Protecting Critical Buses in Power-Grid Against Data Attacks: Adaptive Protection Schemes for Smart Cities

Charith Wickramaarachchi
Department of Computer Science
University of Southern California
Los Angeles, USA
cwickram@usc.edu

Charalampos Chelmis, Rajgopal Kannan and Viktor K. Prasanna
Department of Electrical Engineering
University of Southern California
Los Angeles, USA
{chelmis, rajgopak, prasanna}@usc.edu

***Abstract*—Accurate estimation of complex voltage phase angles at buses in the power-grid is crucial for determining the operational state of the power system. Existing methods for protection of the state estimate of critical buses against data injection attacks focus on design time assuming a static set of critical buses.**

We formulate a set of *optimal* protection schemes to enable operational time protection, where the set of critical buses that needs to be protected changes over time. Protection schemes are optimized against two dimensions: 1) cost of allocating the resources to secure measurements 2) cost of resource relocation. Given the intractable computation time complexity of *optimal* protection schemes, heuristic algorithms with reduced computation time complexity are presented.

Using simulations on transmission network datasets, we show that our heuristic algorithms yield good approximate results with low latency while being able to scale for large power transmission networks.

***Keywords*—smart-grid security; data injection attacks; adaptive protection**

I. Introduction

The unprecedented developments in Internet and sensor technologies (i.e. IoT) in the past years have accelerated the movement towards smart environments like smart mega cities [1] and smart-grids [2]. These smart environments consist of both cyber and physical components. Physical systems are governed by the laws of physics while cyber systems are used to control and monitor the state of the physical components. As an example, smart-grid consist of power transmission and distribution systems governed by power flow laws while the communication system is responsible for managing and monitoring these systems. Information available about the state of these environments can be used for cost-effective maintenance and protection.

In the case of a smart-grid power system, operating state is given by the complex phaser voltages at the buses [3]. The operational state of the system is continuously monitored by SCADA (Supervisory Control and Data Acquisition) systems.

Accurate state estimation is critical for maintaining the power system in a normal secure state [3]; Invalid state estimates can have severe socioeconomic impact [4], [5], [6]. Unfortunately state estimation is prone to data injection attacks (DIA) [7]. While existing bad data detectors in SCADA systems are capable of detecting random data injection attacks, in [7] Liu et al., showed that attackers could carefully formulate an undetectable structured DIA using the topological information of the power system. Methods to protect a given set of critical buses against DIAs have been proposed [8], [9].

Existing *protection schemes* for DIAs [10], [8], [9] are developed focusing on design time of the power grid assuming the set of critical buses does not change over time. A protection scheme finds a set of measurements to protect from data injections to secure a given set of critical buses. Existing approaches to protect measurements from such attacks include placing guards, video surveillance and tamper proofing the devices [8].

The critical set of buses in a smart-grid can change over time. As an example, even though the buses providing power to hospitals, universities, electric public transportation hubs can be considered critical on normal operating days, during a crisis, buses that distribute power to mission critical operation centers will be more critical. Data-driven methods have been discussed to find the strategic set of buses that needs to be protected using operational time data in power-grids [11]. We assert that protection schemes should adapt to these changes fast, so that adversaries will not be able to take advantage of such situations.

As shown in Figure 1 we assert a smart environment consist of multiple information layers. The critical set of buses that needs to be protected changes over time based on the dynamically changing inputs from other information layers (e.g. military intelligence, power consumption based data driven analytic results[11], weather data, etc.). An *adaptive protection scheme* should change the protection strategy (the set of measurement to protect) to protect the new set of critical buses from DIAs. The cost associated with protecting the measurements should be minimized in order to reduce the operational cost of smart-grid.

In this paper, we present a set of *adaptive protection schemes* against DIAs where the set of critical buses that needs to be protected change over time. Protection schemes

[1] http://www.energy.ca.gov/maps/

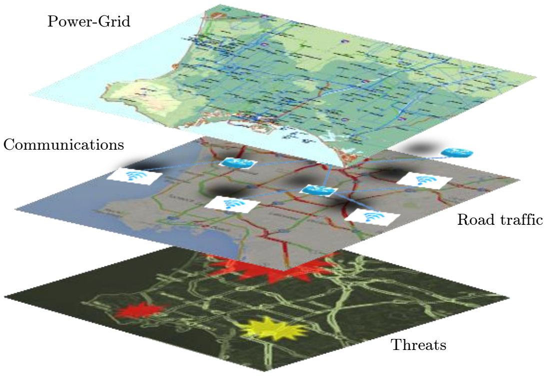


Fig. 1: Illustration of multiple information layers in a smart environment. (Image sources: Google maps and California energy commission maps[1])

are optimized against two dimensions: 1) *cost of allocating the resources to secure measurements* 2) *cost of resource relocation*.

Main technical contributions of this paper are summarized below:

- We formalize a set of optimal adaptive protection schemes against DIA. Protection schemes are optimized against two dimensions: 1) *cost of allocating the resources to secure measurements*. 2) *cost of resource relocation*.
- Due to the intractable computational time complexity of above mentioned *optimal adaptive protection schemes*, we propose a set of heuristic algorithms with reduced computational time complexity.
- Using simulations on transmission network datasets, we show that our heuristic algorithms provide good approximate results with low latency while being able to scale for large power transmission networks.

The rest of the paper is organized as follows. In Section II, we introduce necessary concepts and definitions used in this paper. Section III and IV presents our proposed protection schemes. We present related work in Section V. Section VI presents of our experimental evaluation results. Section VII draws our conclusions.

II. Background

In this paper, we focus on the DC power flow model (linearized) with n buses and m measurements [12]. States of the power system include voltage magnitudes and complex phase angles at buses. While voltage magnitudes can be directly measured at the buses, phase angles are determined using the power flow measurements of transmission lines [8]. In modern power systems, phase measurement units (PMUs) are installed on some buses, from which phase angles can be directly measured. In this paper, we consider a power system transmission network consisting of both power flow and direct phase measurements as it closely resembles modern power systems.

In the DC power flow model the relationship between measurements and the state of the buses is given by:

$$z = H\theta + e \tag{1}$$

$z \in \mathbb{R}^m$ is a vector of measurements, $\theta \in \mathbb{R}^n$ is a vector of state variables. H is the measurement matrix and $e \in \mathbb{R}^m$ represents measurement errors (noise).

Attackers can use an attack vector $a \in \mathbb{R}^m$ to introduce malicious data into the measurements, resulting in measurement vector $z = \bar{z} + a$, where $\bar{z}$ is the actual measurements. While the bad data detectors at SCADA systems can detect random, unstructured attacks, in [7] Liu et al., showed that attackers could carefully formulate a structured DIA such that $a = Hc$, to bypass existing bad data detectors undetected making the state estimate deviate by an arbitrary quantity.

In [8] Bi et al, proposed a method to protect a given set of state variables against DIAs based on a graph $G_H = (V, E)$ constructed using H as the incidence matrix. State variables θ and measurements z becomes vertices and edges in this graph. Specifically, given a transmission network topology and measurement information, G_H is constructed as follows:

- First, each state variable associated with a bus is represented as a vertex $v \in V$.
- Each flow measurement at transmission line is represented as an edge $e = (u, v) \in E$.
- A new vertex called reference vertex ($v_r \in V$) is introduced representing a bus with zero phase angle.
- Each direct phase measurement is denoted by an edge connecting the vertices associated with phase measurement with the reference vertex.

In [8], Bi et al showed that, in order to protect a given set of buses D from DIAs, it is sufficient and necessary to protect measurements represented by the edges in a Steiner tree of G_H that connect reference vertex and vertices that represent D ($V_D \subset V$). As a result, the minimum set of measurements to protect D against DIAs is given by the edges in Steiner minimum tree (SMT) with terminals $V_D \cup \{v_r\}$.

Figure 2 illustrates an example transmission network with measurement information and G_H constructed following above mentioned steps.

III. Optimal Adaptive Protection

The objective of an adaptive protection scheme for DIAs is to find a protection strategy (a set of measurements to protect) when the set of strategic buses change over time.

Specifically, let $D_t \subset \mathbb{I}$ be the subset of buses that are under protection from DIAs at time t where $\mathbb{I}$ is the set of all buses in the power system. Let $M_t \subset \mathbb{M}$ be the subset of measurements that are currently protected in order to secure D_t where $\mathbb{M}$ is the set of all measurements in the power system. If the subset of buses that needs to be protected changed at time $t+1$ to $D_{t+1} \subset \mathbb{I}$, an adaptive protection scheme finds $M_{t+1} \subset \mathbb{M}$ to be protected from data injections in order to secure D_{t+1} from DIAs at each time step t.

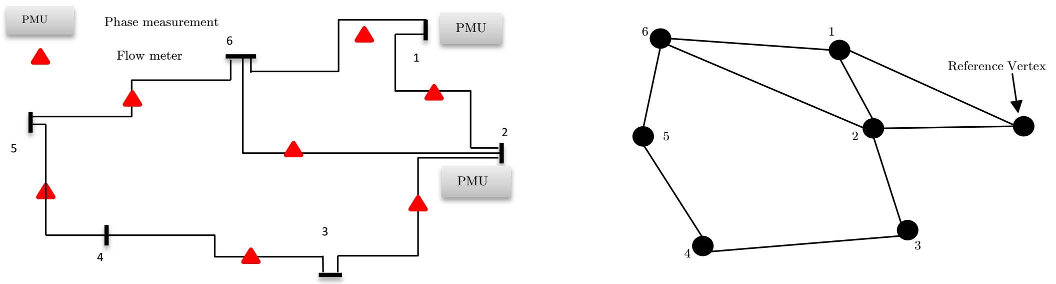


Fig. 2: 6 bus power transmission network with measurements (Left) and G_H constructed for the transmission network following the steps in Section II (Right)

In this paper, we present a set of adaptive protection schemes that minimizes the protection cost. We assert that the protection cost (P) in an adaptive protection scheme consists of two factors: 1) cost of allocating the resources to secure measurements (A) 2) cost of resource relocation (R).

As mentioned in section I, existing methods for protecting measurements include video surveillance, guards, and tamper proofing the equipment [8]. A is the cost associated with allocating these resources.

When the set of strategic buses changes, resources used for protecting the measurements may have to be relocated/activated/deactivated in order to protect a new set of measurements. The cost associated with resource relocation/activation/deactivation is defined as the cost of resource relocation (R). An optimal adaptive protection scheme finds a protection strategy with minimum protection cost (P) where P is defined as:

$$P = A + R \tag{2}$$

In this section, we formalize three such optimal adaptive protection schemes for different use cases.

A. Optimal Adaptive Protection with No Relocation Cost (NR)

We consider the scenario, in which relocation cost is zero. A smart-grid with surveillance instruments installed at all the measurement locations is an example. Surveillance devices do not have to be relocated as a result. We assume that a cost has to be paid for each active surveillance instrument. The objective is to minimize this cost.

As a result, minimum cost set of measurements to protect is given by the edges of a Steiner minimum tree (SMT) on G_H, where edge weights represent the cost of protecting associated measurements. This can be formulated as an integer linear program (ILP) [13] where $C(e)$ represents the cost of protecting each measurement represented by edge $e \in E$. This ILP use set of variables x_{t+1} where $x_{t+1}(e) \in \{0,1\}$. $x_{t+1}(e) = 1$ indicates $e \in E$ in the SMT. Terminal vertex set of Steiner tree is given by: $T_{t+1} = V_{D_{t+1}} \cup \{v_r\}$.

ILP to find the SMT is given below. This ILP considers all vertex partitions S_{t+1}, $\bar{S}_{t+1}$ of G that partition T_{t+1} to find the Steiner minimum tree. $\delta(S_{t+1})$ is the set of cross partition edges and $X(E')$ is a function that provides number of edges of $E' \in E$ in SMT.

$$\begin{aligned}
&\text{minimize} \sum_{e\in E} C(e) \times x_{t+1}(e)\\
&\text{subject to:}\\
&X(\delta(S_{t+1})) \geqslant 1\ \forall S_{t+1} \subset V : \emptyset \neq S_{t+1} \cap T_{t+1} \neq T_{t+1}\\
&x_{t+1}(e) \in \{0,1\}\ \forall e \in E
\end{aligned} \tag{3}$$

Measurements in M_{t+1} is given by the measurements associated with edges in this SMT.

SMT problem for weighted graphs is known to be NP-Hard [14].

B. Optimal Adaptive Protection with Minimum Change (MinDiff)

Next, we present MinDiff protection scheme, an extension of NR. We assume that the resource relocation cost is directly proportional to the magnitude of change in protection strategy formally defined as:

$$\sum_{e\in E} (x_{t+1}(e) - x_t(e))^2 \tag{4}$$

Where $x_t(e) = 1$ indicates that the measurement associated with $e \in E$ was in M_t.

A scenario in which activating and deactivating surveillance instruments incurs a fixed cost is an example usecase for this protection scheme. In MinDiff objective is to minimize the number of activations/deactivations while minimizing the resource allocation cost. MinDiff is formalized as an optimization problem below:

$$\begin{aligned}
&\text{minimize} \sum_{e\in E} C(e) \times x_{t+1}(e) + \sum_{e\in E} (\frac{C(e)}{2})(x_{t+1}(e) - x_t(e))^2\\
&\text{subject to:}\\
&X(\delta(S_{t+1})) \geqslant 1\ \forall S_{t+1} \subset V : \emptyset \neq S_{t+1} \cap T_{t+1} \neq T_{t+1}\\
&x_{t+1}(e) \in \{0,1\}\ \forall e \in E
\end{aligned} \tag{5}$$

The set of measurements to protect at time $t+1$ (M_{t+1}) for MinDiff is given by the measurements associated with edges in the Steiner tree given by x_{t+1}.

MinDiff is at least as computationally hard as NR, since NR is a special case of MinDiff.

C. Optimal Adaptive Protection with Minimum Transfer Cost (MinTC)

MinTC protection scheme assumes that the resources protecting the measurements can be relocated to other measurement locations. MinTC extends MinDiff by considering a transfer cost associated with each relocation. $R_{C_{t+1}}$ is the relocation cost matrix in which $R_{C_{t+1}}(i,j)$ provides the cost of transporting a resource from location i to j at time $t+1$. Set of locations (R_L) include all the measurement locations and the location of a resource hub (h) that maintains additional resources.

When there is a change in protection strategy, resources that protect measurements can be moved either to the resource hub or to a new measurement location that needs to be protected. Additional resources can also be transferred from the resource hub to new measurement locations if necessary. We assert that all resources should either protect measurements that need to be protected or should be transferred to the resource hub.

We define Δ_{t+1} as:

$$\Delta_{t+1}(i) = x_{t+1}(i) - x_t(i),\ i \in E \tag{6}$$

$\Delta_{t+1}(i) = 1$ indicates that measurement represented by i is a new measurement that should be protected where $\Delta_{t+1}(i) = -1$ indicates that the measurement represented by i no longer needs protection. $\Delta_{t+1}(i) = 0$ indicates that the measurement represented by i is in both protection strategies at time t and $t+1$. We enforce that these resources should not be moved.

Tr provides the optimal transfer schedule where $Tr(i,j) \in \{0,1\} = 1$ indicates a transfer of resource from location i to j.

Assuming a cost have to be paid for each resource that protects a measurement, optimal cost protection scheme for MinTC is formalized an optimization problem below:

minimize:

$$\sum_{e\in E} C(e) \times x_{t+1}(e) + \sum_{\forall i\in R_L}\sum_{\forall j\in R_L} R_{C_{t+1}}(i,j) \times Tr_{t+1}(i,j)$$

subject to:

$$\begin{aligned}
&X(\delta(S_{t+1})) \geqslant 1\ \forall S_{t+1} \subset V : \emptyset \neq S_{t+1} \cap T_{t+1} \neq T_{t+1}\\
&x_{t+1}(e) \in \{0,1\}\ \forall e \in E\\
&\forall i \in R_L \backslash \{h\} :\\
&Tr_{t+1}(i,k) = Tr_{t+1}(k,i) = 0,\ \forall \Delta_{t+1}(i) = 0,\ \forall k \in R_L\\
&\sum_{\forall k\in R_L} Tr_{t+1}(i,k) = 0,\ \sum_{\forall k\in R_L} Tr_{t+1}(k,i) = 1,\ \forall \Delta_{t+1}(i) > 0\\
&\sum_{\forall k\in R_L} Tr_{t+1}(i,k) = 1,\ \sum_{\forall k\in R_L} Tr_{t+1}(k,i) = 0,\ \forall \Delta_{t+1}(i) < 0\\
&\forall k,j \in R_L :\\
&Tr_{t+1}(k,k) = 0\\
&Tr_{t+1}(k,j) \in \{0,1\}
\end{aligned} \tag{7}$$

Constraints in the above optimization formulation for MinTC enforce following conditions:

- Edges associated with M_{t+1} makes a Steiner tree that spans $V_{D_{t+1}} \cup \{v_r\}$.
- Each new measurement ($\Delta_{t+1}(i) = 1$) should receive exactly one protecting resource (either from location with $\Delta_{t+1}(i) = -1$ or resource hub).
- Each old measurement ($\Delta_{t+1}(i) = -1$) should transfer its protecting resource (either to a location with $\Delta_{t+1}(i) = 1$ or to resource hub).
- Protecting resources associated with $\Delta_{t+1}(i) = 0$ should not be relocated.
- No self relocations.

The set of measurements to protect at time $t+1$ (M_{t+1}) for MinTC is given by the measurements associated with edges in the Steiner tree given by x_{t+1}.

MinTC is at least as computationally hard as NR, since NR is a special case of MinTC.

IV. Heuristic Algorithms For Optimal Adaptive Protection

Given the intractable computation time complexity of the optimal adaptive protection problems, we observed that it could take hours, even days or years to compute the optimal protection strategies on real scale transmission networks. An attacker can leverage these long time windows to attack unprotected measurements compromising the state estimate of critical buses. In order to address this challenge, we present a set of simple heuristic algorithms to compute protection strategies with low latencies on real scale transmission networks.

A. Heuristic For Optimal Adaptive Protection with No Relocation (H-NR)

A heuristic for NR is presented in Algorithm 1. Algorithm 1 takes graph G_H and a set of terminal vertices ($V_{D_{t+1}} \cup$

$\{v_r\}$) that represent the new set of critical buses (D_{t+1}) and reference vertex as input. G_H is constructed using the bus topology information as mentioned in Section II. The cost of protecting each measurement is represented as the edge weight of the associated edge.

Algorithm 1 finds a subgraph $SMT_{H_{t+1}}$ whose edges represent the set of measurements that needs to be protected at time $t+1$.

Algorithm 1 Heuristic Algorithm for Optimal Adaptive Protection with No Relocation

```
procedure HAP-NR($G$, $V_{D_{t+1}} \cup \{v_r\}$)
    Initialize $SMT_{H_{t+1}}$ by adding a $v \in V_{D_{t+1}} \cup \{v_r\}$
    while $SMT_{H_{t+1}}$ not contain all $v \in V_{D_{t+1}} \cup \{v_r\}$ do
        find a terminal vertex $v' \notin SMT_{H_{t+1}}$ closest to $SMT_{H_{t+1}}$
        Add shortest path that connect $v'$ to $SMT_{H_{t+1}}$
    return $SMT_{H_{t+1}}$
```

Proposition 1: Protecting the measurements associated with edges in $SMT_{H_{t+1}}$ is sufficient to protect D_{t+1} from DIAs.

It can be easily observed that $SMT_{H_{t+1}}$ spans all the terminal vertices in $V_{D_{t+1}} \cup \{v_r\}$. There exist a Steiner tree in $SMT_{H_{t+1}}$ which span $V_{D_{t+1}} \cup \{v_r\}$ as a result.

Shortest paths between all pairs of vertices are precomputed so that the shortest path information can be reused when recomputing the $SMT_{H_{t+1}}$ for a new set of critical buses.

$SMT_{H_{t+1}}$ can be further reduced by finding its minimum spanning tree and removing the leaf vertices (vertices with degree 1) that are not in $V_{D_{t+1}} \cup \{v_r\}$.

B. Heuristic For Optimal Adaptive Protection with Minimum Change (H-MinDiff)

A heuristic for optimal protection with minimum change extends the H-NR by reassigning the edge weights in G when computing $SMT_{H_{t+1}}$. Edge weights are reassigned by adding a penalty to the measurements that are not in M_t by increasing its protection cost. The objective is to maximize the reuse of M_t while minimizing the protection cost. Let E_{M_t} be set of edges that represent the measurements in M_t. Weight reassignment criteria is given below where $w(e)$ represents the edge weight of $e \in E$.

$$w(e) = \begin{cases} C(e), & \text{if } e \in E_{M_t}. \\ 2 * C(e), & \text{otherwise.} \end{cases} \tag{8}$$

$SMT_{H_{t+1}}$ is computed using Algorithm 1, once the weight reassignment is complete.

C. Heuristics For Optimal Adaptive Protection with Minimum Transfer Cost (H-MinTC)

We propose a set of heuristics for optimal adaptive protection with minimum transfer cost. The heuristic algorithm follows a structure similar to H-MinDiff where a penalty is added to the measurements that are not in M_t. We present two weight reassignment criteria where the penalty for an edge e is given by $R(e)$.

$$w(e) = \begin{cases} C(e), & \text{if } e \in E_{M_t}. \\ C(e) + R(e), & \text{otherwise.} \end{cases} \tag{9}$$

Minimum Transfer Cost From Existing Protected Measurements (H-MinTC-Min):

In this case, the penalty is defined as the minimum transfer cost from existing protected measurement locations or resource hub.

$$R(e) = min\{Tr(i, L(e)) | (i = h) \vee (i = L(e')),\ \forall e' \in E_{M_t}\} \tag{10}$$

Where $L(e)$ provides the measurement location associated with edge $e \in E$.

Maximum Transfer Cost From Existing Protected Measurements (H-MinTC-Max):

In this case, the penalty is defined as the maximum transfer cost from existing protected measurement locations or resource hub.

$$R(e) = max\{Tr(i, L(e)) | (i = h) \vee (i = L(e')),\ \forall e' \in E_{M_t}\} \tag{11}$$

Once $SMT_{H_{t+1}}$ is computed using Algorithm 1, transfer schedule is calculated using the steps summarized in Algorithm 2.

Algorithm 2 Find Transfer Schedule

```
 1: procedure CalculateTransfers($E_{M_t}, E_{M_{t+1}}, R_{C_{t+1}}$)
 2:     while all $E_{M_{t+1}} \setminus E_{M_t}$ have an assigned resource do
 3:         $(s, t) \leftarrow$ MinTransfer($R_{C_{t+1}}, E_{M_t}, E_{M_{t+1}}$)
 4:                 ▷ $s$ : existing resource location
 5:                 ▷ $t$ : measurement location that need protection
 6:         if $s \neq h$ and $(R_{C_{t+1}}(s, h) < R_{C_{t+1}}(s, t))$ then
 7:             AssignResource($s, h$)
 8:         else
 9:             AssignResource($s, t$)
10:     for each unassigned resource $s \in E_{M_t} \setminus E_{M_{t+1}}$ do
11:         AssignResource($s, h$)
```

Algorithm 2 follows a greedy assignment criterion. It initially reassigns resources to the measurements in $M_{t+1} \backslash M_t$. This assignment is done in a greedy manner (Line 2-9 in Algorithm 2). First, it finds the resource that can be transferred with the minimum cost to a measurement in $M_{t+1} \setminus M_t$. If transferring that resource to the hub is cost effective compared to the selected transfer, it assigns the resource to the hub. The resource is assigned to protect the measurement in $M_{t+1} \setminus M_t$ with minimum transfer cost otherwise. Remaining resources in $M_t \setminus M_{t+1}$ are moved to the hub, once all the measurements that need protection have assigned resources.

V. Related Work

In this section, we present a summary of the body of research closely related to this work.

Liu et al. in [7] are the first to show that an attacker can formulate a well-structured attack to bypass existing bad data detectors in the state estimator undetected. In [15] Kosut et al. showed a relationship between DIAs and network observability where data injection attack can only bypass the bad data detector undetected if and only if the network becomes unobservable when the attacked measurements are removed from the network. Bobba et al in [10] extended this result to show that it is necessary and sufficient to protect a set of basic measurements to be able to detect any DIA. Several studies have been conducted on different attack mechanisms of DIAs [16], [17].

The number of basic measurements in a power system is as same as the number of buses in the power system making it costly to protect all the buses from DIAs. In [8] Be et al. proposed protection strategy which can protect a given set of buses from DIAs. As mentioned in section II minimum set of measurements that needs to be protected to secure a given set of critical buses is provided by the edges of Steiner minimum tree that satisfy a given measurement to edge mapping rules. We built on top of this result where we consider the changes in the set of critical buses.

Steiner minimum tree is a well known NP-hard problem [14] in graph theory. Steiner tree of a graph spans a given subset of vertices. Steiner minimum tree is the minimum cost Steiner tree where cost is defined as the sum of its edge weights. Heuristic algorithms have been proposed [18] to find the SMT. In this paper, we adopt and extend the 2-factor shortest path heuristic for SMT [18], [19].

VI. Evaluations

We conducted a detailed experimental evaluation of above mention protection schemes using simulations on transmission network datasets. In this section, we present the details and results of these experiments.

A. Experimental setup

All the experiments were conducted on an Intel Core i5 3.20 GHz computer with 16GB RAM. Gurobi solver [20] was used to implement the NR, MinDiff and MinTC protection schemes (for exact solutions). We implemented heuristic algorithms (H-NR, H-MinDiff and H-MinTC) using Java 1.8. Graph-Stream library [21] was used for calculating shortest paths.

Six different power transmission network datasets downloaded from [22], [23] were used in our experiments. Details of these datasets can be found in Table I. EU 1497 is the main continental European transmission network downloaded from [22]. It is one of the largest transmission networks.

In our experiments, we placed the measurements so that the complete transmission network is observable [3] and power flow of each transmission line is measured. PMUs were assigned to 5% of the buses randomly.

Dataset	# of Buses	# of Transmission Lines
IEEE 14	14	20
IEEE 30	30	41
IEEE 57	57	80
IEEE 118	118	186
IEEE 300	300	409
EU 1497	1494	2322

TABLE I: Datasets

$\mid D \mid$	H-NR	H-MinDiff	H-MinTC-Min	H-MinTC-Max
3	0	0	0.04	0.04
5	0	0.1	0.03	0.03
7	0	0	0.02	0.07

TABLE II: Mean absolute percentage deviation of H-NR, H-MinDiff and H-MinTC compared to NR, MinDiff and MinTC on IEEE 9 dataset.

Resource relocation costs were generated randomly where it was normalized to a real number between 0 and 1. Unit measurement protection cost was assumed ($C(e) = 1, \forall e \in E$) in all experiments for simplicity.

B. Evaluation Results

We first used the IEEE 9 and IEEE 14 datasets to verify the correctness of proposed protection schemes. The cost of protection given by optimal protection schemes was then compared with the proposed heuristic algorithms. Table II and III presents the mean absolute percentage deviation (MAPD) of H-NR, H-MinDiff, H-MinTC-Min, H-MinTC-Max compared to NR, MinDiff and MinTC. We observed that our heuristics provides close approximations. On IEEE 9 and IEEE 14 datasets H-NR was able to find the optimal solution most of the time. Due to the computational intractability, implementations of NR, MinDiff and MinTC could not scale for large transmission networks. ILP for NR did not complete even after 24 hours on IEEE 57 dataset, confirming the need for fast heuristics.

Since no significant difference in MAPD between H-MinTC-Min and H-MinTC-Max was observed, we used H-MinTC-Min for the evaluations to follow (referred as H-MinTC).

Next, we evaluated our adaptive protection schemes to observe its behavior over longer periods of time and compared the results with optimal solutions. In this setup, we ran the adaptive protection schemes over multiple iterations. In each iteration t set of buses that needs protection change from D_{t-1} to D_t. Adaptive protection schemes use M_{t-1} that was calculated in iteration $t-1$ to calculate M_t. We compared H-NR, H-MinDiff and H-MinTC with NR, MinDiff and MinTC

$\mid D \mid$	H-NR	H-MinDiff	H-MinTC-Min	H-MinTC-Max
3	0	0	0.21	0.13
5	0	0.1	0.08	0.12
7	0	0	0.01	0.04
9	0	0.09	0.13	0.13
11	0	0.14	0.10	0.07

TABLE III: Mean absolute percentage deviation of H-NR, H-MinDiff and H-MinTC compared to NR, MinDiff and MinTC on IEEE 14 dataset.

to see the evolution of protection cost (P) over multiple iterations.

Figure 3 shows the evolution of protection cost over multiple iterations where $| D_{t-1} |=| D_t |$ for each iteration t. As observed, protection cost of heuristic algorithms does not increase with t compared to exact solutions making them suitable for long running operations.

One might notice that in some instances in Figures 3, the cost of protection given by H-MinDiff and H-MinTC is lower than the exact solutions. It is important to note that, even though in iteration 1 both exact and heuristic protection schemes start with the same M_0, over iterations measurement sets that need to be protected found by heuristic and exact protection schemes (M_{t+1}) diverge. This can result in scenarios, where in some iterations t, the cost of protection found by heuristic protection scheme to be lower than the one found using the exact protection scheme (Since M_{t-1} used by heuristic and exact solutions can be different).

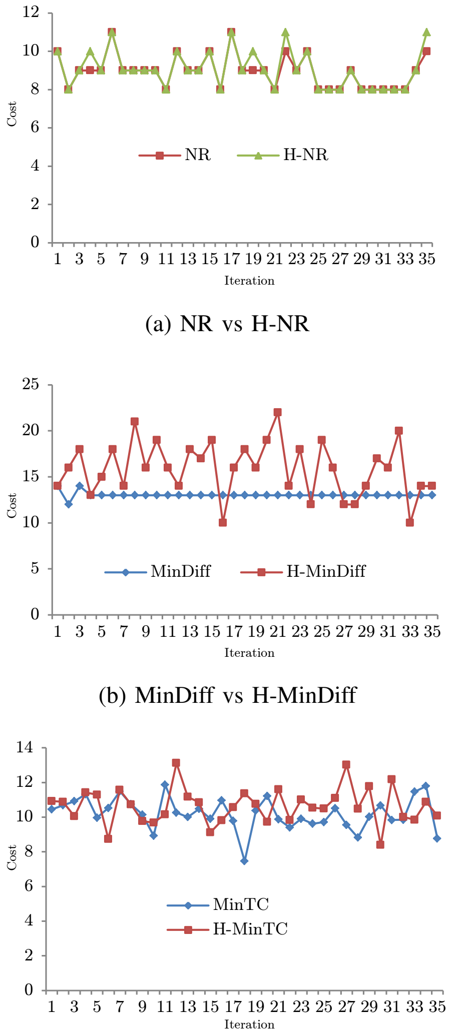
Similarly, we evaluated the protection cost change with increasing $| D |$ (number of critical buses). Comparison of protection costs between exact and heuristic solutions for IEEE 14 dataset is shown in Figure 4. We observed that the protection cost of heuristic protection scheme to closely follow the protection cost of exact solutions.

We evaluated the performance of heuristic protection schemes in terms of computation time on large transmission networks. Figure 5 shows the evaluation results. As mentioned before due to the intractable computation time complexity, exact protection schemes do not scale for real scale transmission networks. As shown in Figure 5 heuristic protection schemes could find a protection strategy in a few seconds on real-scale transmission networks. While we could observe a rapid increase in computation time with increasing size of the transmission network, worst case performance of heuristic protection scheme was $\sim$ 20 minutes on EU 1494 dataset. As mentioned before EU 1494 is one of the largest transmission networks where average power transmission networks are much smaller in size (e.g. Los Angels County power transmission network only consist of 237 transmission lines [24]).

Figure 6, shows the distribution of resource allocation cost (A) and relocation cost (R) of the protection schemes calculated by heuristics. The main observation is that in H-MinDiff both A and R equally contributes to the protection cost wherein H-MinTC the contribution of R is less. We believe that the cost distribution of H-MinTC resulted from our transportation cost distribution as explained in Section VI-A.

We conducted several experiments correlating different features of critical bus set (average/max/min degree and average/max/min distance between buses) with protection cost. We observed a strong correlation between protection cost and the average distance between the critical bus set (distance between two buses is defined as the number of edges in the shortest path between them).

Figures 7, 8 and 9 shows the correlation of protection cost with the average distance between buses in IEEE 14 dataset. We observed a strong correlation between protection cost and the average distance between buses for NR, H-NR, MinTC, H-MinTC protection schemes. As shown in Figure 10 similar correlations were observed on IEEE 300 dataset. We plan to understand these correlations further to improve our heuristics.



(a) NR vs H-NR

(b) MinDiff vs H-MinDiff

(c) MinTC vs H-MinTC

Fig. 3: Comparison of protection cost evolution over time using IEEE 14 dataset

VII. Conclusion

In this paper, we formalize a set of optimal adaptive protection schemes to protect critical buses in power grid against data injection attacks. Protection schemes were optimized against two dimensions: 1) *cost of allocating the resources to secure measurements*. 2) *cost of resource relocation*.

Due to the intractable computational time complexity of above-mentioned optimal protection schemes, we proposed a set of heuristic algorithms with reduced computational time complexity.

We evaluated these protection schemes using simulations on transmission network datasets. Evaluations results showed that our heuristic algorithms provide good approximate results

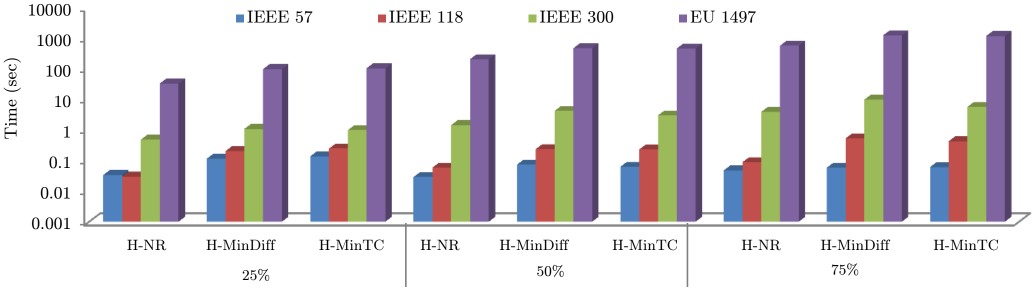
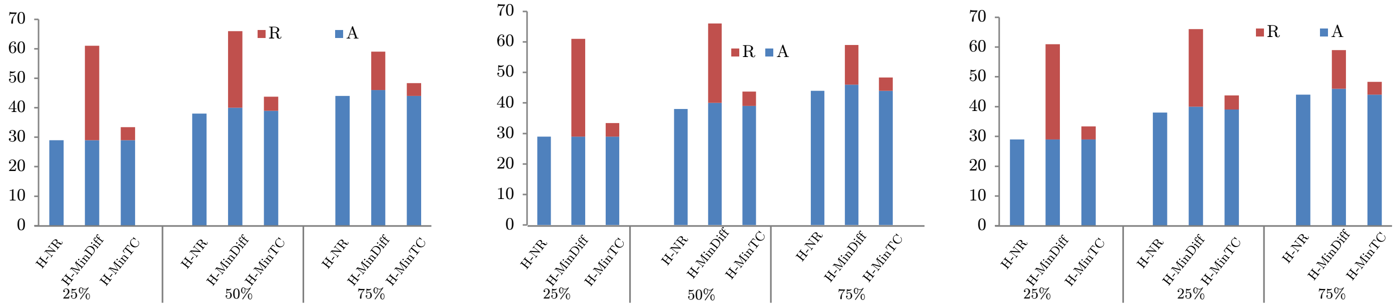


Fig. 5: Comparison of performance of heuristic algorithms on large-scale transmission network datasets. $|D| = 25\%|V|$, $|D| = 50\%|V|$, $|D| = 75\%|V|$.



(a) IEEE-118

(b) IEEE-300

(c) IEEE-1494

Fig. 6: Distribution of resource allocation cost (A) and relocation cost (R) of the protection schemes calculated by heuristics. $|D| = 25\%|V|$, $|D| = 50\%|V|$, $|D| = 75\%|V|$.

with low latency while being able to scale for large power transmission networks.

VIII. Acknowledgments

This work has been funded by US NSF under grant ACI-1339756 and Northrop Grumman Corporation under grant 003570-00001.

References

[1] A. Caragliu, C. Del Bo, and P. Nijkamp, “Smart cities in europe,” *Journal of urban technology*, vol. 18, no. 2, pp. 65–82, 2011.

[2] S. M. Amin and B. F. Wollenberg, “Toward a smart grid: power delivery for the 21st century,” *IEEE power and energy magazine*, vol. 3, no. 5, pp. 34–41, 2005.

[3] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation*. CRC press, 2004.

[4] L. Jia, R. J. Thomas, and L. Tong, “Impacts of malicious data on real-time price of electricity market operations,” in *2012 45th Hawaii International Conference on System Sciences*. IEEE, 2012, pp. 1907–1914.

[5] D.-H. Choi and L. Xie, “Malicious ramp-induced temporal data attack in power market with look-ahead dispatch,” in *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*. IEEE, 2012, pp. 330–335.

[6] Y. Yuan, Z. Li, and K. Ren, “Modeling load redistribution attacks in power systems,” *Smart Grid, IEEE Transactions on*, vol. 2, no. 2, pp. 382–390, 2011.

[7] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[8] S. Bi and Y. J. Zhang, “Graphical methods for defense against false-data injection attacks on power system state estimation,” *Smart Grid, IEEE Transactions on*, vol. 5, no. 3, pp. 1216–1227, 2014.

[9] D. Deka, R. Baldick, and S. Vishwanath, “Data attack on strategic buses in the power grid: Design and protection,” in *PES General Meeting—Conference & Exposition, 2014 IEEE*. IEEE, 2014, pp. 1–5.

[10] 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 *the First Workshop on Secure Control Systems10*, 2010, pp. 1–9.

[11] M. Misyrlis, C. Chelmis, R. Kannan, and V. K. Prasanna, “Sparse causal temporal modeling to inform power system defense,” *Procedia Computer Science*, vol. 62, 2016.

[12] J. J. Grainger and W. D. Stevenson, *Power system analysis*. McGraw-Hill, 1994.

[13] V. V. Vazirani, *Approximation algorithms*. Springer Science & Business Media, 2013.

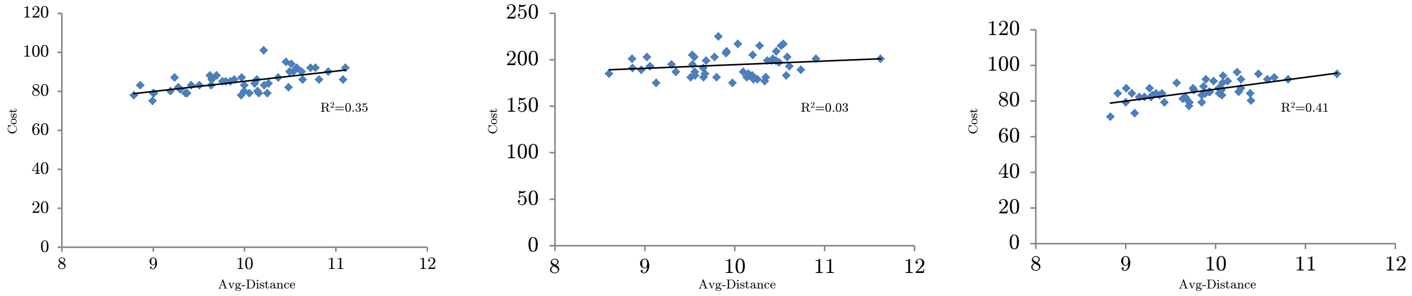
[14] M. R. Garey and D. S. Johnson, *Computers and intractability*. wh freeman New York, 2002, vol. 29.

[15] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, “Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures,” in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010, pp. 220–225.

[16] ——, “Malicious data attacks on the smart grid,” *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645–658, 2011.

[17] M. A. Rahman and H. Mohsenian-Rad, “False data injection attacks with incomplete information against smart power grids,” in *Global Communications Conference (GLOBECOM), 2012 IEEE*. IEEE, 2012, pp. 3153–3158.

[18] F. K. Hwang, D. S. Richards, and P. Winter, *The Steiner tree problem*. Elsevier, 1992, vol. 53.

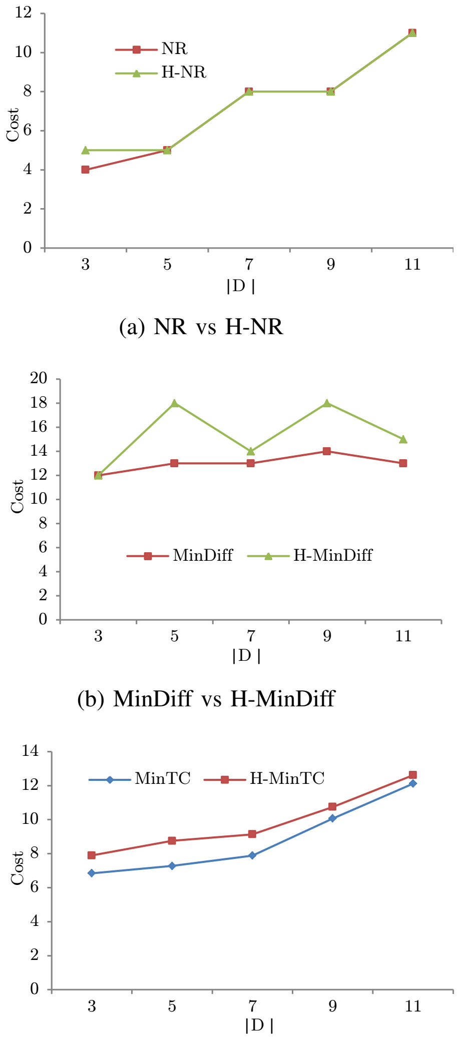


(a) H-NR

(b) H-MinDiff

(c) H-MinTC

Fig. 10: Correlation between protection cost and average distance between buses on IEEE 300 dataset

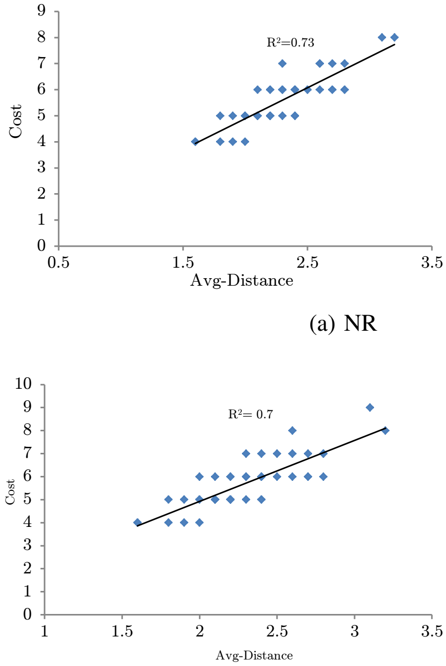


(a) NR vs H-NR

(b) MinDiff vs H-MinDiff

(c) MinTC vs H-MinTC

Fig. 4: Comparison of protection cost with increasing $| D |$ on IEEE 14 dataset.



(a) NR

(b) H-NR

Fig. 7: Correlation between protection cost and average distance between buses on IEEE 14 dataset

[19] P. Winter and J. M. Smith, "Path-distance heuristics for the steiner problem in undirected networks," *Algorithmica*, vol. 7, no. 1-6, pp. 309–327, 1992.

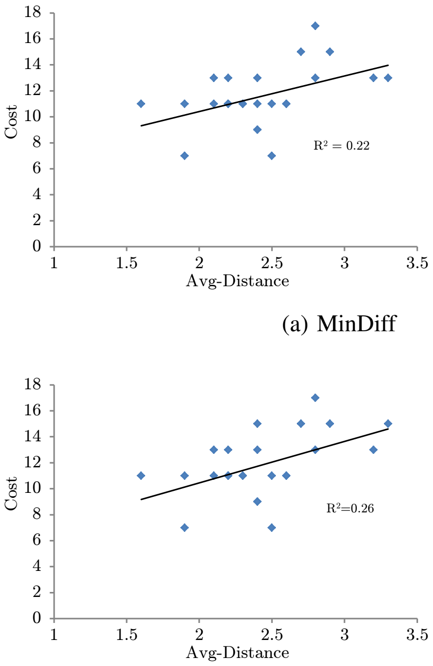
[20] "Gurobi optmizer," http://www.gurobi.com/, accessed: 2016-07-1.

[21] "Graphstream: A dynamic graph library," http://graphstream-project.org/, accessed: 2016-07-1.

[22] "Transmission network datasets," http://wiki.openmod-initiative.org/wiki/Transmission_network_datasets, accessed: 2016-07-1.

[23] "Liines smart power grid test case repository," http://amfarid.scripts.mit.edu/Datasets/SPG-Data/index.php, accessed: 2016-07-1.

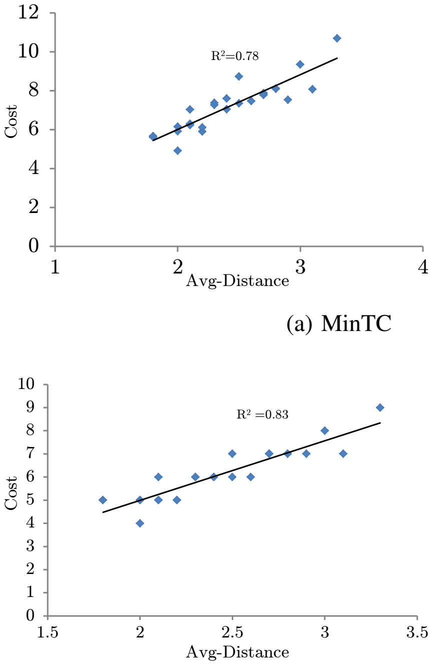
[24] "Los angeles county gis data portal," http://egis3.lacounty.gov/dataportal/, accessed: 2016-07-1.



(a) MinDiff

(b) H-MinDiff

Fig. 8: Correlation between protection cost and average distance between buses on IEEE 14 dataset



(a) MinTC

(b) H-MinTC

Fig. 9: Correlation between protection cost and average distance between buses on IEEE 14 dataset