. Lakshminarasimhan and Girgis [11] have proposed a two-level hierarchical state estimation for wide-area power systems that assumes a highly reliable phasor measurement unit (PMU) at every boundary bus. Vukovic and Dan [19] have described several types of data attacks on decentralized state estimation, but they do not provide details about the computational complexity. Moreover, their proposed mitigation scheme involving an outlier approach can detect errors only after hundreds of iterations and, even then, the attack may not be identified.

False data injection attacks, which were initially studied in the context of conventional state estimation, have been shown to be possible in hierarchical topologies as well [7]. Baiocco and Wolthusen [3] have employed automated (graph) partitioning to support robust hierarchical state estimation during unexpected failures of single or multiple lines, or attacks. Shepard et al. [17] have described GPS spoofing attacks on phasor measurement units, which can result in ill-conditioned Jacobian matrices and divergence by introducing jitter in the communications channels during hierarchical state estimation [2]. A number of state estimators have been proposed, but studies of robustness to attacks have focused on centralized topologies. However, Baiocco et al. [4] have discussed the hierarchical case in the context of smart grid and microgrid environments.

Gul and Wolthusen [9] have highlighted the vulnerability of a communications infrastructure to an attack that reorders measurement vectors, resulting in incorrect estimates and potentially undesirable system states. It is worth noting that Gul and Wolthusen assume that the preceding and present measurement vectors are known to the attacker. In the two distinct scenarios they analyzed, the system diverged as a result of an ill-conditioned Jacobian matrix.

3. Power System State Estimation

A power system is denoted by a graph $\mathcal{G}$ with a set of buses $\mathcal{V}$ and a set of transmission lines $\mathcal{E}$. An AC power flow model is assumed. This is expressed as:

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

where $\mathbf{z} \in R^m$ is the measurement vector; $\mathbf{x} \in R^n$ is the state vector ($m > n$); h is the measurement function relating $\mathbf{z}$ to $\mathbf{x}$; and $\mathbf{e}$ is the noise vector with a mean of zero and known co-variance $\mathbf{R}$. The errors are assumed to be independent; therefore, $\mathbf{R} = diag\{\sigma_1^2, \sigma_2^2, \cdots, \sigma_m^2\}$ is a diagonal matrix.

The states $\hat{\mathbf{x}}$ are estimated by solving the following normal equations:

$$[F^T R^{-1} F]\Delta\hat{\mathbf{x}} = F^T R^{-1}[\mathbf{x} - f(\mathbf{x})] \tag{2}$$

Following this, bad data analysis is performed based on the residual values:

$$\mathbf{r} = \mathbf{z} - h(\hat{\mathbf{x}}) \tag{3}$$

Residual values that are larger than a statistical threshold τ are identified and the corresponding measurements are flagged as bad. After the bad measurements are removed, state estimation is re-run until the system converges. Unfortunately, bad data detection is difficult when there are multiple bad measurements. In practice, bad data goes undetected due to the presence of other bad data, or good measurements are flagged as bad for other reasons such as a change to the topology. Interested readers are referred to [1] for more details about state estimation.

4. Hierarchical State Estimation

Conventional or centralized state estimation can be followed by a multi-region hierarchical procedure in which local state estimators process all the raw measurements that are available locally; thus, only manageable amounts of data are sent to the immediate higher level. This process continues upward until the highest level is able to compute the state of the entire system, which is then conveyed to the lower levels for crucial tasks such as bad data processing [8].

The multi-region hierarchical structure can be symmetric or asymmetric. A symmetric hierarchy has a balanced division of bus-bars/tie-lines over all the regions whereas an asymmetric hierarchy has an unbalanced distribution of bus-bars/tie-lines. While symmetric hierarchical state estimation is trivial, asymmetric hierarchical state estimation models real-world power systems, but is more complex. Only asymmetric hierarchical state estimation is considered in this work. The formulation is taken from [2, 4].

Baiocco et al. [4] have introduced a tree structure for multi-region hierarchical state estimation with the tree root (level k) denoting the highest level state estimation. A lower level may have child nodes; a lower level without child nodes is a leaf node and resides in the lowest level (level 1) of the hierarchy. Each node performs its own state estimation using measurements of the estimated states from lower nodes; for level 1, the measurements are obtained by computing power flows. It is assumed that robust partitioning is already performed and that there are no overlaps between regions, except for common tie-lines that connect neighboring regions.

When a node estimates its state vector, it sends this vector (including the gain matrix) to all its children or to the parent node. This type of multi-region hierarchical state estimation involves two-way transmission of information from the lower levels to the higher levels until the root node is reached, upon which the overall state estimate is sent downwards towards the leaf nodes so that the state estimate is passed to all the tie-line branches.

A general k-level multi-region hierarchical state estimation is expressed as:

$$\begin{aligned} y_{0,j_1} &= f_{1,j_1}(y_{1,j_1}) + e_{1,j_1}, \quad j_1 = 1, \cdots, r_1 \\ y_{0,b_1} &= f_{1,b_1}(y_1) + e_{1,b_1} \\ y_{1,j_2} &= f_{2,j_2}(y_{2,j_2}) + e_{2,j_2}, \quad j_2 = 1, \cdots, r_2 \\ y_{1,b_2} &= f_{2,b_2}(y_2) + e_{2,b_2} \\ &\vdots \\ y_{0,b_1} &= f_{1,b_1}(y_1) + e_{1,b_1} \end{aligned} \tag{4}$$

where y_{0,j_1} is the local measurement vector in S_{j1} in level 1; y_{0,b_1} is the border measurement vector in level 1; y_{1,j_2} is the local measurement vector in S_{j2} in level 2; y_{1,b_2} is the border measurement vector in level 2; y_k is the state vector of the overall system; f_l is the corresponding non-linear measurement function for each level l; and e_l is the corresponding Gaussian measurement noise vector.

Level 1 Multi-Region State Estimation. For level 1, each region S_j estimates its own state $\tilde{y}_{1j}$ by solving the following normal equations iteratively:

$$\begin{aligned} [F_{1,j_1}^T R_{1,j_1}^{-1} F_{1,j_1}] \Delta\tilde{y}_{1,j_1} &= F_{1,j_1}^T R_{1,j_1}^{-1} [y_{0,j_1} - f_{1,j_1}(y_{1,j_1}(k))] \\ [F_{1,b_1}^T R_{1,b_1}^{-1} F_{1,b_1}] \Delta\tilde{y}_{1,j_1} &= F_{1,b_1}^T R_{1,b_1}^{-1} [y_{0,b_1} - f_{1,b_1}(y_{1,j_1}(k))] \end{aligned} \tag{5}$$

where the inputs at this level include the measurement vectors y_{0,j_1} and y_{0,b_1}; Jacobian matrices $F_{1,j1}$ and $F_{1,b1}$; and gain matrices R_{1,j_1} and R_{1,b_1}. Note that the Jacobian matrices are updated at every iteration.

Level *i* Multi-Region State Estimation. The following equations must be solved for each intermediate level hierarchically from the lower levels:

$$\begin{aligned} &[F_{i,j_{i-1}}^T G_{i-1,j_{i-1}} F_{i,j_{i-1}}] \Delta\tilde{y}_{i-1,j_{i-1}}(k) = \\ &\qquad F_{i,j_{i-1}}^T G_{i-1,j_{i-1}} [\tilde{y}_{i-1,j_{i-1}} - f_{i,j_{i-1}}(y_i(k))] \\ &[F_{i,b_i}^T G_{i-1,b_{i-1}} F_{i,b_i}] \Delta\tilde{y}_{i-1}(k) = F_{1,b_1}^T G_{i-1,b_{i-1}} [\tilde{y}_{i-1} - f_i(y_i(k))] \end{aligned} \tag{6}$$

Using the estimate $\tilde{y}_{i-1,j_{i-1}}$ from level $l-1$ as the measurements in a distributed approach, $\tilde{y}_{i,j_i}$ can be obtained as described in [7]. The Jacobian matrices are revised based on the estimates from levels i and $i+1$.

Level l Multi-Region State Estimation. Using the vector $\tilde{y}_{l_1}$ supplied by the lower level $l-1$ as the measurement vector, the system state can be estimated by iteratively solving the following equations:

$$\begin{aligned}
&[F_{l,j_{l-1}}^T G_{l-1,j_{l-1}} F_{l,j_{l-1}}]\Delta\tilde{y}_{l-1,j_{l-1}}(k) = F_{l,j_{l-1}}^T G_{l-1,j_{l-1}}[\tilde{y}_{l-1,j_{l-1}} - f_{l,j_{l-1}}(y_l(k))] \\
&[F_{l,b_l}^T G_{l-1,b_{l-1}} F_{l,b_l}]\Delta\tilde{y}_{l-1}(k) = F_{1,b_1}^T G_{l-1,b_{l-1}}[\tilde{y}_{l-1} - f_l(y_l(k))]
\end{aligned} \tag{7}$$

Note that the hierarchical state estimation process outlined above requires two-way exchange of data between local state estimators in each layer of the hierarchy [2].

5. Three-Level Simplification

This section presents a simplification of the multilevel model as a three-level model. The three-level model is given by:

$$\begin{aligned}
y_{0,j_1} &= f_{1,j_1}(y_{1,j_1}) + e_{1,j_1}, \quad j_1 = 1,2 \\
y_{0,b} &= f_{1,b}(y_{1,b}) + e_{1,b} \\
y_{1,j_2} &= f_{2,j_2}(y_{2,j_2}) + e_{2,j_2}, \quad j_2 = 1,2 \\
y_{1,b} &= f_{2,b}(y_{2,b}) + e_{2,b} \\
y_2 &= f_3(x) + e_3
\end{aligned} \tag{8}$$

where the measurement vectors y_{0,j_1}, y_{1,j_1} and $y_{0,b}$, $y_{1,b}$; state vectors y_{1,j_1}, y_{2,j_2} and y_{b,j_1}, y_{b,j_2}; and non-linear measurement functions f_{1,j_1}, f_{2,j_2} and $f_{1,b}$, $f_{2,b}$ are as described above.

In order to simplify the process, it is assumed that there are no border variables and that the measurement functions are linear. The resulting three-level model is given by:

$$\begin{aligned}
y_{0j} &= F_{1j} y_{1j} + e_{1j}, \quad j = 1,2 \\
y_{1j} &= F_{2j} y_{2j} + e_{2j}, \quad j = 1,2 \\
y_2 &= F_3 x + e_3
\end{aligned} \tag{9}$$

where F_{1j}, F_{2j} and F_3 are the Jacobian matrices of the corresponding measurement functions.

For each region, state estimation employs an iterative algorithm that determines the local state vector along with another iterative process involving the two levels [7]:

- **Level 1:** The inputs to the first level are y_{1j} for regions $j = 1,2$ (assuming two regions) and the weighting matrix R_{1j}^{-1}. The output, which corresponds to the local state vector $\hat{y}_{1j}$ for each region, is obtained by solving the following normal equation iteratively for each region:

$$[F_{1j}^T R_{1j}^{-1} F_{1j}^T]\hat{y}_{1j} = F_{1j}^T R_{1j}^{-1} y_{0j} \tag{10}$$

- **Level 2:** The inputs to the second level are y_{1j} for regions $j = 1, 2$ (assuming two regions) and the weighting matrix R_{1j}^{-1}. The output, which corresponds to the local state vector $\hat{y}_{1j}$ for each region, is obtained by solving the following normal equation iteratively for each region:

$$[F_{2j}^T R_{2j}^{-1} F_{2j}^T]\hat{y}_{2j} = F_{2j}^T R_{2j}^{-1} y_{1j} \tag{11}$$

- **Level 3:** The inputs to the third level are the state vectors of the second level $\hat{y}_2$ and the gain matrices $G_2 = F_{1j}^T R_{2j}^{-1} F_{2j}^T$ (corresponding to the weighting matrix). The output $\hat{x}$, which is the state of the entire system, is obtained by solving the following normal equation for the third level:

$$[F_3^T G_2^{-1} F_3^T]\hat{x} = F_3^T G_2^{-1} \hat{y}_2 \tag{12}$$

  where y_2 and G_2 are obtained by juxtaposing the corresponding y_{2j} and G_{2j}, respectively.

6. Attack Model

The attacker's goal is to disrupt hierarchical state estimation. It is assumed that the attacker can reorder the measurement set $\mathbf{y}^0$ of only one partition $S^0 \in S$ in the lowest level l_1 of the hierarchy, where S is the set of partitions. As a result, incorrect state variables are transmitted to the partitions in the upper levels at the beginning of each hierarchical state estimation iteration.

The structured reordering attack leverages internal knowledge of the partitions in order to maximize its impact. The knowledge required for the success of the reordering attack includes some previous plausible measurement set $\mathbf{y}_{old}$ of the targeted partition. The principal goal of the attack is to have a false local state estimate that propagates to the higher levels to produce an incorrect estimate $\mathbf{x}$.

The following constraints are imposed on an attack on the three-level hierarchical structure:

- After the attack is launched on a single partition in level l_1, the data exchange between the upper two levels (i.e., l_2 and l_3) remains normal. This means that there is no further attack on the upper levels.

- The network configurations (i.e., sub-region partitioning) in levels l_2 and l_3 are not permitted to change over the course of a complete top-down synchro-upgrade. Note that this constraint is usually not imposed on hierarchical state estimation [2].

After the attack, the flow equation for the first level l_1 is:

$$[F_{1j}^T R_{1j}^{-1} F_{1j}^T]\hat{y}_{1j}^* = F_{1j}^T R_{1j}^{-1} y_{0j}^* \tag{13}$$

where y_{0j}^* is the swapped measurement vector of one of the sub-regions in level l_1. The inputs to the second level y_{1j}^* for regions $j = 1, 2$ are the false estimates

from the first level l_1:

$$[F_{2j}^T R_{2j}^{-1} F_{2j}^T]\hat{y}_{2j}^* = F_{2j}^T R_{2j}^{-1} y_{1j}^* \tag{14}$$

Finally, the output $\hat{x}^*$, which is the state of the entire system, is obtained by solving the following normal equation for the third level l_3:

$$[F_3^T G_2^{-1} F_3^T]\hat{x}^* = F_3^T G_2^{-1} \hat{y}_2^* \tag{15}$$

where y_2^* and G_2 are as defined above.

In the case of a false data injection attack, the symbol **a** denotes the attack vector that expresses the amount of change to the original measurement vector [12]:

$$\mathbf{a} = \mathbf{Fc} \tag{16}$$

where the vector **c** denotes the magnitude of change and is bounded by some stealthy condition.

Jamming or delay attacks can be seen as a sub-class of reordering attacks because they resend the previous data after a time interval. Also, attacks that replay or block measurement vectors can be considered to be a special case of reordering attacks with time constraints. The common aspect of all of these attacks is that no attack vector has to be added. Instead, the attacker simply drops/blocks a measurement or injects jitter in the measurement regardless of whether or not it is secure/protected by hacking the communications infrastructure. Therefore, the general term, "reordering of the measurement vector" is introduced to convey that the attacker replaces the true measurement vector with a previous plausible (true) vector.

In this case, the time horizon is critical to the attacker because it determines the strength of the attack. It is assumed that the attacker has measurement information from the present back to some point in time. From among these measurements, the attacker chooses the measurement vector to be swapped with the present measurement vector while continuing to maintain stealth. The term "stealth" implies that the attack is successful in forcing the system state without being detected by the model-based bad data detection algorithm. Sophisticated detection criteria certainly exist, but they are mainly used to determine which measurement devices (vector entries) are compromised, and, therefore, are not relevant to the case at hand. Other models rely on message redundancy to determine compromise, but this approach is not feasible for network-based attacks.

7. Reordering Attack Cost and Impact

The minimum attack cost Γ_y corresponds to the situation where the attacker expends the least effort to obtain the maximum mean square error (MSE). Power grid regions can be secured in one of the three ways: (i) non-tamperproof authentication ($S_{ntp} \subseteq S_m$); (ii) tamperproof authentication ($S_{tp} \subseteq S_m$); or (iii) other protection. Non-tamperproof authentication is implemented by a

bump-in-the-wire device or a remote terminal unit (RTU) with a non-tamperproof authentication module; regions with this type of authentication are only susceptible to attacks that involve physical access to the region from where the measurements originate. In contrast, tamperproof authentication is not susceptible to attacks. Other protection mechanisms include security guards and video surveillance systems that are generally not vulnerable to attacks. However, to be realistic, all the regions of a power grid cannot be protected and there will be at least one vulnerable region $S_{m'}$. If the region where the measurement vector is to be attacked is protected and uses non-tamperproof or tamperproof authentication, then the measurement is not vulnerable and it is assumed that $\Gamma_y = \infty$.

Otherwise, for a measurement y, Γ_y is defined as:

$$\begin{aligned} &\Gamma_y = \min \ \|a\| \ \ s.t. \ \ a = Fc = \hat{y}^{new} - \hat{y}^{old} \ \ \text{and} \\ &a(y) \neq 0 \Longrightarrow |S(m')| \neq 0, \ \ s.t. \ \ S = S(m) \cup S(m') \end{aligned} \tag{17}$$

where S_m denotes the authenticated regions; and $S_{m'}$ denotes the vulnerable regions such that $S = S(m) \cup S(m')$.

In addition, it is assumed that the attacker is free to choose the set of plausible measurements in a particular time frame to be used in a reordering attack. As a result of this freedom and the attack cost Γ_y mentioned above, the maximum attack impact is taken to correspond to the attacker's outcome $\mathcal{I}_y$, which is given by:

$$\begin{aligned} &\mathcal{I}_y = \max \ I = \sqrt{\sum (\tilde{y}^{new} - \tilde{y}^{old})^2} \\ &\text{s.t.} \ \ \ t^{new} - t^{old} \geqslant \epsilon \end{aligned} \tag{18}$$

where t is the time slot from among the time frames available to the attacker; and ϵ is a pre-defined threshold that limits the attacker's choice. The superscripts "old" and "new" denote the original measurement and the measurement to be inserted in its place, respectively.

8. Experimental Results

Before discussing the experimental results, it is important to recall that, in order to perform a reordering attack, the attacker must have knowledge of the system topology. It is assumed that the topology does not change or the topology is static for the duration of the attack.

This section evaluates the proposed model by considering reordering attacks on hierarchical state estimation involving regions of the standard IEEE 118-bus system. The IEEE 118-bus system is divided into six regions, and an intermediate level exists between the top and bottom levels (Figure 1).

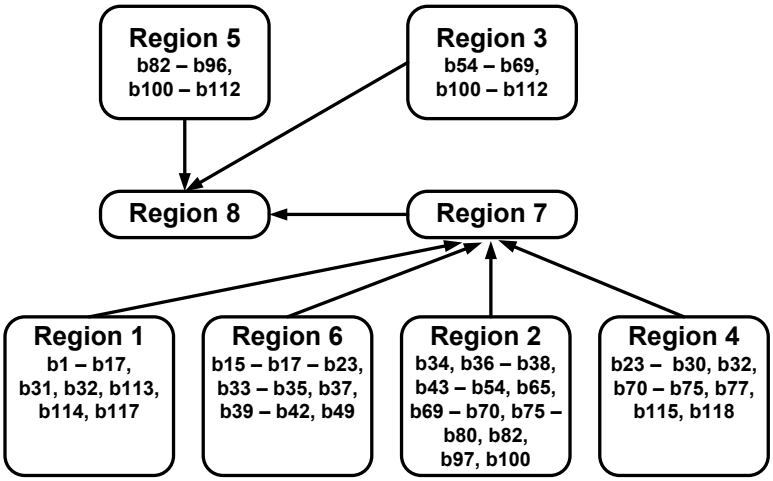

Figure 1. Bus-bar distribution in the IEEE 118-bus system.

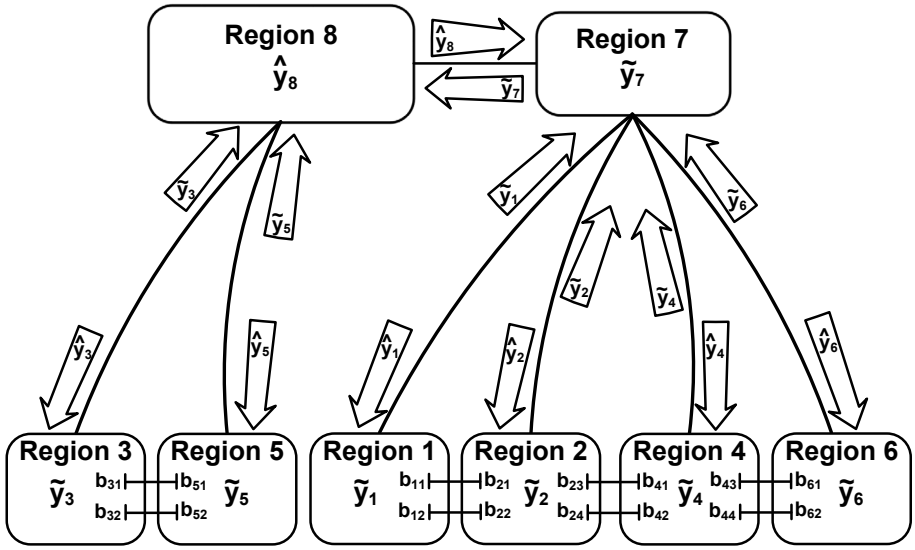

Figure 2. Information flow during hierarchical state estimation.

As shown in Figure 2, since the hierarchical model involves two-way synchro-upgrades (i.e., from the lower levels to the upper levels and subsequently from the topmost level down to the lower levels), it is particularly interesting to observe the error propagation after an attack. The attacker is free to choose data from a certain time frame (i.e., the attacker has a limited amount of knowl-

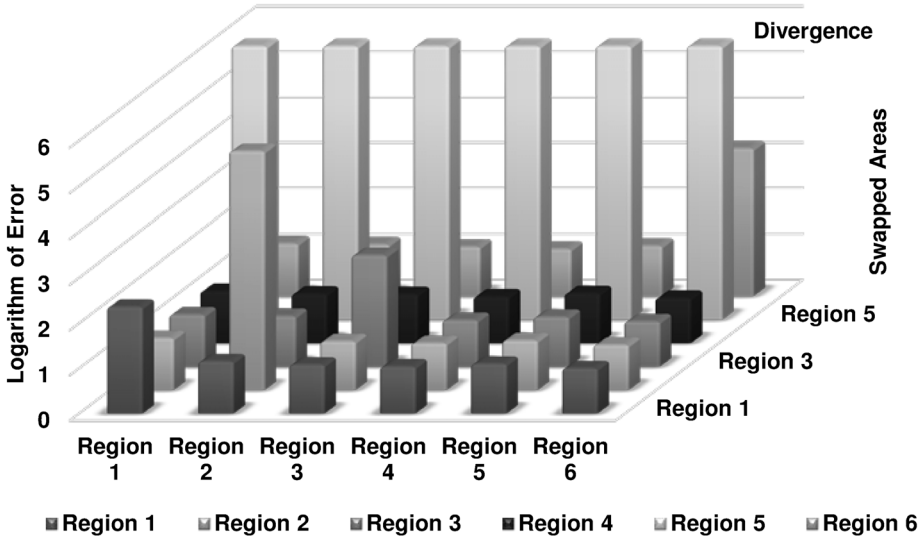

Figure 3. Impact of regionwise reordering in the lower level.

edge about the previous data). The weighted-least-squares (WLS) technique was used to estimate the state and the open-source MATPOWER package was used to load the data associated with the IEEE 118-bus system.

Figure 3 shows the mean squared error after performing least cost reordering attacks on the IEEE 118-bus system. The figure shows the logarithm (base 10) of the mean squared error for a complete round of the weighted-least-squares state estimation – from the lower layer to the top layer and all the way down, detailing how the error propagates up from the lowest level to the top level and back down.

It is clear that, at the end of a complete round after a reordering attack, all the regions are affected regardless of the intensity and the reordering of the individual regions.

A key observation is the epidemic characteristic of the attack, where the error propagates from an infected region in the lower level to all the regions in the lower level. The plot also illustrates how a single region in a lower level influences all the regions in the same level, implying that the attacker can choose the cheapest and most vulnerable region to launch the attack. Clearly, the error is maximum for the region where the attack originates. In the specific partitioning of the IEEE 118-bus system, Region 5 appears to be the most vulnerable because the system diverges when the input data is reordered. However, it is worth noting that the partitioning of the IEEE 118-bus system for the reordering attack is a particular case and other cases may exist.

The measurement reordering attack as described above works when some portions of the power system have integrity protection mechanisms. This is

not an unreasonable assumption because implementing timestamped measurements with authentication would be prohibitively expensive for current power grids. Indeed, as long as a power grid has unprotected legacy components, measurement reordering attacks will always pose a threat. However, in a decade or so, it should be possible to implement cryptographically timestamped authentication mechanisms for an entire grid, which would reduce, if not eliminate, the threat of reordering attacks.

9. Conclusions

This chapter has focused on reordering attacks on hierarchical state estimation as described in [9], where an adversary reorders measurement data without injecting or modifying data, resulting in incorrect estimates and potentially undesirable power system states. The attacks are feasible because it is not possible to implement authentication mechanisms throughout a large power grid. Therefore, this chapter has studied targeted reordering attacks on the most vulnerable region of a power system, which cause errors to propagate all over the system, and not just the attacked region. The results also demonstrate that an attacker can force incorrect estimates in a protected (i.e., authenticated) region of a power system by launching a clever attack on a less protected region.

Future research will attempt to develop protection and mitigation techniques for hierarchical or fully-distributed state estimation as employed in a smart grid. Research will also investigate the number of measurements and the specific measurements that would be swapped by an attacker to achieve maximal impact.

References

[1] A. Abur and A. Gomez-Exposito, *Power System State Estimation: Theory and Implementation*, CRC Press, Boca Raton, Florida, 2004.

[2] A. Baiocco, C. Foglietta and S. Wolthusen, Delay and jitter attacks on hierarchical state estimation, *Proceedings of the IEEE International Conference on Smart Grid Communications*, pp. 485–490, 2015.

[3] A. Baiocco and S. Wolthusen, Dynamic forced partitioning of robust hierarchical state estimators for power networks, *Proceedings of the Power and Energy Society Innovative Smart Grid Technologies Conference*, 2014.

[4] A. Baiocco, S. Wolthusen, C. Foglietta and S. Panzieri, A model for robust distributed hierarchical electric power grid state estimation, *Proceedings of the Power and Energy Society Innovative Smart Grid Technologies Conference*, 2014.

[5] S. Cui, Z. Han, S. Kar, T. Kim, H. Poor and A. Tajer, Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions, *IEEE Signal Processing*, vol. 29(5), pp. 106–115, 2012.

[6] T. Dierks and E. Rescorla, The Transport Layer Security (TLS) Protocol, Version 1.2, RFC 5246, 2008.

[7] Y. Feng, C. Foglietta, A. Baiocco, S. Panzieri and S. Wolthusen, Malicious false data injection in hierarchical electric power grid state estimation systems, *Proceedings of the Fourth International Conference on Future Energy Systems*, pp. 183–192, 2013.

[8] A. Gomez-Exposito, A. Abur, A. de la Villa Jaen and C. Gomez-Quiles, A multilevel state estimation paradigm for smart grids, *Proceedings of the IEEE*, vol. 99(6), pp. 952–976, 2011.

[9] A. Gul and S. Wolthusen, Measurement reordering attacks on power system state estimation, *Proceedings of the IEEE Power and Energy Society Innovative Smart Grid Technologies Conference Europe*, 2017.

[10] O. Kosut, L. Jia, R. Thomas and L. Tong, On malicious data attacks on power system state estimation, *Proceedings of the Forty-Fifth International Universities Power Engineering Conference*, 2010.

[11] S. Lakshminarasimhan and A. Girgis, Hierarchical state estimation applied to wide-area power systems, *Proceedings of the IEEE Power Engineering Society General Meeting*, 2007.

[12] Y. Liu, P. Ning and M. Reiter, False data injection attacks against state estimation in electric power grids, *Proceedings of the Sixteenth ACM Conference on Computer and Communications Security*, pp. 21–32, 2009.

[13] A. Monticelli, *State Estimation in Electric Power Systems: A Generalized Approach*, Springer, New York, 1999.

[14] F. Schweppe and D. Rom, Power system static-state estimation, Part II: Approximate model, *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-89(1), pp. 125–130, 1970.

[15] F. Schweppe and J. Wildes, Power system static-state estimation, Part I: Exact model, *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-89(1), pp. 120–125, 1970.

[16] F. Schweppe and J. Wildes, Power system static-state estimation, Part III: Implementation, *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-89(1), pp. 130–135, 1970.

[17] D. Shepard, T. Humphreys and A. Fansler, Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks, *International Journal of Critical Infrastructure Protection*, vol. 5(3-4), pp. 146–153, 2012.

[18] T. van Cutsem and M. Ribbens-Pavella, Critical survey of hierarchical methods for state estimation of electric power systems, *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-102(10), pp. 3415–3424, 1983.

[19] O. Vukovic and G. Dan, On the security of distributed power system state estimation under targeted attacks, *Proceedings of the Twenty-Eighth Annual ACM Symposium on Applied Computing*, pp. 666–672, 2013.