Error Propagation after Re-ordering Attacks in Hierarchical State Estimation

Ammara Gul[1] and Stephen Wolthusen[1,2]

[1] School of Mathematics and Information Security,
Royal Holloway University of London, Egham, UK
Ammara.Gul.2015@live.rhul.ac.uk, Stephen.Wolthusen@rhul.ac.uk

[2] Department of Information Security and Communication Technology,
Norwegian University of Science and Technology, Norway
stephen.wolthusen@ntnu.no

Abstract. State estimation is vital for the stability of control systems particularly the power system which heavily relies on measurement devices installed throughout the wide area network. Recently, the problems of bad data injection and topology error have been thoroughly analysed, with numerous newly proposed mitigation and protection schemes.
In this paper we consider hierarchical state estimators (HSE) relying on the common WLS formulation and study the propagation of faults in both intermediate and top-level state estimates as a result of re-ordering attack on a single area in the bottom level. Though at present time, our grids are equipped with modern defence but re-ordering attacks are still possible in the presence of such protections via ISO/IEC 62351 controls. We concentrate on how an inexpensive swapping attack in one area of the lower level influence the accuracy of other areas in the same level/upper levels and force the system towards undesirable state. We use the IEEE test cases for validation and illustration of results.

Keywords: Power system, smart grid, hierarchical state estimation, re-ordering attack

1 Introduction

Efficient and reliable Supervisory Control and Data Acquisition (SCADA) systems along with Energy Management Systems (EMS) contribute to efficient and safe operation of the power grid. The SCADA system gathers measurement data from remote substations into a control centre. EMS process all the collected data at the control centre by an on-line application called state estimation. State estimation allows the operator to get an accurate estimate of the state despite noisy or faulty measurement data by using a steady state flow model in the physical system [1],[2]. Numerous EMS applications e.g, contingency analysis use the estimated state and therefore the state estimation is crucial both for the efficiency and the safety of the power grid's operation.

Modern power systems are becoming more inter-connected and less likely to be dependant on a single control centre for operations. This way, operational efficiency can be improved by having multiple operators throughout the system e.g., in hierarchical or distributed structure. Each operator has its own control center and SCADA/EMS system to manage a certain region of the system. Examples of such inter-connected systems include ENTSO-E in Europe and Western

Interconnect (WECC) in the U.S. among others. In the future, power systems are expected to be more inter-connected than before and thus, systems with no central co-ordinators should be anticipated. For the safety of the large inter-connected power network, timely exchange of accurate information between the regional operators is quite important. Practically, the data exchange is limited due to sensitivity related issues. Regardless of this, all the exchanged information is used by the respective regional operators for estimating the local state and that way contribute to the state of the whole system.

HSE requires that control centres on each level exchange data regularly. Standard Inter-Control Center Communications Protocol (ICCP) is a widely used protocol to transmit information from one level to another in HSE. Access control is possible using this protocol but it does not provide key-based authentication for the exchanged data. Therefore standard layer protocols such as TLS as mandated by IEC 62351 are used to provide authentication for ICCP associations [3]. As a result, ICCP messages might be passed in clear text to the protocol stalk providing authentication. An adversary can compromise all incoming and outgoing messages from ICCP by installing a Trojan [4]. The vulnerability of control systems to such attacks can be seen by the fact that ICCP relations are often formed between hosts in civil areas.

The main objective of the present paper is to determine certain conditions under which one compromised region at lower level can have a desired impact on other regions in same level of hierarchy by propagation of faults upto the top level and then way back to each level. An attacker can force its desired impact on other region(s) by manipulating a single region realistically, an attacker is limited in the magnitude of change that can be induced this way. We aim to determine a necessary condition on which a minimum cost attack can be formulated to give maximum impact.

The remainder of the paper is organized as follows: Background and related work are briefly described in section 2 and a description of the system models used in state estimation, bad-data detection and identification is presented in the section 3. Hierarchical state estimation is outlined in section 4 and the novel measurement reordering attack model is presented in section 5 along with the necessary conditions to make the attack feasible. In section 6, simulation results are shown for the introduced attack on IEEE bus systems. We offer concluding remarks and suggest future work directions in section 7.

2 Related Work

The effect of bad data on state estimation in power systems has long been studied including in the influential work by Schweppe and

Wildes [5], with a bad data detection algorithm inside state estimation typically depending on simple statistical threshold to remove outliers.

When the measurement data collected by SCADA system is compromised, a straightforward outcome can be an undesirable state by forcing the state estimator without further constraints on data and correlation among them especially the case examined by Liu et al. [6] relying on DC power flows and a number of consequent studies on how to find the minimal undetectable attacks require the least manipulation of data [7], [8].

One of the earliest works on hierarchical state estimation (HSE) is by Van Cutsem in his survey in which he over-viewed the advancements in HSE that helps in building present models. Lakshmin proposed a two-level HSE algorithm for wide area power systems assuming a highly reliable PMU at every boundary bus. Several types of data attacks on decentralised state estimation are explained while no argument about computational complexity is made [4]. Moreover, the offered mitigation scheme involving outlier approach that can detect the errors after hundreds of iterations and even then the identification of attack can not be made possible.

False data injection (FDI) attacks that were initially formulated on conventional state estimation, were proved to be possible in hierarchical topology as well [9]. Further, Baiocco et al. present au-

tomated (graph) partitioning of robust HSE as a result of some unexpected failure of single/multiple lines or due to some attack [10]. Motivated by PMU's spoofing attack in [11], ill-conditionality of Jacobian can be achieved that leads to divergence by including jitter in communication channels of HSE [12]. A number of state estimators have been proposed, but studies of robustness against attacks has concentrated solely on the centralised case hence Baiocco et al. discuss the hierarchical case particularly relevant for smart and micro-grid environments [15].

In [13], we highlighted the vulnerabilities in the existing communication infrastructure by introducing an attack relying solely on re-ordering of the measurement vector which result in undesirable estimates by formulating targeted re-ordering attack. It is worth noting that we assumed that the preceding and present measurement vectors are known to the attacker. Specifically, considering two distinct scenarios, the system diverged as a result of ill-conditioned Jacobian.

3 Power System State Estimation

As usual, we denote the power system by a graph $\mathcal{G}$ with a set of $\mathcal{V}$ buses and $\mathcal{E}$ transmission lines. We consider AC power flow model for the network. It is given by

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

where $\mathbf{z} \in R^m$ is 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 having zero mean 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.

Once the states (let us call them $\hat{\mathbf{x}}$) are estimated by solving Normal Equations,

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

bad data analysis is done by a statistical threshold τ

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

Residual values larger than τ are detected and corresponding measurements are flagged as bad and after their removal, state estimation can be re-run until the system converges. But bad data detection is not easy if there is more than one bad measurement. In practice a bad data goes undetected due to the presence of other bad data or good measurements are flagged as bad due to other reasons such as topology change (for more details of state estimation, please visit [1]).

4 Hierarchical State Estimation

The conventional or centralized state estimation which is currently in use worldwide can be followed by a multi-area hierarchical procedure in which local state estimators processes all the raw measurements available locally, hence transferring only a manageable data set to its immediate higher level. This process continues until the highest level where the state for the whole system is evaluated and conveyed to the lower levels for other crucial tasks for example bad data processing [14]. The multi-area hierarchical structure is of two types, i.e., symmetric hierarchy and asymmetric hierarchy. Symmetric hierarchy is the one with a balanced division of bus-bars/tie-lines in all regions whereas, asymmetric hierarchy is the one with an unbalanced distribution of bus-bars/tie-lines among regions. While symmetric HSE is trivial and easy to understand, asymmetric is more realistic and general in power systems. For this reason, from now onwards, we are considering only asymmetric hierarchical state estimation. It is worth mentioning here that the following HSE formulation in this section is taken from [12] and [15].

Baioccoo et al. introduced a tree structure to represent multi-area hierarchical SE with the tree root (level k) denoting the highest level state estimation [15]. At lower levels, each level can have child nodes and those without child nodes are known as leaf nodes and lie on the lowest level (level 1) of hierarchy. Each node performs its

own state estimation using the measurements available in terms of estimated states from the lower nodes and for level 1, measurements are obtained by computing power flows. We assume here that the partitioning is already done and it is robust that ensures and there is no overlapping between areas except the common tie-lines connecting the neighbouring areas.

When a node estimates its state vector, it must send this output (including the Gain matrix) over to all the child or to the parent node. This kind of multi-area HSE works on a two-way transmission of information i.e, from lower levels information flow towards the higher ones until it reaches the root node and then re-send the estimation towards leaf nodes such that the updated state spread on all the tie-line branches.

A general k level multi-area state estimation can be expressed as:

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

$$\begin{aligned} y_{1,j_2} &= f_{2,j_2}(y_{2,j_2}) + e_{2,j_2}, \quad j_2 = 1, \cdots, r_2 \\ y_{1,b_2} &= f_{2,b_2}(y_2) + e_{2,b_2} \end{aligned} \tag{5}$$

$$\vdots$$

$$y_{0,b_1} = f_{1,b_1}(y_1) + e_{1,b_1} \tag{6}$$

where

y_{0,j_1} local measurement vector in S_{j1} at level 1;

y_{0,b_1} border measurement vector at level 1;

y_{1,j_2} local measurement vector in S_{j2} at level 2;

y_{1,b_2} border measurement vector at level 2;

y_k state vector of over all system;

f_l corresponding non-linear measurement functions for each level l;

e_l corresponding Gaussian measurement noise vector.

Now, let us formulate each level

<u>*Level* 1 *multi-area state estimation:*</u> For level 1, each area S_j estimates its own state $\tilde{y}_{1j}$ by solving the corresponding Normal Equations iteratively

$$\begin{aligned} [F_{1,j_1}^T R_{1,j_1}^{-1} F_{1,j_1}] \Delta\tilde{y}_{1,j_1} &= F_{1,j_1}^T R_{1,j_1}^{-1} [y_{0,j_1} - f_{1,j_1}(y_{1,j_1}(k))] \\ [F_{1,b_1}^T R_{1,b_1}^{-1} F_{1,b_1}] \Delta\tilde{y}_{1,j_1} &= F_{1,b_1}^T R_{1,b_1}^{-1} [y_{0,b_1} - f_{1,b_1}(y_{1,j_1}(k))] \end{aligned} \tag{7}$$

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

<u>*Level i multi-area state estimation:*</u> The following two equations must be solved for each intermediate level hierarchically from the lower levels. Using the estimate $\tilde{y}_{i-1,j_{i-1}}$ from the level $l-1$ as the mea-

surements in a distributed approach, $\tilde{y}_{i,j_i}$ can be obtained from [9]

$$
\begin{aligned}
&[F_{i,j_{i-1}}^T G_{i-1,j_{i-1}} F_{i,j_{i-1}}] \Delta\tilde{y}_{i-1,j_{i-1}}(k) = F_{i,j_{i-1}}^T G_{i-1,j_{i-1}} [\tilde{y}_{i-1,j_{i-1}} - f_{i,j_{i-1}}(y_i(k))] \\
&[F_{i,b_i}^T G_{i-1,b_{i-1}} F_{i,b_i}] \Delta\tilde{y}_{i-1}(k) = F_{1,b_1}^T G_{i-1,b_{i-1}} [\tilde{y}_{i-1} - f_i(y_i(k))]
\end{aligned} \tag{8}
$$

Based on the estimates from level i and $i+1$, the Jacobian matrices are revised.

<u>*Level l multi-area state estimation:*</u> 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

$$
\begin{aligned}
&[F_{l,j_{l-1}}^T G_{l-1,j_{l-1}} F_{l,j_{l-1}}] \Delta\tilde{y}_{l-1,j_{l-1}}(k) = F_{l,j_{l-1}}^T G_{l-1,j_{l-1}} [\tilde{y}_{l-1,j_{l-1}} - f_{l,j_{l-1}}(y_l(k))] \\
&[F_{l,b_l}^T G_{l-1,b_{l-1}} F_{l,b_l}] \Delta\tilde{y}_{l-1}(k) = F_{1,b_1}^T G_{l-1,b_{l-1}} [\tilde{y}_{l-1} - f_l(y_l(k))]
\end{aligned} \tag{9}
$$

The HSE outlined above requires two-way interchange of data between local state estimators at each layer of the hierarchy [12].

4.1 Simplification of a multi-level HSE to a 3-level HSE

Now, Let us simplify the multi-level approach to three level for better understanding. Then the three-level model can be explained as

$$\begin{aligned} y_{0,j_1} &= f_{1,j_1}(y_{1,j_1}) + e_{1,j_1}, \quad j_1 = 1,2 \\ y_{0,b} &= f_{1,b}(y_{1,b}) + e_{1,b} \\ y_{1,j_2} &= f_{2,j_2}(y_{2,j_2}) + e_{2,j_2}, \quad j_2 = 1,2 \\ y_{1,b} &= f_{2,b}(y_{2,b}) + e_{2,b} \\ y_2 &= f_3(x) + e_3 \end{aligned} \tag{10}$$

where, the measurement vectors y_{0,j_1}, y_{1,j_1} and $y_{0,b}$, $y_{1,b}$, the state vectors y_{1,j_1}, y_{2,j_2} and y_{b,j_1}, y_{b,j_2} and the non-linear measurement functions f_{1,j_1}, f_{2,j_2} and $f_{1,b}$, $f_{2,b}$ are as described earlier. For making the process more simpler, lets assume that there are no border variables and the measurement functions are linear as well. Now, more simplified version of three-level can be seen as

$$\begin{aligned} y_{0j} &= F_{1j}y_{1j} + e_{1j}, \quad j = 1,2 \\ y_{1j} &= F_{2j}y_{2j} + e_{2j}, \quad j = 1,2 \\ y_2 &= F_3 x + e_3 \end{aligned} \tag{11}$$

where F_{1j}, F_{2j} and F_3 are the Jacobian matrices of the corresponding measurement functions. For each area, the state estimator carries out iterative solution algorithm and determines the local state vector

along with another iterative process among the two levels [9]

Level 1: The inputs at the first level are y_{1j} for area $j = 1, 2$ (assuming two areas) and the weighting matrix R_{1j}^{-1}. The output is the local state vector $\hat{y}_{1j}$ for each area, Normal equations to be solved by each area iteratively are

$$[F_{1j}^T R_{1j}^{-1} F_{1j}^T]\hat{y}_{1j} = F_{1j}^T R_{1j}^{-1} y_{0j} \tag{12}$$

Level 2: The inputs at the second level are y_{1j} for area $j = 1, 2$ (assuming two areas) and the weighting matrix R_{1j}^{-1}. The output is the local state vector $\hat{y}_{1j}$ for each area, Normal equations to be solved by each area iteratively are

$$[F_{2j}^T R_{2j}^{-1} F_{2j}^T]\hat{y}_{2j} = F_{2j}^T R_{2j}^{-1} y_{1j} \tag{13}$$

Level 3: The inputs of this level are state vectors of level-2 $\hat{y}_2$ and the gain matrices $G_2 = F_{1j}^T R_{2j}^{-1} F_{2j}^T$ as the weighting matrix. The output $\hat{x}$ is the state of the entire system when solving the following Normal equations for the third level

$$[F_3^T G_2^{-1} F_3^T]\hat{x} = F_3^T G_2^{-1} \hat{y}_2 \tag{14}$$

where y_2 and G_2 can be found by juxtaposing the corresponding y_{2j} an G_{2j} respectively.

5 Attack Model

The goal of our proposed attack is to create disruption in HSE. To attain this goal, we consider that the attacker is capable of re-ordering the measurement set $\mathbf{y}^0$ of only one partition $S^0 \in S$ in the lower level l_1 of hierarchy where S is the set of all partitions. As a result, the untrue state variables are being transmitted to the partitions at upper levels at the beginning of each iteration of HSE. A structured re-ordering attack is considered while assuming the internal knowledge of the partitions to launch the re-ordering attack in a way that maximizes its effect. The knowledge required for the success of the re-ordering attack includes some previous plausible measurement set $\mathbf{y}_{old}$ of the targeted partition. The main aim of the attack is to have a desired/false local state estimate that propagate to higher levels to produce certain estimate $\mathbf{x}$.

The scheme we are following for the attack is a three level hierarchical structure with the following constraints:

- Once the attack is launched on a single partition of level l_1, the data exchange between the upper two levels i.e, l_2 and l_3 would still remain normal. That means there is no further attack on upper levels.
- The network configuration, i.e, the sub area partitioning at level l_2 and l_2 is not permitted to change over a course of full top-

down synchro-upgrade (This constraint is usually not required by HSE[12].

After the attack, the flow equations of the first level would be like

$$[F_{1j}^T R_{1j}^{-1} F_{1j}^T]\hat{y}_{1j}^* = F_{1j}^T R_{1j}^{-1} y_{0j}^* \tag{15}$$

where y_{0j}^* is the swapped measurement vector of one of the sub-areas at level one. The inputs at the second level y_{1j}^* for area $j = 1, 2$ are the false estimates from the first level and then

$$[F_{2j}^T R_{2j}^{-1} F_{2j}^T]\hat{y}_{2j}^* = F_{2j}^T R_{2j}^{-1} y_{1j}^* \tag{16}$$

and finally, the output $\hat{x}^*$ is the state of the entire system when solving the following Normal equations for the third level

$$[F_3^T G_2^{-1} F_3^T]\hat{x}^* = F_3^T G_2^{-1} \hat{y}_2^* \tag{17}$$

where y_2^* and G_2 are as defined earlier in section 4.1.

In case of False Data Injection (FDI), **a** generally denotes the attack vector that shows the amount of change to the original measurement vector [6].

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

where **c** is a vector denotes the magnitude of change and is bounded by some stealthy condition. Jamming or delay attacks can be seen as a sub-class of re-ordering as they resend the previous data with some time interval. Also, attacks performed by replaying or blocking the measurement vector can be considered a special case of re-ordering with a time constraint on them. The common aspect among all of the above is that there is no attack vector to be added, rather adversary just drop/block or jitter the measurements irrespective of whether they are secure/protected or not by hacking the communication infrastructure. Therefore, a general term, **re-ordering** of the measurement vector is introduced where the adversary swap the true measurement vector with the previously plausible (true) vector.

In this case, time horizon is critical for the attacker and it determines the strength of the attack. Being realist, we assume that the attacker has the measurement information from the present till some particular limited point in time. Within these time instances, the attacker can choose the measurement vector to be swapped the present one while keeping itself hidden. By hidden, we mean an attack that is successful in state forcing or non-convergence while being in-noticed by the model-based bad data detection. There may be more sophisticated detection criteria, of course, but these apply mostly to determining whether measurement devices (vector entries) are compromised, and that doesn't apply here. Other models rely on

redundancy among measurements to determine compromise, but for a network-based attack this does not match very well.

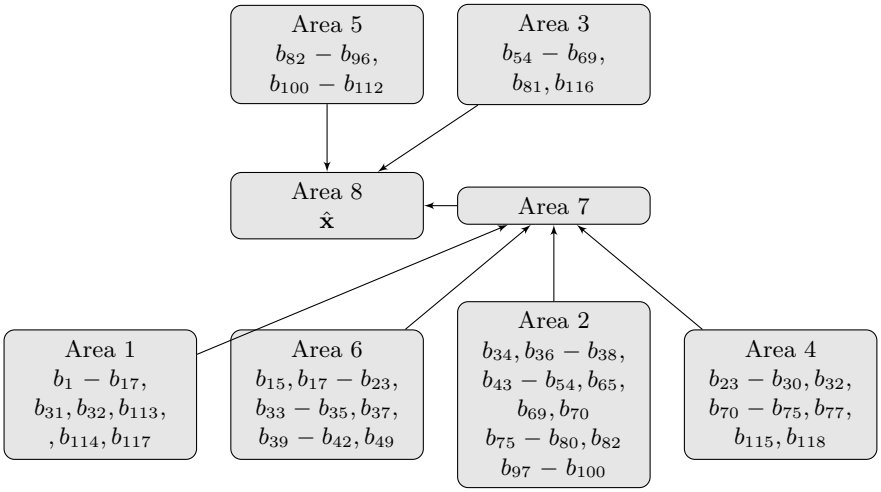

Fig. 1: Bus-bars distribution of 118-bus system

5.1 Re-ordering Attack Cost and Attack Impact

We quantify the minimum attack cost as the attacking cost where attacker needs to put the least effort to get the maximum Mean Square Error (MSE) and denote it by Γ_y. All the regions in the power grid can be secured in one of the three ways, i.e. non tamper proof authentication ($S_{ntp} \subseteq S_m$), tamper-proof authentication ($S_{tp} \subseteq S_m$) or protected. Non-tamper proof authentication is of Bump-in-the-Wire (BITW) type device authentication or a Remote Terminal Unit (RTU) with a non tamper-proof authentication module. The regions

with this type of authentication are only susceptible to attacks by some physical access to the region from where the data is originated. Tamper-proof authentication is not susceptible to attacks in any case. Other cases of protection are also possible by guards or video surveillance and generally this type is also not vulnerable to attacks. But realistically, all regions of the power grid can not be made protected by all means and there must be at least one region that is vulnerable ($S_{m'}$). If the region where the measurement vector to be attacked is located is protected and uses non tamper-proof authentication or tamper-proof authentication then the measurement is not vulnerable and we define $\Gamma_y = \infty$. Otherwise, for a measure-

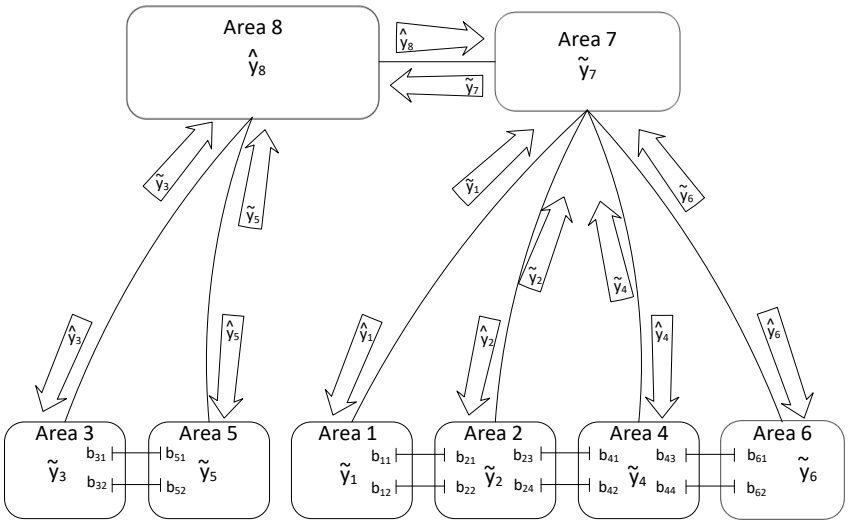

Fig. 2: Information flow in Hierarchical State Estimation

ment y, we define Γ_y as

$$\begin{aligned} &\Gamma_y = \min \ \|a\| \ \ s.t. \ \ a = Fc = \hat{y}^{new} - \hat{y}^{old} \quad \text{and} \\ &a(y) \neq 0 \Longrightarrow |S(m')| \neq 0, \quad s.t. \ \ S = S(m) \cup S(m') \end{aligned} \tag{18}$$

where S_m denotes authenticated areas/regions and $S_{m'}$ denotes the vulnerable areas s.t. $S = S(m) \cup S(m')$.

In addition, we assume that the attacker is free to choose the set from plausible measurements in a particular time frame to be used for re-ordering attack. As a result of this freedom and the attack cost (Γ_y) mentioned above, we quantify the maximum attack impact as the attacker's outcome and denote it by $\mathcal{I}_y$

$$\begin{aligned} &\mathcal{I}_y = \max \ \ I = \sqrt{\sum (\tilde{y}^{new} - \tilde{y}^{old})^2} \\ &\text{s.t.} \quad t^{new} - t^{old} \geqslant \epsilon \end{aligned} \tag{19}$$

where t denotes the time slot among the available time frames to the attacker and ϵ is the pre-defined threshold to limit the attacker's choice. Superscripts "old" and "new" denotes the measurement used in the swapping and the measurement to be swapped respectively.

6 Numerical Results

Before going into the detail of simulation results, it should be recalled that to perform re-ordering attacks, the attacker requires the topol-

ogy/subspace knowledge of the system and it is assumed that the topology is not changing or it is static in the duration of the attack. In this section, we discuss the performance of the above mentioned model in constructing the re-ordering attacks on each region of a hierarchical state estimation by simulations on IEEE 118-bus systems. We divide the 118-bus system into 6 sub-areas/regions and additionally there is an intermediate level between the top and bottom layers (shown in Fig. 1). Since the presented hierarchical model is two-way synchro-upgrade model i.e., at first, from lower level to the top-most and then the way back to the bottom levels again, it is very interesting to see the error propagation after the proposed attack. The attacker is free to choose the particular data set from a certain time frame i.e, attacker has a limited amount previous data knowledge. The technique used to estimate the state is WLS and MATPOWER is used for loading the data for AC model.

Mean square error (MSE) after performing least cost re-ordering attacks of the type described in subsection 5.1, is illustrated in Fig. 3 for 118-bus system. Figure denotes the logarithm (base 10) of MSE for one complete round of WLS state estimation i.e., from the lower layer the the top (Fig. 3) and all the way down detailing how that error propagates from the lower level to the top and back again. We can clearly see that in the end of a complete round after re-ordering attack, all areas are affected no matter what the intensity is and

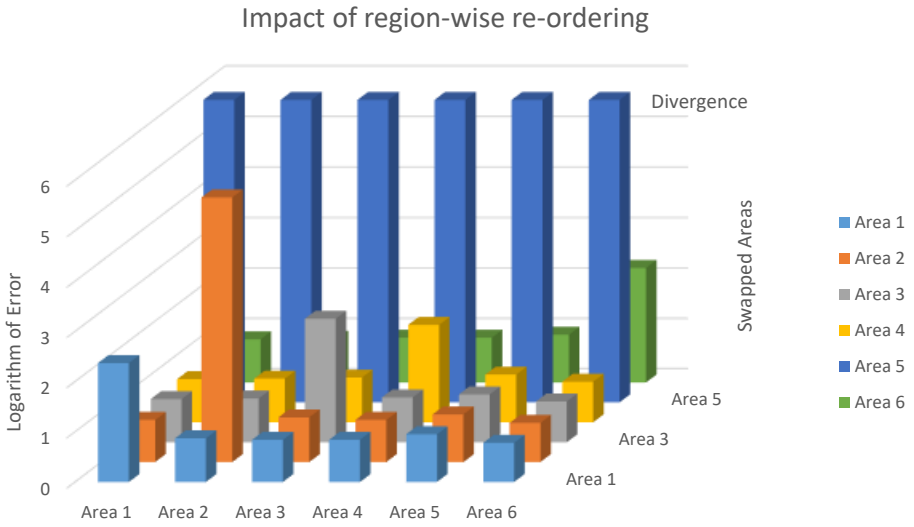

Fig. 3: Effect of re-ordering at lower level of HSE

which area is re-ordered individually. The important point to notice is the epidemic property of the attack and it shows the error propagation from one infected area at lower level to all the areas at lower level. The plot illustrates how a single area from lower level hierarchy influence all the areas at lower level such that the attacker can choose for the cheapest and the most vulnerable area to perform the attack. An obvious observation is that the error is maximum for the areas from where the attack originates. In the given partitioning of 118-bus system, area-5 seems to be the most vulnerable as the system diverges when the input data is re-ordered. It is worth noting here that the partitioning of 118-bus system for the re-ordering attack is a particular one and other cases may exist.

The measurement re-ordering attack as described in section 5 is made to work even if some parts of power system are integrity protected. Key observation is that currently in our power grid, all the measurements are not authenticated time-stamped to detect such re-ordering and such authentication for detection purposes is adequately expensive to implement all over the grid atleast till near future. This implies that as long as there are old components in our power network, there can be a chance of such kind of attacks. But, in ten years time, cryptographically time-stamped authentication can be made possible over the entire network leaving the re-ordering attack less effective.

7 Conclusion

We proposed an attack termed as "re-ordering attacks" on hierarchical state estimation that we introduced earlier in [13] where the adversary uses swapping of data sets as a tool to swap the order of data with some previous data set while not injecting or modifying any data. The present paper relied on the fact that not all parts of the grid can be made tamper/non-tamper proof authenticated over night. Therefore, a targeted re-ordering attack on the most vulnerable region of the system is studied that can provide desirable propagation of error all over the system and not just the attacked area. Moreover, it can be clearly seen that such an attacker can force the estimate of a authenticated region by launching an intelligent attack in less protected region.

Our ongoing research includes determining the mitigation/protection

to the re-ordering on hierarchical or fully distributed state estimation which is more realistic in the smart grid. Other possible future research includes answering how much and which particular measurements should be swapped for the optimal swapping attack.

References

1. Abur, A., Exposito, A.G. In: Power System State Estimation: Theory and Implementation. CRC Press (March 2004)
2. Monticellii, A. Business and Economics. In: State Estimation in Electric Power System: A generalized approach. Springer Science and Business Media (May 1999)
3. Dierks, T., Rescorla, E.: RFC5246: The transport layer security (TLS) protocol version 1.2. http://tools.ietf.org/html/rfc5246 (August 2008)
4. Vukovic, O., Dan, G.: On the Security of Distributed Power System State Estimation under Targeted Attacks. (March 2013)
5. Schweppe, F.C., Wildes, J.: Power System Static-State Estimation Part I-III. IEEE Transactions on Power Apparatus and Systems **PAS-89** (January 1970) 120–135
6. Y. Liu, P.N., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. In: Proceedings of 16th ACM conference on Computer and communications security, NY, USA (November 2009) 21–32
7. O. Kosut, L. Jia, R.J.T., Tong, L.: On Malicious Data Attacks on Power System State Estimation. In: Universities Power Engineering Conference (UPEC), 2010 45th International, Cardiff, Wales, IEEE (2010)
8. S. Cui, Z. Han, S.K.T.K.H.P., Tajer, A.: Coordinated Data-Injection Attack and Detection in the Smart Grid: A Detailed Look at Enriching Detection Solutions. Volume 29.
9. Y. Feng, A. Baiocco, C.F.S.P., Wolthusen, S.D.: Malicious False Data Injection in Heirarchical Electric Power Grid State Estimation Systems. (May 2013)
10. Baiocco, A., Wolthusen, S.: Dynamic Forced Partitioning of Robust Hierarchical State Estimators for Power Networks. In: IEEE PES Innovative Smart Grid Technologies Conference (ISGT), IEEE (February 2014) 1–5

11. Shepard, D.P., Humphreys, T.E.: Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks. In: Sixth annual IFIP Conference on Critical Infrastructure Protection. Volume 5., Washington DC (December 2012)
12. A. Baiocco, C.F., Wolthusen, S.D.: Delay and Jitter Attacks on Hierarchical State Estimation. In: Proceedings of 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm), Miami, FL, IEEE (November 2015) 485–490
13. : Anonymised for review
14. A. G. Exposito, A. Abur, A.D.L.V.J., Quiles, C.G.: A Multi Level State Estimation Paradigm for Smart Grids. Proceedings of the IEEE **99** (April 2011) 952 – 976
15. A. Baiocco, C. Foglietta, S.P., Wolthusen, S.: A Model for Robust Distributed Hierarchical Electric Power Grid State Estimation. In: IEEE PES Innovative Smart Grid Technologies Conference (ISGT), IEEE (February 2014) 1–5