August 2020

Attack Resilient Pulse Based Synchronization

Zhenqian Wang
Clemson University, zhenqiw@g.clemson.edu

ATTACK RESILIENT PULSE BASED SYNCHRONIZATION

A Dissertation
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy
Electrical Engineering

---

by
Zhenqian Wang
August 2020

Accepted by:
Dr. Yongqiang Wang, Committee Chair
Dr. Yingjie Lao
Dr. Linke Guo
Dr. Shitao Liu

Abstract

Synchronization of pulse-coupled oscillators (PCOs) has gained significant attention recently due to increased applications in sensor networks and wireless communications. However, most existing results are obtained in the absence of malicious attacks. Given the distributed and unattended nature of wireless sensor networks, it is imperative to enhance the resilience of pulse-based synchronization against malicious attacks. To achieve this goal, we first show that by using a carefully designed phase response function (PRF), pulse-based synchronization of PCOs can be guaranteed despite the presence of a stealthy Byzantine attacker, even when legitimate PCOs have different initial phases. Next, we propose a new pulse-based synchronization mechanism to improve the resilience of pulse-based synchronization to multiple stealthy Byzantine attackers. We rigorously characterize the condition for mounting stealthy Byzantine attacks under the proposed new pulse-based synchronization mechanism and prove analytically that synchronization of legitimate oscillators can be achieved even when their initial phases are unrestricted, i.e., randomly distributed in the entire oscillation period. Since most existing results on resilient pulse-based synchronization are obtained only for all-to-all networks, we also propose a new pulse-based synchronization mechanism to improve the resilience of pulse-based synchronization that is applicable under general connected topologies. Under the proposed synchronization mechanism, we prove that synchronization of general connected legitimate PCOs 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 distributed in a half circle. Then, to relax the limitation of the stealthy attacker model and the constraint on the legitimate oscillators' initial phase distribution, we improved our synchronization mechanism and proved that finite time synchronization of legitimate oscillators can be guaranteed in the presence of multiple Byzantine attackers who can emit attack pulses arbitrarily without any constraint except that practical bit rate constraint renders the number of pulses from an attacker to be finite. The improved mechanism can guarantee synchronization even when the initial phases of all legitimate

oscillators are arbitrarily distributed in the entire oscillation period. The new attack resilient pulse-based synchronization approaches in this dissertation are in distinct difference from most existing attack-resilient synchronization algorithms (including the seminal paper from Lamport and Melliar-Smith [1]) which require a priori (almost) synchronization among all legitimate nodes. Numerical simulations are given to confirm the theoretical results.

Acknowledgments

I would like to sincerely thank my academic advisor Dr. Yongqiang Wang for the continuous support and advice to my Ph.D. study and research at Clemson University. His profound knowledge and patient guidance helped me get through challenges and difficulties both in my research and life. His contributions of time and novel ideas make my Ph.D. experience productive and stimulating. Under the supervision of Dr. Wang, I am fortunate to build up critical thinking in research and gain rigorous attitude in study. None of the accomplishments in my Ph.D. journey would have been possible without his support. Besides my advisor, I would like to thank my committee members: Dr. Yingjie Lao, Dr. Linke Guo, and Dr. Shitao Liu for their insightful comments and valuable feedbacks on my comprehensive exam and dissertation. In addition, I want to express my sincere gratitude to my parents Zipo Wang, Liduo Feng, and my fiancée Mengzhe Li. They always stand by me, providing me with their warm encouragement, continued care, and endless love. They make me to be a friendly, healthy, and happy person. My sincere thanks also goes to my friends, lab mates and roommates. Whenever I was worried or not in a good mood, they lift me up. I appreciate all of your support and encouragement throughout my life!

Contents

List of Tables

List of Figures

Chapter 1

Introduction

Inspired by flashing fireflies and contracting cardiac cells, pulse-based synchronization is attracting increased attention in sensor networks and wireless communications [5–10]. 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 [11]. These inherent advantages make pulse-based synchronization extremely appealing for event coordination and clock synchronization in various networks [12–15]. Moreover, using a simple phase response function (PRF) which governs how a node adjusts its phase upon receiving an anonymous pulse, PCOs do not need to store or distinguish the source/destination of exchanged pulses, which makes pulse-based synchronization implicitly scalable [11, 16, 17].

In recent years, due to the increased applications of pulse-based synchronization in smart grid [18, 19], surveillance [15], wireless beam-forming [13], and motion coordination [20, 21], research on pulse-based synchronization has blossomed. For example, by optimizing the interaction function, i.e., phase response function, the synchronization speed of pulse-coupled oscillators (PCOs) is maximized in [4]; with a judiciously-added refractory period in the phase response function, the energy consumption of pulse-based synchronization is reduced in [22–24]; [25–27] show that PCOs can achieve synchronization under a general coupling topology even when their initial phases are randomly distributed in the entire oscillation period. Recently, synchronization of PCOs in the presence of time-delays and unreliable links is also discussed [28–30]. Other relevant results include [31–46].

However, all 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, 47–63], results are very sparse on the attack-resilience of pulse-based synchronization [2, 3, 64]. In [64], the authors showed that pulse-based synchronization is more robust than its packet-based counterpart in the presence of a faulty node. In [2], a new phase response function was proposed to improve the precision of pulse-based synchronization against non-persistent random attacks. The authors in [3] 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 dissertation, we consider the synchronization of PCOs in the presence of Byzantine attacks which may compromise oscillators with arbitrary malicious behaviors. In the pulse-based interaction framework where exchanged messages are only identical and content-free pulses, Byzantine attacks mean compromised nodes injecting pulses using judiciously crafted patterns to disturb the synchronization process. So compared with existing results in [2, 3, 64] which address faulty PCO nodes with random or periodic pulse emitting patterns, the situation considered in this dissertation is more difficult to deal with due to the intelligent behavior of malicious attackers.

In Chapter 2, by using a carefully designed PRF, we characterize the condition under which an attacker could launch stealthy Byzantine attacks without being detected and show that perfect synchronization of legitimate oscillators can be achieved under a stealthy Byzantine attacker if some initial conditions on legitimate oscillators' phases are satisfied. In Chapter 3, we propose a new pulse-based synchronization mechanism to improve the resilience of pulse-based synchronization. We rigorously characterize the condition for mounting stealthy Byzantine attacks under the proposed pulse-based synchronization mechanism and prove analytically that synchronization of legitimate oscillators can be achieved in the presence of multiple stealthy Byzantine attackers even when the initial phases of legitimate oscillators are unrestricted, i.e., randomly distributed in the entire oscillation period. In Chapter 4, we present a new pulse-based synchronization mechanism for general connected PCOs that can achieve phase synchronization even in the presence of multiple stealthy Byzantine attackers, irrespective of whether the attackers collude with each other or not. Under the proposed synchronization mechanism, we rigorously characterize the condition for stealthy Byzantine attacks and prove that perfect synchronization of general connected legitimate oscillators can be guaranteed

even when their initial phases are widely distributed in a half circle. The result in Chapter 4 is in distinct difference from our results in Chapters 2 and 3 which can only guarantee phase synchronization under all-to-all topologies. To relax the limitation of the stealthy attacker model and the constraint on the legitimate oscillators' initial phase distribution in Chapter 4, we improved our synchronization mechanism in Chapter 5 and proved that perfect synchronization of legitimate oscillators can be guaranteed in the presence of multiple Byzantine attackers who can emit attack pulses arbitrarily without any constraint except that practical bit rate constraint renders the number of pulses from an attacker to be finite. The improved mechanism can guarantee synchronization even when the initial phases of all legitimate oscillators are arbitrarily distributed in the entire oscillation period. We conclude the dissertation in Chapter 6.

It is worth noting that this dissertation is comprised of four papers from our research work [65–68]. More specifically, [65], [66], [67], and [68] are included in Chapters 2, 3, 4, and 5, respectively.

Chapter 2

An Attack-Resilient Phase Response Function for PCO networks

2.1 Introduction

In this chapter, we consider the synchronizability of PCOs in the presence of Byzantine attacks which may compromise oscillators with arbitrary malicious behaviors. So compared with the assumption in [3] where faulty oscillators only fail to respond to pulses, the attack model in this chapter is much stronger because an intelligent malicious attacker can strategically drive the network away from synchronization. Using a carefully designed PRF, we characterize the condition under which an attacker could launch stealthy attacks without being detected. Moreover, we show that perfect synchronization of legitimate oscillators can still be achieved under such stealthy Byzantine attacks if some initial conditions on legitimate oscillators' phases are satisfied.

Contribution: Although plenty of discussions exist for conventional packet-based synchronization under Byzantine attacks [1,47,48,60–63], to the best of our knowledge, this chapter is the first effort dealing with Byzantine attacks in the pulse-based synchronization framework. By using a carefully designed PRF, we show that legitimate oscillators can still be synchronized under stealthy Byzantine attacks even when they have different initial phases. The synchronization condition is much less conservative than most existing attack-resilient synchronization approaches (including the seminal paper [1] and those addressing the robustness of pulse-based synchronization under attacks [2,3,64]), which require that all legitimate oscillators must

have identical or almost identical initial phases to achieve synchronization under attacks.

The organization of this chapter is as follows. Section 2.2 presents a new PRF which can guarantee synchronization in the absence of attacks. Section 2.3 characterizes the condition for stealthy Byzantine attacks, i.e., attacks that cannot be detected by a detection mechanism introduced under the pulse-coupled interaction framework. Sections 2.4 and 2.5 show that the proposed PRF is able to guarantee synchronization of legitimate oscillators even in the presence of stealthy Byzantine attacks.

2.2 Synchronization under a New PRF

2.2.1 A New PRF

Consider a network of N pulse-coupled oscillators whose phases are denoted as $\phi_i(t)$ at time instant t for $i = 1, 2, \cdots, N$. All phase variables evolve from 0 to 2π with a constant speed (natural frequency) ω. Without loss of generality, we assume $\omega = 1$ throughout this chapter. When the phase of an oscillator (e.g., oscillator i) reaches 2π, it fires (emits a pulse) and simultaneously resets its phase to 0. When oscillator i receives a pulse from an adjacent oscillator at time instant t, it will shift its phase to $\phi_i(t) + l \times F(\phi_i(t))$, i.e.,

$$\phi_i(t^+) = \phi_i(t) + l \times F(\phi_i(t)) \tag{2.1}$$

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

$$F(\phi(t)) := \begin{cases} 0 & 0 \leq \phi(t) < D \\ 2\pi - \phi(t) & D \leq \phi(t) \leq 2\pi \end{cases} \tag{2.2}$$

In (2.2), D is the length of the refractory period and it is assumed to satisfy $\pi \leq D < 2\pi$ in this chapter. When an oscillator's phase $\phi(t)$ resides in the refractory period $[0,\ D)$, the oscillator will ignore incoming pulses and its phase will evolve freely without perturbation. If a pulse arrives when $\phi(t)$ is outside of the refractory period, it will induce a jump on $\phi(t)$ with value determined by the product of PRF in (2.2) and the coupling strength l.

Remark 2.1. *Different from existing PRFs in [2] and [3] (which was originally proposed in [4] to maximize synchronization speed), the new PRF can significantly improve the resilience of synchronization to malicious pulse attacks, as illustrated by numerical simulation results in Fig.2.1. Rigorous analysis will be substantiated in Section* 2.4 *and Section* 2.5 *as well as numerical simulations in Section* 2.6.

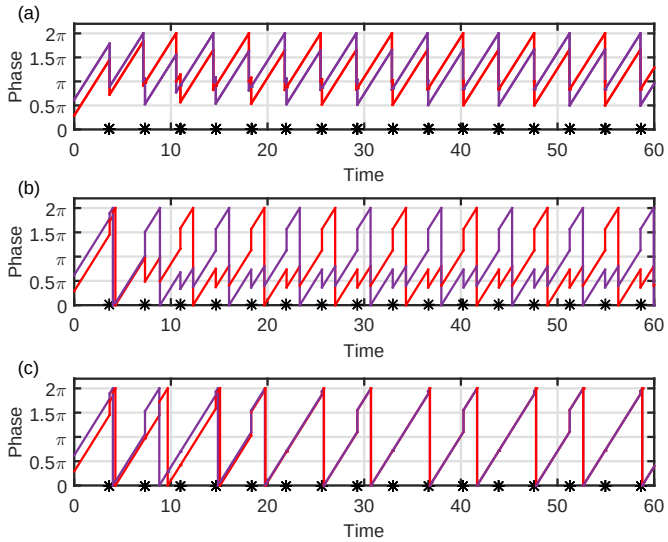

Figure 2.1: Phase evolutions of an all-to-all network of three PCOs, one of which is compromised by an attacker with firing time instants represented by asterisks. Plots (a), (b), and (c) present the phase evolutions of the two legitimate oscillators under the PRFs in [2], [3] (which was originally proposed in [4] to maximize synchronization speed), and the proposed PRF, respectively. l and D are set to 0.5 and π, respectively. We can see that synchronization of legitimate oscillators can be achieved only under our PRF.

Assumption 2.1. *Following [35,36,42], we assume that when a legitimate oscillator receives multiple pulses simultaneously, it will process these pulses consecutively. In other words, no two pulses will be regarded as an aggregated pulse.*

In this Chapter, the interaction topology of the PCO network is assumed to be all-to-all in Chapter 2-Chapter 4. Generalization to general strongly-connected topologies is given in Chapter 5.

2.2.2 Synchronization Condition in the Absence of Attacks

In this subsection, we give a synchronization condition under the proposed PRF. As in most studies [4, 6, 22–27], PCOs are synchronized when all legitimate oscillators' phases are identical. We introduce the following definitions to facilitate the analysis.

We assume 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 which contains all legitimate oscillators' phases. The starting point and the ending point of a containing arc are defined as the leading point and the terminating point of the containing arc in the clockwise direction, respectively. Moreover, the interior of a

containing arc is defined as the set of all points residing in the containing arc except the starting and ending points.

When synchronization is achieved, the starting and ending points of a containing arc overlap and the interior of the containing arc becomes an empty set. We next present the synchronization condition for a PCO network under the proposed PRF in (2.2) when there are no attacks.

Lemma 2.1. *For an all-to-all PCO network with PRF given in (2.2), if the length of the initial containing arc is less than* $2\pi - D$ *with the refractory period* D *satisfying* $\pi \leq D < 2\pi$*, then all PCOs can be perfectly synchronized in the absence of attacks.*

Proof. Lemma 2.1 is a special case of Theorem 1 in [24]. □

2.3 Byzantine Attacks and Attack Detection Mechanism

2.3.1 Byzantine Attacks

The concept of Byzantine attacks stems from the Byzantine generals problem [48]. It is used to describe a traitor commander who sends or relays fake information to other commanders to avoid the loyal ones from reaching agreement [47]. In the case of PCO synchronization, Byzantine attacks mean that a compromised oscillator is completely taken over by an attacker and will deviate from the prescribed behavior in an arbitrary way, i.e., it will send out pulses at arbitrary time instants. Clearly, if an attacker keeps sending pulses continuously without rest, it will prevent legitimate oscillators from achieving synchronization. However, such a manner of attacks will also render themselves easily detectable, just as jamming of communication channels which is easy to detect, isolate, and remove [69]. Therefore, we are only interested in Byzantine attacks which are unable to detect in the pulse-coupled interaction framework.

2.3.2 Attack Detection Mechanism under Pulse Interaction

In this subsection, we characterize the condition for stealthy Byzantine attacks that cannot be detected in the pulse-coupled framework in which all exchanged messages are identical pulses and free of source/destination information. To this end, we first give a lemma to characterize the time-invariant firing sequence of PCOs under the PRF in (2.2). Firing sequence is the order in which legitimate oscillators fire. The time-invariant firing sequence of PCOs is an important property of all-to-all PCO networks, which means that the phase of an oscillator cannot overpass another oscillator's phase on the unit circle.

Lemma 2.2. *For an all-to-all network of N legitimate PCOs with PRF given in (2.2), the firing sequence of all oscillators is time-invariant.*

Proof. The proof is given in Appendix A. □

In PCO networks, since all exchanged messages (pulses) are identical with no embedded content, conventional content-checking based attack detection mechanisms such as [1] cannot be applied. We propose to detect potential attacks in the network by monitoring the number of the emitted pulses within a certain time interval. The basic idea is as follows. In a short time interval, if the number of detected pulses is more than the maximally possible number of pulses (emitted by all legitimate oscillators) in this time interval, then it is safe to conclude that attackers or compromised oscillators are present which send the additional pulses. More specially, under PRF (2.2), we can characterize the respective longest and shortest time intervals during which N pulses can be emitted if all oscillators are legitimate, which is detailed in Theorem 2.1.

Theorem 2.1. *For an all-to-all network of N legitimate PCOs with PRF given in (2.2), if the length of the containing arc is no more than δ with $\delta < 2\pi - D$, then*

1. *within any time interval $[t, t+T_L)$ for*

$$T_L = 2\pi - \delta + (1-l)^{N-1}\delta \tag{2.3}$$

   and $\forall t \in R$, there can be at most N pulses;

2. *within any time interval $[t, t+T_U]$ for*

$$T_U = 2\pi \tag{2.4}$$

   and $\forall t \in R$, there can be at least N pulses.

Proof. The proof is given in Appendix B. □

2.3.3 A Condition for Stealthy Attacks

Next we present a condition for an attacker to launch attacks that cannot be detected by the detection mechanism in Section 2.3.2. We consider an all-to-all network with N PCOs wherein one is compromised. The length of the containing arc of the $N-1$ legitimate oscillators is $\delta < 2\pi - D$.

Under the attack detection mechanism in Theorem 2.1, if the compromised PCO sends more than one pulse within an arbitrary time interval of length T_L, or does not send out any pulse during an arbitrary

time interval of length T_U, the detection system will successfully detect the presence of attacks. Therefore, to keep stealthy, an attacker should send pulses with period no larger than T_U and no less than T_L. In summary, the condition for a compromised oscillator to launch stealthy Byzantine attacks can be depicted as follows:

Definition 2.1. *A compromised oscillator can launch stealthy Byzantine attacks if it exerts pulses persistently with a (time-varying) firing interval arbitrarily chosen from the set* $[T_L, T_U]$.

Assumption 2.2. *In Section* 2.4 *and Section* 2.5*, we assume that there exists only one attacker. The multiple attacker case is studied in Section* 2.6 *via numerical simulations.*

2.4 Synchronization of All-To-All PCO Networks under Stealthy Attacks

In this section, we consider an all-to-all PCO network with N oscillators, one of which is compromised. If all $N-1$ legitimate oscillators are already synchronized, their synchronization state cannot be disturbed by the compromised oscillator because the pulse from the compromised one (attacker) will cause equal offsets on all the legitimate oscillators' phases. Therefore, our work aims to synchronize all legitimate oscillators in the presence of a compromised oscillator when they are not initially synchronized. More specifically, we can prove that the $N-1$ legitimate oscillators can still be perfectly synchronized if their initial phases satisfy certain conditions. To this end, we first analyze how a single malicious pulse affects the length of the containing arc. According to Lemma 2.1, if the containing arc is no less than $2\pi - D$, synchronization cannot be guaranteed even in the absence of attacks. So in order to guarantee synchronization, the length of the containing arc should always be less than $2\pi - D$ after receiving a malicious pulse. Theorem 2.2 gives conditions under which such a requirement can be met.

Theorem 2.2. *For an all-to-all network of N PCOs with PRF in (2.2) wherein* $D \geq \pi$ *and one compromised oscillator sending attack pulses according to the stealthy attack model in Definition 2.1, the length of the containing arc will still be less than* $2\pi - D$ *after receiving a malicious pulse if either of the following conditions is met:*

1. *the containing arc of legitimate oscillators does not have phase D in its interior or as its starting point and its length is less than* $2\pi - D$ *before receiving a malicious pulse;*

2. *the containing arc of legitimate oscillators has phase D in its interior or as its starting point and its length is less than* $(1-l)(2\pi - D)$ *before receiving a malicious pulse.*

Proof. The proof is given in Appendix C. □

Clearly, if a malicious pulse does not increase the length of the containing arc of legitimate oscillators, it cannot disturb the synchronization process. Therefore, we proceed to analyze the condition under which a persistent stealthy attacker with a series of malicious pulses could never increase the length of the containing arc. If such a condition can be established, synchronization can be guaranteed even in the presence of such attacks since the malicious pulses do not increase the length of the containing arc whereas legitimate pulses sent by legitimate oscillators will always decrease the length of the containing arc.

Theorem 2.3. *For an all-to-all network of N PCOs with PRF in (2.2) wherein* $D \geq \pi$ *and one compromised oscillator sending malicious pulses according to the stealthy attack model in Definition 2.1, then synchronization of all legitimate oscillators can be guaranteed if either of the following conditions is met:*

1. *when the first malicious pulse is sent, the containing arc of all legitimate oscillators does not have phase D in its interior or as its starting point and its length is less than*

$$\delta_1 = \frac{l}{1-(1-l)^{N-1}}(2\pi - D) \tag{2.5}$$

2. *when the first malicious pulse is sent, the containing arc of all legitimate oscillators has phase D in its interior or as its starting point and its length is less than*

$$\delta_2 = \min\left\{\frac{l^2}{2-l-(1-l)^{N-1}},\ (1-l)\right\}(2\pi - D) \tag{2.6}$$

Proof. The proof is given in Appendix D. □

Based on Theorem 2.3, we have the following Corollary:

Corollary 2.1. *For an all-to-all network of N PCOs with PRF in (2.2) wherein* $D \geq \pi$ *and one compromised oscillator sending malicious pulses according to the stealthy attack model in Definition 2.1, if the initial length of the containing arc of all legitimate oscillators is less than* δ_2 *in (2.6), then synchronization of all legitimate oscillators can be guaranteed.*

Proof. Noticing $\delta_2 \leq \delta_1$, Corollary 2.1 can be easily obtained from Theorem 2.3. □

Remark 2.2. *Following [24], if the condition on initial phases are not met naturally, we can use a 'reset' packet to reduce the length of the containing arc of all legitimate oscillators to within a certain range.*

Remark 2.3. *The intentionally added large refractory period is the fundamental difference between our PRF and existing PRFs and it is key to enable the resilience to attacks. In fact, it can be obtained that under our PRF and initial conditions in Corollary 2.1, no attack pulses except the first one can increase the phase distances between legitimate oscillators and hence can harm the synchronization process of legitimate oscillators.*

2.5 Synchronization of Strongly-Connected PCO Networks under Stealthy Byzantine Attacks

In this section, we will show that the proposed PRF in (2.2) is also able to synchronize PCO networks under a stealthy Byzantine attacker, even when the legitimate oscillations are connected under a general strongly-connected topology. To this end, we first consider the attack-free case. It is worth noting that strongly-connected PCOs means that there is a multi-hop path between any pair of oscillators. Due to the reduced number of links among legitimate oscillators, synchronization of strongly-connected PCOs is much more difficult to achieve than the fully connected all-to-all case. A mathematical model of a strongly-connected PCO network can be found in Sec. II.B of [24].

Lemma 2.3. *For strongly-connected PCOs with PRF given in (2.2), if the length of the initial containing arc is less than $2\pi - D$ wherein $\pi \leq D < 2\pi$, then all oscillators can be perfectly synchronized in the absence of attacks.*

Proof. Lemma 2.3 is a special case of Theorem 1 in [24]. □

Next we characterize the number of legitimate pulses that an oscillator can receive under a strongly-connected topology. Denote the number of oscillators that can affect oscillator i as $d^{-}(i)$. Then we have the following result:

Theorem 2.4. *For N strongly-connected PCOs with PRF given in (2.2), if there are no attacks and the length of the containing arc is no greater than δ with $\delta < 2\pi - D$, then*

1. *within any time interval* $[t, t+T_L)$ *for*

$$T_L = 2\pi - \delta + (1-l)^{N-1}\delta \tag{2.7}$$

and $\forall t \in R$*, oscillator i can receive at most* $d^-(i)$ *pulses;*

2. *within any time interval* $[t, t+T_U]$ *for*

$$T_U = 2\pi \tag{2.8}$$

and $\forall t \in R$*, oscillator i can receive at least* $d^-(i)$ *pulses.*

Proof. Noticing $d^-(i) \leq N-1$ always holds for strongly-connected PCO networks, Theorem 2.4 can be obtained by following the same line of reasoning for Theorem 2.1. □

Based on the attack detection mechanism in Theorem 2.4, to keep stealthy, a compromised oscillator must send pulses with an interval residing in $[T_L, T_U]$, which means that the condition for stealthy attacks is the same as Definition 2.1.

Next, we show that the PRF in (2.2) is also resilient to stealthy Byzantine attacks even when the interaction topology is strongly-connected. Because when the legitimate oscillators are partially affected by the malicious pulse (some are affected but others not), they can never maintain synchronization as malicious pulses can always exert a nonzero phase shift on affected legitimate oscillators and make them deviate from the rest of non-affected legitimate oscillators, we assume that all legitimate oscillators are affected by malicious pulses.

Theorem 2.5. *For a network of N PCOs with PRF in (2.2) wherein* $D \geq \pi$ *and one compromised oscillator broadcasting malicious pulses to all legitimate ones following the stealthy Byzantine attack model in Definition 2.1, if all legitimate oscillators are strongly-connected and the length of the containing arc is less than* δ_3 *in (2.9), then synchronization of all legitimate oscillators can be guaranteed.*

$$\delta_3 = \min\left\{\frac{l^{N-1}}{2 - l^{N-2} - (1-l)^{N-1}},\ (1-l)\right\}(2\pi - D) \tag{2.9}$$

Proof. Proof of Theorem 2.5 can be obtained following Theorem 2.3 and is omitted. □

Remark 2.4. *It is worth noting that although plenty of discussions exist on the attack-resilience of conventional packet-based synchronization (e.g., [1, 47, 48, 60–63]), results on the resilience of pulse-coupled*

synchronization to attacks are very sparse. In this chapter, we show that pulse-coupled synchronization can be achieved in the presence of a malicious attacker even when legitimate oscillators have different initial phases. This is in distinct difference from most existing attack-resilient synchronization approaches (including the seminal paper [1] and those addressing the robustness of pulse-coupled synchronization under attacks [2, 3, 64]), which require that all legitimate oscillators must have identical or almost identical initial phases to achieve synchronization in the presence of attacks.

Remark 2.5. *In this chapter, a simple model in (2.1) is followed by every legitimate oscillator. It is worth noting that the simplicity of the model is one of the main advantages of pulse-coupled synchronization protocols over conventional packet-based synchronization methods: By exchanging identical content-free pulses, synchronization of legitimate oscillators can be achieved with much less communication overhead and energy consumption; moreover, the simple framework restricts the attack surface, i.e., the attacker can only launch attacks via pulse injections, which greatly facilitated the goal of synchronizing legitimate oscillators in the presence of attacks.*

2.6 Simulations

2.6.1 Performance of the proposed synchronization approach

We first simulated an all-to-all network of five PCOs, one of which was compromised. The coupling strength was set to $l = 0.4$ and the length of refractory period was chosen as $D = \pi$.

According to condition 1) of Theorem 2.3, if the length of the containing arc is no larger than $\delta_1 = 0.46\pi$ and the phase conditions of legitimate oscillators are satisfied when the first malicious pulse is sent, then all legitimate oscillators will synchronize despite repeated malicious pulses from the compromised oscillator.

Setting the initial phases of the oscillators to 0, 0.15π, 0.3π, and 0.45π, respectively, we first simulated the network with malicious pulses arriving at time instant $t = 0.5\pi$. At this time instant, the phases of the legitimate oscillators were given by 0.5π, 0.65π, 0.8π, 0.95π, which were all in the refractory period. So according to condition 1) of Theorem 2.3, the oscillators would synchronize. This was confirmed by numerical simulations in Fig. 2.2, which showed that the length of the containing arc converged to zero.

According to condition 2) of Theorem 2.3, the legitimate oscillators can synchronize if the length of the containing arc is no larger than $\delta_2 = 0.109\pi$. So we reduced the containing arc by setting the initial

phases of the legitimate oscillators to 0, 0.03π, 0.06π, and 0.1π, respectively, which led to a length of the initial containing arc 0.1π. The arriving time instant of the first malicious pulse was set to $t = 0.9\pi$. Condition 2) of Theorem 2.3 was satisfied, which means that legitimate oscillators could still synchronize. This was confirmed by numerical simulations in Fig. 2.3, which showed that the length of the containing arc indeed converged to zero. It is worth noting that Fig. 2.3 shows that the first malicious pulse increased the length of the containing arc, but to a value less than $2\pi - D = \pi$, which confirmed Theorem 2.2.

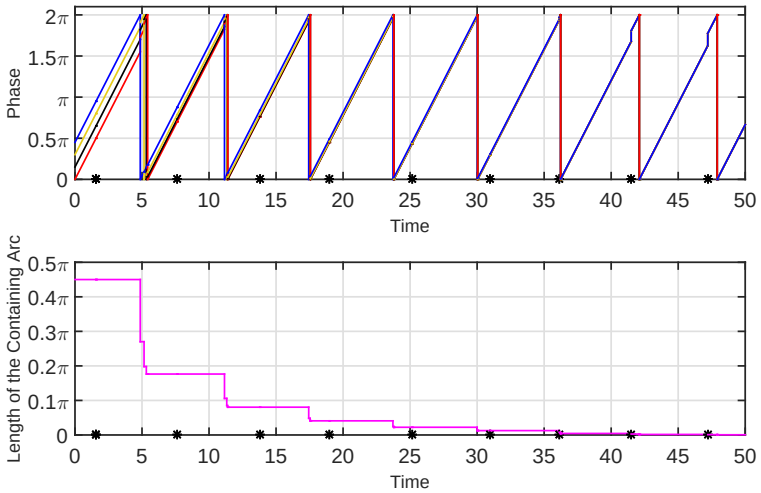

Figure 2.2: Phase evolution and the length of the containing arc of four legitimate oscillators in a five PCO all-to-all network. One oscillator was compromised and its firing time instants were represented by the asterisks. The initial phases of the legitimate oscillators were set to 0, 0.15π, 0.3π, and 0.45π.

We also simulated the phase evolution of a strongly-connected network of five PCOs, one of which was compromised and launched stealthy attacks according to Definition 2.1. The coupling strength was set to $l = 0.75$ and the length of refractory period was chosen as $D = \pi$. The topology of the network is shown in Fig. 2.4, wherein the four solid black dots represent the legitimate oscillators and the red star represents the attacker. According to Theorem 2.5, legitimate oscillators can synchronize if the length of the containing arc is less than $\delta_3 = 0.209\pi$. We set the initial phases of the legitimate oscillators to 0, 0.06π, 0.12π, and 0.18π, respectively, which leads to a length of the initial containing arc 0.18π satisfying synchronization condition in Theorem 2.5. Numerical simulations in Fig. 2.5 confirmed that legitimate oscillators indeed synchronized.

Under all-to-all topology and the strongly-connected topology in Fig. 2.4, we also compared the analytically obtained maximally allowable lengths of the initial containing arc with numerically obtained maximal lengths of the containing arc, which are represented by the red and blue curves in Fig. 2.6. In

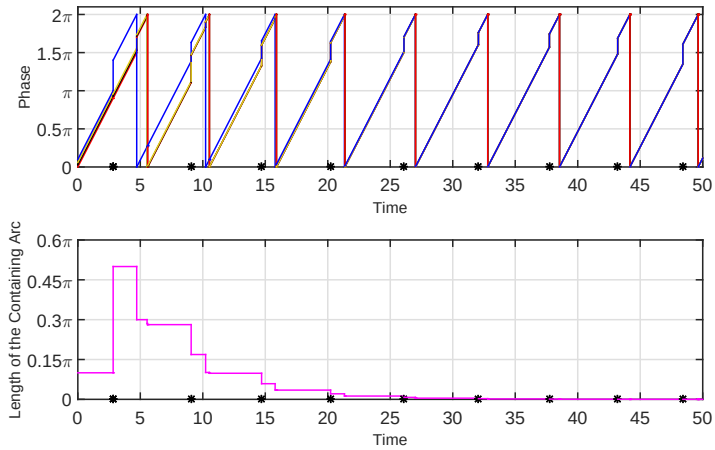

Figure 2.3: Phase evolution and the length of the containing arc of four legitimate oscillators in a five PCO all-to-all network. One oscillator was compromised and its firing time instants were represented by the asterisks. The initial phases of the legitimate oscillators were set to 0, 0.03π, 0.06π, and 0.1π.

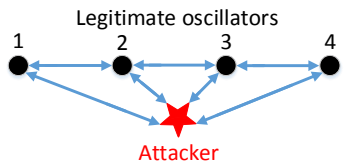

Figure 2.4: A strongly-connected network of five oscillators.

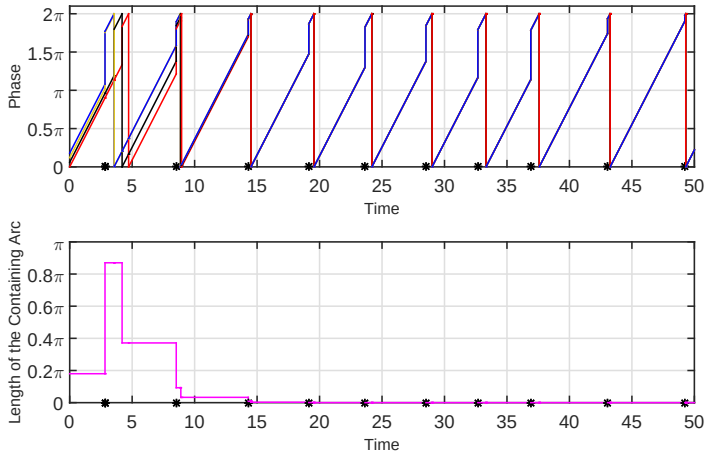

Figure 2.5: Phase evolution and the length of the containing arc of four legitimate oscillators in a five PCO strongly-connected network. One oscillator was compromised and its firing time instants were represented by the asterisks. The initial phases of the legitimate oscillators were set to 0, 0.06π, 0.12π, and 0.18π.

the simulations, synchronization is defined to be achieved when the length of the containing arc of legitimate oscillators becomes less than 1×10^{-5}. The comparison confirmed the limited conservativeness of the analytical predictions.

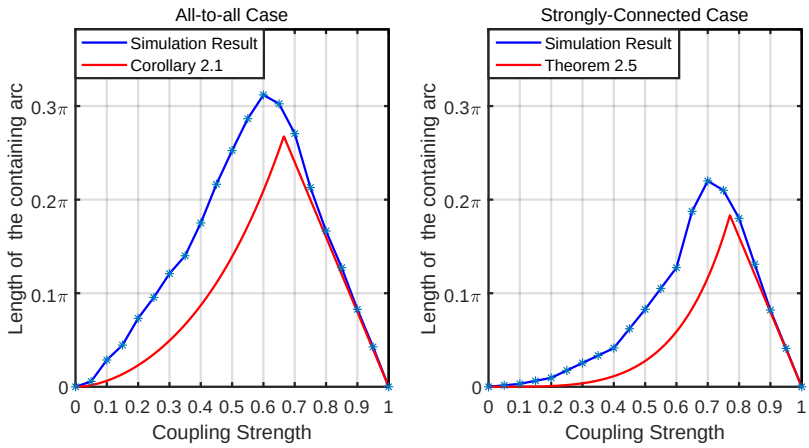

Figure 2.6: Comparison of the theoretically obtained maximally allowable lengths of the initial containing arc with numerical simulations in a five PCO network. l is the coupling strength; the red lines are the maximal lengths of the containing arc obtained from Corollary 2.1 and Theorem 2.5; the blue lines are the corresponding results obtained via numerical simulations.

We also numerically studied the effects of coupling strength l and refractory period D on the convergence rate. We considered an all-to-all network with four legitimate oscillators and a stealthy Byzantine attacker. The initial phases of legitimate oscillators were set to 0, 0.04π, 0.08π, and 0.12π, respectively, which led to a containing arc of length 0.12π. Synchronization is defined to be achieved when the length of the containing arc is less than 1×10^{-5}. The mean synchronization times of legitimate oscillators of $10,000$ runs under different l and D were shown in Fig. 2.7. It can be seen that a larger l leads to a faster convergence rate (shorter convergence time) whereas the variation of D has no obvious influence on the convergence time. This is because the speed of convergence is determined by the frequency and amplitude of phase shifts caused by legitimate pulses, and a larger l increases the amplitude of phase shifts, whereas the variation of D has no influence on the frequency of phase shifts under the specified conditions in Theorems 2.1-2.3 (since under a given length of the containing arc δ, no legitimate pulses will arrive when a legitimate oscillator's phase resides in the interval $[\pi, 2\pi - \delta)$, and hence no difference will be made on the frequency of phase shifts when D varies between $[\pi, 2\pi - \delta)$).

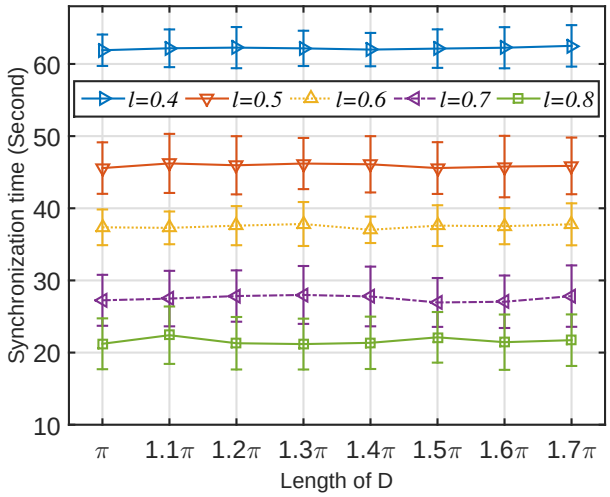

Figure 2.7: Synchronization time of four legitimate oscillators in a five PCO all-to-all network under different l and D. One oscillator was compromised and acts as a stealthy Byzantine attacker. The initial length of the containing arc was set to $\delta = 0.12\pi$. Synchronization of the network is defined to be achieved when the length of the containing arc becomes less than 1×10^{-5}.

2.6.2 Performance comparison with existing results

We also numerically compared the performance of the proposed PRF in (2.2) with the PRFs in [2] and [3]. The initial phases of legitimate oscillators were randomly chosen from the interval $[0, 2\pi]$ and the coupling strength was set to $l = 0.3$. The attacker(s) sent malicious pulses with a random period uniformly distributed in $[1.85\pi, 2.15\pi]$. Synchronization of the network is defined to be achieved when the length of the containing arc of legitimate oscillators is less than 1×10^{-5}. In the presence of one attacker, the probabilities under the three PRFs were given by the red curves in Fig. 2.8. It can be seen that the proposed PRF is more robust in enabling synchronization in the presence of attacks. Of course, the paid price is increased synchronization time, as illustrated by the blue curves in Fig. 2.8. Similar conclusions were obtained for the two-attacker and three-attacker cases, as illustrated in Fig. 2.9 and Fig. 2.10, respectively.

2.6.3 Application to general interaction topologies

As indicated earlier, under a strongly-connected topology, synchronization cannot be guaranteed when only a portion of legitimate oscillators is affected by a malicious attacker. To evaluate the performance of the synchronization approach under such a scenario, we used the synchronization error defined in [2] to

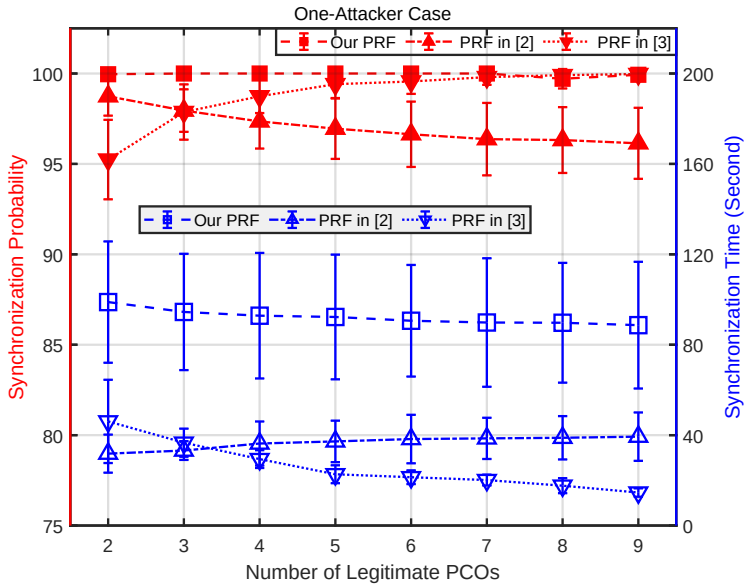

Figure 2.8: Comparison of the proposed PRF and the respective PRFs in [2] and [3] in terms of synchronization probability (red solid marker lines) and synchronization time (blue hollow marker lines) in the presence of one attacker.

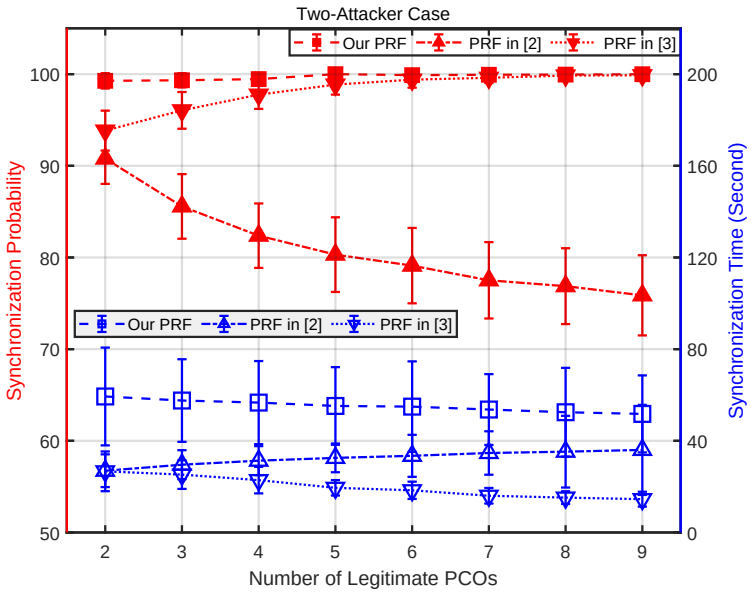

Figure 2.9: Comparison of the proposed PRF and the respective PRFs in [2] and [3] in terms of synchronization probability (red solid marker lines) and synchronization time (blue hollow marker lines) in the presence of two attackers.

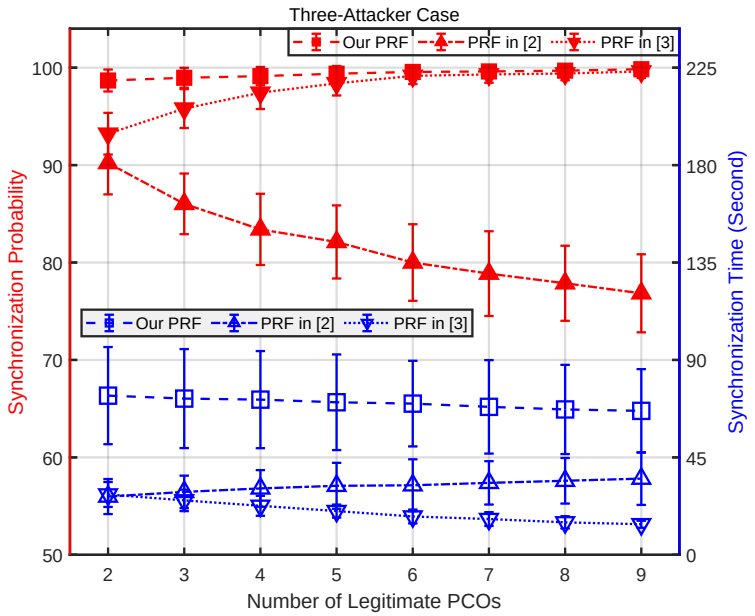

Figure 2.10: Comparison of the proposed PRF and the respective PRFs in [2] and [3] in terms of synchronization probability (red solid marker lines) and synchronization time (blue hollow marker lines) in the presence of three attackers.

compare the performance of our synchronization approach with existing results in [2] and [3].

$$Synchronization\ Error = \max_{i,j\in\mathbb{N}}\{\min\{2\pi - |\phi_i - \phi_j|, |\phi_i - \phi_j|\}$$

where $\mathbb{N}$ is the index set of all legitimate oscillators.

Under three different topologies illustrated in Fig. 2.11, the evolution of synchronization error under our PRF and those in [2, 3] are shown in Fig. 2.12, Fig. 2.13, and Fig. 2.14. In the simulations, the initial phases of legitimate oscillators were randomly chosen from $[0, 2\pi]$ and the coupling strength was set to $l = 0.7$. The attack pulses were sent with a random time separation uniformly distributed in $[1.85\pi, 2.15\pi]$. It can be seen that the proposed PRF has the smallest synchronization error.

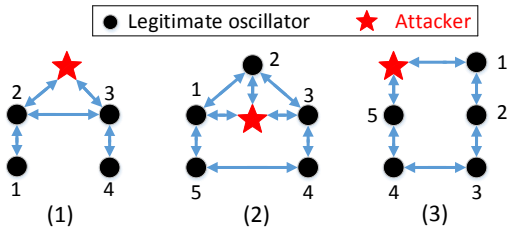

Figure 2.11: Strongly-connected interaction topologies used in simulation.

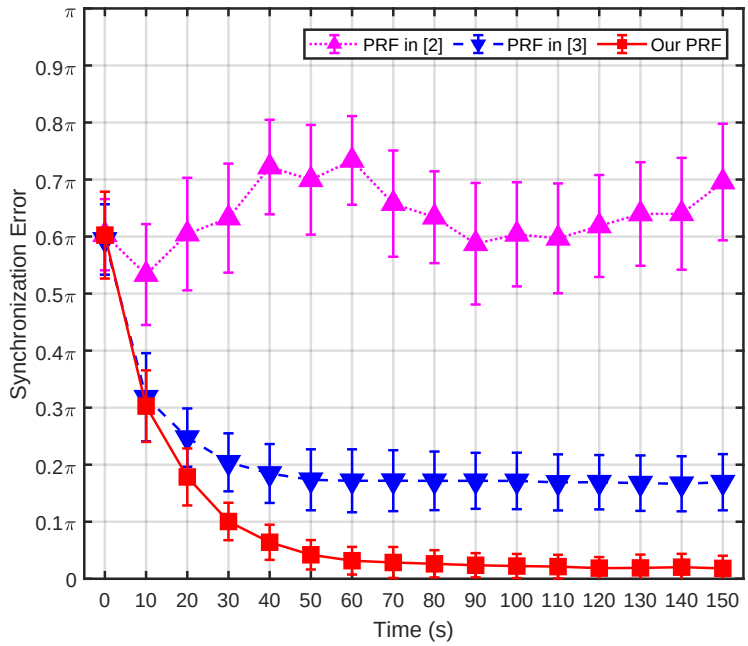

Figure 2.12: Comparison of the new PRF with the PRFs in [2] and [3] in terms of synchronization error in a strongly-connected network of five PCOs (one is the attacker) with topology given in Fig. 2.11. (1). The coupling strength was set to $l = 0.7$.

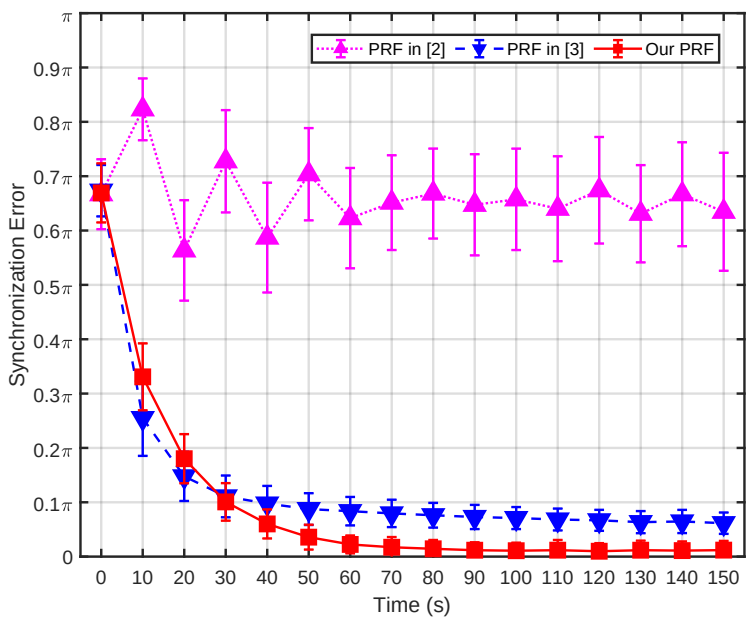

Figure 2.13: Comparison of the new PRF with the PRFs in [2] and [3] in terms of synchronization error in a strongly-connected network of six PCOs (one is the attacker) with topology given in Fig. 2.11. (2). The coupling strength was set to $l = 0.7$.

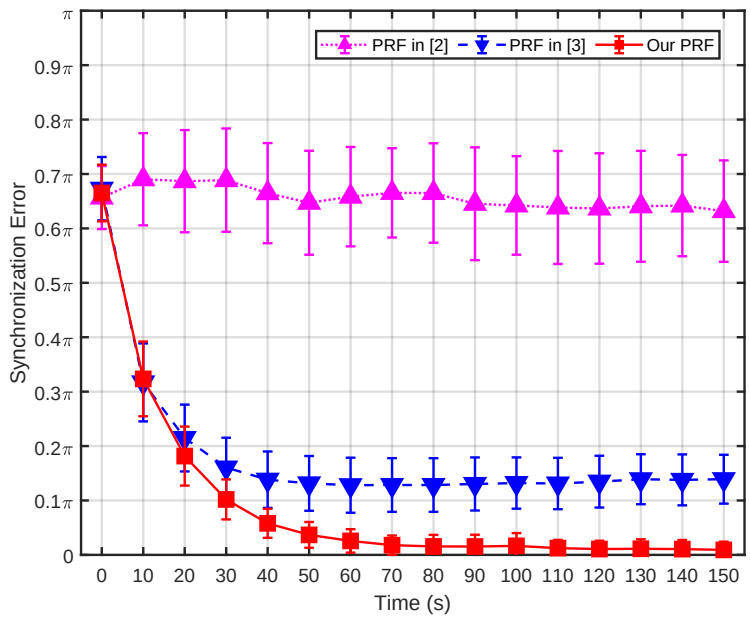

Figure 2.14: Comparison of the new PRF with the PRFs in [2] and [3] in terms of synchronization error in a strongly-connected network of six PCOs (one is the attacker) with topology given in Fig. 2.11. (3). The coupling strength was set to $l = 0.7$.

Chapter 3

A New Attack-Resilient Pulse-Based Synchronization Mechanism for All-to-all PCO Networks

3.1 Introduction

In this chapter, we consider the synchronization of PCOs under multiple stealthy Byzantine attackers. In the pulse-based interaction framework where exchanged messages (so-called pulses) are identical and content-free, Byzantine attacks mean compromised nodes injecting pulses using judiciously crafted patterns to disturb the synchronization process. We consider stealthy Byzantine attacks which are intelligent and only use pulse injection patterns undetectable by legitimate nodes. So compared with existing results in [2, 3, 64], the situation considered in this chapter is more difficult to deal with due to the intelligent behavior of malicious attackers. By proposing a new pulse-based synchronization mechanism, we show that perfect synchronization of legitimate oscillators can still be guaranteed even when their initial phases are randomly distributed in the entire oscillation period $[0, 2\pi]$, which is in distinct difference from our recent results in Chapter 2 requiring initial phases to be restricted in a certain interval. The approach is applicable even when individual oscillators do not have access to the total number of oscillators in a network.

This chapter is organized as follows. Section 3.2 introduces a new pulse-based synchronization mechanism. Section 3.3 characterizes the synchronization condition of all-to-all PCOs under the new syn-

chronization mechanism in the absence of attacks. In Section 3.4, under a pulse-number based detection mechanism, we characterize the condition for an attacker to keep stealthy, i.e., mounting attacks without being detected. In Section 3.5, we prove that synchronization of legitimate oscillators can be guaranteed even in the presence of multiple stealthy Byzantine attackers. We also extend the results to relaxed initial conditions, i.e., arbitrary distribution on the entire oscillation period $[0, 2\pi]$ in Section 3.5. In Section 3.6, we further show that our approach is still applicable even when the total number of oscillators in a network is unknown to individual oscillators. Simulation results are presented in Section 3.7.

3.2 A New Pulse-Based Interaction Mechanism

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

Conventional Pulse-Based Synchronization Mechanism [24]:

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:

$$\phi_i^+ = \phi_i + l \times F(\phi_i) \tag{3.1}$$

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

$$F(\phi) := \begin{cases} -\phi & 0 \leq \phi \leq \pi \\ 2\pi - \phi & \pi < \phi \leq 2\pi \end{cases} \tag{3.2}$$

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

New Pulse-Based Synchronization Mechanism (Mechanism 3.1):

---

1. The phase ϕ_i of oscillator i evolves from 0 to 2π rad with a constant speed $\omega = 1$ rad/second.

2. Once ϕ_i reaches 2π rad, oscillator i fires (emits a pulse) and resets its phase to 0.

3. When oscillator i receives a pulse at time instant t, it shifts its phase according to (3.1) only when both of the following conditions are satisfied:

   (a) an entire period $T = 2\pi$ seconds has elapsed since initiation;

   (b) in the past quarter period, oscillator i fired and received at least $\lambda - 1$ pulses, or oscillator i did not fire but received at least λ pulses within this past quarter period, where $\lambda = \lfloor (N-1)/5 \rfloor$ holds and $\lfloor \bullet \rfloor$ is the largest integer no greater than "$\bullet$."

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

Fig. 3.1 gives the evolution of one legitimate oscillator's phase in a network of eleven PCOs. Given $\lambda = \lfloor (N-1)/5 \rfloor = 2$, we have that a pulse can trigger a phase jump on a receiving oscillator only when 1) it is sent after time T has elapsed since initiation; and 2) in the past quarter period, at least two pulses were received by the oscillator, or the oscillator fired and received at least one other pulse in the past quarter period. Therefore, in Fig. 3.1, only the 9th pulse causes a jump on the phase of the considered oscillator.

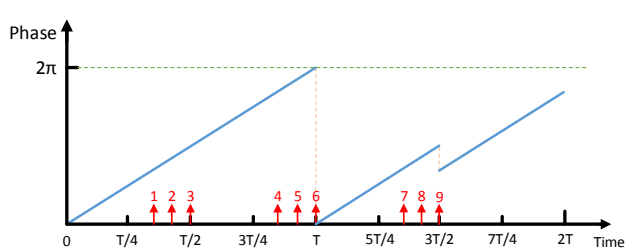

Figure 3.1: The phase evolution of a legitimate oscillator in an all-to-all network of eleven oscillators under Mechanism 3.1. Vertical pulses represent incoming pulses.

Remark 3.1. *Following [35, 36, 42], we assume that when a legitimate oscillator receives multiple pulses simultaneously, it will process these pulses consecutively. In other words, no two pulses will be regarded as an aggregated pulse.*

Remark 3.2. *Compared with the conventional pulse-based synchronization mechanism, the new one is more resilient to malicious pulse attacks, as illustrated later by the simulation results in Fig. 3.7, Fig. 3.8, Fig. 3.9, and Fig. 3.10. Rigorous analysis will be provided in Section* 3.4.

3.3 Synchronization of All-to-All PCOs in the Absence of Attacks

In this section, we will show that all-to-all connected oscillators can be guaranteed to synchronize under Mechanism 3.1 in the absence of attacks. To this end, we first define synchronization:

Definition 3.1 (Synchronization): *We define synchronization to be achieved when all legitimate oscillators fire at the same time instants.*

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

Definition 3.2 (Containing Arc): *The containing arc is defined as the shortest arc on the unit circle that contains all legitimate oscillators' phases.*

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

We first characterize the property of all-to-all PCO networks under Mechanism 3.1.

Lemma 3.1. *In an attack-free all-to-all network of N PCOs, if the firing of an oscillator can trigger a phase jump on another oscillator, then the firing can trigger phase jumps on all the other $N-1$ oscillators.*

Proof. Without loss of generality, we assume that oscillator i's firing at time instant t_i triggers the phase of oscillator j to jump, which, according to Mechanism 3.1, implies that oscillator j either fired and received at least $\lambda - 1$ pulses in the past quarter period, or it did not fire in the past quarter period but received at least λ pulses within. In both cases, it can be inferred that for any oscillator other than i, if it fired in the past quarter period, then it must have received at least $\lambda - 1$ pulses under the considered all-to-all topology; or if it did not fire in the past quarter period, then it must have received at least λ pulses within. Therefore, in an all-to-all topology, if the firing of an oscillator i triggers another oscillator j to jump, then it will trigger all the other $N-1$ oscillators to jump. □

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

Theorem 3.1. *For an attack-free all-to-all network of N PCOs, if the length of the initial containing arc is less than π rad, then Mechanism* 3.1 *can achieve perfect synchronization.*

Proof. First, we will show that the length of the containing arc will never increase. It can be easily inferred that the length of the containing arc remains unchanged if no oscillator jumps in phase. So we only need to consider the case that an oscillator's firing triggers a jump on another oscillator. Based on Lemma 3.1, one can know that if the firing of an oscillator triggers a jump on another oscillator, it will trigger phase jumps on all the other oscillators.

We assume that oscillator i fires at time instant t_i whose pulse triggers phase jumps on all the other oscillators. One can easily get $\phi_i(t_i) = 2\pi$ *rad*, i.e., the containing arc includes the phase point 2π *rad* at time instant t_i. Since the length of the containing arc is less than π *rad*, the phases of the other $N-1$ oscillators at this time instant can only be distributed in the following three ways, as depicted in Fig. 3.2:

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

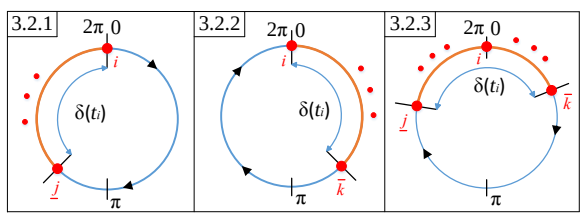

Figure 3.2: Three possible phase distribution of all oscillators when oscillator i fires at time instant t_i.

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

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

$$\delta(t_i) = \phi_i(t_i) - \min_{j \in \mathcal{N}, j \neq i} \{\phi_j(t_i)\} = 2\pi - \phi_{\underline{j}}(t_i) \tag{3.3}$$

where $\mathcal{N} = \{1, 2, \cdots, N\}$ represents the index set and $\underline{j} = \arg\min_{j \in \mathcal{N}, j \neq i} \phi_j(t_i)$. After the firing of oscillator i, we have $\phi_i^+(t_i) = 0$. Under the PRF in (3.2), one can get $\phi_j^+(t_i) = \phi_j(t_i) + l(2\pi - \phi_j(t_i))$

for $j \in \mathcal{N}, j \neq i$. The length of the containing arc becomes

$$\begin{aligned}\delta^+(t_i) &= 2\pi - \min_{j\in\mathcal{N}, j\neq i}\{\phi_j^+(t_i)\} + \phi_i^+(t_i) = 2\pi - \min_{j\in\mathcal{N}, j\neq i}\{\phi_j^+(t_i)\} \\ &= (1-l)(2\pi - \phi_{\underline{j}}(t_i)) = (1-l)\delta(t_i)\end{aligned} \tag{3.4}$$

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

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

$$\delta(t_i) = 2\pi - \phi_i(t_i) + \max_{k\in\mathcal{N}, k\neq i}\{\phi_k(t_i)\} = \phi_{\bar{k}}(t_i) \tag{3.5}$$

where $\bar{k} = \arg\max_{k\in\mathcal{N}, k\neq i}\phi_k(t_i)$. After the firing of oscillator i, we have $\phi_i^+(t_i) = 0$. Under the PRF in (3.2), one can get $\phi_k^+(t_i) = (1-l)\phi_k(t_i)$ for $k \in \mathcal{N}, k \neq i$ and the length of the containing arc becomes

$$\delta^+(t_i) = \max_{k\in\mathcal{N}, k\neq i}\{\phi_k^+(t_i)\} - \phi_i^+(t_i) = \max_{k\in\mathcal{N}, k\neq i}\{\phi_k^+(t_i)\} = (1-l)\phi_{\bar{k}}(t_i) = (1-l)\delta(t_i) \tag{3.6}$$

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

3. When the other $N-1$ oscillators' phases reside partially in $[0, \pi)$ and partially in $(\pi, 2\pi]$, given $\phi_i(t_i) = 2\pi$ *rad*, we represent the set of oscillators with phases in $[0, \pi)$ as $\mathcal{N}_1$ and the set of oscillators with phases in $(\pi, 2\pi]$ as $\mathcal{N}_2$. One can easily get $\mathcal{N}_1 \cup \mathcal{N}_2 = \mathcal{N}$ and $\mathcal{N}_1 \cap \mathcal{N}_2 = \emptyset$. The length of the containing arc at time instant t_i can be expressed as

$$\delta(t_i) = 2\pi + \max_{k\in\mathcal{N}_1}\{\phi_k(t_i)\} - \min_{j\in\mathcal{N}_2, j\neq i}\{\phi_j(t_i)\} = 2\pi + \phi_{\bar{k}}(t_i) - \phi_{\underline{j}}(t_i) \tag{3.7}$$

where $\underline{j} = \arg\min_{j\in\mathcal{N}_2, j\neq i}\phi_j(t_i)$ and $\bar{k} = \arg\max_{k\in\mathcal{N}_1}\phi_k(t_i)$. After the firing of oscillator i, we have $\phi_i^+(t_i) = 0$. Under the PRF in (3.2), we can get $\phi_k^+(t_i) = (1-l)\phi_k(t_i)$ for $k \in \mathcal{N}_1$ and $\phi_j^+(t_i) = \phi_j(t_i) + l(2\pi - \phi_j(t_i))$ for $j \in \mathcal{N}_2, j \neq i$. The length of the containing arc becomes

$$\delta^+(t_i) = 2\pi + \max_{k\in\mathcal{N}_1}\{\phi_k^+(t_i)\} - \min_{j\in\mathcal{N}_2, j\neq i}\{\phi_j^+(t_i)\} = (1-l)(2\pi + \phi_{\bar{k}}(t_i) - \phi_{\underline{j}}(t_i)) = (1-l)\delta(t_i) \tag{3.8}$$

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

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

Next, we proceed to prove that the length of the containing arc will decrease to 0. To this end, we first show that every oscillator will fire at least once within a certain time period. Without loss of generality, we set the initial time instant as $t_0 = 0$. Since the initial length of the containing arc is less than π *rad* and it is non-increasing, as analyzed earlier, there exists a time instant $t_1 > T$ at which all oscillators' phases reside in $(\pi, 2\pi]$. At this time instant, noting that the PRF in (3.2) is non-negative in $(\pi, 2\pi]$, we can get that exchanged pulses can only advance or have no effect on a receiving oscillator's phase. Therefore, all oscillators will reach phase 2π *rad* and fire within the time interval $[t_1, t_1 + T/2]$. On the other hand, since the PRF in (3.2) is non-positive in $[0, \pi]$, we can get that exchanged pulses can only delay or have no effect on a receiving oscillator's phase residing in $[0, \pi]$. So it takes at least $T/2$ time for an oscillator's phase to evolve from 0 to π *rad*. Therefore, no oscillator can surpass phase point π *rad* at time instant $t_1 + T/2$. In other words, each oscillator fired once within $[t_1, t_1 + T/2]$ and all oscillators' phases reside in $[0, \pi]$ at time instant $t_1 + T/2$.

Next, we proceed to prove that there exists at least one oscillator, whose firing can trigger jumps on all the other oscillators' phases within the time interval $[t_1, t_1 + T/2]$. Assume to the contrary that no oscillator's firing triggers a jump on any other oscillators within $[t_1, t_1 + T/2]$. So condition b) of Mechanism 3.1 cannot be satisfied, which means that no greater than λ oscillators fired in any quarter period within the time interval $[t_1, t_1 + T/2]$. Hence, no greater than λ oscillators fired in the time interval $[t_1, t_1 + T/4]$ and the same is true for the interval $[t_1 + T/4, t_1 + T/2]$. Therefore, no greater than $2\lambda < N$ oscillators fired within $[t_1, t_1 + T/2]$, which contradicts the fact that all oscillators fired once within $[t_1, t_1 + T/2]$. So we can conclude that there exists at least one firing event that triggers phase jumps on the other $N-1$ oscillators within $[t_1, t_1 + T/2]$.

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

At time instant $t_1 + T/2$, the phases of all oscillators reside in $[0, \pi]$ and they will evolve freely toward

$(\pi, 2\pi]$. By repeating the above analyses, we can get that the length of the containing arc will be decreased by the firing of at least one oscillator in a firing round until it converges to 0. Therefore, synchronization of the network can be achieved. □

Next, we show that the initial phase distribution requirement in Theorem 3.1 can be removed, i.e., under all-to-all topology, the new synchronization mechanism can guarantee synchronization even when the phases of oscillators are arbitrarily distributed in $[0, 2\pi]$.

Theorem 3.2. *For an attack-free all-to-all network of N PCOs, if the initial phases of all oscillators are randomly distributed in* $[0, 2\pi]$*, then Mechanism* 3.1 *can achieve perfect synchronization as long as the coupling strength satisfies* $l > 0.5$.

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

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

Under the assumption that no pulse can trigger a jump on any oscillator's phase within $[t_1, t_1 + T]$, we have that condition $b)$ of Mechanism 3.1 cannot be satisfied, i.e., no greater than λ oscillators fired in any quarter oscillation period within the time interval $[t_1, t_1 + T]$. Hence, no greater than λ oscillators fired in the time interval $[t_1, t_1 + T/4]$ and the same is true for intervals $[t_1 + T/4, t_1 + T/2]$, $[t_1 + T/2, t_1 + 3T/4]$, and $[t_1 + 3T/4, t_1 + T]$. Therefore, no greater than $4\lambda < N$ oscillators fired within $[t_1, t_1 + T]$, which contradicts the assumption that N oscillators fired within $[t_1, t_1 + T]$. So at least one oscillator's firing will trigger all the other oscillators' phases to jump in $[t_1, t_1 + T]$.

We assume that oscillator i's firing at $t_i \in [t_1, t_1 + T]$ triggers a jump on all the other $N-1$ oscillators. Denoting $\phi_k(t_i)$ as the phase of oscillator $k \in \mathcal{N} = \{1, 2, \cdots, N\}$ at time instant t_i, one can get $\phi_i^+(t_i) = 0$ and $\phi_k^+(t_i) = \phi_k(t_i) + F(\phi_k(t_i))$ for $k \in \mathcal{N}, k \neq i$. When $l > 0.5$ is true, the PRF in (3.2) leads to $\phi_k^+(t_i) \in (3\pi/2, 2\pi]$ for $\phi_k(t_i) \in (\pi, 2\pi]$ and $\phi_k^+(t_i) \in [0, \pi/2)$ for $\phi_k(t_i) \in [0, \pi]$. Hence, the phase of all oscillators reside in $(3\pi/2, 2\pi] \cup [0, \pi/2)$ and the length of the containing arc is less than π *rad*. Using Theorem 3.1, we have that all oscillators will synchronize. □

3.4 Stealthy Byzantine Attacks

The concept of Byzantine attacks stems from the Byzantine generals problem [48]. It is used to describe a traitor commander who sends or relays fake information to other commanders to avoid the loyal ones from reaching agreement [47]. In the case of PCO synchronization, Byzantine attacks are assumed to be able to compromise an oscillator and completely take over its behavior. So an oscillator compromised by Byzantine attacks will emit pulses at arbitrary time instants. Apparently, if an attacker keeps sending pulses continuously without rest, it can effectively prevent legitimate oscillators from reaching synchronization. However, such a manner of attacks will also render themselves easily detectable, just as jamming of communication channels being easy to detect, isolate, and remove [69]. Therefore, we are only interested in "stealthy" Byzantine attacks which cannot be detected by legitimate oscillators in the pulse-based interaction framework.

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

Theorem 3.3. *For an all-to-all network of N legitimate PCOs under Mechanism* 3.1*, one oscillator can receive at most $N-1$ pulses within any time interval $[t, t+T/2]$ for $t \geq 0$.*

Proof. Without loss of generality, we assume that oscillator i emits a pulse and resets its phase to 0 at time instant t_1, i.e., $\phi_i(t_1) = 2\pi$ *rad* and $\phi_i^+(t_1) = 0$. Under Mechanism 3.1 and the PRF in (3.2), one can get that the phase evolution of oscillator i from 0 to π *rad* can only be decelerated (or unaffected) by received pulses. Hence, it takes oscillator i at least $T/2$ time to evolve from 0 to π *rad*, which, combined with the fact that a node cannot jump from π *rad* to 2π *rad* instantaneously (the value of PRF in (3.2) is $-\pi$ *rad* at phase π *rad*), further means that it takes oscillator i over $T/2$ to evolve from 0 to 2π *rad*. In other words, within any time interval $[t, t+T/2]$ for $t \geq 0$, oscillator i can emit at most one pulse. Therefore, an oscillator can emit at most one pulse during an arbitrary time interval $[t, t+T/2]$ for $t \geq 0$.

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

$N-1$ pulses within an arbitrary time interval $[t, t+T/2]$ for $t \geq 0$. □

Based on Theorem 3.3, we have, under the pulse number based detection mechanism, that any oscillator's receiving more than $N-1$ pulses within an arbitrary time interval $[t, t+T/2]$ implies the presence of attacks.

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

Stealthy Byzantine Attack Model: *For an all-to-all network of N PCOs under Mechanism* 3.1*, one compromised oscillator can launch stealthy Byzantine attacks as long as it injects pulses with a time separation of length over* $T/2$.

Remark 3.3. *In this chapter, the detection mechanism only considers the minimal separation within which one oscillator can receive at most* $N-1$ *pulses (i.e.,* $T/2$*) because it is extremely hard to find a tight maximal separation during which one oscillator can receive at least* $N-1$ *pulses. Another reason for not imposing a maximal separation is that in practice, pulse dropout is unavoidable, which makes it impossible to guarantee that each oscillator will receive at least* $N-1$ *pulses within a certain time interval.*

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

In this section, we address the synchronization of PCO networks in the presence of stealthy Byzantine attacks. Among N PCOs, we assume that M are compromised and act as stealthy Byzantine attackers. Specifically, we will show that the proposed pulse-based interaction mechanism can synchronize legitimate oscillators even in the presence of multiple stealthy Byzantine attackers. More interestingly, we can prove that legitimate oscillators can synchronize even when their initial phases are randomly distributed in the entire oscillation period $[0, 2\pi]$. Similar to Lemma 3.1, we first establish the following property for PCO networks:

Lemma 3.2. *For an all-to-all network of N PCOs among which M are compromised and act according to the stealthy Byzantine attack model in Section* 3.4*, if the firing of an arbitrary oscillator (either legitimate or malicious) triggers a phase jump on a legitimate oscillator, then the firing can trigger phase jumps on all legitimate oscillators.*

Proof. Noting that the topology of the network is all-to-all, one can get that an oscillator's pulse can be received by all the other oscillators. Hence, Lemma 3.2 can be acquired by following the same line of

reasoning in Lemma 3.1. □

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

Theorem 3.4. *For an all-to-all network of N PCOs among which M are compromised and act according to the stealthy Byzantine attack model in Section* 3.4*, if the number of compromised oscillators M is no greater than $\lfloor (N-1)/5 \rfloor$ and the initial length of the containing arc is less than $\pi/2$ rad, then all legitimate oscillators can be perfectly synchronized under Mechanism* 3.1.

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

Part I (The length of the containing arc of legitimate oscillators is non-increasing): It can be easily inferred that the length of the containing arc of legitimate oscillators remains unchanged if no legitimate oscillator jumps in phase. So we only consider the case that an oscillator's firing (say oscillator i, either legitimate or malicious) triggers a jump on a legitimate oscillator, say oscillator j where $j \neq i$. Based on Lemma 3.2, if the firing of oscillator i triggers a phase jump on a legitimate oscillator j, it will trigger phase jumps on all legitimate oscillators.

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

Case 1: Oscillator i is legitimate.

When oscillator i is legitimate, we have $\phi_i(t_i) = 2\pi$ *rad*, i.e., the containing arc of legitimate oscillators includes point 2π *rad* at time instant t_i. Since the number of legitimate oscillators is $N-M$ and the length of the containing arc of legitimate oscillators is less than $\pi/2$ *rad*, the phases of the other $N-M-1$ legitimate oscillators can only be distributed in the following three ways at time instant t_i, as depicted in Fig. 3.3:

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

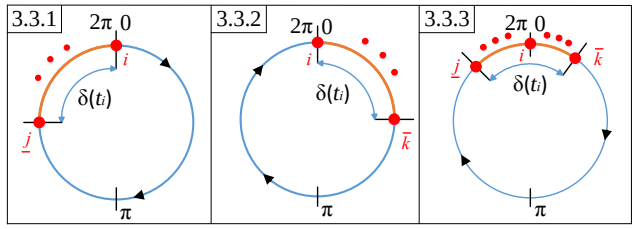

Figure 3.3: Three possible phase distribution of all legitimate oscillators when legitimate oscillator i fires at time instant t_i.

Denoting $\delta(t_i)$ as the length of the containing arc of legitimate oscillators at time instant t_i, one can easily obtain $\delta^+(t_i) \leq \delta(t_i)$ in all above three cases by following the same line of reasoning in Theorem 3.1. Hence, we can get that the firing of a legitimate oscillator cannot increase the length of the containing arc of legitimate oscillators.

Case 2: Oscillator i is a stealthy Byzantine attacker.

According to Mechanism 3.1, upon receiving a pulse, legitimate oscillator j will jump in phase when it either fired and received at least $\lambda - 1$ pulses in the past quarter period, or it did not fire but received at least λ pulses in the past quarter period. In both cases, it can be inferred that at least λ oscillators fired in the quarter period immediately prior to t_i.

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

Since the PRF in (3.2) is non-positive in $[0, \pi/2]$, we can get that exchanged pulses can only delay or have no effect on a receiving legitimate oscillator whose phase resides in $[0, \pi/2]$. So it takes at least $T/4$ time for a legitimate oscillator to evolve from 0 to $\pi/2$ *rad*. Hence, at least one legitimate oscillator (who fired in the past quarter period) has phase residing in $[0, \pi/2]$ at time instant t_i. Since the length of the containing arc of legitimate oscillators is less than $\pi/2$ *rad*, the phases of all $N-M$ legitimate oscillators can only be distributed in the following two ways at t_i, as depicted in Fig. 3.4:

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

2. the $N-M$ legitimate oscillators reside partially in $[0, \pi/2]$ and partially in $(3\pi/2, 2\pi]$.

Denoting $\delta(t_i)$ as the length of the containing arc of legitimate oscillators at time instant t_i, next we

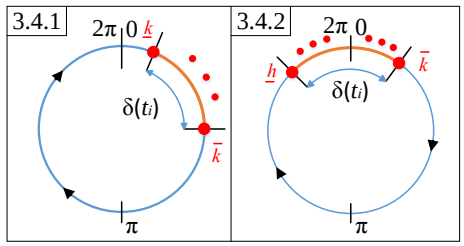

Figure 3.4: Two possible phase distribution of all legitimate oscillators when compromised oscillator i fires at time instant t_i.

show that $\delta(t_i)$ cannot be increased by the firing of oscillator i in both scenarios, i.e., $\delta^+(t_i) \leq \delta(t_i)$ always holds.

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

$$\delta(t_i) = \max_{k\in\mathcal{N}_3}\{\phi_k(t_i)\} - \min_{k\in\mathcal{N}_3}\{\phi_k(t_i)\} = \phi_{\bar{k}}(t_i) - \phi_{\underline{k}}(t_i) \tag{3.9}$$

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

$$\begin{aligned}\delta^+(t_i) &= \max_{k\in\mathcal{N}_3}\{\phi_k^+(t_i)\} - \min_{k\in\mathcal{N}_3}\{\phi_k^+(t_i)\} = \phi_{\bar{k}}^+(t_i) - \phi_{\underline{k}}^+(t_i) = (1-l)(\phi_{\bar{k}}(t_i) - \phi_{\underline{k}}(t_i)) \\ &= (1-l)\delta(t_i)\end{aligned} \tag{3.10}$$

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

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

$$\delta(t_i) = 2\pi + \max_{k\in\mathcal{N}_4}\{\phi_k(t_i)\} - \min_{h\in\mathcal{N}_5}\{\phi_h(t_i)\} = 2\pi + \phi_{\bar{k}}(t_i) - \phi_{\underline{h}}(t_i) \tag{3.11}$$

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

the containing arc of legitimate oscillators becomes

$$\begin{aligned}\delta^+(t_i) &= 2\pi + \max_{k\in\mathcal{N}_4}\{\phi_k^+(t_i)\} - \min_{h\in\mathcal{N}_5}\{\phi_h^+(t_i)\} = 2\pi + \phi_{\bar{k}}^+(t_i) - \phi_{\underline{h}}^+(t_i) \\ &= (1-l)(2\pi + \phi_{\bar{k}}(t_i) - \phi_{\underline{h}}(t_i)) = (1-l)\delta(t_i) \end{aligned} \tag{3.12}$$

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

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

Part II (The length of the containing arc of legitimate oscillators will decrease to 0): To prove that the length of the containing arc of legitimate oscillators will keep decreasing, we only need to show that pulses which trigger phase jumps on legitimate oscillators will keep occurring until the length of the containing arc of legitimate oscillators reaches zero. Because if none of legitimate oscillators' phases are trapped in some sub-interval within $[0, 2\pi]$, then all legitimate oscillators will keep firing repeatedly within one quarter period interval from each other (note that as proven before, the containing arc of legitimate oscillators is non-increasing and hence is always less than $\pi/2$ *rad*). Given that the number of legitimate oscillators is $N - M > \lambda$, it can be easily inferred that at least the firing of one legitimate oscillator will trigger a phase jump according to Mechanism 3.1 in Section 3.2. Therefore, to prove that the length of the containing arc of legitimate oscillators will decrease to zero, it is sufficient to show that no legitimate oscillator will stop from firing.

Given that once the phase of a legitimate oscillator surpasses π *rad*, it cannot be stopped from firing (because its phase can only be advanced under the PRF in (3.2)). Further taking into account the fact that pulses from stealthy attackers alone (no greater than λ) are not enough to trigger any phase shift according to Mechanism 3.1 in Section 3.2, we have that at least one legitimate oscillator can fire repeatedly (Note that if no phase jumps are triggered, then legitimate oscillators will evolve freely and fire periodically).

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

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

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

Next, we show that the initial phase distribution requirement in Theorem 3.4 can be removed, i.e., Mechanism 3.1 can guarantee synchronization in the presence of attacks even when all legitimate oscillators' initial phases are arbitrarily distributed in $[0, 2\pi]$.

Theorem 3.5. *For an all-to-all network of N PCOs, within which M oscillators are compromised and act as stealthy Byzantine attackers, if the number of compromised oscillators M is no greater than* $\lfloor (N-1)/5 \rfloor$*, then all legitimate oscillators can be perfectly synchronized under Mechanism* 3.1 *from any initial phase distribution when the coupling strength satisfies* $l > 0.75$.

Proof. Without loss of generality, we set the initial time instant to $t_0 = 0$. Similar to the proof of Theorem 3.2, we first show that for any time interval $[t_1, t_1 + T]$ with $t_1 > T$, there exists one firing event which can trigger a phase jump on a legitimate oscillator.

Assume to the contrary that no pulse can trigger a phase jump on a legitimate oscillator within $[t_1, t_1 + T]$. One can get that the phase distance between any two legitimate oscillators is invariant within $[t_1, t_1 + T]$. Since T is the natural period, every legitimate oscillator will evolve freely for a full cycle on the unit circle and fire once during $[t_1, t_1 + T]$. In other words, $N - M$ legitimate oscillators fired within $[t_1, t_1 + T]$. On the other hand, under the stealthy Byzantine attack model in Section 3.4, every attacker can fire at most twice during $[t_1, t_1 + T]$. Hence, at least $N - M$ oscillators fired during $[t_1, t_1 + T]$.

Under the assumption that no pulse can trigger a jump on any legitimate oscillator within $[t_1, t_1 + T]$, we have that condition $b)$ of Mechanism 3.1 cannot be satisfied, i.e., no greater than λ oscillators fired in any quarter oscillation period within the time interval $[t_1, t_1 + T]$. Hence, no greater than λ oscillators fired in the time interval $[t_1, t_1 + T/4]$ and the same is true for intervals $[t_1 + T/4, t_1 + T/2]$, $[t_1 + T/2, t_1 + 3T/4]$, and

$[t_1+3T/4, t_1+T]$. Therefore, no greater than 4λ oscillators fired within $[t_1, t_1+T]$ and one can easily get

$$4\lambda < N - M \tag{3.13}$$

which contradicts the assumption that at least $N-M$ oscillators fired within $[t_1, t_1+T]$. Therefore, at least one oscillator's firing can trigger a phase jump on a legitimate oscillator within $[t_1, t_1+T]$. Based on Lemma 3.2, we further know that the pulse will trigger phase jumps on all legitimate oscillators.

Denoting $\phi_k(t_i)$ as the phase of a legitimate oscillator jumps in phase at time instant t_i, one can get $\phi_k^+(t_i) = \phi_k(t_i) + F(\phi_k(t_i))$. When $l > 0.75$ is true, phase shift under PRF in (3.2) leads to $\phi_k^+(t_i) \in (7\pi/4, 2\pi]$ for $\phi_k(t_i) \in (\pi, 2\pi]$ and $\phi_k^+(t_i) \in [0, \pi/4)$ for $\phi_k(t_i) \in [0, \pi]$. Hence, the phase of all legitimate oscillators will reside in $(7\pi/4, 2\pi] \cup [0, \pi/4)$ after this firing event and the length of the containing arc will become less than $\pi/2$ *rad*. Using Theorem 3.4, we have that all oscillators will synchronize despite the presence of attackers. □

Remark 3.4. *The proof above also contains the reason for us to set λ to $\lfloor (N-1)/5 \rfloor$ in Mechanism 3.1: Our key idea for attack resilience is to avoid attack pulses alone from being able to trigger phase jumps on legitimate oscillators, so we have to choose λ that is no less than M, the number of attackers. Further taking into consideration of (3.13), which is necessary to guarantee global synchronization, we can have $\lambda < N/5$. Therefore, we set $\lambda = \lfloor (N-1)/5 \rfloor$, the maximal integer satisfying $\lambda < N/5$, to make the Mechanism be able to tolerate more attackers.*

Remark 3.5. *It is worth noting that existing resilient pulse-based synchronization approaches in [2] and [3] cannot guarantee perfect synchronization for all-to-all PCO networks under the considered stealthy Byzantine attackers even when the coupling strength is larger than 0.5, as illustrated by the numerical simulations in Fig. 3.9 and Fig. 3.10. Hence, our synchronization approach is highly non-trivial and more resilient in enabling PCO synchronization in the presence of such attackers.*

Next, we analyze the convergence speed of Mechanism 3.1. From the proof of Theorem 3.4 and Theorem 3.5, we know that the speed at which the containing arc of legitimate oscillators decreases to zero is proportional to the number of effective pulses (i.e., pulses which can trigger jumps on all legitimate oscillators' phases) and the magnitude of phase jumps. Hence we have the following results on the convergence speed of Mechanism 3.1:

Theorem 3.6. *Under the synchronization conditions in Theorem 3.5, the time to synchronization of all legitimate oscillators under Mechanism* 3.1 *is propositional to*

$$\frac{\lambda}{l(N-M)} \tag{3.14}$$

Proof. According to the proof of Theorem 3.4 and Theorem 3.5, we know that the speed at which the containing arc of legitimate oscillators decreases to zero is proportional to the number of effective pulses (i.e., pulses which can trigger jumps on all legitimate oscillators' phases) and the magnitude of phase jumps. One can easily get that the number of effective pulses is proportional to the number of legitimate oscillators, i.e., $N-M$, but inversely proportional to λ, and the magnitude of phase jumps is proportional to the coupling strength l under a given phase response function. Therefore, we can get that the time to synchronization is proportional to (3.14). □

Remark 3.6. *From Theorem 3.6, and the synchronization derivations in Theorem 3.5, we can get that if λ were to allowed to be chosen from $\{1,2,...,\lfloor(N-1)/5\rfloor\}$ and is no less than the number of attackers in the network, then synchronization can also be achieved. Furthermore, combining Theorem 3.6 (which indicates that a larger λ reduces synchronization speed) and Remark 3.4 (which implies that a larger λ leads to resilience to more stealthy attackers), we have that a trade-off exists between resilience to attackers and synchronization speed if λ in Mechanism* 3.1 *were allowed to be chosen from $\{1,2,...,\lfloor(N-1)/5\rfloor\}$. In this chapter, we set λ to $\lfloor(N-1)/5\rfloor$ to guarantee resilience to more attackers.*

3.6 Extension to the Case where N is Unknown

In this section, we extend our approach to the case where the total number of oscillators, i.e., N, is unknown to individual oscillators. In this case, the exact number of compromised oscillators that a network can tolerate, i.e., λ in Mechanism 3.1, cannot be determined precisely by each individual oscillator. As the implementation of Mechanism 3.1 requires the knowledge of λ, we have to revise it to accommodate the fact that λ is unavailable. Based on the observation that under the stealthy attacker model in Section 3.4, each oscillator can use the number of received pulses to estimate the number of oscillators in a network, we revise Mechanism 3.1 to make it applicable to cases where N is unknown to individual oscillators. More specifically, we will prove that the revised mechanism can still guarantee global synchronization in the presence of compromised oscillators as long as their number is no larger than 10% of the total number of oscillators in

the network.

The same as Mechanism 3.1, we allow each oscillator to evolve freely for the first oscillation period $[0,T]$. So each oscillator's phase will reach 2π *rad* at a certain time instant within $[0,T]$ upon which the oscillator will emit a pulse. Note that when the network is all-to-all, every oscillator will receive the same number of pulses. Based on the number of received pulses in the first oscillation period $[0,T]$, we propose the following mechanism:

New Pulse-Based Synchronization Mechanism (Mechanism 3.2):

---

1. The phase ϕ_i of oscillator i evolves from 0 to 2π rad with a constant speed $\omega = 1$ rad/second.

2. Once ϕ_i reaches 2π rad, oscillator i fires (emits a pulse) and resets its phase to 0.

3. In the first oscillation period $[0,T]$, each oscillator i counts the number of received pulses, and stores this number as P_i.

4. When oscillator i receives a pulse at time instant t, it shifts its phase according to (3.1) only when both of the following conditions are satisfied:

   (a) an entire period T has elapsed since initiation;

   (b) in the past quarter period, oscillator i fired and received at least $\lfloor (P_i - 1)/5.5 \rfloor - 1$ pulses, or oscillator i did not fire but received at least $\lfloor (P_i - 1)/5.5 \rfloor$ pulses within this past quarter period, where $\lfloor \bullet \rfloor$ means the largest integer no greater than "$\bullet$."

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

Next, we show that Mechanism 3.2 can guarantee synchronization even when the total number of oscillators, i.e., N, is unknown to individual oscillators. Under the assumption that the portion of compromised oscillators is no larger than 10%, we first give a condition for local synchronization, i.e., synchronization when the initial phases of legitimate oscillators are constrained in a certain range, then we prove that when the coupling strength is over 0.75, the network can synchronize from an arbitrary initial phase distribution.

Theorem 3.7. *For an all-to-all PCO network of N oscillators where no more than* 10% *of all oscillators are compromised and act as stealthy Byzantine attackers, if the initial length of the containing arc of all legitimate oscillators is less than* $\pi/2$ *rad, even with N completely unknown to individual oscillators, all legitimate oscillators can be perfectly synchronized under Mechanism* 3.2.

Proof. Under Mechanism 3.2, no pulse will trigger a jump on any legitimate oscillator's phase within the first oscillation period $[0,T]$. So every legitimate oscillator will evolve freely for a full cycle, i.e., every legitimate oscillator will fire once within the first oscillation period. In the meantime, according to the stealthy Byzantine attack model in Section 3.4, every stealthy Byzantine attacker can emit at most two pulses within the first oscillation period $[0,T]$. Further more, under all-to-all connection, the number of pulses each legitimate oscillator receives within the first oscillation period, i.e., P_i, is identical.

The proof follows the same line of reasoning as Theorem 3.4. More specifically, using a same argument as Part I of the proof of Theorem 3.4, we can obtain that if the number of attackers in the network is no larger than the $\lfloor (P_i-1)/5.5 \rfloor$ in step 4). *b*) in Mechanism 3.2, then a pulse from neither a legitimate oscillator nor a stealthy Byzantine attacker could expand the containing arc of legitimate oscillators, i.e., the length of the containing arc is non-increasing. Moreover, following the same argument in Part II of the proof of Theorem 3.4, we know that if $\lfloor (P_i-1)/5.5 \rfloor \leq \lfloor (N-1)/5 \rfloor = \lambda$ holds, then at least the firing of one legitimate oscillator will reduce the length of the containing arc of legitimate oscillators and no legitimate oscillator will stop from firing until synchronization is achieved. Therefore, to prove that synchronization of legitimate oscillators will be achieved, it suffices to show $\lfloor 0.1N \rfloor \leq \lfloor (P_i-1)/5.5 \rfloor \leq \lfloor (N-1)/5 \rfloor$ is true, where $\lfloor 0.1N \rfloor$ is the maximal number of attackers in the network and $\lfloor \bullet \rfloor$ denotes the largest integer no greater than "$\bullet$."

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

$$N-1-\lfloor 0.1N \rfloor \leq P_i \leq N-1+\lfloor 0.1N \rfloor \tag{3.15}$$

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

$$\begin{aligned}
&N-1-0.1N \leq P_i \leq N-1+0.1N \\
\Rightarrow &0.9N-2 \leq P_i-1 \leq N-1+0.1(N-1) \\
\Rightarrow &(0.9N-2)/5.5 \leq (P_i-1)/5.5 \leq (N-1)/5 \\
\Rightarrow &\lfloor (0.9N-2)/5.5 \rfloor \leq \lfloor (P_i-1)/5.5 \rfloor \leq \lfloor (N-1)/5 \rfloor
\end{aligned} \tag{3.16}$$

One can easily get $\lfloor 0.1N \rfloor \leq \lfloor (0.9N-2)/5.5 \rfloor$ for $N \geq 3$. (Note that under the attacker less than 10% assumption, the network will contain no attackers when $N < 3$ and hence every oscillator can use P_i to

precisely estimate the number of oscillators in the network and achieve synchronization according to Theorem 3.1.) Substituting the above inequality into (3.16) lead to

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

for $N \geq 3$. Therefore, we can get that all legitimate oscillators can be perfectly synchronized under Mechanism 3.2. □

Next, we show that the initial phase distribution requirement in Theorem 3.7 can be removed, i.e., Mechanism 3.2 can guarantee synchronization in the presence of stealthy Byzantine attacks even when all legitimate oscillators' initial phases are arbitrarily distributed in $[0, 2\pi]$.

Theorem 3.8. *For an all-to-all PCO network of N oscillators where no more than* 10% *of all oscillators are compromised and act as stealthy Byzantine attackers, even with N completely unknown to individual oscillators, all legitimate oscillators can be perfectly synchronized under Mechanism* 3.2 *from any initial phase distribution as long as the coupling strength satisfies* $l > 0.75$.

Proof. Proof of Theorem 3.8 can be obtained following Theorem 3.5 and Theorem 3.7 and is omitted. □

Remark 3.7. *It is worth noting that the maximally allowable number of attackers in a PCO network is* $\lfloor 0.1N \rfloor$ *when the network size N is unknown, which is less than the maximally allowable number of composed oscillators* $\lambda = \lfloor (N-1)/5 \rfloor$ *when the network size N is known. This reduction of maximally allowable compromised oscillators is consistent with our intuition that less knowledge of a PCO network reduces the capability of attack-resilient synchronization design.*

Next, similar to Theorem 3.6, we present the convergence speed of Mechanism 3.2 where N is unknown to individual oscillators:

Theorem 3.9. *Under the synchronization conditions in Theorem 3.8, the time to synchronization of all legitimate oscillators under Mechanism* 3.2 *is propositional to*

$$\frac{\lfloor (P_i - 1)/5.5 \rfloor}{l(N - \lfloor 0.1N \rfloor)} \tag{3.17}$$

Proof. Proof of Theorem 3.9 can be obtained following the argument in Theorem 3.6 and is omitted. □

3.7 Simulations

3.7.1 Attack-Free Case

We first considered the situation without attackers. We simulated an all-to-all network of 11 PCOs under Mechanism 3.1. The initial time was set to $t_0 = 0$ and the phases of oscillators were randomly chosen from $[0, \pi)$. Hence, the initial length of the containing arc satisfied $\delta(t_0) < \pi$. According to Theorem 3.1, the network will synchronize. This was confirmed by numerical simulations in Fig. 3.5, which showed that the length of the containing arc converged to zero.

To verify Theorem 3.2, we randomly distributed the initial phases across the entire oscillation period $[0, 2\pi]$ and simulated the network under coupling strength $l = 0.51$. The evolution of the containing arc was presented in Fig. 3.6, which confirmed that Mechanism 3.1 can achieve synchronization even when the initial phases are randomly distributed in the entire phase space $[0, 2\pi]$.

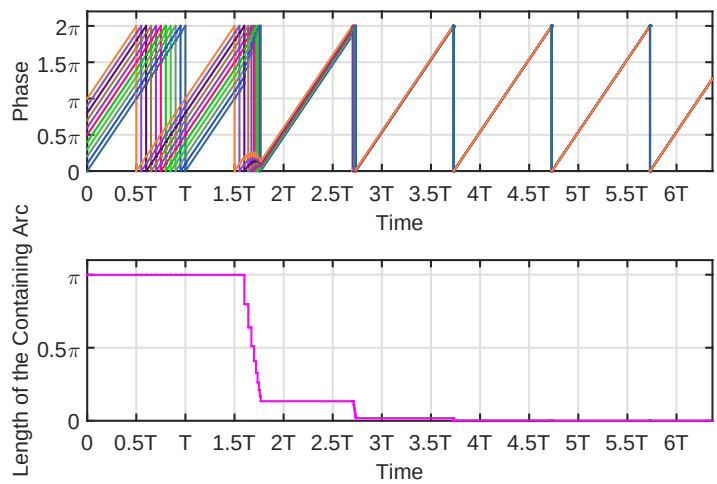

Figure 3.5: Phase evolution and the length of the containing arc of 11 PCOs under Mechanism 3.1 in the absence of attacks. The initial phases of all oscillators were randomly chosen from $[0, \pi)$. The coupling strength was set to $l = 0.2$.

3.7.2 In the Presence of Stealthy Byzantine Attacks

Using the same network, we ran simulations in the presence of stealthy Byzantine attacks. We assumed that 2 of the 11 oscillators were compromised and acted as stealthy Byzantine attackers. The initial time was set to $t_0 = 0$ and the initial phases of the 9 legitimate oscillators were randomly distributed in

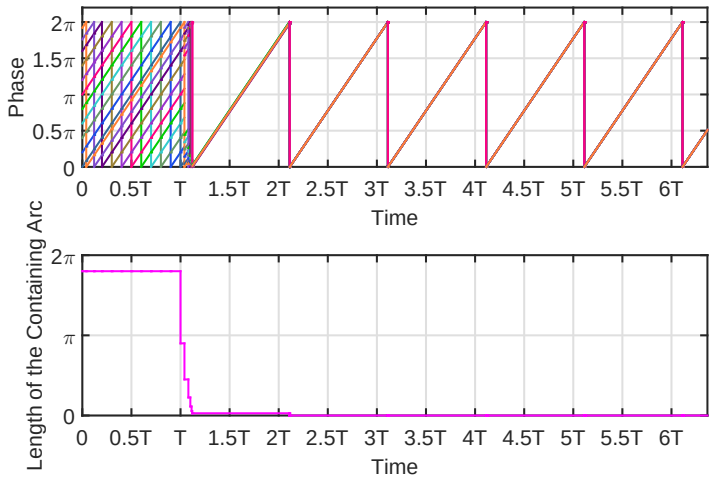

Figure 3.6: Phase evolution and the length of the containing arc of 11 PCOs under Mechanism 3.1 in the absence of attacks. The initial phases of all oscillators were randomly chosen from $[0, 2\pi]$. The coupling strength was set to $l = 0.51$.

$[0, \pi/2)$. Hence, the initial length of the containing arc was less than $\pi/2$ *rad*.

The phase evolution of the 9 legitimate oscillators under Mechanism 3.1 is given in Fig. 3.7 (b) and Fig. 3.8 (b), with the firing time instants of attackers denoted by asterisks on the x-axis. The results confirmed that Mechanism 3.1 is resilient to stealthy attacks. However, conventional pulse-base synchronization approaches in [2] and [3] failed to achieve synchronization, as illustrated in Fig. 3.7 (a) and Fig. 3.8 (a), respectively, which confirmed the advantages of the new mechanism.

Theorem 3.5 indicates that Mechanism 3.1 can achieve synchronization in the presence of stealthy Byzantine attacks even when the initial phase distribution is not restricted, i.e., the phases are randomly distributed in $[0, 2\pi]$. To verify Theorem 3.5, we set $l = 0.76$ and simulated the network. Results in Fig. 3.9 (b) and Fig. 3.10 (b) confirmed Theorem 3.5. Phase evolution under the same condition was also simulated under the conventional pulse-based synchronization approaches in [2] and [3], respectively. The results in Fig. 3.9 (a) and Fig. 3.10 (a) showed that neither of the conventional approaches can achieve synchronization, which further confirmed the advantages of Mechanism 3.1.

We also ran simulations when the network size was unknown to individual oscillators. For an all-to-all network of 20 oscillators, we assumed that two were compromised and acted as stealthy Byzantine attackers. The initial time was set to $t_0 = 0$ and the initial phases of the legitimates oscillators were randomly distributed in $[0, \pi/2)$. Hence, the initial length of the containing arc is less than $\pi/2$. According to Theorem 3.7, all legitimate oscillators will synchronize. This was confirmed by numerical simulations in Fig. 3.11

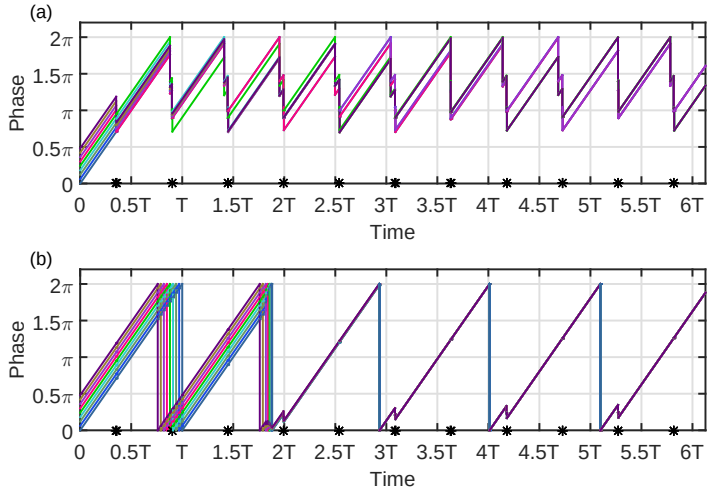

Figure 3.7: Phase evolutions of an all-to-all network of 11 PCOs, two of which are compromised with firing time instants represented by asterisks. Plot (a) and (b) present the phase evolutions of the 9 legitimate oscillators under the conventional pulse-based synchronization mechanism in [2] and Mechanism 3.1, respectively. The coupling strength was set to $l = 0.3$.

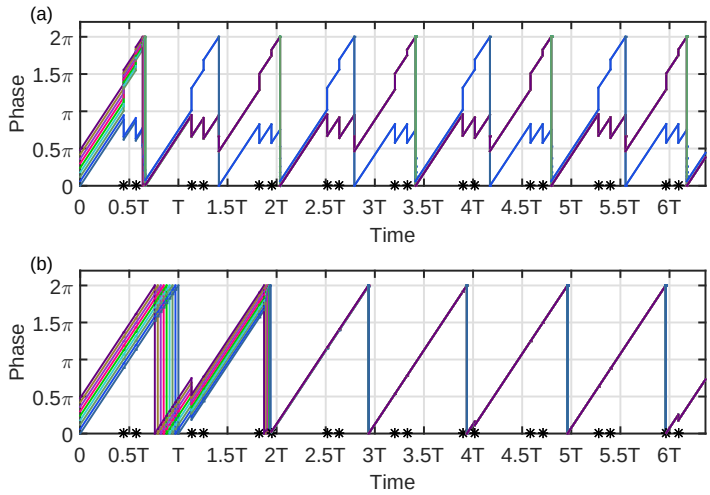

Figure 3.8: Phase evolutions of an all-to-all network of 11 PCOs, two of which are compromised with firing time instants represented by asterisks. Plot (a) and (b) present the phase evolutions of the 9 legitimate oscillators under the conventional pulse-based synchronization mechanism in [3] and Mechanism 3.1, respectively. The coupling strength was set to $l = 0.3$.

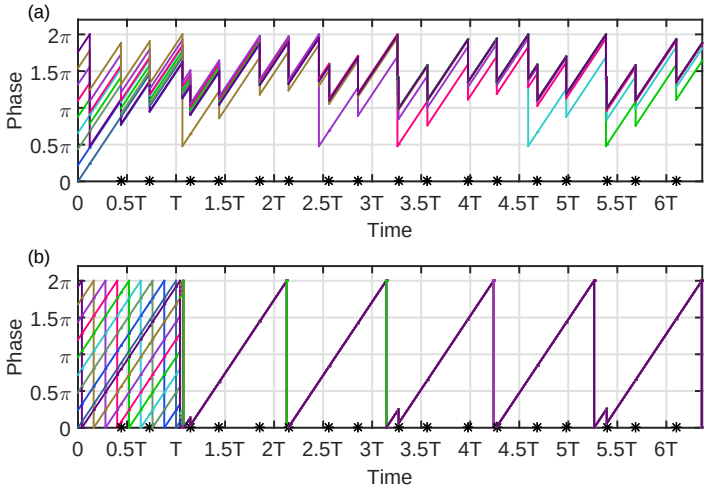

Figure 3.9: Phase evolutions of an all-to-all network of 11 PCOs, two of which are compromised with firing time instants represented by asterisks. Plot (a) and (b) present the phase evolutions of the 9 legitimate oscillators under the conventional pulse-based synchronization mechanism in [2] and Mechanism 3.1, respectively. The coupling strength was set to $l = 0.76$.

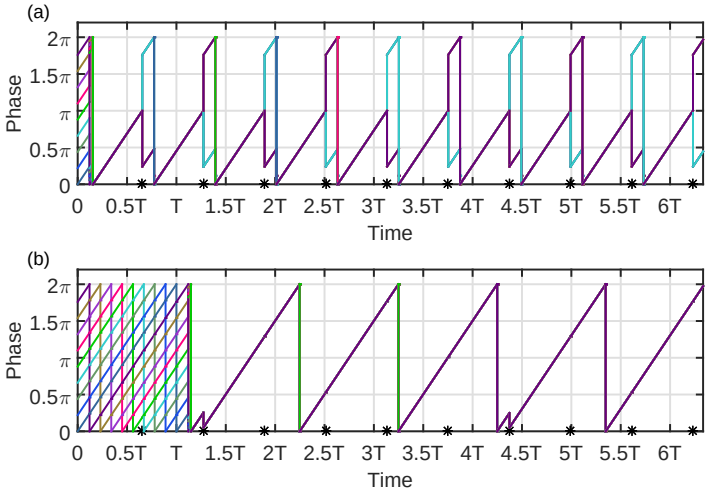

Figure 3.10: Phase evolutions of an all-to-all network of 11 PCOs, two of which are compromised with firing time instants represented by asterisks. Plot (a) and (b) present the phase evolutions of the 9 legitimate oscillators under the conventional pulse-based synchronization mechanism in [3] and Mechanism 3.1, respectively. The coupling strength was set to $l = 0.76$.

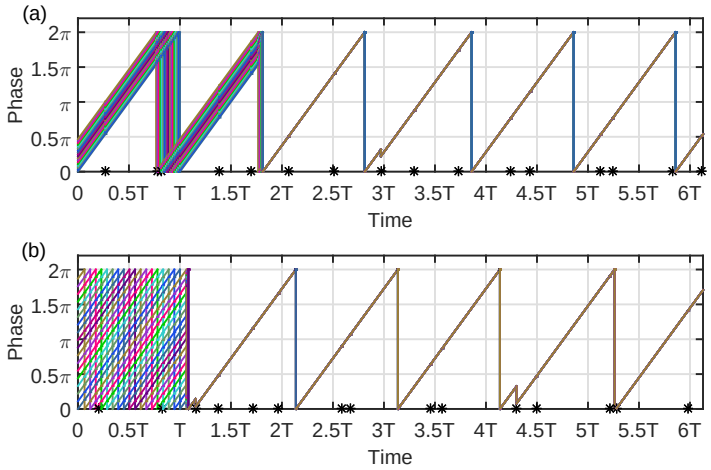

Figure 3.11: Phase evolutions of an all-to-all network of 20 PCOs, two of which are compromised with firing time instants represented by asterisks. The network size is unknown to individual oscillators. Plot (a) shows the phase evolutions of the 18 legitimate oscillators under Mechanism 3.2 with coupling strength $l = 0.3$ and the phases of all legitimate oscillators distributing randomly within $[0, \pi/2)$. Plot (b) shows the phase evolutions of the 18 legitimate oscillators under Mechanism 3.2 with coupling strength $l = 0.76$ and the phases of all legitimate oscillators distributing randomly within $[0, 2\pi]$.

(a), which showed that Mechanism 3.2 was resilient to stealthy Byzantine attacks even when the number of oscillators is unknown to individual oscillators.

Moreover, with the total number of oscillators N is unknown to individual oscillators, Theorem 3.8 indicates that Mechanism 3.2 can achieve synchronization in the presence of stealthy Byzantine attacks even when the phases of legitimate oscillators are randomly distributed in $[0, 2\pi]$. Results in Fig. 3.11 (b) confirmed Theorem 3.8.

We also numerically compared the attack-resilience and the convergence speed of Mechanism 3.1 if λ were allowed to be chosen from $1, 2, ..., \lfloor (N-1)/5 \rfloor$. We considered all-to-all PCO networks within which zero/one/two/three oscillator(s) were compromised and λ was set to 1, 2, and 3, respectively. The initial phases of legitimate oscillators were randomly chosen from $[0, 2\pi]$ and the coupling strength was set to $l = 0.76$. Synchronization was defined to be achieved when the length of the containing arc became and remained less than 1×10^{-6}. The mean synchronization probabilities and times to synchronization of $10,000$ runs under random attackers were shown in Fig. 3.12 and Fig. 3.13 (when 100% synchronization is not achieved, only synchronized runs were considered in the time-to-synchronization statistics). It can be seen that when $M \leq \lambda$ holds, synchronization of legitimate oscillators can be guaranteed and a larger λ renders a longer synchronization time; when $M > \lambda$ holds, a larger λ leads to a higher synchronization probability

but a lower convergence speed. Similar simulation results were obtained for Mechanism 3.2 but omitted here due to space limits.

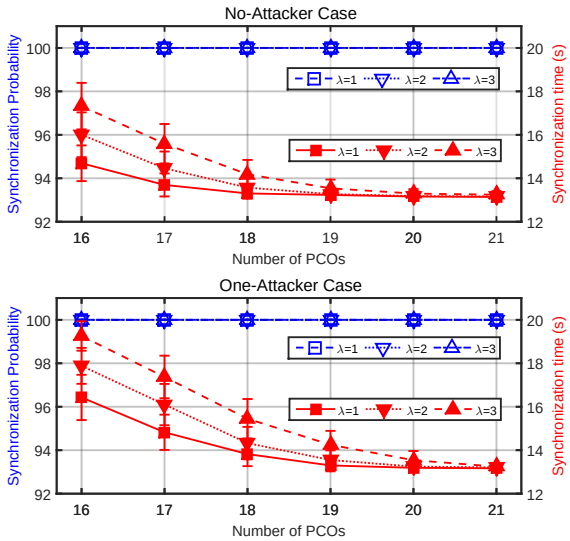

Figure 3.12: Comparison of synchronization probability and synchronization time under Mechanism 3.1 when λ was set to 1, 2, and 3 in the presence of 0 or 1 attacker. The initial phases of legitimate oscillators were randomly chosen from $[0, 2\pi]$ and the coupling strength was set to $l = 0.76$. Synchronization of the network was defined to be achieved when the length of the containing arc became and remained less than 1×10^{-6}.

We also numerically compared the performance of Mechanisms 3.1 and 3.2 with the mechanisms in [2] and [3] under random attacks, which was addressed in [2]. Random attackers inject pulses randomly in their own pace irrespective of legitimate oscillators' phases. Note that random attacks may not be stealthy. The initial phases of legitimate oscillators were randomly chosen from $[0, 2\pi]$ and the coupling strength was set to $l = 0.3$. The attacker(s) sent pulses with a random period uniformly distributed in $[T/4,\ 9T/4]$. Synchronization was defined to be achieved when the length of the containing arc became and remained less than 1×10^{-6}. In the presence of one attacker, the synchronization probabilities under Mechanism 3.1, Mechanism 3.2 and the approaches in [2] and [3] were given by the red curves in Fig. 3.14 and Fig. 3.15, respectively. It can be seen that Mechanisms 3.1 and 3.2 are more robust in enabling synchronization in the presence of random attacks. However, they render a longer synchronization time when compared with the conventional pulse-based synchronization mechanism in [3], as illustrated by the blue curves in Fig. 3.14 and Fig. 3.15. Similar conclusions were obtained for the two-attacker case, as illustrated in Fig. 3.16 and Fig. 3.17.

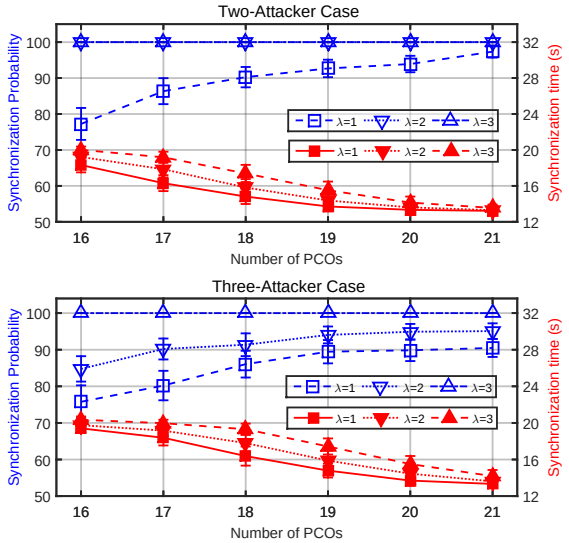

Figure 3.13: Comparison of synchronization probability and synchronization time under Mechanism 3.1 when λ was set to 1, 2, and 3 in the presence of 2 or 3 attackers. The initial phases of legitimate oscillators were randomly chosen from $[0, 2\pi]$ and the coupling strength was set to $l = 0.76$. Synchronization of the network was defined to be achieved when the length of the containing arc became and remained less than 1×10^{-6}.

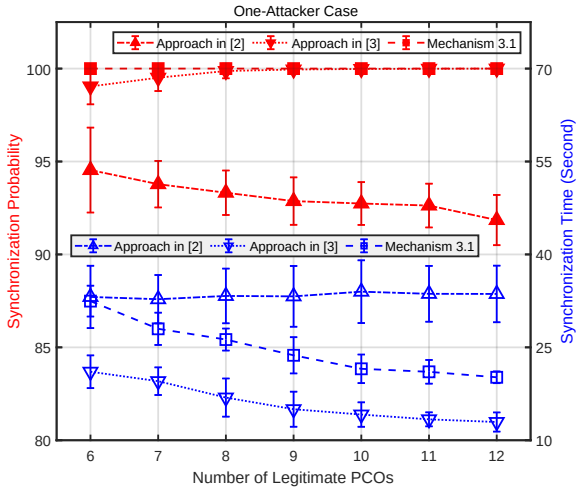

Figure 3.14: Comparison of Mechanism 3.1 and the conventional pulse-based synchronization mechanisms in [2] and [3] in terms of synchronization probability (red solid marker lines) and synchronization time (blue hollow marker lines) in the presence of one attacker.

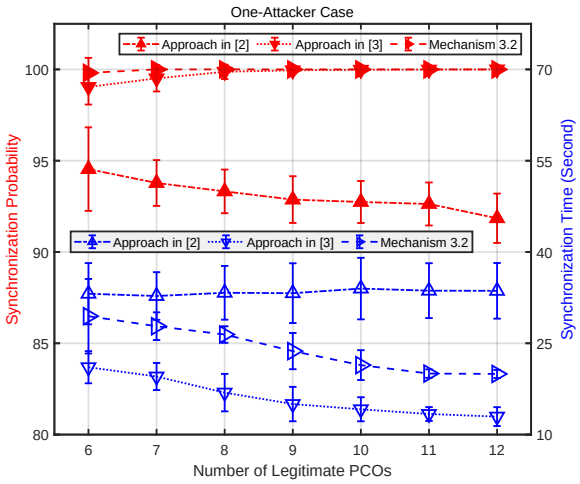

Figure 3.15: Comparison of Mechanism 3.2 and the conventional pulse-based synchronization mechanisms in [2] and [3] in terms of synchronization probability (red solid marker lines) and synchronization time (blue hollow marker lines) in the presence of one attacker.

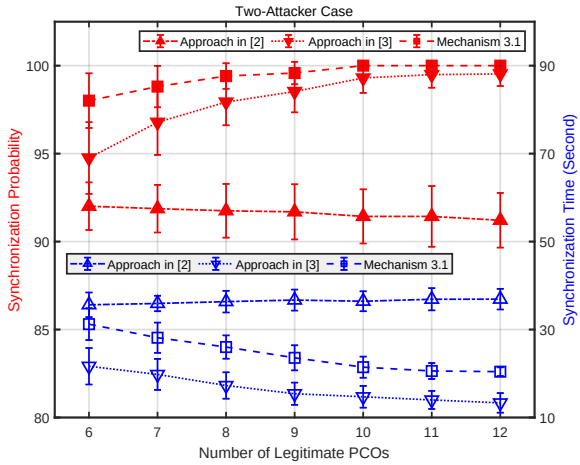

Figure 3.16: Comparison of Mechanism 3.1 and the conventional pulse-based synchronization mechanisms in [2] and [3] in terms of synchronization probability (red solid marker lines) and synchronization time (blue hollow marker lines) in the presence of two attackers.

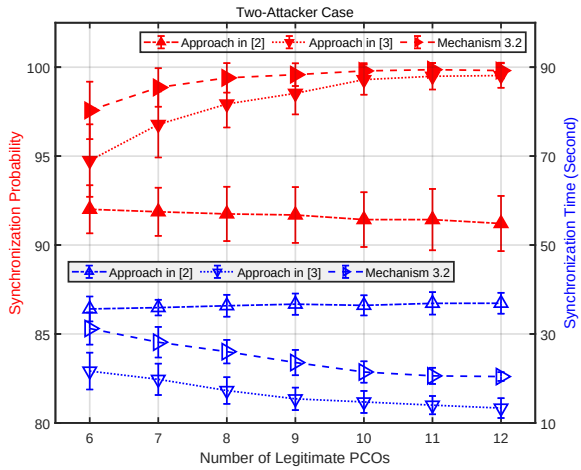

Figure 3.17: Comparison of Mechanism 3.2 and the conventional pulse-based synchronization mechanisms in [2] and [3] in terms of synchronization probability (red solid marker lines) and synchronization time (blue hollow marker lines) in the presence of two attackers.

3.7.3 General Interaction Topologies

The new pulse-based interaction approach (Mechanisms 3.1 and 3.2) also shows promising resilience to random attacks even under non-all-to-all interaction topologies. One can easily get that perfect synchronization of legitimate oscillators in a general strongly-connected PCO network cannot be achieved when some legitimate oscillators are affected by attackers whereas others are not. This is because malicious pulses can exert nonzero phase shifts on affected legitimate oscillators and make them deviate from the non-affected legitimate ones. So similar to [2], we numerically studied the synchronization error of strongly-connected PCO networks under random attacks. The synchronization error was quantified as follows:

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

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

We compared the synchronization errors of the proposed Mechanisms 3.1 and 3.2 with the mechanisms in [2] and [3] under a network of 20 oscillators distributed on a $50m \times 40m$ rectangle. All the oscillators are fixed in the rectangle with position represented by the blue dots in Fig. 3.18. Two oscillators in the network can communicate with each other if and only if their distance is less than 30 meters. The initial phases of all oscillators were randomly chosen from $[0, 2\pi]$ and the coupling strength was set to $l = 0.5$.

Fig. 3.19 shows the synchronization errors of our approaches (Mechanisms 3.1 and Mechanism 3.2)

and existing synchronization approaches in [2] and [3]. In Fig. 3.19, each data point was obtained under $10,000$ runs. In each run, all approaches used the same initial phase distribution (randomly chosen from $[0, 2\pi]$) and are subject to identical malicious pulse patterns (time interval between two consecutive malicious pulses randomly chosen from $[T/4, 9T/4]$). The vertical error bars denote standard deviations. It can be seen that in the presence of one attacker, our approach (Mechanisms 3.1&3.2) provides not only less average synchronization error but also less standard deviations. Fig. 3.20 shows the results in the presence of two attackers, which also confirmed that the proposed approach (Mechanisms 3.1&3.2) led to reduced average synchronization errors and standard deviations compared with existing results in [2] and [3]. It is worth noting that Mechanism 3.2 led to a slightly larger synchronization error than Mechanism 3.1. This reduction of synchronization performance is consistent with our intuition that less knowledge (the network size N is unknown to individual oscillators in Mechanism 3.2) reduces the capacity of attack-resilient synchronization design.

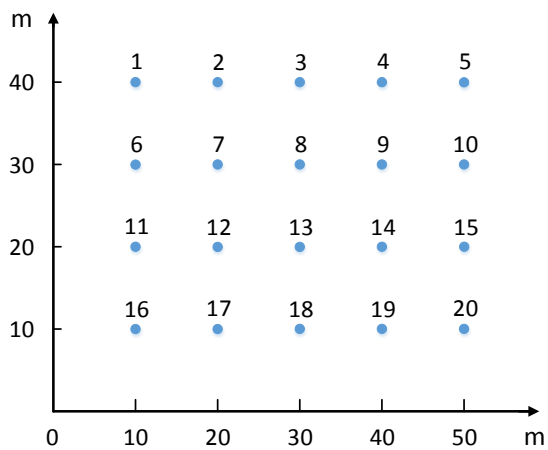

Figure 3.18: The positions of the 20 oscillators used in simulation.

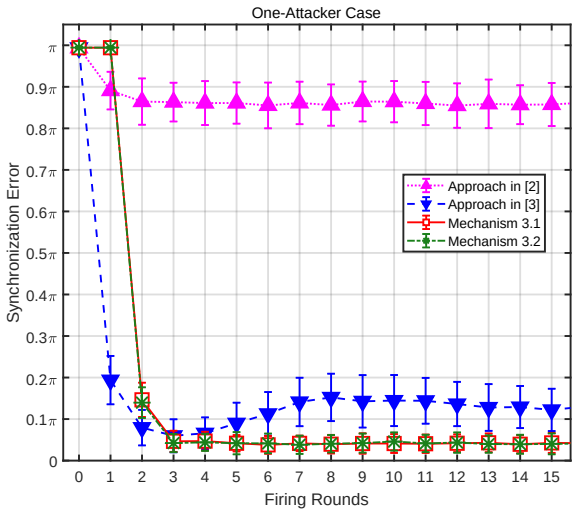

Figure 3.19: Comparison of Mechanisms 3.1 and 3.2 with the conventional pulse-based synchronization mechanisms in [2] and [3] in terms of synchronization error when oscillator 7 in Fig. 3.18 was compromised. The coupling strength was set to $l = 0.5$.

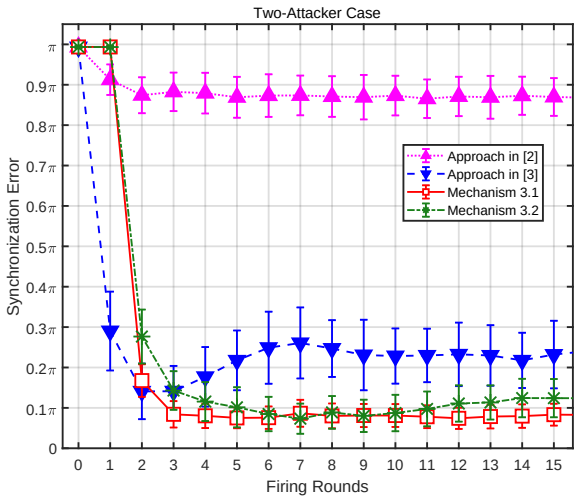

Figure 3.20: Comparison of Mechanisms 3.1 and 3.2 with the conventional pulse-based synchronization mechanisms in [2] and [3] in terms of synchronization error when oscillators 7 and 20 in Fig. 3.18 were compromised. The coupling strength was set to $l = 0.5$.

Chapter 4

An Attack-Resilient Pulse-Based Synchronization Strategy for General Connected PCO Networks under Stealthy Attacks

4.1 Introduction

In this chapter, 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 chapter, we use "general connected" to describe undirected 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 [2, 3, 64] which address faulty PCO nodes with random or periodic pulse emitting patterns, the situation considered in this chapter 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 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 Chapters 2 and 3 which can only guarantee phase synchronization under all-to-all topologies.

The main contributions of this chapter 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. 4.15 and Fig. 4.16), 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 Chapters 2 and 3; 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., Chapters 2 and 3) 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-based 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 Chapters 2 and 3. In Chapters 2 and 3, 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 chapter, 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 chapter is organized as follows. Section 4.2 introduces a new pulse-based synchronization mechanism. Under the new mechanism, Section 4.3 presents a synchronization condition for general connected PCOs in the absence of attacks. In Section 4.4, we characterize the condition for an attacker to keep stealthy, i.e., mounting attacks without being detected. In Section 4.5, we prove that synchronization of legitimate oscillators can be guaranteed in the presence of multiple stealthy Byzantine attackers, with and without collusion. In Section 4.6, we prove the applicability of our approach even when the total number of oscillators is unknown to individual oscillators. Simulation results are presented in Section 4.7.

4.2 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 $d \triangleq \min_{i=1,2,\cdots,N}\{d(i)\}$. The conventional pulse-based synchronization mechanism is presented below:

Conventional Pulse-Based Synchronization Mechanism [3]:

---

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:

$$\phi_i^+ = \phi_i + l \times F(\phi_i) \tag{4.1}$$

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

$$F(\phi) := \begin{cases} -\phi & 0 \leq \phi \leq \pi \\ 2\pi - \phi & \pi < \phi \leq 2\pi \end{cases} \tag{4.2}$$

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 Chapters 2 and 3 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 4.1):

---

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 (4.1) 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

   $$\lambda_i = \lfloor (d(i) - \lfloor N/2 \rfloor)/4 \rfloor \tag{4.3}$$

   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

   $$\bar{\lambda}_i = d(i) - 2\lambda_i \tag{4.4}$$

   Otherwise, the pulse has no effect on ϕ_i.

Fig. 4.1 illustrates the phase evolution of oscillator i having degree $d(i) = 9$ in a network of 11

PCOs. According to (4.3) and (4.4), 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. 4.1 as an example, only the 11th and the 12th pulses triggered phase jumps on oscillator i.

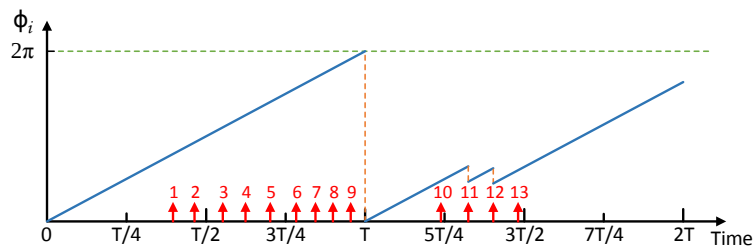

Figure 4.1: The phase evolution of oscillator i in a network of 11 PCOs under Mechanism 4.1. Indexed red arrows represent incoming pulses.

Remark 4.1. *Following [35, 36, 42], 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.*

4.3 Synchronization of General Connected PCOs in the Absence of Attacks

In this section, we will show that Mechanism 4.1 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 4.1 (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 4.2. *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 [2, 3], Chapter* 2*, and Chapter* 3*, the collective firing period could be affected by attack pulses.*

We next give two important properties of general connected PCO networks under Mechanism 4.1.

Lemma 4.1. *For a general connected network of N legitimate PCOs evolving under Mechanism* 4.1*, 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 3.1, 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 $\phi_i(t_i) = 2\pi$ rad 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. 4.2:

1) all the other $N-1$ oscillators' phases reside in $(\pi, 2\pi]$;

2) all the other $N-1$ oscillators' phases reside in $[0, \pi)$;

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

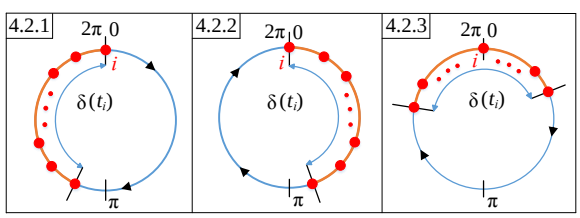

Figure 4.2: Three scenarios of phase distributions of oscillators when oscillator i fires at time instant t_i.

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.

1) 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

$$\delta(t_i) = 2\pi - \min_{j\in\mathscr{N}, j\neq i}\{\phi_j(t_i)\} \tag{4.5}$$

where $\mathscr{N} = \{1, 2, \cdots, N\}$ is the index set of all oscillators. After the firing of oscillator i, we have $\phi_i^+(t_i) = 0$. Since the PRF in (4.2) 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 $j \in \mathscr{N}, j \neq i$. In both cases we have $\phi_j(t_i) \leq \phi_j^+(t_i)$ for $j \in \mathscr{N}, j \neq i$, which implies

$$\min_{j\in\mathscr{N}, j\neq i}\{\phi_j(t_i)\} \leq \min_{j\in\mathscr{N}, j\neq i}\{\phi_j^+(t_i)\} \tag{4.6}$$

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

$$\delta^+(t_i) = 2\pi - \min_{j\in\mathscr{N}, j\neq i}\{\phi_j^+(t_i)\} + \phi_i^+(t_i) = 2\pi - \min_{j\in\mathscr{N}, j\neq i}\{\phi_j^+(t_i)\} \tag{4.7}$$

One can easily get $\delta^+(t_i) \leq \delta(t_i)$ by combining (4.5), (4.6) and (4.7).

2) When all the other $N-1$ oscillators' phases reside in $[0, \pi)$ at time instant t_i (note that phases 0 and 2π rad are the same point on the unit circle), noting that under Mechanism 4.1, 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 1).

3) 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 1) and Scenario 2).

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

□

Based on Lemma 4.1, next we show that every oscillator will fire at least once within any time interval of length $3T/2$ under Mechanism 4.1.

Lemma 4.2. *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* 4.1.

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. 4.3:

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 rad;

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 rad.

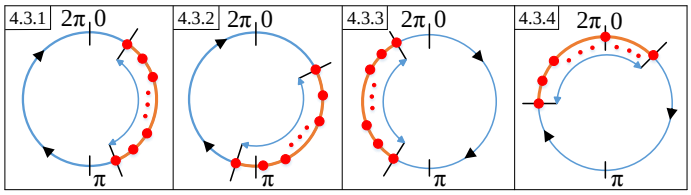

Figure 4.3: Four possible scenarios of phase distribution at time instant t.

Since all oscillators are legitimate, according to Mechanism 4.1, 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 (4.2) is non-negative on $(\pi, 2\pi]$, the pulse can only advance or have no 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 4.1. *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* 4.1.

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 4.1, we have that the containing arc is non-increasing and $0 \leq \delta(t) < \pi$ for $t \geq 0$. From Lemma 4.2, 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.

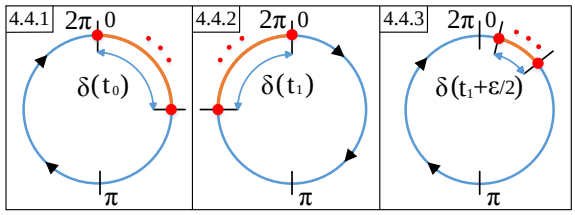

Figure 4.4: Phase distributions of all oscillators at different time instants in *Scenario 1.1*.

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. 4.4.1), 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. 4.4.2). 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 (4.2) 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., $2\pi - \varepsilon = \phi_1(t_1) \leq \phi_2(t_1) \leq \cdots \leq \phi_N(t_1) = 2\pi$ 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. 4.4.3.

Since the PRF in (4.2) 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 $0 \le \delta(t_1+\varepsilon/2) \le \varepsilon/2 = \delta(t_1)/2$. Given $l \in (0, 1]$, one can obtain $\delta(t_1+\varepsilon/2) \le (1-l/2)\delta(t_1)$. According to the non-increasing property of the containing arc in Lemma 4.1, we have $\delta(t_1+\varepsilon) \le (1-l/2)\delta(t_1)$.

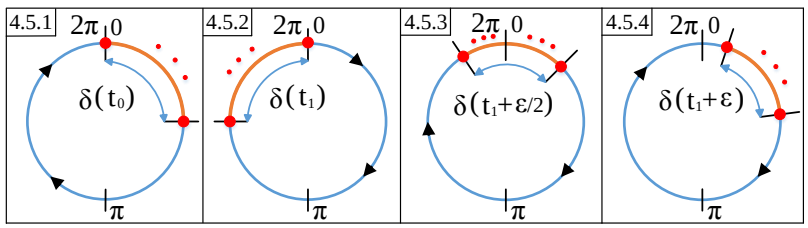

Figure 4.5: Phase distributions of all oscillators at different time instants in *Scenario 1.2* and *Scenario 1.3*.

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. 4.5.3. The length of the containing arc at $t_1+\varepsilon/2$ can be obtained as

$$\delta(t_1+\varepsilon/2) = \max_{i\in\mathcal{N}_f}\{\phi_i(t_1+\varepsilon/2)\} + 2\pi - \min_{j\in\mathcal{N}_n}\{\phi_j(t_1+\varepsilon/2)\} \tag{4.8}$$

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.,

$$\max_{i\in\mathcal{N}_f}\{\phi_i(t_1+\varepsilon/2)\} \le \varepsilon/2 \tag{4.9}$$

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 (4.2), we have the phase of oscillator j immediately after the jump at $\hat{t}_j$ as

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

Noting that the PRF in (4.2) 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

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

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 $j \in \mathscr{N}_n$, i.e.,

$$\min_{j\in\mathscr{N}_n}\{\phi_j(t_1+\varepsilon/2)\} \geq 2\pi-(1-l)\varepsilon/2 \tag{4.10}$$

Combining (4.8), (4.9), and (4.10), 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 4.1, 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. 4.5.3. To prove $\delta(t_1+\varepsilon) \leq (1-l/2)\delta(t_1)$, we first characterize the number of oscillators in $\mathscr{N}_f$ and $\mathscr{N}_n$.

We assume oscillator $j' \in \mathscr{N}_n$ 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 4.1, 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 4.1 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 $\mathscr{N}_n$ is at least $d(j')-\lambda_{j'}$. According to the definition of $\lambda_{j'}$ in (4.3), 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 $\mathscr{N}_n$ is at least $\lfloor N/2\rfloor+1$ and the number of oscillators in $\mathscr{N}_f$ 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 $\mathscr{N}_n$ fired within $(t_1+\varepsilon/2, t_1+\varepsilon]$, following the same line of reasoning as in *Scenario 1.1*, we have

$$\phi_j(t_1+\varepsilon) \in [0, \varepsilon/2] \tag{4.11}$$

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 (4.3), 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 4.1 is satisfied. Next we proceed to prove that at $\tilde{t}_i$, condition c) in Mechanism 4.1 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 (4.4), implying that at $\tilde{t}_i$, condition c) of Mechanism 4.1 is also satisfied. Therefore, according to Mechanism 4.1, 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 (4.2), the phase of oscillator i immediately after the jump at $\hat{t}_i$ can be obtained as

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

Noting that the PRF in (4.2) 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

$$\phi_i(t_1+\varepsilon) \leq \phi_i^+(\hat{t}_i) + (t_1+\varepsilon) - \hat{t}_i \leq (1-l)\phi_j(t_1+\varepsilon/2) + \varepsilon/2 + (t_1+\varepsilon/2-\hat{t}_i)l \tag{4.12}$$

Substituting $\phi_i(t_1+\varepsilon/2) \in [0, \varepsilon/2]$ and $\hat{t}_i \in (t_1+\varepsilon/2, t_1+\varepsilon]$ into (4.12) 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 (4.11) 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 (4.2) 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., $2\pi-\varepsilon = \phi_1(t_1) \leq \phi_2(t_1) \leq \cdots \leq \phi_N(t_1) = 2\pi$ 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 4.1, 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 4.1 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 4.1 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 $\delta(t_1+\varepsilon) \leq (1-l/2)\delta(t_1)$.

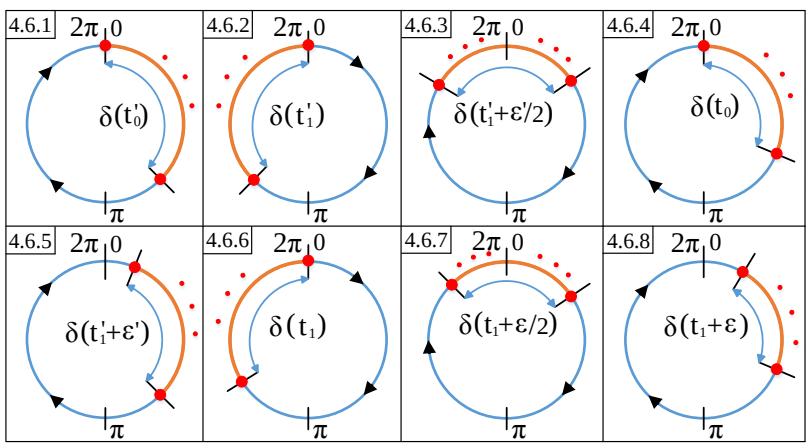

Figure 4.6: Phase distributions of all oscillators at different time instants in *Scenario 2.3.2*.

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 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. 4.6.1). As the containing arc is non-increasing (Lemma 4.1), 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. 4.6.2). 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 (4.2) 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. 4.6.5. 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. 4.6.3 at time instant $t_1'+\varepsilon'/2$. We denote $\mathscr{N}_f'$ (respectively $\mathscr{N}_n'$) 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 4.1 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 (4.2) 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 (4.3) and (4.4), 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 $\mathscr{N}_n'$ is at least $\lfloor N/2 \rfloor+1$ and the number of oscillators in $\mathscr{N}_f'$ 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 $\mathscr{N}_f'$ and $\mathscr{N}_n'$, 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 4.2, 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 4.1. □

Corollary 4.1. *Under conditions in Theorem 4.1, Mechanism* 4.1 *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 4.1 and hence is omitted. □

Remark 4.3. *Besides enabling attack resilience, Mechanism* 4.1 *also has better robustness against time-varying delays. For example, numerical simulations in Fig. 4.15 and Fig. 4.16 show that Mechanism* 4.1 *has much smaller synchronization errors compared with synchronization mechanisms in [2, 3] and Chapter* 3 *when the communication is subject to random time-varying delays.*

4.4 Stealthy Byzantine Attacks and Attack Detection Mechanism

The concept of Byzantine attacks stems from the Byzantine generals problem [48]. 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 [47]. 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 [69]. 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 4.3. *For a general connected network of N legitimate PCOs, under Mechanism* 4.1*, 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 4.3 can be obtained following the same line of reasoning as in Theorem 3.3. □

Based on Lemma 4.3, 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.

4.5 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 4.1) 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 4.4. *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* 4.4*, if the initial length of the containing arc of legitimate oscillators is less than π and $d > \lfloor N/2 \rfloor$, then under Mechanism* 4.1*, 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 4.1, 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. 4.3:

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 $d \triangleq \min_{i=1,2,\cdots,N}\{d(i)\}$, 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 4.1, 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 4.2. *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 Section* 4.4*, 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* 4.1.

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 4.1, 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 4.4, 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 4.1, 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. 4.9. 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 4.4, 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 4.2, 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 4.4, 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 (4.2) 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 1.1*, *1.2*, and *1.3* of Theorem 4.1 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 (4.2) 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 convergence 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 4.1, 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 4.1 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 4.1 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 4.2. *Under conditions in Theorem 4.2, Mechanism* 4.1 *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 4.2, 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 4.1 can guarantee the $T=2\pi$ seconds oscillation period even in the presence of attacks. □

Next, we prove that Mechanism 4.1 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 4.5. *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* 4.4*, if the initial length of the containing arc is less than π rad and $d > \lfloor N/2 \rfloor$, then under Mechanism* 4.1*, 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 4.4, 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. 4.3.

According to the stealth Byzantine attack model in Section 4.4, 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 4.1 that attacks pulses alone are not enough to trigger a legitimate oscillator to jump in phase. Therefore, following an argument similar to Lemma 4.4, 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 4.3. *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 Section* 4.4*, 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* 4.1.

Proof. Similar to the proof in Theorem 4.2, 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 4.2, 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 4.1 and Lemma 4.5, 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 4.2 and is omitted. □

Remark 4.4. *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 (4.4) to decrease the length of the containing arc.

Corollary 4.3. *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 (4.4) in Mechanism* 4.1.

Proof. According the stealthy requirement in Section 4.4, $M \leq \lfloor (d - \lfloor N/2 \rfloor)/4 \rfloor$ 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 (4.4) cannot be made unsatisfied for all legitimate pulses. □

Remark 4.5. *Following Corollary 4.3 and the proof in Theorem 4.2, one can get that there always exist legitimate pulses satisfying condition (4.4), 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.

4.6 Extension to the Case where N is Unknown to Individual Oscillators

The implementation of the "cut-off" algorithm in Mechanism 4.1 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 4.2):

---

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 (4.1) only when all the following three conditions are satisfied:

   (a) an entire period $T = 2\pi$ seconds has elapsed since initiation.

   (b) 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 "$\bullet$."

   (c) 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 as Theorem 4.1, Theorem 4.2, and Theorem 4.3, we can prove that Mechanism 4.2 can synchronize legitimate oscillators both in the absence and presence of attackers.

Corollary 4.4. *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* 4.2.

Proof. Proof of Corollary 4.4 can be obtained following Theorem 4.1 and is omitted. □

Theorem 4.4. *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* 4.2 *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 4.2. More specifically, using the same arguments as Part I of Theorem 4.2, 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 4.2, 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 4.2, 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. □

Theorem 4.5. *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* 4.2 *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 4.3 and is omitted. □

Remark 4.6. *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* 4.1 *summarizes the conditions for Mechanism* 4.1 *and Mechanism* 4.2 *to achieve synchronization.*

4.7 Simulations

Consider a network of 30 PCOs distributed on a two-dimension plane as illustrated in Fig. 4.7. 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 $\delta(0) < \pi$.

Table 4.1: Synchronization conditions of Mechanism 4.1 and Mechanism 4.2 (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	$M \leq 2 \times \lfloor d/9 \rfloor \rfloor$	$M \leq \lfloor d/9 \rfloor \rfloor$

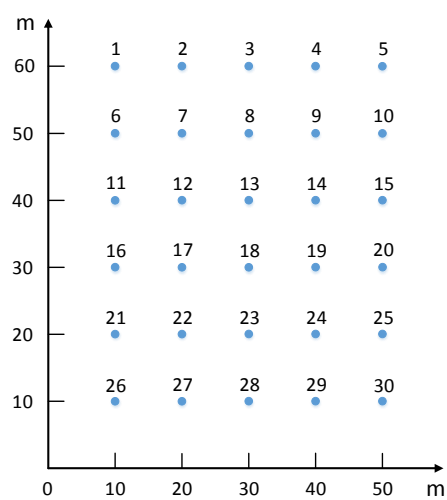

Figure 4.7: The deployment of the 30 oscillators used in simulations.

4.7.1 In the Absence of Attacks

We first considered the situation without attackers. As $d > \lfloor 2N/3 \rfloor = 20$, we know from Theorem 4.1 and Corollary 4.4 that the network will always synchronize, whether or not N is available to individual oscillators. This was confirmed in Fig. 4.8.

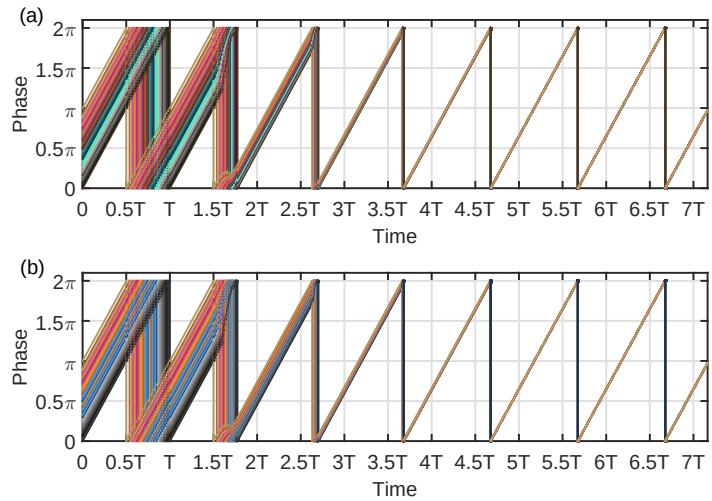

Figure 4.8: Plot (a) and (b) presented the phase evolutions of the 30 PCOs under Mechanism 4.1 and Mechanism 4.2, respectively. The coupling strength was set to $l = 0.1$.

4.7.2 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 Byzantine attackers. As $M = 2 \times \lfloor (d - \lfloor N/2 \rfloor)/4 \rfloor = 4$, we know from Theorem 4.2 that the network will synchronize. This was confirmed by numerical simulations in Fig. 4.9, 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.

When the 4 attackers colluded with each other, according to Theorem 4.3, the maximally allowable number of colluding attackers is $\lfloor (d - \lfloor N/2 \rfloor)/4 \rfloor = 2$. Hence, the condition in Theorem 4.3 was not satisfied. Simulation results confirmed that legitimate oscillators indeed could not synchronize, as illustrated in Fig. 4.10.

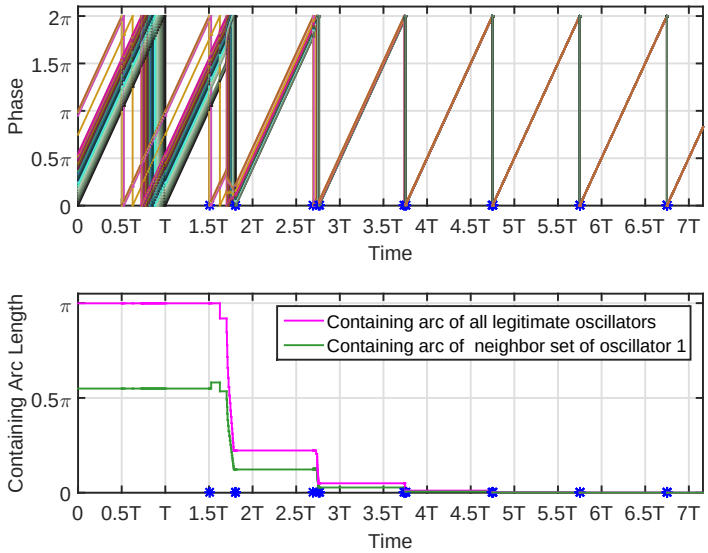

Figure 4.9: Phase evolution and the length of the containing arc of 26 legitimate oscillators under Mechanism 4.1 in the presence of 4 non-colluding stealthy Byzantine attackers (oscillators 1, 6, 26, 30) with attacking pulse time instants represented by asterisks. The coupling strength was set to $l = 0.1$.

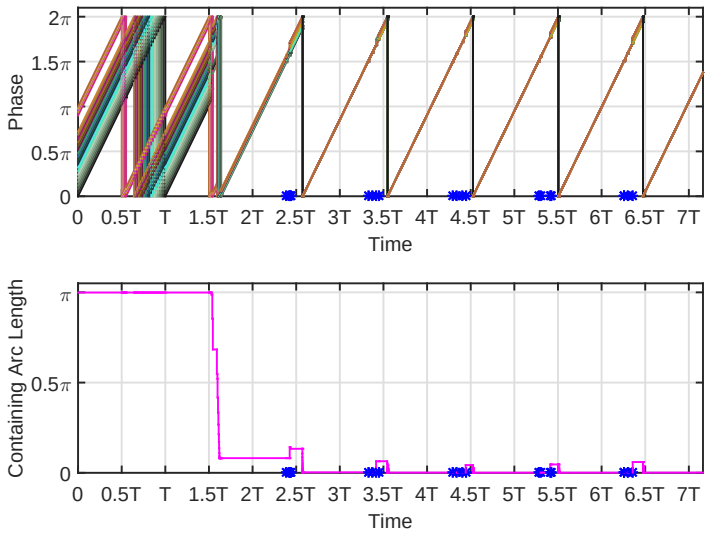

Figure 4.10: Phase evolution and the length of the containing arc of 26 legitimate oscillators under Mechanism 4.1 in the presence of 4 colluding stealthy Byzantine attackers (oscillators 1, 6, 26 and 30) with attacking pulse time instants represented by asterisks. The coupling strength was set to $l = 0.1$.

However, when we decreased the number of attackers to 2 (oscillators 1 and 6), all legitimate oscillators synchronized (cf. Fig. 4.11), confirming the results in Theorem 4.3. It is worth noting that the containing arc of attacker 1's legitimate neighbors were enlarged by attacker pulses, cf. Fig. 4.11.

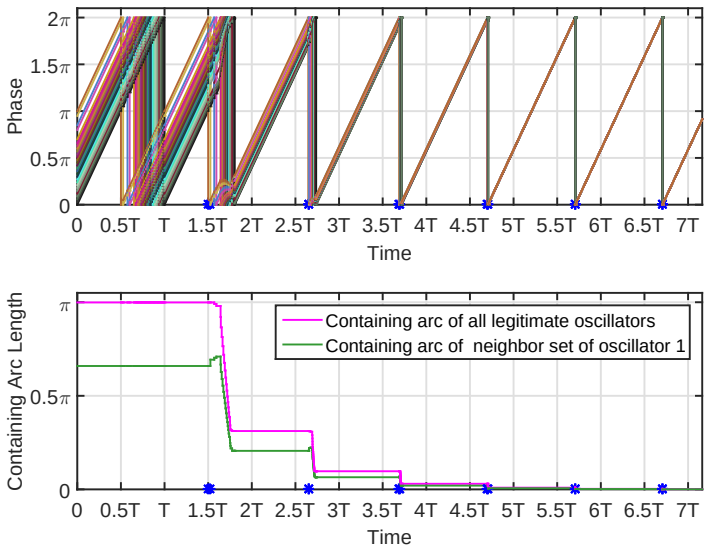

Figure 4.11: Phase evolution and the length of the containing arc of 28 legitimate oscillators under Mechanism 4.1 in the presence of 2 colluding stealthy Byzantine attackers (oscillators 1 and 6) with attacking pulse time instants represented by asterisks. The coupling strength was set to $l = 0.1$.

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 4.4, all legitimate oscillators can be synchronized under Mechanism 4.2. This was confirmed by numerical simulations in Fig. 4.12, 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 Theorem 4.5, the maximally allowable number of attackers is $\lfloor d/9 \rfloor = 2$. Hence, the condition in Theorem 4.5 is not satisfied. Simulation results confirmed that legitimate oscillators indeed could not synchronize, as illustrated in Fig. 4.13.

However, when we reduced the number of colluding attackers to 2 (oscillators 1 and 6), all legitimate oscillators achieved synchronization (cf. Fig. 4.14), which confirmed Theorem 4.5.

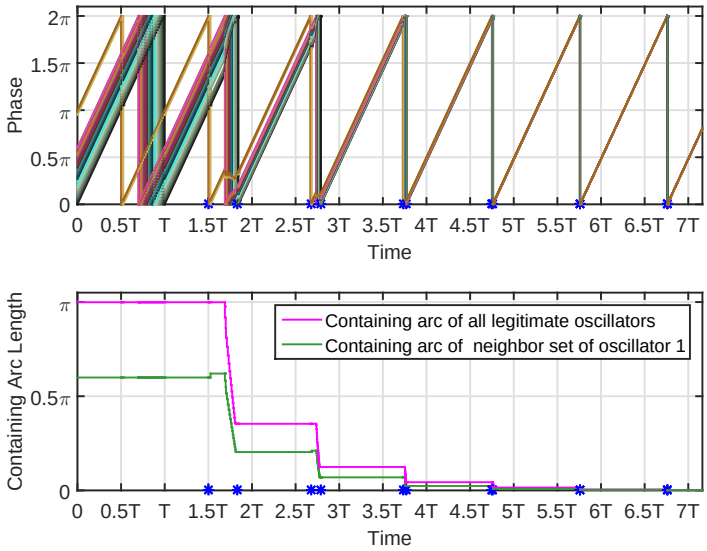

Figure 4.12: Phase evolution and the length of the containing arc of 26 legitimate oscillators under Mechanism 4.2 in the presence of 4 stealthy non-colluding Byzantine attackers (oscillators 1, 6, 18 and 26) with attacking pulse time instants represented by asterisks. The coupling strength was set to $l = 0.1$.

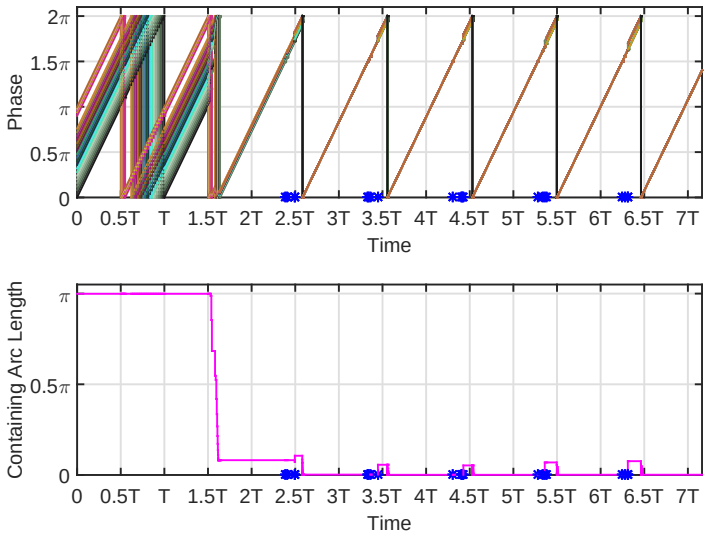

Figure 4.13: Phase evolution and the length of the containing arc of 26 legitimate oscillators under Mechanism 4.2 in the presence of 4 colluding stealthy Byzantine attackers (oscillators 1, 6, 18 and 26) with firing time instants represented by asterisks. The coupling strength was set to $l = 0.1$.

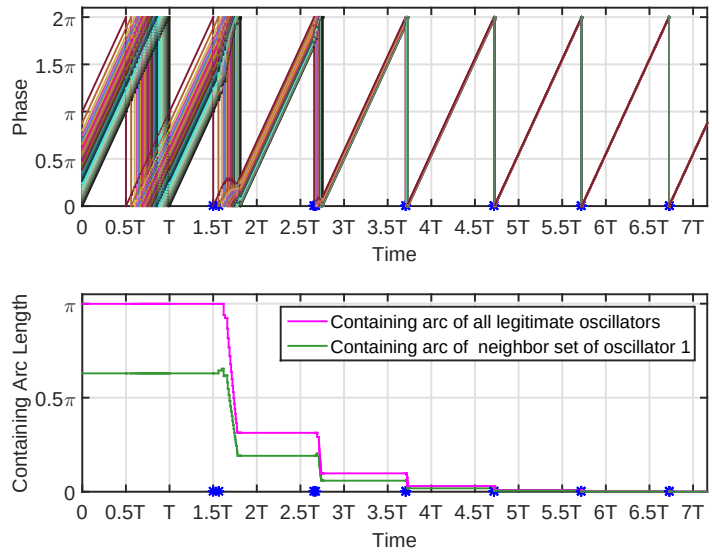

Figure 4.14: Phase evolution and the length of the containing arc of 28 legitimate oscillators under Mechanism 4.2 in the presence of 2 colluding stealthy Byzantine attackers (oscillators 1 and 6) with attacking pulse time instants represented by asterisks. The coupling strength was set to $l = 0.1$.

4.7.3 Comparison with Existing Results

In the absence of attacks, we compared Mechanism 4.1 with existing approaches in [2,3] and Chapter 3 under the PCO network in Fig. 4.7 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 [2], we evaluated the performance using synchronization errors defined as follows:

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

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

Fig. 4.15 and Fig. 4.16 show the synchronization errors of Mechanism 4.1 and approaches in [2,3] and Chapter 3 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 renders a smaller synchronization error. It is worth noting that Mechanism 4.2 also renders a smaller synchronization error than the approaches in [2,3] and Chapter 3 under the same set up. However, the results are omitted due to space limitations.

We also compared our proposed approach with existing approaches in [2,3] and Chapter 3 under

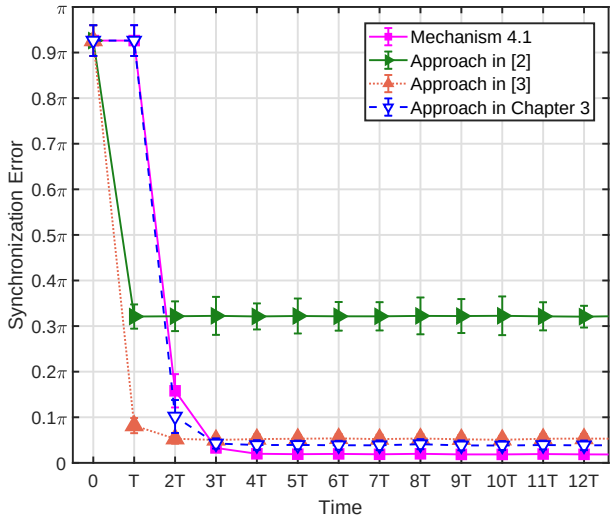

Figure 4.15: Comparison of our Mechanism 4.1 with the approaches in [2, 3] and Chapter 3 in terms of synchronization error in the presence of time-varying delays uniformly distributed in $[0, 0.1T]$. The coupling strength was set to $l = 0.3$.

the PCO network in Fig. 4.7 in the presence of non-colluding and colluding stealthy Byzantine attackers, respectively.

Fig. 4.17 shows the synchronization errors of Mechanism 4.1 and approaches in [2, 3] and Chapter 3 in the presence of 4 non-colluding stealthy Byzantine attackers (oscillators 1, 6, 26, 30) and Fig. 4.18 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 synchronization whereas all existing approaches are subject to substantial synchronization errors. It is worth noting that our Mechanism 4.2 also achieved perfect synchronization under the same set up. However, the results are omitted due to space limitations.

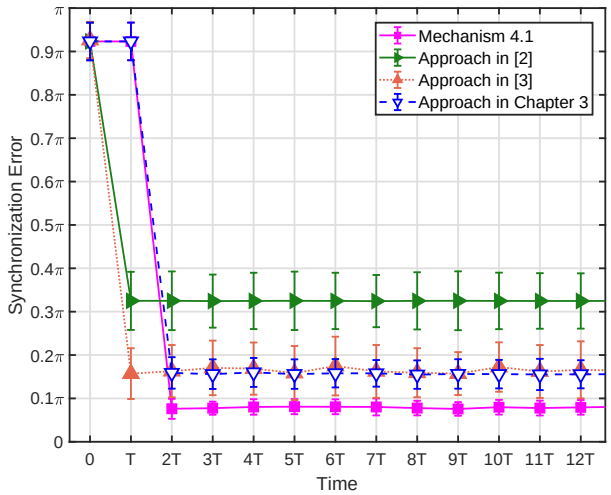

Figure 4.16: Comparison of our Mechanism 4.1 with the approaches in [2, 3] and Chapter 3 in terms of synchronization error in the presence of time-varying delays uniformly distributed in $[0, 0.1T]$. The coupling strength was set to $l = 0.6$.

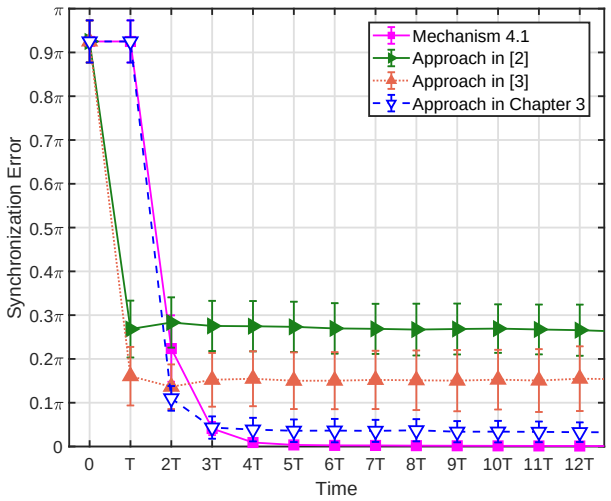

Figure 4.17: Comparison of our Mechanism 4.1 with the attack resilient approaches in [2, 3] and Chapter 3 in terms of synchronization error in the presence of 4 non-colluding stealthy Byzantine attackers (oscillators 1, 6, 26, 30). The coupling strength was set to $l = 0.3$.

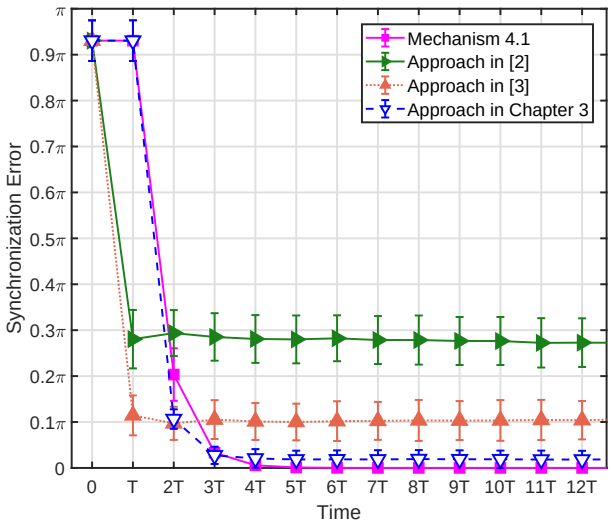

Figure 4.18: Comparison of our Mechanism 4.1 with the attack resilient approaches in [2,3] and Chapter 3 in terms of synchronization error in the presence of 2 colluding stealthy Byzantine attackers (oscillators 1 and 6). The coupling strength was set to $l = 0.3$.

Chapter 5

An Attack-Resilient Pulse-Based Synchronization Strategy for Densely Connected PCO Networks under Byzantine Attacks

5.1 Introduction

In this chapter, we propose an approach to synchronizing densely connected PCO networks from an arbitrary initial phase distribution under Byzantine (arbitrary) attacks. The approach only employs content-free pulses. It is worth noting that the content-free pulse-based communication reduces the attack surface and avoids the manipulation of message contents by Byzantine attacks. In fact, what can be manipulated by Byzantine attacks becomes the timing of attack pulses, which will be elaborated in Section 5.3.

Table 5.1 summarizes the advantage of our approach over existing results on pulse-based synchronization. More specifically, compared with existing results, our contributions are as follows: 1) Under Byzantine attacks, our proposed mechanism can synchronize legitimate oscillators even when their initial phases are arbitrarily distributed in the entire oscillation period; 2) Our mechanism is applicable to densely connected PCO networks that are not necessarily all-to-all; 3) We consider an attack model that is much more difficult

to deal with than existing results like [2, 3, 65–67]; 4) Our mechanism only use contend-free pulses, which is different from [53–59] relying on the assistance of packet communication to achieve synchronization; 5) Our proposed mechanism guarantees that the collective oscillation period is identical to the free-running period irrespective of attacks, which is superior to existing mechanisms (e.g., [3, 65, 66]) that lead to a collective oscillation period affected by attacker pulses.

Table 5.1: Comparison of attack-resilient pulse synchronization approaches.

Approaches \ Merits	Unrestricted phase distribution conditions	Not restricted to all-to-all networks	Attack model is Byzantine attacks	Communication uses content-free pulses only
[2, 3], Chapter 2	×	×	×	√
Chapter 3	√	×	×	√
Chapter 4	×	√	×	√
[54–57]	√	×	√	×
[58] [59]	√	√	√	×
[53]	√	√	×	×
Chapter 5	√	√	√	√

It is worth noting that the results in this chapter are fundamentally different from our recent result in Chapter 4 in the following aspects: 1) The attack model in this chapter is much stronger. Chapter 4 considers an attack model in which an attacker is restricted to send at most one attack pulse in any time interval of length $T/2$ (to stay stealthy) whereas this chapter allows attackers to send as many attack pulses as possible under a given communication channel with a fixed bit rate. So synchronization under attacks in this chapter is much more challenging; 2) This chapter has more relaxed requirement on the initial distribution of oscillator phases compared with Chapter 4. Chapter 4 requires legitimate oscillators to have initial phases contained in a half cycle whereas this chapter allows legitimate oscillators' phases to be arbitrarily distributed in the entire cycle; 3) This chapter proves finite-time synchronization whereas Chapter 4 only proves asymptotic synchronization even in the case of $l = 1$. More specifically, Chapter 4 proves that the length of the containing arc of legitimate oscillators will decrease to no greater than $(1 - l/2)$ of its original value after every two consecutive firing rounds, and hence can only yield synchronization when time goes to infinity. (It is worth noting that our prior result on non-all-to-all PCO networks in [65] needs $0 < l < 1$ to address the practical case of non-identical initial phases of legitimate oscillators and hence also only proves asymptotic synchronization.)

This Chapter is organized as follows: Section 5.2 reviews the main concepts of PCO networks. Section 5.3 presents the attack model considered in this chapter. Section 5.4 presents a new pulse-based synchronization mechanism. Section 5.5 addresses the case of multiple Byzantine attackers and Section 5.6 addresses the case where the total number of oscillators is unknown to individual oscillators. Simulation results are presented in Section 5.7.

5.2 Preliminaries

Consider a network of N pulse-coupled oscillators. Each oscillator is equipped with a phase variable which evolves clockwise on a unit circle. When the evolving phase of an oscillator reaches 2π rad, the oscillator fires (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. To define synchronization, we first introduce the concept of containing arc. The containing arc of legitimate oscillators is defined as the shortest arc on the unit circle that contains all legitimate oscillators' phases.

Definition 5.1 *(Phase Synchronization)*: We define phase synchronization as a state on which all legitimate oscillators have identical phases and fire simultaneously with a period of $T = 2\pi$ seconds.

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 $d \triangleq \min_{i=1,2,\cdots,N}\{d_i\}$. Since an oscillator cannot receive the pulse emitted by itself, the maximal degree of a network of N PCOs is $d = N-1$, meaning that the network is all-to-all connected. In this chapter, we consider dense networks where the network degree d is assumed to be greater than $\lfloor 2N/3 \rfloor$. Making use of the fact $d \triangleq \min_{i=1,2,\cdots,N}\{d_i\}$, we always have $d_i - \lfloor 2N/3 \rfloor - 1 \geq 0$ for $i = 1, 2, \cdots, N$.

5.3 Attacker Model

In this section, we present the model of Byzantine attacks. We assume that Byzantine attacks are able to compromise an oscillator and completely take over its behavior. Since the communicated messages in PCO networks are identical and content-free, i.e., pulses, a Byzantine attacker cannot manipulate the content

of pulses, but rather, it will judiciously craft attacks via injecting pulse trains at certain time instants to negatively affect pulse-based synchronization.

Because in realistic wireless sensor networks (WSNs), the bit rate of a communication channel between two connected oscillators is limited, an attacker cannot send infinitely many pulses in any finite time interval. In other words, there is always a nonzero time interval between two consecutive pulses from an attacker. Therefore, Byzantine attackers will launch attacks with a time separation greater than ε seconds, where ε is the minimum time separation between two consecutive pulses that can be conveyed by a channel. We summarize the Byzantine attacker model in this chapter as follows:

Byzantine Attacker: a Byzantine attacker will emit attack pulses with a time separation greater than ε seconds, where ε is the minimum time separation between two pulses that can be successfully conveyed by a communication channel.

Remark 5.1. *In PCO networks, the communication messages are all content-free pulses. So the transmission of one pulse will only occupy the communication channel for a very short time. Only after finishing transmitting one pulse, an attacker can initiate the transmission of another attack pulse. Hence, ε is determined by the length of the pulse and the bit rate of the communication channel. For example, the bit rate of the IEEE 802.15.4 channel is $250kbps$. If we use a control packet (21 bytes) to realize a pulse, then transmitting such pulses will need time separation $\varepsilon = (21 \times 8)/250000 = 0.672 \times 10^{-3}$ seconds [14, 70].*

Remark 5.2. *All existing attack patterns considered under pulse-based synchronization such as random attacks [2, 64], static attacks [3], and stealthy attacks in Chapters* 2-4 *are special cases of the attacker model considered in this chapter.*

5.4 A New Pulse-Based Synchronization Mechanism

Motivated by the fact that the conventional pulse-based synchronization mechanism is vulnerable to attacks, we propose a new pulse-based synchronization mechanism to combat attacks. To present our new mechanism, we first describe the conventional pulse-based synchronization mechanism.

Conventional Pulse-Based Synchronization Mechanism [3]:

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:

$$\phi_i^+ = \phi_i + l \times F(\phi_i) \tag{5.1}$$

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

$$F(\phi) := \begin{cases} -\phi & 0 \leq \phi \leq \pi \\ 2\pi - \phi & \pi < \phi \leq 2\pi \end{cases} \tag{5.2}$$

For $l = 1$, oscillator i will fire immediately if it has $\phi_i^+ = 2\pi$ rad.

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 hence destroy their synchronization. Moreover, we have that synchronization can never be maintained when attackers only affect part of the network, 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. This is also confirmed by numerical simulation results in Figure 5.8 and Figure 5.9, which illustrate that existing results in [3], Chapter 2, and Chapter 3 cannot achieve synchronization in the presence of Byzantine attacks when the topology is not all-to-all.

To overcome the inherent vulnerability of existing pulse-based synchronization approaches, we propose a new pulse-based synchronization mechanism (Mechanism 5.1) to improve the attack resilience of PCO networks. Our key idea to enable attack resilience is a "pulse response mechanism" which can restrict the number of pulses able to affect a receiving legitimate oscillator's phase in any oscillation period and a "phase resetting mechanism" which resets the phase value of a legitimate oscillator upon reaching phase 2π rad to different values depending on the number of received pulses. The "pulse response mechanism" and the "phase resetting mechanism" only allow 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 synchroniza-

tion process. Noting that all pulses are identical and content-free, Mechanism 5.1 is judiciously designed based on the number of pulses an oscillator received in the past, i.e., based on memory. The new pulse-based synchronization mechanism is detailed below:

New Pulse-Based Synchronization Mechanism (Mechanism 5.1):

---

1. The phase ϕ_i of legitimate oscillator i evolves from 0 to 2π rad with a constant speed $\omega = 1$ rad/second.

2. Once ϕ_i reaches 2π rad at time t, oscillator i fires (emits a pulse) if it did not fire within $(t-\varepsilon, t]$ and an entire period $T = 2\pi$ seconds has elapsed since initiation. Then oscillator i resets its phase from 2π rad to 0 if it received over $\lfloor N/3 \rfloor$ pulses within $(t-\varepsilon, t]$, where $\lfloor \bullet \rfloor$ is the largest integer no greater than "$\bullet$." Otherwise, it resets its phase from 2π rad to π rad.

3. When oscillator i receives a pulse at time t', it shifts its phase to 2π rad only if $\phi_i \in [\pi, 2\pi]$ at time instant t' and one of the following conditions is satisfied:

   (a) before receiving the current pulse, oscillator i has already received at least $d_i - \lfloor 2N/3 \rfloor - 1$ pulses in $[t' - T/2, t']$ and it did not reset its phase from 2π rad to 0 within $(t' - T, t')$.

   (b) before receiving the current pulse, oscillator i has already received at least $d_i - \lfloor 2N/3 \rfloor - 1$ pulses in $(t' - \varepsilon, t']$.

   Otherwise, the pulse has no effect on ϕ_i who will evolve freely towards 2π rad.

Remark 5.3. *Following [13, 35, 36, 42], we assume that when a legitimate oscillator receives multiple pulses simultaneously, it can determine the number of received pulses and processes them consecutively. In other words, no two pulses will be regarded as an aggregated pulse.*

5.5 Synchronization of PCO Networks in the Presence Attacks

In this section, we address the synchronization of PCO networks in the presence of Byzantine attacks. Among N PCOs, we assume that M are compromised and act as Byzantine attackers. We will show that Mechanism 5.1 synchronizes legitimate oscillators even in the presence of multiple Byzantine attackers. Specifically, we will prove that under Mechanism 5.1, legitimate oscillators achieve synchronization even when their topology is non-all-to-all and their initial phases are distributed arbitrarily in the entire oscillation period $[0, 2\pi]$. More interestingly, when synchronization is achieved, the collective oscillation period of all

legitimate oscillators is invariant under attacks and is identical to the free-running oscillation period $T = 2\pi$ seconds. To facilitate theoretical analysis, we first establish Lemma 5.1 about the properties of floor function $\lfloor \bullet \rfloor$.

Lemma 5.1. *For three arbitrary positive integers x, y, and Q, with $x > y$, the following inequalities always hold:*

$$\begin{cases} \lfloor y \cdot Q/x \rfloor \geq y \cdot \lfloor Q/x \rfloor \\ \\ \lfloor y \cdot Q/x \rfloor + \lfloor (x-y) \cdot Q/x \rfloor + 1 \geq Q \end{cases}$$

Proof. First, we prove $\lfloor y \cdot Q/x \rfloor \geq y \cdot \lfloor Q/x \rfloor$. Since x and Q are positive integers, dividing Q by x and letting q and r be the quotient and remainder, respectively, we have $Q = x \cdot q + r$ and $0 \leq r/x < 1$. By substituting them into $\lfloor y \cdot Q/x \rfloor - y \cdot \lfloor Q/x \rfloor$, we have:

$$\lfloor y \cdot Q/x \rfloor - y \cdot \lfloor Q/x \rfloor = \lfloor y \cdot q + y \cdot r/x \rfloor - y \cdot \lfloor q + r/x \rfloor = y \cdot q + \lfloor y \cdot r/x \rfloor - y \cdot q = \lfloor y \cdot r/x \rfloor \geq 0.$$

Hence, we obtain $\lfloor y \cdot Q/x \rfloor \geq y \cdot \lfloor Q/x \rfloor$.

Next, we proceed to prove $\lfloor y \cdot Q/x \rfloor + \lfloor (x-y) \cdot Q/x \rfloor + 1 \geq Q$. Dividing $y \cdot Q$ by x and letting $\bar{q}$ and $\bar{r}$ be the quotient and remainder, respectively, we have $y \cdot Q = \bar{q} \cdot x + \bar{r}$ and $0 \leq \bar{r}/x < 1$. Substituting them into $\lfloor y \cdot Q/x \rfloor + \lfloor (x-y) \cdot Q/x \rfloor + 1 - Q$ leads to

$$\begin{aligned} \lfloor y \cdot Q/x \rfloor + \lfloor (x-y) \cdot Q/x \rfloor + 1 - Q &= \lfloor \bar{q} + \bar{r}/x \rfloor + \lfloor Q - \bar{q} - \bar{r}/x \rfloor + 1 - Q \\ &\geq \lfloor \bar{q} \rfloor + \lfloor Q - \bar{q} - 1 \rfloor + 1 - Q = 0. \end{aligned}$$

Thus, we obtain $\lfloor y \cdot Q/x \rfloor + \lfloor (x-y) \cdot Q/x \rfloor + 1 \geq Q$. □

Now we are in position to prove that all legitimate oscillators will synchronize under Mechanism 5.1 in the presence of Byzantine attacks even when legitimate oscillators are under a non-all-to-all connection and the initial phases are arbitrarily distributed in the entire oscillation period $[0, 2\pi]$.

Theorem 5.1. *For a network of N PCOs among which M are compromised and launch attacks following the Byzantine attack model in Section* 5.3*, if the degree of the PCO network satisfies $d > \lfloor 2N/3 \rfloor$ and the number of attackers M satisfies $M < d - \lfloor 2N/3 \rfloor$, then all legitimate oscillators will synchronize under Mechanism* 5.1 *from any initial phase distribution.*

Proof. We set the initial time instant to t_0. The following proof is divided into two parts. In part I, we prove that all $N-M$ legitimate oscillators' phases reside in $[\pi, 2\pi]$ at t_0+T from any initial phase distribution. In Part II, we prove that these legitimate oscillators will reset their phases to 0 at the same time and will keep having identical phases with a collective oscillation period $T = 2\pi$ seconds, i.e., they will achieve synchronization.

Part I (all $N-M$ legitimate oscillators' phases reside in $[\pi, 2\pi]$ at t_0+T): Since the number of attackers satisfies $M < d - \lfloor 2N/3 \rfloor$ for $d \leq N-1$, using Lemma 5.1, we have

$$M < d - \lfloor 2N/3 \rfloor \leq N - 1 - \lfloor 2N/3 \rfloor \leq \lfloor N/3 \rfloor.$$

According to the attacker model in Section 5.3, we know that $M < \lfloor N/3 \rfloor$ attackers can emit at most $M < \lfloor N/3 \rfloor$ pulses within any time interval of length ε. Since no legitimate oscillator fires within time interval $[t_0, t_0+T]$ under Mechanism 5.1, a legitimate oscillator can receive at most $M < \lfloor N/3 \rfloor$ pulses in any time interval of length ε within $[t_0, t_0+T]$. Therefore, upon reaching 2π rad within $[t_0, t_0+T]$, a legitimate oscillator will reset its phase to π rad instead of 0.

Since the initial phases of all $N-M$ legitimate oscillators distribute arbitrarily in $[0, 2\pi]$, at time t_0, they can be categorized into three possible scenarios, as depicted in Figure 5.1:

Scenario a): all legitimate oscillators' initial phases reside in $[\pi, 2\pi]$;

Scenario b): all legitimate oscillators' initial phases reside in $[0, \pi)$;

Scenario c): legitimate oscillators' initial phases reside partially in $[0, \pi)$ and partially in $[\pi, 2\pi]$.

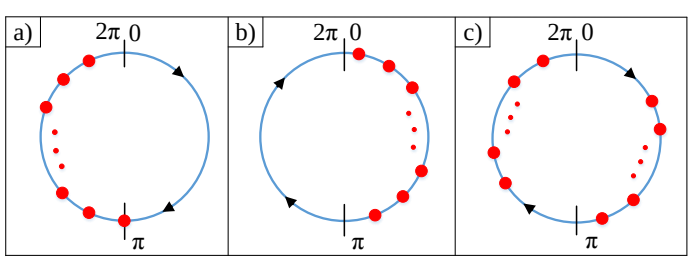

Figure 5.1: Three possible initial phase distributions of legitimate oscillators.

Next, we show that no matter which of the three scenarios the initial phase distribution belongs to, all legitimate oscillators' phases will reside in $[\pi, 2\pi]$ at time t_0+T. We discuss all three scenarios of initial phase distribution one by one:

Scenario a): All legitimate oscillators' initial phases reside in $[\pi, 2\pi]$. After reaching 2π rad within $[t_0, t_0+T]$, because a legitimate oscillator will receive less than $\lfloor N/3 \rfloor$ pulses in any time interval of length ε, it will reset its phase to π rad according to Mechanism 5.1. Therefore, we have that all legitimate oscillators will reside in $[\pi, 2\pi]$ at time t_0+T.

Scenario b): All legitimate oscillators' initial phases reside in $[0, \pi)$. According to Mechanism 5.1, a legitimate oscillator will not respond to incoming pulses when its phase resides in $[0, \pi)$. So all legitimate oscillators' phases will evolve freely towards π rad without perturbation and will enter $[\pi, 2\pi]$ no later than time instant $t_0+T/2$. After reaching 2π rad within $[t_0, t_0+T]$, because a legitimate oscillator will receive less than $\lfloor N/3 \rfloor$ pulses in any time interval of length ε, it will reset its phase to π rad according to Mechanism 5.1. Therefore, we have that all legitimate oscillators' phases will reside in $[\pi, 2\pi]$ at time t_0+T.

Scenario c): Legitimate oscillators' initial phases reside partially in $[0, \pi)$ and partially in $[\pi, 2\pi]$. Since legitimate oscillators with phases residing in $[0, \pi)$ will evolve freely into $[\pi, 2\pi]$ under Mechanism 5.1, we have that no later than time instant $t_0+T/2$, these oscillators' phase will be in $[\pi, 2\pi]$. Further making use of the fact that a legitimate oscillator will reset its phase to π rad upon reaching 2π rad since less than $\lfloor N/3 \rfloor$ pulses will be received by a single oscillator in any time interval of length ε, we obtain that all legitimate oscillators' phases will reside in $[\pi, 2\pi]$ at time t_0+T.

Summarizing the above three scenarios, we have that regardless of the initial phase distribution, all legitimate oscillators' phases will reside in $[\pi, 2\pi]$ at time t_0+T despite the presence of attacker pulses.

Part II (all legitimate oscillators will reset their phases to 0 *at the same time and will keep having identical phases with a collective oscillation period* $T = 2\pi$ *seconds)*: From Part I, we know that no legitimate oscillator fires or resets its phase to 0 within time interval $[t_0, t_0+T]$ and all legitimate oscillators' phases reside in $[\pi, 2\pi]$ at time t_0+T. Therefore, all legitimate oscillators' phases will reach 2π rad and fire at least once within $(t_0+T, t_0+3T/2]$. Without loss of generality, we label all $N-M$ legitimate oscillators according to the order of their first firing time[1] and denote $t_1 \in (t_0+T, t_0+3T/2]$ as the first firing time of legitimate oscillator $\lfloor N/3 \rfloor + 1$. Only the following two scenarios could happen right before legitimate oscillator $\lfloor N/3 \rfloor + 1$ fires at t_1:

Scenario 1.1: no legitimate oscillator has reset its phase to 0 before legitimate oscillator $\lfloor N/3 \rfloor + 1$ fires at t_1.

Scenario 1.2: at least one legitimate oscillator has reset its phase to 0 before legitimate oscillator $\lfloor N/3 \rfloor + 1$

[1] For example, if the firing sequence of legitimate oscillators A, B, C is A, A, B, A, C, then oscillators A, B, C are labeled as oscillators 1, 2, 3, respectively.

fires at t_1.

Next, we show that in both scenarios all legitimate oscillators will reset their phases to 0 at the same time and will keep having identical phases with a collective oscillation period $T = 2\pi$ seconds, i.e., they will achieve synchronization.

We first consider *Scenario 1.1*, i.e., no legitimate oscillator has reset its phase to 0 before legitimate oscillator $\lfloor N/3 \rfloor + 1$ fires at t_1. Since all the $N-M$ legitimate oscillators are labeled according to the order of their first firing time instants and no legitimate oscillator fired within $[t_0, t_0+T]$ according to Mechanism 5.1, we have that before the firing of legitimate oscillator $\lfloor N/3 \rfloor + 1$ at t_1, $\lfloor N/3 \rfloor$ legitimate oscillators fired within time interval $(t_0+T, t_1]$ and every legitimate oscillator i for $i = 1, 2, \cdots, N-M$ received at least $\lfloor N/3 \rfloor - (N-d_i)$ pulses within time interval $(t_0+T, t_1]$, where $(N-d_i)$ is the number of oscillators which are not connected with oscillator i. According to Lemma 5.1, we have:

$$\lfloor N/3 \rfloor - (N-d_i) = \lfloor N/3 \rfloor + \lfloor 2N/3 \rfloor - N + d_i - \lfloor 2N/3 \rfloor \geq d_i - \lfloor 2N/3 \rfloor - 1 \tag{5.3}$$

meaning that before the firing of legitimate oscillator $\lfloor N/3 \rfloor + 1$, every legitimate oscillator i for $i = 1, 2, \cdots, N-M$ has already received at least $d_i - \lfloor 2N/3 \rfloor - 1$ pulses within time interval $(t_0+T, t_1]$ (note that this interval has length less than $T/2$).

When legitimate oscillator i fires at t_1, at least d legitimate oscillators will receive the pulse. As every legitimate oscillator has received at least $d_i - \lfloor 2N/3 \rfloor - 1$ pulses within $(t_0+T, t_1]$ (as proven in the previous paragraph), we have that for all legitimate oscillators, the condition $3a)$ of Mechanism 5.1 is satisfied (note that in Scenario 1.1 we consider the case that no legitimate oscillators reset their phases to 0 within (t_1-T, t_1)) and hence all legitimate oscillators that receive the pulse from legitimate oscillator $\lfloor N/3 \rfloor + 1$ (with quantity at least $d-M$) will shift their phases to 2π rad.

Next, we proceed to proved that among the $d-M$ legitimate oscillators whose phases are shifted to 2π rad by the pulse from legitimate oscillator $\lfloor N/3 \rfloor + 1$ at t_1, at least $d - M - \lfloor N/3 \rfloor$ of them will fire. According to condition 2) of Mechanism 5.1, if an oscillator fired within $(t_1-\varepsilon, t_1]$, it cannot fire again at t_1. Since only $\lfloor N/3 \rfloor$ legitimate oscillators fired before the firing of legitimate oscillator $\lfloor N/3 \rfloor + 1$ at t_1 (note that these oscillators might fire within $(t_1-\varepsilon, t_1]$), we obtain that among the $d-M$ legitimate oscillators whose phases are shifted to 2π rad at t_1 by the pulse from legitimate oscillator $\lfloor N/3 \rfloor + 1$, at least $d - M - \lfloor N/3 \rfloor$ of

them will fire at t_1. From Lemma 5.1 and making use of the fact $M < d - \lfloor 2N/3 \rfloor$, we have

$$d - M - \lfloor N/3 \rfloor > \lfloor N/3 \rfloor$$

meaning that the firing of legitimate oscillator $\lfloor N/3 \rfloor + 1$ will trigger at least $\lfloor N/3 \rfloor + 1$ other legitimate oscillators to fire simultaneously at t_1. The firing of these oscillators will further makes every legitimate oscillator i for $i = 1, 2, \cdots, N - M$ to receive at least $d_i - \lfloor 2N/3 \rfloor$ pulses at t_1 based on the relationship in (5.3). Since all legitimate oscillators' phases reside in $[\pi, 2\pi]$, according to Mechanism 5.1, they will be shifted to 2π rad at t_1. Then, all the non-firing legitimate oscillators except those fired within the past ε time will fire at t_1.

Recalling that only $\lfloor N/3 \rfloor$ legitimate oscillators fired before legitimate oscillator $\lfloor N/3 \rfloor + 1$ fires at t_1, we obtain that at least $N - M - \lfloor N/3 \rfloor$ legitimate oscillators will fire at t_1 and every legitimate oscillator i for $i = 1, 2, \cdots, N - M$ will receive at least $N - M - \lfloor N/3 \rfloor - (N - d_i)$ pulses from this firing event. According to Lemma 5.1 and combining the fact $M < d - \lfloor 2N/3 \rfloor$, we have

$$N - M - \lfloor N/3 \rfloor - (N - d_i) = d_i - M - \lfloor N/3 \rfloor > \lfloor N/3 \rfloor$$

meaning that every legitimate oscillator receives over $\lfloor N/3 \rfloor$ pulses at t_1. Since every legitimate oscillator has phase residing on 2π and receives over $\lfloor N/3 \rfloor$ pulses within $(t_1 - \varepsilon, t_1]$, all legitimate oscillators' phases will reset to 0 after the firing event at t_1.

Next, we proceed to prove that after time instant t_1, all legitimate oscillators will keep having identical phases and their collective oscillation period is $T = 2\pi$ seconds, i.e., they will achieve synchronization.

From the above analysis, all legitimate oscillators' phases will be reset to 0 at t_1. Because a legitimate oscillator's phase can only be affected by an incoming pulse when it resides in $[\pi, 2\pi]$, we have that all legitimate oscillators' phases will evolve freely towards π rad within time interval $(t_1, t_1 + T/2)$. As soon as all legitimate oscillators' phases reach π rad at time instant $t_1 + T/2$, according to Mechanism 5.1, legitimate oscillator i's phase can be affected by an incoming pulse at time instant $t_1' \in [t_1 + T/2, t_1 + T)$ only if it receives over $d_i - \lfloor 2N/3 \rfloor - 1$ pulses within $(t_1' - \varepsilon, t_1']$. Since the number of attackers satisfies $M \leq d - \lfloor 2N/3 \rfloor - 1 \leq d_i - \lfloor 2N/3 \rfloor - 1$ and each attacker can emit at most one attack pulse within a time interval less than ε, so attack pulses alone are not enough to trigger a phase shift on any legitimate oscillator's phase. Therefore, all legitimate oscillators will have identical phases and evolve freely towards 2π rad.

At time instant $t_1 + T$, all legitimate oscillators reach phase 2π rad and fire simultaneously, which makes legitimate oscillator i for $i = 1, 2, \cdots, N-M$ receive at least $N - M - (N - d_i) = d_i - M > \lfloor N/3 \rfloor$ pulses. Therefore, all legitimate oscillators will reset their phases to 0 immediately. By repeating the above analyses, we can get that after time instant t_1, all legitimate oscillators will have identical phases with a collective oscillation period $T = 2\pi$ seconds, i.e., phase synchronization of all legitimate oscillators is achieved immediately after time instant t_1.

Next, we consider *Scenario 1.2*, i.e., at least one legitimate oscillator has reset its phase to 0 before legitimate oscillator $\lfloor N/3 \rfloor + 1$ fires at t_1. Without loss of generality, we assume that legitimate oscillator k is the first legitimate oscillator who resets its phase to 0 within time interval $(t_0 + T, t_1]$ and it resets its phase to 0 at $t_k \in (t_0 + T, t_1]$. According to Mechanism 5.1, legitimate oscillator k must have received over $\lfloor N/3 \rfloor$ pulses within $(t_k - \varepsilon, t_k]$.

We assume that legitimate oscillator k receives the $\lfloor N/3 \rfloor + 1$'th pulse at time t'_k within time interval $(t_k - \varepsilon, t_k]$ and the pulse is sent by oscillator k'. According to condition 2) of Mechanism 5.1, an oscillator can only fire once within $(t_k - \varepsilon, t_k]$. So before the firing of oscillator k' at t'_k, at least $\lfloor N/3 \rfloor$ oscillators fired within $(t_k - \varepsilon, t'_k]$. Based on the relationship in (5.3), every legitimate oscillator i for $i = 1, 2, \cdots, N-M$ should have received at least $d_i - \lfloor 2N/3 \rfloor - 1$ pulses within $(t_k - \varepsilon, t'_k]$.

Then following the same line of reasoning in *Scenario 1.1*, we have that the pulse of oscillator k' will shift the phases of at least $d - M$ legitimate oscillators (which receive the pulse) to 2π rad and at least $\lfloor N/3 \rfloor + 1$ of them will fire at t'_k. Then, all legitimate oscillators' phases will be shifted to 2π rad and at least $N - M - \lfloor N/3 \rfloor$ legitimate oscillators will fire at t'_k. Every legitimate oscillator will receive over $\lfloor N/3 \rfloor$ pulses in this firing event at t'_k and will reset its phase to 0. We can also infer $t'_k = t_k = t_1$.

Next, following the same line of reasoning in *Scenario 1.1*, we obtain that after time instant t_1, all legitimate oscillators will have identical phases and their collective oscillation period is $T = 2\pi$ seconds, i.e., phase synchronization of all legitimate oscillators is achieved immediately after time instant t_1. □

Remark 5.4. *Theorem 5.1 requires that the degree of the network is over $\lfloor 2N/3 \rfloor$, which, according to [24], also guarantees that the network is strongly connected.*

Remark 5.5. *The mechanism requires that all legitimate oscillators to start at the same time instant. However, starting at the same time instant does not avoid dealing with arbitrary phase distribution since even after synchronization, for a non-all-to-all topology on which different attackers can affect different legitimate oscillators, attackers considered in this chapter can disturb the phases of legitimate oscillators to an arbitrary*

distribution under existing pulse-coupled synchronization strategies.

Remark 5.6. *It is worth noting that the theoretical analysis in this chapter is significantly different from our prior results in Chapters* 2-4*. In Chapters* 2-4*, we can prove that the length of the containing arc will decrease monotonically with time. However, in this chapter, since the initial phases of all legitimate oscillators are arbitrarily distributed in the entire oscillation period and the considered attacker model is much stronger, such monotonic decreasing does not exist (see numerical simulation results in Fig. 5.5, Fig. 5.7, Fig. 5.8, and Fig. 5.9. Instead, we opt to prove that after initiation, our judiciously designed interaction mechanism can drive the phases of legitimate oscillators to within a half cycle in finite time. Then we proceed to prove that one legitimate oscillator's firing can (either directly or indirectly) trigger all legitimate oscillators to reset their phases to* 0 *and the interaction mechanism can maintain phase synchronization even in the presence of attack pulses.*

Mechanism 5.1 can also guarantee synchronization of densely connected PCO networks in the absence of attacks, as detailed below:

Corollary 5.1. *For a network of N legitimate PCOs, if the degree of the PCO network satisfies* $d > \lfloor 2N/3 \rfloor$*, then all oscillators will synchronize under Mechanism* 5.1 *from an arbitrary initial phase distribution.*

Proof. Corollary 5.1 is a special case of Theorem 5.1 when the number of attackers M is set to 0 and hence is omitted. □

5.6 Extension to the Case where N is Unknown to Individual Oscillators

The implementation of Mechanism 5.1 requires each node to have access to N, which may not be feasible in a completely decentralized network. Therefore, in this section, we propose a mechanism for the case where N is unknown to individual oscillators. The essence is to leverage the degree information of individual oscillators, as detailed below:

New Pulse-Based Synchronization Mechanism (Mechanism 5.2):

1. The phase ϕ_i of legitimate oscillator i evolves from 0 to 2π rad with a constant speed $\omega = 1$ rad/second.

2. Once ϕ_i reaches 2π rad at time t, oscillator i fires (emits a pulse) if it did not fire within $(t-\varepsilon, t]$ and an entire period $T = 2\pi$ seconds has elapsed since initiation. Then oscillator i resets its phase from 2π rad to 0 if it received at least $\lfloor d_i/3 \rfloor$ pulses within $(t-\varepsilon, t]$. Otherwise, it resets its phase from 2π rad to π rad.

3. When oscillator i receives a pulse at time instant t', it shifts its phase to 2π rad only if $\phi_i \in [\pi, 2\pi]$ at time instant t' and one of the following conditions is satisfied:

   (a) before receiving the current pulse, oscillator i has already received at least $\lfloor d_i/6 \rfloor - 1$ pulses in $[t'-T/2, t']$ and it did not reset its phase from 2π rad to 0 within $(t'-T, t')$.

   (b) before receiving the current pulse, oscillator i has already received at least $\lfloor d_i/6 \rfloor - 1$ pulses in $(t'-\varepsilon, t']$.

   Otherwise, the pulse has no effect on ϕ_i who will evolve freely towards 2π rad.

Following a similar line of reasoning in Section 5.5, we can prove that Mechanism 5.2 can synchronize densely connected PCO networks both in the presence and absence of Byzantine attackers.

Theorem 5.2. *For a network of N PCOs among which M are compromised and launch attacks following the attack model in Section* 5.3*, if the degree of the PCO network satisfies $d > \lfloor 3N/4 \rfloor$ and the number of attackers M satisfies $M < \lfloor d/6 \rfloor$, then all legitimate oscillators will synchronize under Mechanism* 5.2 *from any initial phase distribution even if N is unknown to individual oscillators.*

Proof. We set the initial time instant to t_0. Similar to the proof in Theorem 5.1, the following proof is divided into two parts. In part I, we prove that all $N-M$ legitimate oscillators will have phases residing in $[\pi, 2\pi]$ at t_0+T. In Part II, we prove that these legitimate oscillators will reset their phases to 0 at the same time and will keep having identical phases with a collective oscillation period $T = 2\pi$ seconds, i.e., they will achieve synchronization.

Part I (all $N-M$ legitimate oscillators' phases reside in $[\pi, 2\pi]$ at t_0+T): Since the number of

attackers satisfies $M < \lfloor d/6 \rfloor$, we have

$$M < \lfloor d/6 \rfloor \leq \lfloor d/3 \rfloor \leq \lfloor d_i/3 \rfloor$$

for $i = 1, 2, \cdots, N-M$. Following the same line of reasoning in the proof of Theorem 5.1, Part I, we have that a legitimate oscillator will only reset its phases to π rad within time interval $[t_0, t_0+T]$ and all legitimate oscillators' phases will reside in $[\pi, 2\pi]$ at time instant t_0+T no matter what the initial phase distribution is.

Part II (all legitimate oscillators will reset their phases to 0 *at the same time and will keep having identical phases with a collective oscillation period* $T = 2\pi$ *seconds)*: Since no legitimate oscillator fires or resets its phase to 0 within time interval $[t_0, t_0+T]$ and all legitimate oscillators' phases reside in $[\pi, 2\pi]$ at time t_0+T, all legitimate oscillators' phases will reach 2π rad and fire at least once within $(t_0+T, t_0+3T/2]$. Without loss of generality, we label all $N-M$ legitimate oscillators according to the order of their first firing time and denote $t_1' \in (t_0+T, t_0+3T/2]$ as the first firing time instant of legitimate oscillator $\lfloor d/2 \rfloor + 1$. Only the following two scenarios could happen before legitimate oscillator $\lfloor d/2 \rfloor + 1$ fires at t_1':

Scenario 2.1: no legitimate oscillator has reset its phase to 0 before legitimate oscillator $\lfloor d/2 \rfloor + 1$ fires at t_1'.

Scenario 2.2: at least one legitimate oscillator has reset its phase to 0 before legitimate oscillator $\lfloor d/2 \rfloor + 1$ fires at t_1'.

Next, we show that in both scenarios all legitimate oscillators will reset their phases to 0 at the same time and will keep having identical phases with a collective oscillation period $T = 2\pi$ seconds, i.e., they will achieve synchronization.

We first consider *Scenario 2.1*, i.e., no legitimate oscillator has reset its phase to 0 before legitimate oscillator $\lfloor d/2 \rfloor + 1$ fires at t_1'. Since all the $N-M$ legitimate oscillators are labeled according to the order of their first firing time instants and no legitimate oscillator fired within $[t_0, t_0+T]$ according to Mechanism 5.1, we have that before the firing of legitimate oscillator $\lfloor d/2 \rfloor + 1$ at t_1', $\lfloor d/2 \rfloor$ legitimate oscillators should have fired within time interval $(t_0+T, t_1']$ and every legitimate oscillator i for $i = 1, 2, \cdots, N-M$ should have received at least $\lfloor d/2 \rfloor - (N-d_i)$ pulses within $(t_0+T, t_1']$, where $(N-d_i)$ is the number of oscillators which are not connected to oscillator i. Since we have $d > \lfloor 3N/4 \rfloor$, one can obtain $d_i \geq d \geq \lfloor 3N/4 \rfloor + 1 > 3N/4$

for $i = 1, 2, \cdots, N-M$. Using Lemma 5.1 and combining the fact $d_i > 3N/4$, we have:

$$\lfloor d/2 \rfloor - (N - d_i) \geq \lfloor d/2 \rfloor - N + \lfloor 5d_i/6 \rfloor + \lfloor d_i/6 \rfloor \geq \lfloor 3N/8 \rfloor + \lfloor 5N/8 \rfloor - N + \lfloor d_i/6 \rfloor \geq \lfloor d_i/6 \rfloor - 1 \quad (5.4)$$

meaning that before the firing of legitimate oscillator $\lfloor d/2 \rfloor + 1$, every legitimate oscillator i for $i = 1, 2, \cdots, N-M$ has already received at least $\lfloor d_i/6 \rfloor - 1$ pulses within time interval $(t_0 + T, t_1']$ (note that this interval has length less than $T/2$). Then following the same line of reasoning in *Scenario 1.1* of Theorem 5.1, we can prove that every legitimate oscillator i will receive at least $\lfloor d_i/3 \rfloor$ pulses at t_1' and reset its phases to 0. Then starting from time instant t_1', all legitimate oscillators will have identical phases with a collective oscillation period $T = 2\pi$ seconds, i.e., they will achieve synchronization.

The proof of *Scenario 2.2* follows the same line of reasoning in *Scenario 1.2* of Theorem 5.1 and is omitted.

Summarizing the above analyses, we conclude that Mechanism 5.2 can synchronize densely connected PCO networks in the presence of Byzantine attacks even when N is unknown to individual oscillators and initial phases are distributed arbitrarily. □

It is worth noting that Mechanism 5.2 can also guarantee synchronization of densely connected PCO networks in the absence of attacks when N is unknown to individual oscillators, as shown below:

Corollary 5.2. *For a network of N legitimate PCOs, if the degree of the PCO network satisfies $d > \lfloor 3N/4 \rfloor$, then all oscillators will synchronize under Mechanism* 5.2 *from any initial phase distribution even if N is unknown to individual oscillators.*

Proof. Corollary 5.2 is a special case of Theorem 5.2 when the number of attackers M is set to 0 and hence is omitted. □

Remark 5.7. *According to Theorem 5.1 and Theorem 5.2, Mechanism* 5.1 *and Mechanism* 5.2 *guarantee that all legitimate oscillators synchronize with a collective oscillation period $T = 2\pi$ seconds (which is equal to the free-running period) even in the presence of Byzantine attacks. This is in distinct difference from existing results where the collective oscillation period is affected by attacks.*

Remark 5.8. *When N is unknown to individual oscillators, d has to be larger than $\lfloor 3N/4 \rfloor$, which is greater than $\lfloor 2N/3 \rfloor$ for the case where N is known. The requirement of increased connectivity is intuitive in that less knowledge of a PCO network requires stronger connectivity conditions to guarantee synchronization.*

5.7 Simulations

We considered a network of $N = 24$ PCOs placed on a circle with diameter 40 meters as illustrated in Figure 5.2. Two oscillators can communicate if and only if their distance is less than 39 meters. Thus, the degree of the network is $d = 20$. We set $t_0 = 0$ and chose initial phases of oscillators randomly from $[0, 2\pi]$.

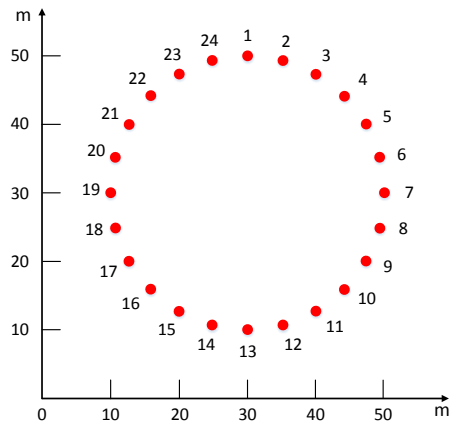

Figure 5.2: The deployment of the 24 oscillators used in simulations.

5.7.1 In the Absence of Attacks

We first considered the attacker-free case. As $d = 20 > \lfloor 3N/4 \rfloor = 18$, we know from Corollary 5.1 and Corollary 5.2 that the network will always synchronize from any initial phase distribution, whether or not N is available to individual oscillators. This was confirmed by the numerical simulation results in Figure 5.3.

Using the same initial phase distribution as in Figure 5.3, we also simulated the phase evolution of PCOs under the pulse-based synchronization mechanism in [3]. It can be seen in Figure 5.4 that the pulse-based synchronization mechanism in [3] cannot achieve synchronization, which shows the advantage of our new mechanisms even when attack-resilience is not relevant.

5.7.2 In the Presence of Attacks

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

We assumed that 3 out of the 24 PCOs (oscillators 1, 8, and 20) were compromised and acted as Byzantine attackers. As $3 < d - \lfloor 2N/3 \rfloor = 4$, we know from Theorem 5.1 that the network will synchronize.

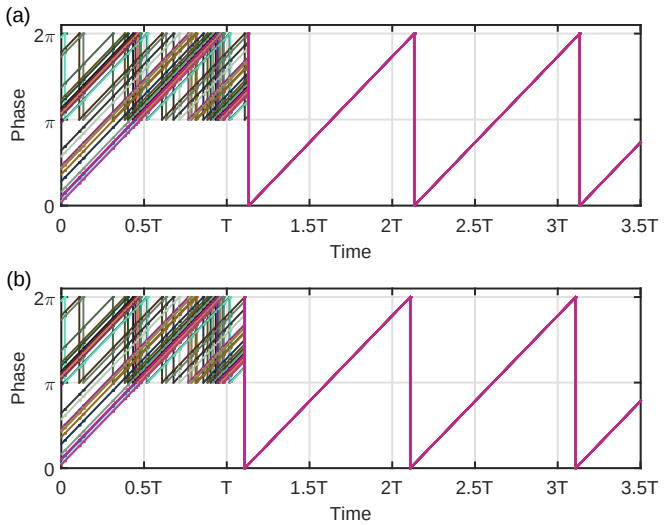

Figure 5.3: Plot (a) and (b) presented the phase evolutions of the 24 PCOs under Mechanism 5.1 and Mechanism 5.2, respectively. ε was set to $0.01T$.

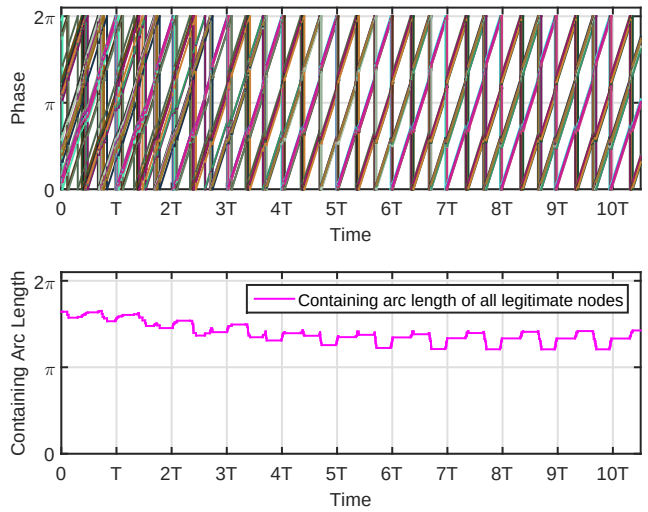

Figure 5.4: Phase evolution and the length of the containing arc of the 24 PCOs under the pulse-based synchronization mechanism in [3]. l was set to 0.021.

This was confirmed by numerical simulations in Figure 5.5, which showed that even under Byzantine attacks the length of the containing arc of legitimate oscillators converged to zero.

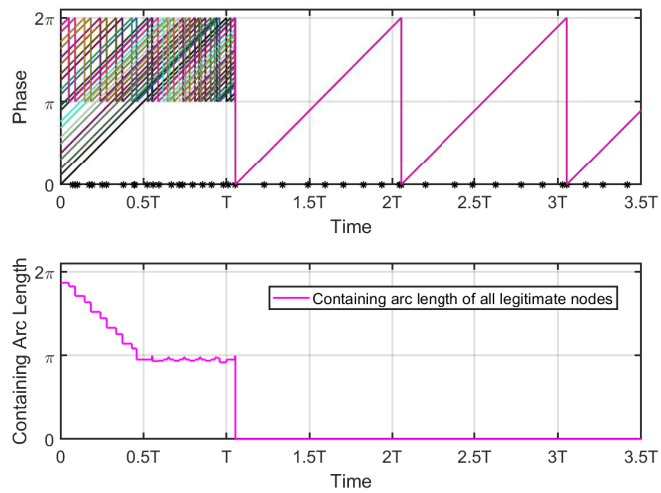

Figure 5.5: Phase evolution and the length of the containing arc of 21 legitimate oscillators under Mechanism 5.1 in the presence of 3 Byzantine attackers (oscillators 1, 8, and 20) with attacking pulse time instants represented by asterisks. ε was set to $0.01T$.

Using the same network, when N is unknown to individual oscillators, according to Theorem 5.2, the maximal allowable number of attackers is $\lfloor d/6 \rfloor - 1 = 2$. Hence, the condition in Theorem 5.2 was not satisfied. Simulation results confirmed that legitimate oscillators indeed could not synchronize as the collective oscillation period is time-varying and less than $T = 2\pi$ seconds, which is illustrated in Figure 5.6.

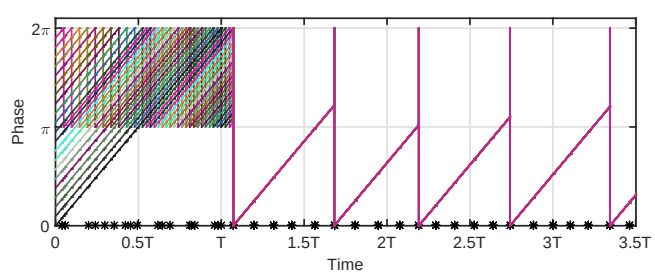

Figure 5.6: Phase evolution of 21 legitimate oscillators under Mechanism 5.2 in the presence of 3 attackers (oscillators 1, 8, and 20) with attacking pulse time instants represented by asterisks. N was unknown to individual oscillators and ε was set to $0.01T$.

However, when we decreased the number of attackers to 2 (oscillators 1 and 8), all legitimate oscillators synchronized under Mechanism 5.2 (see Figure 5.7), confirming the results in Theorem 5.2.

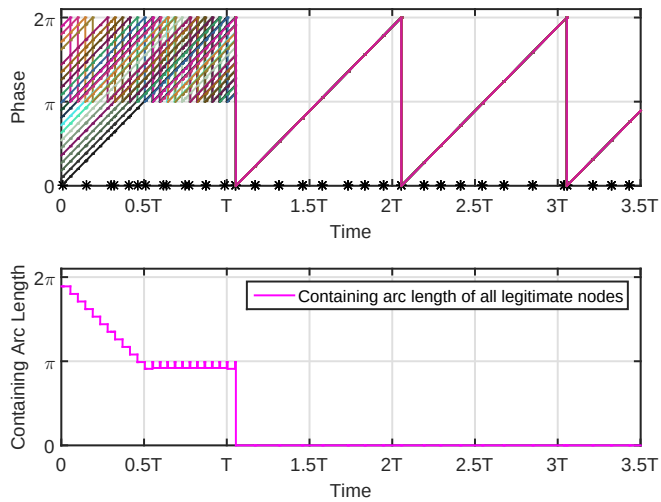

Figure 5.7: Phase evolution and the length of the containing arc of 22 legitimate oscillators under Mechanism 5.2 in the presence of 2 attackers (oscillators 1 and 8) with attacking pulse time instants represented by asterisks. N was unknown to individual oscillators and ε was set to $0.01T$.

5.7.3 Comparison with Existing Results

Under the same PCO network deployment, we also compared our proposed Mechanisms 5.1 and 5.2 with existing attack resilient pulse-based synchronization approaches in [3] and Chapters 2-4 which solely use content-free pulses in communications. When comparing with [3] and Chapters 2-4, we did not use the settings in [3] and Chapters 2-4 since they are special cases of our setting, as can be seen in Table 1.

Figure 5.8 showed the evolutions of containing arc length of legitimate oscillators under Mechanism 5.1 and approaches in [3] and Chapters 2-4 in the presence of 3 Byzantine attackers (oscillators 1, 8, and 20) when N was known to individual oscillators. All approaches used the same initial phase distribution (randomly chosen from $[0, 2\pi]$) and identical malicious pulse attack patterns. It can be seen in Figure 5.8 that Mechanism 5.1 can achieve perfect synchronization whereas pulse-base synchronization approaches in [3] and Chapters 2-4 failed to achieve synchronization even when the coupling strength was set to $l = 1$. It is worth noting that similar results were obtained in all $1,000$ runs of our simulation with the initial phases randomly chosen from $[0, 2\pi]$ and 40 attack pulses randomly distributed in $[0, 3.5T]$.

Figure 5.9 showed the evolutions of containing arc length of legitimate oscillators under Mechanism 5.2 and the approaches in [3] and Chapters 2-4 in the presence of 2 Byzantine attackers (oscillators 1 and 8) when N was unknown to individual oscillators. Under the same set up, it can be seen in Figure 5.9 that Mechanism 5.2 can achieve perfect synchronization whereas existing pulse-base synchronization approaches

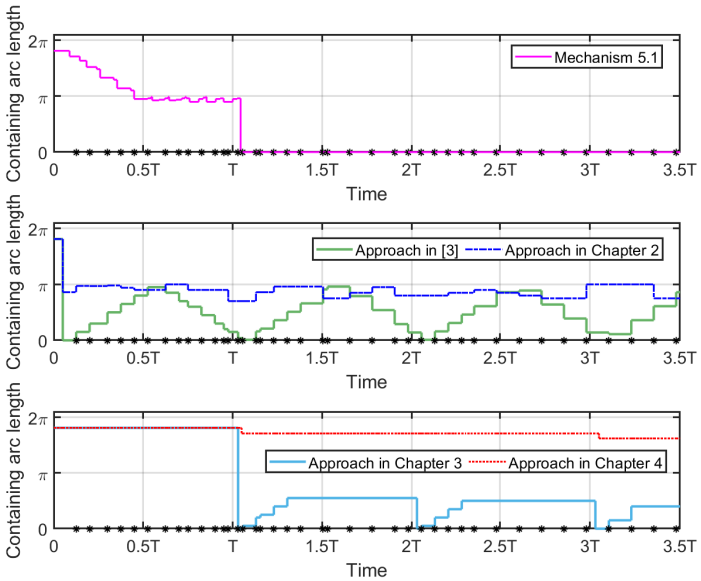

Figure 5.8: The length of the containing arc of 21 legitimate oscillators under Mechanism 5.1 and approaches in [3] and Chapters 2-4 in the presence of 3 Byzantine attackers (oscillators 1, 8, and 20). The attack pulse time instants were represented by asterisks. The coupling strength in [3] and Chapters 2-4 was set to $l = 1$, N was known to individual oscillators, and ε was set to $0.01T$.

in [3] and Chapters 2-4 cannot, which confirmed the advantages of our new mechanism. It is worth noting that similar results were obtained in all $1,000$ runs of our simulation with the initial phases randomly chosen from $[0, 2\pi]$ and 40 attack pulses randomly distributed in $[0, 3.5T]$.

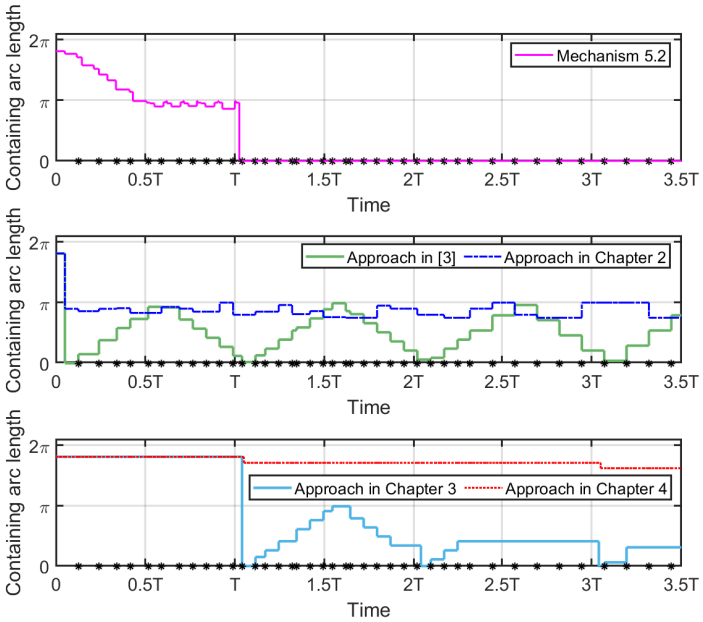

Figure 5.9: The length of the containing arc of 22 legitimate oscillators under Mechanism 5.2 and approaches in [3] and Chapters 2-4 in the presence of 2 Byzantine attackers (oscillators 1 and 8). The attack pulse time instants were represented by asterisks. The coupling strength in [3] and Chapters 2-4 was set to $l = 1$, N was unknown to individual oscillators, and ε was set to $0.01T$.

Chapter 6

Conclusions and Discussion

In this dissertation, we considered attack-resilient pulse-base synchronization. First, by using a carefully designed PRF, we characterize the condition under which an attacker could launch stealthy Byzantine attacks without being detected and show that perfect synchronization of legitimate oscillators can be achieved in the presence of a stealthy Byzantine attacker if some initial conditions on legitimate oscillators' phases are satisfied. Next, we propose a new pulse-based synchronization mechanism to improve the resilience of pulse-based synchronization. We rigorously characterize the condition for mounting stealthy Byzantine attacks under the proposed pulse-based synchronization mechanism and prove analytically that synchronization of legitimate oscillators can be achieved in the presence of multiple stealthy Byzantine attackers even when the initial phases of legitimate oscillators are unrestricted. Then we present a new pulse-based synchronization mechanism for general connected PCOs that can achieve phase synchronization even in the presence of multiple stealthy Byzantine attackers, irrespective of whether the attackers collude with each other or not. Under the proposed synchronization mechanism, we rigorously characterize the condition for stealthy Byzantine attacks and prove that perfect synchronization of general connected legitimate oscillators can be guaranteed even when their initial phases are widely distributed in a half circle. Finally, we revised our pulse-based interaction mechanism to improve the resilience of PCO networks against Byzantine attacks. The revised mechanism can enable synchronization in the presence of multiple Byzantine attackers even when the PCO network is not restricted to all-to-all and the initial phases are distributed arbitrarily. Our results are in distinct difference from most of the existing attack-resilience algorithms which require a priori (almost) synchronization among all legitimate oscillators. The approach is also applicable when the total number of oscillators are unknown to individual oscillators. Numerical simulations confirmed the analytical results.

Appendices

Appendix A Proof of Lemma 2.2

Without loss of generality, we label all oscillators in the increasing order of their phases, i.e., $\phi_1(t_0) \leq \phi_2(t_0) \leq \cdots \leq \phi_N(t_0)$ where t_0 denotes the initial time instant. Since the interaction is all-to-all, i.e., every node can affect every other node, it can be easily obtained that a time-invariant firing sequence can be guaranteed if for any pair of non-firing oscillators i and j, their phase relationship will not be affected by the firing of a third oscillator. In other words, if ϕ_i is larger than ϕ_j immediately before oscillators i and j receive a pulse from a third firing oscillator, then ϕ_i will remain no smaller than ϕ_j immediately after receiving the pulse.

We next prove that this relationship can be guaranteed under the PRF given in (2.2). For the sake of simplicity, we divide the analysis into three cases when an external pulse is received:

1. If both ϕ_i and ϕ_j are less than D, then they will not be affected by the pulse. Hence ϕ_i is still no smaller than ϕ_j after the firing of any oscillator.

2. If $\phi_i \geq D$ and $\phi_j < D$ hold, then upon firing of a third oscillator, ϕ_i will be increased but ϕ_j will not change according to the PRF in (2.2). Therefore, ϕ_i is still no smaller than ϕ_j after the firing event.

3. If both ϕ_i and ϕ_j are larger than D, then both of them will increase upon receiving a pulse from a third node. According to (2.1) and (2.2) , they will become $\phi_i^+ = \phi_i + l(2\pi - \phi_i)$ and $\phi_j^+ = \phi_j + l(2\pi - \phi_j)$, respectively. The difference between ϕ_i^+ and ϕ_j^+ is $\phi_i^+ - \phi_j^+ = (1-l)(\phi_i - \phi_j)$ which is non-negative since $0 < l \leq 1$ and $\phi_i > \phi_j$ hold. So oscillator $i's$ phase is still no smaller than oscillator $j's$ after the firing event.

In conclusion, in a PCO network with PRF (2.2), one oscillator will not surpass another one on the unit circle, which means that the firing sequence is time-invariant.

Appendix B Proof of Theorem 2.1

We first consider statement 1) in Theorem 2.1, i.e., within any time interval of length T_L, at most N pulses can be generated when all oscillators are legitimate. If we can find the shortest time interval T_L during which a network of N legitimate PCOs can emit $N+1$ pulses, then we can detect at most N pulses within $[t, t+T_L)$ for any t.

Without loss of generality, we label all oscillators in an increasing order of their phases, i.e., $\phi_1(t_0) \leq \phi_2(t_0) \leq \cdots \leq \phi_N(t_0)$ where t_0 denotes the initial time instant. According to Lemma 2.2, the firing sequence will not change. So for the network to emit $N+1$ pulses, oscillator N has to send out two pulses and all the other oscillators have to send one pulse each. Therefore, the problem of finding the minimum time interval to detect $N+1$ pulses is reduced to finding the minimum time interval for oscillator N to fire twice.

Apparently, in order to acquire the minimum time interval for oscillator N to fire twice, the initial phase of oscillator N should be $\phi_N(t_0) = 2\pi$. Furthermore, because the PRF in (2.2) is non-negative, the phase evolution of an oscillator can only be accelerated or unaffected by exchanged pulses. Therefore, the minimal time interval is attained when oscillator $N's$ phase is accelerated by the firing of all the other oscillators, i.e., its phase should reside in $[D, 2\pi]$ when other oscillators fire.

According to the above analysis, at the initial time instant t_0, oscillator $N's$ phase should be 2π and all the other oscillators' initial phases should be less than $2\pi - D$. So that when they fire, the phase of oscillator N is larger than D. Because $2\pi - D \leq D$ holds from the definition of the PRF in (2.2), we can get that oscillators N and $N-1$ are the respective ending and starting points of the containing arc and the length of the containing arc is $2\pi - (\phi_N(t_0) - \phi_{N-1}(t_0))$, which is no greater than δ according to the assumption of the theorem. So we have $\phi_{N-1}(t_0) \leq \delta$.

At time instant t_0^+, oscillator N emits a pulse and resets its phase to 0, i.e. $\phi_N(t_0^+) = 0$. Because all the other oscillators reside in the refractory period, their phases' evolutions are not affected by the firing of oscillator N, i.e., $\phi_i(t_0^+) = \phi_i(t_0)$ for $i = 1, 2, \cdots, N-1$. At this time instant, oscillator $N-1$ has the largest phase and will reach 2π at $t_1 = t_0 + \Delta t_1$ where $\Delta t_1 = 2\pi - \phi_{N-1}(t_0)$. At time instant t_1, we have $\phi_N(t_1) = 2\pi - \phi_{N-1}(t_0)$ and $\phi_i(t_1) = 2\pi - \phi_{N-1}(t_0) + \phi_i(t_0)$ for $i = 1, 2, \cdots, N-1$. Because $0 \leq \phi_{N-1}(t_0) < 2\pi - D$ holds, we have $D \leq \phi_i(t_1) \leq 2\pi$ for $i = 1, 2, \cdots, N$.

At time instant t_1, oscillator $N-1$ emits a pulse and resets its phase to 0, i.e., $\phi_{N-1}(t_1^+) = 0$. Because all the other oscillators' phases reside in $[D, 2\pi]$, they will be expedited by the firing of oscillator $N-1$. Since their phases immediately before the firing of oscillator $N-1$ are $\phi_N(t_1) = 2\pi - \phi_{N-1}(t_0)$ and $\phi_i(t_1) = 2\pi -$

$\phi_{N-1}(t_0)+\phi_i(t_0)$ for $i=1,2,\cdots,N-2$, after the firing of oscillator $N-1$, their phases become $\phi_N(t_1^+)=2\pi-(1-l)\phi_{N-1}(t_0)$, $\phi_i(t_1^+)=2\pi-(1-l)(\phi_{N-1}(t_0)-\phi_i(t_0))$ for $i=1,2,\cdots,N-2$. Then, oscillator $N-2$ has the maximal phase and will fire next at time instant t_2. We have $t_2=t_1+\Delta t_2$ where $\Delta t_2=(1-l)(\phi_{N-1}(t_0)-\phi_{N-2}(t_0))$.

At time instant t_2, oscillator $N-2$ emits a pulse and resets its phase to 0, i.e., $\phi_{N-2}(t_2^+)=0$. Since the phases of the other oscillators are $\phi_N(t_2)=2\pi-(1-l)\phi_{N-2}(t_0)$, $\phi_{N-1}(t_2)=\Delta t_2$ and $\phi_i(t_2)=2\pi-(1-l)(\phi_{N-2}(t_0)-\phi_i(t_0))$ for $i=1,2,\cdots,N-3$, it can be verified that only $\phi_{N-1}(t_2)=\Delta t_2$ resides in the refractory period and the other oscillators will be expedited by the firing of oscillator $N-2$. Therefore, after the firing of oscillator $N-2$, the phases of all the oscillators are $\phi_N(t_2^+)=2\pi-(1-l)^2\phi_{N-2}(t_0)$, $\phi_{N-1}(t_2^+)=\Delta t_2$, $\phi_{N-2}(t_2^+)=0$ and $\phi_i(t_2^+)=2\pi-(1-l)^2(\phi_{N-2}(t_0)-\phi_i(t_0))$ for $i=1,2,\cdots,N-3$.

Repeating the same analysis, we can get that $\Delta t_i=(1-l)^{i-1}(\phi_{N-i+1}(t_0)-\phi_{N-i}(t_0))$ for $i=2,3,\cdots,N-1$. After the firing of oscillator 1 at time instant t_{N-1}, we have $\phi_1(t_{N-1}^+)=0$, $\phi_N(t_{N-1}^+)=2\pi-(1-l)^{N-1}\phi_1(t_0)$, and $\phi_i(t_{N-1}^+)=\sum_{N-i+1}^{N-1}\Delta t_j$ for $i=2,3,\cdots,N-1$. At this time instant, oscillator N has the largest phase and will fire the second time after a time interval $\Delta t_N=(1-l)^{N-1}\phi_1(t_0)$. Therefore, the total time consumption for oscillator N to fire twice can be obtained as follows:

$$T_L=\sum_{i=1}^{N}\Delta t_i=2\pi-\phi_{N-1}(t_0)+(1-l)^{N-1}\phi_1(t_0)+\sum_{i=2}^{N-1}(1-l)^{i-1}(\phi_{N-i+1}(t_0)-\phi_{N-i}(t_0)) \tag{B.1}$$

Denoting $\varepsilon_i=\phi_{N-i+1}(t_0)-\phi_{N-i}(t_0)$ for $i=2,3,\cdots,N-1$ and $\varepsilon=\sum_{i=2}^{N-1}((1-l)^{i-1}-(1-l)^{N-1})\varepsilon_i$, we can get

$$\begin{aligned}T_L&=(1-l)^{N-1}(\phi_{N-1}(t_0)-\sum_{i=2}^{N-1}\varepsilon_i)+\sum_{i=2}^{N-1}(1-l)^{i-1}\varepsilon_i+2\pi-\phi_{N-1}(t_0)\\&=2\pi-(1-(1-l)^{N-1})\phi_{N-1}(t_0)+\varepsilon\end{aligned} \tag{B.2}$$

Clearly, the minimal T_L is obtained when $\phi_{N-1}(t_0)$ is maximized and ε is minimized. Since we have $\phi_{N-1}(t_0)\leq\delta$, the maximal value of $\phi_{N-1}(t_0)$ can be obtained as δ. Furthermore, according to the arrangement of oscillator indexes, we have $\phi_{N-i+1}(t_0)-\phi_{N-i}(t_0)\geq 0$ for $i=2,3,\cdots,N-1$, which means that the smallest value of ε is 0 when $\phi_{N-i+1}(t_0)=\phi_{N-i}(t_0)$ holds for $i=2,3,\cdots,N-1$. Therefore, the minimal value of T_L can be obtained as $2\pi-\delta+(1-l)^{N-1}\delta$.

Next, we proceed to prove that during any time interval of length T_U, we can detect at least N pulses. Because all oscillators are labeled in an increasing order of their phases and the oscillation firing sequence will

not change with time, the problem of finding the maximal time period containing N firing events transforms to finding the maximal time for oscillator 1 to fire, which is obtained when ϕ_1 is not accelerated by the firing of any other oscillators, and hence is given by $2\pi - \phi_1(t_0)$. Given $\phi_1(t_0) \geq 0$, the maximal value of T_U can be acquired as $T_U = 2\pi$ seconds.

Appendix C Proof of Theorem 2.2

We first consider statement 1). If the conditions in statement 1) are met, the phases of legitimate oscillators can only be distributed in the following three ways when the malicious pulse is sent, as illustrated in plots a, b, and c in Fig. C.1:

a) All legitimate oscillators' phases reside in $[D, 2\pi]$;

b) All legitimate oscillators' phases reside in $[0, D)$;

c) Some of the legitimate oscillators' phases reside in $[D, 2\pi]$ and the rest reside in $[0, D)$ but phase D does not belong to the containing arc.

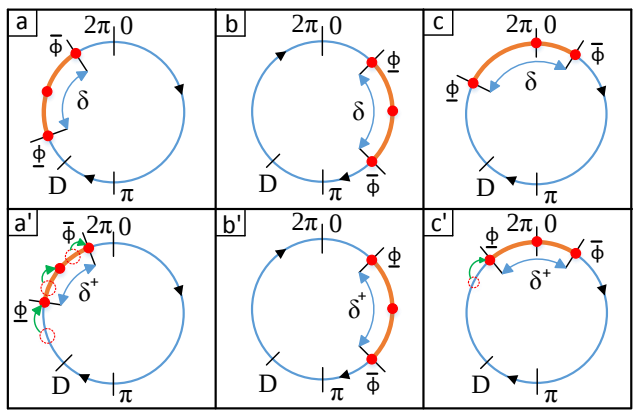

Figure C.1: a, b, and c correspond to three possible phase distributions satisfying the conditions in statement 1) of Theorem 2.2. δ and δ^+ denote the respective length of the containing arc of legitimate oscillators right before and after receiving the malicious pulse. $\bar{\phi}$ and $\underline{\phi}$ represent the starting and ending points of the containing arc, respectively. The dashed and solid red circles represent the phases of legitimate oscillators right before and after the malicious pulse is sent, respectively.

In Fig. C.1, δ and δ^+ are used to denote the length of the containing arc of legitimate oscillators right before and after the malicious pulse is sent. According to statement 1), we have $\delta < 2\pi - D$. Next, we show that in all the three cases, the malicious pulse cannot increase the length of the containing arc, i.e., $\delta^+ \leq \delta < 2\pi - D$.

a) All legitimate oscillators' phases reside in $[D, 2\pi]$. Denoting the phases of the starting and ending points of the containing arc as $\bar{\phi}$ and $\underline{\phi}$, respectively before receiving the malicious pulse, we have $\delta = \bar{\phi} - \underline{\phi}$. According to the PRF in (2.2), it can be obtained that the phases of oscillators $\bar{\phi}$ and $\underline{\phi}$ will become $\bar{\phi}^+ = \bar{\phi} + l(2\pi - \bar{\phi})$ and $\underline{\phi}^+ = \underline{\phi} + l(2\pi - \underline{\phi})$ after receiving the malicious pulse. Therefore, the length of the

containing arc becomes $\delta^+ = \bar{\phi}^+ - \underline{\phi}^+ = (1-l)(\bar{\phi} - \underline{\phi})$ which is no larger than the length before receiving the pulse, i.e., $\delta = \bar{\phi} - \underline{\phi}$. Hence, we obtain that the length of the containing arc will be less than $2\pi - D$ after receiving the malicious pulse;

b) All legitimate oscillators' phases reside in $[0, D)$. In this case, the malicious pulse cannot affect the phase of any legitimate oscillator, and the length of the containing arc is not affected, i.e., $\delta^+ = \delta < 2\pi - D$;

c) Some of the legitimate oscillators' phases reside in $[D, 2\pi]$ and the rest in $[0, D)$ but phase D does not belong to the containing arc. In this case, denote the phases of the starting and ending points of the containing arc as $\bar{\phi}$ and $\underline{\phi}$, respectively before receiving the malicious pulse. The length of the containing arc is $\delta = 2\pi - \underline{\phi} + \bar{\phi}$. According to the PRF (2.2), it can be obtained that the phases of oscillators $\bar{\phi}$ and $\underline{\phi}$ will become $\bar{\phi}^+ = \bar{\phi}$ and $\underline{\phi}^+ = \underline{\phi} + l(2\pi - \underline{\phi})$, respectively upon receiving the malicious pulse. Therefore, the length of the containing arc becomes $\delta^+ = 2\pi - \underline{\phi}^+ + \bar{\phi}^+ = 2\pi - \underline{\phi} - l(2\pi - \underline{\phi}) + \bar{\phi}$, which is no larger than the length before receiving the pulse, i.e., $\delta = 2\pi - \underline{\phi} + \bar{\phi}$. Hence, we can obtain that the length of the containing arc is less than $2\pi - D$ after receiving the malicious pulse.

Statement 1) gives conditions under which the containing arc is not expanded by the malicious pulse, i.e., $\delta^+ \leq \delta < 2\pi - D$. Next, we consider statement 2). When the containing arc has phase D in its interior or as its starting point and its length is less than $(1-l)(2\pi - D)$ before the malicious pulse is sent, we can obtain that the starting point should reside in $[D, 2\pi]$ and the ending point should reside in $[0, D)$. Denote the starting and ending points as $\bar{\phi}$ and $\underline{\phi}$, respectively before receiving the malicious pulse. The length of the containing arc can be obtained as $\delta = \bar{\phi} - \underline{\phi}$. According to the PRF in (2.2), the phases of oscillators $\bar{\phi}$ and $\underline{\phi}$ will become $\bar{\phi}^+ = \bar{\phi} + l(2\pi - \bar{\phi})$ and $\underline{\phi}^+ = \underline{\phi}$ upon receiving the malicious pulse and the length of the containing arc will become $\delta^+ = \bar{\phi}^+ - \underline{\phi}^+ = \delta + l(2\pi - \bar{\phi})$, which is greater than δ. Using the facts $\delta < (1-l)(2\pi - D)$ and $\bar{\phi} \in [D, 2\pi]$, we have $\delta^+ < (1-l)(2\pi - D) + l(2\pi - D) = 2\pi - D$. Hence, we can get that the length of the containing arc will be increased by the malicious pulse, but its length after the increment is less than $2\pi - D$.

The situation in statement 2) is visualized in Fig. C.2, where δ and δ^+ in plot d and plot d' represent the lengths of the containing arc before and after the malicious pulse is sent, respectively.

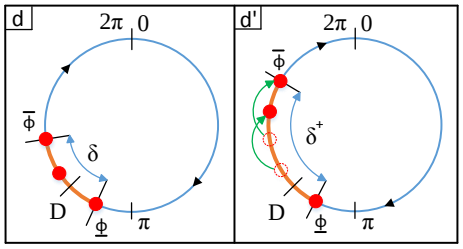

Figure C.2: The phase distribution corresponding to statement 2) in Theorem 2.2. δ and δ^+ denote the respective length of the containing arc of legitimate oscillators right before and after receiving the malicious pulse. $\bar{\phi}$ and $\underline{\phi}$ represent the starting and ending points of the containing arc, respectively. The dashed and solid red circles represent the phases of legitimate oscillators right before and after the malicious pulse is sent, respectively.

Appendix D Proof of Theorem 2.3

We first consider condition 1) of Theorem 2.3. According to Theorem 2.2, the first malicious pulse cannot increase the length of the containing arc if condition 1) of Theorem 2.3 is met. In this proof, we will first show that if the phases of legitimate oscillators satisfy condition 1) of Theorem 2.3 when the first malicious pulse is sent, then they will still satisfy condition 1) of Theorem 2.3 when the following malicious pulses are emitted. Therefore, we can reach the conclusion that no malicious pulses can increase the length of the containing arc. Further making use of Lemma 2.1, we can show that synchronization of legitimate oscillators can be guaranteed.

Without loss of generality, we assume that oscillator N is compromised and emits malicious pulses at time instants T_k for $k = 1, 2, \cdots, \infty$. Denote $\Delta T_k = T_{k+1} - T_k$ as the time interval between the kth and $k+1^{th}$ malicious pulses. According to Definition 2.1, ΔT_k can be time-varying but resides in the interval $[T_L, T_U]$. Similar as before, let the phase of oscillator i be denoted as $\phi_i(t)$ and the length of the containing arc of all legitimate oscillators at time instant t as $\delta(t)$. At time instant T_1, we label all legitimate oscillators in an increasing order of their phases, i.e., $\phi_1(T_1) \leq \phi_2(T_1) \leq \cdots \leq \phi_{N-1}(T_1)$.

The following proof is divided into three parts to make the logical flow smooth. Part I is for the scenario where the containing arc of legitimate oscillators resides in $[D, 2\pi]$ when the first malicious pulse is sent; Part II is for the scenario where the containing arc of legitimate oscillators resides in $[0, D)$ when the first malicious pulse is sent; Part III is for the scenario where the containing arc resides partially in $[0, D)$ and partially in $[D, 2\pi]$ but phase D does not belong to the containing arc when the first malicious pulse is sent.

Part I (The containing arc of legitimate oscillators resides in the interval $[D, 2\pi]$ when the first malicious pulse is sent):

Since all legitimate oscillators reside in the interval $[D, 2\pi]$, the length of the containing arc at this time instant is determined by $\delta(T_1) = \phi_{N-1}(T_1) - \phi_1(T_1)$ and it satisfies $\delta(T_1) \leq \delta_1$ according to the assumption in condition 1) of Theorem 2.3. After receiving the first malicious pulse, we have $\phi_i(T_1^+) = 2\pi - (1-l)(2\pi - \phi_i(T_1))$ for $i = 1, 2, \cdots, N-1$. The next malicious pulse will be sent after ΔT_1. According to Theorem 2.1 and Definition 2.1, to stay stealthy, the compromised oscillator will send the second malicious pulse after some time $\Delta T_1 \in [T_L, T_U]$ where

$$\begin{cases} T_L = 2\pi - \delta_1 + (1-l)^{N-1}\delta_1 \\ T_U = 2\pi \end{cases} \tag{D.1}$$

Because $\delta_1 \leq 2\pi - D$ is true, one can easily get $T_L > D \geq 2\pi - D$. Therefore, it follows $\phi_i(T_1^+) + T_L > 2\pi$ for all $i = 1, 2, \ldots, N-1$ which means that every legitimate oscillator will fire at least once before the second malicious pulse is emitted. Next, we proceed to characterize the phases of all legitimate oscillators when the second malicious pulse is sent at time instant T_2 by carefully analyzing the evolution of all legitimate oscillators' phases.

At time instant T_1^+, ϕ_{N-1} is the largest phase and will reach 2π freely after time $\Delta t_1 = (1-l)(2\pi - \phi_{N-1}(T_1))$. Denoting $t_1 = T_1 + \Delta t_1$, we have $\phi_i(t_1) = 2\pi - (1-l)(\phi_{N-1}(T_1) - \phi_i(T_1))$ for $i = 1, 2, \cdots, N-1$. Then, oscillator $N-1$ emits a pulse and resets its phase to 0 at time instant t_1^+. Meanwhile, its pulse will trigger the phase shift of other legitimate oscillators, which leads to $\phi_i(t_1^+) = 2\pi - (1-l)^2(\phi_{N-1}(T_1) - \phi_i(T_1))$, for $i = 1, 2, \cdots, N-2$.

After the firing of oscillator $N-1$, ϕ_{N-2} becomes the largest and will reach 2π after time $\Delta t_2 = (1-l)^2(\phi_{N-1}(T_1) - \phi_{N-2}(T_1))$. Denoting $t_2 = t_1 + \Delta t_2$, we have $\phi_{N-1}(t_2) = \Delta t_2$ and $\phi_i(t_2) = 2\pi - (1-l)^2(\phi_{N-2}(T_1) - \phi_i(T_1))$ for $i = 1, 2, \cdots, N-2$. At time instant t_2^+, oscillator $N-2$ will emit a pulse and reset its phase to 0. It can be derived that $\phi_{N-1}(t_2) \in [0, D)$ which means that oscillator $N-1$ still resides in the refractory period. So we have $\phi_{N-1}(t_2^+) = \Delta t_2$ and $\phi_i(t_2^+) = 2\pi - (1-l)^3(\phi_{N-2}(T_1) - \phi_i(T_1))$ for $i = 1, 2, \cdots, N-3$.

Repeating the above analysis, we can deduce that the time between the firing events of oscillators $i+1$ and i is $\Delta t_{N-i} = (1-l)^{N-i}(\phi_{i+1}(T_1) - \phi_i(T_1))$ for $i = 1, 2, \cdots, N-2$. After the firing of oscillator 1 at time instant t_{N-1}, the phase of all legitimate oscillators are given by $\phi_1(t_{N-1}^+) = 0$ and $\phi_i(t_{N-1}^+) = \sum_{N-i+1}^{N-1} \Delta t_j$ for $i = 2, 3, \cdots, N-1$. At this time instant, oscillator $N-1$ has the largest phase and oscillator 1 has the smallest phase.

Denoting Γ_1 as the total time it takes for all legitimate oscillators to fire once since T_1, we have

$$\Gamma_1 = \sum_{i=1}^{N-1} \Delta t_i = (1-l)(2\pi - \phi_{N-1}(T_1)) + \sum_{i=1}^{N-2} (1-l)^{N-i}(\phi_{i+1}(T_1) - \phi_i(T_1)) \tag{D.2}$$

According to the derivation below (D.1), one has $\Delta T_1 > \Gamma_1$ and hence as the process evolves, the second malicious pulse will be emitted after time $\Delta T_1 - \Gamma_1$ at time instant T_2. Under no interaction, the phase of oscillator $N-1$ will reach 2π the second time after $2\pi - \phi_{N-1}(t_{N-1}^+)$. Next, we prove that it is larger than $\Delta T_1 - \Gamma_1$, which means that the phase of oscillator $N-1$ will be no larger than 2π at time instant T_2.

Based on (D.2) and the relationship $\Delta T_1 \in [T_L, T_U]$, which is specified in (D.1), we have $2\pi - \phi_{N-1}(t_{N-1}^+) - (\Delta T_1 - \Gamma_1) = 2\pi - \Delta T_1 + \Delta t_1 \geq 0$. Therefore, the phase of oscillator $N-1$ is no larger than 2π

at time instant T_2, and hence all legitimate oscillators' phases will be no larger than 2π at time instant T_2. So the phases of all legitimate oscillators at time instant T_2 can be obtained as $\phi_i(T_2) = \Delta T_1 - \Gamma_1 + \phi_i(t_{N-1}^+)$ for $i = 1, 2, \cdots, N-1$.

Next, we proceed to examine the lower and upper bounds of $\phi_i(T_2)$. Let $\Gamma_1' = \Gamma_1 - \phi_i(t_{N-1}^+)$, then the phases of all legitimate oscillators at time instant T_2 can be represented as

$$\phi_i(T_2) = \Delta T_1 - \Gamma_1' \tag{D.3}$$

The lower and upper bounds of $\phi_i(T_2)$ can be acquired by examining the lower and upper bounds of Γ_1' and ΔT_1. At time instant t_{N-1}^+, oscillator $N-1$ has the largest phase and oscillator 1 has the smallest phase. So we have

$$\Gamma_1 - \phi_{N-1}(t_{N-1}^+) \leq \Gamma_1' \leq \Gamma_1 - \phi_1(t_{N-1}^+)$$

Recall $\phi_{N-1}(t_{N-1}^+) = \sum_{i=2}^{N-1} \Delta t_i$ and $\phi_1(t_{N-1}^+) = 0$, one can get $\Delta t_1 \leq \Gamma_1' \leq \Gamma_1$. The lower bound of Γ_1' can be obtained when Δt_1 is minimized and the upper bound of Γ_1' can be obtained when Γ_1 is maximized. Since Δt_1 is determined by $(1-l)(2\pi - \phi_{N-1}(T_1))$, it is minimized when $\phi_{N-1}(T_1)$ is maximized. Given $\phi_{N-1}(T_1) \in [D, 2\pi]$, we get the lower bound of Δt_1 as 0 when $\phi_{N-1}(T_1)$ is 2π.

Next, we determine the maximal value of Γ_1. Denoting $\varepsilon_i = \phi_{i+1}(T_1) - \phi_i(T_1)$ for $i = 1, 2, \cdots, N-2$ and $\varepsilon = \sum_{i=1}^{N-2}((1-l) - (1-l)^{N-i})\varepsilon_i$, we have the following equation from (D.2):

$$\Gamma_1 = (1-l)(2\pi - \phi_{N-1}(T_1)) + \sum_{i=1}^{N-2}(1-l)^{N-i}\varepsilon_i = (1-l)(2\pi - \phi_1(T_1)) - \varepsilon \tag{D.4}$$

Γ_1 is maximized when $\phi_1(T_1)$ and ε are minimized. Because $\phi_1(T_1) \in [D, 2\pi]$ and $\varepsilon_i \geq 0$ for $i = 1, 2, \cdots, N-2$ hold, which means that the minimal value of $\phi_1(T_1)$ and ε are D and 0, respectively. Therefore, the maximal value of Γ_1 can be obtained as $(1-l)(2\pi - D)$. Hence, the upper and lower bounds of Γ_1' can be acquired as:

$$0 \leq \Gamma_1' \leq (1-l)(2\pi - D) \tag{D.5}$$

Using the fact $\Delta T_1 \in [T_L, T_U]$ and combining (2.5), (D.3), and (D.5), give the upper and lower bounds of $\phi_i(T_2)$ as $D \leq \phi_i(T_2) \leq 2\pi$, which means that when the second malicious pulse is sent at time instant T_2, all legitimate oscillators' phases will reside in the set $[D, 2\pi]$.

On the other hand, according to Theorem 2.2, the first malicious pulse could not increase the length

of the containing arc of legitimate oscillators, i.e., we have $\delta(T_2) \leq \delta(T_1) \leq \delta_1$. Therefore, at time instant T_2, all conditions for the derivations conducted at T_1 still hold. So repeating the above analysis, we can get $\phi_i(T_k) \in [D, 2\pi]$ and $\delta(T_k) \leq \delta_1$ for $i = 1, 2, \cdots, N-1$ and $k = 1, 2, \cdots, \infty$, i.e., no malicious pulse can increase the length of the containing arc of legitimate oscillators.

Part II (The containing arc of legitimate oscillators resides in $[0, D)$ *when the first malicious pulse is sent)*:

Because oscillators will not respond to pulses when their phases resides in the refractory period, the first attack pulse does not affect the legitimate oscillators' phases, i.e., we have $\phi_i(T_1^+) = \phi_i(T_1)$ for $i = 1, 2, \cdots, N-1$.

Since all legitimate oscillators are labeled in an increasing order of their phases, i.e., $\phi_1(T_1) \leq \phi_2(T_1) \leq \cdots \leq \phi_{N-1}(T_1)$, the starting and ending points of the containing arc are ϕ_{N-1} and ϕ_1, respectively. Since $\Delta T_1 > D$ and $\phi_i(T_1) \geq 0$ hold for $i = 1, 2, \cdots, N-1$, we know that when receiving the second malicious pulse at time instant T_2, all legitimate oscillators' phases have already passed the phase D.

On the other hand, since ϕ_{N-1} is the starting point of the containing arc, it is not affected by the firing of all the other legitimate oscillators (when other legitimate oscillators fire, oscillator $N-1$ resides in the refractory period since the length of the containing arc is less than δ_1 which is less than D). Therefore, at time instant T_2, the phase of oscillator $N-1$ is determined by ΔT_1 and $\phi_{N-1}(T_1)$. If $\Delta T_1 + \phi_{N-1}(T_1) \leq 2\pi$ is true, we have $\phi_{N-1}(T_2) = \phi_{N-1}(T_1) + \Delta T_1 \leq 2\pi$, which means that all legitimate oscillators reside in the set $[D, 2\pi]$ at time instant T_2. On the other hand, if $\Delta T_1 + \phi_{N-1}(T_1) > 2\pi$ is true, we have $\phi_{N-1}(T_2) = \phi_{N-1}(T_1) + \Delta T_1 - 2\pi$. Since $\Delta T_1 \in [T_L, T_U]$ and $\phi_{N-1}(T_1) \in [0, D)$ hold, one can get that the upper bound of $\phi_{N-1}(T_2)$ is less than D in this situation, which means that all legitimate oscillators may reside in the set $[0, D)$, or partially in $[D, 2\pi]$ and partially in $[0, D)$ but with phase D not in the interior or on the starting point of the containing arc of legitimate oscillators.

Furthermore, according to Theorem 2.2, the first malicious pulse cannot increase the length of the containing arc and we have $\delta(T_2) \leq \delta(T_1) \leq \delta_1$. Therefore, at time instant T_2, the phases of legitimate oscillators still satisfy the phase distribution conditions in condition 1) of Theorem 2.3.

Part III (The containing arc resides partially in $[0, D)$ *and partially in* $[D, 2\pi]$ *but phase D does not belong to the containing arc when the first malicious pulse is sent)*:

Without loss of generality, we assume $\phi_1(T_1), \phi_2(T_1), \cdots, \phi_j(T_1)$ reside in $[0, D)$ and $\phi_{j+1}(T_1)$, $\phi_{j+2}(T_1)$, $\cdots$, $\phi_{N-1}(T_1)$ reside in $[D, 2\pi]$. Because phase D does not belong to the interior or on the starting point of the containing arc, we have $\delta(T_1) = 2\pi - (\phi_{j+1}(T_1) - \phi_j(T_1))$ and $\delta(T_1) \leq \delta_1$.

After receiving the first malicious pulse at time instant T_1, we have $\phi_i(T_1^+) = \phi_i(T_1)$ for $i = 1, 2, \cdots, j$ and $\phi_i(T_1^+) = 2\pi - (1-l)(2\pi - \phi_i(T_1))$ for $i = j+1, j+2, \cdots, N-1$. At time instant T_1^+, ϕ_{N-1} is the largest and will reach 2π freely after time $\Delta t_1 = (1-l)(2\pi - \phi_{N-1}(T_1))$. Denoting $t_1 = T_1 + \Delta t_1$, we have $\phi_i(t_1) = 2\pi - (1-l)(\phi_{N-1}(T_1) - \phi_i(T_1))$ for $i = j+1, j+2, \cdots, N-1$ and $\phi_i(t_1) = \phi_i(T_1) + \Delta t_1$ for $i = 1, 2, \cdots, j$.

Then oscillator $N-1$ emits a pulse and resets its phase to 0 at time instant t_1^+. At this time instant, its pulse will trigger the phase shift of legitimate oscillators whose phases reside in the set $[D, 2\pi]$, which leads to $\phi_i(t_1^+) = 2\pi - (1-l)^2(\phi_{N-1}(T_1) - \phi_i(T_1))$ for $i = j+1, j+2, \cdots, N-2$.

Similar to the analysis in Part 1), we can acquire the time between the firing events of oscillators $i+1$ and i for $i = j+1, j+2, \cdots, N-2$ as $\Delta t_{N-i} = (1-l)^{N-i}(\phi_{i+1}(T_1) - \phi_i(T_1))$.

At time instant t_{N-j-1}, oscillator $j+1$ reaches 2π for the first time. It emits a pulse and resets its phase to 0, i.e, $\phi_{j+1}(t_{N-j-1}^+) = 0$. The phase of all the other legitimate oscillators become $\phi_i(t_{N-j-1}^+) = \phi_i(T_1) + \sum_{k=1}^{N-j-1} \Delta t_k$ for $i = 1, 2, \cdots, j$ and $\phi_i(t_{N-j-1}^+) = \sum_{k=N-i+1}^{N-j-1} \Delta t_k$ for $i = j+2, j+3 \cdots, N-1$. At this time instant, oscillator j has the largest phase and oscillator $j+1$ has the smallest phase.

Denoting Γ_2 as the total time it takes for all legitimate oscillators residing in the set $[D, 2\pi]$ to fire once, we have

$$\Gamma_2 = \sum_{i=1}^{N-j-1} \Delta t_i = (1-l)(2\pi - \phi_{N-1}(T_1)) + \sum_{i=j+1}^{N-2} (1-l)^{N-i}(\phi_{i+1}(T_1) - \phi_i(T_1)) \tag{D.6}$$

Because $\Delta T_1 > D \geq 2\pi - D$ and $\Gamma_2 \leq 2\pi - D$ hold, the second malicious pulse will be emitted after time $\Delta T_1 - \Gamma_2$. Letting $\Gamma_2' = \Delta T_1 - \Gamma_2$, we proceed to examine the minimal value of Γ_2'. Since ΔT_1 and Γ_2 are independent of each other, the minimal value of Γ_2' is obtained when ΔT_1 is minimized and Γ_2 is maximized.

We first determine the maximal value of Γ_2. Denoting $\varepsilon = \sum_{i=j+1}^{N-2}((1-l) - (1-l)^{N-i})\varepsilon_i$ where $\varepsilon_i = \phi_{i+1}(T_1) - \phi_i(T_1)$ holds for $i = j+1, j+2, \cdots, N-2$ and substituting them into (D.6), one can get

$$\Gamma_2 = (1-l)(2\pi - \phi_{N-1}(T_1)) + \sum_{i=j+1}^{N-2} (1-l)^{N-i}\varepsilon_i = (1-l)(2\pi - \phi_{j+1}(T_1)) - \varepsilon \tag{D.7}$$

Γ_2 is maximized when $\phi_{j+1}(T_1)$ and ε are minimized. Because $\varepsilon_i \geq 0$ holds for $i = j+1, j+2, \cdots, N-2$, the minimal value of ε is 0 which is obtained when $\phi_{j+1} = \phi_{j+2} = \cdots = \phi_{N-1}$ is true. Next we proceed to check the minimal value of $\phi_{j+1}(T_1)$. Since $\phi_i(T_1) \in [D, 2\pi]$ for $i = j+1, j+2, \cdots, N-1$ and $\phi_i(T_1) \in [0, D)$ for $i = 1, 2, \cdots, j$ hold and the length of the containing arc at time instant T_1 is no larger than δ_1, the minimal value of $\phi_{j+1}(T_1)$ is $2\pi - \delta_1$. Hence, the maximal value of Γ_2 is $(1-l)\delta_1$.

Since ΔT_1 resides in the interval $[T_L, T_U]$, the minimal value of ΔT_1 is T_L which is given in (D.1). Therefore, the minimal value of Γ_2' can be obtained as follows

$$\Gamma_2' = T_L - \Gamma_2 = 2\pi - (2 - l - (1-l)^{N-1})\delta_1 \tag{D.8}$$

Combing (2.5) and (D.8) gives the minimal value of Γ_2':

$$\Gamma_2' = 2\pi - D - \frac{(2 - l - (1-l)^{N-1})l}{1-(1-l)^{N-1}}(2\pi - D) + D = \frac{(1-l)^2 - (1-l)^N}{1-(1-l)^{N-1}}(2\pi - D) + D \tag{D.9}$$

Since $N \geq 2$, we have $\Gamma_2' \geq D$, which means that at time instant t^+_{N-j-1} the second malicious pulse will be sent after at least a time interval of length D. Because oscillator $j+1$ has the smallest phase which is equal to 0 at time instant t^+_{N-j-1}, when the second malicious pulse is sent at time instant T_2, the phase of oscillator $j+1$ will be no less than D. Therefore, the phases of all legitimate oscillators will pass or be equal to phase D at time instant T_2.

On the other hand, oscillator j has the largest phase at time instant t^+_{N-j-1} and it is the starting point of the containing arc, hence the phase evolution of oscillator j is not affected by the firing of all the other legitimate oscillators. The phase of oscillator j can be formulated as follows:

1. If $\phi_j(t^+_{N-j-1}) + \Gamma_2' \leq 2\pi$ is true, we have $\phi_j(T_2) = \phi_j(t^+_{N-j-1}) + \Gamma_2' \leq 2\pi$, which means that at time instant T_2, all legitimate oscillators reside in the set $[D, 2\pi]$;

2. If$\phi_j(t^+_{N-j-1}) + \Gamma_2' > 2\pi$ is true, we have $\phi_j(T_2) = \phi_j(t^+_{N-j-1}) + \Gamma_2' - 2\pi$. Since $\phi_j(t^+_{N-j-1}) = \phi_j(T_1) + \Gamma_2$ and $\Gamma_2' = \Delta T_1 - \Gamma_2$ hold, we can get $\phi_j(T_2) = \phi_j(T_1) + \Delta T_1 - 2\pi$. Further noticing $\Delta T_1 \in [T_L, T_U]$ and $\phi_j(T_1) \in [0, D)$, we can get $\phi_j(T_2) < D$ at time instant T_2, which means that all legitimate oscillators' phases may reside in $[0, D)$, or partially in $[D, 2\pi]$ and partially in $[0, D)$ but with phase D not in the interior or on the starting point of the containing arc of legitimate oscillators.

In addition, according to Theorem 2.2, the first malicious pulse does not increase the length of the containing arc and we have $\delta(T_2) \leq \delta(T_1) \leq \delta_1$. Hence, at time instant T_2, the phases of legitimate oscillators still satisfy condition 1) in Theorem 2.3.

Summarizing the analysis on the three parts, we can conclude that when the first malicious pulse is sent at time instant T_1, if the length of the containing arc of all legitimate oscillators is no larger than δ_1 and the initial phase conditions are satisfied, then the length of the containing arc of all legitimate oscillators is still no larger than δ_1 when the second malicious pulse is sent at time instant T_2, and the phases will still

satisfy condition 1) of Theorem 2.3. Repeating the above argument, we can conclude that the length of the containing arc will not be increased by any of the malicious pulses sent at T_k for $k = 1, 2, \cdots, \infty$ and it is always less than δ_1. Further invoking Lemma 2.1 leads to the conclusion that all legitimate oscillators will synchronize because the interactions among legitimate oscillators will always decrease the length of the containing arc.

The proof of Theorem 2.3 under condition 2) can be obtained following the same line of reasoning and is omitted.

Bibliography

[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] 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.

[3] 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.

[4] 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.

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

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

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

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

[9] Y. Zong, X. W. Dai, Z. W. Gao, K. Busawon, and J. W. Zhu. Modelling and synchronization of pulse-coupled non-identical oscillators for wireless sensor networks. In *2018 IEEE 16th International Conference on Industrial Informatics (INDIN)*, pages 101–107. IEEE, 2018.

[10] S. Chandra, D. Hathcock, K. Crain, T. M. Antonsen, M. Girvan, and E. Ott. Modeling the network dynamics of pulse-coupled neurons. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 27(3):033102, 2017.

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

[12] 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.

[13] 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.

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

[15] 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.

[16] C. Canavier and S. Achuthan. Pulse coupled oscillators and the phase resetting curve. *Mathematical biosciences*, 226(2):77–96, 2010.

[17] 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.

[18] L. Ferrari, R. Gentz, A. Scaglione, and M. Parvania. The pulse coupled phasor measurement units. In *2014 IEEE International Conference on Smart Grid Communications*, pages 320–325. IEEE, 2014.

[19] Y. Zong, X. W. Dai, K. Busawon, Z. W. Gao, and R. Binns. Time synchronization of pulse-coupled oscillators for smart grids. In *2018 5th International Symposium on Environment-Friendly Energies and Applications (EFEA)*, pages 1–4. IEEE, 2018.

[20] H. Gao and Y. Q. Wang. Integrated communication and control for collective motion with limited communication. *IFAC-PapersOnLine*, 50(1):8826–8831, 2017.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] U. Ernst, K. Pawelzik, and T. Geisel. Synchronization induced by temporal delays in pulse-coupled oscillators. *Physical review letters*, 74(9):1570, 1995.

[32] P. Goel and B. Ermentrout. Synchrony, stability, and firing patterns in pulse-coupled oscillators. *Physica D: Nonlinear Phenomena*, 163(3-4):191–216, 2002.

[33] J. Nishimura and E. J. Friedman. Robust convergence in pulse-coupled oscillators with delays. *Physical Review Letters*, 106(19):194101, 2011.

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

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

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

[37] K. P. O'Keeffe, P. L. Krapivsky, and S. Strogatz. Synchronization as aggregation: Cluster kinetics of pulse-coupled oscillators. *Physical review letters*, 115(6):064101, 2015.

[38] J. Y. Wang, C. Xu, J. W. Feng, M. Chen, X. F. Wang, and Y. Zhao. Synchronization in moving pulse-coupled oscillator networks. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 62(10):2544–2554, 2015.

[39] J. Nishimura. Frequency adjustment and synchrony in networks of delayed pulse-coupled oscillators. *Physical Review E*, 91(1):012916, 2015.

[40] L. Ferrari, A. Scaglione, R. Gentz, and Y. W. Hong. Convergence results on pulse coupled oscillator protocols in locally connected networks. *IEEE/ACM Transactions on Networking*, 25(2):1004–1019, 2016.

[41] F. Ferrante and Y. Q. Wang. Robust almost global splay state stabilization of pulse coupled oscillators. *IEEE Transactions on Automatic Control*, 62(6):3083–3090, 2017.

[42] 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, 2017.

[43] B. Chen, J. R. Engelbrecht, and R. Mirollo. Cluster synchronization in networks of identical oscillators with α-function pulse coupling. *Physical Review E*, 95(2):022207, 2017.

[44] H. Lyu. Global synchronization of pulse-coupled oscillators on trees. *SIAM Journal on Applied Dynamical Systems*, 17(2):1521–1559, 2018.

[45] H. Gao and Y. Q. Wang. On the global synchronization of pulse-coupled oscillators interacting on chain and directed tree graphs. *Automatica*, 104:196–206, 2019.

[46] T. Anglea and Y. Q. Wang. Pulse-coupled synchronization with guaranteed clock continuity. *IEEE Transactions on Signal Processing*, 67(6):1596–1609, 2019.

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

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

[49] 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.

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

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

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

[53] 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.

[54] P. Khanchandani and C. Lenzen. Self-stabilizing byzantine clock synchronization with optimal precision. In *International Symposium on Stabilization, Safety, and Security of Distributed Systems*, pages 213–230. Springer, 2016.

[55] S. Dolev and J. L. Welch. Self-stabilizing clock synchronization in the presence of byzantine faults. *Journal of the ACM (JACM)*, 51(5):780–799, 2004.

[56] A. Daliot, D. Dolev, and H. Parnas. Linear time byzantine self-stabilizing clock synchronization. In *International Conference On Principles Of Distributed Systems*, pages 7–19. Springer, 2003.

[57] M. Ben-Or, D. Dolev, and E. N. Hoch. Fast self-stabilizing byzantine tolerant digital clock synchronization. In *Proceedings of the twenty-seventh ACM symposium on Principles of distributed computing*, pages 385–394. ACM, 2008.

[58] A. Daliot, D. Dolev, and H. Parnas. Self-stabilizing pulse synchronization inspired by biological pacemaker networks. In *Symposium on Self-Stabilizing Systems*, pages 32–48. Springer, 2003.

[59] D. Dolev and E. N. Hoch. Byzantine self-stabilizing pulse in a bounded-delay model. In *Symposium on Self-Stabilizing Systems*, pages 234–252. Springer, 2007.

[60] H. J. LeBlanc and X. Koutsoukos. Resilient first-order consensus and weakly stable, higher order synchronization of continuous-time networked multi-agent systems. *IEEE Transactions on Control of Network Systems*, 2017.

[61] Y. Abdallah, Z. Z. Zheng, N. B. Shroff, H. E. Gamal, and T. El-Fouly. The impact of stealthy attacks on smart grid performance: Tradeoffs and implications. *IEEE Transactions on Control of Network Systems*, 2016.

[62] B. Ojetunde, N. Shibata, and J. T. Gao. Securing link state routing for wireless networks against byzantine attacks: A monitoring approach. In *2017 IEEE 41st Annual Computer Software and Applications Conference*, volume 1, pages 596–601. IEEE, 2017.

[63] C. C. Zhao, J. P. He, and J. M. Chen. Resilient consensus with mobile detectors against malicious attacks. *IEEE Transactions on Signal and Information Processing over Networks*, 2017.

[64] A. Tyrrell, G. Auer, C. Bettstetter, and R. Naripella. How does a faulty node disturb decentralized slot synchronization over wireless networks? In *2010 IEEE International Conference on Communications*, pages 1–5, 2010.

[65] Z. Q. Wang and Y. Q. Wang. Attack-resilient pulse-coupled synchronization. *IEEE Transactions on Control of Network Systems*, 6(1):338–351, 2018.

[66] Z. Q. Wang and Y. Q. Wang. Pulse-coupled oscillators resilient to stealthy attacks. *IEEE Transactions on Signal Processing*, 66(12):3086–3099, 2018.

[67] Z. Q. Wang and Y. Q. Wang. An attack-resilient pulse-based synchronization strategy for general connected topologies. *IEEE Transactions on Automatic Control*, 2020.

[68] Z. Q. Wang and Y. Q. Wang. Global synchronization of pulse-coupled oscillator networks under byzantine attacks. *IEEE Transactions on Signal Processing*, 2020.

[69] 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.

[70] Y. Zong, X. W. Dai, Z. W. Gao, K. Busawon, R. Binns, and I. Elliott. Synchronization of pulse-coupled oscillators for ieee 802.15. 4 multi-hop wireless sensor networks. In *2018 IEEE Global Communications Conference (GLOBECOM)*, pages 1–7. IEEE, 2018.