Network Topology-aware Mitigation of Undetectable PMU Time Synchronization Attacks

Ezzeldin Shereen and György Dán,
School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology

***Abstract*—Time Synchronization attacks constitute a major threat to PMU-based smart grid applications, their cost-efficient detection and mitigation is thus of utmost importance. In this paper we propose a mitigation approach based on authenticated network-based time synchronization. Our approach relies on the observation that a time synchronization attack can be undetectable if and only if it targets at least three time references in the power system, and such attacks need to be mitigated through appropriate security controls. We first provide a formal proof of this result, including a characterization of the degrees of freedom of the attacker in constructing an attack. We then formulate the problem of mitigating undetectable attacks at minimum cost as an integer linear program, and prove that it is NP-hard. To solve the problem, we propose two approximation algorithms based on (1) computing shortest paths, and (2) solving a linear relaxation of the problem. Extensive simulations suggest the superiority of the proposed algorithms on IEEE benchmark power system graphs compared to baseline solutions. We report mitigation cost savings of at least 76% compared to a naive approach for mitigation and at least 30% compared the state-of-the-art.**

I. Introduction

Wide Area Monitoring Protection And Control (WAMPAC) systems rely primarily on Phasor Measurement Units (PMUs). The high-frequency, timestamped measurements of voltage and current phasors generated by PMUs enable a variety of applications, such as phase angle monitoring [1], oscillation monitoring [2], and fault localization [3]. Synchrophasor measurements require, however, precise time synchronization between PMUs, and thus secure and reliable time synchronization is of utmost importance to modern power system operators.

PMUs have traditionally relied on space-based time synchronization, provided by multiple satellites (e.g., GPS) equipped with atomic clocks. Recent years have seen the emergence of Network-Based Time Synchronization (NBTS) as an alternative to space based solutions [4], enabling operators to reduce the dependence on external systems. In the case of NBTS, each PMU clock acts as a *slave* clock and receives time information through a packet switched network from a *master* clock that is connected to an accurate time reference. The most prominent protocol for NBTS is the Precision Time Protocol (PTP) [5].

Unfortunately both space-based and network-based time synchronization are vulnerable to cyber-attacks, referred to as Time Synchronization Attacks (TSAs) [6] [7]. Unauthenticated civilian GPS signals are vulnerable to spoofing attacks, and despite optional security features in PTPv2.1 [8], PTP messages are not authenticated by default and are thus also vulnerable to spoofing attacks. A TSA would induce a phase angle shift in synchrophasor measurements and can have a serious impact on WAMPAC applications [6]. Intuitively, one would expect that Linear State Estimation (LSE) combined with commonly used Bad Data Detection (BDD) algorithms could serve for the detection of TSAs [9]. Nonetheless, as shown recently, a careful attacker can compute TSAs that bypass state-of-the-art BDDs [10]. The detection and mitigation of TSAs thus require additional security controls.

In this paper we formulate the problem of cost-efficient mitigation of TSAs by combining PTPv2.1 message authentication [8] and BDD. Our problem formulation is based on the observation that undetectable TSAs [10] are feasible against only a subset of PMUs, and thus it is possible to minimize the system level cost of deploying PTP authentication (e.g., in terms of network equipment to upgrade and associated key management) and the number of devices containing keying material by protecting an appropriately chosen subset of PMUs. Even though PTPv2.1 message authentication cannot eliminate all types of TSAs, e.g., delay attacks through inserting a delay-box, it does mitigate cyber attacks that involve message spoofing or injection. Therefore, in the rest of the paper, TSA mitigation refers to the mitigation of these classes of TSAs.

The main contributions of the paper are threefold. First, we prove a necessary and sufficient condition for the existence of undetectable TSAs and for the attackers degrees of freedom in performing an attack. Second, we use these findings to formulate the problem of mitigating undetectable TSAs at minimum cost as an Integer Linear Program (ILP). Third, we propose approximation algorithms to solve the problem and show through extensive simulations on IEEE benchmark systems that the proposed cyber-physical mitigation allows to make TSAs detectable at up to 95% cost reduction.

The rest of the paper is organized as follows. Section II accounts for previous research on the detection and mitigation of TSAs. In Section III we present a model for PTP time synchronization in power systems and introduce the theory of undetectable TSAs. Necessary and sufficient conditions for the existence of undetectable TSAs are shown in Section IV. Section V formulates the problem of mitigating undetectable TSAs at minimum cost and presents the proposed approximation algorithms. Section VI evaluates the performance of the proposed algorithms through extensive simulations. Finally, Section VII concludes the paper.

II. Related Work

Undetectable TSAs are akin to false data injection attacks (FDIA) [11; 12], but typical FDIA mitigation approaches that protect the integrity of the measured data are not efficient against TSAs [12; 13; 14]. Solutions have also been proposed for detecting FDIAs based on historical data and meta-data, e.g., authors in [15] analyzed correlations in consecutive estimated system states using wavelet transform and deep neural networks. Moreover, [16] proposed using a Kalman filter for the detection of FDIAs. More recently, graph signal processing has been utilized to detect FDIAs and identify the attacked PMUs [17; 18]. A recent survey for FDIA detection methods is presented in [19].

A number of recent works proposed anomaly detectors specifically designed for detecting TSAs, mostly relying on

TABLE I: Table of Notation

N	Number of buses in the power system
$\mathcal{T}$,T	Set of PMUs, $\lvert\mathcal{T}\rvert=T$
M	Number of synchrophasor measurements taken by PMUs
x	System state (bus voltage phasors), $x\in\mathbb{C}^N$
z	Measurement vector, $z\in\mathbb{C}^M$
H	Measurement matrix, $H\in\mathbb{C}^{M\times N}$
F	Verification matrix, $F\in\mathbb{C}^{M\times M}$
$\hat{r}$	Measurement residual vector, $\hat{r}\in\mathbb{C}^M$
$\mathcal{G}=(\mathcal{V},\mathcal{E})$	Communication infrastructure graph
v_r	Root vertex of $\mathcal{G}$
$\mathcal{T}^a$	Set of attacked PMUs
P	Number of attacked time references (PMUs)
Ψ	Attack measurement matrix, $\Psi\in\{0,1\}^{M\times P}$
W	Attack angle matrix, $W\in\mathbb{C}^{P\times P}$
u_p,α_p	Phase angle shift induced by the attack on time reference p, $u_p=e^{j\alpha_p}\in\mathbb{C}$
z^a	Attacked measurement vector, $z^a\in\mathbb{C}^M$
$\mathcal{C}$,C	Collection of equivalence classes, $\lvert\mathcal{C}\rvert=C$
$\mathcal{C}_i$,C_i	Set of time references in equivalence class i, $\lvert\mathcal{C}_i\rvert=C_i$
$\mathcal{C}_i^+$	Augmented equivalence class i
$\mathcal{C}^{+4}$,K	Set of vulnerable quadruplets of time references, $\lvert\mathcal{C}^{+4}\rvert=K$
$v_{s,k}$, $v_{t,k}$	k^{th} source vertex and k^{th} terminal vertex

information from the time synchronization system (GPS or PTP). For detecting GPS spoofing against PMUs, [20] proposed utilizing the carrier-to-noise-ratio of the GPS signal. For PTP, [21] proposed introducing *guard clocks* in order to detect PTP delay attacks. More recent work proposed combining data from both the power system and the time synchronization system to increase the detection accuracy [22]. Nevertheless, anomaly detectors are prone to false negatives, and thus they may not detect skillful adversaries.

Works focusing on the mitigation of TSAs proposed authentication of GPS messages [23] or PTP messages [24]. One disadvantage of such works is that they do not consider the system level cost of TSA mitigation, (e.g., cost of upgrading network switches in a PTP network, overhead due to key management, and compatibility issues) and are thus cost-inefficient for power systems. Similar to our work, [25] aims to reduce the TSA mitigation cost by deploying PTP authentication only on the subset of the network equipment that is vulnerable to undetectable TSAs. While [25] motivated the approach by a conjecture that only TSAs against 3 time references or more can be undetectable [26], this paper provides a proof of this conjecture in Section IV, and provides a different problem formulation in Section V, which allows to achieve significant cost savings compared to that in [25], by considering a wider range of TSA mitigation strategies.

III. System Model

A. Power System and Network Model

Table I summarizes the most important notations used in the paper. We consider a power system with N buses and $M \geq N$ measurements taken by PMUs to ensure system observability. We denote the vector of PMU measurements by $z \in \mathbb{C}^M$, $z_m = |z_m|e^{j\theta_m}$, where $j=\sqrt{-1}$ and θ_m is the phase angle. We further denote the system state (voltage phasors at the buses) by $x\in\mathbb{C}^N$. The linear measurement model is then

$$z=Hx+e, \tag{1}$$

where $H\in\mathbb{C}^{M\times N}$ denotes the measurement matrix, and $e\in\mathbb{C}^M$ is white Gaussian measurement noise. The linear model (1) is justified by that PMUs measure current and voltage phasors, and it allows for efficient computation of the Least-Squares (LS) state estimate $\hat{x} = (H^\dagger H)^{-1}H^\dagger z$, where $H^\dagger$ denotes the conjugate transpose of H. Alternative approaches using non-linear least squares based on power flow measurements or using dynamic state estimation (DSE) are more computationally intensive as they involve iterative algorithms [27]. The verification matrix is defined as $F = H(H^\dagger H)^{-1}H^\dagger - I$ [10], and allows us to express the measurement residual $\hat{r}=Fz\in\mathbb{C}^M$. The residual $\hat{r}$ is typically used for BDD, e.g., using the LNR test [9] for identifying measurements with suspiciously high residuals. Bad measurement data identified by the BDD are typically discarded, as long as system observability is maintained.

The measurements are taken by a set $\mathcal{T}=\{\tau_1,...,\tau_T\}$ of PMUs, $T\leq M$, which depend on precise time synchronization. We denote by $M_i \geq 1$ the number of measurements taken by PMU τ_i. We consider securing the time references of a subset of these PMUs using PTP, and thus we model the communication infrastructure used for time synchronization in the WAMPAC by an undirected graph $\mathcal{G}=(\mathcal{V},\mathcal{E})$, where $\mathcal{V}=\mathcal{T}\cup\mathcal{N}$ is the set of vertices, $\mathcal{N}$ is the set of network switches and routers, and $\mathcal{E}$ is the set of edges (communication links) in the graph. We consider that the edges $\mathcal{E}$ of $\mathcal{G}$ form a tree that spans the PMUs $\mathcal{T}$. This assumption is motivated by that the active communication topology in power systems typically is a tree, and PTP networks use a tree topology as well for disseminating time references in a network [5]. Furthermore, we denote by $v_r\in\mathcal{V}$ the root vertex of the tree, which corresponds to where the PTP master clock is deployed.

B. Attack Model

We consider an attacker that is able to spoof PTP messages [7] or the GPS signals [6]. This way, the attacker can manipulate the time references of a subset $\mathcal{T}^a=\{\tau_1^a,...,\tau_P^a\}\subseteq\mathcal{T}$ of PMUs, where P is the number of manipulated time references (and PMUs). To capture the dependence of measurements on the attacked time references we define the attack-measurement matrix $\Psi\in\{0,1\}^{M\times P}$ as

$$\Psi_{m,p}=\begin{cases}1, & \text{if } m \text{ is measured by } \tau_p^a\\ 0, & \text{otherwise,}\end{cases}$$

for all $m\in\{1,...,M\}$ and $p\in\{1,...,P\}$ [10]. Due to the attack, the phasors measured by PMU τ_p^a will be rotated by α_p. Thus, using the notation $u_p=e^{j\alpha_p}$, the m^{th} measurement taken by PMU τ_p^a,$p\in\{1,...,P\}$ can be written as $z_{p,m}^a = |z_{p,m}|e^{j(\theta_{p,m}+\alpha_p)} = z_{p,m}u_p$, where $|z_{p,m}|$ is the measured magnitude, $\theta_{p,m}$ is the unattacked phase angle, and α_p is the phase angle shift introduced by the attack.

C. Undetectable TSAs

Let z^a be the attacked measurement vector. If linear state estimation based on (1) is employed in the WAMPAC then a TSA

should ideally yield high residuals and consequently it should be detected by BDD. It is thus natural to introduce the notion of undetectability as follows.

Definition 1. *A TSA $u = (u_1, \dots, u_P)$ against PMUs $\mathcal{T}^a$ is undetectable if and only if it does not change the measurement residual, i.e., $Fz = Fz^a$.*

A necessary and sufficient condition for a TSA to be undetectable according to Defintion 1 was formulated in [10], as follows.

Lemma 1. *Consider a TSA against PMUs $\mathcal{T}^a$. The TSA is undetectable if and only if the vector $u \in \mathbb{C}^P$, s.t., $u_p = e^{j\alpha_p}, p \in \{1,...,P\}$ satisfies*

$$W(u-1) = 0, \tag{2}$$

where $W = \Psi^T diag(z)^\dagger F^\dagger F diag(z) \Psi$ is the complex attack angle matrix, $W \in \mathbb{C}^{P\times P}$, and is Hermitian.

Observe that an undetectable TSA corresponds to any solution to (2) other than ($u_i = 1, \forall i \in \{1,...,P\}$), which corresponds to not attacking any time reference. Interestingly, when $rank(W) = 1$, (2) can be simplified to

$$\sum_{i=1}^{P} W_{1i}(u_i - 1) = 0,$$

where W_{1i} is the i^{th} element of the row with highest ℓ_2 norm of the W matrix, and $|u_i| = 1, \forall i \in \{1,...,P\}$. The row with highest ℓ_2 norm in W is chosen in order to avoid choosing rows that are equal to the zero vector, and in order to provide better computational stability of the computed solutions. Moving the term related to u_P from the LHS to the RHS of the above equation, the undetectability condition can be written as

$$\sum_{i=1}^{P-1} W_{1i}(u_i - 1) = -W_{1P}(u_P - 1), \tag{3}$$

A geometric interpretation of the above in the complex plane, defined by the real and imaginary parts of the equation, is that the solution to (3) are the intersection points between an annular region (LHS of (3)), and a circle (RHS) [26]. In what follows we denote by $AR_{1,P-1} = (c_{1,P-1}, r^o_{1,P-1}, r^i_{1,P-1})$ the annular region with center $c_{1,P-1} = -\sum_{i=1}^{P-1} W_{1i}$, outer radius $r^o_{1,P-1} = \sum_{i=1}^{P-1} |W_{1i}|$, and inner radius $r^i_{1,P-1} = max\{0, 2|W_{1i^*}| - \sum_{i=1}^{P-1} |W_{1i}|\}$, where $i^* = argmax_{i\in\{1,\cdots,P-1\}} |W_{1i}|$. Furthermore, we denote by $O_P = (c_P, r_P)$ the circle with center $c_P = W_{1P}$ and radius $r_P = |W_{1P}|$. Figure 1 shows an illustration of the geometrical problem and the solution to be computed (shown in red) for two different cases of O_P. Based on the previous discussion, let us recall the following result from [26].

Lemma 2. *Consider the case when $rank(W) = 1$.*

- *If $P = 1$ then there is no undetectable TSA.*
- *If $P = 2$ then there is 1 undetectable TSA.*
- *The pairs of time references that are vulnerable to undetectable TSAs for $P = 2$ form equivalence classes $\mathcal{C} = \{\mathcal{C}_1, \dots, \mathcal{C}_C\}$, where $C = |\mathcal{C}|$ is the number of equivalence classes.*
- *For $P \geq 3$, undetectable TSAs against $\mathcal{T}^a$ exist if $\exists \mathcal{C}_i \in \mathcal{C}$ s.t. $\mathcal{T}^a \subseteq \mathcal{C}_i$. In addition, the set of undetectable TSAs (i.e., $\alpha_p, p \in \{1, \dots, P\}$ that solves (3)) is either a non-empty connected compact subset of $\mathbb{R}$ or the union of two non-empty connected compact subsets of $\mathbb{R}$.*

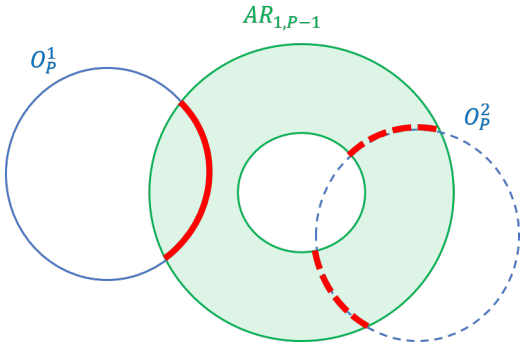


Fig. 1: Computing attacks when $rank(W) = 1$ and $p \geq 3$.

The equivalence classes are calculated by computing a metric called the minimum index of separation (IoS*), as proposed in [26], for all $\binom{T}{2}$ pairs of PMUs. When IoS*$= 1$ for a pair of PMUs, this means that the rank of the W matrix corresponding to attacking this pair is always equal to 1, independent on the measurement values z. Vulnerable PMU pairs that have pairwise IoS*$= 1$ were shown to form equivalence classes [26], i.e., $IoS^*(a,b) = 1$ and $IoS^*(b,c) = 1$ implies $IoS^*(a,c) = 1$. Consequently, solving (3) for a set of PMUs $\mathcal{T}^a$ that is a subset of an equivalence class can result in undetectable TSAs according to Definition 1, while solving the same equation for a set of PMUs that is not a subset of an equivalence class does not result in undetectable TSAs.

TSAs against $P = 2$ time references were shown to be computable using a closed form expression in [10]. For $P \geq 3$, [26] proposed a recursive algorithm that selects $u_i, i \in \{3,...,P\}$ (i.e., $P-2$ variables) from unions of connected sets of feasible values based on the geometric interpretation of (3), and thus conjectured that the solution to (3) has $P-2$ degrees of freedom. The next section provides a formal definition of degrees of freedom and a proof of the conjecture, which is the first contribution of this paper.

IV. Feasibility Analaysis of TSAs

In this section we investigate the feasibility of computing undetectable TSAs by solving (3). We first provide necessary and sufficient conditions under which an attack does not exist for $P \geq 2$ and $rank(W) = 1$. Next, we provide conditions for the set of attacks not to be a singleton and we characterize the degrees of freedom of the attack solution space.

A. Infeasibility of Attacks

We first formulate a lemma that we will use later for deriving conditions for the infeasibility of attacks.

Lemma 3. *Let $\overline{w}(q,s) = |(\sum_{i=1}^{q} W_{1i}) + s|$. Consider the equation*

$$\sum_{i=1}^{q-1} W_{1i}(u_i - 1) = -W_{1q}(u_q - 1) + s, \tag{4}$$

where $W_{1i}, i \in \{1,\cdots,q\}$, $u_i, i \in \{1,\cdots,q\}$, and s are complex numbers, and $|u_i| = 1$. Then there exists exactly one solution $[u_1,\cdots,u_q]$ to (4) if and only if one or both of the two conditions

$$\overline{w}(q,s) = \sum_{i=1}^{q} |W_{1i}|, \tag{5}$$

$$\overline{w}(q,s) = 2|W_{1i^*}| - \sum_{i=1}^{q} |W_{1i}|, \tag{6}$$

is satisfied, where $i^* = argmax_{i\in\{1,\cdots,q\}} |W_{1i}|$.

Proof. The proof is given in the appendix. □

We can now formulate the following result regarding the infeasibility of attacks.

Proposition 1. *Consider an attack on $P \geq 2$ PMUs such that $rank(W) = 1$. Then an undetectable TSA does not exist if and only if at least one of the following conditions is satisfied.*

$$\overline{w}(P,0) = \sum_{i=1}^{P} |W_{1i}|, \tag{7}$$

$$\overline{w}(P,0) = 2|W_{1i^*}| - \sum_{i=1}^{P} |W_{1i}|, \tag{8}$$

where $i^* = argmax_{i\in\{1,\cdots,P\}} |W_{1i}|$.

Proof. Recall that every attack corresponds to a solution to (3). We know that (3) has at least one solution ($u_i = 1, \forall i \in \{1,\cdots,P\}$), i.e., no attack. If this solution is the only feasible solution to (3), then there does not exist a feasible attack. By comparing equations (3) and (4) we observe that they are identical when $q = P$ and $s = 0$. Therefore, we can use Lemma 3 with $q = P$ and $s = 0$ to obtain the necessary and sufficient conditions (7) and (8). □

Note that (7) holds if and only if W_{1i} are co-directed. Since W is Hermitian, i.e., W_{ii} is real, therefore W_{1i} must be real, and thus W is a real symmetric matrix. Similarly, (8) holds if and only if all $W_{1i}, i \neq i^*$ point in the opposite direction of W_{1i^*}, which implies also that all W_{1i} are real, and hence W is real. This is extremely improbable in practice due to the noisy nature of the complex-valued measurements affecting W.

B. Conditions for finding a non-empty attack solution set

Based on the previous discussion, we can now formulate the following result for the existence of undetectable TSAs.

Proposition 2. *Consider that $rank(W) = 1$ and $P \geq 2$. Then an undetectable TSA exists if and only if*

$$2|W_{1i^*}| - \sum_{i=1}^{P} |W_{1i}| < \overline{w}(P,0) < \sum_{i=1}^{P} |W_{1i}|, \tag{9}$$

where $i^* = argmax_{i\in\{1,\cdots,P\}} |W_{1i}|$.

Proof. Observe that it is impossible to have $\overline{w}(P,0) > \sum_{i=1}^{P} |W_{1i}|$ due to the triangle inequality. Furthermore, observe that it is impossible to have $2|W_{1i^*}| - \sum_{i=1}^{P} |W_{1i}| > \overline{w}(P,0)$ because when $\overline{w}(P,0)$ is minimal, that is when all $W_{1i}, i \neq i^*$ point in the opposite direction of W_{1i^*} then we have $2|W_{1i^*}| - \sum_{i=1}^{P} |W_{1i}| = \overline{w}(P,0)$. Therefore we have

$$2|W_{1i^*}| - \sum_{i=1}^{P} |W_{1i}| \leq \overline{w}(P,0) \leq \sum_{i=1}^{P} |W_{1i}|. \tag{10}$$

We know from Proposition 1 that equality on at least one side of (10) is a necessary and sufficient condition for the non-existence of attacks. Therefore, having strict inequality on both sides, i.e., (9), is a necessary and sufficient condition for the existence of undetectable TSAs, which proves the proposition.

□

C. Degrees of freedom of the set of undetectable TSAs

In order to characterize the set of undetectable TSAs, we rely on the notion of the *degrees of freedom* of the solution of a system of equations. In our work, the system of equations consists of equation (3) as well as the constraint $|u_p| = 1$, $p \in \{1,...,P\}$, in the variables $(u_1,...,u_P)$. Let us denote by $\mathcal{U} \subseteq \Pi_{p=1}^{P} \mathbb{S}^1$ the set of feasible solutions, where $\mathbb{S}^1$ is the circle group.

Definition 2. *We say that $\mathcal{U}$ has n degrees of freedom around $u \in \mathcal{U}$ if there is a nonempty open set $\Theta \subset \mathbb{R}^n$ and an injective mapping $\psi : \Theta \to \mathcal{U}$ such $u = \psi(\alpha)$ for some $\alpha \in \Theta$.*

As an example, $\mathbb{S}^1$ has one degree of freedom around any point $u \in \mathbb{S}^1$. Without loss off generality, we can consider that the attacker starts to compute a solution $u \in \mathcal{U}$ by choosing $u_P \in \mathcal{U}_P$, where $\mathcal{U}_P \subseteq \mathbb{S}^1$ is the set of all feasible values of u_P (c.f., the bold arcs in Fig. 1). For the chosen u_P, the attacker then chooses $u_{P-1} \in \mathcal{U}_{P-1}(u_P)$, etc. In general, when choosing $u_i, i \in \{1,...,P\}$, let us denote by $u_i^+ = (u_{i+1},\dots,u_P)$ the values already chosen, by $u_i^- = (u_1,...,u_{i-1})$ the values that remain to be chosen, and by $\mathcal{U}_i(u_i^+) \subseteq \mathbb{S}^1$ the set of all feasible values of u_i given earlier choices u_i^+ such that there is $u_i^- \in \Pi_{p=1}^{i-1} \mathbb{S}^1$ for which $(u_i^-, u_i, u_i^+) \in \mathcal{U}$. Next we define the notion of *free variables* and *leading variables*, tightly related to the degrees of freedom of the solution set.

Definition 3. *A variable $u_i \in \mathcal{U}_i(u_i^+)$ is called a free variable if:*

- *There is a nonempty open interval $\Theta_i \subset \mathbb{R}$ and an injective mapping $\psi_i : \Theta_i \to \mathcal{U}_i(u_i^+)$ s.t. $\forall u_i \in \mathcal{U}_i(u_i^+) : u_i = \psi_i(\alpha_i)$ for some $\alpha_i \in \Theta_i$.*
- *$\forall u_i \in \mathcal{U}_i(u_i^+)\, \exists u_i^- \in \Pi_{p=1}^{i-1} \mathbb{S}^1$ such that $(u_i^-, u_i, u_i^+) \in \mathcal{U}$.*

Definition 4. *A variable $u_i \in \mathcal{U}(u_i^+)$ is called a leading variable if it is not a free variable.*

Intuitively, a variable $u_i \in \mathcal{U}_i(u_i^+)$ is a free variable w.r.t. the solution of (3) if its value could be arbitrarily chosen from a set of feasible values. The degrees of freedom of the solution of (3) is the number of arbitrarily chosen variables whose values can be fixed (i.e., free variables) so that the values of the remaining variables (i.e., leading variables) can be uniquely determined to satisfy (3). In other words, the solution set $\mathcal{U}$ has n degrees of freedom around every interior point $u \in \mathcal{U}$ if there are n free variables in $(u_1,\cdots,u_P)$. That is, given an arbitrary ordering of variable choice, the first n chosen variables (i.e., $(u_{P-n+1},...,u_P)$) will be free variables, and the remaining variables (i.e., $(u_1,...,u_{P-n})$) will be leading variables. In what follows we characterize the degrees of freedom of the attack solution set for $rank(W) = 1$.

Theorem 1. *Consider that $rank(W)=1$ and a TSA is feasible. Then the solution set $\mathcal{U}$ has $P-2$ degrees of freedom around every interior point $u\in\mathcal{U}$.*

In order to prove this result, we first introduce two lemmas.

Lemma 4. *If an undetectable TSA is feasible for $P\geq 3$ then u_P is a free variable.*

Proof. Let us denote by $\mathcal{U}_P$ the set of feasible values for u_P, excluding the boundary values corresponding to intersection points in Figure 1. Furthermore, let us define the set of feasible attack angles $\Theta_P=\{\alpha_P : u_P=e^{j\alpha_P}, u_P\in\mathcal{U}_P\}$. Note that the mapping $\psi_P:\Theta_P\rightarrow\mathcal{U}_P$ is injective, as required by Definition 3. By Proposition 1 we know that it is with negligible probability that $AR_{1,P-1}$ and O_P intersect in only one point. Furthermore, Θ_P is either a non-empty connected bounded open interval (e.g., if $O_P=O_P^1$ in Figure 1), or the union of two such intervals (e.g., if $O_P=O_P^2$ in Figure 1), both cases satisfying the requirement on Θ_i in Definition 3. Therefore, u_P is a free variable according to Definition 3. □

This establishes that for $P\geq 3$ the attack solution has at least one degree of freedom corresponding to u_P being a free variable. Next, let us consider that $u_q^+=(u'_{q+1},\cdots,u'_P)$, $q\geq 3$ are already chosen. The next lemma establishes the conditions for $u_q\in\mathcal{U}_q(u_q^+)$ to be a free variable.

Lemma 5. *Let $u_q^+=(u'_{q+1},\cdots,u'_P)$. Then u_q is a free variable if and only if*

$$r_{1,q}^i<\left|\left(\sum_{i=1}^{q}W_{1i}\right)+\sum_{j=q+1}^{P}s_j\right|<r_{1,q}^o, \tag{11}$$

where $s_j=-W_{1j}(u'_j-1)$.

Proof. The proof is given in the appendix. □

We can now proceed to prove Theorem 1.

Proof of Theorem 1. By Lemma 4, the first chosen variable (i.e., u_P) is always a free variable. Next, Lemma 5 establishes that $u_{P-1}\in\mathcal{U}(u_P)$ is also a free variable given that u_P is chosen such that the intersection point between $AR_{1,P-1}$ and O_P does not lie on the inner or outer bounding circle of the annular region (i.e., the end points of the bold arcs in Figure 1). Similarly, Lemma 5 states that the intersection point between $AR_{1,q}$ and O_{q+1} (corresponding to u_{q+1}) must not lie on the inner or outer bounding circle of the annular region

Therefore, choosing suitable values for u_q^+ (i.e., values that do not lie in the inner or outer circles) ensures that u_q, $q\in\{3,\cdots,P-1\}$ are free variables. Note however that u_2 and u_1 cannot be free variables because $AR_{1,1}$ becomes a circle, and thus it can intersect with O_2 in at most two points. Since u_P is also a free variable by Lemma 4, the number of free variables is $P-2$. □

Observe that the order in which the terms are moved from the left hand side to the right hand side of (3) determines which $P-2$ variables in $\{u_1,...,u_P\}$ will be free variables and which 2 variables will be leading variables.

V. Minimum Cost rank-1 TSA Mitigation Problem

In this section we formulate the problem of mitigating undetectable TSAs at minimum cost, making use of Theorem 1. Recall that our approach mitigates TSAs involving message spoofing or injection against sets of PMUs with rank$(W)=1$. In principle, undetectable TSAs could still be possible even when rank$(W)>1$. However, from our experience, identifying sets of PMUs for which $rank(W)>1$ and computing undetectable TSAs for those usually requires the attacker to manipulate a larger number of PMUs. Hence attacks against PMUs with $rank(W)=1$ are easiest to perform. Moreover, the sets of PMUs for which $rank(W)>1$ in most cases contain subsets of PMUs that have a rank-1 W matrix. Therefore, mitigating rank-1 TSAs would typically mitigate rank-k attacks, for $k>1$.

Together with Lemma 2, Theorem 1 characterizes the minimum number of PMUs that an attacker needs to manipulate in order to launch an undetectable TSA. The theorem implies that for an equivalence class $\mathcal{C}_i$, $C_i=|\mathcal{C}_i|$, any subset of $3\leq P\leq C_i$ time references in $\mathcal{C}_i$ can be attacked in an undetectable manner (i.e., 1 or more degrees of freedom). Furthermore, an attack against any subset of $P=2$ time references (i.e., zero degrees of freedom) can be constructed, but due to the lack of degrees of freedom in the solution, the attack can be detected by BDD in practice, as shown in [26]. Therefore, it is sufficient to only consider the mitigation of TSAs against $P\geq 3$ time references if BDD is used in the system.

A. Securing Time References

We consider a power system operator that wants to upgrade its network infrastructure to mitigate TSAs. We assume that LSE based on (1) is used with BDD, and hence the objective is to mitigate attacks against the collection $\{\mathcal{C}_1,...,\mathcal{C}_C\}$ of equivalence classes of time references vulnerable to undetectable TSAs, as defined in Section III. We consider mitigation through authenticated time synchronization, e.g., using PTPv2.1. Upgrading a device (vertex) to PTPv2.1 means that the device will be able to use authenticated PTP messages. An edge is then secured if both incident vertices are upgraded. Therefore, we call a path in $\mathcal{G}$ to be secured if and only if all edges along the path are secured, and hence all vertices along the path are upgraded. Based of the previous discussion, the time reference of a PMU τ_t can be either *absolutely* or *relatively* secured, defined as follows.

Definition 5. *A time reference $\tau_t\in\mathcal{C}_i$ is absolutely secured if a path in $\mathcal{G}$ from the root vertex $v_r\in\mathcal{V}$ (PTP master) to τ_t is secured, including all intermediate vertices.*

Definition 6. *Two time references $\tau_t,\tau_c\in\mathcal{C}_i$ are relatively secured (denoted by $\tau_t\leftrightarrow\tau_c$) if a path in $\mathcal{G}$ between τ_t and τ_c is secured, including all intermediate vertices.*

In practice, securing a path means that the network equipment on the path have to be upgraded to support authenticated PTP messages, and related key management. Absolutely securing a time reference τ_t mitigates any TSA including τ_t. On the contrary, having $\tau_t\leftrightarrow\tau_c$ makes that a TSA must impose the same phase angle shift on the corresponding PMU measurements. Observe that absolutely securing τ_t can be thought of as relatively securing τ_t and v_r. We can thus define the augmented equivalence classes $\mathcal{C}_i^+=\mathcal{C}_i\cup\{v_r\},\forall i\in\{1,...,C\}$.

In what follows we show the effect of relatively securing time references in an equivalence class $\mathcal{C}_i$ on the rank of the resulting

W matrix, and hence the vulnerability of $\mathcal{C}_i$ to undetectable TSAs. Recall that attacking time references in $\mathcal{C}_i$ would always result in a rank-1 W matrix. However, relatively securing two time references would make them dependent, thus effectively reducing the number of independent time references in $\mathcal{C}_i$ by one. However, in order to make sure the results in Theorem 1 apply to the reduced set of time of references (i.e., that they form a vulnerable equivalence class), we have to ensure that attacking any subset yields a rank-1 W matrix, which is proven by the following Proposition. In the proposition, we consider an attack against P time references affecting $m \geq P$ measurements. Furthermore, we say that the matrix Ψ is targeting the set of measurements $\mathcal{M}_a$ (denoted by $\Psi \rightarrow \mathcal{M}_a$) if and only if $\Psi_{i,j}=0, \forall i \notin \mathcal{M}_a$, and $\forall i \in \mathcal{M}_a\ \exists j \in \{1,...,P\}$ s.t. $\Psi_{i,j}=1$.

Proposition 3. *Let* $W = \Psi^T diag(z)^\dagger F^\dagger F diag(z)\Psi$, *where* $W \in \mathbb{C}^{P\times P}$, $\Psi \in \{0,1\}^{M\times P}$, $\Psi \rightarrow \mathcal{M}_a$, *and* $m = P$, *i.e., one measurement per time reference. Now consider any matrix* $\bar{W} = \bar{\Psi}^T diag(z)^\dagger F^\dagger F diag(z)\bar{\Psi}$ *where* $\bar{W} \in \mathbb{C}^{\bar{P}\times\bar{P}}$, $\bar{\Psi} \in \{0,1\}^{M\times\bar{P}}$, $\bar{\Psi} \rightarrow \mathcal{M}_a$, *and* $\bar{P} \leq P = m$. *If* $rank(W)=1$ *then* $rank(\bar{W})=1$.

Proof. Let $V = Fdiag(z)\Psi$, $V \in \mathbb{C}^{M\times P}$. Furthermore, let $G = Fdiag(z), G \in \mathbb{C}^{M\times M}$. Therefore $V = G\Psi$. If $rank(W)=1$, then $rank(V) = 1$ as well, since $W = V^\dagger V$ and $rank(A) = rank(A^\dagger A)$ for any matrix A. Now observe that V can be also written as $V = G_0\Psi_0$, where G_0 is defined as $G_0 = Fdiag(z)_0$ s.t. $diag(z)_0 \in \mathbb{C}^{M\times m}$ is the sub-matrix of $diag(z)$ including only the column indexes in $\mathcal{M}_a$, and $\Psi_0 \in \{0,1\}^{m\times P}$ is the sub-matrix of Ψ including only the rows with indexes in $\mathcal{M}_a$.

Since Ψ corresponds to attacking one measurement per time reference, then w.l.o.g. we can assume that $\Psi_0 = I_P$, i.e., the $P\times P$ identity matrix. This implies that $rank(V) = rank(G_0) = 1$. Given that $rank(AB) \leq min(rank(A), rank(B))$ for any two matrices A and B, the rank of any $\bar{V} = G_0\bar{\Psi}_0 = G\bar{\Psi}$ s.t. $\bar{\Psi}_0 \in \{0,1\}^{m\times\bar{P}}$, $1 \leq \bar{P} \leq m$, and $\bar{\Psi}_0 \rightarrow \mathcal{M}_a$ will be at most 1. Then it follows that $rank(\bar{W}) \leq 1$, since $\bar{W} = \bar{V}^\dagger\bar{V}$. Note that $rank(\bar{W}) = 0$ if and only if the sum of each row in G_0 is 0, which is extremely unlikely due to the noisy nature of z. Therefore $rank(\bar{W}) = 1$. □

The above result illustrates the effect of relative securing of time references of the same equivalence class. Since relative securing of two PMUs forces a TSA to have the same time shift for both PMUs, the time reference of these PMUs will not be independent. Therefore, this corresponds to having a modified Ψ matrix targeting the same set of measurements. The proposition then shows that if the rank of the original W matrix is equal to 1 then the rank of the W matrix obtained using the modified Ψ matrix will also be equal to 1. Therefore, for an equivalence class $\mathcal{C}_i$ with m measurements, $rank(W) = 1$ holds independent of the number of time references in $\mathcal{C}_i$ that are relatively secured. Moreover, given that the number of degrees of freedom of a rank-1 TSA against $\mathcal{C}_i$ is $P-2$ (Theorem 1), and that a rank-1 TSA with $P=2$ is detectable by BDD, relatively securing two time references in $\mathcal{C}_i$ decrements P by 1, and similarly decrements the number of degrees of freedom by 1. As a consequence, relatively securing time references in $\mathcal{C}_i$, s.t., there are only $P=2$ independent time references will render any attack against $\mathcal{C}_i$ detectable by BDD.

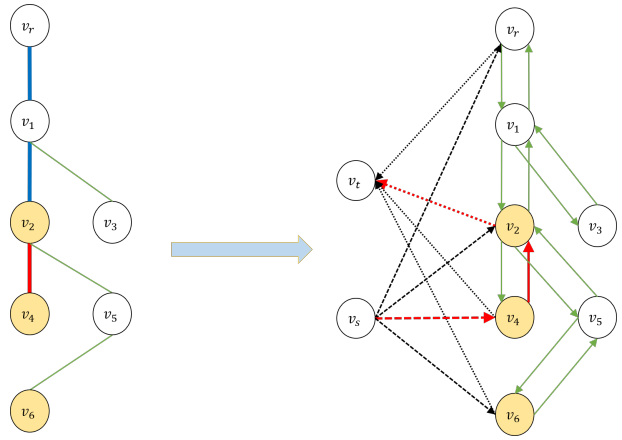


Fig. 2: An illustration of converting the original graph $\mathcal{G}$ (to the left) into the extended directed graph $\mathcal{G}'$ (to the right), for a simple case of $K=1$ vulnerable quadruplets, with $\mathcal{C}_1^{+4} = \{v_r, v_2, v_4, v_6\}$. The optimal solution is highlighted in red, while the optimal solution when considering only absolutely securing is highlighted in blue.

B. TSA Mitigation Problem Formulation

In what follows we formulate the problem of mitigating TSAs at minimum cost. We define the cost as the number of network equipment and PMUs (vertices in $\mathcal{V}$) that need to be upgraded to support authenticated PTP messages. In the formulation we make use of the collection $\mathcal{C}^{+4} = \{\mathcal{C}_k^{+4} : |\mathcal{C}_k^{+4}| = 4, v_r \in \mathcal{C}_k^{+4}, \exists i \in \{1,...,C\}$ s.t. $\mathcal{C}_k^{+4} \subseteq \mathcal{C}_i^{+}\}$ of vulnerable quadruplets of time references, where $k \in \{1,...,K\}$ and $K = |\mathcal{C}^{+4}| = \sum_{i=1}^{C} \binom{C_i}{3}$. The problem of mitigating undetectable TSAs at minimum cost can then be formulated as follows.

Minimum-Cost TSA Mitigation (MIN-TM): Given the communication infrastructure graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ of the WAMPAC and a collection $\mathcal{C}^{+4}$ of vulnerable quadruplets of time references. Find a subgraph $\mathcal{G}^* = (\mathcal{V}^*, \mathcal{E}^*)$ of $\mathcal{G}$ with minimum $|\mathcal{V}^*|$ s.t. $\exists \tau_1, \tau_2 \in \mathcal{C}_k^{+4} : \tau_1 \leftrightarrow \tau_2, \forall \mathcal{C}_k^{+4} \in \mathcal{C}^{+4}$.

In the above problem formulation, observe that mitigation relies on identifying the collection $\mathcal{C}^{+4}$ of vulnerable quadruplets, which is based on the collection $\mathcal{C}$ of equivalence classes. In turn, equivalence classes in $\mathcal{C}$ include only PMUs for which the pairwise IoS* metric is equal to 1, which holds only when the corresponding W matrix is rank-1. Therefore, by definition, MIN-TM attempts only to mitigate those attacks corresponding to rank(W)=1. Observe also that the above problem formulation is based on that in order to mitigate all undetectable TSAs with rank$(W)=1$, each equivalence class can contain at most two independent time references.

In the following we present an Integer Linear Programming (ILP) formulation of the problem, generalizing an ILP formulation proposed for the Group Steiner Tree (GST) problem [28]. The formulation is based on converting $\mathcal{G}$ into a directed graph and then solving a max-flow problem, as demonstrated in Fig. 2. The first step in the conversion is to replace each undirected edge $e \in \mathcal{E}$ with two directed edges, one in each direction. The next step is to add two sets $\mathcal{V}_s = \{v_{s,1},...,v_{s,K}\}$ (source vertices) and $\mathcal{V}_t = \{v_{t,1},...,v_{t,K}\}$ (terminal vertices), each consisting of K additional vertices, to $\mathcal{G}$. Next, we add a directed edge from each vertex $v_{s,k}$ to each of its corresponding four vertices in $\mathcal{C}_k^{+4}$, and another directed edge from each vertex in $\mathcal{C}_k^{+4}$ to its corresponding terminal vertex $v_{t,k}$, as shown in Fig. 2. We let the augmented directed graph be $\mathcal{G}' = (\mathcal{V}', \mathcal{E}')$ where

$\mathcal{V}' = \mathcal{V} \cup \mathcal{V}_s \cup \mathcal{V}_t$, and $|\mathcal{E}'| = 2|\mathcal{E}| + 4K + 4K$. The objective is to find a sub-graph with minimum number of vertices that includes a path from each source vertex $v_{s,k}$ to its corresponding terminal vertex $v_{t,k}$ (excluding trivial solutions using only two edges), yielding the ILP

$$
\begin{aligned}
\min_{y} \quad & \sum_{v \in \mathcal{V}} y_v \\
\text{s. t.} \quad & \sum_{(i,l) \in \delta^+(i)} f_{il}^k - \sum_{(l,i) \in \delta^-(i)} f_{li}^k = d_{i,k}, \quad \forall k \in \mathcal{V}_t, i \in \mathcal{V}' \\
& f_{il}^k \le y'_{il}, \qquad \forall \{i,l\} \in \mathcal{E}, k \in \{1,...,K\} \\
& f_{il}^k \ge 0, \qquad \forall (i,l) \in \mathcal{E}', k \in \{1,...,K\} \\
& f_{v_{s,k},i}^k + f_{i,v_{t,k}}^k \le 1, \ \forall i \in \mathcal{C}_k^{+4}, k \in \{1,...,K\} \\
& y'_{il} \le y_i, \qquad \forall \{i,l\} \in \mathcal{E} \\
& y'_{il} \le y_l, \qquad \forall \{i,l\} \in \mathcal{E} \\
& y_v, y'_e \in \{0,1\}, \qquad \forall e \in \mathcal{E}, v \in \mathcal{V},
\end{aligned}
\tag{12}
$$

where y and y' are decision variables that indicate whether a vertex or an edge is included $\mathcal{G}^*$, respectively. f is a decision variable indicating the flow from each source vertex in $\mathcal{V}_s$ to its corresponding terminal vertex in $\mathcal{V}_t$ on each directed edge in $\mathcal{E}'$, $\delta^+(i)$ is the set of directed edges $(i,l), \forall l \in \mathcal{V}'$ originating from vertex i, $\delta^-(i)$ is the set of directed edges $(l,i), \forall l \in \mathcal{V}'$ terminating at vertex i, and $d_{i,k}$ is defined as

$$
d_{i,k} = \begin{cases} 1, & i = v_{s,k} \\ -1, & i = v_{t,k} \\ 0, & i \in \mathcal{V}' \setminus \{v_{s,k}, v_{t,k}\}. \end{cases}
$$

A special case of the problem arises when considering absolute securing of time references only. The mitigation problem can then be solved by absolutely securing at least $C_i - 2$ time references per equivalence class $\mathcal{C}_i$ [25]. However, solving this problem is not guaranteed to minimize the mitigation cost, since the entire paths from vertices in $\mathcal{C}_i$ to v_r have to be secured, resulting a cost at least as high as when securing paths between pairs of vertices in each $\mathcal{C}_i$ is allowed. This difference is demonstrated in Fig. 2, by showing the optimal solution of [25] (blue) and that of MIN-TM (red).

Proposition 4. *The MIN-TM problem is NP-hard.*

Proof. We prove NP-hardness through reduction from the case when considering absolute securing only (we call it MIN-TM-A), which was shown to be NP-hard [25]. Given an instance of MIN-TM-A with $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ and $\mathcal{C}^{+4}$, we construct an instance of MIN-TM with $\overline{\mathcal{G}} = (\overline{\mathcal{V}}, \overline{\mathcal{E}})$ and $\overline{\mathcal{C}}^{+4}$. First let $\mathcal{C}_k^{+3} = \mathcal{C}_k^{+4} \setminus \{v_r\} = \{v_{k,l} : l \in \{1,2,3\}\}$. Now for each vertex $v_{k,l}$ we append a set $\overline{\mathcal{V}}_{k,l} = \{v_{k,l}^{(1)}, ..., v_{k,l}^{(D)}\}$ of vertices in series to $v_{k,l}$, such that D is larger than the diameter of $\mathcal{G}$, $v_{k,l}^{(D)}$ is a leaf vertex, and $v_{k,l}$ is the parent of $v_{k,l}^{(1)}$. Let the set of extra edges be denoted by $\overline{\mathcal{E}}_{k,l}$. Furthermore, let $\overline{\mathcal{V}}_+ = \bigcup_{k,l} \overline{\mathcal{V}}_{k,l}$ and $\overline{\mathcal{E}}_+ = \bigcup_{k,l} \overline{\mathcal{E}}_{k,l}$. Letting $\overline{\mathcal{C}}_k^{+3} = \{v_{k,l}^{(D)} : l \in \{1,2,3\}\}$ and $\overline{\mathcal{C}}_k^{+4} = \overline{\mathcal{C}}_k^{+3} \cup \{v_r\}$, we can now set $\overline{\mathcal{V}} = \mathcal{V} \cup \overline{\mathcal{V}}_+$, $\overline{\mathcal{E}} = \mathcal{E} \cup \overline{\mathcal{E}}_+$, and $\overline{\mathcal{C}}^{+4} = \{\overline{\mathcal{C}}_1^{+4}, ..., \overline{\mathcal{C}}_K^{+4}\}$. Solving this instance of MIN-TM is guaranteed to solve MIN-TM-A since paths from any vertex in $\overline{\mathcal{C}}_k^{+3}$ to v_r will be shorter than paths between any two vertices in $\overline{\mathcal{C}}_k^{+3}$. The solution for MIN-TM-A can be reconstructed by removing the added vertices $\overline{\mathcal{V}}_{k,l}$ and edges $\overline{\mathcal{E}}_{k,l}$.

Algorithm 1 LP-Greedy

input: Collection of vulnerable quadruplets $\mathcal{C}^{+4}$
output: Set of secured vertices $\mathcal{V}^*$

$\mathcal{V}^* \leftarrow \phi$
$\underline{\mathcal{C}} \leftarrow \phi$ (set of extra constraints)
$f \leftarrow$ Solve LP relaxation of (12) with constraint (13)
for $\mathcal{C}_k^{+4} \in \mathcal{C}^{+4}$ **do**
  Select $v_k^{s*} \in argmax_{v_k^s \in \mathcal{C}_k^{+4}} f_{v_{s,k}, v_k^s}^k$
  $\underline{\mathcal{C}} \leftarrow \underline{\mathcal{C}} \cup \{f_{v_{s,k}, v_k^{s*}}^k = 1\}$
end for
$f \leftarrow$ Solve LP relaxation of (12) with constr. (13) and $\underline{\mathcal{C}}$
for $\mathcal{C}_k^{+4} \in \mathcal{C}^{+4}$ **do**
  Select $v_k^{t*} \in argmax_{v_k^t \in \mathcal{C}_k^{+4}} f_{v_k^t, v_{k,t}}$
  $\mathcal{V}_k \leftarrow$ vertices on the path from v_k^{s*} and v_k^{t*}
  $\mathcal{V}^* \leftarrow \mathcal{V}^* \cup \mathcal{V}_k$
end for

□

C. Proposed Mitigation Algorithms

In what follows we propose two approximation algorithms for solving MIN-TM. Both algorithms solve the problem greedily for each set of vertices $\mathcal{C}_k^{+4}, k \in \{1,...,K\}$, and then combine the respective results. We denote by c_* the cost of the optimal solution for MIN-TM.

Shortest Path Greedy (*SP-Greedy*): For each $\mathcal{C}_k^{+4} \in \mathcal{C}^{+4}$ choose the shortest path among all $\binom{4}{2} = 6$ paths between pairs of vertices in $\mathcal{C}_k^{+4}$. The output of the algorithm is the union of all vertices in all K chosen shortest paths. We denote by c_{SP} the cost of the solution achieved by SP-Greedy.

Proposition 5. *SP-Greedy is a K-approximation of MIN-TM. i.e., $c_{SP} \le K c_*$*

Proof. Consider that the cost (number of vertices) of the shortest path chosen by SP-Greedy for $\mathcal{C}_k^{+4}$ is $\beta_k, k \in \{1, \dots, K\}$. Now consider the worst case that there exists a path (that was not chosen by SP-Greedy) that has a cost of $max_{k \in \{1,...,K\}} \beta_k$, and that this path by itself solves MIN-TM. This is indeed the worst case, since SP-greedy would have chosen this path if it had lower cost. The optimal solution for MIN-TM in this case has a cost of $c_* = max_{k \in \{1,...,K\}} \beta_k$. The solution by SP-Greedy would have a cost of $c_{SP} = \sum_{k=1}^{K} \beta_k$, which can be upper-bounded by $K max_{k \in \{1,...,K\}} \beta_k = K c_*$. □

The second proposed algorithm includes solving a linear relaxation of ILP (12). In order to avoid trivial solutions (solutions with zero cost, e.g., using only edges (v_s, v_6) and (v_6, v_t) in Fig. 2) of the resulting LP, we complement the formulation with the extra constraint

$$
f_{il}^k \le \Big(\sum_{(l,j) \in \delta^+(l)} f_{lj}^k \Big) - \overline{f}_{il}^k, \forall k \in \{1,...,K\}, (i,l) \in \mathcal{E}', l \notin \mathcal{V}_t, \tag{13}
$$

where $\overline{f}_i^k$ is defined as

$$
\overline{f}_{il}^k = \begin{cases} f_{li}^k, & i \in \mathcal{V}' \setminus \{v_{s,k}\} \\ f_{l,v_{t,k}}^k, & i = v_{s,k}. \end{cases}
$$

Algorithm 2 Proposed Mitigation Scheme

input: Measurement matrix H, network graph $\mathcal{G}=(\mathcal{V},\mathcal{E})$, and root vertex v_r

output: Set of secured vertices $\mathcal{V}^*$

1: $\mathcal{C} \leftarrow$ Equivalence classes computed using IoS* (Lemma 2)
2: $\mathcal{C}^{+4} \leftarrow \{\mathcal{C}_k^{+4} : |\mathcal{C}_k^{+4}|=4, v_r \in \mathcal{C}_k^{+4}, \exists i \in \{1,...,C\} \text{ s.t. } \mathcal{C}_k^{+4} \subseteq \mathcal{C}_i^{+}\}$
3: $\mathcal{V}^* \leftarrow$ *SP-Greedy*($\mathcal{C}^{+4}$) or $\mathcal{V}^* \leftarrow$ *LP-Greedy*($\mathcal{C}^{+4}$)

Linear Programming Greedy (*LP-Greedy*): Algorithm 1 shows the pseudo code of *LP-Greedy*. Among all $\binom{4}{2}$ paths between pairs of vertices in each $\mathcal{C}_k^{+4} \in \mathcal{C}^{+4}$, the algorithm chooses the path with the highest flow in the fractional solution of the LP relaxation of ILP (12), along with the extra constraint (13). The output of the algorithm is the union of all vertices in the K paths chosen. We denote by c_{LP} the cost of the solution achieved by LP-Greedy.

Proposition 6. *LP-Greedy is a $4K$-approximation of MIN-TM. i.e., $c_{LP} \leq 4Kc_*$*

Proof. Solving the LP for the first time yields a cost that is at most c_*. Since $max_{v_k^s \in \mathcal{C}_k^{+4}} f_{v_{s,k},v_s^k} \geq 0.25$ always holds, then setting $f^k_{v_{s,k},v_k^{s*}} = 1$ will increase the cost of connecting $\mathcal{C}_i^{+4}$ by a factor of 4 in the worse case. Since this constraint is added K times for each set in $\mathcal{C}^{+4}$, then the cost of the resulting solution c_{LP} will be at most $4Kc_*$. □

The computations needed to implement the proposed mitigation scheme are shown in Algorithm 2.

VI. Numerical Results

In what follows we evaluate the performance of both proposed approximation algorithms through extensive simulations on synthetic graph topologies and on IEEE benchmark power systems. To quantify how well the proposed algorithms solve MIN-TM, we compared their performance in terms of the mitigation cost to the optimal solution obtained by brute-force search (denoted by *Brute-Force*) for small graphs. To evaluate the performance on larger problem instances, we compared the algorithms to the optimal fractional solution of the linear relaxation of ILP (12) along with the constraint (13). Note that this approach only provides a lower bound on the optimal solution, and is thus denoted by *Optimal-LB*. We also compare the performance of the proposed algorithms to the greedy algorithm proposed in [25], which works as SP-Greedy but considering only absolute securing of time references. Since v_r will be included in each shortest path, the output will always be a tree, and thus we refer to this algorithm as *SP-Greedy-T*. In our simulations, we further optimize SP-Greedy, LP-Greedy, and SP-Greedy-T by removing all shortest paths for quadruplets that were already secured by earlier paths. All simulations were carried out on a notebook with Intel Core i7-8550 CPU @ 1.8 GHz and 16 GB of RAM.

A. Performance on Synthetic graphs

To generate random tree graphs with $|\mathcal{V}|$ vertices, we randomly choose $|\mathcal{V}|-1$ edges from all possible $\binom{|\mathcal{V}|}{2}$ edges, such that the graph connectivity is ensured. We then choose v_r to be the vertex with the highest betweenness-centrality in $\mathcal{G}$. To simulate equivalence classes, we randomly choose C disjoint subsets of $\mathcal{V}$ to form the collection $\mathcal{C}$, considering two scenarios for the cardinality of the equivalence classes: (I) $C = 3, C_i \sim \mathcal{U}(3,4)$, and (II) $C=5, C_i \sim \mathcal{U}(3,7)$, where $\mathcal{U}(a,b)$ is a discrete uniform distribution defined by the interval $[a,b]$. Fig. 3 shows the mitigation cost (Fig. 3a) and the execution time (Fig. 3b) for the considered methods to solve MIN-TM, as a function of the number of vertices $|\mathcal{V}|$ in $\mathcal{G}$. Each point represents an averaged value from 200 simulations, along with 95% confidence intervals. From Fig 3a we first observe that Optimal-LB is a loose lower bound on the optimal solution (Brute-force) for smaller graphs in Scenario I, suggesting that the proposed algorithms actually perform much better than indicated by their distance to Optimal-LB. Compared to a naive approach of securing all vertices (i.e., mitigation cost = $|\mathcal{V}|$, assuming $\mathcal{T}=\mathcal{V}$), the proposed algorithms (SP-Greedy and LP-Greedy) achieve cost savings ranging between 50% and 89% for Scenario I, and between 44% and 70% for scenario II. Compared to SP-Greedy-T [25], we observe that the proposed algorithms perform similarly. In fact, SP-Greedy-T performs slightly better, especially for Scenario II when C and C_i (and hence K) were larger. SP-Greedy-T favors shortest paths that are intersecting, which is expected to reduce its cost when vertices in $\mathcal{C}$ are placed randomly in the graph.

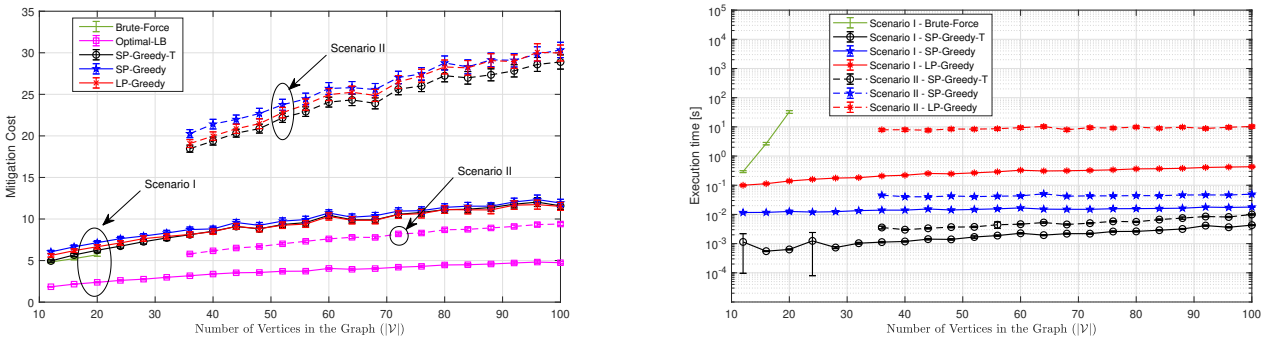
Fig. 3b confirms that the average execution time of SP-Greedy, LP-Greedy, and SP-Greedy-T scale polynomially with $|\mathcal{V}|$, in contrast to Brute-Force which has an exponential execution time. Moreover, the execution time of SP-Greedy-T was consistently one order of magnitude lower than SP-Greedy for both Scenario I and II. The execution time of LP-Greedy was the highest among the polynomial time algorithms, one to two orders of magnitude higher than SP-Greedy.

B. Performance on IEEE Benchmark Power Systems

We used power system topology information in the MATPOWER package [29] in Matlab to evaluate the proposed mitigation scheme on the 118-bus, the 145-bus, and the 300-bus IEEE benchmark power systems. We used the effective rank ratio metric introduced in [30] for computing the equivalence classes $\mathcal{C}$ (and hence, C and C_i). For each of the considered benchmark power systems, we chose $\mathcal{V}$ to be the set of buses in the system. The set $\mathcal{E}$ of edges was chosen to be a random subset of connections between buses, such that $\mathcal{G}=(\mathcal{V},\mathcal{E})$ forms a tree. Similar to synthetic graphs, v_r was chosen as the vertex with the highest betweenness-centrality in $\mathcal{G}$. Furthermore, we set the set $\mathcal{T}$ of time references to be the buses (vertices) that have a PMU installed. In a practical deployment, each bus with a PMU may correspond to multiple vertices, e.g., one for the PTP switch in the corresponding substation, and one for the PMU itself, but this simplifcation does not change the solution to the MIN-TM problem.

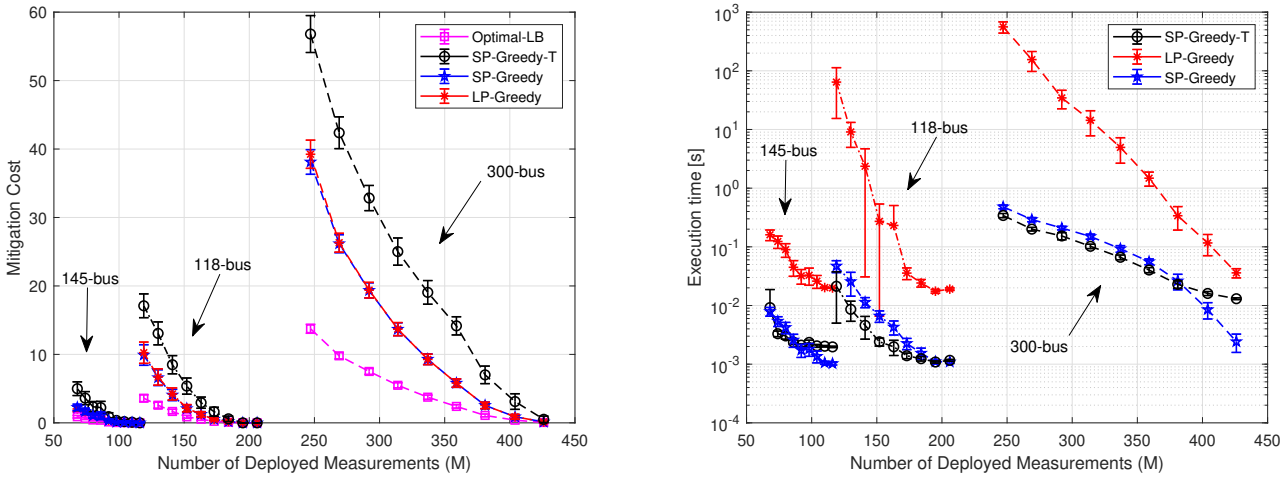
Fig. 4 shows the mitigation cost (Fig. 4a) and the execution time (Fig. 4b) for the considered methods, as a function of the number of measurements M deployed in the system. Each point represents an averaged value from 100 deployments of M voltage and current injection phasor measurements, along with 95% confidence intervals. The M measurements were located at random, given that they ensure the observability of the power system and the absence of critical measurements. That is, the rank of the measurement matrix H and all its possible $M-1 \times N$ sub-matrices is N (i.e., they have full column rank). Note that we do not deploy PMUs on zero-injection buses (i.e., buses that do not have either generators or loads, as

This article has been accepted for publication in IEEE Transactions on Control of Network Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2024.3368316



(a) (b)

Fig. 3: Mitigation cost (a) and execution time (b) for synthetic graphs with either $C=3$ and $C=5$ equivalence classes.



(a) (b)

Fig. 4: Mitigation cost (a) and execution time (b) for the IEEE 118-bus, the IEEE 145-bus, and the IEEE 300-bus systems.

specified in the MATPOWER package). The number of measurable buses N^* (i.e., not zero-injection buses) for the IEEE 118-bus, 145-bus, and 300-bus systems was 108, 61, and 224, respectively.

Fig. 4a shows higher cost savings achieved by the proposed algorithms on IEEE benchmark systems compared to synthetic graphs. A naive approach that secures all time references will have an average mitigation cost of $|\mathcal{T}|=0.75N^*$ when $M=N$ (sparsest possible PMU deployment). Compared to that, SP-Greedy and LP-Greedy can reduce the cost by at least 87%, 95%, and 76% for the IEEE 118-bus, 145-bus, and 300-bus systems, respectively. Moreover, SP-Greedy and LP-Greedy significantly outperform SP-Greedy-T for all three IEEE benchmark systems, reducing the cost by at least 40%, 53%, and 30% for the IEEE 118-bus, 145-bus, and 300-bus systems, respectively. In this realistic setting, an equivalence class $\mathcal{C}_i$ typically consists of vertices that are closer to each other than they are to v_r, and thus relatively securing time references in $\mathcal{C}_i$ is more efficient than absolute securing. Moreover, even though the performance of the proposed algorithms is not close to Optimal-LB, Fig. 3a suggests that the distance to the optimal solution achieved by e.g., Brute-Force would be much smaller. Overall, Fig. 4a demonstrates an important trade-off between the cost of deploying extra measurements in the system and that of securing time references. For the execution time, Fig. 4b shows that SP-Greedy-T is slightly more time efficient than SP-Greedy, while LP-Greedy takes signifcantly higher execution time (upto 3 orders of magnitudes) than that of SP-Greedy. Overall, the results suggest that SP-Greedy performs well in terms of both mitigation cost and execution time compared to its competitors. When time complexity is not an issue, the operator can simply choose the algorithm that yields the smallest cost.

VII. Conclusion

We considered the problem of mitigating undetectable TSAs against power systems, by using a combination of LSE and PTP authentication. We provided necessary and sufficient conditions for the existence of undetectable TSAs that implies that a TSA is undetectable if and only if at least 3 time references are manipulated. Based on that, we then formulated the problem of mitigating undetectable TSAs at minimum cost, and proposed two approximation algorithms for solving it. Beside being computationally efficient, the proposed algorithms were shown to result in huge cost savings compared to the naive mitigation approach, and significant savings compared to previous work, both for synthetic graph topologies and for realistic IEEE benchmark systems.

Acknowledgement

The work was partly funded by the Swedish Civil Contingencies Agency (MSB) through the CERCES2 project and by the Swedish Research Council through project 2020-03860.

REFERENCES

[1] A. Xue, S. Leng, Y. Li, F. Xu, K. E. Martin, and J. Xu, "A novel method for screening the PMU phase angle difference data based on hyperplane clustering," *IEEE Access*, vol. 7, 2019.

[2] G. Liu, J. Quintero, and V. M. Venkatasubramanian, "Oscillation monitoring system based on wide area synchrophasors in power systems," in *iREP Symposium - Bulk Power System Dynamics and Control - VII. Revitalizing Operational Reliability*, 2007, pp. 1–13.

[3] M. Jamei, A. Scaglione, and S. Peisert, "Low-resolution fault localization using phasor measurement units with community detection," in *Proc. of IEEE SmartGridComm*, 2018, pp. 1–6.

[4] V. Pallares-Lopez, A. Moreno-Muñoz, M. Gonzalez-Redondo, R. Real-Calvo, I. M. García, and J. J. G. de la Rosa, "Synchrophasor integration in iec 61850 standard for smartgrid and synchronism with ptp-base system," in *IEEE Conference on Industrial Electronics and Applications*, 2011, pp. 1507–1512.

[5] *1588-2019 - IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*, 2019 (accessed Dec. 1, 2020). [Online]. Available: https://standards.ieee.org/content/ieee-standards/en/standard/1588-2019.html

[6] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Trans. on Smart Grid*, vol. 4, no. 1, pp. 87–98, 2013.

[7] M. Han and P. Crossley, "Vulnerability of ieee 1588 under time synchronization attacks," in *IEEE Power Energy Society General Meeting (PESGM)*, 2019.

[8] E. Shereen, F. Bitard, G. Dán, T. Sel, and S. Fries, "Next steps in security for time synchronization: Experiences from implementing IEEE 1588 v2.1," in *Proc. of IEEE ISPCS*, 2019, pp. 1–6.

[9] A. Abur and A. G. Expósito, "Power system state estimation : Theory and implementation." Marcel Dekker, 2004.

[10] S. Barreto, M. Pignati, G. Dán, J. Le Boudec, and M. Paolone, "Undetectable PMU timing-attack on linear state-estimation by using rank-1 approximation," *IEEE Trans. on Smart Grid*, vol. 9, no. 4, pp. 3530–3542, 2018.

[11] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. of ACM CCS*, 2009, p. 21–32.

[12] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proc. of IEEE SmartGridComm*, 2010, pp. 214–219.

[13] O. Vukovic, K. C. Sou, G. Dán, and H. Sandberg, "Network-aware mitigation of data integrity attacks on power system state estimation," *IEEE J. on Sel. Areas Commun. (JSAC)*, vol. 30, no. 6, pp. 1108–1118, 2012.

[14] K. C. Sou, "Protection placement for power system state estimation measurement data integrity," *IEEE Transactions on Control of Network Systems*, vol. 7, no. 2, pp. 638–647, 2020.

[15] J. J. Q. Yu, Y. Hou, and V. O. K. Li, "Online false data injection attack detection with wavelet transform and deep neural networks," *IEEE Trans. on Industr. Informatics*, vol. 14, no. 7, 2018.

[16] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using kalman filter," *IEEE Transactions on Control of Network Systems*, vol. 1, no. 4, pp. 370–379, 2014.

[17] R. Ramakrishna and A. Scaglione, "Grid-graph signal processing (Grid-GSP): A graph signal processing framework for the power grid," *IEEE Trans. on Signal Processing*, 2021.

[18] E. Shereen, R. Ramakrishna, and G. Dán, "Detection and localization of PMU time synchronization attacks via graph signal processing," *IEEE Trans. on Smart Grid*, vol. 13, no. 4, pp. 3241–3254, 2022.

[19] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Trans. on Smart Grid*, vol. 11, no. 3, pp. 2218–2234, 2020.

[20] Y. Fan, Z. Zhang, M. Trinkle, A. D. Dimitrovski, J. B. Song, and H. Li, "A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids," *IEEE Trans. on Smart Grid*, vol. 6, no. 6, 2015.

[21] B. Moussa, M. Debbabi, and C. Assi, "A detection and mitigation model for PTP delay attack in an IEC 61850 substation," *IEEE Trans. on Smart Grid*, vol. 9, no. 5, pp. 3954–3965, 2018.

[22] E. Shereen and G. Dán, "Model-based and data-driven detectors for time synchronization attacks against PMUs," *IEEE J. Sel. Areas Commun. (JSAC)*, vol. 38, no. 1, pp. 169–179, 2020.

[23] S. Bhamidipati, T. Y. Mina, and G. X. Gao, "GPS time authentication against spoofing via a network of receivers for power systems," in *IEEE/ION Position, Location and Navigation Symposium (PLANS)*, 2018, pp. 1485–1491.

[24] E. Itkin and A. Wool, "A security analysis and revised security extension for the precision time protocol," *IEEE Trans. on Dependable and Secure Computing*, vol. 17, no. 1, pp. 22–34, 2020.

[25] E. Shereen and G. Dán, "Network-aware mitigation of undetectable PMU time synchronization attacks," in *Proc. of IEEE SmartGridComm*, 2020.

[26] E. Shereen, M. Delcourt, S. Barreto, G. Dán, J. Le Boudec, and M. Paolone, "Feasibility of time-synchronization attacks against PMU-based state estimation," *IEEE Trans. on Instrumentation and Measurement*, vol. 69, no. 6, pp. 3412–3427, 2020.

[27] Y. Liu, A. K. Singh, J. Zhao, A. P. S. Meliopoulos, B. Pal, M. A. b. M. Ariff, T. Van Cutsem, M. Glavic, Z. Huang, I. Kamwa, L. Mili, A. S. Mir, A. Taha, V. Terzija, and S. Yu, "Dynamic state estimation for power system control and protection," *IEEE Trans. on Power Systems*, vol. 36, no. 6, pp. 5909–5921, 2021.

[28] M. X. Goemans and Y. Myung, "A catalog of steiner tree formulations," *Networks*, vol. 23, pp. 19–28, 1993.

[29] R. D. Zimmerman and C. E. Murillo-Sanchez, "(2019). MATPOWER (version 7.0) [Software]," available: https://matpower.org.

[30] M. Delcourt and J.-Y. L. Boudec, "Security measures for grids against rank-1 undetectable time-synchronization attacks," *arXiv, eess.SY*, vol. 2002.12607, 2020.

APPENDIX

Proof of Lemma 3. As shown earlier, the LHS of (4) represents an annular region $AR_{1,q-1} = (c_{1,q-1}, r^o_{1,q-1}, r^i_{1,q-1})$ where $c_{1,q-1} =$

$-\sum_{i=1}^{q-1} W_{1i}$, $r^o_{1,q-1} = \sum_{i=1}^{q-1} |W_{1i}|$, $r^i_{1,q-1} = max\{0, 2|W_{1i^*}| - \sum_{i=1}^{q-1} |W_{1i}|\}$, and $i^* = argmax_{i\in\{1,\cdots,q-1\}}|W_{1i}|$. The RHS represents a circle $O_q = (W_{1q}+s, |W_{1q}|)$.

Observe that the existence of only one solution to (4) implies that there can be only one intersection point between the circle and the annular region. Proving the inverse, i.e., that the existence of only one intersection point implies that only one solution to (4) exists, will be shown later.

The annular region and the circle intersect in only one point in three cases, depending on the relative locations of O_q and $AR_{1,q-1}$.

1) Case A: In the first case, the circle O_q is outside the annular region, thus the distance between the center of the annular region and the center of the circle equals the sum of the outer radius of the annular region and the radius of the circle, i.e.,

$$|c_{1,q-1} - c_q| = r^o_{1,q-1} + r_q. \tag{14}$$

Substituting the definitions for O_q and $AR_{1,q-1}$ into (14) we obtain

$$\left| -\sum_{i=1}^{q-1} W_{1i} - W_{1q} - s \right| = \left(\sum_{i=1}^{q-1} |W_{1i}| \right) + |W_{1q}|,$$

which yields (5).

2) Case B: The second case arises when the radius of the circle O_q is equal to the sum of (1) the distance between the centers of the annular region and the circle, and (2) the outer radius of the annular region, i.e.,

$$\begin{aligned} r_q &= |c_{1,q-1} - c_q| + r^o_{1,q-1} \\ r_q - r^o_{1,q-1} &= |c_{1,q-1} - c_q|. \end{aligned} \tag{15}$$

Substituting into (15) we obtain

$$|W_{1q}| - \sum_{i=1}^{q-1} |W_{1i}| = \overline{w}(q,s). \tag{16}$$

3) Case C: The third case arises if the inner radius of the annular region is equal to the sum of (1) the distance between the centers of the annular region and the circle, and (2) the radius of the circle, i.e.,

$$\begin{aligned} r^i_{1,q-1} &= |c_{1,q-1} - c_q| + r_q \\ r^i_{1,q-1} - r_q &= |c_{1,q-1} - c_q|. \end{aligned} \tag{17}$$

Substituting into (17) we obtain

$$|W_{1i^*}| - \sum_{i\neq i^*} |W_{1i}| = \overline{w}(q,s), \tag{18}$$

where $i^* = argmax_{i\in\{1,\cdots,q-1\}}|W_{1i}|$.

Recall that from case A, (5) is a sufficient condition for having one intersection point between O_q and $AR_{1,q-1}$. Furthermore, observe that (16) and (18) can be combined as

$$\begin{aligned} |W_{1i^*}| - \sum_{i\neq i^*} |W_{1i}| &= \overline{w}(q,s) \\ 2|W_{1i^*}| - \sum_{i=1}^{q} |W_{1i}| &= \overline{w}(q,s), \end{aligned}$$

where $i^* = argmax_{i\in\{1,\cdots,q\}}|W_{1i}|$, which proves that (6) is also a sufficient condition for having one intersection point. Therefore, only one intersection point can be found if either of (5) or (6) holds. Furthermore, the three cases A, B and C are the only cases where the circle has only one intersection point with $AR_{1,p-1}$. Therefore, if O_q and $AR_{1,q-1}$ intersect in only one point, then either (5) or (6) must hold.

To prove that (5) and (6) are necessary and sufficient conditions for having only one solution to (4), we need to show that there exists only one solution to (4) if and only if there exists only one intersection point between $AR_{1,q-1}$ and O_q. Recall that a unique solution to (4) implies that only one intersection point exists. It remains to prove the opposite, i.e., that the existence of only one intersection point between $AR_{1,q-1}$ and O_q implies the existence of only one solution to (4). To prove that, that we consider the conditions (5) and (6) for having only one intersection point.

Notice that since $s = \sum_{i=1}^{q} W_{1i}(u_i - 1)$, we can rewrite (5) and (6) as

$$\left| \sum_{i=1}^{q} W_{1i} u_i \right| = \sum_{i=1}^{q} |W_{1i}|, \tag{19}$$

$$\left| \sum_{i=1}^{q} W_{1i} u_i \right| = 2|W_{1i^*}| - \sum_{i=1}^{q} |W_{1i}|. \tag{20}$$

Observe that since $|u_i| = 1$, then (19) cannot be satisfied unless all $W_{1i}u_i, i \in \{1,\cdots,q\}$ point in the same direction, which is the direction of their sum. In other words, they point in the direction of $(\sum_{i=1}^{q} W_{1i}) + s$. Therefore

$$\begin{aligned} W_{1j}u_j &= \left[\left(\sum_{i=1}^{q} W_{1i} \right) + s \right] * \frac{|W_{1j}|}{|(\sum_{i=1}^{q} W_{1i}) + s|} \\ u_j &= \frac{[(\sum_{i=1}^{q} W_{1i}) + s]}{W_{1j}} * \frac{|W_{1j}|}{|(\sum_{i=1}^{q} W_{1i}) + s|}, \end{aligned} \tag{21}$$

for all $j \in \{1,\cdots,q\}$. It is clear that (21) yields only one solution $(u_1,\cdots,u_q)$, and hence there exist only one solution to (4).

On the other hand, (20) cannot be satisfied unless all $W_{1i}u_i, i \in \{1,\cdots,q\} \setminus \{i^*\}$ point in the same direction, which is the opposite direction to $W_{1i^*}u_{i^*}$ and $(\sum_{i=1}^{q} W_{1i}) + s$. Therefore

$$\begin{aligned} u_{j\neq i^*} &= \frac{-[(\sum_{i=1}^{q} W_{1i}) + s]}{W_{1j}} \frac{|W_{1j}|}{|(\sum_{i=1}^{q} W_{1i}) + s|} \\ u_{i^*} &= \frac{[(\sum_{i=1}^{q} W_{1i}) + s]}{W_{1i^*}} \frac{|W_{1i^*}|}{|(\sum_{i=1}^{q} W_{1i}) + s|}. \end{aligned} \tag{22}$$

Again, it is clear that (22) yields only one solution $(u_1,\cdots,u_q)$, and hence there exists only one solution to (4). □

Proof of Lemma 5. For computing u_q we can rearrange (3) to

$$\sum_{i=1}^{q-1} W_{1i}(u_i - 1) = -W_{1,q}(u_q - 1) + \sum_{j=q+1}^{P} s_j, \tag{23}$$

where $s_j = W_{1j}(u'_j - 1)$. The solution of (23) corresponds to the intersection between an annular region $AR_{1,q-1}$ (the LHS) and a circle O_q, with the same definitions as in Lemma 3, for $s = \sum_{j=q+1}^{P} s_j$. Similar to Lemma 4, having more than one intersection point is equivalent to that the feasible set of attack angles $\Theta_q(\theta_q^+) = \{\theta_q : u_q = e^{j\theta_q}, u_q \in \mathcal{U}_q(u_q^+)\}$ is a non-empty connected bounded open interval or the union of two such intervals, and thus u_q is a free variable.

Therefore, u_q will not be a free variable if (23) has one solution or no solution. To identify the conditions for which (23) has one

solution we can use Lemma 3 with $s=\sum_{j=q+1}^{P} s_j$ to obtain

$$\left|\sum_{i=1}^{q} W_{1i}+\sum_{j=q+1}^{P} s_j\right| = \sum_{i=1}^{q}|W_{1i}| \quad (24)$$

$$\left|\sum_{i=1}^{q} W_{1i}+\sum_{j=q+1}^{P} s_j\right| = 2|W_{1i^*}|-\sum_{i=1}^{q}|W_{1i}|, \quad (25)$$

where $i^* = argmax_{i\in\{1,\cdots,q\}}|W_{1i}|$. Observe that the RHS of (24) and (25) are equal to $r^o_{1,q}$ and $r^i_{1,q}$, respectively. Furthermore, note that the term $\left|\sum_{i=1}^{q} W_{1i}+\sum_{j=q+1}^{P} s_j\right|$ represents the distance between the center of the annular region $AR_{1,q}$ (i.e., $c_{1,q}$) and its intersection point with O_{q+1} (i.e., $\sum_{j=q+1}^{P} s_j$). We can then establish that the two conditions (24) and (25) hold if the intersection point lies on the outer or on the inner bounding circle of the annular region $AR_{1,q}$. Therefore, the inequalities $\left|\sum_{i=1}^{q} W_{1i}+\sum_{j=q+1}^{P} s_j\right| > r^o_{1,q}$, or $\left|\sum_{i=1}^{q} W_{1i}+\sum_{j=q+1}^{P} s_j\right| < r^i_{1,q}$ correspond to choosing the intersection point $\sum_{j=q+1}^{P} s_j$ outside of the annular region, and thus $u_j^{'} \notin \mathcal{U}_j(u_j^+)$ for some $j\in\{q+1,\cdots,P\}$ does not lie in the feasible intervals, which means that $AR_{1,q-1}$ and O_q will not intersect, and thus (23) has no solution. This proves the lemma. □

Ezzeldin Shereen (S'18-M'22) received the B.Sc. and M.Sc. degrees in networking engineering from the German University in Cairo, Egypt, in 2014 and 2015, respectively. He received the Ph.D. degree in 2021 from the School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, Stockholm, Sweden, where he is currently working as a Postdoctoral Researcher. His research interests include cyberphysical systems security with focus on power systems, robustness of machine learning and reinforcement learning, and performance evaluation of wireless networks.

György Dán (M'07–SM'17) received the M.Sc. degree in computer engineering from the Budapest University of Technology and Economics, Budapest, Hungary, in 1999, the M.Sc. degree in business administration from the Corvinus University of Budapest, Budapest, in 2003, and the Ph.D. degree in telecommunications from the KTH Royal Institute of Technology, Stockholm, Sweden, in 2006. From 1999 to 2001, he was a Consultant in the field of access networks, streaming media, and videoconferencing with BCN Ltd., Budapest. He was a Visiting Researcher with the Swedish Institute of Computer Science, Stockholm, in 2008, a Fulbright Research Scholar with the University of Illinois at Urbana–Champaign, Champaign, IL, USA, in 2012 and 2013, and an Invited Professor with the Swiss Federal Institute of Technology of Lausanne (EPFL), Lausanne, Switzerland, in 2014 and 2015. He is currently a Professor with the KTH Royal Institute of Technology. His current research interests include the design and analysis of content management and computing systems, game theoretical models of networked systems, and cyber-physical system security and resilience. Dr. Dán has been an Area Editor of Computer Communications 2014-2021 and the IEEE TRANSACTION ON MOBILE COMPUTING 2019-2023.