Pulse-Coupled Oscillators Resilient to Stealthy Attacks

Zhenqian Wang and Yongqiang Wang, *Senior Member, IEEE*

***Abstract*—Synchronization of bio-inspired pulse-coupled oscillators (PCOs) is receiving increased attention due to its wide applications in sensor networks and wireless communications. However, most existing results are obtained in the absence of malicious attacks. Given the distributed and unattended nature of wireless sensor networks, it is imperative to enhance the resilience of pulse based synchronization against malicious attacks. To achieve this goal, we propose a new pulse based interaction mechanism to improve the resilience of pulse based synchronization. We rigorously characterize the condition for mounting stealthy attacks under the proposed pulse based interaction mechanism and prove analytically that synchronization of legitimate oscillators can be achieved in the presence of multiple stealthy attackers even when the initial phases are unrestricted, i.e., randomly distributed in the *entire* oscillation period. This is in distinct difference from most existing attack-resilient synchronization algorithms (including the seminal paper from Lamport and Melliar-Smith [1]) which require a priori (almost) synchronization among legitimate nodes. Numerical simulations are given to confirm the theoretical results.**

I. Introduction

Inspired by flashing fireflies and contracting cardiac cells, pulse based synchronization is attracting increased attention in wireless networks [2]–[5]. By exchanging simple and identical pulses, pulse based synchronization can be established with much less energy consumption and communication overhead compared with conventional packet-based synchronization approaches [6]. These inherent advantages make pulse based synchronization appealing to the clock synchronization of wireless sensor networks [7]–[11]. In the past decade, plenty of results have been obtained on pulse based synchronization. For example, by optimizing the interaction function, i.e., phase response function, synchronization speed of pulse-coupled oscillators (PCOs) is maximized in [12]; with a judiciously-added refractory period in the phase response function, the energy consumption in PCO synchronization is reduced in [13]–[15]; [16]–[18] show that PCOs can achieve synchronization under a general coupling topology even when their initial phases are randomly distributed in the entire oscillation period. Recently, synchronization of PCOs in the presence of time-delays and unreliable links is also discussed [19], [20]. Other relevant results include [21]–[25].

However, the above results are obtained based on the assumption that all oscillators behave correctly with no nodes compromised by malicious attackers. Due to the distributed and unattended nature, wireless sensor nodes are extremely vulnerable to attacks, which makes it imperative to study synchronization in the presence of attacks. Although plenty of discussions exist for conventional packet-based synchronization, e.g., [1], [26]–[31], results on the attack-resilience of pulse based synchronization are very sparse. In [32], the authors showed that pulse based synchronization is more robust than its packet-based counterpart in the presence of a faulty node. In [33], a new phase response function was proposed to combat non-persistent random attacks in pulse based synchronization. The authors in [34] considered pulse based synchronization in the presence of faulty nodes which fire periodically irrespective of neighboring nodes. However, none of the above pulse based studies address situations where compromised nodes act maliciously and apply disturbing pulses with judiciously-crafted pattern to corrupt synchronization. Furthermore, these results only apply to a *priori* synchronized PCOs, i.e., all legitimate nods are required to have *identical* phases when faulty pulses are emitted.

In this paper, we consider the synchronization of PCOs under stealthy Byzantine attacks. In the pulse based interaction framework where exchanged messages (so-called pulses) are identical and content-free, Byzantine attacks mean compromised nodes injecting pulses using judiciously crafted patterns to disturb the synchronization process. We consider stealthy Byzantine attacks which are intelligent and only use pulse injection patterns undetectable by legitimate nodes. So compared with existing results in [32]–[34], the situation considered in this paper is more difficult to deal with due to the intelligent behavior of malicious attackers. By proposing a new pulse based interaction approach, we show that perfect synchronization of legitimate oscillators can still be guaranteed even when their initial phases are randomly distributed in the entire oscillation period $[0, 2\pi]$, which is in distinct difference from our recent results in [35] requiring initial phases to be restricted in a certain interval. The approach is applicable even when individual oscillators do not have access to the total number of oscillators in a network.

This paper is organized as follows. Sec. II introduces a new pulse based interaction mechanism. Sec. III characterizes the synchronization condition of all-to-all PCOs under the new interaction mechanism in the absence of attacks. In Sec. IV, under a pulse-number based detection mechanism, we characterize the condition for an attacker to keep stealthy, i.e., mounting attacks without being detected. In Sec. V, we prove that synchronization of legitimate oscillators can be guaranteed even in the presence of multiple stealthy Byzantine attackers. We also extend the results to relaxed initial conditions, i.e.,

This work was supported in part by the National Science Foundation under Grant 1738902 and China Scholarship Council.

Zhenqian Wang and Yongqiang Wang are with the Department of Electrical and Computer Engineering, Clemson University, Clemson, SC, 29630 USA. The corresponding author is Yongqiang Wang (yongqiw@clemson.edu).

arbitrary distribution on the entire oscillation period $[0,2\pi]$ in Sec. V. In Sec. VI, we further show that our approach is still applicable even when the total number of oscillators in a network is unknown to individual oscillators. Simulation results are presented in Sec. VII.

II. A New Pulse Based Interaction Mechanism

Consider a network of N pulse-coupled oscillators. Each oscillator is equipped with a phase variable. When the evolving phase of an oscillator satisfies a certain condition, the oscillator will emit a pulse. Receiving a pulse from a neighboring oscillator will lead to the adjustment of the receiving oscillator's phase, which can be designed to achieve a desired collective behavior such as phase synchronization. Motivated by the fact that the conventional pulse based interaction mechanism is vulnerable to attacks, we propose a new pulse based interaction mechanism to enable resilience of PCO synchronization. To this end, we first present the conventional pulse based interaction mechanism.

Conventional pulse based interaction approach [15]:

1) The phase ϕ_i of oscillator i evolves from 0 to 2π *rad* with a constant speed ω. Without loss of generality, we assume $\omega = 1 rad/second$ in this paper.
2) Once ϕ_i reaches 2π *rad*, oscillator i fires (emits a pulse) and resets its phase to 0.
3) *Whenever* oscillator i receives a pulse, it *instantaneously* resets its phase to

$$\phi_i^+ = \phi_i + l \times F(\phi_i) \tag{1}$$

where $l \in (0,1]$ is the coupling strength and $F(\bullet)$ is the phase response function (PRF) with an example given in (2)

$$F(\phi) := \begin{cases} -\phi & 0 \le \phi \le \pi \\ 2\pi - \phi & \pi < \phi \le 2\pi \end{cases} \tag{2}$$

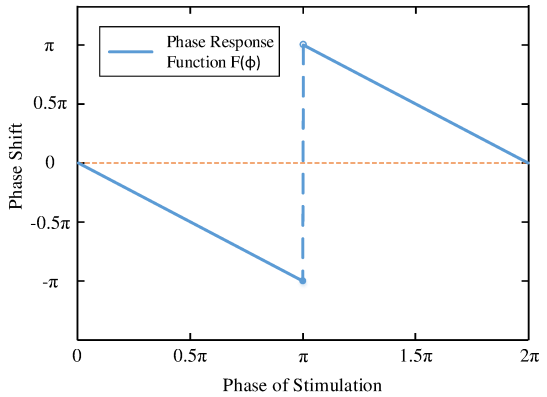

Figure 1: Phase Response Function

The PRF in (2) is visualized in Fig. 1. In the conventional pulse based interaction mechanism, every incoming pulse triggers a jump on the receiving oscillator's phase, which makes attackers easy to perturb the phase of legitimate oscillators and destroy their synchronization. Based on this observation, we propose a new pulse based interaction mechanism to improve the resilience of pulse based synchronization. The key idea is to let an oscillator adjust its phase only when sufficiently many pulses are received, as detailed below:

New pulse based interaction approach (Mechanism 1):

1) The phase ϕ_i of oscillator i evolves from 0 to 2π *rad* with a constant speed $\omega = 1 rad/second$.
2) Once ϕ_i reaches 2π *rad*, oscillator i fires (emits a pulse) and resets its phase to 0.
3) When oscillator i receives a pulse at time instant t, it shifts its phase according to (1) only when both of the following conditions are satisfied:
   a) an entire period $T = 2\pi/\omega = 2\pi$ *seconds* has elapsed since initiation;
   b) in the past quarter period, oscillator i fired and received at least $\lambda - 1$ pulses, or oscillator i did not fire but received at least λ pulses within this past quarter period, where $\lambda = \lfloor (N-1)/5 \rfloor$ holds and $\lfloor \bullet \rfloor$ is the largest integer no greater than "$\bullet$."

   Otherwise, the pulse has no effect on $\phi_i(t)$.

Fig. 2 gives the evolution of one legitimate oscillator's phase in a network of eleven PCOs. Given $\lambda = \lfloor (N-1)/5 \rfloor = 2$, we have that a pulse can trigger a phase jump on a receiving oscillator only when 1) it is sent after time T has elapsed since initiation; and 2) in the past quarter period, at least two pulses were received by the oscillator, or the oscillator fired and received at least one other pulse in the past quarter period. Therefore, in Fig. 2, only the 9th pulse causes a jump on the phase of the considered oscillator.

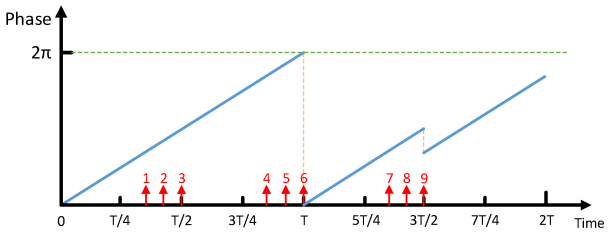

Figure 2: The phase evolution of a legitimate oscillator in an all-to-all network of eleven oscillators under Mechanism 1. Vertical pulses represent incoming pulses.

Remark 1: Following [23]–[25], we assume that when a legitimate oscillator receives multiple pulses simultaneously, it will process these pulses consecutively. In other words, no two pulses will be regarded as an aggregated pulse.

Remark 2: Compared with the conventional pulse based interaction mechanism, the new one is more resilient to malicious pulse attacks, as illustrated later by the simulation results in Fig. 8, Fig. 9, Fig. 10, and Fig. 11. Rigorous analysis will be provided in Sec. V.

III. Synchronization of All-to-All PCOs in the Absence of Attacks

In this section, we will show that all-to-all connected oscillators can be guaranteed to synchronize under Mechanism 1 in the absence of attacks. To this end, we first define synchronization:

Definition 1 (Synchronization): We define synchronization to be achieved when all legitimate oscillators fire at the same time instants.

To facilitate theoretical analysis, we also define containing arc as follows:

Definition 2 (Containing Arc): The containing arc is defined as the shortest arc on the unit circle that contains all legitimate oscillators' phases.

When oscillators' phases approach synchronization, the length of the containing arc converges to zero.

We first characterize the property of all-to-all PCO networks under Mechanism 1.

Lemma 1: In an attack-free all-to-all network of N PCOs, if the firing of an oscillator can trigger a phase jump on another oscillator, then the firing can trigger phase jumps on all the other $N-1$ oscillators.

Proof: Without loss of generality, we assume that oscillator $i's$ firing at time instant t_i triggers the phase of oscillator j to jump, which, according to Mechanism 1, implies that oscillator j either fired and received at least $\lambda-1$ pulses in the past quarter period, or it did not fire in the past quarter period but received at least λ pulses within. In both cases, it can be inferred that for any oscillator other than i, if it fired in the past quarter period, then it must have received at least $\lambda-1$ pulses under the considered all-to-all topology; or if it did not fire in the past quarter period, then it must have received at least λ pulses within. Therefore, in an all-to-all topology, if the firing of an oscillator i triggers another oscillator j to jump, then it will trigger all the other $N-1$ oscillators to jump. ■

Now we are in place to present the synchronization condition in the absence of attacks:

Theorem 1: For an attack-free all-to-all network of N PCOs, if the length of the initial containing arc is less than π *rad*, then Mechanism 1 can achieve perfect synchronization.

Proof: First, we will show that the length of the containing arc will never increase. It can be easily inferred that the length of the containing arc remains unchanged if no oscillator jumps in phase. So we only need to consider the case that an oscillator's firing triggers a jump on another oscillator. Based on Lemma 1, one can know that if the firing of an oscillator triggers a jump on another oscillator, it will trigger phase jumps on all the other oscillators.

We assume that oscillator i fires at time instant t_i whose pulse triggers phase jumps on all the other oscillators. One can easily get $\phi_i(t_i)=2\pi$ *rad*, i.e., the containing arc includes the phase point 2π *rad* at time instant t_i. Since the length of the containing arc is less than π *rad*, the phases of the other $N-1$ oscillators at this time instant can only be distributed in the following three ways, as depicted in Fig. 3:

1) all the other $N-1$ oscillators' phases reside in $(\pi,2\pi]$;
2) all the other $N-1$ oscillators' phases reside in $[0,\pi)$;
3) the other $N-1$ oscillators' phases reside partially in $[0,\pi)$ and partially in $(\pi,2\pi]$.

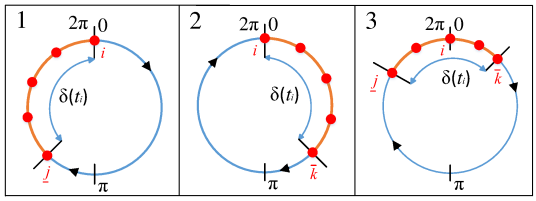

Figure 3: Three possible phase distribution of all oscillators when oscillator i fires at time instant t_i.

Denoting $\delta(t_i)$ as the length of the containing arc at time instant t_i, we next show that $\delta(t_i)$ cannot be increased by the firing of oscillator i in any of the three cases, i.e., $\delta^+(t_i)\le\delta(t_i)$ always holds.

1) When all the other $N-1$ oscillators' phases reside in $(\pi,2\pi]$, at time instant t_i, the length of the containing arc can be obtained as follows:

$$\delta(t_i)=\phi_i(t_i)-\min_{j\in\mathcal{N},j\neq i}\{\phi_j(t_i)\}=2\pi-\phi_{\underline{j}}(t_i) \tag{3}$$

where $\mathcal{N}=\{1,2,\cdots,N\}$ represents the index set and $\underline{j}=\arg\min_{j\in\mathcal{N},j\neq i}\phi_j(t_i)$. After the firing of oscillator i, we have $\phi_i^+(t_i)=0$. Under the PRF in (2), one can get $\phi_j^+(t_i)=\phi_j(t_i)+l(2\pi-\phi_j(t_i))$ for $j\in\mathcal{N},j\neq i$. The length of the containing arc becomes

$$\begin{aligned}\delta^+(t_i)&=2\pi-\min_{j\in\mathcal{N},j\neq i}\{\phi_j^+(t_i)\}+\phi_i^+(t_i)\\&=2\pi-\min_{j\in\mathcal{N},j\neq i}\{\phi_j^+(t_i)\}\\&=(1-l)(2\pi-\phi_{\underline{j}}(t_i))=(1-l)\delta(t_i)\end{aligned} \tag{4}$$

Since $0<l\le 1$ holds, one can easily get $\delta^+(t_i)\le\delta(t_i)$ in this case (Note that the equality mark holds only when $\delta(t_i)=0$ is true, meaning that the network is synchronized).

2) When all the other oscillators' phases reside in $[0,\pi)$, at time instant t_i, the length of the containing arc can be obtained as follows:

$$\delta(t_i)=2\pi-\phi_i(t_i)+\max_{k\in\mathcal{N},k\neq i}\{\phi_k(t_i)\}=\phi_{\bar{k}}(t_i) \tag{5}$$

where $\bar{k}=\arg\max_{k\in\mathcal{N},k\neq i}\phi_k(t_i)$. After the firing of oscillator i, we have $\phi_i^+(t_i)=0$. Under the PRF in (2), one can get $\phi_k^+(t_i)=(1-l)\phi_k(t_i)$ for $k\in\mathcal{N},k\neq i$ and the length of the containing arc becomes

$$\begin{aligned}\delta^+(t_i)&=\max_{k\in\mathcal{N},k\neq i}\{\phi_k^+(t_i)\}-\phi_i^+(t_i)=\max_{k\in\mathcal{N},k\neq i}\{\phi_k^+(t_i)\}\\&=(1-l)\phi_{\bar{k}}(t_i)=(1-l)\delta(t_i)\end{aligned} \tag{6}$$

Since $0<l\le 1$ holds, one can easily get $\delta^+(t_i)\le\delta(t_i)$ in this case (Note that the equality mark holds only when $\delta(t_i)=0$ is true, meaning that the network is synchronized).

3) When the other $N-1$ oscillators' phases reside partially in $[0,\pi)$ and partially in $(\pi,2\pi]$, given $\phi_i(t_i)=2\pi$ *rad*, we represent the set of oscillators with phases in $[0,\pi)$

as $\mathscr{N}_1$ and the set of oscillators with phases in $(\pi, 2\pi]$ as $\mathscr{N}_2$. One can easily get $\mathscr{N}_1 \cup \mathscr{N}_2 = \mathscr{N}$ and $\mathscr{N}_1 \cap \mathscr{N}_2 = \emptyset$. The length of the containing arc at time instant t_i can be expressed as

$$\begin{aligned}\delta(t_i) =& 2\pi + \max_{k\in\mathscr{N}_1}\{\phi_k(t_i)\} - \min_{j\in\mathscr{N}_2, j\neq i}\{\phi_j(t_i)\} \\ =& 2\pi + \phi_{\bar{k}}(t_i) - \phi_{\underline{j}}(t_i) \end{aligned} \tag{7}$$

where $\underline{j} = \arg\min_{j\in\mathscr{N}_2, j\neq i}\phi_j(t_i)$ and $\bar{k} = \arg\max_{k\in\mathscr{N}_1}\phi_k(t_i)$. After the firing of oscillator i, we have $\phi_i^+(t_i) = 0$. Under the PRF in (2), we can get $\phi_k^+(t_i) = (1-l)\phi_k(t_i)$ for $k \in \mathscr{N}_1$ and $\phi_j^+(t_i) = \phi_j(t_i) + l(2\pi - \phi_j(t_i))$ for $j \in \mathscr{N}_2, j \neq i$. The length of the containing arc becomes

$$\begin{aligned}\delta^+(t_i) &= 2\pi + \max_{k\in\mathscr{N}_1}\{\phi_k^+(t_i)\} - \min_{j\in\mathscr{N}_2, j\neq i}\{\phi_j^+(t_i)\} \\ &= (1-l)(2\pi + \phi_{\bar{k}}(t_i) - \phi_{\underline{j}}(t_i)) \\ &= (1-l)\delta(t_i) \end{aligned} \tag{8}$$

Since $0 < l \leq 1$ holds, one can easily get $\delta^+(t_i) \leq \delta(t_i)$ in this case (Note that the equality mark holds only when $\delta(t_i) = 0$ is true, meaning that the network is synchronized).

Summarizing the above analysis, we can get that the length of the containing arc is non-increasing. In addition, if the firing of an oscillator triggers a jump on another oscillator, then the firing will reduce the length of the containing arc to $\delta^+(t) = (1-l)\delta(t)$.

Next, we proceed to prove that the length of the containing arc will decrease to 0. To this end, we first show that every oscillator will fire at least once within a certain time period. Without loss of generality, we set the initial time instant as $t_0 = 0$. Since the initial length of the containing arc is less than π *rad* and it is non-increasing, as analyzed earlier, there exists a time instant $t_1 > T$ at which all oscillators' phases reside in $(\pi, 2\pi]$. At this time instant, noting that the PRF in (2) is non-negative in $(\pi, 2\pi]$, we can get that exchanged pulses can only advance or have no effect on a receiving oscillator's phase. Therefore, all oscillators will reach phase 2π *rad* and fire within the time interval $[t_1, t_1 + T/2]$. On the other hand, since the PRF in (2) is non-positive in $[0, \pi]$, we can get that exchanged pulses can only delay or have no effect on a receiving oscillator's phase residing in $[0, \pi]$. So it takes at least $T/2$ time for an oscillator's phase to evolve from 0 to π *rad*. Therefore, no oscillator can surpass phase point π *rad* at time instant $t_1 + T/2$. In other words, each oscillator fired once within $[t_1, t_1 + T/2]$ and all oscillators' phases reside in $[0, \pi]$ at time instant $t_1 + T/2$.

Next, we proceed to prove that there exists at least one oscillator, whose firing can trigger jumps on all the other oscillators' phases within the time interval $[t_1, t_1 + T/2]$. Assume to the contrary that no oscillator's firing triggers a jump on any other oscillators within $[t_1, t_1 + T/2]$. So condition b) of Mechanism 1 cannot be satisfied, which means that no greater than λ oscillators fired in any quarter period within the time interval $[t_1, t_1 + T/2]$. Hence, no greater than λ oscillators fired in the time interval $[t_1, t_1 + T/4]$ and the same is true for the interval $[t_1 + T/4, t_1 + T/2]$. Therefore, no greater than $2\lambda < N$ oscillators fired within $[t_1, t_1 + T/2]$, which contradicts the fact that all oscillators fired once within $[t_1, t_1 + T/2]$. So we can conclude that there exists at least one firing event that triggers phase jumps on the other $N-1$ oscillators within $[t_1, t_1 + T/2]$.

Without loss of generality, we assume that oscillator i fires at $t_i \in [t_1, t_1 + T/2]$, which triggers phase jumps on all the other $N-1$ oscillators. Based on the above analysis, we have that the length of the containing arc is decreased by the firing of oscillator i when $\delta(t_i) \neq 0$.

At time instant $t_1 + T/2$, the phases of all oscillators reside in $[0, \pi]$ and they will evolve freely toward $(\pi, 2\pi]$. By repeating the above analyses, we can get that the length of the containing arc will be decreased by the firing of at least one oscillator in a firing round until it converges to 0. Therefore, synchronization of the network can be achieved. ■

Next, we show that the initial phase distribution requirement in Theorem 1 can be removed, i.e., under all-to-all topology, the new synchronization mechanism can guarantee synchronization even when the phases of oscillators are arbitrarily distributed in $[0, 2\pi]$.

Theorem 2: For an attack-free all-to-all network of N PCOs, if the initial phases of all oscillators are randomly distributed in $[0, 2\pi]$, then Mechanism 1 can achieve perfect synchronization as long as the coupling strength satisfies $l > 0.5$.

Proof: Without loss of generality, we set the initial time instant as $t_0 = 0$. First, we will show that in any time interval $[t_1, t_1 + T]$ with $t_1 > T$, there exists one firing event from some oscillator which can trigger phase jumps on all the other $N-1$ oscillators.

Assume to the contrary that no pulse can trigger a jump within $[t_1, t_1 + T]$. One can get that the phase distance between any two oscillators is invariant within $[t_1, t_1 + T]$. Then every oscillator will evolve freely with natural frequency ω for a full cycle and fire once during $[t_1, t_1 + T]$. In other words, N oscillators fired within the interval $[t_1, t_1 + T]$.

Under the assumption that no pulse can trigger a jump on any oscillator's phase within $[t_1, t_1 + T]$, we have that condition b) of Mechanism 1 cannot be satisfied, i.e., no greater than λ oscillators fired in any quarter oscillation period within the time interval $[t_1, t_1 + T]$. Hence, no greater than λ oscillators fired in the time interval $[t_1, t_1 + T/4]$ and the same is true for intervals $[t_1 + T/4, t_1 + T/2]$, $[t_1 + T/2, t_1 + 3T/4]$, and $[t_1 + 3T/4, t_1 + T]$. Therefore, no greater than $4\lambda < N$ oscillators fired within $[t_1, t_1 + T]$, which contradicts the assumption that N oscillators fired within $[t_1, t_1 + T]$. So at least one oscillator's firing will trigger all the other oscillators' phases to jump in $[t_1, t_1 + T]$.

We assume that oscillator $i's$ firing at $t_i \in [t_1, t_1 + T]$ triggers a jump on all the other $N-1$ oscillators. Denoting $\phi_k(t_i)$ as the phase of oscillator $k \in \mathscr{N} = \{1, 2, \cdots, N\}$ at time instant t_i, one can get $\phi_i^+(t_i) = 0$ and $\phi_k^+(t_i) = \phi_k(t_i) + F(\phi_k(t_i))$ for $k \in \mathscr{N}, k \neq i$. When $l > 0.5$ is true, the PRF in (2) leads to $\phi_k^+(t_i) \in (3\pi/2, 2\pi]$ for $\phi_k(t_i) \in (\pi, 2\pi]$ and $\phi_k^+(t_i) \in [0, \pi/2)$ for $\phi_k(t_i) \in [0, \pi]$. Hence, the phase of all oscillators reside in $(3\pi/2, 2\pi] \cup [0, \pi/2)$ and the length of the containing arc is less than π *rad*. Using Theorem 1, we have that all oscillators will synchronize. ■

IV. Stealthy Byzantine Attacks

The concept of Byzantine attacks stems from the Byzantine generals problem [36]. It is used to describe a traitor commander who sends or relays fake information to other commanders to avoid the loyal ones from reaching agreement [26]. In the case of PCO synchronization, Byzantine attacks are assumed to be able to compromise an oscillator and completely take over its behavior. So an oscillator compromised by Byzantine attacks will emit pulses at arbitrary time instants. Apparently, if an attacker keeps sending pulses continuously without rest, it can effectively prevent legitimate oscillators from reaching synchronization. However, such a manner of attacks will also render themselves easily detectable, just as jamming of communication channels being easy to detect, isolate, and remove [37]. Therefore, we are only interested in "stealthy" Byzantine attacks which cannot be detected by legitimate oscillators in the pulse based interaction framework.

In all-to-all PCO networks, since all exchanged pulses are identical with no embedded content such as source or destination information, conventional content-checking based attack-detection mechanisms such as [1] cannot be applied. We propose to let each node detect potential attacks by monitoring the number of pulses it receives within a certain time interval. The basic rationale is as follows: In a given time interval, if the number of received pulses is greater than the maximally possible number of pulses emitted by all legitimate oscillators, then it is safe to conclude that an attacker is present who injected the superfluous pulses. To this end, we first characterize the number of pulses that an oscillator can receive within a certain time interval:

Theorem 3: For an all-to-all network of N legitimate PCOs under Mechanism 1, one oscillator can receive at most $N-1$ pulses within any time interval $[t,t+T/2]$ for $t \geq 0$.

Proof: Without loss of generality, we assume that oscillator i emits a pulse and resets its phase to 0 at time instant t_1, i.e., $\phi_i(t_1) = 2\pi$ *rad* and $\phi_i^+(t_1) = 0$. Under Mechanism 1 and the PRF in (2), one can get that the phase evolution of oscillator i from 0 to π *rad* can only be decelerated (or unaffected) by received pulses. Hence, it takes oscillator i at least $T/2$ time to evolve from 0 to π *rad*, which, combined with the fact that a node cannot jump from π *rad* to 2π *rad* instantaneously (the value of PRF in (2) is $-\pi$ *rad* at phase π *rad*), further means that it takes oscillator i over $T/2$ to evolve from 0 to 2π *rad*. In other words, within any time interval $[t,t+T/2]$ for $t \geq 0$, oscillator i can emit at most one pulse. Therefore, an oscillator can emit at most one pulse during an arbitrary time interval $[t,t+T/2]$ for $t \geq 0$.

Based on the above analysis, we know that for an all-to-all network of N oscillators, at most N pulses can be emitted during an arbitrary time interval $[t,t+T/2]$ for $t \geq 0$. So an oscillator can receive at most $N-1$ pulses within an arbitrary time interval $[t,t+T/2]$ for $t \geq 0$. ■

Based on Theorem 3, we have, under the pulse number based detection mechanism, that any oscillator's receiving more than $N-1$ pulses within an arbitrary time interval $[t,t+T/2]$ implies the presence of attacks.

From the above analysis, the condition for mounting stealthy Byzantine attacks is given as follows:

Stealthy Byzantine Attack Model: For an all-to-all network of N PCOs under Mechanism 1, one compromised oscillator can launch stealthy Byzantine attacks as long as it injects pulses with a time separation of length over $T/2$.

Remark 3: In this paper, the detection mechanism only considers the minimal separation within which one oscillator can receive *at most* $N-1$ pulses (i.e., $T/2$) because it is extremely hard to find a tight maximal separation during which one oscillator can receive *at least* $N-1$ pulses. Another reason for not imposing a maximal separation is that in practice, pulse dropout is unavoidable, which makes it impossible to guarantee that each oscillator will receive at least $N-1$ pulses within a certain time interval.

V. Synchronization of All-to-All PCO Networks in the Presence of Stealthy Byzantine Attacks

In this section, we address the synchronization of PCO networks in the presence of stealthy Byzantine attacks. Among N PCOs, we assume that M are compromised and act as stealthy Byzantine attackers. Specifically, we will show that the proposed pulse based interaction mechanism can synchronize legitimate oscillators even in the presence of multiple stealthy Byzantine attackers. More interestingly, we can prove that legitimate oscillators can synchronize even when their initial phases are randomly distributed in the entire oscillation period $[0,2\pi]$. Similar to Lemma 1, we first establish the following property for PCO networks:

Lemma 2: For an all-to-all network of N PCOs among which M are compromised and act according to the stealthy Byzantine attack model in Sec IV, if the firing of an arbitrary oscillator (either legitimate or malicious) triggers a phase jump on a legitimate oscillator, then the firing can trigger phase jumps on all legitimate oscillators.

Proof: Noting that the topology of the network is all-to-all, one can get that an oscillator's pulse can be received by all the other oscillators. Hence, Lemma 2 can be acquired by following the same line of reasoning in Lemma 1. ■

Now we are in position to present the synchronization condition of all-to-all PCO networks in the presence attacks.

Theorem 4: For an all-to-all network of N PCOs among which M are compromised and act according to the stealthy Byzantine attack model in Sec IV, if the number of compromised oscillators M is no greater than $\lfloor (N-1)/5 \rfloor$ and the initial length of the containing arc is less than $\pi/2$ *rad*, then all legitimate oscillators can be perfectly synchronized under Mechanism 1.

Proof: We divide the proof into two parts. In part I, we will prove that the length of the containing arc of legitimate oscillators is non-increasing. In Part II, we prove that the length of the containing arc of legitimate oscillators will decrease to 0.

Part I (The length of the containing arc of legitimate oscillators is non-increasing): It can be easily inferred that the length of the containing arc of legitimate oscillators remains unchanged if no legitimate oscillator jumps in phase. So we only consider the case that an oscillator's firing (say oscillator i, either legitimate or malicious) triggers a jump on a legitimate

oscillator, say oscillator j where $j \neq i$. Based on Lemma 2, if the firing of oscillator i triggers a phase jump on a legitimate oscillator j, it will trigger phase jumps on all legitimate oscillators.

We assume that oscillator $i's$ firing time instant is t_i. Since oscillator i can be a legitimate oscillator or an attacker, we have to show that in neither case will the length of the containing arc of legitimate oscillators increase.

Case 1: Oscillator i is legitimate.

When oscillator i is legitimate, we have $\phi_i(t_i) = 2\pi$ *rad*, i.e., the containing arc of legitimate oscillators includes point 2π *rad* at time instant t_i. Since the number of legitimate oscillators is $N-M$ and the length of the containing arc of legitimate oscillators is less than $\pi/2$ *rad*, the phases of the other $N-M-1$ legitimate oscillators can only be distributed in the following three ways at time instant t_i, as depicted in Fig. 4:

1) all the other $N-M-1$ legitimate oscillators' phases reside in $(3\pi/2, 2\pi]$;
2) all the other $N-M-1$ legitimate oscillators' phases reside in $[0, \pi/2)$;
3) the other $N-M-1$ legitimate oscillators' phases reside partially in $[0, \pi/2)$ and partially in $(3\pi/2, 2\pi]$.

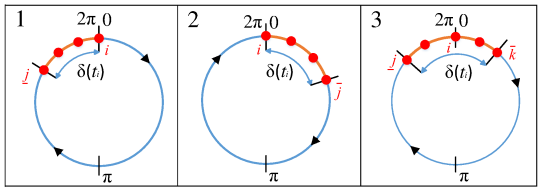

Figure 4: Three possible phase distribution of all legitimate oscillators when legitimate oscillator i fires at time instant t_i.

Denoting $\delta(t_i)$ as the length of the containing arc of legitimate oscillators at time instant t_i, one can easily obtain $\delta^+(t_i) \leq \delta(t_i)$ in all above three cases by following the same line of reasoning in Theorem 1. Hence, we can get that the firing of a legitimate oscillator cannot increase the length of the containing arc of legitimate oscillators.

Case 2: Oscillator i is a stealthy Byzantine attacker.

According to Mechanism 1, upon receiving a pulse, legitimate oscillator j will jump in phase when it either fired and received at least $\lambda - 1$ pulses in the past quarter period, or it did not fire but received at least λ pulses in the past quarter period. In both cases, it can be inferred that at least λ oscillators fired in the quarter period immediately prior to t_i.

Under the assumption that the number of compromised oscillators satisfies $M \leq \lambda$, we can get that at most $M-1$ attack pulses can be emitted in the quarter period prior to t_i. Because $M-1 \leq \lambda - 1$ is true and at least λ pulses are emitted in the past quarter period, one can obtain that at least one legitimate oscillator fired in the quarter period immediately prior to t_i.

Since the PRF in (2) is non-positive in $[0, \pi/2]$, we can get that exchanged pulses can only delay or have no effect on a receiving legitimate oscillator whose phase resides in $[0, \pi/2]$. So it takes at least $T/4$ time for a legitimate oscillator to evolve from 0 to $\pi/2$ *rad*. Hence, at least one legitimate oscillator (who fired in the past quarter period) has phase residing in $[0, \pi/2]$ at time instant t_i. Since the length of the containing arc of legitimate oscillators is less than $\pi/2$ *rad*, the phases of all $N-M$ legitimate oscillators can only be distributed in the following two ways at t_i, as depicted in Fig. 5:

1) all $N-M$ legitimate oscillators reside in $[0, \pi)$, wherein at least one legitimate oscillator resides in $[0, \pi/2]$;
2) the $N-M$ legitimate oscillators reside partially in $[0, \pi/2]$ and partially in $(3\pi/2, 2\pi]$.

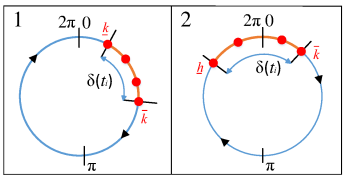

Figure 5: Two possible phase distribution of all legitimate oscillators when compromised oscillator i fires at time instant t_i.

Denoting $\delta(t_i)$ as the length of the containing arc of legitimate oscillators at time instant t_i, next we show that $\delta(t_i)$ cannot be increased by the firing of oscillator i in both scenarios, i.e., $\delta^+(t_i) \leq \delta(t_i)$ always holds.

1) When the phases of all $N-M$ legitimate oscillators reside in $[0, \pi)$ at time instant t_i, the length of the containing arc can be described by

$$\begin{aligned} \delta(t_i) &= \max_{k \in \mathcal{N}_3} \{\phi_k(t_i)\} - \min_{k \in \mathcal{N}_3} \{\phi_k(t_i)\} \\ &= \phi_{\bar{k}}(t_i) - \phi_{\underline{k}}(t_i) \end{aligned} \tag{9}$$

where $\mathcal{N}_3$ is the index set of all legitimate oscillators, $\underline{k} = \arg\min_{k \in \mathcal{N}_3} \phi_k(t_i)$ and $\bar{k} = \arg\max_{k \in \mathcal{N}_3} \phi_k(t_i)$. After the firing of oscillator i, one can get $\phi_k^+(t_i) = (1-l)\phi_k(t_i)$ for $k \in \mathcal{N}_3$. Hence, the length of the containing arc of legitimate oscillators becomes

$$\begin{aligned} \delta^+(t_i) &= \max_{k \in \mathcal{N}_3} \{\phi_k^+(t_i)\} - \min_{k \in \mathcal{N}_3} \{\phi_k^+(t_i)\} \\ &= \phi_{\bar{k}}^+(t_i) - \phi_{\underline{k}}^+(t_i) = (1-l)(\phi_{\bar{k}}(t_i) - \phi_{\underline{k}}(t_i)) \\ &= (1-l)\delta(t_i) \end{aligned} \tag{10}$$

Sine $0 < l \leq 1$ holds, one can get $\delta^+(t_i) < \delta(t_i)$ whenever $\delta(t_i)$ is nonzero.

2) When the $N-M$ legitimate oscillators reside partially in $[0, \pi/2]$ and partially in $(3\pi/2, 2\pi]$, we denote $\mathcal{N}_4$ as the set of legitimate oscillators with phases in $[0, \pi/2]$ and $\mathcal{N}_5$ as the set of legitimate oscillators with phases in $(3\pi/2, 2\pi]$. Then the length of the containing arc of legitimate oscillators at time instant t_i can be described by

$$\begin{aligned} \delta(t_i) &= 2\pi + \max_{k \in \mathcal{N}_4} \{\phi_k(t_i)\} - \min_{h \in \mathcal{N}_5} \{\phi_h(t_i)\} \\ &= 2\pi + \phi_{\bar{k}}(t_i) - \phi_{\underline{h}}(t_i) \end{aligned} \tag{11}$$

where $\bar{k} = \arg\max_{k \in \mathcal{N}_4} \phi_k(t_i)$ and $\underline{h} = \arg\min_{h \in \mathcal{N}_5} \phi_h(t_i)$. After the firing of oscillator i, one can get $\phi_k^+(t_i) = (1-l)\phi_k(t_i)$ for $k \in \mathcal{N}_4$ and $\phi_h^+(t_i) = \phi_h(t_i) + l(2\pi - \phi_h(t_i))$

for $h \in \mathcal{N}_5$. Hence, the length of the containing arc of legitimate oscillators becomes

$$\begin{aligned}\delta^+(t_i) &= 2\pi + \max_{k\in\mathcal{N}_4}\{\phi_k^+(t_i)\} - \min_{h\in\mathcal{N}_5}\{\phi_h^+(t_i)\} \\ &= 2\pi + \phi_{\bar{k}}^+(t_i) - \phi_{\underline{h}}^+(t_i) \\ &= (1-l)(2\pi + \phi_{\bar{k}}(t_i) - \phi_{\underline{h}}(t_i)) \\ &= (1-l)\delta(t_i) \end{aligned} \tag{12}$$

Sine $0 < l \leq 1$ holds, one can get $\delta^+(t_i) < \delta(t_i)$ whenever $\delta(t_i)$ is nonzero.

In conclusion, the length of the containing arc of legitimate oscillators is non-increasing. In addition, if the firing of an oscillator triggers a jump on a legitimate oscillator, then the firing will reduce the length of the containing arc of legitimate oscillators to $\delta^+(t_i) = (1-l)\delta(t_i)$.

Part II (The length of the containing arc of legitimate oscillators will decrease to 0): To prove that the length of the containing arc of legitimate oscillators will keep decreasing, we only need to show that pulses which trigger phase jumps on legitimate oscillators will keep occurring until the length of the containing arc of legitimate oscillators reaches zero. Because if none of legitimate oscillators' phases are trapped in some sub-interval within $[0, 2\pi]$, then all legitimate oscillators will keep firing repeatedly within one quarter period interval from each other (note that as proven before, the containing arc of legitimate oscillators is non-increasing and hence is always less than $\pi/2$ *rad*). Given that the number of legitimate oscillators is $N - M > \lambda$, it can be easily inferred that at least the firing of one legitimate oscillator will trigger a phase jump according to Mechanism 1 in Sec. II. Therefore, to prove that the length of the containing arc of legitimate oscillators will decrease to zero, it is sufficient to show that no legitimate oscillator will stop from firing.

Given that once the phase of a legitimate oscillator surpasses π *rad*, it cannot be stopped from firing (because its phase can only be advanced under the PRF in (2)). Further taking into account the fact that pulses from stealthy attackers alone (no greater than λ) are not enough to trigger any phase shift according to Mechanism 1 in Sec. II, we have that at least one legitimate oscillator can fire repeatedly (Note that if no phase jumps are triggered, then legitimate oscillators will evolve freely and fire periodically).

Next, we proceed to prove that if one legitimate oscillator can fire, i.e., can evolve into the interval $(\pi, 2\pi]$, then all legitimate oscillators can evolve into $(\pi, 2\pi]$. Without loss of generality, we assume that the legitimate oscillator which can fire surpasses phase π *rad* at time instant t_i. Given that the length of the containing arc of legitimate oscillators is always strictly less than $\pi/2$ *rad*, as proven before, we have that at time instant t_i, all legitimate oscillators have phases residing in $(\pi/2, 3\pi/2)$.

Noting that the phase of a legitimate oscillator having phase in $[0, \pi]$ can only be delayed (or unaffected) by received pulses, it can be easily inferred that after the most recent firing from legitimate oscillators, it took all legitimate oscillators at least $T/4$ to evolve to the current phase in $(\pi/2, 3\pi/2)$, during which no legitimate oscillators sent any pulse. Therefore, starting from t_i, attack pulses will not affect the phase of legitimate oscillators until at least one legitimate oscillator reaches 2π *rad* to fire, which takes at least $T/4$. So after the at least $T/4$ time of free evolution, the phases of legitimate oscillators become residing in $(\pi, 2\pi]$, which means that all legitimate oscillators will fire.

Therefore, we can conclude that the length of the containing arc of legitimate oscillators will keep decreasing until it reaches 0, i.e., the achievement of synchronization of legitimate oscillators. ■

Next, we show that the initial phase distribution requirement in Theorem 4 can be removed, i.e., Mechanism 1 can guarantee synchronization in the presence of attacks even when all legitimate oscillators' initial phases are arbitrarily distributed in $[0, 2\pi]$.

Theorem 5: For an all-to-all network of N PCOs, within which M oscillators are compromised and act as stealthy Byzantine attackers, if the number of compromised oscillators M is no greater than $\lfloor (N-1)/5 \rfloor$, then all legitimate oscillators can be perfectly synchronized under Mechanism 1 from any initial phase distribution when the coupling strength satisfies $l > 0.75$.

Proof: Without loss of generality, we set the initial time instant to $t_0 = 0$. Similar to the proof of Theorem 2, we first show that for any time interval $[t_1, t_1 + T]$ with $t_1 > T$, there exists one firing event which can trigger a phase jump on a legitimate oscillator.

Assume to the contrary that no pulse can trigger a phase jump on a legitimate oscillator within $[t_1, t_1 + T]$. One can get that the phase distance between any two legitimate oscillators is invariant within $[t_1, t_1 + T]$. Since T is the natural period, every legitimate oscillator will evolve freely for a full cycle on the unit circle and fire once during $[t_1, t_1 + T]$. In other words, $N - M$ legitimate oscillators fired within $[t_1, t_1 + T]$. On the other hand, under the stealthy Byzantine attack model in Sec. IV, every attacker can fire at most twice during $[t_1, t_1 + T]$. Hence, at least $N - M$ oscillators fired during $[t_1, t_1 + T]$.

Under the assumption that no pulse can trigger a jump on any legitimate oscillator within $[t_1, t_1 + T]$, we have that condition b) of Mechanism 1 cannot be satisfied, i.e., no greater than λ oscillators fired in any quarter oscillation period within the time interval $[t_1, t_1 + T]$. Hence, no greater than λ oscillators fired in the time interval $[t_1, t_1 + T/4]$ and the same is true for intervals $[t_1 + T/4, t_1 + T/2]$, $[t_1 + T/2, t_1 + 3T/4]$, and $[t_1 + 3T/4, t_1 + T]$. Therefore, no greater than 4λ oscillators fired within $[t_1, t_1 + T]$ and one can easily get

$$4\lambda < N - M \tag{13}$$

which contradicts the assumption that at least $N - M$ oscillators fired within $[t_1, t_1 + T]$. Therefore, at least one oscillator's firing can trigger a phase jump on a legitimate oscillator within $[t_1, t_1 + T]$. Based on Lemma 2, we further know that the pulse will trigger phase jumps on all legitimate oscillators.

Denoting $\phi_k(t_i)$ as the phase of a legitimate oscillator jumps in phase at time instant t_i, one can get $\phi_k^+(t_i) = \phi_k(t_i) + F(\phi_k(t_i))$. When $l > 0.75$ is true, phase shift under PRF in (2) leads to $\phi_k^+(t_i) \in (7\pi/4, 2\pi]$ for $\phi_k(t_i) \in (\pi, 2\pi]$ and $\phi_k^+(t_i) \in [0, \pi/4)$ for $\phi_k(t_i) \in [0, \pi]$. Hence, the phase of

all legitimate oscillators will reside in $(7\pi/4, 2\pi] \cup [0, \pi/4)$ after this firing event and the length of the containing arc will become less than $\pi/2$ *rad*. Using Theorem 4, we have that all oscillators will synchronize despite the presence of attackers. ■

Remark 4: The proof above also contains the reason for us to set λ to $\lfloor (N-1)/5 \rfloor$ in Mechanism 1: Our key idea for attack resilience is to avoid attack pulses alone from being able to trigger phase jumps on legitimate oscillators, so we have to choose λ that is no less than M, the number of attackers. Further taking into consideration of (13), which is necessary to guarantee global synchronization, we can have $\lambda < N/5$. Therefore, we set $\lambda = \lfloor (N-1)/5 \rfloor$, the maximal integer satisfying $\lambda < N/5$, to make the Mechanism be able to tolerate more attackers.

Remark 5: It is worth noting that existing resilient pulse-based synchronization approaches in [33] and [34] cannot guarantee perfect synchronization for all-to-all PCO networks under the considered stealthy Byzantine attackers even when the coupling strength is larger than 0.5, as illustrated by the numerical simulations in Fig. 10 and Fig. 11. Hence, our synchronization approach is highly non-trivial and more resilient in enabling PCO synchronization in the presence of such attackers.

Next, we analyze the convergence speed of Mechanism 1. From the proof of Theorem 4 and Theorem 5, we know that the speed at which the containing arc of legitimate oscillators decreases to zero is proportional to the number of effective pulses (i.e., pulses which can trigger jumps on all legitimate oscillators' phases) and the magnitude of phase jumps. Hence we have the following results on the convergence speed of Mechanism 1:

Theorem 6: Under the synchronization conditions in Theorem 5, the time to synchronization of all legitimate oscillators under Mechanism 1 is propositional to

$$\frac{\lambda}{l(N-M)} \tag{14}$$

Proof: According to the proof of Theorem 4 and Theorem 5, we know that the speed at which the containing arc of legitimate oscillators decreases to zero is proportional to the number of effective pulses (i.e., pulses which can trigger jumps on all legitimate oscillators' phases) and the magnitude of phase jumps. One can easily get that the number of effective pulses is proportional to the number of legitimate oscillators, i.e., $N-M$, but inversely proportional to λ, and the magnitude of phase jumps is proportional to the coupling strength l under a given phase response function. Therefore, we can get that the time to synchronization is proportional to (14). ■

Remark 6: From Theorem 6, and the synchronization derivations in Theorem 5, we can get that if λ were to allowed to be chosen from $\{1, 2, ..., \lfloor (N-1)/5 \rfloor\}$ and is no less than the number of attackers in the network, then synchronization can also be achieved. Furthermore, combining Theorem 6 (which indicates that a larger λ reduces synchronization speed) and Remark 4 (which implies that a larger λ leads to resilience to more stealthy attackers), we have that a trade-off exists between resilience to attackers and synchronization speed if λ in Mechanism 1 were allowed to be chosen from $\{1, 2, ..., \lfloor (N-1)/5 \rfloor\}$. In this paper, we set λ to $\lfloor (N-1)/5 \rfloor$ to guarantee resilience to more attackers.

VI. Extension to the Case where N is Unknown

In this section, we extend our approach to the case where the total number of oscillators, i.e., N, is unknown to individual oscillators. In this case, the exact number of compromised oscillators that a network can tolerate, i.e., λ in Mechanism 1, cannot be determined precisely by each individual oscillator. As the implementation of Mechanism 1 requires the knowledge of λ, we have to revise it to accommodate the fact that λ is unavailable. Based on the observation that under the stealthy attacker model in Sec. IV, each oscillator can use the number of received pulses to estimate the number of oscillators in a network, we revise Mechanism 1 to make it applicable to cases where N is unknown to individual oscillators. More specifically, we will prove that the revised mechanism can still guarantee global synchronization in the presence of compromised oscillators as long as their number is no larger than 10% of the total number of oscillators in the network.

The same as Mechanism 1, we allow each oscillator to evolve freely for the first oscillation period $[0, T]$. So each oscillator's phase will reach 2π *rad* at a certain time instant within $[0, T]$ upon which the oscillator will emit a pulse. Note that when the network is all-to-all, every oscillator will receive the same number of pulses. Based on the number of received pulses in the first oscillation period $[0, T]$, we propose the following mechanism:

New pulse based interaction approach (Mechanism 2):

---

1) The phase ϕ_i of oscillator i evolves from 0 to 2π *rad* with a constant speed $\omega = 1 rad/second$.
2) Once ϕ_i reaches 2π *rad*, oscillator i fires (emits a pulse) and resets its phase to 0.
3) In the first oscillation period $[0, T]$, each oscillator i counts the number of received pulses, and stores this number as P_i.
4) When oscillator i receives a pulse at time instant t, it shifts its phase according to (1) only when both of the following conditions are satisfied:
   a) an entire period T has elapsed since initiation;
   b) in the past quarter period, oscillator i fired and received at least $\lfloor (P_i - 1)/5.5 \rfloor - 1$ pulses, or oscillator i did not fire but received at least $\lfloor (P_i - 1)/5.5 \rfloor$ pulses within this past quarter period, where $\lfloor \bullet \rfloor$ means the largest integer no greater than "$\bullet$."

   Otherwise, the pulse has no effect on $\phi_i(t)$.

Next, we show that Mechanism 2 can guarantee synchronization even when the total number of oscillators, i.e., N, is unknown to individual oscillators. Under the assumption that the portion of compromised oscillators is no larger than 10%, we first give a condition for local synchronization, i.e., synchronization when the initial phases of legitimate

oscillators are constrained in a certain range, then we prove that when the coupling strength is over 0.75, the network can synchronize from an arbitrary initial phase distribution.

Theorem 7: For an all-to-all PCO network of N oscillators where no more than 10% of all oscillators are compromised and act as stealthy Byzantine attackers, if the initial length of the containing arc of all legitimate oscillators is less than $\pi/2$ *rad*, even with N completely unknown to individual oscillators, all legitimate oscillators can be perfectly synchronized under Mechanism 2.

Proof: Under Mechanism 2, no pulse will trigger a jump on any legitimate oscillator's phase within the first oscillation period $[0,T]$. So every legitimate oscillator will evolve freely for a full cycle, i.e., every legitimate oscillator will fire once within the first oscillation period. In the meantime, according to the stealthy Byzantine attack model in Sec. IV, every stealthy Byzantine attacker can emit at most two pulses within the first oscillation period $[0,T]$. Further more, under all-to-all connection, the number of pulses each legitimate oscillator receives within the first oscillation period, i.e., P_i, is identical.

The proof follows the same line of reasoning as Theorem 4. More specifically, using a same argument as Part I of the proof of Theorem 4, we can obtain that if the number of attackers in the network is no larger than the $\lfloor (P_i-1)/5.5 \rfloor$ in step 4). *b*) in Mechanism 2, then a pulse from neither a legitimate oscillator nor a stealthy Byzantine attacker could expand the containing arc of legitimate oscillators, i.e., the length of the containing arc is non-increasing. Moreover, following the same argument in Part II of the proof of Theorem 4, we know that if $\lfloor (P_i-1)/5.5 \rfloor \leq \lfloor (N-1)/5 \rfloor = \lambda$ holds, then at least the firing of one legitimate oscillator will reduce the length of the containing arc of legitimate oscillators and no legitimate oscillator will stop from firing until synchronization is achieved. Therefore, to prove that synchronization of legitimate oscillators will be achieved, it suffices to show $\lfloor 0.1N \rfloor \leq \lfloor (P_i-1)/5.5 \rfloor \leq \lfloor (N-1)/5 \rfloor$ is true, where $\lfloor 0.1N \rfloor$ is the maximal number of attackers in the network and $\lfloor \bullet \rfloor$ denotes the largest integer no greater than "$\bullet$."

Based on the assumption that the portion of compromised oscillators is no larger than 10% and every stealthy Byzantine attacker can emit at most two pulses within the first oscillation period $[0,T]$, we have the following relationship:

$$N-1-\lfloor 0.1N \rfloor \leq P_i \leq N-1+\lfloor 0.1N \rfloor \tag{15}$$

Noticing $\lfloor 0.1N \rfloor \leq 0.1N$, we further have

$$\begin{aligned} & N-1-0.1N \leq P_i \leq N-1+0.1N \\ \Rightarrow & 0.9N-2 \leq P_i-1 \leq N-1+0.1(N-1) \\ \Rightarrow & (0.9N-2)/5.5 \leq (P_i-1)/5.5 \leq (N-1)/5 \\ \Rightarrow & \lfloor (0.9N-2)/5.5 \rfloor \leq \lfloor (P_i-1)/5.5 \rfloor \leq \lfloor (N-1)/5 \rfloor \end{aligned} \tag{16}$$

One can easily get $\lfloor 0.1N \rfloor \leq \lfloor (0.9N-2)/5.5 \rfloor$ for $N \geq 3$. (Note that under the attacker less than 10% assumption, the network will contain no attackers when $N < 3$ and hence every oscillator can use P_i to precisely estimate the number of oscillators in the network and achieve synchronization according to Theorem 1.) Substituting the above inequality into (16) lead to

$$\lfloor 0.1N \rfloor \leq \lfloor (P_i-1)/5.5 \rfloor \leq \lfloor (N-1)/5 \rfloor = \lambda$$

for $N \geq 3$. Therefore, we can get that all legitimate oscillators can be perfectly synchronized under Mechanism 2. ■

Next, we show that the initial phase distribution requirement in Theorem 7 can be removed, i.e., Mechanism 2 can guarantee synchronization in the presence of stealthy Byzantine attacks even when all legitimate oscillators' initial phases are arbitrarily distributed in $[0,2\pi]$.

Theorem 8: For an all-to-all PCO network of N oscillators where no more than 10% of all oscillators are compromised and act as stealthy Byzantine attackers, even with N completely unknown to individual oscillators, all legitimate oscillators can be perfectly synchronized under Mechanism 2 from any initial phase distribution as long as the coupling strength satisfies $l > 0.75$.

Proof: Proof of Theorem 8 can be obtained following Theorem 5 and Theorem 7 and is omitted. ■

Remark 7: It is worth noting that the maximally allowable number of attackers in a PCO network is $\lfloor 0.1N \rfloor$ when the network size N is unknown, which is less than the maximally allowable number of composed oscillators $\lambda = \lfloor (N-1)/5 \rfloor$ when the network size N is known. This reduction of maximally allowable compromised oscillators is consistent with our intuition that less knowledge of a PCO network reduces the capability of attack-resilient synchronization design.

Next, similar to Theorem 6, we present the convergence speed of Mechanism 2 where N is unknown to individual oscillators:

Theorem 9: Under the synchronization conditions in Theorem 8, the time to synchronization of all legitimate oscillators under Mechanism 2 is propositional to

$$\frac{\lfloor (P_i-1)/5.5 \rfloor}{l(N-\lfloor 0.1N \rfloor)} \tag{17}$$

Proof: Proof of Theorem 9 can be obtained following the argument in Theorem 6 and is omitted. ■

VII. Simulations

A. Attack-Free Case

We first considered the situation without attackers. We simulated an all-to-all network of 11 PCOs under Mechanism 1. The initial time was set to $t_0 = 0$ and the phases of oscillators were randomly chosen from $[0,\pi)$. Hence, the initial length of the containing arc satisfied $\delta(t_0) < \pi$. According to Theorem 1, the network will synchronize. This was confirmed by numerical simulations in Fig. 6, which showed that the length of the containing arc converged to zero.

To verify Theorem 2, we randomly distributed the initial phases across the entire oscillation period $[0,2\pi]$ and simulated the network under coupling strength $l = 0.51$. The evolution of the containing arc was presented in Fig. 7, which confirmed that Mechanism 1 can achieve synchronization even when the initial phases are randomly distributed in the entire phase space $[0,2\pi]$.

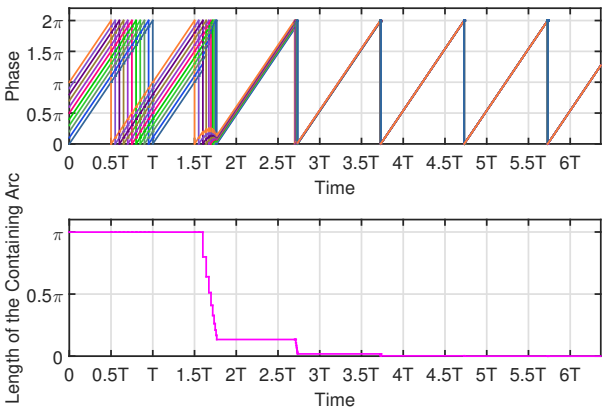

Figure 6: Phase evolution and the length of the containing arc of 11 PCOs under Mechanism 1 in the absence of attacks. The initial phases of all oscillators were randomly chosen from $[0,\pi)$. The coupling strength was set to $l = 0.2$.

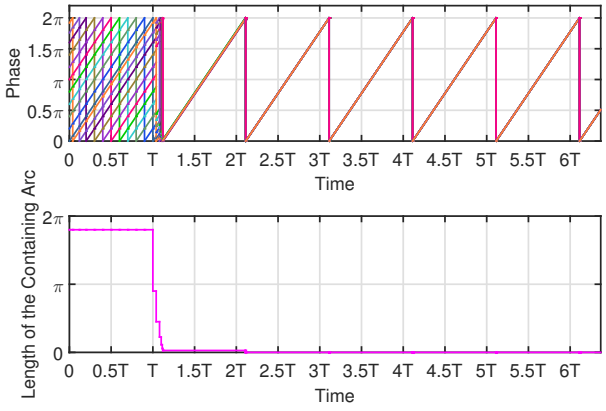

Figure 7: Phase evolution and the length of the containing arc of 11 PCOs under Mechanism 1 in the absence of attacks. The initial phases of all oscillators were randomly chosen from $[0,2\pi]$. The coupling strength was set to $l = 0.51$.

B. In the Presence of Stealthy Byzantine Attacks

Using the same network, we ran simulations in the presence of stealthy Byzantine attacks. We assumed that 2 of the 11 oscillators were compromised and acted as stealthy Byzantine attackers. The initial time was set to $t_0 = 0$ and the initial phases of the 9 legitimate oscillators were randomly distributed in $[0,\pi/2)$. Hence, the initial length of the containing arc was less than $\pi/2$ *rad*.

The phase evolution of the 9 legitimate oscillators under Mechanism 1 is given in Fig. 8 (b) and Fig. 9 (b), with the firing time instants of attackers denoted by asterisks on the x-axis. The results confirmed that Mechanism 1 is resilient to stealthy attacks. However, conventional pulse base synchronization approaches in [33] and [34] failed to achieve synchronization, as illustrated in Fig. 8 (a) and Fig. 9 (a), respectively, which confirmed the advantages of the new mechanism.

Theorem 5 indicates that Mechanism 1 can achieve synchro-

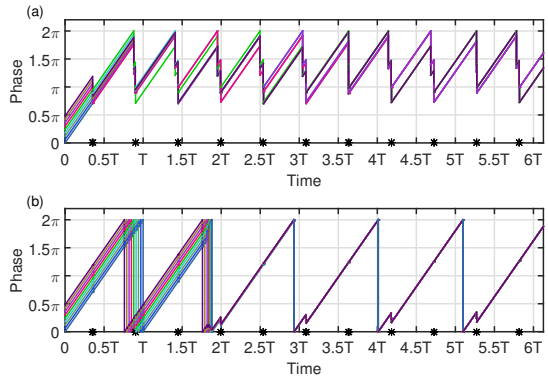

Figure 8: Phase evolutions of an all-to-all network of 11 PCOs, two of which are compromised with firing time instants represented by asterisks. Plot (a) and (b) present the phase evolutions of the 9 legitimate oscillators under the conventional pulse based interaction mechanism in [33] and Mechanism 1, respectively. The coupling strength was set to $l = 0.3$.

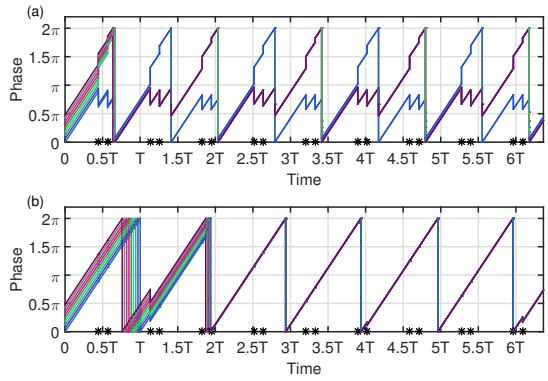

Figure 9: Phase evolutions of an all-to-all network of 11 PCOs, two of which are compromised with firing time instants represented by asterisks. Plot (a) and (b) present the phase evolutions of the 9 legitimate oscillators under the conventional pulse based interaction mechanism in [34] and Mechanism 1, respectively. The coupling strength was set to $l = 0.3$.

nization in the presence of stealthy Byzantine attacks even when the initial phase distribution is not restricted, i.e., the phases are randomly distributed in $[0,2\pi]$. To verify Theorem 5, we set $l = 0.76$ and simulated the network. Results in Fig. 10 (b) and Fig. 11 (b) confirmed Theorem 5. Phase evolution under the same condition was also simulated under the conventional pulse based synchronization approaches in [33] and [34], respectively. The results in Fig. 10 (a) and Fig. 11 (a) showed that neither of the conventional approaches can achieve synchronization, which further confirmed the advantages of Mechanism 1.

We also ran simulations when the network size was unknown to individual oscillators. For an all-to-all network of 20 oscillators, we assumed that two were compromised and acted as stealthy Byzantine attackers. The initial time was set

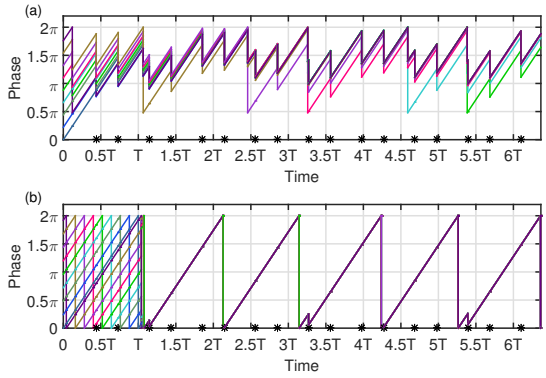

Figure 10: Phase evolutions of an all-to-all network of 11 PCOs, two of which are compromised with firing time instants represented by asterisks. Plot (a) and (b) present the phase evolutions of the 9 legitimate oscillators under the conventional pulse based interaction mechanism in [33] and Mechanism 1, respectively. The coupling strength was set to $l = 0.76$.

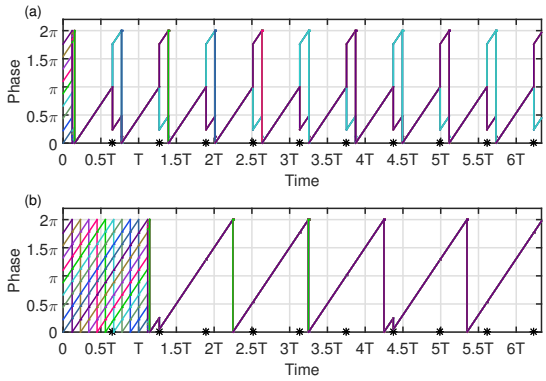

Figure 11: Phase evolutions of an all-to-all network of 11 PCOs, two of which are compromised with firing time instants represented by asterisks. Plot (a) and (b) present the phase evolutions of the 9 legitimate oscillators under the conventional pulse based interaction mechanism in [34] and Mechanism 1, respectively. The coupling strength was set to $l = 0.76$.

to $t_0 = 0$ and the initial phases of the legitimates oscillators were randomly distributed in $[0, \pi/2)$. Hence, the initial length of the containing arc is less than $\pi/2$. According to Theorem 7, all legitimate oscillators will synchronize. This was confirmed by numerical simulations in Fig. 12 (a), which showed that Mechanism 2 was resilient to stealthy Byzantine attacks even when the number of oscillators is unknown to individual oscillators.

Moreover, with the total number of oscillators N is unknown to individual oscillators, Theorem 8 indicates that Mechanism 2 can achieve synchronization in the presence of stealthy Byzantine attacks even when the phases of legitimate oscillators are randomly distributed in $[0, 2\pi]$. Results in Fig. 12 (b) confirmed Theorem 8.

We also numerically compared the attack-resilience and the

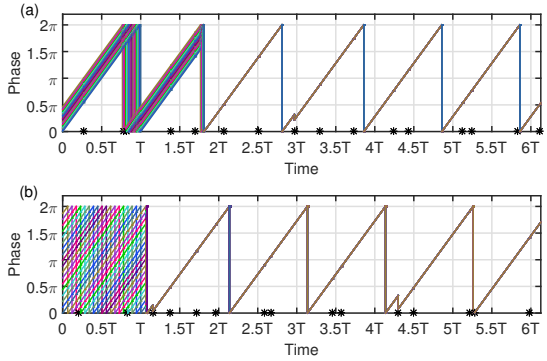

Figure 12: Phase evolutions of an all-to-all network of 20 PCOs, two of which are compromised with firing time instants represented by asterisks. The network size is unknown to individual oscillators. Plot (a) shows the phase evolutions of the 18 legitimate oscillators under Mechanism 2 with coupling strength $l = 0.3$ and the phases of all legitimate oscillators distributing randomly within $[0, \pi/2)$. Plot (b) shows the phase evolutions of the 18 legitimate oscillators under Mechanism 2 with coupling strength $l = 0.76$ and the phases of all legitimate oscillators distributing randomly within $[0, 2\pi]$.

convergence speed of Mechanism 1 if λ were allowed to be chosen from $1, 2, ..., \lfloor (N-1)/5 \rfloor$. We considered all-to-all PCO networks within which zero/one/two/three oscillator(s) were compromised and λ was set to 1, 2, and 3, respectively. The initial phases of legitimate oscillators were randomly chosen from $[0, 2\pi]$ and the coupling strength was set to $l = 0.76$. Synchronization was defined to be achieved when the length of the containing arc became and remained less than 1×10^{-6}. The mean synchronization probabilities and times to synchronization of $10,000$ runs under random attackers were shown in Fig. 13 and Fig. 14 (when 100% synchronization is not achieved, only synchronized runs were considered in the time-to-synchronization statistics). It can be seen that when $M \leq \lambda$ holds, synchronization of legitimate oscillators can be guaranteed and a larger λ renders a longer synchronization time; when $M > \lambda$ holds, a larger λ leads to a higher synchronization probability but a lower convergence speed. Similar simulation results were obtained for Mechanism 2 but omitted here due to space limits.

We also numerically compared the performance of Mechanisms 1 and 2 with the mechanisms in [33] and [34] under random attacks, which was addressed in [33]. Random attackers inject pulses randomly in their own pace irrespective of legitimate oscillators' phases. Note that random attacks may not be stealthy. The initial phases of legitimate oscillators were randomly chosen from $[0, 2\pi]$ and the coupling strength was set to $l = 0.3$. The attacker(s) sent pulses with a random period uniformly distributed in $[T/4,\ 9T/4]$. Synchronization was defined to be achieved when the length of the containing arc became and remained less than 1×10^{-6}. In the presence of one attacker, the synchronization probabilities under Mechanism 1, Mechanism 2 and the approaches in [33] and [34] were given by the red curves in Fig. 15 and Fig. 16,

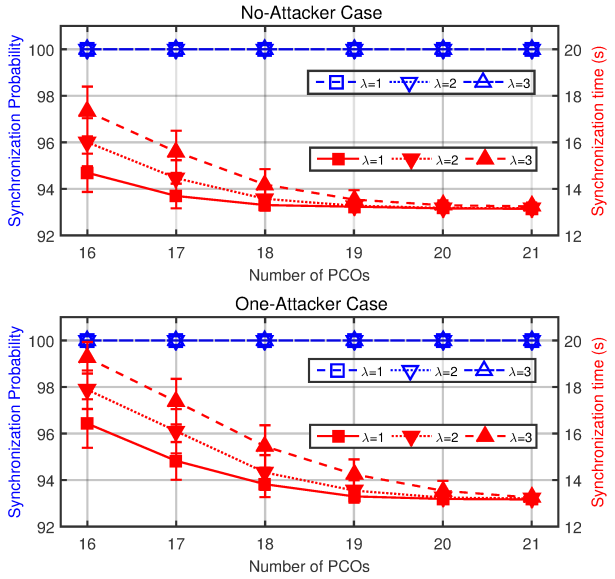

Figure 13: Comparison of synchronization probability and synchronization time under Mechanism 1 when λ was set to 1, 2, and 3 in the presence of 0 or 1 attacker. The initial phases of legitimate oscillators were randomly chosen from $[0, 2\pi]$ and the coupling strength was set to $l = 0.76$. Synchronization of the network was defined to be achieved when the length of the containing arc became and remained less than 1×10^{-6}.

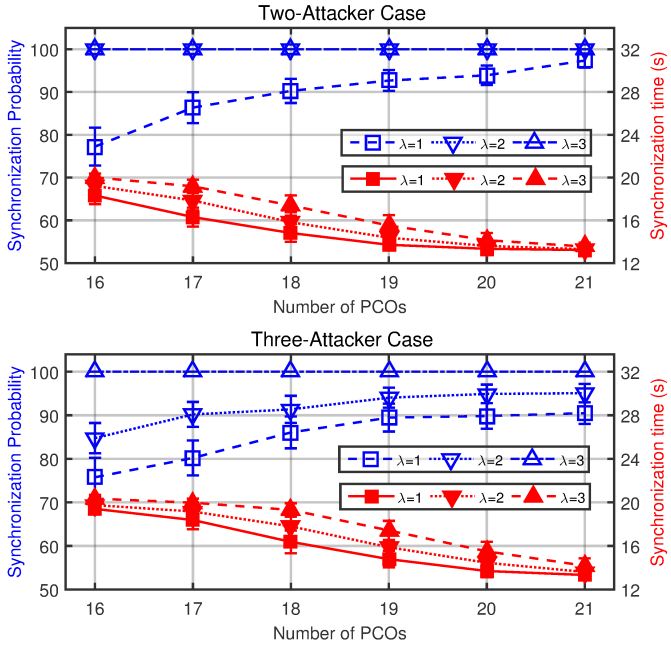

Figure 14: Comparison of synchronization probability and synchronization time under Mechanism 1 when λ was set to 1, 2, and 3 in the presence of 2 or 3 attackers. The initial phases of legitimate oscillators were randomly chosen from $[0, 2\pi]$ and the coupling strength was set to $l = 0.76$. Synchronization of the network was defined to be achieved when the length of the containing arc became and remained less than 1×10^{-6}.

respectively. It can be seen that Mechanism 1 and 2 are more robust in enabling synchronization in the presence of random attacks. However, they render a longer synchronization time when compared with the conventional pulse based interaction mechanism in [34], as illustrated by the blue curves in Fig. 15 and Fig. 16. Similar conclusions were obtained for the two-attacker case, as illustrated in Fig. 17 and Fig. 18.

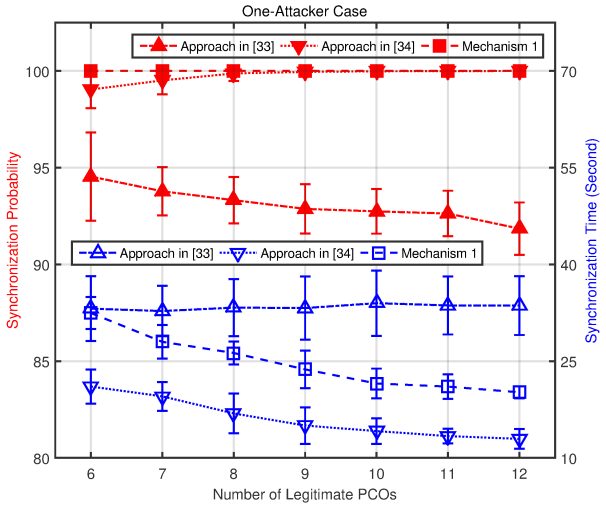

Figure 15: Comparison of Mechanism 1 and the conventional pulse based interaction mechanisms in [33] and [34] in terms of synchronization probability (red solid marker lines) and synchronization time (blue hollow marker lines) in the presence of one attacker.

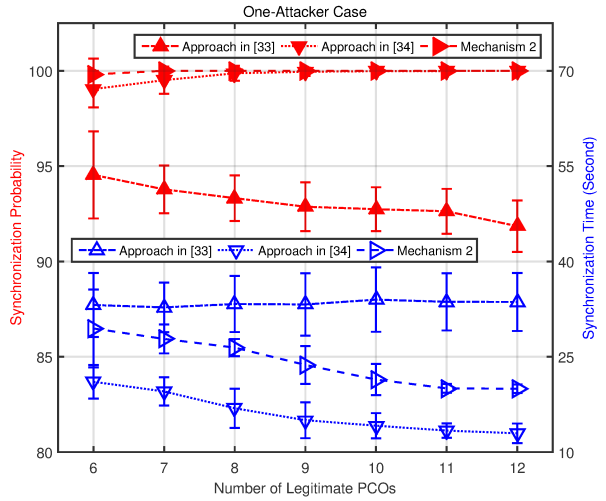

Figure 16: Comparison of Mechanism 2 and the conventional pulse based interaction mechanisms in [33] and [34] in terms of synchronization probability (red solid marker lines) and synchronization time (blue hollow marker lines) in the presence of one attacker.

C. *General Interaction Topologies*

The new pulse based interaction approach (Mechanisms 1 and 2) also shows promising resilience to random attacks

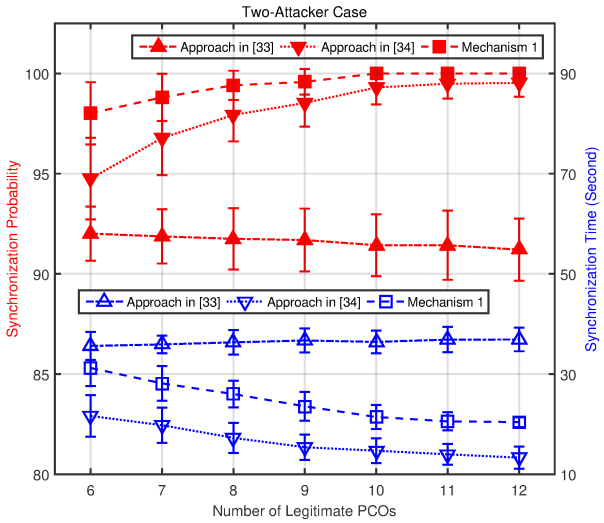

Figure 17: Comparison of Mechanism 1 and the conventional pulse based interaction mechanisms in [33] and [34] in terms of synchronization probability (red solid marker lines) and synchronization time (blue hollow marker lines) in the presence of two attackers.

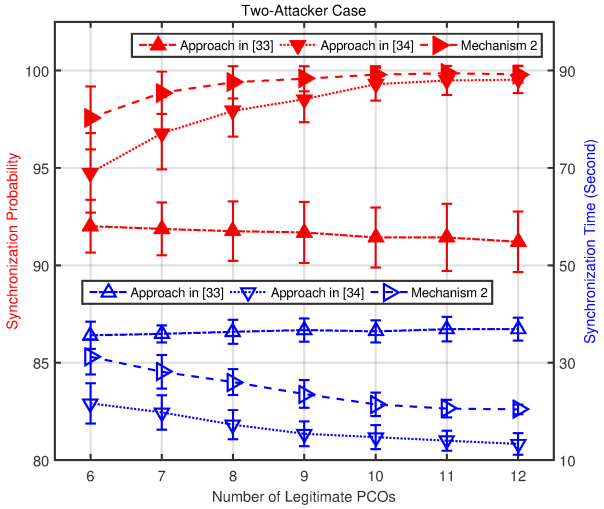

Figure 18: Comparison of Mechanism 2 and the conventional pulse based interaction mechanisms in [33] and [34] in terms of synchronization probability (red solid marker lines) and synchronization time (blue hollow marker lines) in the presence of two attackers.

even under non-all-to-all interaction topologies. One can easily get that perfect synchronization of legitimate oscillators in a general strongly-connected PCO network cannot be achieved when some legitimate oscillators are affected by attackers whereas others are not. This is because malicious pulses can exert nonzero phase shifts on affected legitimate oscillators and make them deviate from the non-affected legitimate ones. So similar to [33], we numerically studied the synchronization error of strongly-connected PCO networks under random attacks. The synchronization error was quantified as follows:

$$\textit{Synchronization Error} = \max_{i,j\in\mathcal{N}_6}\{\min(2\pi-|\phi_i-\phi_j|,|\phi_i-\phi_j|)\}$$

where $\mathcal{N}_6$ is the index set of all legitimate oscillators. One can get that synchronization is achieved only when $\textit{Synchronization Error} = 0$ holds.

We compared the synchronization errors of the proposed Mechanisms 1 and 2 with the mechanisms in [33] and [34] under a network of 20 oscillators distributed on a $50m \times 40m$ rectangle. All the oscillators are fixed in the rectangle with position represented by the blue dots in Fig. 19. Two oscillators in the network can communicate with each other if and only if their distance is less than 30 meters. The initial phases of all oscillators were randomly chosen from $[0, 2\pi]$ and the coupling strength was set to $l = 0.5$.

Fig. 20 shows the synchronization errors of our approaches (Mechanisms 1 and Mechanism 2) and existing synchronization approaches in [33] and [34]. In Fig. 20, each data point was obtained under $10,000$ runs. In each run, all approaches used the same initial phase distribution (randomly chosen from $[0, 2\pi]$) and are subject to identical malicious pulse patterns (time interval between two consecutive malicious pulses randomly chosen from $[T/4, 9T/4]$). The vertical error bars denote standard deviations. It can be seen that in the presence of one attacker, our approach (Mechanisms 1&2) provides not only less average synchronization error but also less standard deviations. Fig. 21 shows the results in the presence of two attackers, which also confirmed that the proposed approach (Mechanisms 1&2) led to reduced average synchronization errors and standard deviations compared with existing results in [33] and [34]. It is worth noting that Mechanism 2 led to a slightly larger synchronization error than Mechanism 1. This reduction of synchronization performance is consistent with our intuition that less knowledge (the network size N is unknown to individual oscillators in Mechanism 2) reduces the capacity of attack-resilient synchronization design.

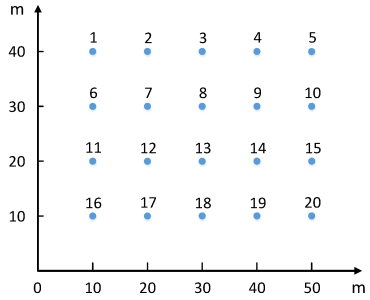

Figure 19: The positions of the 20 oscillators used in simulation.

VIII. Conclusions

Due to unique advantages over conventional packet-based synchronization approaches in terms of simplicity, scalability, and energy efficiency, pulse based synchronization has been widely studied. However, few results are available to address the attack-resilience of pulse base synchronization. In this

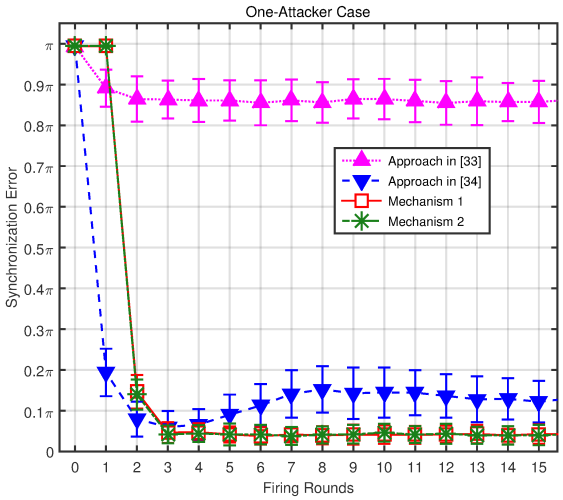

Figure 20: Comparison of Mechanisms 1 and 2 with the conventional pulse based interaction mechanisms in [33] and [34] in terms of synchronization error when oscillator 7 in Fig. 19 was compromised. The coupling strength was set to $l = 0.5$.

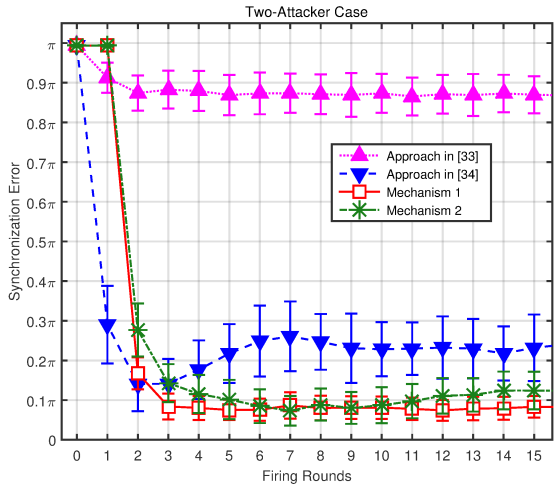

Figure 21: Comparison of Mechanisms 1 and 2 with the conventional pulse based interaction mechanisms in [33] and [34] in terms of synchronization error when oscillators 7 and 20 in Fig. 19 were compromised. The coupling strength was set to $l = 0.5$.

paper, we propose new pulse based interaction mechanisms to improve the attack resilience of PCO networks. More interestingly, we show that the new mechanism can enable synchronization in the presence of multiple stealthy Byzantine attackers even when the initial phases of legitimate oscillators are unrestricted, i.e., randomly distributed in the entire oscillator period. This is in distinct difference from most of the existing attack-resilience algorithms which require a priori (almost) synchronization among all legitimate oscillators. The approach is also applicable when the total number of oscillators are unknown to individual oscillators. Numerical simulations confirmed the analytical results.

REFERENCES

[1] L. Lamport and P. M. Melliar-Smith. Synchronizing clocks in the presence of faults. *Journal of the ACM (JACM)*, 32(1):52–78, 1985.

[2] R. Mirollo and S. Strogatz. Synchronization of pulse-coupled biological oscillators. *SIAM Journal on Applied Mathematics*, 50(6):1645–1662, 1990.

[3] Charles S Peskin. *Mathematical aspects of heart physiology*. Courant Institute of Mathematical Sciences, New York University, 1975.

[4] R. Mathar and J. Mattfeldt. Pulse-coupled decentral synchronization. *SIAM Journal on Applied Mathematics*, 56(4):1094–1106, 1996.

[5] O. Simeone, U. Spagnolini, Y. Bar-Ness, and S. Strogatz. Distributed synchronization in wireless networks. *IEEE Signal Processing Magazine*, 25(5):81–97, 2008.

[6] R. Pagliari and A. Scaglione. Scalable network synchronization with pulse-coupled oscillators. *IEEE Transactions on Mobile Computing*, 10(3):392–405, 2011.

[7] G. Werner-Allen, G. Tewari, A. Patel, M. Welsh, and R. Nagpal. Firefly-inspired sensor network synchronicity with realistic radio effects. In *Proceedings of the 3rd international conference on Embedded networked sensor systems*, pages 142–153. ACM, 2005.

[8] Y. W. Hong and A. Scaglione. A scalable synchronization protocol for large scale sensor networks and its applications. *IEEE Journal on Selected Areas in Communications*, 23(5):1085–1099, 2005.

[9] A. Hu and S. D. Servetto. On the scalability of cooperative time synchronization in pulse-connected networks. *IEEE Transactions on Information Theory*, 52(6):2725–2748, 2006.

[10] R. Leidenfrost and W. Elmenreich. Firefly clock synchronization in an 802.15. 4 wireless network. *EURASIP Journal on Embedded Systems*, 2009(1):1, 2009.

[11] F. Núñez, Y. Q. Wang, D. Grasing, S. Desai, G. Cakiades, and F. J. Doyle III. Pulse-coupled time synchronization for distributed acoustic event detection using wireless sensor networks. *Control Engineering Practice*, 60:106–117, 2017.

[12] Y. Q. Wang and F. J. Doyle III. Optimal phase response functions for fast pulse-coupled synchronization in wireless sensor networks. *IEEE Transactions on Signal Processing*, 60(10):5583–5588, 2012.

[13] K. Konishi and H. Kokame. Synchronization of pulse-coupled oscillators with a refractory period and frequency distribution for a wireless sensor network. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 18(3):033132, 2008.

[14] T. Okuda, K. Konishi, and N. Hara. Experimental verification of synchronization in pulse-coupled oscillators with a refractory period and frequency distribution. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 21(2):023105, 2011.

[15] Y. Q. Wang, F. Núñez, and F. J. Doyle III. Energy-efficient pulse-coupled synchronization strategy design for wireless sensor networks through reduced idle listening. *IEEE Transactions on Signal Processing*, 60(10):5293–5306, 2012.

[16] Y. Q. Wang, F. Núñez, and F. J. Doyle III. Statistical analysis of the pulse-coupled synchronization strategy for wireless sensor networks. *IEEE Transactions on Signal Processing*, 61(21):5193–5204, 2013.

[17] F. Núñez, Y. Q. Wang, and F. J. Doyle III. Synchronization of pulse-coupled oscillators on (strongly) connected graphs. *IEEE Transactions on Automatic Control*, 60(6):1710–1715, 2015.

[18] F. Núñez, Y. Q. Wang, A. R. Teel, and F. J. Doyle III. Synchronization of pulse-coupled oscillators to a global pacemaker. *Systems & Control Letters*, 88:75–80, 2016.

[19] J. Klinglmayr, C. Kirst, C. Bettstetter, and M. Timme. Guaranteeing global synchronization in networks with stochastic interactions. *New Journal of Physics*, 14(7):073031, 2012.

[20] Johannes Klinglmayr, Christian Bettstetter, Marc Timme, and Christoph Kirst. Convergence of self-organizing pulse-coupled oscillator synchronization in dynamic networks. *IEEE Transactions on Automatic Control*, 2016.

[21] Deepti Kannapan and Francesco Bullo. Synchronization in pulse-coupled oscillators with delayed excitatory/inhibitory coupling. *SIAM Journal on Control and Optimization*, 54(4):1872–1894, 2016.

[22] J. Nishimura and E. J. Friedman. Probabilistic convergence guarantees for type-ii pulse-coupled oscillators. *Physical Review E*, 86(2):025201, 2012.

[23] L. Lücken and S. Yanchuk. Two-cluster bifurcations in systems of globally pulse-coupled oscillators. *Physica D: Nonlinear Phenomena*, 241(4):350–359, 2012.

[24] A. V. Proskurnikov and M. Cao. Synchronization of pulse-coupled oscillators and clocks under minimal connectivity assumptions. *IEEE Transactions on Automatic Control*, 2016.

[25] F. Núñez, Y. Q. Wang, and F. J. Doyle. Global synchronization of pulse-coupled oscillators interacting on cycle graphs. *Automatica*, 52:202–209, 2015.

[26] M. Pease, R. Shostak, and L. Lamport. Reaching agreement in the presence of faults. *Journal of the ACM (JACM)*, 27(2):228–234, 1980.

[27] M. Manzo, T. Roosta, and S. Sastry. Time synchronization attacks in sensor networks. In *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, pages 107–116. ACM, 2005.

[28] Q. Li and D. Rus. Global clock synchronization in sensor networks. *IEEE Transactions on computers*, 55(2):214–226, 2006.

[29] H. Song, S. Zhu, and G. H. Cao. Attack-resilient time synchronization for wireless sensor networks. *Ad Hoc Networks*, 5(1):112–125, 2007.

[30] X. J. Du and H. Chen. Security in wireless sensor networks. *IEEE Wireless Communications*, 15(4), 2008.

[31] R. Leidenfrost, W. Elmenreich, and C. Bettstetter. Fault-tolerant averaging for self-organizing synchronization in wireless ad hoc networks. In *2010 7th International Symposium on Wireless Communication Systems*, pages 721–725, 2010.

[32] Alexander Tyrrell, Gunther Auer, Christian Bettstetter, and Rahul Naripella. How does a faulty node disturb decentralized slot synchronization over wireless networks? In *2010 IEEE International Conference on Communications*, pages 1–5, 2010.

[33] J. Klinglmayr and C. Bettstetter. Self-organizing synchronization with inhibitory-coupled oscillators: Convergence and robustness. *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, 7(3):30, 2012.

[34] S. Yun, J. Ha, and B. J. Kwak. Robustness of biologically inspired pulse-coupled synchronization against static attacks. In *2015 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2015.

[35] Z. Q. Wang and Y. Q. Wang. Attack-resilient pulse-coupled synchronization. *Accepted to IEEE Transactions on Control of Network Systems*, 2018.

[36] L. Lamport, R. Shostak, and M. Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3):382–401, 1982.

[37] W. Y. Xu, W. Trappe, Y. Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, pages 46–57. ACM, 2005.