Verification of k-Step and Definite Critical Observability in Discrete-Event Systems

Yin Tong, *Member, IEEE*, Ziyue Ma, *Member, IEEE*

Abstract

In this paper, we study the verification of critical observability in discrete-event systems in which a plant and its observer are connected via an unreliable communication channel. We consider a communication protocol in which each packet sent from the plant consists of an event and the sequence number of the packet. We define two novel notions of critical observability called (i) the *k-step critical observability* that requires that the critical states can be distinguished from non-critical ones after a loss of consecutive k events, and (ii) the *definite critical observability* that is a generalization of k-step critical observability for all nonnegative integers k. Then a structure called *k-extended detector* is proposed. Necessary and sufficient conditions for k-step critical observability are derived, which can be verified with polynomial complexity. Moreover, we prove that the definite critical observability can be verified by checking the $(\frac{1}{2}(|Q|^2+|Q|))$-step critical observability, where Q is the set of states of a plant. For a plant that is not definitely critically observable, a polynomial algorithm has been proposed to obtain a maximal nonnegative integer k_{max} (if it exists) such that the plant is k_{max}-step critically observable.

Index Terms

Critical observability, state estimation, discrete-event systems, networked systems

Published as:

Y. Tong, and Z.Y. Ma, "Verification of k-Step and Definite Critical Observability in Discrete-Event Systems, IEEE Transactions on Automatic Control, 2022, doi: 10.1109/TAC.2022.3202983. Early Access: https://ieeexplore.ieee.org/document/9870531

Note:

There are a few errors in the above published version which has been corrected (marked in red) in this document. The corrections do not affect the validity of the method developed in this work. The authors thank Dr. Xuya Cong for noticing some of them.

This work was supported in part by the National Natural Science Foundation of China under Grant No. 61803317, the Natural Science Foundation of Sichuan Province under Grant No. 2022NSFSC0955, the Natural Science Foundation of ShaanXi Province under Grant No. 2022JM-323, and the Fundamental Research Funds for the Central Universities under Grant No. JB210413. (Corresponding author: Yin Tong)

Y. Tong is with the School of Information Science and Technology, Southwest Jiaotong University, Chengdu 611756, China (e-mail: yintong@swjtu.edu.cn).

Z. Ma is with the School of Electro-Mechanical Engineering, Xidian University, Xi'an 710071, China (e-mail: maziyue@xidian.edu.cn).

I. INTRODUCTION

State estimation in partially observed discrete-event systems (DESs) has drawn much attention in recent years. The solutions to many important problems in the field of partially observed DES, such as opacity [1]–[3], diagnosability [4], [5], detectability [6], [7], and controller design [8], rely on the estimation of the current/historical state of a system. In this paper, we are interested in a state estimation problem called the *critical observability* problem. A system is *critically observable* if, given any observation from the system, we can always determine whether the plant is currently at a pre-defined set of *critical states* or not without ambiguity. Such a property is useful in practice where an administrator of a plant may expect to know if the plant has reached some states of physical importance.

The first work on critical observability was established by De Santis *et al.* [9] in hybrid systems and be used in the air traffic management. The approach in [9] is to design a hybrid state observer for reconstructing the hybrid state evolution of the system. Later, this method was extended to networks of finite state automata by Pola *et al.* [10] in which a decentralized architecture for critical observers is developed. Recently, Masopust [11] proves that the verification of critical observability is NL-complete in partially observed automata and is PSPACE-complete in networks of automata. Recently, Cong *et al.* [12] propose a method to verify the critical observability for labeled Petri nets using integer linear programming.

The aforementioned works all assume that the communication between the plant and the observing agent (called the *observer*) is fully reliable, i.e., all observations generated by the plant are correctly received by the observer without losses. However, in practice, the plant and its observer is usually linked by a cable/fiber or wireless channel in which case communication losses are unavoidable. In such a scenario, the connection between the plant and the observer may be temporarily lost. For example, a wireless connection between an auto-guided vehicle and a central controller may temporarily suffer from interference due to surrounding obstacles. Hence, it is necessary to study the critical observability in systems with such unreliable communication environment.

Many works on networked discrete-event systems (NDESs) have studied the state-estimation-related problems in systems with unreliable communication channels where event delays and losses may occur. In [13], it is assumed that a given subset of observable events is subject to intermittent losses, i.e., these observable events may become unobservable from time to time. It is proved that a model with intermittent observation losses can be transformed into a conventional system without event losses such that diagnosability can be verified using conventional methods. The work of [14] studies the supervisory control problem in systems with permanent observation losses and delays of control decisions and observations. Later, in [15] an on-line supervisor is proposed for NDESs where control decisions may be delayed with an upper bound. The control decisions of the supervisor is made based on the estimation of the current state of the plant. State estimation in NDESs with multiple communication channels is studied in [16]. In such a case, observable events may be sent through different channels, where communication delays and losses may occur. As a result, the order of the received observation may not be consistent with the order of the corresponding observable events occurrences. In [17], state estimation problem in systems with intermittent and permanent observation losses is studied. In particular, it is assumed that some observable events will become

permanently unobservable after a finite number of their occurrences.

The works [13]–[17] consider networked systems with a communication protocol such that each transmitted data packet contains only a single observable event of the plant. However, we notice that such a model maybe over-simplified in practice. In fact, to enhance the ability of error correction and detection, many practical communication protocols transfer data packets with a sequence number of it. With the sequence numbers, it is possible to correct the order of events occurrences under delays, or to know how many packets are lost during communication failures. Many widely used Cell Relay Protocols use fixed-length data packets with sequence numbers, for instance, the Asynchronous Transfer Mode ANSI standard protocol [18]. As far as we know, there has been no study on networked DESs with such type of protocols. Moreover, in the literature it is usually assumed that some channels or transitions are vulnerable to disturbances to a certain extent (e.g., delay with bound, intermittent loss, or permanently loss; see [13], [16], [17]). However, in practice the designer of a system possibly does not know a priori about which events may be affected or about when delays/losses occur. Instead, it is more common that the communication between the plant and the observer may randomly and temporary fail due to environmental interferences or the instability of the devices, and all transmissions are lost during such a period of time. However, the works in the literatures cannot be applied to such cases.

By the motivation above, in this paper we study the critical observability in NDESs with a new communication protocol where each data packet consists of an observable event and a sequence number of the packet. The communication failure we consider is that the channel may be temporarily unavailable such that all transmitted data packets during this period are lost. We propose two novel notions of critical observability called the k-step critical observability and the definite critical observability. A plant is k-step critically observable if, after a loss of k consecutive events in a communication failure, the observer can infer whether the plant is in the critical set or not after receiving a sufficient number of events and hereafter. On the other hand, a plant is *definitely critically observable* if it is k-step critically observable for any value of k, i.e., the observer can bear a loss of any number of consecutive events in a communication failure. The main contributions of this work are summarized as follows:

- We consider a new communication protocol where the sequence number of observable events is included. Such a protocol is widely used in networked systems (Cell-Relay, Asynchronous Transfer Mode, etc.) but has not been considered in the existing NDES works as far as we know.
- The notions of k-step critical observability (k-CO) and definite critical observability (def-CO) are first formalized in DESs with such communication protocol. Their properties are studied.
- A structure called *k-extended detector* is proposed to verify k-CO. Necessary and sufficient conditions for k-CO are derived. The complexity of our approach to verify k-CO and def-CO is polynomial in the number of plant states.
- Finally, we prove that the definite critical observability can be verified by checking the $(\frac{1}{2}(|Q|^2+|Q|))$-CO. For a plant that is not definitely critically observable, a polynomial algorithm is proposed to obtain a maximal nonnegative integer $k_{\max}$ (if it exists) such that the plant is $k_{\max}$-CO.

II. PRELIMINARY

A *finite state automaton* is a four-tuple $G = (Q, \Sigma, \delta, q_0)$, where Q is a set of *states*; Σ is a set of *events*; $\delta : Q \times \Sigma \to Q$ is the partial transition function; and $q_0 \in Q$ is the initial state. We also denote by $G = (Q, \Sigma, \delta, Q_0)$ for G that has multiple initial states in set $Q_0 \subseteq Q$.

We use Σ^* to denote the *Kleene closure* of Σ, consisting of all finite sequences composed by the events in Σ (including the *empty sequence* ε). Given a sequence $s \in \Sigma^*$, $|s|$ denotes the *length* of s. The transition function δ is extended to $\delta : Q \times \Sigma^* \to Q$ by recursively defining $\delta(q, \varepsilon) = q$ and $\delta(q, se) = \delta(\delta(q, s), e)$, where $s \in \Sigma^*$ and $e \in \Sigma$. The *language generated* by G, denoted by $L(G)$, is defined as $L(G) = \{s \in \Sigma \mid \delta(q_0, s) \in Q\}$.

We use $\Gamma_G(q) = \{e \in \Sigma \mid \delta(q, e) \text{ is defined}\}$ to denote the set of events that are *enabled* at state $q \in Q$, and we use $\Gamma_G(s) = \Gamma_G(\delta(q_0, s))$ to denote the set of events that are *enabled* after sequence s.

Given an automaton $G = (Q, \Sigma, \delta, q_0)$, the *accessible part* of G, denoted as $Ac(G)$, is the automaton $G' = (Q', \Sigma, \delta', q_0)$ obtained from G by removing all unreachable states and their corresponding transitions. Precisely speaking, $Q' = \{q \in Q \mid (\exists s \in L(G))\delta(q_0, s) = q\}$, and δ' is the restriction of δ to $Q' \times \Sigma^* \to Q'$.

The event set of a plant $G = (Q, \Sigma, \delta, q_0)$ is partitioned into the set of observable events Σ_{o} and the set of unobservable events Σ_{uo}, i.e., $\Sigma = \Sigma_{\text{o}} \cup \Sigma_{\text{uo}}$. Given a sequence $s \in \Sigma^*$, the natural projection $P : \Sigma^* \to \Sigma_{\text{o}}^*$ is defined as: (i) $P(\varepsilon) = \varepsilon$; (ii) $P(e) = e$ if $e \in \Sigma_{\text{o}}$ and $P(e) = \varepsilon$ otherwise; (iii) $P(se) = P(s)P(e)$.

We use $L_{\text{o}}(G)$ to denote the observed language of G, i.e., $L_{\text{o}}(G) = P[L(G)] = \{P(s) \mid s \in L(G)\}$. Given an observation $w \in L_{\text{o}}(G)$, the set of reachable states consistent with w is denoted as

$$C(w) = \{q \in Q \mid (\exists s \in L(G))P(s) = w \text{ and } \delta(q_0, s) = q\}.$$

The unobservable reach of a state $q \in Q$ is

$$UR(q) = \{q' \in Q \mid (\exists s \in \Sigma_{\text{uo}}^*)\ \delta(q, s) = q'\},$$

i.e., $UR(q)$ is the set of states reachable from state q via sequences consisting of unobservable events only.

III. CRITICAL OBSERVABILITY IN DESS WITH UNRELIABLE CHANNELS

In practice, an administrator of a plant may expect to know if the plant has reached some states of physical importance, which are formally defined as the *critical states* whose set is denoted as Q_{c}. The conventional notion of critical observability requires that, given any observation from the system, one can always determine whether the plant is currently at some critical states or not without ambiguity.

Definition 1: [10][Critical Observability] Given a plant $G = (Q, \Sigma, \delta, q_0)$ with $\Sigma = \Sigma_{\text{o}} \cup \Sigma_{\text{uo}}$ and a set of critical states $Q_{\text{c}} \subseteq Q$, G is *critically observable* (with respect to Q_{c}) if for all $w \in L_{\text{o}}(G)$, $C(w) \subseteq Q_{\text{c}} \vee C(w) \subseteq Q \setminus Q_{\text{c}}$ holds. ◇

Example 1: Consider the plant G in Figure 1 (a) that models the ground of a smart vehicle (SV) in a logistics warehouse. States q_i represents that the state of the SV being in zone i (with $i = 0, 1, 2, 3$). Zone 3 is the place where the SV unloads. This ground is equipped with a series of sensors to detect the passage of the SV from

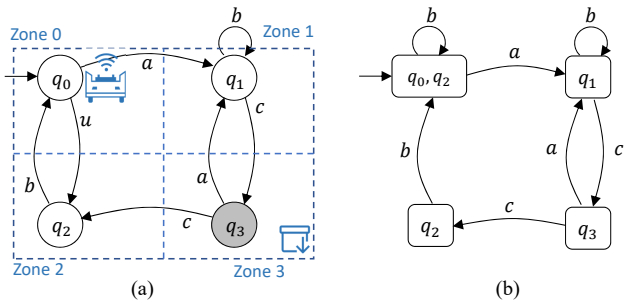

Fig. 1: The plant (a) and its observer (b).

one zone to another, which are modeled as $\Sigma_{\rm o} = \{a, b, c\}$. However, the movement from zone 0 to zone 2 cannot be detected. Therefore, $\Sigma_{\rm uo} = \{u\}$. Assume that the set of critical state is $Q_{\rm c} = \{q_3\}$ (in grey). Since in the corresponding observer automaton in Figure 1 (b) each state is a subset of either $Q_{\rm c}$ or $Q \setminus Q_{\rm c}$, we can conclude that the plant is critically observable with respect to $Q_{\rm c} = \{q_3\}$. $\diamond$

A. Transmission Protocol with Sequence Numbers

In practice, a plant and its observer is usually connected via some channel on the mediate of cable/fiber or wireless. Hence, the communication may temporarily suffer from interference such as temporary noise and/or the instability of devices. In the works on networked DESs, a simple transmission protocol is considered such that, whenever an observable event is executed in the plant, a data packet that contains only the event is sent. However, in practice sequence numbers usually are included in the packet to improve the capability of error correction and detection. Such a type of communication protocols has been widely applied to many *cell relay protocols*, including the *Asynchronous Transfer Mode* ANSI standard protocol [18], where fixed-length data packets with sequence numbers are transmitted. In this paper, we consider that each data packet is composed by an event and the sequence number of the packet. We use the following example to illustrate this.

Example 2: Consider again the plant G in Figure 1 (a) but with an unreliable communication channel between the observer and the SV. Initially, the trajectory of the SV is $q_0 \xrightarrow{u} q_2 \xrightarrow{b} q_0 \xrightarrow{a} q_1 \xrightarrow{b} q_1$. The observer receives a series of packets $(b,1)-(a,2)-(b,3)$, from which it can reconstruct the event sequence $s = bab$. The corresponding set of consistent states with s, which can be read from the observer automaton, is $C(bab) = \{q_1\}$, i.e., the observer can infer that the SV is at location q_1.

Suppose that the communication encounters some disturbance and becomes unavailable after the third packet "$(b,3)$" is received. During the failure of the communication, the SV runs $q_1 \xrightarrow{b} q_1 \xrightarrow{c} q_3$. From the SV's side, the SV sends packets $(b,4)$ and $(c,5)$ normally. However, these two packets are permanently lost so that the observer does not receive any packet from the plant.

Finally, the disturbance is resolved and the connection is reestablished. The SV runs $q_3 \xrightarrow{c} q_2 \xrightarrow{b} q_0$ next and sends $(c,6)$ and $(b,7)$ accordingly. The observer receives the two packages. As a result, the observer can reconstruct

a sequence "$b-a-b-\mathrm{x}-\mathrm{x}-c-b$" of events sent from the plant, where each "x" denotes a sent but unreceived event. $\diamond$

Remark 1: The sequence number in the data packet considered in this paper is different from *time stamps* used in time-automata (in which a packet is (e,τ) where $\tau \in \mathbb{R}$ is the time stamp). First, the sequence number is a counter used to keep track of every packet sent outward by the plant, which does not carry temporal information. Secondly, with the sequence number, the observer can recognize how many packets are lost when reconstructing the sequence. For instance, in Example 2 by receiving $(b,1)-(a,2)-(b,3)-(c,6)-(b,7)$ the observer knows that two packets with sequence numbers 4 and 5 are lost. However, when the time stamp is used, the observer may erroneously conclude that the packet carrying event c is the fourth packet, i.e., it may not realize that two events are missing between b and c. $\diamond$

Now we summarize the main set-ups used in this paper:

- The protocol for data transmission from the plant and the observer is that each data packet is a pair (e,n) where $e \in \Sigma_{\mathrm{o}}$ is a plant event and n is the sequence number of the packet, i.e., packet (e,n) is the n-th one sent so far.
- When the connection is normal, any packet sent by the plant is received by the observer with no delay.
- When the connection fails, any packet sent by the plant is permanently lost.

Besides, to simplify the presentation, we make the following two assumptions.

- **A1**: The plant is critically observable (see Definition 1) when there is no communication loss.

If a plant is not critically observable when there is no communication loss, it is not critically observable either when communication losses exist. Therefore, to have the problem meaningful, Assumption A1 is made.

- **A2**: During the running of the system, the communication may fail only once.

We point out that Assumption A2 is purely technical, which does not reduce the applicability of our method. In fact, our method can be easily extended to systems in which the communication may fail more than once, which will be explained in Section V-C.

B. k-Step and Definite Critical Observability

The conventional notion of critical observability [9] requires that *at any moment* the observer must be able to determine if the plant is at a critical state or not. However, such a notion may be too strict and in general not satisfiable in systems with communication failures considered in this paper. In fact, if the communication fails when the plant is currently at the edge of the non-critical set (i.e., it is at a non-critical state and is about to enter a critical one), obviously an observer can not tell if the plant is currently at a critical state or not. Under the data transmission protocol that each data packet is a pair (e,n) of observable event and a sequence number, the observer is able to determine whether there are communication losses and, if so, how many consecutive observable events are lost by checking the sequence numbers. This extra information may enable the observer to understand whether the plant is currently at a critical state or not. By such motivations, we define two new notions called the (k,l)-*critical observability* and the *definite critical observability* for systems with communication failures.

Definition 2 (k-Step Critical Observability): Given a plant $G = (Q, \Sigma, \delta, q_0)$ with $\Sigma = \Sigma_{\text{o}} \cup \Sigma_{\text{uo}}$, a set of critical states $Q_{\text{c}} \subseteq Q$, and two nonnegative integers $k, l \in \mathbb{N}$, G is called (k,l)-*critically observable* ((k,l)-CO for short[1]) (w.r.t Q_{c}) if for all sequence $s = uvw \in L(G)$ with $|P(v)| = k$ and $|P(w)| \geq l$, either of the following conditions holds

1) $(\forall v' \in \Sigma^*, |P(v')| = k)\ C(P(uv'w)) \subseteq Q_{\text{c}}$;
2) $(\forall v' \in \Sigma^*, |P(v')| = k)\ C(P(uv'w)) \subseteq Q \setminus Q_{\text{c}}$.

A plant is called k-*step critically observable* (k-CO) if there exists $l \in \mathbb{N}$ such that G is (k,l)-CO. $\diamond$

Condition 1) (resp., Condition 2)) implies that for any other string $uv'w$ that has the same prefix u and suffix w with s, if the substring v' has the same number of observable events with v and $C(P(s)) \subseteq Q_{\text{c}}$ (resp. $C(P(s)) \subseteq Q \setminus Q_{\text{c}}$), the set of states consistent with $P(uv'w)$ must also satisfy $P(uv'w) \subseteq Q_{\text{c}}$ (resp. $C(P(s)) \subseteq Q \setminus Q_{\text{c}}$).

Definition 3: Given a plant $G = (Q, \Sigma, \delta, q_0)$ with $\Sigma = \Sigma_{\text{o}} \cup \Sigma_{\text{uo}}$ and a set of critical states $Q_{\text{c}} \subseteq Q$, G is called *definitely critically observable* (def-CO) (w.r.t Q_{c}) if G is k-CO (w.r.t Q_{c}) for all $k \in \mathbb{N}$. $\diamond$

The physical interpretation of (k,l)-CO is the following. Whenever a temporary disturbance erases k consecutive events, the observer is always able to distinguish the critical states and the non-critical ones after receiving additional l events hereafter. Note that (k,l)-CO is more general than conventional critical observability since $(0,0)$-CO is equivalent to the latter.

Now we prove two properties of (k,l)-CO. First, we show that (k,l)-CO implies (k,l')-CO for any $l' > l$. We use $L_G(k,l)$ to denote the set of sequences in $L(G)$ which contains at least $k+l$ observable events, i.e.:

$$L_G(k,l) = \{s \in L(G) \mid |P(s)| \geq k + l\}.$$

Hence, Definition 2 can be equivalently rewritten as: G is (k,l)-CO if for all $s = uvw \in L_G(k,l)$ with $|P(v)| = k$ and $|P(w)| \geq l$, Condition 1) or 2) in Definition 2) holds.

Proposition 1: If a plant G is (k,l)-CO, then G is (k,l')-CO for any $l' > l$ (w.r.t the same Q_{c}).

Proof: Suppose that G is (k,l)-CO with respect to Q_{c}. Clearly, $L_G(k,l') \subseteq L_G(k,l)$ when $l' > l$. Since G is (k,l)-CO, $\forall s' = uvw' \in L(k,l') \subseteq L(k,l)$ with $|P(v)| = k$ and $|P(w')| \geq l'$, Condition 1) or 2) holds. Therefore, G is also (k,l')-CO. ■

By Proposition 1, given a plant G that is (k,l)-CO, we can find a minimal l_{min} such that G is (k, l_{min})-CO and for any $l < l_{\text{min}}$, G is not (k,l)-CO. On the other hand, the second property shows the monotonicity of (k,l)-CO on k, which is summarized in Proposition 2.

Proposition 2: If a plant G is k-CO, then G is k'-CO for any $k' < k$ (w.r.t the same Q_{c}).

Proof: Suppose that G is (k,l)-CO with respect to Q_{c}, i.e., for any $s = uvw \in L_G(k,l)$ with $|P(v)| = k$ and $|P(w)| \geq l$, Condition 1) or 2) holds. Let $k' \in \mathbb{N}$ be an integer smaller than k. Notice that $L_G(k,l) = L_G(k', l+(k-k'))$. Therefore, for any $s = uvw \in L_G(k', l+(k-k'))$ with $|P(v)| = k'$ and $|P(w)| \geq l+(k-k')$, Condition 1) or 2) holds, which implies that G is $(k', l+(k-k'))$-CO. ■

[1]The abbreviation "CO" is used as the abbreviation of both "critical observability" and "critically observable", depending on the context.

Intuitively speaking, given a plant G and a set of critical states, the fact that G is k-CO with a larger k implies a higher robustness of G against disturbances without compromising the critical observability. On the other hand, when k is fixed, G is (k,l)-CO with a small l implies that the critical observability can be quickly regained after the disturbance is resolved.

In the rest of this paper we aim to solve the following two problems.

- The first problem is to verify if G is k-CO for a given value of k. Moreover, if G is k-CO, we aim to determine the minimal $l_{\min} \in \mathbb{N}$ such that G is $(k, l_{\min})$-CO. This problem will be solved in Section V-A.
- The second problem is to verify if G is def-CO. We will prove in Section V-A that def-CO is equivalent to $(\frac{1}{2}(|Q|^2+|Q|))$-CO so that its verification can be done using the method of verification of k-CO. Notice that by Proposition 2, if G is 0-CO (which is guaranteed by Assumption A1) and not def-CO, there always exists an upper bound $k_{\max}$ for k-CO. In Section V-A we will also propose an iterative method to determine this upper bound $k_{\max}$.

IV. Construction of k-Extended Detectors

In this section, a structure, called *k-extended detector*, is proposed to verify k-step critical observability. Since the disturbance occurs only once, a run of a plant can be divided into three stages according to the status of the connection:

1) *Normal stage*. In this stage, the observer receives packets from the plant correctly.
2) *Failure stage*. In this stage the connection between the plant and the observer is lost. The plant may still be running, while all packets sent by the plant are lost. Note that the system may enter this stage at any moment when it is in the normal stage.
3) *Recover stage*. In this stage, the connection is reestablished, and the observer again receives packets from the plant normally.

A. The Normal Stage

We introduce the notion of *confusable states* to characterize the information of the observer for the first stage.

Definition 4: Given a plant $G = (Q, \Sigma, \delta, q_0)$ with $\Sigma = \Sigma_{\text{o}} \cup \Sigma_{\text{uo}}$, a pair of states $q', q'' \in Q$ are called *confusable* if there exist $s', s'' \in L(G)$ such that $P(s') = P(s'')$, $\delta(q_0, s') = q'$, and $\delta(q_0, s'') = q''$. The set of all pairs of confusable states is denoted as $\Omega(G)$. $\diamond$

Set $\Omega(G)$ consists of all pairs of states in G such that the observer may not distinguish based on the output of the system. Clearly, if $(q', q'') \in \Omega(G)$, $(q'', q') \in \Omega(G)$. Since the order of two confusable states does not matter to our problem, (q', q'') is defined as an unordered pair, i.e., (q', q'') and (q'', q') are equivalent.

Note that for the verification of k-CO, we do not need to keep the transitions in the detector at this stage. Given a pair $(q', q'') \subseteq Q$, we denote by $UR(q', q'')$ the set of pairs that can be reached from (q', q'') with the occurrence of one or more unobservable events. Precisely speaking,

$$UR(q', q'') = \{(\hat{q}', \hat{q}'') \mid \exists \hat{q}' \in UR(q'), \hat{q}'' \in UR(q'')\}. \tag{1}$$

Since $\forall q \in Q$, $\delta(q, \varepsilon) = q$, (q', q'') always belongs to $UR(q', q'')$. Note that $UR(q', q'')$ may contain multiple pairs of states. We also denote by $Next((q', q''), \sigma)$ the pair of states that can be reached from q', q'' immediately upon the occurrence of an observable event. Precisely speaking, given $\sigma \in \Sigma_{\text{o}}$ that is enabled at both q' and q'',

$$Next((q', q''), \sigma) = (\delta(q', \sigma), \delta(q'', \sigma)).$$

The set $\Omega(G)$ can be obtained by repeatedly doing the following procedure.

1) Initially let $\Omega(G) = \{(q_0, q_0)\}$;
2) For all $(q', q'') \in \Omega(G)$, let $\Omega(G) = \Omega(G) \cup UR(q', q'')$;
3) For all $(q', q'') \in \Omega(G)$ and $\sigma \in \Sigma_{\text{o}}$, let $\Omega(G) = \Omega(G) \cup \{Next((q', q''), \sigma)\}$;
4) Repeat steps 2 and 3 until no new pairs obtained in the two steps.

Example 3: As a running example, we still use the plant in Figure 1 (a) with $\Sigma_{\text{o}} = \{a, b, c\}$, $\Sigma_{\text{uo}} = \{u\}$, and $Q_{\text{c}} = \{q_3\}$. Let us consider 1-CO, i.e., $k = 1$ (note that the set of confusable pairs is independent on the value of k). Following the procedure above, the set of all confusable pairs are $\Omega(G) = \{(q_0, q_0), (q_0, q_2), (q_1, q_1), (q_2, q_2), (q_3, q_3)\}$ (as shown in Stage 1 in Figure 2). $\diamond$

B. The Failure Stage

Set $\Omega(G)$ consists of all confusable pairs before the communication fails. In the failure stage, the observer does not receive any packet from the plant. Hence, in this period of time, the observer does not update its estimation. When the failure stage is over, by receiving the first packet after the recovery of the connection, the observer immediately knows how many consecutive events are lost during the failure. Suppose that k observable events are lost during the failure stage. The observer can use this information to update its estimation on the plant states using the following notion called the *k-step reach*.

Definition 5: Given a plant $G = (Q, \Sigma, \delta, q_0)$, a state $q \in Q$, and an integer $k \in \mathbb{N}$, the *k-step reach* of q is:

$$R(q, k) = \{q' \in Q \mid (\exists s \in \Sigma^*)|P(s)| = k \text{ and } \delta(q, s) = q'\}. \quad \diamond$$

The physical interpretation of $R(q, k)$ is the set of states in G reachable from state q after the occurrence of k observable events. Note that, according to the definition, $R(q, k)$ may *not* be a subset of $R(q, k+1)$. The notion of k-step reach is extended to a pair of states.

Definition 6: Given a plant $G = (Q, \Sigma, \delta, q_0)$, a pair of states $(q', q'') \in Q \times Q$, and an integer $k \in \mathbb{N}$, the *k-step reach* of (q', q'') is defined as $R((q', q''), k) = \{(\hat{q}', \hat{q}'') \in Q \times Q | \hat{q}' \in R(q', k) \wedge \hat{q}'' \in R(q'', k)\}$. For a set of pairs S, we define

$$R(S, k) = \bigcup_{(q', q'') \in S} R((q', q''), k). \qquad \diamond$$

We propose Algorithm 1 that directly follows Definition 5 to compute $R(q, k)$ for given q and k. Set $R((q', q''), k)$ is obtained by choosing one element from $R(q', k)$ and one element from $R(q'', k)$, and hence it can be directly computed. Since the complexity of $R(q, k)$ is $\mathcal{O}(|Q|)$ due to $R(q, k) \subseteq Q$, the complexity of computing $R((q', q''), k)$ is $\mathcal{O}(|Q|^2)$.

Algorithm 1 Computing $R(q,k)$

Input: A plant $G=(Q,\Sigma,\delta,q_0)$ with $\Sigma=\Sigma_{\rm o}\cup\Sigma_{\rm uo}$, a state $q\in Q$, and an integer $k\in\mathbb{N}\setminus\{0\}$

Output: $R(q,k)$ the k-step reach of q

Let $Search_{new}=\{(q,0)\}$ and $R(q,k)=\emptyset$;
while $Search_{new}\neq\emptyset$, **do**
  Pop a (q',i) from $Search_{new}$;
  for all $\sigma\in\Sigma$, **do**
    if $\delta(q',\sigma)\in Q\wedge\sigma\in\Sigma_{\rm o}$, **then**
      Let $i=i+1$ and $y=(\delta(q',\sigma),i)$;
    else if $\delta(q',\sigma)\in Q\wedge\sigma\in\Sigma_{\rm uo}$, **then**
      Let $y=(\delta(q',\sigma),i)$;
    end if
    if $i<k\wedge y\notin Search_{new}$, **then**
      Let $Search_{new}=Search_{new}\cup\{y\}$;
    else if $i=k$, **then**
      Let $R(q,k)=R(q,k)\cup\{\delta(q',\sigma)\}$;
    end if
  end for
end while
Output $R(q,k)$.

Example 4 (Ex. 3 cont.): Let us consider a pair (q_1,q_1) in $\Omega(G)$. The 1-step reach of state q_1 is $R(q_1,1)=\{q_1,q_3\}$. Therefore, the 1-step reach of (q_1,q_1) is $R((q_1,q_1),1)=\{(q_1,q_1),(q_1,q_3),(q_3,q_3)\}$.

The set $R(\Omega(G),1)$ is the union of $R((q',q''),1)$ for all (q',q'') in $\Omega(G)$. The values of $R(q,1)$ for all $q\in Q$, and the values of $R((q',q''),1)$, for all $(q',q'')\in\Omega(G)$, are listed in Table I. The set $R(\Omega(G),1)$ consists of 8 pairs listed in Stage 2 of Figure 2. ◇

Here, set $R(\Omega(G),k)$ consists of all pairs of states such that the observer may not distinguish after k consecutive packets are lost (which is equivalent to the fact that k consecutive observable events are lost).

C. The Recover Stage

Finally, in the recover stage, the observer continues to receive observable events from the plant. Since $R(\Omega(G),k)$ contains all pairs of states the observer may be confused as soon as the communication recovers, if there exists an $l\in\mathbb{N}$ such that G is (k,l)-CO, then by observing l and more events the observer can always distinguish the two sets $Q_{\rm c}$ and $Q\setminus Q_{\rm c}$. Precisely speaking, we need to examine if there exists an $l\in\mathbb{N}$ such that for any pair (q',q'') in $R(\Omega(G),k)$, any sequences $s',s''\in\Sigma^*$ with $P(s')=P(s'')$ and $|P(s')|=|P(s'')|\geq l$ satisfy either of the

q	$R(q,1)$	(q',q'')	$R((q',q''),1)$
q_0	$\{q_0,q_1,q_2\}$	(q_0,q_0)	$\{(q_0,q_0),(q_0,q_1),(q_0,q_2),$ $(q_1,q_1),(q_1,q_2),(q_2,q_2)\}$
q_1	$\{q_1,q_3\}$	(q_1,q_1)	$\{(q_1,q_1),(q_1,q_3),(q_3,q_3)\}$
q_2	$\{q_0,q_2\}$	(q_2,q_2)	$\{(q_0,q_0),(q_0,q_2),(q_2,q_2)\}$
q_3	$\{q_1,q_2\}$	(q_3,q_3)	$\{(q_1,q_1),(q_1,q_2),(q_2,q_2)\}$
		(q_0,q_2)	$\{(q_0,q_0),(q_0,q_1),(q_0,q_2),$ $(q_1,q_2),(q_2,q_2)\}$

TABLE I: Values of $R(q_i,1)$ and $R((q',q''),1)$ in Example 5.

following conditions: (i) $\delta(q',s'),\delta(q'',s'')$ are both in $Q_{\rm c}$, (ii) $\delta(q',s'),\delta(q'',s'')$ are both in $Q\setminus Q_{\rm c}$, (iii) either $\delta(q',s')$ or $\delta(q'',s'')$ are not defined. Such a condition can be verified using the *extended detector* defined below which is an extension of the detector automaton.

Definition 7: Given a plant $G=(Q,\Sigma,\delta,q_0)$ with $\Sigma=\Sigma_{\rm o}\cup\Sigma_{\rm uo}$, a set of critical states $Q_{\rm c}$, and an integer $k\in\mathbb{N}$, the *k-extended detector* is an automaton $G_{{\rm d},k}=Ac(Q_{\rm d},\Sigma,\delta_{\rm d},Q_{{\rm d},0})$ such that:

- the state set is $Q_{\rm d}\subsetneq Q\times Q$;
- the event set is Σ;
- the transition function $\delta_{\rm d}:Q_{\rm d}\times\Sigma\to Q_{\rm d}$ is defined as:

$$\delta_{\rm d}((q',q''),\sigma)=\begin{cases}(\hat{q}',\hat{q}''), & \sigma\in\Sigma\cap\Gamma_G(q')\cap\Gamma_G(q''),\\ (\hat{q}',q''), & \sigma\in\Sigma_{\rm uo}\cap\Gamma_G(q'),\\ (q',\hat{q}''), & \sigma\in\Sigma_{\rm uo}\cap\Gamma_G(q''),\\ \text{Not defined}, & \text{Otherwise}\end{cases}$$

  where $\hat{q}'=\delta(q',\sigma)$ and $\hat{q}''=\delta(q'',\sigma)$.
- the initial state is $Q_{{\rm d},0}=R(\Omega(G),k)\setminus\Omega(G)$.
- $Ac(\cdot)$ denotes the operation of taking the accessible part of an automaton. ◇

In plain words, an extended detector $G_{d,k}$ can be viewed as a detector automaton with multiple initial states $R(\Omega(G),k)\setminus\Omega(G)$. Recall that G is critically observable in the conventional sense (Assumption A1), we do not need to examine the states in $R(\Omega(G),k)\cap\Omega(G)$, since for any pair (q',q'') in $R(\Omega(G),k)\cap\Omega(G)$ there does not exist any sequence $s',s''\in\Sigma^*$ such that $\delta(q',s')\in Q_{\rm c}$ and $\delta(q'',s'')\in Q\setminus Q_{\rm c}$, or vice versa. Therefore, the initial state is $Q_{{\rm d},0}=R(\Omega(G),k)\setminus\Omega(G)$. Note that, according to their definitions, sets $R(\Omega(G),k)$ and $\Omega(G)$ are in general incomparable, which implies that the extended detector is probably not a subautomaton of detector (see Example 5). Since the pairs of states in $Q_{\rm d}$ are unordered, $Q_{\rm d}$ is a strict subset of $Q\times Q$ and there are maximally $\frac{1}{2}(|Q|^2+|Q|)$ pairs in $Q_{\rm d}$.

Example 5 (Ex. 4 cont.): The procedures to compute $G_{d,1}$ are stepwise illustrated in Figure 2. In the normal and the failure stages, as done in Examples 3 and 4, $\Omega(G)$ and $R(\Omega(G),1)$ are computed which consists of 5 and 8

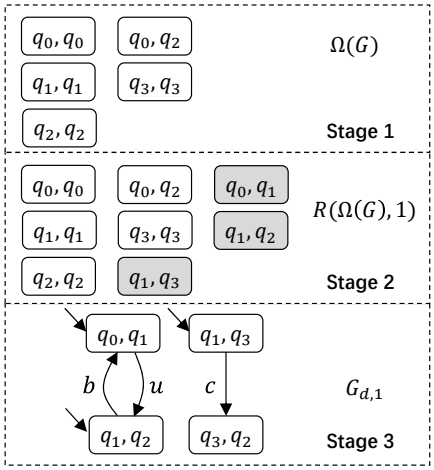

Fig. 2: Illustration of the three stages in Section IV.

pairs of states respectively. Therefore, the elements in $R(\Omega(G), 1) \setminus \Omega(G)$ (colored in grey in Stage 2 in Figure 2) are

$$R(\Omega(G), 1) \setminus \Omega(G) = \{(q_0, q_1), (q_1, q_2), (q_1, q_3)\}.$$

The corresponding extended detector $G_{d,1}$, which has all three pairs in $R(\Omega(G), 1) \setminus \Omega(G)$ as initial states, is depicted in Stage 3 in Figure 2. $\diamond$

V. Verification of k-Step Critical Observability

In this section, based on the k-extended detector, a necessary and sufficient conditions for k-step critical observability of a given plant G for a given $k \in \mathbb{N}$ is proposed. Moreover, if G is k-CO, a method of determining the minimal value of l such that G is (k, l)-CO is presented. Finally, a necessary and sufficient condition to def-CO is developed.

A. Verification of k-CO for a Given k

Definition 8: Given an automaton $G = (Q, \Sigma, \delta, Q_0)$ with $\Sigma = \Sigma_{\rm o} \cup \Sigma_{\rm uo}$, the *$l$-distant set* is defined as

$$D_l(G) = \{q \in Q \mid (\exists s \in L(G), \exists q_0 \in Q_0)|P(s)| \geq l \text{ and } \delta(q_0, s) = q\} \quad \diamond$$

In plain words, given an automaton G with a set of initial states Q_0, the *l-distant set* is the set of states that are reachable from an initial state by a sequence of events which contains at least l observable events. For given $k, l \in \mathbb{N}$, the following theorem shows that, in the extended detector $G_{{\rm d},k}$, if and only if all states (q', q'') that are l (or more) steps "away" from an initial state, satisfy that q', q'' are both in $Q_{\rm c}$ or both in $Q \setminus Q_{\rm c}$, then G is (k, l)-CO.

Theorem 1: Given a plant $G = (Q, \Sigma, \delta, q_0)$ with $\Sigma = \Sigma_{\rm o} \cup \Sigma_{\rm uo}$, a set of critical states $Q_{\rm c}$, and two integers $k, l \in \mathbb{N}$, G is (k,l)-CO w.r.t $Q_{\rm c}$ if and only if the following condition holds:

$$(\forall (q', q'') \in D_l(G_{{\rm d},k})) \quad q', q'' \in Q_{\rm c} \ \vee \ q', q'' \in Q \setminus Q_{\rm c}.$$

Proof: By the discussion in Sections IV-A and IV-B, as soon as the connection is recovered, all confusable pairs from the viewpoint of the observer is in $R(\Omega(G), k)$. Since the plant is assumed to be critically observable in the conventional sense, for all confusable pairs (q', q'') in $\Omega(G)$ there does not exist sequences $s', s'' \in L(G), P(s') = P(s'')$ such that $\delta(q', s') \in Q_{\rm c}$ and $\delta(q'', s'') \in Q \setminus Q_{\rm c}$. Hence, we only need to consider the confusable pairs in $R(\Omega(G), k) \setminus \Omega(G)$.

Let (q', q'') be an arbitrary pair in $R(\Omega(G), k) \setminus \Omega(G)$. By the definition of (k,l)-CO (in Definition 2), G is (k,l)-CO if and only if for any sequence $s', s'' \in L(G)$ such that $P(s') = P(s''), |P(s')| = |P(s'')| \geq l$, either $\delta(q', s'), \delta(q'', s'') \in Q_{\rm c}$ or $\delta(q', s'), \delta(q'', s'') \in Q \setminus Q_{\rm c}$. Hence, by Definition 8, G is (k,l)-CO if and only if all pairs $(\hat{q}', \hat{q}'')$ in $D_l(G_{{\rm d},k})$ satisfy either $\hat{q}', \hat{q}'' \in Q_{\rm c}$ or $\hat{q}', \hat{q}'' \in Q \setminus Q_{\rm c}$. ■

Theorem 1 provides a condition to verify (k,l)-CO for a given k and a given l. In the following, we prove that the minimal value of l that guarantees (k,l)-CO for a given k can be obtained by solving a *shortest path problem* in an underlying weighted digraph of the automaton.

Definition 9: Given an automaton $G = (Q, \Sigma, \delta, Q_0)$ with $\Sigma = \Sigma_{\rm o} \cup \Sigma_{\rm uo}$, we define $\mathcal{G} = (V, E)$ as the *underlying weighted digraph* of G where $V = Q$ and $E \subseteq Q \times \{0, -1\} \times Q$ are the set of nodes and edges, respectively. For each transition $\delta(q', \sigma) = q''$ in G, the weight of the corresponding arc from node q' to q'' in $\mathcal{G}$ is defined as: $\omega(q', q'', \sigma) = -1$ if $\sigma \in \Sigma_{\rm o}$ and $\omega(q', q'', \sigma) = 0$ otherwise. ◇

Given a path $q_0 \sigma_{i1} q_1 \dots q_{r-1} \sigma_{ir} q_r$ from q_0 to q_r, the sum $\sum_{j=1}^{r} \omega(q_{j-1}, q_j, \sigma_{ij})$ of the weights is called the *length* of the path. If the length of one path is smaller than that of another, we say the former path is *shorter*. Note that a shorter path may contain even more arcs and nodes, as they are measured by the sum of the weights on arcs.

Proposition 3: Given an automaton $G = (Q, \Sigma, \delta, Q_0)$ with $\Sigma = \Sigma_{\rm o} \cup \Sigma_{\rm uo}$, a state $q \in Q$ belongs to $D_l(G)$ if and only if $d(Q_0, q) \leq -l$, where $d(Q_0, q)$ is the length of the shortest path from q_0 to q for all $q_0 \in Q_0$ in $\mathcal{G}$.

Proof: (Only if) Suppose that $q \in D_l(G)$, which indicates that there exist $s \in L(G)$ and $q_0 \in Q_0$ such that $|P(s)| \geq l$ and $\delta(q_0, s) = q$. Hence, s corresponds to a path in $\mathcal{G}$ that passes at least l edges whose weights are -1. Therefore, the length of the shortest path from Q_0 to q is equal to or fewer than $-l$. The "If" part can be proved analogously. ■

Note that the shortest path from q to q' in $\mathcal{G}$ corresponds to the longest path in the diagraphs where the weight of arcs associated with observable events is 1. In the literature, the shortest path problem in weighted digraphs has been proven solvable in polynomial time (e.g., the Bellman-Ford algorithm [19], which can handle arcs with negative weights). Therefore, the weight of arcs corresponding to observable events is assigned as -1.

We have the following two results that can be used to verify k-CO for a given k and, when G is indeed k-CO, to determine the minimal integer $l_{\rm min}$ for $(k, l_{\rm min})$-CO. Note that since (q', q'') is an unordered pair, the condition "$q' \in Q_{\rm c}, q'' \in Q \setminus Q_{\rm c}$" in Theorem 2 and Corollary 1 means that "one state belongs to $Q_{\rm c}$ while the other state

does not". It does not specify the first state or the second state.

Theorem 2: Given a plant $G = (Q, \Sigma, \delta, q_0)$ with $\Sigma = \Sigma_o \cup \Sigma_{uo}$, a set of critical states Q_c, and an integer $k \in \mathbb{N}$, G is k-CO with respect to Q_c if and only if $G_{d,k} = (Q_d, \Sigma, \delta_d, Q_{d,0})$ satisfies the following condition:

$$(\forall (q', q'') \in Q_d : q' \in Q_c, q'' \notin Q_c)\ d(Q_{d,0}, (q', q'')) > -\infty.$$

Corollary 1: Given a plant $G = (Q, \Sigma, \delta, q_0)$ with $\Sigma = \Sigma_o \cup \Sigma_{uo}$, a set of critical states Q_c, and an integer $k \in \mathbb{N}$, if G is k-CO, there exists an integer $l_{min} \in \mathbb{N}$ such that:

1) G is (k, l_{min})-CO where

$$l_{min} = -\min\{d(Q_{d,0}, (q', q'')), \\ \forall (q', q'') \in Q_d \text{ with } q' \in Q_c, q'' \notin Q_c\} + 1;$$

2) G is not (k, l)-CO for any $l < l_{min}$.

Proof: Theorem 2 and Corollary 1 are straightforward from Theorem 1 and Proposition 3. ■

In plain words, given a fixed integer $k \in \mathbb{N}$: (i) the k-CO property of G can be necessarily and sufficiently verified by checking whether in the k-extended detector the distance from $Q_{d,0}$ to all confusable pairs (q', q'') with $q' \in Q_c, q'' \in Q \setminus Q_c$ are finite; (ii) if G is k-CO, the minimal integer $l_{min} \in \mathbb{N}$ that guarantees (k, l_{min})-CO equals to the absolute value of the length of the shortest path from $Q_{d,0}$ to a confusable pair (q', q'') with $q' \in Q_c, q'' \in Q \setminus Q_c$ in the k-extended detector. As a result, the verification of k-CO of a plant for a given k can be done by first computing the extended detector $G_{d,k}$ followed by solving a shortest path problem in the underlying digraph of it.

Example 6: Still consider the plant in Figure 1 (a) with $\Sigma_o = \{a, b, c\}$, $\Sigma_{uo} = \{u\}$, and $Q_c = \{q_3\}$. Its extended detector $G_{d,1}$ is shown in Figure 2 Stage 3. There are two pairs: (q_1, q_3) and (q_3, q_2) in $G_{d,1}$, satisfying that one state in Q_c while the other not. In the underlying graph, the length of the shortest path from $Q_{d,0}$ to each pair (q', q'') with $q' \in Q_c, q'' \notin Q_c$ is: (i) $d(Q_{d,0}, (q_1, q_3)) = 0$; (ii) $d(Q_{d,0}, (q_3, q_2) = -1$ (via $(q_1, q_3) \xrightarrow{c} (q_3, q_2)$ with weight -1). Since the minimal weight of such shortest paths is -1, we can conclude $l_{min} = 2$, i.e., G is $(1, 2)$-CO. ◇

In the end of this section we discuss the complexity of the proposed method. First, since the elements in Q_d, $\Omega(G)$ and $R(\Omega(G), k)$ are unordered pairs of states in Q, these sets contain at most $\frac{1}{2}(|Q|^2 + |Q|)$ elements. Thus, the complexity of constructing the k-extended detector $G_{d,k}$ is $\mathcal{O}(|Q|^2)$. Second, the conversion from $G_{d,k}$ to its weighted digraph $\mathcal{G}$ is of linear complexity $\mathcal{O}(|E|)$. After the conversion, there are maximally $2|V|^2$ arcs in the graph. Finally, solving a shortest path problem using the Bellman-Ford algorithm is proven to be $\mathcal{O}(|V||E|)$ [19], which is equivalent to $\mathcal{O}(|Q|^6)$. By the analysis above, the verification of k-CO of a plant for a given k can be done in complexity $\mathcal{O}(|Q|^6)$, i.e., polynomial in the number of states of the plant.

B. Verification of Definite Critical Observability

In this section we propose a method to verify def-CO which requires a plant to be k-CO for all k. We first present an upper bound of k in k-step critical observability. By the following theorem, we prove that for any

$k' > k \geq \frac{1}{2}(|Q|^2 + |Q|)$, k-CO and k'-CO are equivalent, which indicates that $\frac{1}{2}(|Q|^2 + |Q|)$ is an upper bound of k for k-CO.

Theorem 3: Given a plant $G = (Q, \Sigma, \delta, q_0)$ with $\Sigma = \Sigma_{\rm o} \cup \Sigma_{\rm uo}$, and a set of critical states $Q_{\rm c}$, for $k' > k \geq \frac{1}{2}(|Q|^2 + |Q|)$, plant G is k-CO w.r.t $Q_{\rm c}$ if and only if G is k'-CO w.r.t $Q_{\rm c}$.

Proof: By Proposition 2, the fact that G is k'-CO implies that G is k-CO. Therefore we only need to prove that G is k'-CO if G is k-CO. In the following, we prove that if G is n-CO, then G is $(n+1)$-CO, where $n \geq \frac{1}{2}(|Q|^2 + |Q|)$.

Suppose that G is n-CO. By Proposition 2, G is k-CO for all $k \in \{1, 2, \ldots, n-1, n\}$. By Theorem 2, for all extended detector $G_{{\rm d},k} = (Q_{\rm d}, \Sigma, \delta_{\rm d}, Q_{{\rm d},0})$ where $k \in \{1, 2, \ldots, n-1, n\}$, it holds: for all pairs $(q', q'') \in Q_{\rm d}$ such that $q' \in Q_{\rm c}, q'' \notin Q_{\rm c}$, $d(Q_{{\rm d},0}, (q', q'')) > -\infty$. Notice that $Q_{{\rm d},0} = R(\Omega(G), k) \setminus \Omega(G) \subsetneq Q \times Q$ for any $k \in \mathbb{N}$. By the definition of $G_{{\rm d},k}$, there are maximally $\frac{1}{2}(|Q|^2 + |Q|)$ states in $G_{{\rm d},k}$, and thus the length (without considering the weights) of the longest simple path[2] in $G_{{\rm d},k}$ is $\frac{1}{2}(|Q|^2 + |Q|)$. Suppose that $(\hat{q}', \hat{q}'') \in Q_{\rm d}$ is reachable from $(q', q'') \in Q_{\rm d}$ through a path with length $n+1 > \frac{1}{2}(|Q|^2 + |Q|)$. Clearly, a cycle is formed between (q', q'') and $(\hat{q}', \hat{q}'')$. Therefore, $(\hat{q}', \hat{q}'')$ is also reachable from (q', q'') through a path with length $n' < n+1$, where $n' = n - \frac{r}{2}(|Q|^2 + |Q|)$ and $r \in \mathbb{N}$, i.e., $R((q', q''), n+1) = R((q', q''), n')$. For the case that $R((q', q''), n+1) = \emptyset$, there exists $\frac{1}{2}(|Q|^2 + |Q|) < n' \leq n$ such that $R((q', q''), n') = \emptyset$. Therefore, for $n \geq \frac{1}{2}(|Q|^2 + |Q|)$, there necessarily exists $n' \in \{1, 2, \ldots, n-1, n\}$ such that $R(\Omega(G), n+1) = R(\Omega(G), n')$. Hence, the initial states of $G_{d,n+1}$ and $G_{d,n'}$ are identical, and $G_{d,n+1}$ is exactly same as $G_{d,n'}$, which indicates that in $G_{d,n+1}$, $d(Q_{{\rm d},0}, (q', q'')) > -\infty$ holds for all pairs (q', q'') where $q' \in Q_{\rm c}, q'' \notin Q_{\rm c}$. By Theorem 2, G is $(n+1)$-CO. ■

Corollary 2: Given a plant $G = (Q, \Sigma, \delta, q_0)$ with $\Sigma = \Sigma_{\rm o} \cup \Sigma_{\rm uo}$, and a set of critical states $Q_{\rm c}$, if and only if G is $(\frac{1}{2}(|Q|^2 + |Q|))$-CO with respect to $Q_{\rm c}$, then G is def-CO with respect to $Q_{\rm c}$.

Proof: (If) On one hand, Theorem 3 indicates that if G is $(\frac{1}{2}(|Q|^2 + |Q|))$-CO, then G is k-CO for any $k > \frac{1}{2}(|Q|^2 + |Q|)$. On the other hand, by Proposition 2, $(\frac{1}{2}(|Q|^2 + |Q|))$-CO implies k-CO for any $k < \frac{1}{2}(|Q|^2 + |Q|)$. Therefore, G is k-CO for any $k \in \mathbb{N}$. By Definition 3, G is def-CO.

(Only if) Suppose G is def-CO. By Definition 3, G is also $(\frac{1}{2}(|Q|^2 + |Q|))$-CO. ■

According to Corollary 2, whether a plant is def-CO or not can be verified by just checking the $(\frac{1}{2}(|Q|^2 + |Q|))$-CO. Therefore, as we have discussed in the previous section, the verification of def-CO can also be done in polynomial time.

On the other hand, when a plant G is not def-CO, by Proposition 2, there necessarily exists a maximal integer $k_{\rm max} \in \mathbb{N}$ such that G is $k_{\rm max}$-CO (and not k'-CO for any integer $k' > k_{\rm max}$). In some cases, one many be interested in determining the value of $k_{\rm max}$. This can be done by using Algorithm 2. Although the algorithm seems enumerating all i's starting from $i = 1$ in a brute-force way, the computational complexity of Algorithm 2 is still polynomial. In fact, if G is $(\frac{1}{2}(|Q|^2 + |Q|))$-CO (and hence is k-CO for any $k \in \mathbb{N}$), Algorithm 2 is of complexity $\mathcal{O}(|Q|^6)$, since only $(\frac{1}{2}(|Q|^2 + |Q|))$-extended detector is constructed). On the other hand, if G is k-CO for some maximal

[2]If no arcs appear more than once in a path, the path is called a simple path.

$0 < k < \frac{1}{2}(|Q|^2 + |Q|)$, the complexity of Algorithm 2 is $\mathcal{O}(k \cdot |Q|^6)$, i.e., the complexity is $\mathcal{O}(|Q|^8)$.

Algorithm 2 Determining Maximal k for k-CO

Input: A plant $G = (Q, \Sigma, \delta, q_0)$ with $\Sigma = \Sigma_{\rm o} \cup \Sigma_{\rm uo}$, a set of critical states $Q_{\rm c} \subseteq Q$

Output: A maximal k such that G is k-CO with respect to $Q_{\rm c}$, or "NA"

Compute n-extended detector $G_{d,n}$, where $n = \frac{1}{2}(|Q|^2 + |Q|)$.
Determine ℓ the length of the shortest path problem in the corresponding underlying digraph $\mathcal{G}$;
if $\ell > -\infty$, **then**
    output "def-CO" and exit;
end if
Let $k = 1$;
while true, **do**
    Compute k-extended detector $G_{{\rm d},k}$ and determine ℓ the length of the shortest path problem in the corresponding underlying digraph $\mathcal{G}$;
    if $\ell = -\infty$, **then**
        if $k = 1$, **then**
            output "NA";
        else
            output $k-1$, "$(k-1)$-CO" and exit;
        end if
    end if
    let $k = k + 1$;
end while

C. Relaxation of Assumption A2

In Section III, we have introduced a technical assumption (A2) such that the communication may fail only once during the running of the system. In this section, we discuss how to apply the proposed method recursively to the case where failures occur more than once. Suppose that a sequence $s = uv_1w_1v_2w_2\cdots v_mw_m \in L(G)$ occurs in G, and communication losses occur for all v_i $(i = 1, \ldots, m)$ substrings for m times, as illustrated in the Figure 3. In the figure, $|P(v_i)| = k_i$ and $|P(w_i)| = l_i$ for $i = 1, 2, \ldots, m$.

The construction of the extended detector is the following.

1) Normal Stage N: compute the set $\Omega(G)$ of all confusable state pairs.
2) Failure Stage F1: compute the k_1-step reach $R(\Omega(G), k_1)$ (by Definition 6) and $F_1 = R(\Omega(G), k_1) \setminus \Omega(G)$.
3) Recover Stage R1: construct the k_1-extended detector $G_{{\rm d},k_1}$ starting from initial state(s) F_1, and then compute the l_1-step reach of F_1 in $G_{{\rm d},k_1}$, denoted as $L_1 = R(F_1, l_1)$.

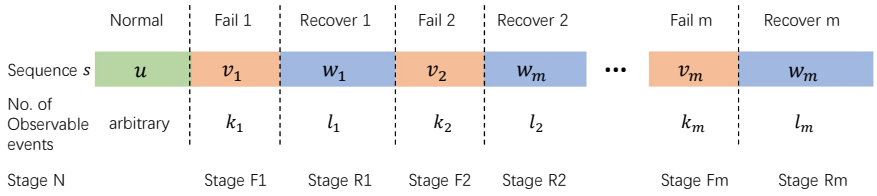

Fig. 3: Illustration of communication failure occurring m times.

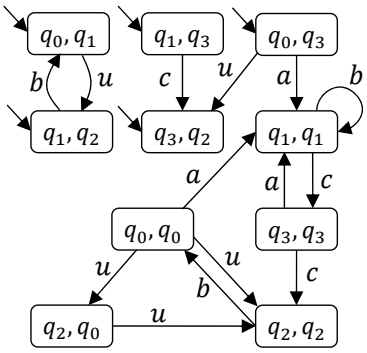

Fig. 4: The 2-extended detector in Example 7.

4) Failure Stage F2: compute the k_2-step reach $R(L_1, k_2)$ and $F_2 = R(L_1, k_2) \setminus \Omega(G)$.
5) Recover Stage R2: construct the k_2-extended detector G_{d,k_2} starting from initial state(s) F_2, and then compute the l_2-step reach of F_2 in G_{d,k_2}, denoted as $L_2 = R(F_2, l_2)$.
6) ...
7) Failure Stage Fm: compute the k_m-step reach $R(L_{m-1}, k_m)$ and $F_m = R(L_{m-1}, k_m) \setminus \Omega(G)$.
8) Recover Stage Rm: construct the k_m-extended detector G_{d,k_m} starting from initial state(s) F_m.

In brief, after constructing the set $\Omega(G)$ (Section IV.A) we iteratively compute the corresponding k_i-step reach (Section IV.B) and the l_i-step reach in the corresponding extended detector (Section IV.C) for m times, and check if the final extended detector $G_{\mathrm{d},km}$ satisfies the condition in Theorem 1.

Example 7: Let us take the plant in Figure 2 as an example and verify its critical observability with respect to $Q_{\mathrm{c}} = \{q_3\}$ when communication failures occur twice and $k_1 = 1$, $k_2 = 2$, $l_1 = 1$, l_2=4.

1) Normal Stage to Recover State R1: Based on the 1-extended detector $G_{\mathrm{d},1}$ in Figure 2, we compute $L_1 = R(Q_{\mathrm{d},0}, 1) = \{(q_0, q_1), (q_1, q_2), (q_3, q_2)\}$, i.e., after observing 1 observable event, the possible pairs of confusable states are all in L_1.
2) Failure Stage F2: compute $R(L_1, 2) = \{(q_0, q_1), (q_0, q_2), (q_0, q_3), (q_1, q_2), (q_2, q_2), (q_2, q_3), (q_1, q_3), (q_3, q_3), (q_1, q_1), (q_0, q_0)\}$, i.e., after losing 2 observable events, the set of possible current confusable state pairs. Then, we have $F_2 = R(L_1, 2) \setminus \Omega(G) = \{(q_0, q_1), (q_0, q_3), (q_1, q_2), (q_1, q_3), (q_2, q_3)\}$.
3) Recover Stage R2: construct the 2-extended detector $G_{\mathrm{d},2}$ (as shown in Figure 4 starting from F_2.

Since $D_4(G_{\mathrm{d},2}) = \{(q_0,q_0),(q_1,q_1),(q_2,q_2),(q_3,q_3),(q_0,q_1),(q_0,q_2),(q_1,q_2)\}$, by Theorem 1, the plant is critically observable. Indeed, after the two times of communication failure, the only possible confusable pairs of (different) states are (q_0,q_1), (q_0,q_2), and (q_1,q_2), and none of them is a critical state. $\diamond$

On the other hand, we also point out that, in practice the operator of a plant does not have the priori knowledge about the forthcoming disturbance, i.e., it does not know a priori the values of $k_1,\ldots,k_m$ and $l_1,\ldots,l_m$. Hence, if the communication channel may suffer from multiple unforeseen failures, it is more realistic to consider def-CO in such a case. If a plant is def-CO, then it is critically observable for all m, all $k_1,\ldots,k_m$ and $l_1,\ldots,l_m$. In summary, the (k,l)-CO and k-CO defined in Section III describes the robustness of a system against occasional single-time failure, and the def-CO describes the robustness against frequent multiple failures.

VI. Conclusion

In this paper, we have studied the problem of verifying k-step critical observability and definite critical observability in discrete-event systems in which a plant and its observer are linked via an unreliable communication channel. A structure, called k-extended detector, is proposed. A necessary and sufficient condition for k-step critical observability can be derived from the k-extended detector for a given k, and a method of polynomial complexity is proposed to verify the condition. It is shown that the definite critical observability can be verified by checking the $(\frac{1}{2}(|Q|^2+|Q|))$-critical observability. For a plant that is not definitely critically observable, a polynomial algorithm has been proposed to obtain the maximal value of k such that the plant is k-step critically observable.

References

[1] J. C. Basilio, C. N. Hadjicostis, and R. Su, "Analysis and control for resilience of discrete event systems: Fault diagnosis, opacity and cyber security," *Foundations and Trends in Systems and Control*, vol. 8, no. 4, pp. 285–443, 2021.

[2] Y. Tong, Z. Li, C. Seatzu, and A. Giua, "Verification of state-based opacity using Petri nets," *IEEE Transactions on Automatic Control*, vol. 62, no. 6, pp. 2823–2837, 2017.

[3] Z. Ma, X. Yin, and Z. Li, "Verification and enforcement of strong infinite-and k-step opacity using state recognizers," *Automatica*, vol. 133, p. 109838, 2021.

[4] X. Yin and Z. Li, "Decentralized fault prognosis of discrete-event systems using state-estimate-based protocols," *IEEE Transactions on Cybernetics*, vol. 49, pp. 1302–1313, 2019.

[5] S. Takai and T. Ushio, "Verification of codiagnosability for discrete event systems modeled by mealy automata with nondeterministic output functions," *IEEE Transactions on Automatic Control*, vol. 57, no. 3, pp. 798–804, 2012.

[6] H. Lan, Y. Tong, and C. Seatzu, "Analysis of strong and strong periodic detectability of bounded labeled Petri nets," *Nonlinear Analysis: Hybrid Systems*, vol. 42, p. 101087, 2021.

[7] L. Zhou, S. Shu, and F. Lin, "Detectability of discrete-event systems under nondeterministic observations," *IEEE Transactions on Automation Science and Engineering*, vol. 18, no. 3, pp. 1315–1327, 2021.

[8] X. Yin and S. Lafortune, "A uniform approach for synthesizing property-enforcing supervisors for partially-observed discrete-event systems," *IEEE Transactions on Automatic Control*, vol. 61, no. 8, pp. 2140–2154, 2016.

[9] E. De Santis, M. D. Di Benedetto, S. Di Gennaro, A. D'Innocenzo, and G. Pola, *Critical Observability of a Class of Hybrid Systems and Application to Air Traffic Management*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 141–170.

[10] G. Pola, E. De Santis, M. D. Di Benedetto, and D. Pezzuti, "Design of decentralized critical observers for networks of finite state machines: A formal method approach," *Automatica*, vol. 86, pp. 174–182, 2017.

[11] T. Masopust, "Critical observability for automata and Petri nets," *IEEE Transactions on Automatic Control*, vol. 65, no. 1, pp. 341–346, 2020.

[12] X. Cong, M. P. Fanti, A. M. Mangini, and Z. Li, "Critical observability of discrete-event systems in a Petri net framework," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 5, pp. 2789–2799, 2022.

[13] L. K. Carvalho, J. C. Basilio, and M. V. Moreira, "Robust diagnosis of discrete event systems against intermittent loss of observations," *Automatica*, vol. 48, no. 9, pp. 2068–2078, 2012.

[14] F. Lin, "Control of networked discrete event systems: Dealing with communication delays and losses," *SIAM Journal on Control and Optimization*, vol. 52, no. 2, pp. 1276–1298, 2014.

[15] Z. Liu, X. Yin, S. Shu, F. Lin, and S. Li, "Online supervisory control of networked discrete event systems with control delays," *IEEE Transactions on Automatic Control*, vol. 67, no. 5, pp. 2314–2329, 2022.

[16] F. Lin, W. Wang, L. Han, and B. Shen, "State estimation of multichannel networked discrete event systems," *IEEE Transactions on Control of Network Systems*, vol. 7, no. 1, pp. 53–63, 2020.

[17] Y. Tong, J. Luo, and C. Seatzu, "State estimation of discrete-event systems subject to intermittent and permanent loss of observations," in *the 60th IEEE Conference on Decision and Control (CDC)*, 2021, pp. 1048–1053.

[18] R. J. Vetter, "Asynchronous transfer mode: An emerging network standard for high-speed communications," in *Advances in Computers*. Elsevier, 1997, vol. 44, pp. 285–330.

[19] J. Bang-Jensen and G. Z. Gutin, *Digraphs: theory, algorithms and applications*. Springer Science & Business Media, 2008.