Stealth Attacks and Protection Schemes for State Estimators in Power Systems

Authors: Gyorgy Dan and Henrik Sandberg

Presenter: Shan Liu

Submitted in Partial Fulfillment of the Course Requirements for
ECEN 689: Cyber Security of the Smart Grid
Instructor: Dr. Deepa Kundur

May 02, 2011

Outline

Stealth Attacks

Stealth Attacks (also called false data injection attacks) are routing attacks which minimize the cost and visibility of the attacker but which are about as harmful as brute force attacks.

State Estimators facilitate accurate and efficient monitoring of operational constraints on quantities such as transmission line loadings or bus voltage magnitudes of power systems.

Motivation

- SCADA/EMS systems are increasingly more connected to the Internet. Data is often sent without encryption. Therefore, many potential cyber security threats exist for modern power control systems.
- Future smart power grids will be more dependent on accurate state estimators to fulfill their task of optimally and dynamically routing power flows.

P1: False data injection attacks against state estimation in electric power grids

Title:	**False data injection attacks against state estimation in electric power grids**
Authors:	Y.Liu, P.Ning, and M.Reiter
Appears in:	proceedings of the 16th ACM conference on Computer and Communication Security, 2009.

- An attacker can manipulate the state estimate while avoiding bad data alarms in the control center.
- Simple false-data attacks can often be constructed by an attacker with access to the power network model.

P2: Detecting false data injection attacks on DC state estimation

Title:	**Detecting false data injection attacks on DC state estimation**
Authors:	R.B.Bobba, K.M.Rogers, Q.Wang, H.Khurana, K.Nahrstedt, and T.J.Overbye
Appears in:	Preprints of the First Workshop on Secure Control Systems,2010.

- The operator can completely protect a state estimator from unobservable attacks by encrypting a sufficient number of measurement devices.
- The number of measurements need to be encrypted to ensure security is equal to the number of state variables in the system.

P3: On security indices for state estimators in power networks

Title:	**On security indices for state estimators in power networks**
Authors:	H.Sandberg, A.Teixeira,and K.H.Johansson
Appears in:	Preprints of the First Workshop on Secure Control Systems,2010.

- Two security indices were defined that quantify how difficult it is to perform a successful stealth attack against particular measurements.

Power Network Modeling

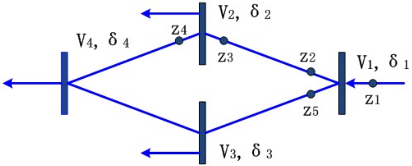

Fig. 1. A simple small 4-bus power network

V_i: voltage levels;
δ_i: bus phase angles;
z_i: power flow measurements.

Power Network Modeling

Consider a $n+1$ bus system

$$P_{ij} = \frac{V_i V_j}{X_{ij}} sin(\delta_i - \delta_j)$$

$$P_i = \sum_{k \in \mathcal{N}_i} P_{ik}$$

where $i, j = 1, \ldots, n+1$.

P_{ij}: active power flow from bus i to bus j;
V_i: voltage levels;
X_{ij}: reactance of transition lines;
δ_i: bus phase angles;
P_i: active power injections;
$\mathcal{N}_i$: set of all buses connected to bus i.

Power Network Modeling

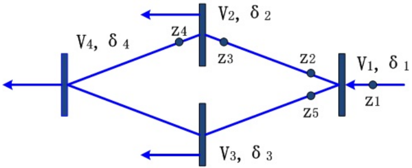

Fig.1. A simple small 4-bus power network

Using the measurements z_1 and z_2, we obtain

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} P_1 \\ P_{12} \end{pmatrix} + \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = \begin{pmatrix} \frac{V_1 V_2}{X_{12}} sin(\delta_1 - \delta_2) + \frac{V_1 V_3}{X_{13}} sin(\delta_1 - \delta_3) \\ \frac{V_1 V_2}{X_{12}} sin(\delta_1 - \delta_2) \end{pmatrix} + \begin{pmatrix} e_1 \\ e_2 \end{pmatrix}$$

Power Network Modeling

In general, the model can be written as

$$z = P + e = h(x) + e$$

$z \in \mathbb{R}^m$:	m active power flow measurements;
P:	actual power flow;
$e \in \mathcal{N}(0, R)$:	independent random measurement noise (Gaussian distribution of zero mean);
$h(x)$:	power flow model;
$x \in \mathbb{R}^{n+1}$:	vector of $n+1$ unknown bus phase angles.

State Estimation

Assumption

- Fixed $\delta_1 := 0$ as reference angle. Therefore, only n phase angles δ_i have to be estimated.
- m active power flow measurements z_i are given.
- The voltage level V_i of each bus is known.
- The reactance X_{ij} of each transmission line is known.
- The phase differences $\delta_i - \delta_j$ in the power network are small.

The linear approximation can be obtain by

$$z = Hx + e$$

where $H \in \mathbb{R}^{m \times n}$ is a constant Jacobian matrix.

State Estimation

Then the estimation problem can be solved by

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

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

$$\hat{z} = H\hat{x} = H(H^T R^{-1} H)^{-1} H^T R^{-1} z := Kz$$

where K is the hat matrix.

State Estimation

Bad Data Detection system identify faulty sensors and bad data by calculating the measurement residue which is defined as

$$r := z - \hat{z} = P + e - H\hat{x} = (I - K)z$$

If the residue r is larger than expected, then an alarm is triggered and bad measurements z_i are identified and removed.

Stealth Attacks

Consider a $n+1$ buses power system with m meters

- An attacker is able to change some, or all, of the measurements from z into $z_a := z + a$, where attack vector a is the corruption added to the real measurement z.
- The attacker's goal is to fool the EMS and the human operator either by physically tampering with the individual meters or by getting access to some communication channels.

Stealth Attacks

Recall

- An attack is undetectable if $a = Hc$, where c is estimation errors due to a.
- And we have $r := z - \hat{z} = P + e - H\hat{x} = (I - K)z$.

Therefore, a necessary condition for a successful stealth attack is that the Bad Data Detection system is not triggered if a lies in the nullspace of $I - K$.

Attack and Protection Cost Model

To capture the cost of the attacker and the system operator, we introduce a partition $\mathcal{M} = \{M_1, \ldots, M_{|\mathcal{M}|}\}$ of the set of measurements $\{1, \ldots, m\}$.

Assumption

- The attacker can attack any number of measurements in the same block M_j of the partition at unit cost.
- The operator can protect all measurements belonging to the same block M_j at unit cost.

Attack and Protection Cost Model

Stealth Meter Attacks: This scenario corresponds to a partition $\mathcal{M} = \{\{1\}, \ldots, \{m\}\}$ in which every measurement is a partition block.

- The attacker has to gain access to each individual meter it needs to compromise in order to achieve its attack goal.
- The cost of the attacker is the number of meters that have to be compromised.
- The protection cost of the operator is the number of meters that are protected.
- This scenario corresponds to physically tampering with the individual meters.

Attack and Protection Cost Model

Stealth RTU Attacks: This scenario corresponds to a partition of size $|\mathcal{M}| = n + 1$ in which the measurements in a bus form a partition block, and there is an RTU associated to every bus.

- An attacker that gains access to an RTU or its communication channel can compromise any number of measurements associated with the RTU.
- The cost of the attacker is the number of compromised RTUs.
- The protection cost of the operator is the number of RTUs that are protected.
- This scenario corresponds to attacks on the communication channels that carry the measurement data from individual RTUs, typically the load and branch power flows into the corresponding bus.

Minimum Cost Stealth Attacks

In order to find a minimal stealth attack on measurement k, the attacker has to solve the problem

$$\alpha_k := \min_c ||S|Hc|||_0$$
$$s.t.$$
$$1 = \sum_i H_{ki} c_i$$
$$(Hc)_j = 0 \quad \forall j \in \mathcal{P}$$

$\mathcal{P}$:	the subset of the partition protected by the operator;
$\mathcal{S}$:	$\lvert\mathcal{M}\rvert \times m$ matrix whose element $\mathcal{S}_{jk} = 1$ if $k \in M_j$, and $\mathcal{S}_{jk} = 0$ otherwise;
$\lvert a\rvert$:	the vector of the magnitudes of the elements in a;
$\lvert\lvert\cdot\rvert\rvert_0$:	the number of non-zero elements in a vector;
$\lvert\lvert S\lvert a\rvert\rvert\rvert_0$:	the cost of an attack a for the attacker;
H_{ki}:	the element (k, i) of H.

Minimum Cost Stealth Attacks

An attacker would be interested in finding an attack vector $a \neq 0$ with minimum cost, i.e., The number of partition blocks to which the compromised meters belong should be minimal, with the constraint that the attacker cannot compromise any protected measurement $k \in \mathcal{P}$.

To optimize over all corruptions $a = Hc$ that do not trigger bad data alarms and do not involve compromising protected measurements. A solution c^* can be re-scaled to obtain $a^* = a_k Hc^*$ such that the measurement attack $z_a = z + a^*$ achieves that attacker's goal and corrupts as few blocks of measurements as possible.

Minimum Cost Stealth Attacks

Therefore, $\alpha_k = ||\mathcal{S}|a^*|||_0$ blocks of measurements have to be corrupted to manipulate the measurement z_k.

The lower bound $\alpha_k = ||\mathcal{S}|a^*|||_0 \geq 1$ holds, since at least one measurements is corrupted.

Since the problem is non-convex and is generally hard to solve for large problems, we can use upper bound on α_k by looking at the kth row of H to calculate the optimal solution.

Minimum Cost Stealth Attacks

Upper Bound on the Minimum Cost: Any column i of H with a non-zero entry in the kth row of H can be used to construct a false data attack vector a that achieves the attack goal, if $H_{ji} = 0, \forall j \in \mathcal{P}$.

Assume that H_{ki} is non zero, we obtain an upper bound $\hat{\alpha}_k$ by

$$\hat{\alpha}_k := \min_{i:H_{ki} \neq 0} ||S|H_{.,i}|||_0$$

Where $H_{.,i}$ denotes the ith column of H.

Since H is typically sparse for power networks, this bound is very fast to compute, and exists whenever $\mathcal{P} = \emptyset$.

Finding the Minimum Cost Attack

Finding α_k is equivalent to finding a set of rows $N \subseteq \{1, \dots, m\} \backslash \{k\}$ that is maximal in terms of the number of partition blocks M_j it covers, and for which the following two conditions hold

$$rank(H_N) = n - 1$$

$$rank(H_{N \cup \{k\}}) = n$$

H_N: submatrix of H formed by the rows in N.

Given N the attack can be constructed by calculating the nullspace of the submatrix H_N, which is 1 dimensional due to the rank-nullity theorem.

Since $\forall c \in null(H_N)$ we have $(Hc)_k = 0$, $\forall k \in N$, and N is maximal, it follows that $\alpha_k = ||\mathcal{S}|Hc|||_0$.

Finding the Minimum Cost Attack

$\mathcal{A}^{(1)} = \{M_j\},\ k \in M_j,\ \mathcal{A}^* = \emptyset$
for $i = 1$ to $|\mathcal{M}| - |\mathcal{P}|$
  for $A \in \mathcal{A}^{(i)}$
    $A' = \{l \mid l \in A, \nexists j \notin A\ s.t.\ j \sim l\}$
    if $rank(H_{\{1,\ldots,m\}\setminus A'}) = n-1$ and $rank(H_{(\{1,\ldots,m\}\setminus A')\cup\{k\}}) = n$ then
      $\mathcal{A}^* = \mathcal{A}^* \cup A$
    end if
  end for
  if $\mathcal{A}^* \neq \emptyset$ then return $\mathcal{A}^*$
  for $A \in \mathcal{A}^{(i)}$
    for $M_j \subseteq A$
      for $M_k \in \mathcal{N}(M_j), M_k \cap \mathcal{P} = \emptyset, M_k \cap A = \emptyset$
        $\mathcal{A}^{(i+1)} = \mathcal{A}^{(i+1)} \cup (A \cup M_k)$
      end for
    end for
  end for
end for

- Iteration starts with an attack that consists of the partition block to which measurement k belongs
- In iteration i the algorithm first considers all attacks of cost i
- For every attack $A \in \mathcal{A}^i$ it creates the corresponding attack A' by only keeping the rows l of H for which there is no row j not in attack A that is linearly dependent on row l $(l \sim j)$
- Verify if the set $N = \{1, \ldots, m\} \setminus A'$ satisfies the rank conditions
- If no such attack is found, the algorithm augments every attack $A \in \mathcal{A}^i$ of cost i with one additional partition block M_k that is unprotected $(M_k \bigcap \mathcal{P} = \emptyset)$ and is neighboring to a partition block already in the attack $(M_k \in \mathcal{N}(M_j)$ for some $M_j \subseteq A)$

The iterative augmentation algorithm used to calculate the attacks with minimal cost for measurement k

Protection Against Stealth Attacks

Consider the operator has a budget π in terms of the number of protected measurement partition blocks that it can spend.

The goal of the operator is to achieve the best possible protection of the state estimator against stealth attacks given its budget. Thus,

$$C_{\mathcal{M}}(\mathcal{P}) \leq \pi$$

$\mathcal{P}$: the set of chosen protected measurements;
$C_{\mathcal{M}}(\mathcal{P})$: the cost of protecting $\mathcal{P}$ considering the partition $\mathcal{M}$.

$C_{\mathcal{M}}(\mathcal{P})$ can be calculated as the number of partition blocks M_j s.t. $M_j \bigcap \mathcal{P} \neq \emptyset$.

Perfect Protection

Perfect Protection: No stealth attacks are possible in the set of protected measurements $\mathcal{P}$, i.e., $\alpha_k = \infty$, $\forall k \in \{1, \ldots, m\}$.

- **Stealth Meter Attacks**: The budget required to achieve perfect protection is $\pi = n$, since it is necessary and sufficient for the operator to protect $|\mathcal{P}| = n$ measurements chosen such that $rank(H_{\mathcal{P}}) = n$.
- **Stealth RTU Attacks**: For sparse power network graphs, the budget required to achieve perfect protection is $\pi \ll n$. Condition $\pi = n$ is not necessary, since the number of protected blocks can contain more than one measurement each.

Perfect Protection

The **RTU level power network graph** is the graph where each vertex is an RTU in the power system, and every edge is a transmission link between the RTUs.

Definition

A dominating set $\mathcal{P}$ of the RTU level power network graph is a subset of vertices such that each vertex not in $\mathcal{P}$ is adjacent to at least one member in $\mathcal{P}$.

Proposition

- A perfect RTU protection is a dominating set of the RTU level power network graph.
- A dominating set of the RTU level power network graph is not necessarily a perfect RTU protection.

Perfect Protection

Dominating Set Augmentation Algorithm (DSA):

- Initialize the set of protected measurements $\mathcal{P}$ with a minimal dominating set of the RTU level power network graph.
- Iterate over $k = \{1, \ldots, m\}$ and set $\mathcal{P} = \mathcal{P} \bigcup \{k\}$ if $\alpha_k < \infty$ for some k.

Non-perfect Protection

In practice the operator's budget π might be insufficient for perfect protection. Then the operator would be interested in protecting a set of measurements $\mathcal{P}$ that maximizes its protection level according to some metric.

- **Maximal Minimum Attack Cost**: The goal of the operator is to maximize the minimum attack cost among all measurements that are possible to attack.
- **Maximal Average Minimum Attack Cost**: The goal of the operator is to maximize the average minimum attack cost of the measurements that are possible to attack.

Non-perfect Protection

Maximal Minimum Attack Cost:Aims to find an optimal set of protected measurements $\mathcal{P}$ for given budget π.

$$\mathcal{P}^{MM} = \arg \max_{\mathcal{P}:C_{\mathcal{M}}(P)\leq\pi} \min_{k} \alpha_k$$

Most Shortest Minimal Attacks Algorithm (MSM):

- Initially set $\mathcal{P} = \emptyset$.
- In every iteration calculate α_k, $\forall k \in \{1, \ldots, m\}$ and $\min_k \alpha_k$.
- Pick a partition block M_j that appears in most minimal attacks $A \in \mathcal{A}^*$ with least cost, i.e., $C_{\mathcal{M}}(A) = \min_k \alpha_k$.
- Set $\mathcal{P} = \mathcal{P} \bigcup M_j$.
- Continue until $C_{\mathcal{M}}(P) = \pi$.

Non-perfect Protection

Maximal Average Minimum Attack Cost:Aims to find an optimal set of protected measurements $\mathcal{P}$ for given budget π.

$$\mathcal{P}^{MA} = \arg \max_{\mathcal{P}:C_{\mathcal{M}}(P)\leq\pi} \frac{1}{|\{k:\alpha_k \neq \infty\}|} \sum_{k:\alpha_k\neq\infty} \alpha_k$$

Most Minimal Attacks Algorithm (MMA):

- Initially set $\mathcal{P} = \emptyset$.
- In every iteration calculate α_k, $\forall k \in \{1,\ldots,m\}$.
- Pick a partition block M_j that appears in most minimal attacks $A \in \mathcal{A}^*$.
- Set $\mathcal{P} = \mathcal{P} \bigcup M_j$.
- Continue until $C_{\mathcal{M}}(P) = \pi$.

Minimum Cost Attack

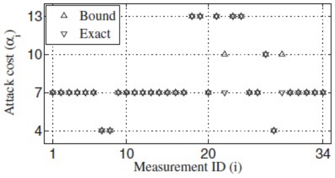

Fig.2. The minimum attack costs α_k and their upper bounds $\hat{\alpha}_k$ for the IEEE 14-bus network [1]

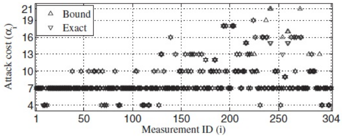

Fig.3. The minimum attack costs α_k and their upper bounds $\hat{\alpha}_k$ for the IEEE 118-bus network [1]

- Except for a few meters, the bound $\hat{\alpha}_k$ is almost always tight.
- Most measurements can be attacked by modifying only 7 measurements for both networks.
- The minimal attacks involve the same measurements for the meter attacks and the RTU attacks, because the meters that constitute the minimal attack belong to $\lfloor(\alpha_k - 1)/3\rfloor$ RTUs.

Protection Against Stealth Attacks

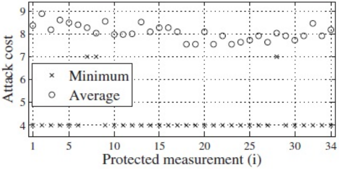

Fig.4. The minimum attack costs $\min_{k\neq i}\alpha_k$ and the average minimum attack costs $\sum_{k\neq i}\alpha_k/(m-1)$ as a function of $\mathcal{P}=\{i\}$ for meter attacks of IEEE 14-bus network [1]

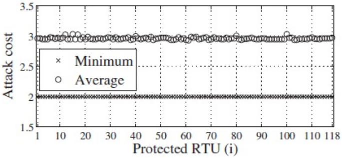

Fig.5. The minimum attack costs $\min_{k\neq i}\alpha_k$ and the average minimum attack costs $\sum_{k\neq i}\alpha_k/n$ as a function of $\mathcal{P}=\{M_i\}$ for RTU attacks of IEEE 118-bus network[1]

- The least minimum cost attack increases only when the protected measurements are the ones involved in the attack $A=\{7,8,28\}$.
- The average minimum cost attack shows some variation depending on the protected measurement.
- Protecting a single meter does not provide significant improvement in terms of minimum attack costs.

Protection Against Stealth Attacks

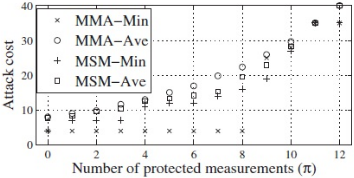

Fig.6. The minimum attack cost $\min_k \alpha_k$ and the average minimum attack cost $\sum_{k:\alpha_k<\infty} \alpha_k/|\{k : \alpha_k < \infty\}|$ for meter attacks of IEEE 14-bus network [1]

- Using MMA the average minimum attack cost increases with the protection budget, but the least minimum attack cost is unchanged while $\pi \leq 8$.
- Using MSM the minimum attack cost increases faster than using MMA, but the average minimum attack cost is lower.
- For a budget of $\pi = n = 13$ both MMA and MSM find the set of meters that provides perfect protection.
- Incremental protection of the meters does not lead to extra costs for the operator even if the ultimate goal is perfect protection.

Protection Against Stealth Attacks

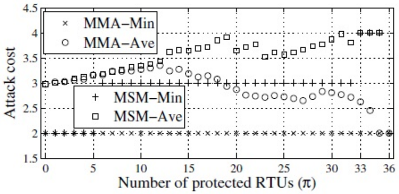

Fig.7. The minimum attack cost $\min_k \alpha_k$ and the average minimum attack cost $\sum_{k:\alpha_k<\infty} \alpha_k / |\{k : \alpha_k < \infty\}|$ for RTU attacks of IEEE 118-bus network [1]

- MSM and MMA achieve perfect protection by protecting 36 and 37 RTUs respectively.
- The minimal attacks and the average attack length are rather small even close to perfect protection.
- MSM outperforms MMA both in terms of minimal and average attack cost.
- Under the RTU attack cost model, perfect protection is desirable if all measurements are equally important.

Critical Assessment

- A contribution is an algorithm to compute a security index for a state estimator. This security index will identify which input sources to the state estimator are vulnerable to manipulate.
- Proposed an extension where clusters of measurements are available at the same cost for the attacker. This scenario is realistic if an attack is taking place from a substation, and potentially all measurements originating from the substation can be corrupted at once.
- Because the smart grid is going to rely on an accurate state estimation model more than the current electrical power system. This can be done by using encryption; however, it is expensive to install encryption. Therefore, the work in this paper can be used to identify locations where the encryption will have the most affect.

Conclusion and Future Work

- The paper proposed an efficient method for computing the security index α_k for sparse stealth attacks.
- Proposed an algorithm that can find the least cost false-data injection attack.
- Proposed a protection scheme for how to allocate encryption devices to strengthen security.
- It is also of interest to study reactive power flows and the voltage levels in the future.

References

[1] G. Dan and H. Sandberg, "Stealth Attacks and Protection Schemes for State Estimators in Power Systems", *in 2010 First IEEE International Conference on Smart Grid Communications*, 2010, PP.214-219.

[2] A. Abur and A. G. Exposito, *"Power System State Estimation: Theory and Implementation"*, Marcel Dekker, Inc., 2004.

[3] Y. Liu, P. Ning, and M. Reiter, "False Data Injection Attacks Against State Estimation in Electric Power Grids", *in Proceedings of the 16th ACM Conference on Computer and Communications Security*, Chicago, Illinois, 2009, pp. 21-32.

[4] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting False Data Injection Attacks on DC State Estimation", *in Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010*, 2010.

[5] L. Mili, T. V. Cutsem, and M. Ribbens-Pavella, "Bad Data Identification Methods in Power System State Estimation - A comparative Study", *IEEE Transactions on Power Apparatus and Systems*, vol. 104, no. 11, pp. 3037-3049, Nov. 1985.

[6] F.F. Wu and W.-H. E. Liu, "Detection of Topology Errors by State Estimation", *IEEE Transactions on Power Systems*, vol. 4, no. 1, pp. 176–183, Feb. 1989.