

An Attack-Resilient Pulse-Based Synchronization Strategy for General Connected Topologies

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

Abstract—Synchronization of pulse-coupled oscillators (PCOs) has gained significant attention recently due to increased applications in sensor networks and wireless communications. Given the distributed and unattended nature of wireless sensor networks, it is imperative to enhance the resilience of pulse-based synchronization against malicious attacks. However, most existing results on resilient PCO synchronization are obtained for all-to-all networks. We propose a new pulse-based synchronization mechanism to improve the resilience of PCO synchronization that is applicable under general connected topologies. Under the proposed synchronization mechanism, we rigorously characterize the condition for stealthy Byzantine attacks and prove that perfect synchronization of legitimate oscillators can be guaranteed in the presence of multiple stealthy Byzantine attackers, irrespective of whether the attackers collude with each other or not. The new mechanism can guarantee resilient synchronization even when the initial phases of legitimate oscillators are widely distributed in a half circle, which is in distinct difference from most existing attack-resilient synchronization algorithms (including the seminal paper from Lamport and Melliar-Smith [1]) that require *a priori* (almost) synchronization among legitimate oscillators. Numerical simulation results are given to confirm the theoretical results.

Index Terms—Synchronization, Pulse-Coupled Oscillators, General Connected Topologies, Stealthy Byzantine Attacks.

I. INTRODUCTION

Inspired by flashing fireflies and contracting cardiac cells, pulse-based synchronization is attracting increased attention in sensor networks and wireless communications [2]–[5]. By exchanging simple and identical messages (so-called pulses), pulse-based synchronization incurs much less energy consumption and communication overhead compared with conventional packet-based synchronization approaches [6]. These inherent advantages make pulse-based synchronization extremely appealing for event coordination and clock synchronization in various networks [7]–[11]. In the past decade, plenty of results have been reported on pulse-based synchronization. For example, by optimizing the interaction function, i.e., phase response function, the 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 of 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

Zhenqian Wang and Yongqiang Wang are with the Department of Electrical and Computer Engineering, Clemson University, Clemson, SC, 29630 USA. e-mail: {zhenqiw, yongqiw}@clemson.edu. The work was supported in part by the National Science Foundation under Grants 1738902, 1912702, and in part by the China Scholarship Council.

presence of time-delays and unreliable links is also discussed [19], [20]. Other relevant results include [21]–[29].

However, the above results are obtained under 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, making it imperative to study synchronization in the presence of attacks. Although plenty of discussions exist for conventional packet-based synchronization, e.g., [1], [30]–[35], results are very sparse on the attack-resilience of pulse-based synchronization. In [36], the authors showed that pulse-based synchronization is more robust than its packet-based counterpart in the presence of a faulty node. In [37], a new phase response function was proposed to improve the precision of pulse-based synchronization against non-persistent random attacks. The authors in [38] considered pulse-based synchronization in the presence of faulty nodes which fire periodically ignoring neighboring nodes' influence. However, none of the above results address phase synchronization of PCOs when compromised nodes act maliciously to corrupt synchronization by applying disturbing pulses with judiciously-crafted patterns. Furthermore, the above results only apply to *a priori* synchronized PCOs, i.e., all legitimate nodes are required to have identical phases when faulty pulses are emitted.

In this paper, we present a new pulse-based synchronization strategy for general connected PCOs that can achieve phase synchronization even in the presence of multiple stealthy Byzantine attackers. Throughout this paper, we use “general connected” to describe directed graphs in which there exists a (multi-hop) path between any pair of nodes. In the pulse-based interaction framework where exchanged messages are identical and content-free, Byzantine attacks mean compromised nodes injecting pulses using judiciously crafted patterns to disturb the synchronization process. So compared with existing results in [36]–[38] which address faulty PCO nodes with random or periodic pulse emitting patterns, 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 mechanism, we show that perfect phase synchronization of legitimate oscillators can still be guaranteed as long as their initial phases are distributed within a half oscillation period. The approach is applicable even when individual oscillators do not have access to the total number of oscillators in a network. The result is in distinct difference from our recent results in [39], [40] which can only guarantee phase synchronization under all-to-all topologies.

The main contributions of this paper are as follows: 1) We

propose a new mechanism for pulse-coupled synchronization that employs a “cut-off” algorithm to restrict the number of pulses able to affect a receiving oscillator’s phase in any three-quarter oscillation period, which is key to enable resilience to attacks; 2) The “cut-off” algorithm also brings superior robustness to time-varying delays (see the numerical-simulation based comparison with existing algorithms in the absence of attacks in Fig. 15 and Fig. 16), making the new pulse-coupled synchronization mechanism fundamentally different from existing ones and important in its own even in the absence of attacks; 3) We rigorously analyze the condition for an attacker to stay stealthy in a general connected pulse-coupled oscillator network, and address an attack model that is more difficult to deal with than existing results like [39], [40]; 4) We guarantee that the collective oscillation period is invariant under attacks and identical to the free-running period, which is superior to existing results (e.g., [39], [40]) that lead to a collective oscillation period affected by attacker pulses; 5) The results are applicable to general connected topologies whereas existing results on attack-resilience of pulse-coupled synchronization all assume an all-to-all topology.

It is worth noting that the analysis method here is also significantly different from the methods in [39], [40]. In [39], [40], one can prove that the length of the containing arc will decrease to a value no greater than $(1 - l)$ of its original value after each round of firing, where $l \in (0, 1]$ is the coupling strength. However, in this paper, while enabling resilience to attacks, the new interaction mechanism also leads to more complicated dynamics, as reflected by the fact that we cannot prove length reduction in the containing arc after each round of firing. In fact, in the worse case, we can only prove that the length of the containing arc will decrease to a value no greater than $(1 - l/2)$ of its original value after every two consecutive firing rounds.

This paper is organized as follows. Sec. II introduces a new pulse-based synchronization mechanism. Under the new mechanism, Sec. III presents a synchronization condition for general connected PCOs in the absence of attacks. In Sec. IV, 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 in the presence of multiple stealthy Byzantine attackers, with and without collusion. In Sec. VI, we prove the applicability of our approach even when the total number of oscillators is unknown to individual oscillators. Simulation results are presented in Sec. VII.

II. A NEW PULSE-BASED SYNCHRONIZATION MECHANISM

Consider a network of N pulse-coupled oscillators. Each oscillator is equipped with a phase variable. When the evolving phase of an oscillator reaches 2π rad, the oscillator emits a pulse. Receiving pulses from neighboring oscillators 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. An edge (i, j) from oscillator i to oscillator j means that oscillator j can receive pulses from

oscillator i but not necessarily vice versa. The number of edges entering oscillator i is called the indegree of oscillator i and is represented as $d^-(i)$. The number of edges leaving oscillator i is called the outdegree of oscillator i and is represented as $d^+(i)$. The value $d(i) \triangleq \min\{d^-(i), d^+(i)\}$ is called the degree of oscillator i . The degree of a network is defined as $d \triangleq \min_{i=1,2,\dots,N} \{d(i)\}$.

The conventional pulse-based synchronization mechanism is presented below:

Conventional Pulse-Based Synchronization Mechanism [38]:

- 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 and resets its phase to 0.
- 3) Whenever oscillator i receives a pulse, it *instantaneously* resets its phase to:

$$\phi_i^+ = \phi_i + l \times F(\phi_i) \quad (1)$$

where $l \in (0, 1]$ is the coupling strength and $F(\bullet)$ is the phase response function (PRF) given below:

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

In the above conventional pulse-based synchronization mechanism, every incoming pulse will trigger a jump on the receiving oscillator’s phase, which makes it easy for attackers to perturb the phases of legitimate oscillators and destroy their synchronization. Moreover, one can easily get that synchronization can never be maintained for general connected PCOs under the conventional mechanism, even when the coupling strength is set to $l = 1$. This is because attack pulses can always exert nonzero phase shifts on affected legitimate oscillators and make them deviate from unaffected ones. Due to the same reason, existing attack resilient pulse-coupled synchronization mechanisms in [39] and [40] for all-to-all graphs cannot be applied to general connected graphs, either. Motivated by these observations on the inherent vulnerability of existing pulse-based synchronization mechanisms, we propose a new pulse-based synchronization mechanism to improve the attack resilience of general connected PCO networks. Our key idea to enable attack resilience is a “cut-off” mechanism which can restrict the number of pulses able to affect a receiving oscillator’s phase in any three-quarter oscillation period. The “cut-off” mechanism only allows pulses meeting certain conditions to affect a receiving oscillator’s phase and hence can effectively filter out attack pulses with extremely negative effects on the synchronization process. Noting that all pulses are identical and content-free, so the “cut-off” mechanism is judiciously designed based on the number of pulses an oscillator received in the past, i.e., based on memory. This is also the reason that we let an entire oscillation period $T = 2\pi$ seconds elapse so that each oscillator can acquire memory.

New Pulse-Based Synchronization Mechanism (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 and resets its phase to 0.
- 3) When oscillator i receives a pulse at time instant t , it resets its phase according to (1) only when all the following three conditions are satisfied:
 - a) an entire period of $T = 2\pi$ seconds has elapsed since initiation.
 - b) before receiving the current pulse, oscillator i has received at least

$$\lambda_i = \lfloor (d(i) - \lfloor N/2 \rfloor)/4 \rfloor \quad (3)$$

pulses within $(t - T/4, t]$, where $d(i)$ is the degree of oscillator i and $\lfloor \bullet \rfloor$ is the largest integer no greater than “ \bullet ”

- c) before receiving the current pulse, oscillator i has received less than $\bar{\lambda}_i$ pulses within $(t - 3T/4, t]$, where

$$\bar{\lambda}_i = d(i) - 2\lambda_i \quad (4)$$

Otherwise, the pulse has no effect on ϕ_i .

Fig. 1 illustrates the phase evolution of oscillator i having degree $d(i) = 9$ in a network of 11 PCOs. According to (3) and (4), we have $\lambda_i = 1$ and $\bar{\lambda}_i = 7$. So a pulse received at time instant t can shift oscillator i 's phase when all the following three conditions are met: 1) $t > T$; 2) oscillator i has received at least 1 pulse within $(t - T/4, t]$; and 3) oscillator i has received less than 7 pulses within $(t - 3T/4, t]$. Take the scenario in Fig. 1 as an example, only the 11th and the 12th pulses triggered phase jumps on oscillator i .

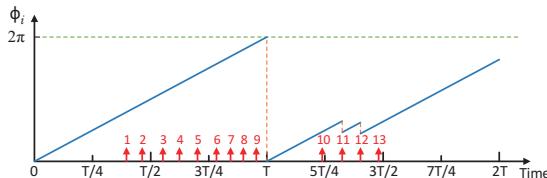


Figure 1: The phase evolution of oscillator i in a network of 11 PCOs under Mechanism 1. Indexed red arrows represent incoming pulses.

Remark 1: Following [24], [25], [28], we assume that when a legitimate oscillator receives multiple pulses simultaneously, it will process the incoming pulses consecutively. In other words, no two pulses will be regarded as an aggregated pulse.

III. SYNCHRONIZATION OF GENERAL CONNECTED PCOS IN THE ABSENCE OF ATTACKS

In this section, we will show that Mechanism 1 can guarantee the synchronization of general connected PCOs in the absence of attacks.

Assuming that all oscillators' phases rotate clockwise on a unit circle, the containing arc of legitimate oscillators is defined as the shortest arc on the unit circle that contains all legitimate oscillators' phases. The leading and terminating points of a containing arc are defined as the starting and

ending points of the containing arc in the clockwise direction, respectively.

Based on the definition of containing arc, we can define phase synchronization:

Definition 1 (Phase Synchronization): A network of pulse-coupled oscillators achieves phase synchronization if the length of the containing arc of all legitimate oscillators converges to 0 upon which all legitimate oscillators fire simultaneously with a fixed period $T = 2\pi$ seconds.

Remark 2: Requiring the firing period to be $T = 2\pi$ seconds in *Definition 1* is important for two reasons. First, this requirement guarantees that all legitimate oscillators will not have irregular behaviors. For example, otherwise all oscillators having fixed and constant phases 0 meets the condition of containing arc converging to 0 but is unacceptable for pulse-coupled oscillators. Secondly, this additional requirement on firing period guarantees that the collective oscillation period after synchronization is not affected by attacks. In fact, in existing results [37]–[40], the collective firing period could be affected by attack pulses.

We next give two important properties of general connected PCO networks under Mechanism 1.

Lemma 1: For a general connected network of N legitimate PCOs evolving under Mechanism 1, when the initial length of the containing arc is less than π rad, the length of the containing arc is non-increasing.

Proof: Following the same line of reasoning as in Theorem 1 of [39], the containing arc's length will change only when an oscillator's firing triggers a phase jump on at least one other oscillator. We assume that oscillator i fires at time instant t_i whose pulse triggers a phase jump on at least one other oscillator. One can easily get $\phi_i(t_i) = 2\pi$ and the phase distribution of all the other $N - 1$ oscillators can only fall within one of the following three scenarios, as depicted in Fig. 2:

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

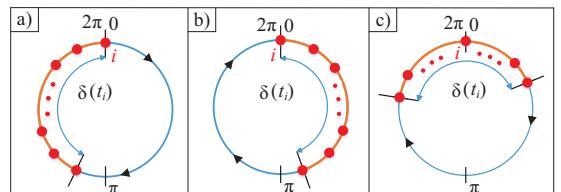


Figure 2: Three scenarios of phase distributions of oscillators when oscillator i fires at time instant t_i .

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

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

expressed as

$$\delta(t_i) = 2\pi - \min_{j \in \mathcal{N}, j \neq i} \{\phi_j(t_i)\} \quad (5)$$

where $\mathcal{N} = \{1, 2, \dots, N\}$ is the index set of all oscillators. After the firing of oscillator i , we have $\phi_i^+(t_i) = 0$. Since the PRF in (2) is non-negative on $(\pi, 2\pi]$, the pulse can only trigger a forward jump or have no effect on an oscillator with phase residing in $(\pi, 2\pi]$. Hence, we have $\phi_j^+(t_i) = \phi_j(t_i) + F(\phi_j(t_i)) \geq \phi_j(t_i)$ or $\phi_j^+(t_i) = \phi_j(t_i)$ for $j \in \mathcal{N}, j \neq i$. In both cases we have $\phi_j(t_i) \leq \phi_j^+(t_i)$ for $j \in \mathcal{N}, j \neq i$, which implies

$$\min_{j \in \mathcal{N}, j \neq i} \{\phi_j(t_i)\} \leq \min_{j \in \mathcal{N}, j \neq i} \{\phi_j^+(t_i)\} \quad (6)$$

The length of the containing arc immediately after oscillator i 's firing at t_i becomes

$$\begin{aligned} \delta^+(t_i) &= 2\pi - \min_{j \in \mathcal{N}, j \neq i} \{\phi_j^+(t_i)\} + \phi_i^+(t_i) \\ &= 2\pi - \min_{j \in \mathcal{N}, j \neq i} \{\phi_j^+(t_i)\} \end{aligned} \quad (7)$$

One can easily get $\delta^+(t_i) \leq \delta(t_i)$ by combining (5), (6) and (7).

- b) When all the other $N - 1$ oscillators' phases reside in $[0, \pi]$ at time instant t_i (note that phases 0 and 2π are the same point on the unit circle), noting that under Mechanism 1, the pulse can only trigger a backward jump or have no effect on an oscillator with phase residing in $[0, \pi]$, one can easily get $\delta^+(t_i) \leq \delta(t_i)$ following the same line of reasoning as in Scenario a).
- c) When the other $N - 1$ oscillators' phases reside partially in $(\pi, 2\pi]$ and partially in $[0, \pi]$ at time instant t_i , one can easily get $\delta^+(t_i) \leq \delta(t_i)$ by combining the arguments in Scenario a) and Scenario b).

Summarizing the above three scenarios, we get that the length of the containing arc is non-increasing. ■

Based on Lemma 1, next we show that every oscillator will fire at least once within any time interval of length $3T/2$ under Mechanism 1.

Lemma 2: For a general connected network of N legitimate PCOs with their initial length of the containing arc less than π rad, every oscillator will fire at least once within any time interval of length $3T/2$ under Mechanism 1.

Proof: From Lemma 1, we know that the length of the containing arc is non-increasing. So the phase distribution of all oscillators at an arbitrary time instant t can only fall within one of the following four scenarios, as illustrated in Fig. 3:

- 1) all oscillators' phases reside in $[0, \pi]$;
- 2) oscillators' phases reside partially in $[0, \pi]$, partially in $(\pi, 2\pi]$ and the containing arc includes phase π ;
- 3) all oscillators' phases reside in $(\pi, 2\pi]$;
- 4) oscillators' phases reside partially in $[0, \pi]$, partially in $(\pi, 2\pi]$ and the containing arc includes phase 2π .

Since all oscillators are legitimate, according to Mechanism 1, one can easily get that in Scenarios 1), 2) and 3), all oscillators will evolve towards phase 2π rad and fire within $[t, t + T]$. In Scenario 4), given that the PRF in (2) is non-negative on $(\pi, 2\pi]$, the pulse can only advance or have no

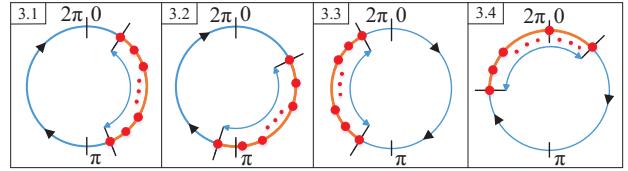


Figure 3: Four possible scenarios of phase distribution at time instant t .

effect on the oscillators with phase residing in $(\pi, 2\pi]$. Hence, all oscillators residing in $(\pi, 2\pi]$ will evolve towards phase 2π rad and fire within $[t, t + T/2]$. Since the length of the containing arc is less than π rad and non-increasing, all oscillators reside in $[0, \pi]$ immediately after the firing of the oscillator on the ending point of the containing arc, meaning that the network shifts to Scenario 1). Then all oscillators will evolve towards phase 2π rad and fire within the following T seconds. Therefore, we can get that in Scenario 4), every oscillator will fire within $[t, t + 3T/2]$. By iterating the above argument, we know that every oscillator will fire at least once within any time interval of length $3T/2$. ■

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

Theorem 1: For a general connected network of N legitimate PCOs, if the initial length of the containing arc is less than π rad and the degree of the PCO network satisfies $d > \lfloor N/2 \rfloor$, then the containing arc of all oscillators will converge to zero under Mechanism 1.

Proof: Without loss of generality, we denote $\delta(t)$ as the length of the containing arc at time t and set the initial time to $t = 0$. According to Lemma 1, we have that the containing arc is non-increasing and $0 \leq \delta(t) < \pi$ for $t \geq 0$. From Lemma 2, every oscillator will fire at least once within any time interval of length $3T/2$ and hence there exists a time instant $t_0 > 2T$ at which the ending point of the containing arc resides at phase 0. Denoting the starting point of the containing arc at this time instant as $0 \leq \varepsilon < \pi$, we have $\delta(t_0) = \varepsilon$. Next, we separately discuss the $0 \leq \varepsilon < \pi/2$ case and the $\pi/2 \leq \varepsilon < \pi$ case to prove the convergence of $\delta(t)$ to 0.

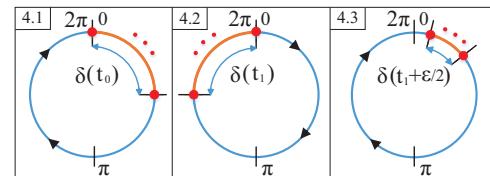


Figure 4: Phase distributions of all oscillators at different time instants in Scenario 1.1.

Case 1 ($0 \leq \varepsilon < \pi/2$): If ε is 0, the network is synchronized. So we only consider $0 < \varepsilon < \pi/2$. Noting that the ending and starting points of the containing arc reside on phases 0 and $0 < \varepsilon < \pi/2$ rad at time instant t_0 , respectively (as depicted in Fig. 4.1), so after t_0 , all oscillators will evolve freely without firing for exactly $T - \varepsilon > 3T/4$ seconds before the starting point of the containing arc reaches phase 2π rad at time $t_1 = t_0 + T - \varepsilon$ (as depicted in Fig. 4.2). Meanwhile, the ending

point of the containing arc resides on phase $2\pi - \varepsilon$ rad and we have $\delta(t_1) = \delta(t_0) = \varepsilon$.

Given that the PRF in (2) is non-negative on $[2\pi - \varepsilon, 2\pi]$, a pulse can only trigger a forward jump or have no effect on an oscillator with phase residing in $[2\pi - \varepsilon, 2\pi]$. So all oscillators will reach phase 2π rad and fire no later than $t_1 + \varepsilon$ and within $[t_1, t_1 + \varepsilon/2]$, we can only have one of the following three scenarios:

Scenario 1.1: all oscillators fired within $[t_1, t_1 + \varepsilon/2]$;

Scenario 1.2: some oscillators did not fire within $[t_1, t_1 + \varepsilon/2]$ but all these oscillators jumped in phase within $[t_1, t_1 + \varepsilon/2]$;

Scenario 1.3: some oscillators neither fired nor jumped in phase within $[t_1, t_1 + \varepsilon/2]$.

Next, we prove $\delta(t_1 + \varepsilon) \leq (1 - l/2)\delta(t_1)$ in all above three scenarios, based on which we can further prove such a decrease of containing arc after each round of firing and hence the convergence of $\delta(t)$ to zero. Without loss of generality, we label all oscillators in an increasing order of their phases at time instant t_1 , i.e., $2\pi - \varepsilon = \phi_1(t_1) \leq \phi_2(t_1) \leq \dots \leq \phi_N(t_1) = 2\pi$ and denote \mathcal{N}_f (respectively \mathcal{N}_n) as the index set of oscillators fired (respectively did not fire) in $[t_1, t_1 + \varepsilon/2]$.

Scenario 1.1 (all oscillators fired within $[t_1, t_1 + \varepsilon/2]$): One can easily know that in this case \mathcal{N}_f contains all oscillators and \mathcal{N}_n is an empty set. The phases of all oscillators at $t_1 + \varepsilon/2$ should follow the pattern depicted in Fig. 4.3.

Since the PRF in (2) is non-positive on $[0, \pi]$, the phase evolution of an oscillator cannot be advanced by received pulses when its phase resides in $[0, \pi]$. So all oscillators' phases reside in $[0, \varepsilon/2]$ at time $t_1 + \varepsilon/2$, which means $0 \leq \delta(t_1 + \varepsilon/2) \leq \varepsilon/2 = \delta(t_1)/2$. Given $l \in (0, 1]$, one can obtain $\delta(t_1 + \varepsilon/2) \leq (1 - l/2)\delta(t_1)$. According to the non-increasing property of the containing arc in Lemma 1, we have $\delta(t_1 + \varepsilon) \leq (1 - l/2)\delta(t_1)$.

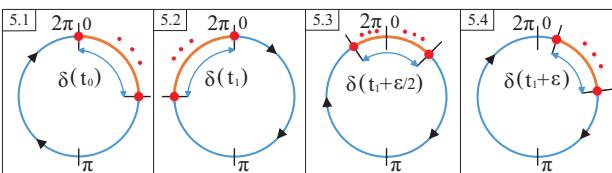


Figure 5: Phase distributions of all oscillators at different time instants in *Scenario 1.2* and *Scenario 1.3*.

Scenario 1.2 (some oscillators did not fire within $[t_1, t_1 + \varepsilon/2]$ but all these oscillators jumped in phase within $[t_1, t_1 + \varepsilon/2]$): At time instant $t_1 + \varepsilon/2$, the phase distribution of all oscillators should follow the pattern depicted in Fig. 5.3. The length of the containing arc at $t_1 + \varepsilon/2$ can be obtained as

$$\delta(t_1 + \varepsilon/2) = \max_{i \in \mathcal{N}_f} \{\phi_i(t_1 + \varepsilon/2)\} + 2\pi - \min_{j \in \mathcal{N}_n} \{\phi_j(t_1 + \varepsilon/2)\} \quad (8)$$

Following the same line of reasoning as in *Scenario 1.1*, one can get $\phi_i(t_1 + \varepsilon/2) \in [0, \varepsilon/2]$ for $i \in \mathcal{N}_f$, i.e.,

$$\max_{i \in \mathcal{N}_f} \{\phi_i(t_1 + \varepsilon/2)\} \leq \varepsilon/2 \quad (9)$$

Next, we characterize $\min_{j \in \mathcal{N}_n} \{\phi_j(t_1 + \varepsilon/2)\}$. Since all oscillators in \mathcal{N}_n jumped at least once within $[t_1, t_1 + \varepsilon/2]$, we denote $\hat{t}_j \in [t_1, t_1 + \varepsilon/2]$ as the time instant of oscillator j 's first jump within $[t_1, t_1 + \varepsilon/2]$. So the phase of oscillator j immediately before the jump at \hat{t}_j is $\phi_j(\hat{t}_j) = \phi_j(t_1) + \hat{t}_j - t_1$. According to the PRF in (2), we have the phase of oscillator j immediately after the jump at \hat{t}_j as

$$\begin{aligned} \phi_j^+(\hat{t}_j) &= \phi_j(\hat{t}_j) + (2\pi - \phi_j(\hat{t}_j))l \\ &= 2\pi l + (1 - l)(\phi_j(t_1) + \hat{t}_j - t_1) \end{aligned}$$

Noting that the PRF in (2) is non-negative on $[2\pi - \varepsilon, 2\pi]$ and oscillator j can be triggered to jump multiple times within $[t_1, t_1 + \varepsilon/2]$, the phase of oscillator j at $t_1 + \varepsilon/2$ satisfies

$$\begin{aligned} \phi_j(t_1 + \varepsilon/2) &\geq \phi_j^+(\hat{t}_j) + t_1 + \varepsilon/2 - \hat{t}_j \\ &= 2\pi l + (1 - l)\phi_j(t_1) + \varepsilon/2 - (\hat{t}_j - t_1)l \end{aligned}$$

Using the facts $\phi_j(t_1) \in [2\pi - \varepsilon, 2\pi]$ and $\hat{t}_j \in [t_1, t_1 + \varepsilon/2]$, we have $\phi_j(t_1 + \varepsilon/2) \geq 2\pi - (1 - l)\varepsilon/2$ for $j \in \mathcal{N}_n$, i.e.,

$$\min_{j \in \mathcal{N}_n} \{\phi_j(t_1 + \varepsilon/2)\} \geq 2\pi - (1 - l)\varepsilon/2 \quad (10)$$

Combining (8), (9), and (10), we have $\delta(t_1 + \varepsilon/2) \leq (1 - l/2)\delta(t_1)$. According to the non-increasing property of the containing arc in Lemma 1, one can obtain $\delta(t_1 + \varepsilon) \leq (1 - l/2)\delta(t_1)$.

Scenario 1.3 (some oscillators neither fired nor jumped in phase within $[t_1, t_1 + \varepsilon/2]$): At time instant $t_1 + \varepsilon/2$, the phase distribution of all oscillators should also follow the pattern depicted in Fig. 5.3. To prove $\delta(t_1 + \varepsilon) \leq (1 - l/2)\delta(t_1)$, we first characterize the number of oscillators in \mathcal{N}_f and \mathcal{N}_n .

We assume oscillator $j' \in \mathcal{N}_n$ neither fired nor jumped in phase within $[t_1, t_1 + \varepsilon/2]$. Recall that no oscillators fired in (t_0, t_1) of duration $t_1 - t_0 = T - \varepsilon > 3T/4$, according to Mechanism 1, oscillator j' being not triggered to jump in phase within $[t_1, t_1 + \varepsilon/2]$ implies it receiving no greater than $\lambda_{j'}$ pulses within $[t_1, t_1 + \varepsilon/2]$ of duration less than $T/4$, i.e., condition *b*) of Mechanism 1 is not satisfied.

As all oscillators will reach 2π rad and fire within $[t_1, t_1 + \varepsilon]$, every oscillator k ($1 \leq k \leq N$) should receive at least $d(k)$ pulses within $[t_1, t_1 + \varepsilon]$. Since oscillator j' was not triggered to jump and hence received no greater than $\lambda_{j'}$ pulses within $[t_1, t_1 + \varepsilon/2]$, it will receive at least $d(j') - \lambda_{j'}$ pulses in $(t_1 + \varepsilon/2, t_1 + \varepsilon]$, i.e., the number of oscillators that did not fire in $[t_1, t_1 + \varepsilon/2]$ is at least $d(j') - \lambda_{j'}$. In other words, the number of oscillators in \mathcal{N}_n is at least $d(j') - \lambda_{j'}$. According to the definition of $\lambda_{j'}$ in (3), we have $4\lambda_{j'} \leq d(j') - \lfloor N/2 \rfloor$, which further leads to $d(j') - \lambda_{j'} \geq \lfloor N/2 \rfloor + 3\lambda_{j'}$. Given $\lambda_{j'} \geq 0$ and $d(j') > \lfloor N/2 \rfloor$, we always have $d(j') - \lambda_{j'} \geq \lfloor N/2 \rfloor + 1$. Therefore, the number of oscillators in \mathcal{N}_n is at least $\lfloor N/2 \rfloor + 1$ and the number of oscillators in \mathcal{N}_f is at most $N - (\lfloor N/2 \rfloor + 1)$, which is no greater than $\lfloor N/2 \rfloor$.

Next, we characterize the phases of oscillators at $t_1 + \varepsilon$. Since all oscillators in \mathcal{N}_n fired within $(t_1 + \varepsilon/2, t_1 + \varepsilon]$, following the same line of reasoning as in *Scenario 1.1*, we have

$$\phi_j(t_1 + \varepsilon) \in [0, \varepsilon/2] \quad (11)$$

for $j \in \mathcal{N}_n$.

To determine $\phi_i(t_1 + \varepsilon)$ for $i \in \mathcal{N}_f$, we first determine $\phi_i(t_1 + \varepsilon/2)$ for $i \in \mathcal{N}_f$. Recall that all oscillators in \mathcal{N}_f fired within $[t_1, t_1 + \varepsilon/2]$, following the same line of reasoning as in *Scenario 1.1*, we have $\phi_i(t_1 + \varepsilon/2) \in [0, \varepsilon/2]$ for $i \in \mathcal{N}_f$. Next, we prove that all oscillators in \mathcal{N}_f will be triggered to jump in phase within $(t_1 + \varepsilon/2, t_1 + \varepsilon]$.

As has been proven, the number of oscillators in \mathcal{N}_f is no greater than $\lfloor N/2 \rfloor$ and all oscillators in \mathcal{N}_f fired within $[t_1, t_1 + \varepsilon/2]$. So every oscillator i in \mathcal{N}_f can receive at most $\lfloor N/2 \rfloor - 1$ pulses within $[t_1, t_1 + \varepsilon/2]$ (note that oscillator i cannot receive its own pulse) and will receive at least $d(i) - (\lfloor N/2 \rfloor - 1)$ pulses within $(t_1 + \varepsilon/2, t_1 + \varepsilon]$ of duration less than $T/4$. Using the definition of λ_i in (3), we have $d(i) - (\lfloor N/2 \rfloor - 1) > \lambda_i$, i.e., there must exist a time instant $\tilde{t}_i \in (t_1 + \varepsilon/2, t_1 + \varepsilon]$ for every oscillator i at which it receives the $(\lambda_i + 1)th$ pulse since (but not including) time instant $t_1 + \varepsilon/2$, i.e., condition *b*) in Mechanism 1 is satisfied. Next we proceed to prove that at \tilde{t}_i , condition *c*) in Mechanism 1 is also satisfied (note that condition *a*) is always satisfied since we start at $t_0 > 2T$), and hence all oscillators in \mathcal{N}_f will be triggered to jump in phase in $(t_1 + \varepsilon/2, t_1 + \varepsilon]$.

As no oscillators fire within (t_0, t_1) of duration $t_1 - t_0 = T - \varepsilon > 3T/4$ and oscillator i receives at most $\lfloor N/2 \rfloor - 1$ pulses within $[t_1, t_1 + \varepsilon/2]$, we have that within $(t_0, t_1 + \varepsilon/2]$ of duration $t_1 + \varepsilon/2 - t_0 > 3T/4$, oscillator i receives at most $\lfloor N/2 \rfloor - 1$ pulses, which is less than $\bar{\lambda}_i - 2\lambda_i$ according to (4), implying that at \tilde{t}_i , condition *c*) of Mechanism 1 is also satisfied. Therefore, according to Mechanism 1, the phase of oscillator i will be triggered to jump by the pulse received at \tilde{t}_i , i.e., every oscillator i in \mathcal{N}_f will be triggered to jump in phase within $(t_1 + \varepsilon/2, t_1 + \varepsilon]$.

Now we are in position to determine the phase of oscillator i for $i \in \mathcal{N}_f$ at time instant $t_1 + \varepsilon$. Since every oscillator i jumped at least once within $(t_1 + \varepsilon/2, t_1 + \varepsilon]$, we denote $\hat{t}_i \in (t_1 + \varepsilon/2, t_1 + \varepsilon]$ as the time instant of oscillator i 's first jump within $(t_1 + \varepsilon/2, t_1 + \varepsilon]$. So the phase of oscillator i immediately before the jump at \hat{t}_i is $\phi_i(\hat{t}_i) = \phi_i(t_1 + \varepsilon/2) + \hat{t}_i - (t_1 + \varepsilon/2)$. According to the PRF in (2), the phase of oscillator i immediately after the jump at \hat{t}_i can be obtained as

$$\begin{aligned}\phi_i^+(\hat{t}_i) &= (1 - l)\phi_i(\hat{t}_i) \\ &= (1 - l)(\phi_i(t_1 + \varepsilon/2) + \hat{t}_i - (t_1 + \varepsilon/2))\end{aligned}$$

Noting that the PRF in (2) is non-positive on $[0, \pi]$ and oscillator i can be triggered to jump multiple times within $(t_1 + \varepsilon/2, t_1 + \varepsilon]$, the phase of oscillator i at $t_1 + \varepsilon$ satisfies

$$\begin{aligned}\phi_i(t_1 + \varepsilon) &\leq \phi_i^+(\hat{t}_i) + (t_1 + \varepsilon) - \hat{t}_i \\ &\leq (1 - l)\phi_i(t_1 + \varepsilon/2) + \varepsilon/2 + (t_1 + \varepsilon/2 - \hat{t}_i)l\end{aligned}\quad (12)$$

Substituting $\phi_i(t_1 + \varepsilon/2) \in [0, \varepsilon/2]$ and $\hat{t}_i \in (t_1 + \varepsilon/2, t_1 + \varepsilon]$ into (12) leads to $\phi_i(t_1 + \varepsilon) \in [0, (1 - l/2)\varepsilon]$ for $i \in \mathcal{N}_f$. In combination with the fact $\phi_j(t_1 + \varepsilon) \in [0, \varepsilon/2]$ for $j \in \mathcal{N}_n$ in (11) and $l \in (0, 1]$, we have that the phases of all oscillators reside in $[0, (1 - l/2)\varepsilon]$ at time $t_1 + \varepsilon$, i.e., $\delta(t_1 + \varepsilon) \leq (1 - l/2)\delta(t_1)$.

In summary, we have $\delta(t_1 + \varepsilon) \leq (1 - l/2)\delta(t_1)$ in all three *Scenarios 1.1, 1.2, and 1.3*. At $t_1 + \varepsilon$, all oscillators reside

in $[0, \pi]$ and will evolve towards phase 2π rad and fire. By repeating the above analyses, we can get that the length of the containing arc $\delta(t)$ decreases to a value no greater than $(1 - l/2)\delta(t)$ after each round of firing until it converges to 0. Therefore, synchronization can be achieved in Case 1.

Case 2 ($\pi/2 \leq \varepsilon < \pi$): Similar to the reasoning in *Case 1*, there exists a time instant $t_0 > 2T$ at which the ending and starting points of the containing arc reside on phases 0 and $\pi/2 \leq \varepsilon < \pi$ rad, respectively. After t_0 , all oscillators evolve freely for exactly $T - \varepsilon > T/2$ seconds before the starting point of the containing arc reaches phase 2π rad at $t_1 = t_0 + T - \varepsilon$. At t_1 , the ending point of the containing arc resides on phase $2\pi - \varepsilon$ rad and we have $\delta(t_1) = \delta(t_0) = \varepsilon$.

Given that the PRF in (2) is non-negative on $[2\pi - \varepsilon, 2\pi]$, a pulse can only trigger a forward jump or have no effect on an oscillator with phase residing in $[2\pi - \varepsilon, 2\pi]$. So all oscillators will reach phase 2π rad and fire no later than time instant $t_1 + \varepsilon$ and within $[t_1, t_1 + \varepsilon/2]$, only one of the following three scenarios can happen:

Scenario 2.1: all oscillators fired within $[t_1, t_1 + \varepsilon/2]$;

Scenario 2.2: some oscillators did not fire within $[t_1, t_1 + \varepsilon/2]$ but all of these oscillators jumped in phase within $[t_1, t_1 + \varepsilon/2]$;

Scenario 2.3: some oscillators neither fired nor jumped in phase within $[t_1, t_1 + \varepsilon/2]$.

Next, we show that $\delta(t)$ will decrease to less than $\pi/2$ rad in finite time, meaning that *Case 2* will shift to *Case 1* in finite time. Therefore, $\delta(t)$ will also converge to 0 for $\pi/2 \leq \varepsilon < \pi$.

Similar to *Case 1*, we label all oscillators in an increasing order of their phases at t_1 , i.e., $2\pi - \varepsilon = \phi_1(t_1) \leq \phi_2(t_1) \leq \dots \leq \phi_N(t_1) = 2\pi$ and denote \mathcal{N}_f (respectively \mathcal{N}_n) as the index set of oscillators fired (respectively did not fire) in $[t_1, t_1 + \varepsilon/2]$. Following the same line of reasoning as in *Scenario 1.1* and *Scenario 1.2*, one can easily obtain $\delta(t_1 + \varepsilon) \leq (1 - l/2)\delta(t_1)$ in *Scenario 2.1* and *Scenario 2.2*, respectively. For *Scenario 2.3*, i.e., some oscillators neither fired nor jumped in phase within $[t_1, t_1 + \varepsilon/2]$, we assume oscillator j' is such an oscillator. According to Mechanism 1, there could be two reasons for the not firing of oscillator j' in $[t_1, t_1 + \varepsilon/2]$:

Scenario 2.3.1: oscillator j' receives no greater than $\lambda_{j'}$ pulses within $[t_1, t_1 + \varepsilon/2]$, i.e., condition *b*) of Mechanism 1 is not satisfied;

Scenario 2.3.2: oscillator j' receives over $\lambda_{j'}$ pulses within $[t_1, t_1 + \varepsilon/2]$, but the number of pulses it received within the past period of length $3T/4$ is no less than $\bar{\lambda}_{j'}$, i.e., condition *c*) of Mechanism 1 is not satisfied.

Next, we show that in both scenarios, the length of the containing arc will keep decreasing to less than $(1 - l/2)$ of its original value.

Scenario 2.3.1: Following the same line of reasoning as in *Scenario 1.3*, all oscillators' phases reside in $[0, (1 - l/2)\varepsilon]$ at time instant $t_1 + \varepsilon$, which means $\delta(t_1 + \varepsilon) \leq (1 - l/2)\delta(t_1)$.

Scenario 2.3.2: In this case, we cannot prove length decrease in the containing arc by focusing on the time interval $[t_0, t_1 + \varepsilon]$ (one firing round), so we extend our considered time span to two firing rounds. Without loss of generality, we assume that

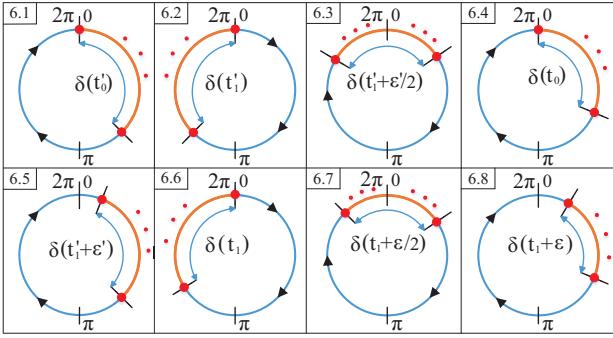


Figure 6: Phase distributions of all oscillators at different time instants in *Scenario 2.3.2*.

the previous firing round starts at $t'_0 < t_0$ at which the ending and starting points of the containing arc reside on phases 0 and ε' rad, respectively (as depicted in Fig. 6.1). As the containing arc is non-increasing (Lemma 1), we have $\varepsilon \leq \delta(t'_0) = \varepsilon' < \pi$. After t'_0 , all oscillators evolve freely for exactly $2\pi - \varepsilon' > T/2$ seconds before the starting point of the containing arc reaches phase 2π rad at time $t'_1 = t'_0 + 2\pi - \varepsilon'$ (as depicted in Fig. 6.2). At t'_1 , the ending point of the containing arc resides on phase $2\pi - \varepsilon'$ rad and we have $\delta(t'_1) = \delta(t'_0) = \varepsilon'$.

Given that the PRF in (2) is non-negative on $[2\pi - \varepsilon', 2\pi]$, a pulse can only trigger a forward jump or have no effect on an oscillator with phase residing in $[2\pi - \varepsilon', 2\pi]$. So all oscillators will reach phase 2π rad and fire no later than $t'_1 + \varepsilon'$. The phases of all oscillators at $t'_1 + \varepsilon'$ should follow the pattern depicted in Fig. 6.5. Next, we prove $\delta(t'_1 + \varepsilon') \leq (1 - l/2)\delta(t'_1)$. To this end, we need to characterize the number of oscillators fired within $[t'_1, t'_1 + \varepsilon'/2]$. The phases of all oscillators follow the pattern depicted in Fig. 6.3 at time instant $t'_1 + \varepsilon'/2$. We denote \mathcal{N}'_f (respectively \mathcal{N}'_n) as the index set of oscillators fired (respectively did not fire) within $[t'_1, t'_1 + \varepsilon'/2]$ and analyze the numbers of oscillators in the two sets.

Recall that in *Scenario 2.3.2*, condition *c*) of Mechanism 1 is not satisfied. So oscillator j' should receive at least $\bar{\lambda}_{j'} - \lambda_{j'}$ pulses within $(t_1 - 3T/4, t_1)$. Since no oscillators fired within (t_0, t_1) , the number of oscillators fired in $(t_1 - 3T/4, t_0]$ is at least $\bar{\lambda}_{j'} - \lambda_{j'}$. Next, by proving $(t_1 - 3T/4, t_0] \subseteq (t'_1 + \varepsilon'/2, t'_1 + \varepsilon']$, we show that the number of oscillators fired in $(t'_1 + \varepsilon'/2, t'_1 + \varepsilon']$ is no less than $\bar{\lambda}_{j'} - \lambda_{j'}$. As indicated earlier, all oscillators will reach phase 2π rad and fire no later than $t'_1 + \varepsilon'$. So we have $t_0 \leq t'_1 + \varepsilon'$. On the other hand, since the starting point of the containing arc resides on phase $\pi/2 \leq \varepsilon < \pi$ at t_0 and the PRF in (2) is non-positive on $[0, \varepsilon]$, oscillators having phase in $[0, \varepsilon]$ will not be advanced by incoming pulses. So it takes an oscillator at least ε time to evolve from 0 to ε rad. Therefore, we can obtain $t_0 - t'_1 \geq \varepsilon$. Given $\varepsilon' < \pi = T/2$ and $t_1 = t_0 + T - \varepsilon$, one can get

$$t'_1 + \varepsilon'/2 \leq t_0 - \varepsilon + \varepsilon'/2 < t_0 - \varepsilon + T/4 = t_1 - 3T/4$$

and hence $(t_1 - 3T/4, t_0] \subseteq (t'_1 + \varepsilon'/2, t'_1 + \varepsilon']$, implying that at least $\bar{\lambda}_{j'} - \lambda_{j'}$ oscillators fired within $(t'_1 + \varepsilon'/2, t'_1 + \varepsilon']$. According to the definition of $\lambda_{j'}$ and $\bar{\lambda}_{j'}$ in (3) and (4), we have $4\lambda_{j'} \leq d(j') - \lfloor N/2 \rfloor$ and $\bar{\lambda}_{j'} - \lambda_{j'} = d(j') - 3\lambda_{j'}$, which further lead to $d(j') - 3\lambda_{j'} \geq \lfloor N/2 \rfloor + \lambda_{j'}$. Given $\lambda_{j'} \geq 0$

and $d(j') > \lfloor N/2 \rfloor$, we always have $d(j') - 3\lambda_{j'} \geq \lfloor N/2 \rfloor + 1$. Therefore, the number of oscillators in \mathcal{N}'_f is at least $\lfloor N/2 \rfloor + 1$ and the number of oscillators in \mathcal{N}'_n is at most $N - (\lfloor N/2 \rfloor + 1)$, which is no greater than $\lfloor N/2 \rfloor$.

Based on obtained knowledge of the numbers of oscillators in \mathcal{N}'_f and \mathcal{N}'_n , respectively, we can characterize the phases of all oscillators at time instant $t'_1 + \varepsilon'$. Following the same line of reasoning as in *Scenario 1.3*, one can obtain that all oscillators' phases reside in $[0, (1 - l/2)\varepsilon']$ at time instant $t'_1 + \varepsilon'$, which means $\delta(t'_1 + \varepsilon') \leq (1 - l/2)\delta(t'_1)$. Note that proving such a length decrease of the containing arc requires a careful characterization of phase evolution starting from t'_0 to $t_1 + \varepsilon$, which spans two consecutive firing rounds. After $t_1 + \varepsilon$, the phase evolution could follow *Scenario 2.1*, *Scenario 2.2*, *Scenario 2.3.1* (in which we can prove such $(1 - l/2)$ length decrease after each round of firing) or *Scenario 2.3.2* (in which we can prove such $(1 - l/2)$ length decrease after every two consecutive firing rounds).

In summary, we can prove that the length of the containing arc will reduce to $(1 - l/2)$ of its original value after every firing round in *Scenarios 2.1*, *2.2*, and *2.3.1*, whereas in *Scenario 2.3.2*, we can prove such a decrease after every two consecutive firing rounds. Since every oscillator will fire at least once within any time interval of length $3T/2$ according to Lemma 2, we can get that the length of the containing arc $\delta(t)$ will decrease to a value less than $\pi/2$ rad within finite time (in fact, after at most $2m$ firing rounds with m satisfying $(1 - l/2)^m \delta(t_0) < \pi/2$). And then, the containing arc will keep decreasing to 0 following the derivations in *Case 1*.

By combining *Case 1* and *Case 2*, one can obtain that $\delta(t)$ will always converge to 0 under the conditions of Theorem 1. ■

Corollary 1: Under conditions in Theorem 1, Mechanism 1 guarantees that all oscillators synchronize with an oscillation period $T = 2\pi$ seconds in the absence of attacks.

Proof: The result can be easily obtained from the reasoning in the proof of Theorem 1 and hence is omitted. ■

Remark 3: Besides enabling attack resilience, Mechanism 1 also has better robustness against time-varying delays. For example, numerical simulations in Fig. 15 and Fig. 16 show that Mechanism 1 has much smaller synchronization errors compared with synchronization mechanisms in [37]–[39] when the communication is subject to random time-varying delays.

IV. STEALTHY BYZANTINE ATTACKS AND ATTACK DETECTION MECHANISM

The concept of Byzantine attacks stems from the Byzantine generals problem [41]. It was used to describe a traitor commander who sends or relays fake information to other commanders to avoid the loyal ones from reaching agreement [30]. In the case of PCO synchronization, a node compromised by Byzantine attacks can emit malicious pulses at arbitrary time instants. However, given that the purpose of Byzantine attacks is to delay or damage the synchronization of legitimate oscillators, we assume that a compromised oscillator sends malicious pulses only when such pulses can negatively affect the

synchronization process of legitimate oscillators, i.e., enlarge the containing arc of affected legitimate oscillators.

A compromised node decides the timing of its malicious pulses based on information of other oscillator's phases that it can perceive from received pulses. Given that in a general connected PCO network, an oscillator can only receive pulses from its neighbors, a compromised oscillator can only perceive phase information of nodes that it can receive pulses from and decide its optimal attacking strategy accordingly.

We consider two types of attacks, non-colluding attacks and colluding attacks. In non-colluding attacks, an attacker determines its attacking strategy based on its own neighbors' phase information. In colluding attacks, two attackers can share perceived phase information about each other's neighbors, which is equivalent to expanding the neighbor sets of both attackers to the union of their neighbor sets. The same concept can be extended to three or more colluding attackers.

Now we proceed to discuss the attacking strategy. If an attacker keeps sending pulses continuously without rest, it can effectively prevent legitimate oscillators from reaching synchronization. However, such attacks are not energy efficient and will also render themselves easily detectable, just as jamming of communication channels being easy to detect, isolate, and remove [42]. Therefore, we are only interested in "stealthy" Byzantine attacks, in which attack pulses are emitted in a way that cannot be detected by legitimate oscillators in the pulse-based interaction framework.

In PCO networks, since all exchanged pulses are identical without embedded content such as source or destination information, conventional content-checking based attack-detection mechanisms such as [1] are inapplicable. We propose to let each oscillator 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 in the absence of attacks.

Lemma 3: For a general connected network of N legitimate PCOs, under Mechanism 1, an oscillator i can receive at most $d^-(i)$ pulses within any time interval $[t, t + T/2]$ for $t \geq 0$ where $d^-(i)$ is the indegree of oscillator i .

Proof: Noting that the number of edges entering oscillator i is $d^-(i)$ in the considered general connected PCO network, Lemma 3 can be obtained following the same line of reasoning as in Theorem 3 of [39]. ■

Based on Lemma 3, we have, under the pulse-number based detection mechanism, that oscillator i 's receiving more than $d^-(i)$ pulses within an arbitrary time interval $[t, t + T/2]$ implies the presence of attackers among its neighbors. Therefore, to keep stealthy, one compromised oscillator should launch stealthy attacks by sending pulses with a time separation over $T/2$ seconds.

From the above analysis, we summarize the attacking models as follows:

In non-colluding attacks, a Byzantine attacker emits an

attack pulse only when the pulse can enlarge the containing arc of its neighbors. In addition, to keep stealthy, every individual attacker sends malicious pulses with a time separation over $T/2$ seconds.

In colluding attacks, a Byzantine attacker emits an attack pulse either when the pulse can enlarge the containing arc of the union set of colluding attackers' neighbor sets, or when the pulse can help other attack pulse to do so.

V. SYNCHRONIZATION OF PCO NETWORKS UNDER STEALTHY BYZANTINE ATTACKS

In this section, we address the synchronization of general connected PCO networks in the presence of stealthy Byzantine attacks. Among N PCOs, we assume that M are compromised and act as stealthy Byzantine attackers. We first show that the proposed pulse-based synchronization mechanism (Mechanism 1) can synchronize legitimate oscillators when attackers do not collude, i.e., every attacker determines its attacking strategy based on its own neighbors' phase information. Then we further prove that all legitimate oscillators can still be synchronized even when attackers collude with each other, i.e., attackers can exchange phase information of their neighbors. To this end, we first analyze the phase evolution of legitimate oscillators in the presence of non-colluding attackers.

Lemma 4: For a general connected network of N PCOs, within which $M \leq 2 \times \lfloor (d - \lfloor N/2 \rfloor)/4 \rfloor$ oscillators are compromised non-colluding attackers launching attacks following the stealthy Byzantine attack model in Section IV, if the initial length of the containing arc of legitimate oscillators is less than π and $d > \lfloor N/2 \rfloor$, then under Mechanism 1, the $N - M$ legitimate oscillators encounter attack pulses only when their phases reside partially in $[0, \pi]$, partially in $(\pi, 2\pi]$ with phase 2π belonging to the containing arc.

Proof: According to Mechanism 1, all legitimate oscillators will evolve freely for an entire period $T = 2\pi$. Since the initial length of the containing arc is assumed to be less than π , the possible phase distribution of all legitimate oscillators immediately after the initial period of free evolution can only fall within one of the following four scenarios, as depicted in Fig. 3:

- I) all legitimate oscillators' phases reside in $[0, \pi]$;
- II) legitimate oscillators' phases reside partially in $(0, \pi]$, partially in $(\pi, 2\pi]$ with phase π belonging to the containing arc;
- III) all legitimate oscillators' phases reside in $(\pi, 2\pi]$;
- IV) legitimate oscillators' phases reside partially in $[0, \pi]$, partially in $(\pi, 2\pi]$ with phase 2π belonging to the containing arc.

Since in non-colluding attacks, an attacker will emit an attack pulse only when the pulse can enlarge the containing arc of its legitimate neighbors, every attack pulse will trigger a phase shift on at least one legitimate oscillator. Next, we prove that an attacker can trigger a legitimate oscillator (say oscillator j) to jump in phase only under Scenario IV).

- I) All legitimate oscillators' phases reside in $[0, \pi]$. Without loss of generality, we assume that legitimate oscillator k fires last among all legitimate oscillators at time instant

t_k . One can easily get that all legitimate oscillators fired in the past $T/2$ seconds prior to t_k . Recalling $d \triangleq \min_{i=1,2,\dots,N} \{d(i)\}$, we have $M \leq 2 \times \lfloor (d - \lfloor N/2 \rfloor)/4 \rfloor \leq 2 \times \lfloor (d(i) - \lfloor N/2 \rfloor)/4 \rfloor = 2\lambda_i$. Hence, immediately after the firing of oscillator k , legitimate oscillator i has received at least $d(i) - M \geq \bar{\lambda}_i$ legitimate pulses during $[t_k - T/2, t_k]$ for $i \in \mathcal{N}_L$ where \mathcal{N}_L is the index set of all legitimate oscillators. According to Mechanism 1, if legitimate oscillator i received no less than $\bar{\lambda}_i$ pulses within the past $3T/4$, no pulse can trigger oscillator i to jump in phase. Hence, immediately after the firing of legitimate oscillator k , all legitimate oscillators will evolve freely for $T/4$ and no pulses can trigger a legitimate oscillator to jump in phase within this period. After this quarter period, legitimate oscillators will not emit pulses before the network shifts to Scenario II) and the number of attacker pulses is not enough to trigger a legitimate oscillator to jump in phase. Given that an attacker sends pulses only when the containing arc of its legitimate neighbors can be enlarged, no attack pulse will be emitted in this scenario.

- II) Legitimate oscillators' phases reside partially in $(0, \pi]$, partially in $(\pi, 2\pi]$ with phase π belonging to the containing arc. Following the same line of reasoning as in Scenario I), one can get that no legitimate oscillators reach phase 2π and fire in this scenario. Because no attack pulse can shift the phase of a legitimate oscillator, no attacker will emit attack pulses in this scenario.
- III) All legitimate oscillators' phases reside in $(\pi, 2\pi]$. One can get that no legitimate oscillators fire in the past $T/4$. Since the number of attacker pulses is not enough to trigger a legitimate oscillator to jump in phase, no attacker will emit attack pulses in this scenario.
- IV) Legitimate oscillators' phases reside partially in $[0, \pi)$, partially in $(\pi, 2\pi]$ with phase 2π belonging to the containing arc. One can get that a portion of legitimate oscillators fired in the past $T/4$ in this scenario. So an attacker may be able to emit an attack pulse at a right time instant to trigger legitimate neighbors to jump in phase and enlarge the containing arc of its legitimate neighbors.

By iterating the above analysis, we can get that an attacker will emit an attack pulse to shift the phase of a legitimate oscillator only when legitimate oscillators' phases reside partially in $[0, \pi)$, partially in $(\pi, 2\pi]$ with phase 2π rad belonging to the containing arc. ■

Next, we establish the synchronization condition for general connected PCO networks in the presence of non-colluding stealthy Byzantine attackers.

Theorem 2: For a general connected network of N PCOs, within which $M \leq 2 \times \lfloor (d - \lfloor N/2 \rfloor)/4 \rfloor$ oscillators are compromised non-colluding attackers launching attacks following the stealthy Byzantine attack model in Sec IV, if the initial length of the containing arc of legitimate oscillators is less than π rad and $d > \lfloor N/2 \rfloor$, then the containing arc of legitimate oscillators will converge to zero under Mechanism 1.

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

converges 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 oscillators jump in phase. So we only consider the case where a pulse (from either a legitimate oscillator or an attacker) triggers a phase jump on a legitimate oscillator.

As no legitimate oscillators will be triggered to jump in phase in the first free-running period, we only consider pulses sent after $t = T$. We will show that for any pulse sent at $t_i > T$, the length of the containing arc of legitimate oscillators is non-increasing.

When the pulse is from a legitimate oscillator i , we have $\phi_i(t_i) = 2\pi$, i.e., at t_i the containing arc of legitimate oscillators includes phase 2π rad. Following the same line of reasoning as in Lemma 1, one can obtain that the pulse cannot increase the length of the containing arc of legitimate oscillators.

When the pulse is from an attacker, according to Lemma 4, the pulse can only be sent when legitimate oscillators' phases reside partially in $[0, \pi)$, partially in $(\pi, 2\pi]$ with phase 2π rad belonging to the containing arc. Following the same line of reasoning as in Scenario c) of Lemma 1, one can obtain that the length of the containing arc of all legitimate oscillators cannot be increased by the attack pulse, although the containing arc of a subset of legitimate oscillators (an attacker's neighbor set) will be enlarged, as confirmed later in the numerical simulations in Fig. 9. Hence, we can conclude that the length of the containing arc of all legitimate oscillators is non-increasing.

Part II (The length of the containing arc of legitimate oscillators converges to 0): First, we prove that every legitimate oscillator will fire at least once within any time interval of length $3T/2$. According to the argument in Lemma 4, attack pulses will only be emitted when legitimate oscillators' phases reside partially in $[0, \pi)$, partially in $(\pi, 2\pi]$ with phase 2π rad belonging to the containing arc. Following the same line of reasoning as in Lemma 2, we can easily get that every legitimate oscillator will fire at least once within any time interval of length $3T/2$.

Next, we prove that the length of the containing arc of legitimate oscillators will decrease to 0. Without loss of generality, we denote $\delta(t)$ as the length of the containing arc of legitimate oscillators at t and set the initial time to $t = 0$. According to the argument in Part I, we have that $\delta(t)$ is non-increasing and $0 \leq \delta(t) < \pi$ for $t \geq 0$. Since every legitimate oscillator will fire at least once within any time interval of length $3T/2$, there exists a time instant $t_0 > 2T$ at which the ending point of the containing arc of legitimate oscillators resides at phase 0. Denoting the starting point of the containing arc at t_0 as $0 \leq \varepsilon < \pi$, we have $\delta(t_0) = \varepsilon$. Next, we separately discuss the $0 \leq \varepsilon < \pi/2$ case and the $\pi/2 \leq \varepsilon < \pi$ case to prove the convergence of $\delta(t)$ to 0.

Case I ($0 \leq \varepsilon < \pi/2$): If ε is 0, the network is synchronized. So we only consider $0 < \delta(t_0) < \pi/2$. At time instant t_0 , the ending and starting points of the containing arc of legitimate oscillators reside on phases 0 and $0 < \varepsilon < \pi/2$ rad, respectively. According to Lemma 4, attack pulses are emitted

only when legitimate oscillators' phases reside partially in $[0, \pi]$, partially in $(\pi, 2\pi]$ with phase 2π rad belonging to the containing arc. So after t_0 , all legitimate oscillators will evolve freely without perturbation for exactly $T - \varepsilon > 3T/4$ seconds before the starting point of the containing arc reaches phase 2π rad at time $t_1 = t_0 + T - \varepsilon$. At t_1 , the ending point of the containing arc resides on phase $2\pi - \varepsilon$ rad and we have $\delta(t_1) = \delta(t_0) = \varepsilon$. Given that the PRF in (2) is non-negative on $[2\pi - \varepsilon, 2\pi]$, a pulse can only trigger a forward jump or have no effect on a legitimate oscillator with phase residing in $[2\pi - \varepsilon, 2\pi]$. All legitimate oscillators will reach phase 2π rad and fire no later than $t_1 + \varepsilon$ and within $[t_1, t_1 + \varepsilon/2]$, we can only have one of the following three scenarios:

Scenario I.1: all legitimate oscillators fired within $[t_1, t_1 + \varepsilon/2]$;

Scenario I.2: some legitimate oscillators did not fire within $[t_1, t_1 + \varepsilon/2]$ but all of these legitimate oscillators jumped in phases within $[t_1, t_1 + \varepsilon/2]$;

Scenario I.3: some legitimate oscillators neither fired nor jumped in phase within $[t_1, t_1 + \varepsilon/2]$.

Next, we prove $\delta(t_1 + \varepsilon) \leq (1 - l/2)\delta(t_1)$ in all above three scenarios, based on which we can further prove such a length decrease of containing arc of legitimate oscillators after each round of firing and hence the convergence of $\delta(t)$ to zero.

Following the same line of reasoning as in *Scenarios I.1, I.2, and I.3* of Theorem 1 and using the fact that the number of attackers M is no greater than $2 \times \lfloor (d - \lfloor N/2 \rfloor)/4 \rfloor$, we can obtain $\delta(t_1 + \varepsilon) \leq (1 - l/2)\delta(t_1)$ in *Scenarios I.1, I.2, and I.3*, respectively. At $t_1 + \varepsilon$, all legitimate oscillators reside in $[0, \pi]$ and will evolve towards phase 2π rad and fire. By repeating the above analyses, we can get that the length of the containing arc of legitimate oscillators $\delta(t)$ will decrease to a value no greater than $(1 - l/2)\delta(t)$ after each round of firing until it converges to 0.

Case II ($\pi/2 \leq \varepsilon < \pi$): Similar to the reasoning in *Case I*, there exists a time instant $t_0 > 2T$ at which the ending and starting points of the containing arc of legitimate oscillators reside on phases 0 and $\pi/2 \leq \varepsilon < \pi$ rad, respectively. After t_0 , all legitimate oscillators will evolve freely for exactly $T - \varepsilon > T/2$ seconds before the starting point of the containing arc of legitimate oscillators reaches phase 2π rad at time $t_1 = t_0 + T - \varepsilon$. At t_1 , the ending point of the containing arc resides on phase $2\pi - \varepsilon$ rad and we have $\delta(t_1) = \delta(t_0) = \varepsilon$. As the PRF in (2) is non-negative on $[2\pi - \varepsilon, 2\pi]$, a pulse can only trigger a forward jump or have no effect on a legitimate oscillator with phase in $[2\pi - \varepsilon, 2\pi]$. So all legitimate oscillators will reach phase 2π rad and fire no later than $t_1 + \varepsilon$ and within $[t_1, t_1 + \varepsilon/2]$, we can only have one of the following three scenarios:

Scenario II.1: all legitimate oscillators fired within $[t_1, t_1 + \varepsilon/2]$;

Scenario II.2: some legitimate oscillators did not fire within $[t_1, t_1 + \varepsilon/2]$ but all of these legitimate oscillators jumped in phase within $[t_1, t_1 + \varepsilon/2]$;

Scenario II.3: some legitimate oscillators neither fired nor jumped in phase within $[t_1, t_1 + \varepsilon/2]$.

Next, we show that $\delta(t)$ will reduce to less than $\pi/2$ rad in finite time, i.e., *Case II* will shift to *Case I* in finite time, after which $\delta(t)$ will converge to zero, as ready proven in *Case I*.

Following the same line of reasoning as in *Scenario 2.1* and *Scenario 2.2* of Theorem 1, one can obtain $\delta(t_1 + \varepsilon) \leq (1 - l/2)\delta(t_1)$ in *Scenario II.1* and *Scenario II.2*, respectively. For *Scenario II.3*, i.e., some legitimate oscillators neither fired nor jumped in phase within $[t_1, t_1 + \varepsilon/2]$, we assume legitimate oscillator j' is such an oscillator. According to Mechanism 1, there could be two reasons for the not firing of oscillator j' in $[t_1, t_1 + \varepsilon/2]$:

Scenario II.3.1: legitimate oscillator j' receives no greater than $\lambda_{j'}$ pulses within $[t_1, t_1 + \varepsilon/2]$, i.e., condition *b*) of Mechanism 1 is not satisfied;

Scenario II.3.2: legitimate oscillator j' receives over $\lambda_{j'}$ pulses within $[t_1, t_1 + \varepsilon/2]$, but the number of pulses it received within the past period of length $3T/4$ is no less than $\bar{\lambda}_{j'}$, i.e., condition *c*) of Mechanism 1 is not satisfied.

Still following the same line of reasoning as in *Scenario 2.3.1* and *Scenario 2.3.2* of Theorem 1 and using the fact that the number of attackers M is no greater than $2 \times \lfloor (d - \lfloor N/2 \rfloor)/4 \rfloor$, we can obtain in *Scenario II.3.1* that the length of the containing arc of legitimate oscillators will reduce to $(1 - l/2)$ of its original value after every firing round whereas in *Scenario II.3.2* such a reduction occurs after every two consecutive firing rounds.

Since every legitimate oscillator will fire at least once within any time interval of length $3T/2$ according to the reasoning at the beginning of Part II, we can get that the length of the containing arc of legitimate oscillators $\delta(t)$ will always decrease to a value less than $\pi/2$ rad within finite time (in fact, after at most $2m$ firing rounds with m satisfying $(1 - l/2)^m \delta(t_0) < \pi/2$), after which it will converge to zero according to the argument in *Case I*.

By combining *Case I* and *Case II*, one can obtain that the containing arc of legitimate oscillators $\delta(t)$ will always converge to 0 even in the presence of attackers. ■

Corollary 2: Under conditions in Theorem 2, Mechanism 1 guarantees that all legitimate oscillators synchronize with an oscillation period $T = 2\pi$ seconds even in the presence of attacks.

Proof: According to the proof of Theorem 2, we know that despite the presence of attacks, the containing arc of legitimate oscillators will shrink to 0 upon which the phases of legitimate oscillators will not be affected by attack pulses. Therefore, Mechanism 1 can guarantee the $T = 2\pi$ seconds oscillation period even in the presence of attacks. ■

Next, we prove that Mechanism 1 can guarantee synchronization of general connected PCO network even when attackers collude with each other and exchange perceived phase information of their neighbors. In this situation, an attacker will emit a malicious pulse either when the pulse can enlarge the containing arc of the union set of colluding attackers' neighbor sets, or when the pulse can help other attack pulse to do so.

To facilitate the analysis, we first characterize the phase evolution of legitimate oscillators in the presence of colluding attackers.

Lemma 5: For a general connected network of N PCOs, within which $M \leq \lfloor (d - \lfloor N/2 \rfloor)/4 \rfloor$ oscillators are compromised colluding attackers launching attacks following the stealthy Byzantine attack model in Section IV, if the initial length of the containing arc is less than π rad and $d > \lfloor N/2 \rfloor$, then under Mechanism 1, the $N - M$ legitimate oscillators will encounter attack pulses only when their phases reside partially in $[0, \pi)$, partially in $(\pi, 2\pi]$ with phase 2π rad belonging to the containing arc.

Proof: Similar to Lemma 4, we know that the phase distribution of legitimate oscillators after the first free-running period can only fall within one of the four scenarios in Fig. 3.

According to the stealth Byzantine attack model in Section IV, we know that M attackers can emit at most M attack pulses in a quarter period. Given $M \leq \lfloor (d - \lfloor N/2 \rfloor)/4 \rfloor \leq \lfloor (d(i) - \lfloor N/2 \rfloor)/4 \rfloor = \lambda_i$ for $i \in \mathcal{N}_L$ where \mathcal{N}_L is the index set of all legitimate oscillators, we know from Mechanism 1 that attacks pulses alone are not enough to trigger a legitimate oscillator to jump in phase. Therefore, following an argument similar to Lemma 4, we know that to enlarge the containing arc of legitimate neighbors, attack pulses are sent only when the phases of legitimate oscillators reside partially in $[0, \pi)$, partially in $(\pi, 2\pi]$ with phase 2π rad belonging to the containing arc. ■

Next, we establish the synchronization condition for general connected PCO networks in the presence of colluding attackers.

Theorem 3: For a general-connected network of N PCOs, within which $M \leq \lfloor (d - \lfloor N/2 \rfloor)/4 \rfloor$ oscillators are colluding attackers launching attacks following the stealthy Byzantine attack model in Sec. IV, if the initial length of the containing arc is less than π rad and $d > \lfloor N/2 \rfloor$, then all legitimate oscillators can be synchronized under Mechanism 1.

Proof: Similar to the proof in Theorem 2, we divide the proof into two parts. In Part I, we prove that the length of the containing arc of legitimate oscillators is non-increasing. In Part II, we prove that it will converge 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 oscillators jump in phase. So we only consider the case where a pulse (from either a legitimate oscillator or an attacker) triggers a phase jump on a legitimate oscillator.

Following the same line of reasoning as in Theorem 2, one can easily get that the firing of a legitimate oscillator cannot increase the length of the containing arc of legitimate oscillators. By combining Lemma 1 and Lemma 5, we can also obtain that no attacker pulses can increase the length of the containing arc of legitimate oscillators, although the containing arc of a subset of legitimate oscillators (the union set of colluding attackers' neighbor sets) may be enlarged. Hence, we can conclude that the length of the containing arc of all legitimate oscillators is non-increasing.

Part II (The length of the containing arc of legitimate oscillators converges to 0): The proof follows the same reasoning as in Part II of Theorem 2 and is omitted. ■

Remark 4: It is worth noting that the maximally allowable number of attackers in a PCO network is $2 \times \lfloor (d - \lfloor N/2 \rfloor)/4 \rfloor$ when attackers do not collude with each other, which is greater than the maximally allowable number of compromised oscillators $\lfloor (d - \lfloor N/2 \rfloor)/4 \rfloor$ when attackers collude and exchange information.

In the colluding case, some attackers can emit attack pulses even if these pulses themselves do not enlarge the containing arc (as long as these pulses can help other attack pulses to enlarge the containing arc). In fact, even if all attackers are allowed to send attack pulses when the containing arc does not change, they still cannot prevent legitimate pulses from satisfying condition (4) to decrease the length of the containing arc.

Corollary 3: For a general connected network of N PCOs, within which $M \leq \lfloor (d - \lfloor N/2 \rfloor)/4 \rfloor$ colluding attackers have the ability to emit attack pulses not only when their pulses can enlarge the length of the containing arc but also when the pulses do not change the containing arc, if the initial length of the containing arc of all legitimate oscillators is less than π rad and $d > \lfloor N/2 \rfloor$, then there always exist legitimate pulses satisfying (4) in Mechanism 1.

Proof: According the stealthy requirement in Sec. IV, $M \leq \lfloor (d - \lfloor N/2 \rfloor)/4 \rfloor$ attackers can emit at most $2M$ attack pulses within an arbitrary three-quarter oscillation period. Since $2M$ is less than $\bar{\lambda}_i$, one can get that (4) cannot be made unsatisfied for all legitimate pulses. ■

Remark 5: Following Corollary 3 and the proof in Theorem 2, one can get that there always exist legitimate pulses satisfying condition (4), which will reduce the length of the containing arc, even though attackers can ensure that all their attack pulses do not change the length of the containing arc of legitimate oscillators. Hence, attackers cannot prevent legitimate oscillators from reaching synchronization by holding the containing arc constant.

VI. EXTENSION TO THE CASE WHERE N IS UNKNOWN TO INDIVIDUAL OSCILLATORS

The implementation of the “cut-off” algorithm in Mechanism 1 requires each node to have access to N , which may be not feasible in a completely decentralized network. Therefore, in this section, we generalize our approach to the case where N is unknown to individual oscillators by leveraging the degree information of individual oscillators. The essence is a new “cut-off” mechanism that is designed based on the degree information of individual oscillators, as detailed below:

New Pulse-Based Synchronization Mechanism (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 and resets its phase to 0.

- 3) When oscillator i receives a pulse at time instant t , it simultaneously resets its phase according to (1) only when all the following three conditions are satisfied:
- an entire period $T = 2\pi$ seconds has elapsed since initiation.
 - before receiving the current pulse, oscillator i has received at least $\lfloor d(i)/9 \rfloor$ pulses within $(t - T/4, t]$, where $\lfloor \bullet \rfloor$ is the largest integer no greater than “ \bullet ”.
 - before receiving the current pulse, oscillator i has received less than $d(i) - 2 \times \lfloor d(i)/9 \rfloor$ pulses within $(t - 3T/4, t]$.

Otherwise, the pulse has no effect on ϕ_i .

Following a similar line of reasoning in Section III and Section V, we can prove that Mechanism 2 can synchronize legitimate oscillators both in the absence and presence of attackers.

Corollary 4: For an attack-free general-connected network of N PCOs, if the degree of the network satisfies $d > \lfloor 2N/3 \rfloor$ and the initial length of the containing arc is less than π rad, then all oscillators can be synchronized under Mechanism 2.

Proof: Proof of Corollary 4 can be obtained following Theorem 1 and is omitted. \blacksquare

Theorem 4: For a general connected network of N PCOs, within which M oscillators are non-colluding stealthy Byzantine attackers, if M is no greater than $2 \times \lfloor d/9 \rfloor$ with $d > \lfloor 2N/3 \rfloor$, then all legitimate oscillators can be synchronized under Mechanism 2 as long as their initial length of the containing arc is less than π rad.

Proof: The proof follows the same line of reasoning as in Theorem 2. More specifically, using the same arguments as Part I of Theorem 2, we can obtain that a pulse from neither a legitimate oscillator nor a stealthy Byzantine attacker could enlarge the containing arc of legitimate oscillators under Mechanism 2, i.e., the length of the containing arc of legitimate oscillators is non-increasing. Then, following the same argument as in Part II of Theorem 2, we know that if $d > \lfloor 2N/3 \rfloor$ and $M \leq 2 \times \lfloor d/9 \rfloor$ hold, the length of the containing arc of legitimate oscillators will keep decreasing until it converges to 0. \blacksquare

Theorem 5: For a general connected network of N PCOs, within which M oscillators are colluding stealthy Byzantine attackers, if M is no greater than $\lfloor d/9 \rfloor$ with $d > \lfloor 2N/3 \rfloor$, then all legitimate oscillators can be synchronized under Mechanism 2 as long as their initial length of the containing arc is less than π rad.

Proof: The proof can be obtained following the same line of argument as in Theorem 3 and is omitted. \blacksquare

Remark 6: When N is unknown to individual oscillators, d has to be over $\lfloor 2N/3 \rfloor$, which is greater than $\lfloor N/2 \rfloor$ in the case where N is known. The increased requirement on the connectivity of PCO networks is intuitive in that less knowledge of a PCO network requires stronger conditions to guarantee synchronization.

Table 1 summarizes the conditions for Mechanism 1 and Mechanism 2 to achieve synchronization.

VII. SIMULATIONS

Consider a network of 30 PCOs distributed on a two-dimension plane as illustrated in Fig. 7. Two oscillators in the network can communicate with each other if and only if their distance is no more than 50 meters. Thus, the degree of the network is $d = 24$. We set the initial time to $t = 0$ and chose phases of oscillators randomly from $[0, \pi]$. Hence, the initial length of the containing arc satisfied $\delta(0) < \pi$.

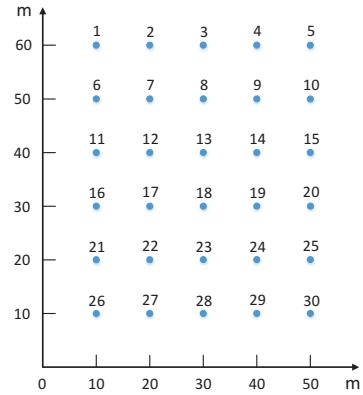


Figure 7: The deployment of the 30 oscillators used in simulations.

A. In the Absence of Attacks

We first considered the situation without attackers. As $d > \lfloor 2N/3 \rfloor = 20$, we know from Theorem 1 and Corollary 4 that the network will always synchronize, whether or not N is available to individual oscillators. This was confirmed in Fig. 8.

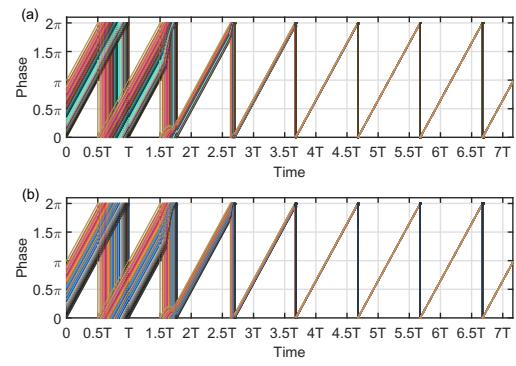


Figure 8: Plot (a) and (b) presented the phase evolutions of the 30 PCOs under Mechanism 1 and Mechanism 2, respectively. The coupling strength was set to $l = 0.1$.

B. In the Presence of Stealthy Byzantine Attackers

Using the same network, we first ran simulations in the presence of stealthy Byzantine attacks when N is known to individual oscillators.

We assumed that 4 out of the 30 oscillators (oscillators 1, 6, 26 and 30) were compromised and acted as non-colluding

Table 1. Synchronization conditions of Mechanism 1 and Mechanism 2 (N denotes the total number of oscillators)

	Initial containing arc length	Degree of network d	Need knowledge of N	Number of attackers M (non-colluding case)	Number of attackers M (colluding case)
Mechanism 1	less than π	$d > \lfloor N/2 \rfloor$	Yes	$M \leq 2 \times \lfloor (d - \lfloor N/2 \rfloor)/4 \rfloor$	$M \leq \lfloor (d - \lfloor N/2 \rfloor)/4 \rfloor$
Mechanism 2	less than π	$d > \lfloor 2N/3 \rfloor$	No	$M \leq 2 \times \lfloor d/9 \rfloor$	$M \leq \lfloor d/9 \rfloor$

Byzantine attackers. As $M = 2 \times \lfloor (d - \lfloor N/2 \rfloor)/4 \rfloor = 4$, we know from Theorem 2 that the network will synchronize. This was confirmed by numerical simulations in Fig. 9, which showed that even under attacks the length of the containing arc of legitimate oscillators converged to zero, despite the fact that the containing arc of oscillator 1's legitimate neighbors was enlarged by these attack pulses.

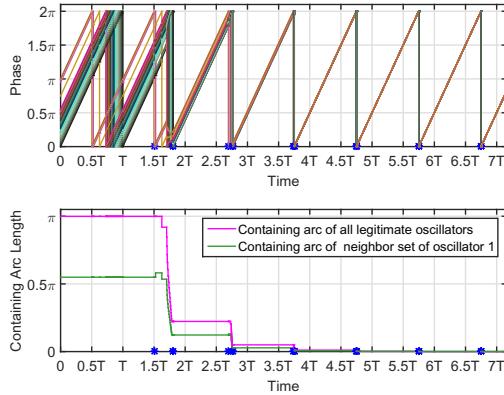


Figure 9: Phase evolution and the length of the containing arc of 26 legitimate oscillators under Mechanism 1 in the presence of 4 non-colluding stealthy Byzantine attackers (oscillators 1, 6, 26, 30) with attacking pulse time instants represented by asterisks. The coupling strength was set to $l = 0.1$.

When the 4 attackers colluded with each other, according to Theorem 3, the maximally allowable number of colluding attackers is $\lfloor (d - \lfloor N/2 \rfloor)/4 \rfloor = 2$. Hence, the condition in Theorem 3 was not satisfied. Simulation results confirmed that legitimate oscillators indeed could not synchronize, as illustrated in Fig. 10.

However, when we decreased the number of attackers to 2 (oscillators 1 and 6), all legitimate oscillators synchronized (cf. Fig. 11), confirming the results in Theorem 3. It is worth noting that the containing arc of attacker 1's legitimate neighbors were enlarged by attacker pulses, cf. Fig. 11.

We also ran simulations in the presence of stealthy Byzantine attacks when N is unknown to individual oscillators. We assumed that 4 out of the 30 oscillators (oscillators 1, 6, 18 and 26) were compromised and acted as stealthy non-colluding Byzantine attackers. According to Theorem 4, all legitimate oscillators can be synchronized under Mechanism 2. This was confirmed by numerical simulations in Fig. 12, which showed that the length of the containing arc of legitimate oscillators converged to zero.

When all 4 attackers colluded with each other, according to

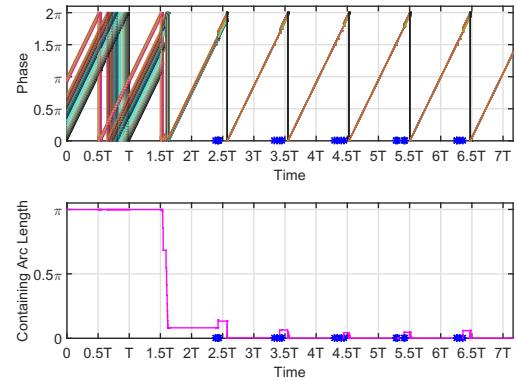


Figure 10: Phase evolution and the length of the containing arc of 26 legitimate oscillators under Mechanism 1 in the presence of 4 colluding stealthy Byzantine attackers (oscillators 1, 6, 26 and 30) with attacking pulse time instants represented by asterisks. The coupling strength was set to $l = 0.1$.

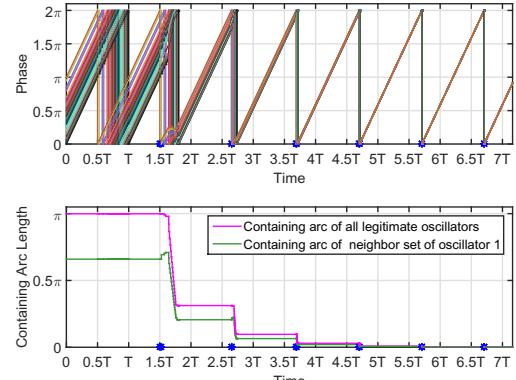


Figure 11: Phase evolution and the length of the containing arc of 28 legitimate oscillators under Mechanism 1 in the presence of 2 colluding stealthy Byzantine attackers (oscillators 1 and 6) with attacking pulse time instants represented by asterisks. The coupling strength was set to $l = 0.1$.

Theorem 5, the maximally allowable number of attackers is $\lfloor d/9 \rfloor = 2$. Hence, the condition in Theorem 5 is not satisfied. Simulation results confirmed that legitimate oscillators indeed could not synchronize, as illustrated in Fig. 13.

However, when we reduced the number of colluding attackers to 2 (oscillators 1 and 6), all legitimate oscillators achieved synchronization (cf. Fig. 14), which confirmed Theorem 5.

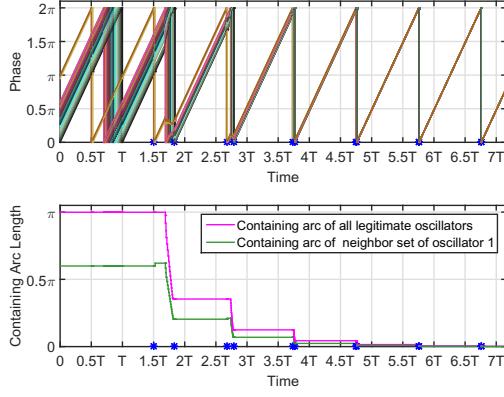


Figure 12: Phase evolution and the length of the containing arc of 26 legitimate oscillators under Mechanism 2 in the presence of 4 stealthy non-colluding Byzantine attackers (oscillators 1, 6, 18 and 26) with attacking pulse time instants represented by asterisks. The coupling strength was set to $l = 0.1$.

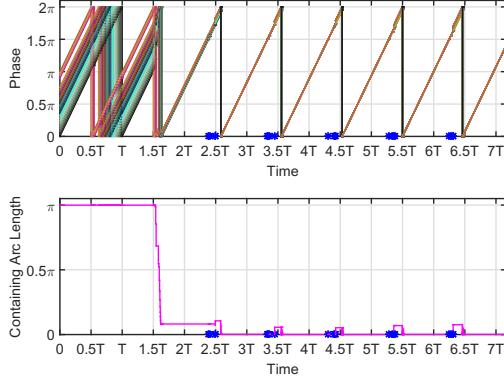


Figure 13: Phase evolution and the length of the containing arc of 26 legitimate oscillators under Mechanism 2 in the presence of 4 colluding stealthy Byzantine attackers (oscillators 1, 6, 18 and 26) with firing time instants represented by asterisks. The coupling strength was set to $l = 0.1$.

C. Comparison with Existing Results

In the absence of attacks, we compared Mechanism 1 with existing approaches in [37]–[39] under the PCO network in Fig. 7 in the presence of time-varying delays. We assume that the delays are randomly distributed in $[0, 0.1T]$. Noting that exact synchronization cannot be achieved in this case, similar to [37], we evaluated the performance using synchronization errors defined as follows:

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

where \mathcal{N}_L is the index set of all legitimate oscillators.

Fig. 15 and Fig. 16 show the synchronization errors of Mechanism 1 and approaches in [37]–[39] when the coupling strength was set to $l = 0.3$ and $l = 0.6$, respectively. Each data point was the average of 10,000 runs with vertical error bars denoting standard deviations. It can be seen that our approach

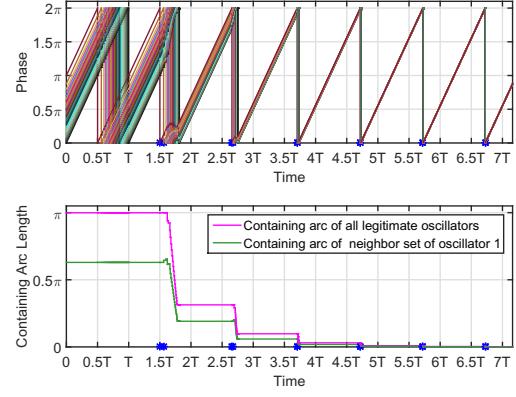


Figure 14: Phase evolution and the length of the containing arc of 28 legitimate oscillators under Mechanism 2 in the presence of 2 colluding stealthy Byzantine attackers (oscillators 1 and 6) with attacking pulse time instants represented by asterisks. The coupling strength was set to $l = 0.1$.

renders a smaller synchronization error. It is worth noting that Mechanism 2 also renders a smaller synchronization error than the approaches in [37]–[39] under the same set up. However, the results are omitted due to space limitations.

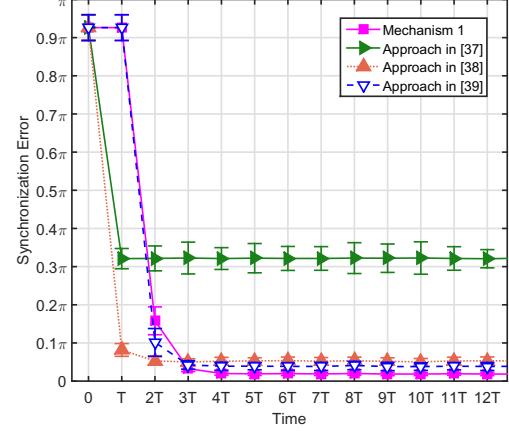


Figure 15: Comparison of our Mechanism 1 with the approaches in [37]–[39] in terms of synchronization error in the presence of time-varying delays uniformly distributed in $[0, 0.1T]$. The coupling strength was set to $l = 0.3$.

We also compared our proposed approach with existing approaches in [37]–[39] under the PCO network in Fig. 7 in the presence of non-colluding and colluding stealthy Byzantine attackers, respectively.

Fig. 17 shows the synchronization errors of Mechanism 1 and approaches in [37]–[39] in the presence of 4 non-colluding stealthy Byzantine attackers (oscillators 1, 6, 26, 30) and Fig. 18 shows the corresponding synchronization errors in the presence of 2 colluding stealthy Byzantine attackers (oscillators 1 and 6). Each data point was the average of 10,000 runs with vertical error bars denoting standard deviations. It can be seen that our approach can achieve perfect

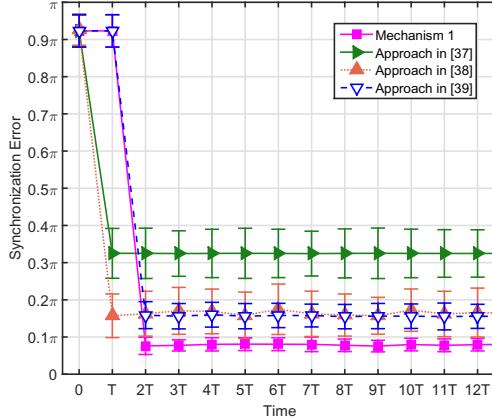


Figure 16: Comparison of our Mechanism 1 with the approaches in [37]–[39] in terms of synchronization error in the presence of time-varying delays uniformly distributed in $[0, 0.1T]$. The coupling strength was set to $l = 0.6$.

synchronization whereas all existing approaches are subject to substantial synchronization errors. It is worth noting that our Mechanism 2 also achieved perfect synchronization under the same set up. However, the results are omitted due to space limitations.

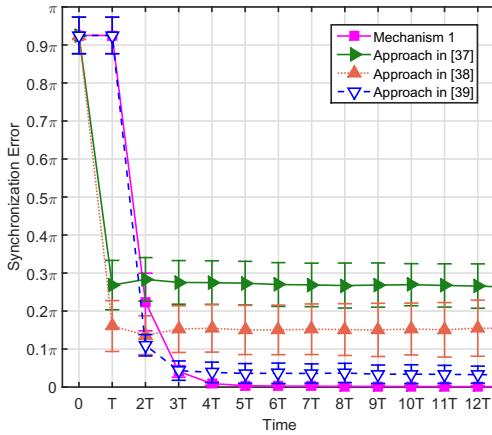


Figure 17: Comparison of our Mechanism 1 with the attack-resilient approaches in [37]–[39] in terms of synchronization error in the presence of 4 non-colluding stealthy Byzantine attackers (oscillators 1, 6, 26, 30). The coupling strength was set to $l = 0.3$.

VIII. CONCLUSIONS

Due to unique advantages over conventional packet-based synchronization approaches in terms of simplicity, scalability, and energy efficiency, pulse-based synchronization gained increased attention in recent years. However, few results are available to address the attack-resilience of pulse-base synchronization. In this paper, we propose a new pulse-based synchronization mechanism to improve the attack-resilience of general connected PCO networks. We rigorously prove that the

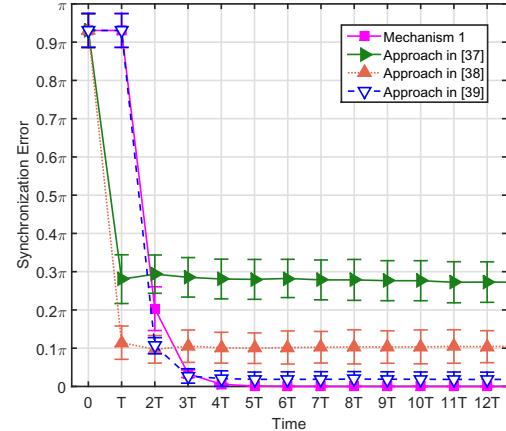


Figure 18: Comparison of our Mechanism 1 with the attack-resilient approaches in [37]–[39] in terms of synchronization error in the presence of 2 colluding stealthy Byzantine attackers (oscillators 1 and 6). The coupling strength was set to $l = 0.3$.

new mechanism can achieve phase synchronization of general connected PCO networks in the presence of multiple stealthy Byzantine attackers, irrespective of whether they are colluding or not. Our results allow the initial phases of legitimate oscillators to reside in a half oscillation period, which is in distinct difference from most existing attack-resilience algorithms that require a priori (almost) synchronization among legitimate oscillators. The approach is also applicable when the total number of oscillators is 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] C. 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] J. Klinglmayr, C. Bettstetter, M. Timme, and C. Kirst. Convergence of self-organizing pulse-coupled oscillator synchronization in dynamic networks. *IEEE Transactions on Automatic Control*, 62(4):1606–1619, 2017.
- [21] C. Canavier and S. Achuthan. Pulse coupled oscillators and the phase resetting curve. *Mathematical biosciences*, 226(2):77–96, 2010.
- [22] J. Nishimura and E. J. Friedman. Robust convergence in pulse-coupled oscillators with delays. *Physical Review Letters*, 106(19):194101, 2011.
- [23] J. Nishimura and E. J. Friedman. Probabilistic convergence guarantees for type-ii pulse-coupled oscillators. *Physical Review E*, 86(2):025201, 2012.
- [24] L. Lücken and S. Yanchuk. Two-cluster bifurcations in systems of globally pulse-coupled oscillators. *Physica D: Nonlinear Phenomena*, 241(4):350–359, 2012.
- [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] D. Kannapan and F. Bullo. Synchronization in pulse-coupled oscillators with delayed excitatory/inhibitory coupling. *SIAM Journal on Control and Optimization*, 54(4):1872–1894, 2016.
- [27] H. Lyu. Global synchronization of pulse-coupled oscillators on trees. *SIAM Journal on Applied Dynamical Systems*, 17(2):1521–1559, 2018.
- [28] A. V. Proskurnikov and M. Cao. Synchronization of pulse-coupled oscillators and clocks under minimal connectivity assumptions. *IEEE Transactions on Automatic Control*, 62(11):5873–5879, 2016.
- [29] H. Gao and Y. Q. Wang. A pulse-based integrated communication and control design for decentralized collective motion coordination. *IEEE Transactions on Automatic Control*, 63(6):1858–1864, 2018.
- [30] M. Pease, R. Shostak, and L. Lamport. Reaching agreement in the presence of faults. *Journal of the ACM (JACM)*, 27(2):228–234, 1980.
- [31] 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.
- [32] Q. Li and D. Rus. Global clock synchronization in sensor networks. *IEEE Transactions on computers*, 55(2):214–226, 2006.
- [33] H. Song, S. Zhu, and G. H. Cao. Attack-resilient time synchronization for wireless sensor networks. *Ad Hoc Networks*, 5(1):112–125, 2007.
- [34] X. J. Du and H. Chen. Security in wireless sensor networks. *IEEE Wireless Communications*, 15(4), 2008.
- [35] 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.
- [36] A. Tyrrell, G. Auer, C. Bettstetter, and R. Nariella. How does a faulty node disturb decentralized slot synchronization over wireless networks? In *2010 IEEE International Conference on Communications*, pages 1–5, 2010.
- [37] 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.
- [38] 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.
- [39] Z. Q. Wang and Y. Q. Wang. Pulse-coupled oscillators resilient to stealthy attacks. *IEEE Transactions on Signal Processing*, 66(12):3086–3099, 2018.
- [40] Z. Q. Wang and Y. Q. Wang. Attack-resilient pulse-coupled synchronization. *IEEE Transactions on Control of Network Systems*, 6(1):338–351, 2018.
- [41] L. Lamport, R. Shostak, and M. Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3):382–401, 1982.
- [42] 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.



Zhenqian Wang was born in Hebei, China. He received the B.E. and M.Sc. degrees in automation and control theory from Tianjin University, Tianjin, China, in 2012 and 2015, respectively. He is currently working toward the Ph.D. degree in the Department of Electrical and Computer Engineering, Clemson University, Clemson, SC, USA. His current research focuses on attack-resilient clock synchronization.



Yongqiang Wang (SM’13) was born in Shandong, China. He received the B.S. degree in Electrical Engineering & Automation, the B.S. degree in Computer Science & Technology from Xi’an Jiaotong University, Shaanxi, China, in 2004. He received the M.Sc. and the Ph.D. degrees in Control Science & Engineering from Tsinghua University, Beijing, China, in 2009.

From 2007–2008, he was with the University of Duisburg-Essen, Germany, as a visiting student. He was a Project Scientist at the University of California, Santa Barbara. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, Clemson University, Clemson, SC, USA. His research interests are cooperative and networked control, synchronization of wireless sensor networks, systems modeling and analysis of biochemical oscillator networks, and model-based fault diagnosis. He received the 2008 Young Author Prize from IFAC Japan Foundation for a paper presented at the 17th IFAC World Congress in Seoul.