International Journal of Latest Trends in Engineering and Technology
Vol.(10)Issue(2), pp.353-359
DOI: http://dx.doi.org/10.21172/1.102.57
e-ISSN:2278-621X

ANALYSIS OF RESIDUAL SMEARING IN LEAST SQUARES STATE ESTIMATOR FOR VARIOUS FALSE DATA INJECTION ATTACK SCENARIOS

Reena Rajendra Ambekar[1], H. A. Mangalvedekar[2]

Abstract: Cyber physical systems (CPS) have become the order of the day. However they are vulnerable to threats under false data injection attacks. The system monitoring in most of the CPS is carried out using state variables of a system. State variables are the minimal set of variables using which one can obtain the entire behavior of the system. Hence generally the aim of the attacker is to bias the state variables of the system. The state variables (complex voltages at nodes) in power system are conventionally calculated using the power flow and power injections, state variables, and transmission system parameters which are measured in real time. If there are any errors in these measurements then the calculated state variables may be biased. This may mislead the power system operators.

Keywords – Cyber physical system, Least Square, Smearing, FDIA

1. INTRODUCTION

1.0 Introduction: The concept of state estimation in power system was introduced by Prof. F. C. Schweppe et al in the early seventies [1,2,3]. State estimation considers the availability of redundant measurements and uses the redundancy to obtain better state estimates even in the presence of erroneous measurements. They also proposed that residues of measurements be used to identify the erroneous measurements [4]. Residue of a measurement is the difference between the given measurement and estimated measurement. This residue is assumed to indicate the error in a given measurement. The residues suffer from the phenomenon of smearing wherein a true measurement may have a large residue indicating the measurement to be bad and a bad measurements may have very low residue meaning that the measurement is good [1,2,3,4]. Various search techniques have been proposed by researchers to identify the exact location of attacked/bad measurements [5,6]. .

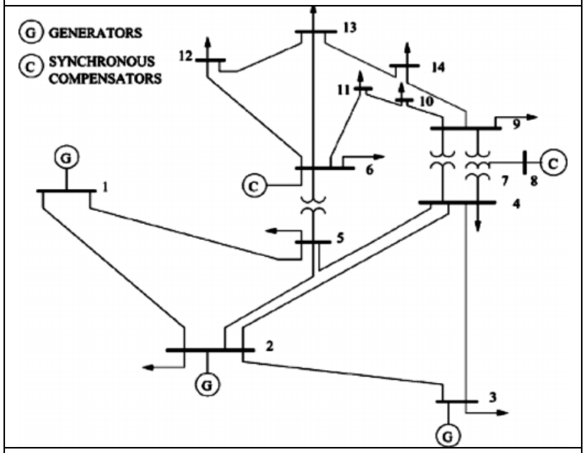
The introduction of cyber attack by Y.Liu et al [7] changed the scenario for identification of measurement errors drastically. They formulated the false data injection attacks (FDIA) on the smart grid accelerating the importance of identifying grossly erroneous measurements [8, 10]. The two basic types of attacks formulated in [7] were the targeted constrained attack and the targeted unconstrained attack. Many other methodologies of attack were then formulated by various researchers [9].

This paper discusses the identification of attack scenarios in least squares (LS) state estimators. In this paper the attack scenarios have been classified as (i) nodal attack, (ii) loop attack and (iii) combined nodal and loop attacks. The LS estimator performance and identification of such attack scenarios on the smearing phenomenon using the estimated state vector are discussed in this paper. With the help of illustrative examples it is shown that the nodal attack scenarios shows less smearing in comparison to the loop attack scenario. It is also shown that the combined loop and nodal attack completely biases the estimated state, leading to heavy residual smearing and may be quantified as a severe attack. During the studies it was also found that an attacker may not be able to attack measurements and introduce error magnitudes as per his wish. It was observed that there is a threshold for the errors introduced into the measurements during an attack. If the errors increase beyond the threshold the LS estimator may not converge. For small change in state variables large errors may be need to be injected into true measurements creating convergence problems. These are the limitations which an attacker may face when biasing a true measurement set. The IEEE-14 bus system is used for the examples. Total sixty eight measurements consisting of node voltages, injection measurements and line flows at one end are taken for simulation purpose. Table-1.1 shows state estimates (voltages and angles at the buses) obtained using the weighted least squares method with true measurements.

---

[1] Ph. D. Student, Electrical Engineering Department, Veermata Jijabai Technological Institute, Matunga, Mumbai 400019, India
[2] Retd. Professor, Electrical Engineering Department, Veermata Jijabai Technological Institute, Matunga, Mumbai 400019, India

Table1.1: State Estimate with LS Method using true Measurements

Bus No	Voltage magnitude in p.u.	Voltage Angle in Degrees
1	1.0205	0.0000
2	1.0043	-5.3715
3	0.9675	-13.7937
4	0.9723	-11.0518
5	0.9756	-9.4673
6	1.0282	-15.7146
7	1.0069	-14.0997
8	1.0430	-14.0804
9	0.9915	-15.7522
10	0.9917	-15.8946
11	1.0092	-15.5941
12	1.0099	-16.7946
13	1.0039	-16.7538
14	0.9783	-17.3101
		
IEEE-14 Bus System.		

2. CYBER ATTACK SCENARIOS

2.0 Attack scenarios : Mainly the node attack scenarios, loop attack scenarios and the combined node plus loop attack scenarios using the least squares state estimator are discussed in this paper.

2.1 Node Attack scenarios using LS method:

Attack Scenario-1:

2.1.1 .Intrusion into single injection measurement

Injection measurement at bus 2 is attacked: In this attack the Real Power value is changed from 0.1830 MW to 0.3660 MW, i.e. it is biased by 100% of the true value. The table-1.1 gives the measurements which have large residues.

Residue of the ith measurement is obtained from equation

$ri = zi-zi$ (estimate) …(1)

where ri is the residue corresponding to the ith measurement zi is the given measurement and Zi (estimate) is the estimated measurement.

Consider an attack on bus no. 2 wherein the real power injection measurement of bus 2 was corrupted by increasing it to twice its true value. It was observed that this does not affect the estimated voltage magnitude drastically from its true value. A small change in voltage angle of about one degree in all measurements except node-2 was observed. This indicates that the error due to attack is distributed amongst the state variables. Table 2.1.1 indicates the type of measurement, true value, error introduced and the magnitude of residue after attack. It also gives the maximum deviation in voltage magnitude and angle due to the attack.

Table-2.1.1 Measurements and their residues for attack on injection measurement-2.

S.No.	Measurement and Type of Measurement	Connection	True Value	Error introduced	Magnitude of Residue After Attack
1	Injection 1 Real	1-0	2.3200	0.0	-4.4902
2	Injection 2	2-0	0.1830	0.1830	-0.5072
3	Injection 3	3-0	-0.9420	0.0	1.8864
4	Injection 4	4-0	-0.4780	0.0	0.9442
29	Line flow Real	1-2	1.5708	0.0	-2.9767
30	Line flow Real	1-5	0.7551	0.0	-1.5076
31	Line flow Real	2-3	0.7340	0.0	-1.5115
33	Line flow Real	4-2	-0.5427	0.0	1.0881
37	Line flow Real	5-4	0.6006	0.0	-1.1654
38	Line flow Real	5-6	0.4589	0.0	-0.9636
SE result: The maximum deviation due to attack in voltage magnitude is 0.0146 and voltage angle is 0.8427.					

Observation from table 2.1.1: The attack on real power injection measurement at node -2 has the lowest residue. The line flow measurements connected to node-2 and node-5 i.e, 1-2, 4-2, 2-3 and 1-5, 5-4, & 5-6, along with neighboring injection measurements 1, 3 and 5 show large residues. This phenomenon of misrepresentation of the errors in measurements by the residues is known as smearing phenomenon. It may be concluded that the zone of network nodes 1 to 5 are attacked. Hence an attack is identified but not its exact location. It may also be noted that the largest residue is in the reference bus no.1. This indicates that the state estimator is trying to dump large quantity of error in the residue of reference bus.

Attack Scenario-2:

2.2. Intrusion of single line flow measurement

Line flow measurement connecting bus no.2 and bus no.3 is attacked. Measurement value is changed from 0.7340 MW to 1 MW, i.e. measurement value is attacked with an increase of 36.2% of true value.

2.2.1) Table with line flow measurement 2-3 attacked

S.No.	Measurement and Type of Measurement	Connection	True Value	Corrupted Value	Magnitude of Residue After Attack
1	Injection 1 Active	1-0	2.3200	2.3200	-4.6155
2	Injection 2	2-0	0.1830	0.1830	-0.5272
3	Injection 3	3-0	-0.9420	-0.9420	2.0933
4	Injection 4	4-0	-0.4780	-0.4780	0.8695
29	Line flow Real	1-2	1.5708	1.5708	-3.1124
30	Line flow Real	1-5	0.7551	0.7551	-1.4972
31	Line flow Real	2-3	0.7340	1.0000	-1.3259
32	Line flow Real	3-4	-0.2314	-0.2314	0.5889
33	Line flow Real	4-2	-0.5427	-0.5427	1.0457
37	Line flow Real	5-4	0.6006	0.6006	-1.2081
38	Line flow Real	5-6	0.4589	0.4589	-0.9316
SE result: The maximum deviation due to attack in voltage magnitude is 0.0093 and voltage angle is 0.2054					

Observation: Real power flow on line 2-3 attacked. Injection measurements 1, 3 & line flow measurements 1-2, 1-5, 2-3, 4-2, 5-4, 5-6 show large residues in comparison with other measurements. It may be noted that 2-3 has a large residue and is one of the erroneous measurements identified. The smearing phenomenon is also visible here. Hence the attack zone consists of nodes 1to 5. The algorithm tries to dump maximum error into the residue of node-1 (reference bus).

Attack Scenario-3:

2. 3. Intrusion into injection and one line flow measurement.

Injection measurement at bus 2 is attacked; value is changed from 0.1830 MW to 1 MW, i.e. 5.46 times of true value and Line flow measurement connecting bus no.2 and bus no.3 is attacked by changing measurement value from 0.7340 MW to 1 MW, i.e. measurement value is attacked 1.362 times of true value.

Table-2.3 Measurements and their residues

S.No.	Measurement and Type of Measurement	Connection	True Value	Corrupted Value	Magnitude of Residue After Attack
1	Injection 1 Active	1-0	2.3200	2.3200	-4.3582
2	Injection 2	2-0	0.1830	1.0000	-1.2229
3	Injection 3	3-0	-0.9420	-0.9420	2.3717
4	Injection 4	4-0	-0.4780	-0.4780	1.0935
29	Line flow Real	1-2	1.5708	1.5708	-2.6815
30	Line flow Real	1-5	0.7551	0.7551	-1.6708
31	Line flow Real	2-3	0.7340	1.0000	-1.6710
33	Line flow Real	4-2	-0.5427	-0.5427	1.3835
36	Line flow Real	5-2	-0.4081	-0.4081	1.1170
37	Line flow Real	5-4	0.6006	0.6006	-1.2722
38	Line flow Real	5-6	0.4589	0.4589	-1.0660
SE result: The maximum deviation due to attack in voltage magnitude is 0.0472 and voltage angle is 3.3813. .					

Observation: Real power injection at bus 2 and real power flow on line 2-3 attacked. Here also the zone of attack is nodes 1 to 5. It may be noted that line flow 2-3 and injection -2 have large residues but not the largest or second largest residue. The algorithm tries to dump maximum error into the residue of node-1 (reference bus).

Attack Scenario-4 :

2.4 .Targeted constrained attack; A= [H]C formulation:

In this attack, the attacker is constrained to accessing some specific meters. It is assumed in this attack that the attacker has knowledge of the complete system, has taken control of all the operations and knowhow of the SCADA system. Targeted constrained attack results when attacker corrupts certain state variable by inserting specified or known amount of error to the state variable. Thus error inserted is specific. Targeted constrained attack is possible only when the equation a= [H]c condition is satisfied. The attacker decides the deviation needed in the state variable and then using the [H] matrix obtains the attack vector a. The measurements are then modified to obtain the attacked measurement set using the equation Z attacked = Z+a. The Least Square state estimation method is used to obtain the state estimates i. e. voltages and angles of 14 bus system. Thus estimation by WLS method is used before and after attack cases. Residue obtained by actual and estimated measurements are used to find the measurements sets which are biased in the process.

The attacked measurements and their values in the set at node-2 using targeted constrained attack. Attack is carried out by corrupting bus 2 by 2% of true value.

2.4 Measurements and their residues:

S.No.	Measurement and Type of Measurement	Connection	True Value	Given measurement	Magnitude of Residue After Attack
1	Injection 1 Real	1-0	2.3200	2.7090	-4.7376
3	Injection 3 Real	3-0	-0.9420	-0.7525	1.5461
15	Injection 1 Reactive	1-0	-0.1523	1.5649	-1.2100
16	Injection 2 Reactive	2-0	0.3523	-2.9515	2.5989
17	Injection 3 Reactive	3-0	0.0876	0.5619	-0.9070
18	Injection 4 Reactive	4-0	0.0390	0.5533	-0.9002
19	Injection 5 Reactive	5-0	-0.0160	0.5142	-0.8164
29	Line flow Real	1-2	1.5708	1.9598	-3.3335
30	Line flow Real	1-5	0.7551	0.7551	-1.3982
31	Line flow Real	2-3	0.7340	0.5330	-1.1608
37	Line flow Real	5-4	0.6006	0.6006	-1.1204
49	Line flow reactive	1-2	-0.1748	1.5424	-1.2412
53	Line flow reactive	4-2	0.0213	0.5356	-0.7090
SE result: The maximum deviation in voltage magnitude is 0.1920 and voltage angle is 5.3069 .					

Observation: The constrained attack was designed to bias the voltage angle at node 2 by 2.5% of its true value. The zone of attack indicated by measurement residues are nodes 1 to 5 and associated line flows. The largest residue is at the reference bus -1. Since it is a targeted constrained attack the residues of the nearby nodes of 2 are also affected because of bad data in them. Errors in state variable have shown large residues in the connected lines and neighboring nodes. This being a massive attack it should be understood from the residues as targeted attack since it has affected all the nodes associated with bus 2. The associated nodes are 1, 3, 4&5. Both real and reactive measurements are attacked. Smearing phenomenon exists.

Important Note: This attack is based on the assumption that the attacker is knowledgeable about the system and he could manipulate the state variables as per his wishes. The attack when implemented indicated that there is upper threshold for manipulating the state variables by changing the power and state variable measurements. It was observed that when the associated measurements were biased as per a= Hc in order to bias certain state variables in C there was a threshold (error which could be implanted into state variables) on c. If the error introduced in the measurements increases the upper threshold, the state estimator may face difficulties in convergence. This was also true for targeted unconstrained attack discussed in the next example.

The phenomenon clarified that it is not easy to bias the state variables by injecting errors in associated node and line flow measurements. The attacker should have adequate system knowledge. He should be able to decide the thresholds to bias different meters, for various attack conditions, loading conditions and network configurations.

3.1 Loop attack scenarios using LS method:

Attack on loop 6-12-13-14-9-10-11-6

Sr.no	Connection Real power	Measurement True	Attacked value	Magnitude increase
1	6-12	0.0806	1	12.4
2	12-13	0.0188	0.5	26.56
3	13-14	0.0646	1.5	23.21
4	14-9	0.0863	1	11.58
5	9-10	0.0439	2	45.55
6	10-11	-0.0461	1	-21.73
7	11-6	0.0817	0.75	9.17
SE result: The maximum deviation in voltage magnitude is 0.185 and voltage angle is 17.8 degrees				

Table-3.1.1. Measurements and their residues.

S.No.	Measurement and Type of Measurement	Connection	True Value	Corrupted Value	Magnitude of Residue After Attack
1	Injection 1 Active	1-0	2.3200	2.3200	-4.6738
3	Injection 3	3-0	-0.9420	-0.9420	1.6945
7	Injection 7	7-0	0	0	-0.8690
9	Injection 9	9-0	-0.2950	-0.2950	-2.1570
10	Injection 10	10-0	-0.0900	-0.0900	1.3590
14	Injection 14	14-0	-0.1490	-0.1490	2.0045
16	Injection 2	2-0	0.3523	0.3523	-0.8744
29	Line flow Real	1-2	1.5708	1.5708	-3.0902
30	Line flow Real	1-5	0.7551	0.7551	-1.5777
31	Line flow Real	2-3	0.7340	0.7340	-1.3993
33	Line flow Real	4-2	-0.5427	-0.5427	1.0231
38	Line flow Real	5-6	0.4589	0.4589	-2.0466
42	Line flow Real	7-9	0.2707	0.2707	-1.4085
46	Line flow Real	11-6	0.0817	0.7500	1.0036
48	Line flow Real	13-14	0.0646	1.5000	0.9699

Observation: Tables 3.1. and 3.1.1 indicates the following.

Largest magnitude deviation in a nodal attack case is comparable with the loop attack case. However the largest angle deviation is much larger than the node attack case. It was observed that smearing is more in loop attack in comparison with nodal attack.

4.1 Combined loop + node attack scenario using LS method:

Attack on bus 6 and loop 2-3-4-2 (node + loop attack)

Injection measurement- 6 is attacked by introducing 2% error in it and loop 2-3-4-2 as in table 4.1.

Table- 4.1 True Measurements and its attacked values.

Sr.No	Connection Active	Measurement True	Attacked value	Magnitude increase
1	2-3	0.7340	1	1.3623
2	3-4	-0.2314	-0.5	2.1608
3	4-2	-0.5427	1	-1.8426

Table- 4.2 True and estimated voltage magnitudes and angles for loop cum node attack

Bus No	True Voltage magnitude in p.u.	Voltage magnitude after attack at node 6	Voltage magnitude Deviation	True Angle in Degrees	Angle in degrees after attack at node 6	Voltage angle Deviation
1	1.0205	1.6475	-0.6270	0	0	0
2	1.0043	1.6345	-0.6301	-5.3715	-2.0887	-3.2828
3	0.9675	1.5995	-0.6321	-13.7937	-6.1981	-7.5957
4	0.9723	1.6102	-0.6379	-11.0518	-3.7506	-7.3012
5	0.9756	1.6102	-0.6346	-9.4673	-3.1460	-6.3213
6	1.0282	1.4514	-0.4232	-15.7146	-4.9058	-10.8089
7	1.0069	1.6433	-0.6363	-14.0997	-4.2878	-9.8119
8	1.0430	1.6625	-0.6195	-14.0804	-4.1741	-9.9062
9	0.9915	1.6343	-0.6428	-15.7522	-4.8294	-10.9228
10	0.9917	1.6330	-0.6413	-15.8946	-4.8431	-11.0515
11	1.0092	1.6403	-0.6311	-15.5941	-4.7446	-10.8495
12	1.0099	1.6555	-0.6456	-16.7946	-5.1197	-11.6749
13	1.0039	1.6481	-0.6442	-16.7538	-5.1013	-11.6526
14	0.9783	1.6331	-0.6547	-17.3101	-5.2669	-12.0432

Maximum voltage magnitude deviations	0.6547	Maximum voltage angle deviations	12.04

Table-4.3 Measurements and their residues.

S.No.	Measurement and Type of Measurement	Connection	True Value	Corrupted Value	Magnitude of Residue After Attack
1	Injection 1 Active	1-0	2.3200	2.3200	-4.4142
3	Injection 3	3-0	-0.9420	-0.9420	3.5616
6	Injection 6	6-0	-0.1120	-2.1919	2.3166
13	Injection 13	13-0	-0.1350	0.8775	-1.0374
19	Injection 5	5-0	-0.0160	1.2816	-1.6172
20	Injection 6	6-0	0.1550	-5.4977	5.3527
27	Injection 13	13-0	-0.0580	1.8494	-2.2091
29	Line flow Real	1-2	1.5708	1.5708	-3.1721
30	Line flow Real	1-5	0.7551	0.7551	-1.2363
31	Line flow Real	2-3	0.7340	1.7340	-1.1122
32	Line flow Real	3-4	-0.2314	-0.7314	0.9898
33	Line flow Real	4-2	-0.5427	0.4573	1.7529
37	Line flow Real	5-4	0.6006	0.6006	-1.1741
58	Line flow reactive	5-6	-0.2084	1.0892	-1.1068
59	Line flow reactive	6-12	0.0317	-1.0040	0.9184
60	Line flow reactive	6-13	0.0998	-1.9015	1.6579
66	Line flow reactive	11-6	-0.0864	1.2134	-1.2841

Observation: Comparison of the state variables before and after the attack in table 4.2 shows that all the state variables have deviated from their true values. This indicates that a node plus loop attack biases almost all the state variables. Table 4.3 shows large residues in many measurements, indicating extreme smearing. This indicates that the simultaneous node cum loop attack is a deadly attack when LS method is used for estimation. Hence LS method should be used only when all the measurements are true and there is no major attack on measurements.

3.CONCLUSION

Smearing is a major drawback when least squares state estimation is used. The node attack scenario has less smearing in comparison with the loop attack scenario. A combination of loop plus node attack biases the estimated state variables away from their true values. Thus the node cum loop attack is very dangerous when LS estimator is used.

However the LS estimator is sensitive to the error added to the measurement. If the error added to the measurements is large such that it deviates the designated state variable beyond a certain threshold then it leads to convergence difficulties in the state estimator. Further research is needed to identify the magnitude of error and the damage it causes to the system for various system conditions.

4. REFERENCES

[1] F. C Schweppe and J.Wildes; Power system static state estimation, Part-1, exact model; .IEEE Tr. Power App. And System; Vol. PAS- 89, No.1, PP. 120-125; Jan 1970.

[2] F. C Schweppe and D. Rom; Power system static state estimation, Part-2, Approx. model; .IEEE Tr. Power App. And System; Vol. PAS- 89, No.1, PP. 125-130; Jan 1970.

[3] F. C. Schweppe; Power system static state estimation, Part-3, Implementation; IEEE Tr. Power App. And System; Vol. PAS- 89, No.1, PP. 130-135; Jan 1970.

[4] E. Handschin, F. C. Schweppe , J. Kohlas, A. Fiechter; Bad data analysis for power system state estimation; IEEE Tr.. Power App. And System; March /April 1975.; Vol. PAS- 94, No.2, PP. 329-337; March- April 1975.

[5] A. Monticelli and A. Garcia; “Reliable bad data processing for real time state estimation”; IEEE Tr.. Power App. And System; March /April 1975. Vol. PAS- 102, No.5, PP. 1126-1139; May- 1983.

[6] L. Mili, Th. Van Cutsem, and M. RibbensPavella; “Hypothesis testing and identification, A new method for bad data analysis in power system state estimation”; IEEE Tr. Power App. And System; March /April 1975; Vol. PAS- 103, No.11, PP. 3239-3252; Nov- 1984.

[7] Y. Liu, M.K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids", in CCS '09:Proceedings of the 16th ACM Conference on Computer and communications security, pp. 21-32,2009

[8] Aditya Ashok, Adam Hahn, ManimaranGovindarasu; Cyber–physical security of wide area monitoring, protection and control in a smart grid environment. Cairo University, Journal of Advanced research; Elsevier B. V; 2014.

[9] Detection of False Data Injection Attacks in Smart-Grid Systems Po-Yu Chen*, Shusen Yang*, Julie A. McCann*, Jie Lin+ ,Xinyu Yang+ *Imperial College London, United Kingdom +Xi’an Jiaotong University, China

[10] D. B. Rawat and C Bajracharya ;Detection of False Data Injection Attacks in Smart Grid Communication Systems; IEEE Signal Processing Letters > Volume: 22 Issue: 10, April 2015.