Measurement Re-Ordering Attacks on Power System State Estimation

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

1. School of Mathematics and Information Security, Royal Holloway, University of London, Egham, UK
2. Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Norway
Email: Ammara.Gul.2015@live.rhul.ac.uk, stephen.wolthusen@rhul.ac.uk

***Abstract*—Power system state estimation is a prerequisite for detecting faults, directing power flows, and other tasks of Energy Management Systems. State estimators have conventionally filtered out so-called bad data or outliers, but in recent years a number of attacks and mitigation mechanisms have been proposed involving deliberate injection of bad data.**

In this paper, we introduce a constrained attack mechanism which will be feasible where the communication channel for measurements is authenticated and integrity-protected. We demonstrate that re-ordering of measurements is sufficient to cause errors in state estimation or preventing convergence and propose an algorithm to introduce such attacks.

Based on this, we introduce two security metrics to quantify the effort required for sparse and minimum magnitude re-ordering attacks, respectively, in the form of security indices based on the assumption of the adversary's full or partial knowledge of previous measurement vectors. We demonstrate success by presenting the Mean Square Error (MSE) for the attacks described and also evaluate the attack model for both the standard IEEE-14 and 30-bus test cases.

Index Terms: Power system, re-ordering attacks, state estimation, stealthy/ hidden attack

I. Introduction

State estimation has been at the core of monitoring and managing power networks for decades, but is increasing in importance in the transition to smart grids. Sensors are becoming more sophisticated as in the case of more widespread adoption of phasor measurement units (PMUs) and relatively inexpensive micro-PMUs as well as more conventional monitoring by way of Intelligent Electronic Devices (IEDs) [1]. State estimation relies on these measurements and topology analysis and is in turn a key input for any Energy Management system operating a power grid and performing contingency analysis [2]. Measurements may, however, be faulty, but can also be the subject to attacks, either on sensors or on communication channels. For the former case statistical detection algorithms have long formed part of state estimation, but the latter has only come to the attention of the research community in recent years. A number of attacks have been proposed ranging from the manipulation of measurements as may be achievable by direct manipulation of sensors to indirect attacks such as manipulating the signal timing proposed by Shepard and Humphreys [3], jamming of signals proposed by Deka et al. [4] or delays in communication channels proposed by Baiocco et al. [5]. Unlike the work mentioned before, most attacks, however, rely on the assumption that arbitrary values may be injected by an adversary. *We argue that this may not be a realistic assumption* and that instead it is of considerable interest to study cases where measurements and communication channels are protected, at least using authentication and integrity protection as provided e.g. by the ISO/IEC 62351 standard. This offers a more realistic adversary model compared to that introduced by Liu et al. [6].

The main aim of this work is to *highlight the vulnerabilities in the existing communication infrastructure by introducing a novel attack relying solely on re-ordering of the measurement vector which result in spurious estimates. Here, we formulate targeted re-ordering attack considering two scenarios for this: 1) swapping the measurements by the previous plausible vector and 2) swapping the measurements by some scalar multiple of previous measurement vector*. It is worth noting that we assume here that the preceding and present measurement vectors are known to the attacker. Specifically, we prove that for scenario I, if the attacker swaps more than 80% of total measurements, it can cause the system to diverge as a result of ill-conditioned Jacobian. Similarly, to execute attacks of the kind as in scenario II, attackers have to pay more (swapping of about 75% measurements will be required) to get maximum mean square error in estimated states.

The remainder of the paper is organized as follows: Background and related work are briefly described in section II and a description of the system models used in state estimation, bad-data detection and identification is presented in the section III. The novel measurement re-ordering attack model and algorithm are proposed in section IV along with the necessary conditions to make the attack feasible. In section V, simulation results are shown for the introduced attack on IEEE bus systems. We discuss the significance and feasibility of the proposed attack in section VI and finally, we offer concluding remarks and suggest future work directions in section VII.

II. Related Work

In [6], Liu et al. discussed the design and impacts of undetectable false data injection attacks. These attacks, constructed with projection matrices, proved to thwart the bad data test. Based on the requirements such as topology,

978-1-5386-1953-7/17/$31.00 ©2017 IEEE

infrastructure and synchrophasor placement, various authors tried to find the optimal solution to such attack problem. Attacks that require minimum manipulation, called sparse attacks are constructed in [7] in which, with the knowledge of system topology, an attacker is able to find the set of meters to inject bad data. Such attacks are also termed as least cost attacks. Then, a greedy algorithm is proposed to evaluate smallest set of measurements to be protected in order to force the attacker to be detected. Following [7], Deka et. al defined the adversary's objective as constructing an attack vector using minimum corruption to produce undetected error in state estimation [8]. Difference between the two lies in using graph theoretic ideas in [8] for finding optimal attack vector.

Data attack on strategic buses is proposed in [9] where a polynomial time algorithm is given to identify the minimum number of measurements to manipulate for a successful stealthy attack on the desired buses. In [10], protection from FDI attacks is proposed by securing a particular set of measurements or by verifying the state variables individually using greedy schemes.

The concept of security index was introduced by Sandberg et al. in [11] and [12] by proposing two metrics. These indices quantify the least effort needed to achieve attack goals while avoiding bad-data alarms in the power network control center [11]. These indices depend on the power network topology and the measurements available to the system operator. The information gained in terms of these metrics can be utilised to strengthen the security of power grid. One of the indices is for the sparse attacks and other for small magnitude attacks. The inspiration of security metrics in the present paper is drawn from their work [12] to quantify how hard re-ordering attacks are to perform.

The majority of the current work on power grid security has been focussed on designing stealthy or undetectable attacks that inject bad data or modify the existing data while avoiding detection completely. However, Kim et al. in [13] proved that detectable *data framing attacks* can be formulated that modify half of the total measurements and damage the other half. Thus, the attack becomes successful after the damaged measurements are detected and removed by traditional bad-data test. This is the first work (to the best of our knowledge) on the notion of detectable attacks. Following this, in [4], a generalized detectable attack model is presented where a particular set of measurements are made protected/non-corruptable by authentication or integrity protection. In [14], Deka et al. considered the same framework as in [4] but with an inclusion of the concept of jamming. It is worth noting here that measurement jamming is less resource-intensive and in addition it only requires to drop/block the readings rather than to modify or inject bad data. The authors then presented in [15] a kind of attack in which both jamming and changing the status of breaker are combined to make the attack feasible. In this case, the adversary changes the status of few closed breakers and blocks the communication of flow measurements on those lines to the control centre to make the attack stealthy.

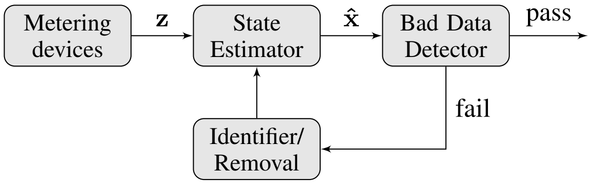

Figure 1: State estimation model and detection test

Later, Sanjab and Saad introduced the concept of multiple adversaries and studied their impacts on power system [16]. It is possible that the adversaries may cancel the effect of each other resulting in normal operating system i.e. no need to mitigate/defend. On the other hand, it is quite likely that the multiple attackers help each other in achieving malicious goals and prove destructive for the grid. In addition, Game theoretic approach is used to formulate the attack model with multiple adversaries [17].

III. Power System State Estimation

State estimator evaluates the most likely state of the system by filtering and processing the measurements from Remote Terminal Units (RTUs) or/and other metering devices installed in the system via transmission lines. We denote the power system by a graph with a set of V buses and E transmission lines. We consider an AC power flow model for the network [2]. It is given by

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

where $\mathbf{z}$ is the vector of measurements (m vector), $\mathbf{x}$ is the state vector (n vector, and $m > n$), h is the measurement function relating measurements to the states and $\mathbf{e}$ is the vector of measurement errors having zero mean and known co-variance, which is denoted by $\mathbf{R}$. The errors are assumed to be independent, therefore $\mathbf{R}$ is a diagonal matrix.

$$Cov(\mathbf{e}) = \mathbf{R} = diag\{\sigma_1^2, \sigma_2^2, \cdots, \sigma_m^2\}$$

There are two well known methods to solve the state estimation problem which are Weighted Least Square (WLS) and Weighted Least Absolute Value (WLAV) method. Although, WLAV is robust and stable in the sense that it is able to reject bad data efficiently but it has some major drawbacks i.e., it involves time consuming Linear Programming (LP) technique, convergence rate reduces due to inclusion of auxiliary variables while minimizing and it is not reliable when encountered with leverage points (i.e, ill-conditionality may occur). Therefore, WLS, although not that effective in presence of bad data, is considered as the most widely used method to SE problems (for more details of WLAV, please see [18]). The WLS problem involves solving a non-linear set of equations relating measurements and state variables that are voltage magnitudes and phase angles, by minimizing the summation of squares of residuals as in [19]

$$J(\mathbf{x}) = \sum_{i=1}^{m} (\mathbf{z}_i - h_i(\mathbf{x}))^2/\mathbf{R}_{ii} = [\mathbf{z} - h(\mathbf{x})]^T \mathbf{R}^{-1} [\mathbf{z} - h(\mathbf{x})]$$

Once the states (let us call them $\hat{\mathbf{x}}$) are estimated, bad data analysis is done by a statistical threshold τ

$$\mathbf{r} = \mathbf{z} - h(\hat{\mathbf{x}}) \tag{2}$$

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 all the bad data are removed and the system converges. There are other testing schemes as well such as, χ^2-test or hypothesis testing identification (HTI) (Please see [2] for more details).

IV. Attack Model

The developments in the notion of attacks and their countermeasures flourished much in the last decade. But as far as mitigation/protection is concerned, the majority of the work focussed integrity protection as one of the possible countermeasures. The attack we are proposing is novel in the sense that it can be launched successfully despite of these modern restrictions. In section 3, a continuous model for state estimation is presented, however, to study attacks and their impacts, discrete approximation of the model is widely used [2] and from now onwards we will also follow discrete time approximation model.

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e} \tag{3}$$

where $\mathbf{H} \ \in \mathcal{R}^{m \times n}$ is a constant Jacobian matrix. Then the estimation problem can be solved by

$$\hat{\mathbf{x}} = (\mathbf{H}^T\mathbf{R}^{-1}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{R}^{-1}\mathbf{z} \tag{4}$$

The active power flows can be estimated by the phase angle estimate $\hat{\mathbf{x}}$

$$\hat{\mathbf{z}} = \mathbf{H}\hat{\mathbf{x}} = \mathbf{H}(\mathbf{H}^T\mathbf{R}^{-1}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{R}^{-1}\mathbf{z} := \mathbf{K}\mathbf{z} \tag{5}$$

where $\mathbf{K}$ is the hat matrix. Bad data detection system identify faulty sensors and bad data by calculating the measurement residue which is defined as

$$\mathbf{r} := \mathbf{z} - \hat{\mathbf{z}} = \mathbf{z} - \mathbf{H}\hat{\mathbf{x}} = (\mathbf{I} - \mathbf{K})\mathbf{z} \tag{6}$$

If the residue $\mathbf{r}$ is larger than the threshold τ, then an alarm is triggered and bad measurements $\mathbf{z}_i$ are identified and removed. In case of False Data Injection (FDI), $\mathbf{a}$ generally denotes the attack vector that shows the amount of change to the original measurement vector [6].

$$\mathbf{a} = \mathbf{H}\mathbf{c}$$

where $\mathbf{c}$ is a vector denotes the magnitude of change and is bounded by some stealthy condition. *A necessary condition for a stealthy FDI attack is that the bad data detection alarm is not triggered if* $\mathbf{a}$ *lies in the null-space of* $\mathbf{I} - \mathbf{K}$. Whereas, in jamming or delay attacks, 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. Similarly, **re-ordering** of the measurement vector is introduced where the goal of the adversary is to misguide the system operators about the type and strength of attack 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.

Now, $\mathbf{z}^*$ is the new measurement vector obtained after swapping/ re-ordering the measurements

$$\mathbf{z}^* = \mathbf{z} + \mathbf{a}$$

where $\mathbf{a}$ is the swapping attack vector. This attack is less recourse intensive as it doesn't require modification or bad data injection into the sensors rather tampering the transmission lines would be enough. After re-ordering, the system model is

$$\mathbf{z}^* = \mathbf{H}\mathbf{x}^* + \mathbf{e}$$

where and $\mathbf{x}^*$ is the corresponding state vector which can be determined by

$$\mathbf{x}^* = (\mathbf{H}^T\mathbf{R}^{-1}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{R}^{-1}\mathbf{z}^* \tag{7}$$

where $\mathbf{H}$ is the Jacobian matrix. As, the final result of the state estimate from the above set of normal equations involves matrix multiplication with $\mathbf{z}^*$, therefore even the swapping of just 2 readings will change the whole state vector. We assume that all data is subjected to outlier removal which is usually a residue test to filter bad data (see section III). We have to show that the attack proposed below will not be affected by this removal while satisfying stealth condition. To make the swapping attack successful, attacker has to know the previous plausible measurement vector (either partial or full). As in [11], Sandberg et al., defined two security indices for sparse attacks as well as for small magnitude attacks. The first security index α_k in [11] is for sparse attacks i.e. the adversary can get the least/minimum cost attack by solving this and the second security index β_k help the attacker to find the small magnitude false data injection attacks to avoid detection tests. The aim of the attacker here is to maximize the impact P of swapping i.e, in terms of convergence time and MSE while keeping the measurement re-ordering to the minimum. This optimization problem can be formulated as

$$\min_{a_i} \ P \quad s.t. \quad \parallel a_i \parallel \leq \mu \tag{8}$$

where $\mu > 0$ is the desired bound on the size of attack. As defined, $P = \infty$ means that the state estimator does not converge.

The two scenarios defined in section I are as follows:

A. Scenario I

Here, we consider the re-ordering of measurement with some measurement vector from the plausible preceding data sets. By plausible we mean that the difference between the

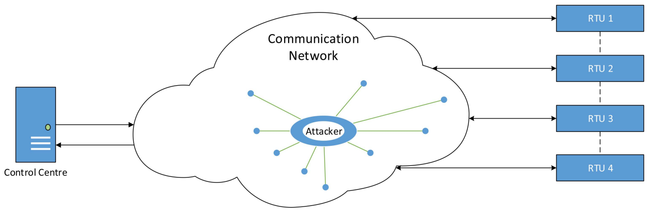

Figure 2: Attack on communication network

corresponding estimates is bounded i.e.,

$$| \mathbf{x}^{new} - \mathbf{x}^{old} | < \mu$$

where μ is some scalar. In other words, attacker is not free to choose any previous data set for swapping attack but only the one satisfying the above condition. Here, we are assuming that a particular set of measurements is secured such that they are integrity protected but not encrypted. By integrity protection we mean, protection of content and processes against injection. Assumptions regarding knowledge that attacker has, include: 1) Order $(m \times n)$of Jacobian matrix H, 2) Arrangement in which the measurements are placed in H and 3) Set of protected measurements is also known to the adversary.
Once the data set to be used in the attack is chosen, the man-in-the-middle attacker now has to select which readings to swap between the two measurement vectors, and which not i.e restricted swapping. This means the attacker can launch minimum cost/sparse attacks with carefully chosen minimum possible swapping. For this purpose, we define a measure to quantify the hardness to perform sparse swapping attacks.

$$\begin{aligned} \text{minimize} \quad & \|z_i^{new} - z_i^{old}\|_0 \\ \text{subject to} \quad & |z_i^{new} - z_i^{old}| < \epsilon \end{aligned} \tag{9}$$

where 0-norm of a vector $\mathbf{v}$ is $\|\mathbf{v}_i\|_0$ is the number of non-zero entries in $\mathbf{v}_i$, solution to (9) is the minimum number of swapping required to make the attack successful and a meter i with higher metric will be considered more secure means the adversary need to swap several measurements to make the swapping attack hidden. In equation (9), we optimize over all re-ordering that lie under a threshold and its solution is $|a^*|$ that can be used to construct sparse attack. The constraint is to limit the attacker to manipulate relatively closer measurements where ϵ is some arbitrary number. The sparse attack vector as a result of optimization problem equation (9) can be formulated as

$$\mathbf{a} = \begin{cases} z_i^{new} - z_i^{old} & : z_i \notin S_m \\ 0 & : otherwise \end{cases}$$

where S_m denotes the set of secured measurements.

We now combine the intuitions attained for the above scenario and propose Algorithm 1 to design the successful re-ordering attack. Step 1 is the input for the adversary about the knowledge of some previous plausible measurement vector M_{old}. From steps 2-6, our attacker which is in fact a man-in-the-middle receive all measurements from the sensors and made M_{new}. Steps 7-8 are the conditions for measurement swapping, after which, attacker successfully create a swapped measurement vector M_{new} ready to use for state estimation. The following arguments for the pre-condition prove its correctness: 1) The sufficient condition for the swapping attack to be not affected by the traditional bad data detection is $\epsilon < \tau$ and 2) As, for FDI attacks, $\mathbf{a}$ is defined to be non-zero entry corresponding to the attacked measurements and zero for the attacked ones. Similarly, for the re-ordering attack vector, as, the two swapped readings will get corresponding non-zero entries in $\mathbf{a}$ while un-swapped measurements will get zero in $\mathbf{a}$. Therefore, a necessary condition for a successful swapping attack is same as that for stealth FDI attacks, i.e., the bad data detection alarm is not triggered if $\mathbf{a}$ lies in the null-space of $\mathbf{I} - \mathbf{K}$.

Algorithm 1 Re-ordering Attack for scenario I

```
1:  Inputs:
        $M_{old} = \{z_1, \cdots z_m\}$
2:  Initialize:
        $hole \leftarrow hole\ in\ array\ M_{new}$
        $z_i \leftarrow measurement,\ i = 1, \cdots m$
3:  for t = 1 to length(M) do
4:      $z_t \leftarrow M[t]$
5:      $hole = t$
6:      $M_{new}[hole] = z_t$
7:      while hole¿0 do
8:          if $|z_{i(new)} - z_{i(old)}| < \epsilon$ then $z_{i(new)} = z_{i(old)}$
9:          else
10:         end if
11:     end while
12: end for
13: return $M_{new}$
14: $\mathbf{z} = M_{new}$
15: Solve $\mathbf{z} = h(\mathbf{x}) + \mathbf{e}$
16: Solve equation (7) for $\mathbf{x}$
17: Calculate Mean Square Error (MSE)
```

B. Scenario II

For this case, the model is same as for scenario I with an additional constraint of a scalar multiple. This attack can be regarded as a constrained injection or injection-swapping attack. Here, to make the attack more effective, the adversary swap the measurements with a scalar multiple of one of the previous plausible data sets. The security metric defined in (9) is appropriate to measure the minimum possible sparsity pattern of the attack vector regardless of whether the magnitude is high or low. However, it is also possible that some attack vector may satisfy the sparsity criteria but instead due to large magnitude, be caught in detection. Therefore, another metric to keep the magnitudes of the swapping attack vector as low as possible while making the attack successful is required.

$$\begin{aligned} \text{minimize} \quad & \|z_i^{new} - z_i^{old}\|_1 \\ \text{subject to} \quad & |z_i^{new} - z_i^{old}| < \epsilon \end{aligned} \tag{10}$$

where the 1-norm of a vector $\mathbf{v}$ is $\|v_i\|_1 := \sum | v_i |$ and ϵ is a predefined scalar which will limit the attacker to swap relatively closer measurements.

The above problem is a convex optimization problem and can be re-cast into a linear program. The solution of the re-scaled problem can be used to obtain $\mathbf{a}^*$ to achieve its goal of adding bad data and remaining unnoticed at the same time. The corresponding small magnitude swapping attack vector obtained after solving the problem (10)

$$\mathbf{a} = \begin{cases} z_i^{new} - d.z_i^{old} & : z_i \notin S_m \\ 0 & : otherwise \end{cases}$$

where d is an arbitrary scalar, "." represents element-wise scalar multiplication and S_m is the set of protected measurements as already defined.

V. Numerical Results

Before going into the detail of simulation results, it should be recalled that to perform re-ordering attacks, the attacker does not require the topology/subspace knowledge of the system unlike already proposed attack strategies. In this section, we discuss the performance of the above mentioned model in constructing the re-ordering attacks in both scenarios by simulations on IEEE 14 and 30-bus systems. It is worth mentioning here that for both scenarios discussed the following two conditions hold: firstly, without any re-ordering, it only takes 4 iterations till convergence and secondly, measurement re-ordering attack is performed after each complete round of WLS. The technique used to estimate the state is WLS and MATPOWER is used for loading the data for AC model.

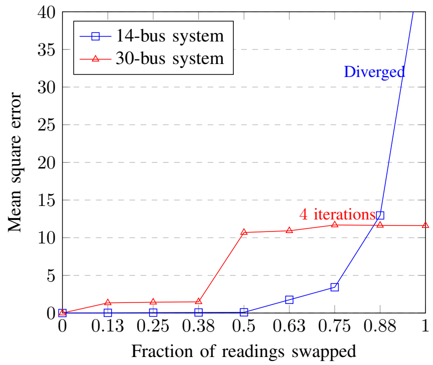

Figure 3: Mean square error when re-ordering attack is performed for scenario I with the same flat start for every round of WLS

Mean square error (MSE) for performing re-ordering attacks of the type described in scenario I, is illustrated in Fig. 3 for 14 and 30-bus systems while taking flat start for H. No reasonable attack impact is seen till 40% of reading are swapped for both the cases. However, afterwards, adequate increase in attack impact when more than 40% of total measurements are re-ordered can be seen. For all the cases of re-ordering, the state estimation converges despite having false data except when about more than 90% measurements are swapped in 14-bus system. It can be observed that for larger systems, the impact of swapping attack is higher as compared to 14-bus except for the case when the state estimation diverges. It is worth noting here that the case considered for this scenario is a particular one and other cases may exist. In Fig. 5, mean square error is shown when Jacobian matrix $\mathbf{H}$ from previous round of WLS is used instead of flat start. This update affects the attack by two means: 1) it is more practical and 2) error propagation is even worse than that depicted in Fig. 3. Another important difference is the convergence of both test systems for every swapping unlike for scenario II having flat start for Jacobian where 14-bus system diverges when all measurement are re-ordered. But, the convergence rate becomes slow and even dead when we re-order more than half of the total measurements.

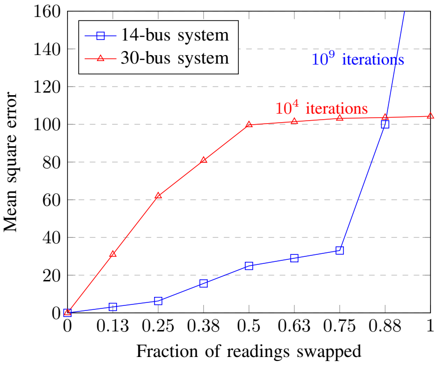

Figure 4: Mean square error when re-ordering attack for scenario I is performed with updated H for every round of WLS

Case II i.e. swapping the measurements with some scalar multiple of the respective readings in one of the preceding plausible measurement vectors can be seen in Fig. 5 for both 14 and 30-bus systems. Here, cost of re-ordering attack or fraction of measurements needed to be re-ordered is concerned, attacker has to swap at least 62% of measurements to get the maximum impact. It is worth mentioning here that there can be other cases for scenario II as well, however only one of them is discussed in which the scalar we are considering is $d = 3$ and the convergence time/number of iterations increased by the factor of 4 if compared with the no-attack case.

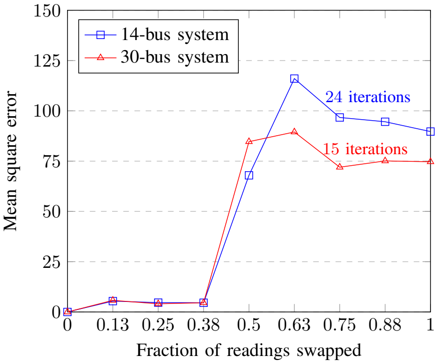

Figure 5: Mean square error when re-ordering attack is performed for scenario III

After examining all of the above simulation results, we can infer that these swapping attacks are most appropriate even when a part of the system is integrity- and confidentiality-protected. Another aspect is that for larger systems, attacker can achieve the error threshold with very low measurement re-ordering (cost) as in Fig. 3 and Fig. 5.

VI. Discussion

The measurement re-ordering attack as described in section IV is made to work even if some parts of power system are integrity protected. Key observation is that currently in our power grid, the measurements are not authenticated time-stamped to detect such re-ordering and such authentication for detection purposes is adequately expensive to implement atleast till near future. But, even assuming time-stamped authentication, which is offered by ISO/IEC 62351 but not widely deployed at present, re-ordering attacks may still succeed when combined with message spoofing. This implies that as long as there are old components in our power network, there can be a chance of these kind of attacks. But, in ten years time, cryptographically time-stamped authentication can be made possible leaving the re-ordering attack less effective.

VII. Conclusion

We have introduced a new attack on power systems termed as "re-ordering attacks", where the adversary uses swapping as a tool to change the order of data while not injecting or modifying any data. Due to targeted re-ordering, it become very difficult for the system operator to detect the source of the error. Three cases for the attacker depending upon the nature of swapping are discussed, and it is demonstrated that, in all of the described cases, we can be successful in achieving malicious goals i.e. state estimation converges for both cases but with an adequate error and even divergence. The significance of the presented attack lies in its applicability despite modern protections.

Our ongoing research includes determining the impacts of the re-ordering on hierarchical or 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.

***Acknowledgements*—This research was supported by a joint scholarship scheme between Pakistani HEC and RHUL. We are thankful to our colleague Alessio Baiocco who provided expertise that greatly assisted the research.**

References

[1] Phadke, A.: Synchronized Phasor Measurements: A Historical Overview. In: Proceedings of Transmission and Distribution Conference and Exhibition 2002: Asia Pacific. IEEE PES. Volume I., (October 2002) 476–479

[2] Abur, A., Exposito, A.G. In: Power System State Estimation: Theory and Implementation. CRC Press (March 2004)

[3] 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)

[4] D. Deka, R.B., Vishwanath, S.: Data Attack on Power Grid: Leveraging Detection, IEEE (February 2015)

[5] 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

[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] Kim, T.T., Poor, H.V.: Strategic Protection Against Data Injection Attacks on Power Grids. IEEE Transactions on Smart Grid **2** (June 2011) 326–333

[8] D. Deka, R.B., Vishwanath, S.: Optimal Hidden SCADA Attacks on Power Grid: A Graph Theoretic Approach, IEEE (2014)

[9] D. Deka, R.B., Vishwanath, S.: Data Attack on Strategic Buses in the Power Grid: Design and Protection, IEEE (July 2014)

[10] R. B. Bobba, K. M. Rogers, Q.W.H.K.K.N., Overbye, T.: Detecting false data injection attacks on DC state estimation. In: Proceedings of First Workshop on Secure Control Systems (SCS 2010), Stockholm, Sweden (April 2010)

[11] H. Sandberg, A.T., Johanasson, K.H.: On Security Indices for State Estimators in Power Networks. In: Preprints of the First Workshop on Secure Control Systems CPSWEEK 2010, Stockholm (2010)

[12] Dan, G., Sandberg, H.: Stealth Attacks and Protection Schemes for State Estimators in Power Systems. In: Proceedings of the 2010 first IEEE Smart Grid Communication, Gaithersburg, MD (October 2010) 214–219

[13] J. Kim, L.T., Thomas, R.J.: Data Framing Attack on State Estimation. IEEE Journal on Selected Areas in Communications **32** (2014)

[14] D. Deka, R.B., Vishwanath, S.: Optimal Data Attack on Power Grid: Leveraging Detection and Measurement Jamming. In: Proceedings of the 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm), Miami, FL, IEEE (November 2015) 392–397

[15] D. Deka, R.B., Vishwanath, S.: One Breaker is Enough: Hidden Topology Attacks on Power Grids. In: Proceedings of the 2015 IEEE Power and Energy Society General Meeting-, Denver,CO, IEEE (July 2015) 1–5

[16] Sanjab, A., Saad, W.: Smart Grid Data Injection Attacks: To Defend or Not? In: Proceedings of the 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm), Miami, FL, IEEE (November 2015) 380–385

[17] Sanjab, A., Saad, W.: Data Injection Attacks on Smart Grids with Multiple Adversaries: A Game-Theoretic Perspective. Number 99 (April 2016)

[18] Ahmed, M. Technology and Engineering. In: Power System State Estimation. Artech House (January 2013)

[19] Monticellii, A. Business and Economics. In: State Estimation in Electric Power System: A generalized approach. Springer Science and Business Media (May 1999)