RESEARCH ARTICLE

The protection and recovery strategy development of dynamic resilience analysis and cost consideration in the infrastructure network

Yi-Zhu Su* and Wei-Chang Yeh

Department of Industrial Engineering and Engineering Management, National Tsing Hua University, Hsinchu 30013, Taiwan

*Corresponding author. E-mail: u102034007@gmail.com

Abstract

Modern life is becoming more and more convenient, all because of the perfect operation of the infrastructure network. However, if these infrastructure networks encounter interference, the operation of the network system will be delayed or even shut down, often causing huge losses in livelihood, economy, and society. Therefore, how to evaluate the resilience of the network system and provide protection and recovery strategies to deal with attacks that interfere with the system are important issues. This study considers a situation with protection, attack, and recovery strategies, proposes the time-related Binary-Addition Tree-based Resilience Assessment to consider more decision variables and parameters, and further includes the costs in the formulation of the protection and recovery strategies. Moreover, a new performance measure oriented to the degree of network reliability recovery to quantify the resilience of the network system is developed.

Keywords: network resilience; binary-state network; binary addition; network reliability; infrastructure network; disruptive events

List of symbols

- $n$: Numbers of nodes in a network
- $m$: Numbers of arcs in a network
- $V$: Node set $V$ in a network; $V = \{1, 2, \ldots, n\}$
- $E$: Arc set $E$ in a network; $E = \{a_1, a_2, \ldots, a_m\}$
- $e_{i,j}$: Directed arc from nodes $i$ to $j$
- $a_k$: $k$th directed arc in $E$
- $D$: Success probability of each arc in a binary-state network
- $G(V, E, D)$: A graph with the source node 1, the sink node $n$, $V$, $E$, and $D$. For example, Fig. 2 is a binary-state network $G(V, E, D)$.
- $b_0$: Time point for original network status
- $t_d$: Time point for disruption event completion
- $t_r$: Time point for recovery completion
- $N_p$: Number of protected arcs
- $N_a$: Number of attacked arcs
- $N_f$: Number of failed arcs
- $N_r$: Total number of recovered arcs
- $T_r$: Number of recovered arcs per unit time
- $P(a_k)$: Success probability of $a_k$ for the original network and the full recovery strategy
- $P'(a_k)$: Success probability of $a_k$ for the partial recovery strategy
- $C_r(a_k)$: Full recovery cost of $a_k$
- $C_r'(a_k)$: Partial recovery cost of $a_k$
- $C_p(a_k)$: Protect variable cost of $a_k$
- $C_p(N_p)$: Protect fixed cost of $N_p$
- $C_r(T_r)$: Recovery daily fixed cost of $T_r$
- $C_p$: Total protection costs

Received: 27 August 2021; Revised: 10 November 2021; Accepted: 21 November 2021

© The Author(s) 2022. Published by Oxford University Press on behalf of the Society for Computational Design and Engineering. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted reuse, distribution, and reproduction in any medium, provided the original work is properly cited.
1. Introduction

Many indispensable infrastructure systems in life are network structures, including power grids (González et al., 2016; Liu et al., 2016), water distribution systems (González et al., 2016; Hosseini & Barker, 2016; Monroe et al., 2016; Sharma et al., 2020), gas networks (González et al., 2016), wildfire warning networks (Hajian et al., 2016; Su & Yeh, 2020), telecommunication networks (Perera et al., 2015; Kabadurmus & Smith, 2017), and transportation networks (Avci & Ozbulut, 2018; Calvert & Snelder, 2018; Gomez & Baker, 2019; Hubbard & Hubbard, 2019; Markolf et al., 2019; Trotter & Ivory, 2019; Hsieh & Feng, 2020). The normal operation of these infrastructure systems is vital to the economic development and community interaction of the society (Hubbard & Hubbard, 2019). Their malfunction would cause huge losses, and the evidences are such as the impact of the fire on Lazienkowski Bridge, in Warsaw, which affected around 104 643 vehicles up to several months in 2015 (Szara & Hoy, 2019), and the Taiwan blackout caused by Xingda power plant shutdown accident in 2021, which affected approximately 10.10 million households and NT$470 million compensation from Taiwan Power Company (Wikipedia, 2021). Therefore, ensuring the reliable operation of such infrastructure has always been a topic of great concern (Perera et al., 2015; González et al., 2016; Hajian et al., 2016; Hosseini & Barker, 2016; Liu et al., 2016; Kabadurmus & Smith, 2017; Avci & Ozbulut, 2018; Calvert & Snelder, 2018; Monroe et al., 2018; Gomez & Baker, 2019; Hosseini & Ivanov, 2019; Hosseini et al., 2019; Hubbard & Hubbard, 2019; Markolf et al., 2019; Trotter & Ivory, 2019; Hsieh & Feng, 2020; Sharma et al., 2020; Poulin & Kane, 2021; Zhu et al., 2021).

These network systems may suffer damage from different disruptive events such as natural disasters (Liu et al., 2016; Markolf et al., 2019; Trotter & Ivory, 2019; Hsieh & Feng, 2020), human errors (Szarata & Hoy, 2019; Wikipedia, 2021), or they did not focus on both protection and recovery aspects (Youn et al., 2011; Pant et al., 2014; Zhang et al., 2015; Gonzalez et al., 2016; Hosseini & Barker, 2016; Hosseini et al., 2016a; Liu et al., 2016; Calvert & Snelder, 2018; Monroe et al., 2018; Rocchi et al., 2018; Gomez & Baker, 2019; Hosseini & Ivanov, 2019; Markolf et al., 2019; Trotter & Ivory, 2019; Hsieh & Feng, 2020; Jia & Zhang, 2020; Sharma et al., 2020; Smith et al., 2020; Su & Yeh, 2020; Xu et al., 2020; Poulin & Kane, 2021; Zhu et al., 2021). The detailed comparison of these studies is summarized in Table 1.

It can be seen from Table 1 that for the analysis of network systems suffering from disruptive events, these studies usually discuss and analyse from the protection aspect (Zhang et al., 2015; Hosseini & Barker, 2016; Hosseini et al., 2016b; Monroe et al., 2018; Hosseini & Ivanov, 2019), the recovery aspect (Pant et al., 2014; Gonzalez et al., 2016; Rocchi et al., 2018; Markolf et al., 2019; Trotter & Ivory, 2019; Hsieh & Feng, 2020; Jia & Zhang, 2020; Sharma et al., 2020; Smith et al., 2020; Su & Yeh, 2020; Xu et al., 2020), or both (Gomez & Baker, 2019; Zhu et al., 2021).

Most studies did not take cost into consideration when analysing network resilience (Rose, 2007; Pant et al., 2014; Hosseini & Barker, 2016; Hosseini et al., 2016b; Liu et al., 2016; Calvert & Snelder, 2018; Monroe et al., 2018; Hosseini & Ivanov, 2019; Markolf et al., 2019; Trotter & Ivory, 2019; Hsieh & Feng, 2020; Xu et al., 2020; Zhu et al., 2021), or they did not focus on both protection and recovery strategies (Youn et al., 2011; Pant et al., 2014; Zhang et al., 2015; Gonzalez et al., 2016; Hosseini & Barker, 2016; Hosseini et al., 2016b; Monroe et al., 2018; Rocchi et al., 2018; Hsieh & Feng, 2020; Jia & Zhang, 2020; Sharma et al., 2020; Su & Yeh, 2020; Xu et al., 2020). In terms of actual implementation, cost considerations are crucial to decision-making executives. If the cost is too high, even with good network resilience performance, this developed strategy may not be implemented. For studies that consider both the protection and recovery aspects (Gomez & Baker, 2019; Zhu et al., 2021), the cost has not been considered at present (Zhu et al., 2021), only a few fixed-parameter design results are provided (Zhu et al., 2021), or only one-time recovery is considered (Gomez & Baker, 2019; Su & Yeh, 2020).

Therefore, when building a resilient network system, in addition to considering network resilience performance, the related costs should also be considered at the same time. In terms of cost, the cost of this study is mainly divided into fixed cost and variable cost. The definitions of fixed costs and variable costs are provided in Table 1. Three studies (Jia & Zhang, 2020; Sharma et al., 2020; Zhu et al., 2021) specifically mentioned Nc in the research. Sharma et al. (2020) further subdivided Nc’s labor cost and discussed in more detail. Smith et al. and Gonzalez et al. (Gonzalez et al., 2016; Smith et al., 2020) considered the cost of flow and the cost of recovery space. The cost related to Nc and recovery space is classified under the fixed cost of the recovery strategy in this study. Moreover, to develop a more comprehensive protection and recovery strategy, it is necessary to discuss the given parameters and decision variables in a more
| Research studies | Pant et al. (2014) | Gonzalez et al. (2016) | Hosseini and Barker (2016) | Hosseini et al. (2016) | Liu et al. (2016) | Monroe et al. (2018) | Rocco et al. (2019) | Gomez and Baker (2019) | Hosseini and Ivanov (2019) | Haeh and Jia and Zhang (2020) | Sharma et al. (2020) | Smith et al. (2020) | Su and Yeh (2020) | Xu et al. (2020) | Zhu et al. (2021) | Proposed model |
|------------------|------------------|---------------------|------------------------|----------------------|-----------------|---------------------|---------------------|------------------------|--------------------------|---------------------------|----------------|----------------|----------------|----------------|----------------|------------------|
| **Features**     |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| All terminals    | √                |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Source-sink      | √                |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Failure component|                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| On node          |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| On arc           |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Failure type     |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Binary-state     |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Multistate       |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Stochastic method|                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Probabilistic    |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| method           |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| PSDA-based       |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Bayesian networks|                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Copeland score   |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Structure-based  |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| model            |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Optimization     |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Deterministic    |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| method           |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Transport diversity |              |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| BAT-based        |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| BATRA-based      |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Capacity         |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Deterministic    |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Stochastic       |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Multivalued      |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Flow             |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Transmission factor |               |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Cost of flow     |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Protection strategy |             |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Fixed $N_p$      |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Variable $N_p$   |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Upper/lower bound of $N_p$ | |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Binary protection vector | |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| One-time protection |           |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Dynamic protection |          |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Protection order  |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Fixed cost       |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Variable cost    |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Attack strategy  |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Fixed $N_a$      |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Variable $N_a$   |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Upper/lower bound of $N_a$ | |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Binary attack vector |         |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| One-time attack  |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Dynamic attack   |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| Fixed $N_f$      |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| \(p_i\)          |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| \(p_{ij}\)       |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |
| \(p_{kl}\)       |                  |                     |                        |                      |                 |                     |                      |                        |                          |                           |                 |                 |                 |                 |                 |                  |

Table 1: A review of literature related to network resilience assessment.
| Features                        | Pant et al. (2014) | González et al. (2016) | Hosseini and Barker (2016) | Hosseini et al. (2016) | Liu et al. (2016) | Monroe et al. (2016) | Rocco et al. (2016) | Gomez and Baker (2019) | Hosseini and Ivanov (2019) | Huieh and Feng (2020) | Jia and Zhang (2020) | Sharma et al. (2020) | Smith et al. (2020) | Su and Wib (2020) | Xu et al. (2020) | Zhu et al. (2021) | Proposed model |
|--------------------------------|--------------------|------------------------|---------------------------|------------------------|-----------------|---------------------|-----------------------|-------------------------|-----------------------------|----------------------|----------------------|----------------------|----------------------|---------------------|---------------------|----------------------|---------------------|
| Variable $N_f$                  |                    |                        |                           |                        |                 |                     |                       |                         |                             |                      |                      |                      |                      |                    |                     |                      |                    |
| Failure state                   | ✓                  | ✓                      | ✓                         | ✓                      |                 |                     | ✓                      | ✓                       |                             |                      |                      |                      |                      |                    | ✓                   | ✓                    |                    |
| Recovery strategy               |                    |                        |                           |                        |                 |                     |                       |                         |                             |                      |                      |                      |                      |                    |                     |                      |                    |
| Fixed $N_r$                     |                    |                        |                           | ✓                      |                 |                     | ✓                      | ✓                       |                             |                      |                      |                      |                      |                    | ✓                   | ✓                    |                    |
| Variable $N_r$                  | ✓                  | ✓                      | ✓                         | ✓                      |                 |                     | ✓                      | ✓                       |                             |                      |                      |                      |                      |                    | ✓                   | ✓                    |                    |
| Upper/lower bound               |                    |                        |                           |                        |                 |                     |                       |                         |                             |                      |                      |                      |                      |                    |                     |                      |                    |
| $N_c$                           | ✓                  | ✓                      | ✓                         | ✓                      |                 |                     | ✓                      | ✓                       |                             |                      |                      |                      |                      |                    | ✓                   | ✓                    |                    |
| Binary recovery vector          |                    |                        |                           |                        |                 |                     |                       |                         |                             |                      |                      |                      |                      |                    |                     |                      |                    |
| Recovery space                  |                    |                        |                           |                        |                 |                     |                       |                         |                             |                      |                      |                      |                      |                    |                     |                      |                    |
| Flow redistribution             |                    |                        |                           |                        |                 |                     |                       |                         |                             |                      |                      |                      |                      |                    |                     |                      |                    |
| (allow overloaded)             |                    |                        |                           |                        |                 |                     |                       |                         |                             |                      |                      |                      |                      |                    |                     |                      |                    |
| One-time recovery               |                    |                        |                           |                        |                 |                     |                       |                         |                             |                      |                      |                      |                      |                    |                     |                      |                    |
| Dynamic recovery                | ✓                  | ✓                      | ✓                         | ✓                      |                 |                     | ✓                      | ✓                       |                             |                      |                      |                      |                      |                    | ✓                   | ✓                    |                    |
| Recovery order                  | ✓                  | ✓                      | ✓                         | ✓                      |                 |                     | ✓                      | ✓                       |                             |                      |                      |                      |                      |                    | ✓                   | ✓                    |                    |
| Fixed cost                      |                    |                        |                           | ✓                      |                 |                     | ✓                      | ✓                       |                             |                      |                      |                      |                      |                    | ✓                   | ✓                    |                    |
| Variable cost                   | ✓                  | ✓                      | ✓                         | ✓                      |                 |                     | ✓                      | ✓                       |                             |                      |                      |                      |                      |                    | ✓                   | ✓                    |                    |
| Recover to perfect              | ✓                  | ✓                      | ✓                         | ✓                      |                 |                     | ✓                      | ✓                       |                             |                      |                      |                      |                      |                    | ✓                   | ✓                    |                    |
| Recover to imperfect            | ✓                  | ✓                      | ✓                         | ✓                      |                 |                     | ✓                      | ✓                       |                             |                      |                      |                      |                      |                    | ✓                   | ✓                    |                    |
| Objective                      |                    |                        |                           |                        |                 |                     |                       |                         |                             |                      |                      |                      |                      |                    |                     |                      |                    |
| Component importance            |                    |                        |                           |                        |                 |                     |                       |                         |                             |                      |                      |                      |                      |                    |                     |                      |                    |
| Static resilience               | ✓                  | ✓                      | ✓                         | ✓                      |                 |                     | ✓                      | ✓                       |                             |                      |                      |                      |                      |                    | ✓                   | ✓                    |                    |
| Dynamic resilience              | ✓                  | ✓                      | ✓                         | ✓                      |                 |                     | ✓                      | ✓                       |                             |                      |                      |                      |                      |                    | ✓                   | ✓                    |                    |
| Flow                           |                    |                        |                           |                        |                 |                     |                       |                         |                             |                      |                      |                      |                      |                    |                     |                      |                    |
| Cost                           | ✓                  | ✓                      | ✓                         | ✓                      |                 |                     | ✓                      | ✓                       |                             |                      |                      |                      |                      |                    | ✓                   | ✓                    |                    |
| Time                           | ✓                  | ✓                      | ✓                         | ✓                      |                 |                     | ✓                      | ✓                       |                             |                      |                      |                      |                      |                    | ✓                   | ✓                    |                    |
| $N_f$                           | ✓                  | ✓                      | ✓                         | ✓                      |                 |                     | ✓                      | ✓                       |                             |                      |                      |                      |                      |                    | ✓                   | ✓                    |                    |
| Vulnerability/loss             |                    |                        |                           |                        |                 |                     |                       |                         |                             |                      |                      |                      |                      |                    |                     |                      |                    |
| Recoverability                  | ✓                  | ✓                      | ✓                         | ✓                      |                 |                     | ✓                      | ✓                       |                             |                      |                      |                      |                      |                    | ✓                   | ✓                    |                    |
| Reliability                    |                     |                        |                           |                        |                 |                     |                       |                         |                             |                      |                      |                      |                      |                    |                     |                      |                    |
| Solution                       | ✓                  | ✓                      | ✓                         | ✓                      |                 |                     | ✓                      | ✓                       |                             |                      |                      |                      |                      |                    | ✓                   | ✓                    |                    |
| Heuristic                      | ✓                  | ✓                      | ✓                         | ✓                      |                 |                     | ✓                      | ✓                       |                             |                      |                      |                      |                      |                    | ✓                   | ✓                    |                    |
| Metaheuristic                  | ✓                  | ✓                      | ✓                         | ✓                      |                 |                     | ✓                      | ✓                       |                             |                      |                      |                      |                      |                    | ✓                   | ✓                    |                    |
| Hybrid                         | ✓                  | ✓                      | ✓                         | ✓                      |                 |                     | ✓                      | ✓                       |                             |                      |                      |                      |                      |                    | ✓                   | ✓                    |                    |
| Simulation                     | ✓                  | ✓                      | ✓                         | ✓                      |                 |                     | ✓                      | ✓                       |                             |                      |                      |                      |                      |                    | ✓                   | ✓                    |                    |
| Exact                          | ✓                  | ✓                      | ✓                         | ✓                      |                 |                     | ✓                      | ✓                       |                             |                      |                      |                      |                      |                    | ✓                   | ✓                    |                    |
systematic way. In this way, decision makers can have a basis when making final decisions about network resilience.

According to Hosseini et al. (Hosseini et al., 2016a, 2019), the resilience quantitative assessment approaches contain stochastic and deterministic approaches. In stochastic approaches, the most common approaches include probabilistic models such as Bayesian networks (Hosseini & Barker, 2016; Hosseini et al., 2016b; Hosseini & Ivanov, 2019), probabilistic solution discovery algorithm-based model (Zhu et al., 2021), and Copeland score (Xu et al., 2020), and structural-based models such as simulation (Pant et al., 2014; Hosseini & Barker, 2016; Hosseini et al., 2016b; Monroe et al., 2018; Rocco et al., 2018; Hosseini & Ivanov, 2019; Xu et al., 2020), optimization (González et al., 2016; Gomez & Baker, 2019; Jia & Zhang, 2020; Sharma et al., 2020; Smith et al., 2020; Zhu et al., 2021), and fuzzy logic models. In deterministic approaches, there are the transport diversity (Hsieh & Feng, 2020), Binary-Addition Tree (BAT)-based model (Su & Yeh, 2020), and the Binary-Addition Tree-based Resilience Assessment (BATRA)-based model proposed by this paper.

It can also be seen from Table 1 that although most of the existing studies use simulation or optimization to solve the resilience of the network system, this research still applies a deterministic approach to solve the resilience of the network system. The simulation solution obtained by the simulation approach is not an exact solution, and it is not intuitive enough for decision makers. In the optimization model, it is usually necessary to fix multiple parameters to obtain the best recovery strategy for a specific protection strategy and attack strategy (Gomez & Baker, 2019). However, in fact, we cannot really predict what kind of attack strategy decision makers will face. Therefore, we believe that in the design and planning stage of the network system, we must consider all reasonable protection strategies, the most likely attack strategies, and the most effective protection strategies. Also, this research tends to focus on discussing more decision variables in protection, attack, and recovery strategies, and provides the whole process of analysing variables to be clearly and completely presented to decision makers for reference. Therefore, this study adopts a deterministic approach to solve the resilience and cost of the network system.

In order to achieve a comprehensive set of protection and recovery strategies to resist external attacks on network systems and make it easier for decision makers to understand the strategy development process, we propose a time-related BATRA based on BATRA (Su & Yeh, 2020). To build a resilient network, the proposed time-related BATRA sequentially generates combinations of relevant decision variables and state vectors for protection, attack, and recovery strategies.

Unlike BATRA, which unconditionally enumerates all strategies, the proposed time-related BATRA provides more available decision variables (i.e. importance weight of arcs, number of arcs to be protected, number of arcs to be attacked, number of arcs to be recovered, etc.). Then, according to these decision variables, the state vector values of the corresponding strategies are listed. In addition, the proposed time-related BATRA considers a more realistic successive recovery (i.e. the number of arcs recovered per unit time) rather than a one-time recovery, which is why it is called time-related.

In the time-related BATRA, we propose a new resilience performance measurement, which is based on the resilience evaluation when considering both protection and recovery strategies proposed by Zhu et al. (2021). Our newly proposed resilience metric can also reflect changes in the network reliability during the recovery process and evaluate the network resilience. The difference is that the resilience metric we propose is based on the degree of network reliability recovery each time, rather than the degree of network reliability still loss each time. Because we found that the assumption that the network is recovered to its original state must be satisfied in order to correctly use the resilience metric based on the degree of network reliability still loss each time (Zhu et al., 2021). We want to give decision makers the choices of full recovery or partial recovery, so we need to escape the assumption that the network can only be recovered to the original state. Therefore, we adopt our newly proposed resilience metric.

To produce a series of protection, attack, and recovery strategies, a large number of calculations are inevitable in a complex network or even a simple network. The foundation of all complex networks starts with a binary-state network. Calculating the reliability of a binary-state network is an NP problem (Colbourn, 1987; Aven, 1988; Levitin, 2005; Hao et al., 2020; Yeh, 2020a), and so is the extended network resilience. In order to cope with the complexity of calculation, both the proposed time-related BATRA and the aforementioned BATRA are developed based on BAT, which has excellent performance in binary-state networks. In addition, BAT has the advantages of being simple and easy to understand and customize, which is easy for decision makers to grasp and accept (Yeh, 2020a). The main contributions of this research can be summarized into three aspects. First, we consider more decision variables and parameters in the protection, attack, and recovery strategies, and further include the costs in the formulation of the protection and recovery strategies. Second, we develop a new performance measure oriented to the degree of network reliability recovery to quantify the resilience of the network system. Third, we propose the time-related BATRA to determine decision variables, obtain protection, attack, and recovery strategies, and calculate the final network resilience and related cost.

The remainder of this article is arranged as follows: Section 2 describes the problem and formulates its performance index and decision variables. Section 3 presents the proposed method with an illustrated example. In Section 4, a case study is analysed through the proposed method. Finally, Section 5 provides the conclusion.

2. Problem Description

This section is divided into four parts to complete the description of the research problem, namely problem background, proposed resilience metric, decision variables and related constraints, and assumptions.

2.1. Problem background

This research aims to build a resilient network system to resist external attacks, so that the network system can operate normally and meet demands. The resilient network model is modeled as a two-terminal binary-state network G(V, E, D) with the source node 1 and the sink node n, where V = {1, 2, ..., n} represents the set of nodes, E = {a1, a2, ..., am} represents the set of arcs, and D represents the success probability of each arc in a binary-state network. The arcs, indexed by k = 1, 2, ..., m = |E|, are used to represent the network components, with their states represented by state vector X = {X(a1), X(a2), ..., X(ak)}, where X(ak) = 1 if arc k is functioning and X(ak) = 0 otherwise. The arcs contained in E are assumed to be imperfect and may be broken, but the nodes contained in V are assumed to be perfect and will not be broken.
The sequential decision-making process between our side and the attacker is our protection strategy, the attacker’s attack strategy, and our recovery strategy. As for the information shared by our side and the attacker, the protected arcs will not be destroyed by the attack, and the network structure, i.e. the number of arcs and the number of nodes. However, the attacker has no way of knowing the probability distribution \( D \) of the arcs in the network and our protection strategy. In the protection strategy, the total number of arcs to be protected, \( N_p \), needs to be determined. Then, the order of the arcs to be protected is determined according to \( N_p \) and the importance weight of arc \( k \), \( l(a_k) \). The state vector used to represent the arc to be protected in the 1th protection strategy is \( X_p = (X_p(a_1), X_p(a_2), \ldots, X_p(a_n)) \), where \( X_p(a_k) = 1 \) if arc \( k \) is functioning and \( X_p(a_k) = 0 \) otherwise. Also, the corresponding protection costs will be calculated.

In the attack strategy, the total number of arcs to be attacked, \( N_a \), needs to be determined. The state vector used to represent the arc to be attacked in the 1th attack strategy is \( X_a = (X_a(a_1), X_a(a_2), \ldots, X_a(a_n)) \), where \( X_a(a_k) = 1 \) if arc \( k \) is functioning and \( X_a(a_k) = 0 \) otherwise. Then, according to \( X_p \) and \( X_a \), the failed status \( v \) of the network after the attack can be obtained, which is \( X_{av} = (X_{av}(a_1), X_{av}(a_2), \ldots, X_{av}(a_n)) \), where \( X_{av}(a_k) = 1 \) if arc \( k \) is functioning and \( X_{av}(a_k) = 0 \) otherwise. In the recovery strategy, the total number of arcs to be recovered, \( N_r \), and the number of recovered arcs per unit time, \( T_r \), need to be determined. According to \( N_r \), \( T_r \), and \( l(a_k) \), we can determine the order of the arcs to be recovered. The state vector used to represent the arc to be recovered in the 1th recovery strategy is \( X_r = (X_r(a_1), X_r(a_2), \ldots, X_r(a_n)) \), where \( X_r(a_k) = 1 \) if arc \( k \) is functioning and \( X_r(a_k) = 0 \) otherwise. Notice that only the attacked arc will be recovered, and the network can recover perfectly to its original status or recover imperfectly to its available status with corresponding costs. During the recovery process, the network reliability under different recovery stages can be obtained. Based on the changes in the recovery degree of the network reliability, the corresponding network resilience performance and the total costs can be obtained.

### 2.2. Proposed resilience metric

For a resilient network system, the network can be divided into three states according to the time horizon as shown in Fig. 1 (Pant et al., 2014; Hosseini et al., 2016a; Zhu et al., 2021): the original state before disruption \( t_0 \leq t < t_d \); the recovery state after disruption \( t_d \leq t < t_r \); and recovery completion state \( t_r \leq t \), where \( t \) is the current time point, \( t_0 \) is the time point of the original state with reliability \( R_0 \), \( t_d \) is the time point right after disruption with reliability \( R_d \), and \( t_r \) is the time point right after recovery with reliability \( R_r \). \( R_0 \) is the network reliability when the network is operating normally. When a disruptive event occurs at \( t_0 \), the network reliability will be reduced to \( R_d \). The network has been in a damaged state or recovery state until the recovery process is completed. Therefore, the network reliability during the network recovery process is represented by \( R_d \). If the full recovery strategy is used, the network reliability at time \( t \) is represented by \( R_d(t) \); if the partial recovery strategy is used, the network reliability at time \( t \) is represented by \( R_d(t) \). In Fig. 1, the recovery process is a stepped shape, because the recovery strategy includes recovering a certain number of arcs per unit time, which is \( T_r \). Moreover, in this article, the network may be completely recovered to its original state with full recovery costs, or it may be partially recovered to an acceptable state with partial recovery costs; that is, \( R_r \) is not necessarily equal to \( R_0 \).

Regarding the calculation of network resilience, Su and Yeh (2020) integrated the previous literature and proposed a resilient performance indicator that simultaneously considers the loss and recovery of reliability, such as equation (1), and applies it to the proposed BATRA to analyse network resilience. However, equation (1) mentioned in Su and Yeh (2020) only considers one-time recovery; that is, it does not consider \( T_r \). Since equation (1) is not related to the time, we name equation (1) a static resilient performance indicator in this article. In our proposed
time-related BATRA, before generating protection, attack, and recovery strategies, equation (1) will only be used to calculate the importance weights of arcs. Equation (1) represents the ratio of the degree of recovery to the degree of loss, which has been proven for its effectiveness (Pant et al., 2014; Hosseini & Barker, 2016; Hosseini et al., 2016a, b; Hosseini & Ivanov, 2019; Su & Yeh, 2020; Zhu et al., 2021).

\[ I = \frac{\varphi_R - \varphi_d}{R_0 - R_d} \]  

(1)

Zhu et al. (2021) proposed equation (2) to calculate the change in the degree of network reliability loss during the recovery process, as shown in the nongray area between the \( t_r \) and \( t_t \) sections in Fig. 1. Since equation (2) is considered from the degree of reliability loss, the smaller the value, the higher the network resilience. However, we found that to correctly use equation (2) proposed in Zhu et al. (2021), it is necessary to assume that the network must be recovered to its original state with reliability \( R_0 \). However, the real recovery situation may be limited by cost, and it may not be able to perfectly recover the network to its original state. We expect to provide decision makers with the option of partially recovering the network; thus, we propose equation (3).

\[ \varphi_D = \int_{t_r}^{t_t} \left[ 100 - 100 \frac{R_d(t)}{R_0} \right] dt \]  

(2)

To calculate the network resilience, what we are concerned about is to calculate the change in the degree of recovery of the network reliability during the recovery process, as shown in the gray area between the \( t_r \) and \( t_t \) sections in Fig. 1 and the content of the square brackets in equation (3). Equation (3) is also multiplied by \( T_r \) to show the effect of different \( T_r \) on resilience performance. Since equation (3) is considered from the degree of reliability recovery, the larger the value, the higher the network resilience. Also, there is no need to assume that the network must be recovered to its original state. In equation (3), a network resilience of around 100 means that the network is recovered to an operational state. This equation (3) is the dynamic resilient performance indicator we proposed, and it is named dynamic because it is related to time. In our proposed time-related BATRA, after generating protection, attack, and recovery strategies, equation (3) will be used to calculate the final network resilience.

\[ \varphi_D = T_r \int_{t_r}^{t_t} \left[ 100 - 100 \frac{R_d(t)}{R_0} \right] dt \]  

(3)

### 2.3. Decision variables and related constraints

In this section, we summarize and explain the main decision variables and related constraints in the decision-making process of this research.

The real-valued decision variables are importance weight of the \( k \)th arc, \( I(a_k) \), total number of arcs protected, \( N_p \), total number of arcs attacked, \( N_a \), total number of arcs recovered, \( N_r \), and number of arcs recovered per unit time, \( T_r \). Also, the vector-formed decision variables are the state vector for the protection strategy \( I \), \( X_{Pj} \), the state vector for the attack strategy \( q \), \( X_{Aq} \), and the state vector for the recovery strategy \( w \) for the network failed status \( v \) at recovery time point \( t \), \( X_{v(t)} \). The vector-formed decision variables can be defined when the real-valued decision variables are determined. Constraints related to the real-valued decision variables are listed and explained as equations (4)–(10) below.

\[ 0 \leq I(a_k) \leq 1 \]  

(4)

\[ \text{Min} \sum_{k} N_p C_{pv}(a) + C_{pf}(N_p) \leq \sum_{k} C_{r}(a_k) \]  

(5)

\[ n_c \leq N_f \leq |E| \]  

(6)

\[ n_c \leq N_f \leq 2n_c \]  

(7)

\[ 0 \leq N_f \leq |E| - N_p \]  

(8)

\[ 1 \leq N_r \leq N_f \]  

(9)

\[ 1 \leq T_r \leq N_t \]  

(10)

\( I(a_k) \) is calculated first among all decision variables, and its value is between 0 and 1, as shown in equation (4). For smart protectors, they will choose a protection strategy whose least sum of protection cost is less than the sum of recovery variable cost and larger than \( n_c \), as shown in equations (5) and (6). \( n_c \) is the number of arcs with the least attack to disconnect the network. \( n_c \) is found beforehand and can be regarded as a known parameter. In equation (5), summation over \( a \) goes from 1 to \( N_p \) means the sum of \( C_{pv}(a) \) from the smallest to the \( N_p \) smallest. If the sum of recovery variable cost (right-hand side of equation 5) is over the least sum of protection cost (left-hand side of equation 5), then the implication will be that the protection strategy only selects at most to \( N_p \) arcs, rather than selecting all the arcs of the network.

In equation (6), the upper bound of \( N_f \) is the number of arcs, \( |E| \), and the bound of \( N_r \) is \( n_c \).

For smart attackers, they will choose to attack \( n_c \) to \( 2n_c \) arcs to disconnect the network more effectively, as shown in equation (7). Both the protector and the attacker know that the protected arc will not be broken when attacked. Therefore, a smart attacker will only attack \( n_c \) to \( 2n_c \) arcs as the constraint in equation (7), where \( n_c \) is the number of arcs with the least attack to disconnect the network and \( 2n_c \) means that the attacker believes that the protector will protect the \( n_c \) arcs. In order to increase the success rate of disconnecting the network, the attacker may attack more arcs at most to twice the \( n_c \).

\( N_p \), \( N_f \), and \( T_r \) have a mutual influence restriction relationship, as shown in equations (8)–(10). After we obtain \( N_p \) and \( N_f \), we can obtain the corresponding \( N_r \). The upper and lower bounds of \( N_f \) depend on \( N_p \) as in equation (8). According to \( N_r \), the upper and lower limits of \( N_f \) are therefore determined as in equation (9). Then, according to \( N_r \), the upper and lower limits of \( T_r \) are therefore determined as in equation (10).

The related usage of equations (4)–(10) will be used and explained in detail in Sections 3.2 and 3.3 as well.

### 2.4. Assumptions

The following are the assumptions used in the research:

1. The arcs may be broken, but the nodes will not.
2. There are two states of each arc: working or failed.
3. There are no parallel arcs or loops in the network.
4. The success probability of each arc does not affect each other.
5. The network can recover perfectly to its original status or recover imperfectly to its available status with corresponding costs.
6. The attacker can see the network structure, but does not know the protection strategy.
7) The main purpose of the attacker is to disconnect the network with the least attack on arcs.
8) Both the protector and the attacker know that the protected arc will not be broken when attacked.
9) Only the attacked arc will be recovered.
10) This paper only considers the cost of our side (protector and recover), not the cost of the attacker.

Relevant explanations about these assumptions are provided as follows:

The failure state usually occurs in the arc component or the node component in the network system. Table 1 summarizes the location of the failure status of different studies. Also, this study assumes that the failure will occur on the arc as assumption 1.

As can be seen from Table 1, most of the studies (Pant et al., 2014; González et al., 2016; Hosseini & Barker, 2016; Hosseini et al., 2016b; Liu et al., 2016; Monroe et al., 2018; Rocco et al., 2018; Gomez & Baker, 2019; Hosseini & Ivanov, 2019; Hsieh & Feng, 2020; Jia & Zhang, 2020; Sharma et al., 2020; Smith et al., 2020; Su & Yeh, 2020; Zhu et al., 2021) discussed the failure state of network components in a binary state. If the component failure status is Boolean value (i.e. two states, False and True), then the component capacity, whether it is deterministic or stochastic, as long as the component is failed, will be reduced from the original capacity to the capacity that cannot make the network system work normally. Therefore, these studies do not specifically discuss or emphasize capacity. Therefore, this study also assumes that there are two states of each arc component: working or failed as assumption 2.

Moreover, among the studies in which the failure state of these network components is a binary state, some failure clearly defines the component state as a binary state, and some are not mentioned in the article. Therefore, this study clearly defines the component state as a binary state. In addition, Xu et al. (2020) proposed a multistate component failure state, and the multistate component capacity. Also, Zhu et al. (2021) is the only known literature that has made an in-depth discussion on component capacity and flow, and proposed a resilient recovery strategy that redistributes flow when overloaded is allowed.

Assumptions 3 and 4 are the basic assumptions for the networks in this research. According to the actual situation, the failure state may not be perfectly recovered, so this research assumes that the network can be recovered to perfect or imperfect as assumption 5. Assumptions 6-9 define the basic rules of network protection, attack, and recovery in this paper. Also, we focus on discussing the cost of our side (protector and recover) as assumption 10.

3. Solution Algorithm

The time-related BATRA we proposed is based on the BATRA proposed by Su and Yeh (Su & Yeh, 2020) in 2020. Before generating protection, attack, and recovery strategies, we use BATRA to first calculate the importance weight of arcs in the network. Then, follow the logic of the binary-addition tree in BATRA and BAT to sequentially generate the strategies. Finally, we use the dynamic resilient performance indicators we proposed to evaluate each strategy combination. In order to make it easier for readers to understand our proposed time-related BATRA, in this section we will first provide the algorithm background related to BATRA and BAT, then introduce our proposed time-related BATRA, and finally use a simple example to illustrate our proposed time-related BATRA.

3.1. Algorithm background

After BAT was formally proposed by Yeh in 2020 (Yeh, 2020a), because of its easy customization and high problem applicability, many researches and extended applications are vigorously developing based on it. For example, there are BAT and maximum-state PageRank on predicting and modeling wildfire propagation areas (Yeh & Kuo, 2020), the bounded BAT for the binary-state network reliability problems (Yeh, 2020b), an improved and enhanced BAT for the reliability of the acyclic multistate information network (Yeh et al., 2021), the BAT-based algorithm on the one-batch preempt multistate multirework network (Hao et al., 2021), the all-pairs BAT on calculating homogeneity-arc binary-state undirected network reliability (Yeh, 2021), the BATRA on the static network resilience issue (Su & Yeh, 2020), and the time-related BATRA on the dynamic network resilience issue proposed by this research.

BAT mainly contains four parts, namely the binary-addition tree, the Path-based Layered-Search Algorithm (PLSA), the reduction methods, and the probability calculations of the connected vectors (Yeh, 2020a). The binary-addition tree lists all possible state vectors in a binary adding way. Then, PLSA filters out connected vectors from these found state vectors. The reduction method is used to reduce unnecessary calculations for unconnected state vectors in the binary-addition tree or PLSA. Finally, the event probability related to the connected state vector is calculated and summed to obtain the network reliability. Among them, the binary-addition tree can be said to be the main spirit of BAT and the calculus logic we emulate. Because the binary-addition tree can generate state vectors with simple binary logic, it is extended to generate protection, attack, and recovery strategies. The other parts of BAT can effectively assist us in calculating network reliability problems. In addition, BAT has also been extended to use in multistate networks (Hao et al., 2021; Yeh et al., 2021). In other words, there are multiple state BAT to generate multiple state vectors. Such multistate BAT is also used in this study to generate decision variables in the recovery strategy. Moreover, the reason why these recent researches, including ours, are based on and adopt BAT is also that it can directly and efficiently obtain the network reliability (Yeh, 2020a) that is an NP-hard problem (Colbourn, 1987; Aven, 1988; Levitin, 2005; Hao et al., 2020, 2021; Su & Yeh, 2020; Yeh, 2020a, b, 2021; Yeh et al., 2021).

In any case, the time-related BATRA we proposed is based on BATRA, and BATRA is developed based on BAT (Su & Yeh, 2020). In the beginning, BATRA inherited the calculation methods of BAT to obtain the reliability of the original network. Next, BATRA uses the binary-addition tree idea in BAT to exhaust all the state vectors that the network may be disrupted and all the corresponding recovery state vectors, and then calculates the network reliability of the corresponding state. Finally, it calculates the corresponding recovery cost, component importance, and static network resilience. It is worth noting that the state vectors considered in BATRA are all listed; that is, the constraints in Section 2.3 in this study are not considered by BATRA. Therefore, the state vector considered in BATRA includes many extreme network disruptive states or ineffective recovery strategies. This is also the focus of this study to improve BATRA.

3.2. Proposed time-related BATRA

The procedure of the proposed time-related BATRA is presented as the following Algorithm 1.
Algorithm 1: Procedure of the time-related BATRA

\textbf{Input:} \(G(V, E, D)\), arc protect and recovery costs.

\textbf{Output:} Network protect, attack and recovery strategies with dynamic network resilience and costs.

\textbf{STEP A.} Apply BATRA algorithm to find the importance weight of each arc.

\textbf{STEP A1.} Obtain original network reliability \(R_0\).

\textbf{STEP A2.} Obtain vulnerability \(R_e\).

\textbf{STEP A3.} Obtain recoverability \(R_r\).

\textbf{STEP A4.} Calculate importance weight of each arc by equation (1).

\textbf{STEP B.} Decide total number of protected arcs and the protected arcs with protect costs.

\textbf{STEP C.} Decide total number of attacked arcs and the attacked arcs.

\textbf{STEP D.} Decide total number of recovered arcs, and the number of arcs recovered per unit time with recovery costs. And then obtain the corresponding network resilience by equation (3).

In the beginning, it is necessary to provide algorithm information about the network, including the network structure \(G(V, E, D)\), the cost of protecting the arcs, and the cost of recovering the arcs. The algorithm is expected to produce results for decision makers containing protect, attack, and recovery strategies with dynamic network resilience and costs. The steps of the algorithm are described as follows.

\textbf{STEP A} is based on BATRA and is for calculating the important weight of arcs and the reliability of original network. There are \textbf{STEP A1 to STEP A4} in the \textbf{STEP A}. \textbf{STEP A1} is based on BAT to reduce the number of impossible solutions and connectivity verifications, implement the binary-addition tree to list state vectors, apply PLSA to verify the connectivity of found state vectors, and obtain the original network reliability. \textbf{STEP A2} to \textbf{STEP A4} are following BATRA to calculate the importance weight of each arc by the static network resilient performance indicator as equation (1), where \(R_e\) is the vulnerability of disruptive network and \(R_r\) is the recoverability of the recovered network. In this study, \(R_0\), \(R_e\), and \(R_r\) are calculated in the same way as in BATRA (Su & Yeh, 2020).

Based on the computation results obtained from \textbf{STEP A} and the logic of binary-addition tree, \textbf{STEP B} to \textbf{STEP D} are developed. \textbf{STEP B} decides the total number of protected arcs based on equation (5), and then lists the protected arcs with protect costs by using the importance weight of arcs obtained from \textbf{STEP A}. \textbf{STEP C} decides total number of attacked arcs based on equation (7), and then lists the attacked arcs by using binary-addition tree. \textbf{STEP D} decides total number of recovered arcs based on equation (9), determines the number of arcs recovered per unit time based on equation (10), and lists the recovered arcs with recovery costs by using binary-addition tree. Then, it obtains the corresponding dynamic network resilience by using equation (3). As a result, the time-related BATRA can provide a decision-making process that is easy for decision makers to understand and implement. Also, based on the final output, i.e. the dynamic network resilience and the total cost required, decision makers can choose a strategy that meets their needs.

\subsection{3.3. Illustrated example}

The proposed time-related BATRA algorithm is illustrated and detailed through the example network shown in Fig. 2. Figure 2 is a binary-state network with four nodes and nine arcs (Yeh, 2020a). There are arc success probability, arc protect costs, and arc recovery costs in Fig. 2. Arc success probability is provided in Table 2. Arc protect cost that contains the variable cost corresponding to each arc is in Table 3 and the fixed cost affected by \(N_p\) is in Table 3. Arc recovery cost that contains the variable cost corresponding to each arc is in Table 2 and the daily fixed cost affected by \(T_r\) is in Table 3. The fixed costs are increased as the number of protected arcs or daily recovered arc increases. Notice that the information in the above tables related to Fig. 2 is only listed to five arcs, since in \textbf{STEP A1}, the original nine arcs are reduced to five arcs. Following is the procedure of the solution.

\textbf{Solution:}

\textbf{STEP A.} Apply the BATRA algorithm to find the importance weight of each arc.

\textbf{STEP A1.} Obtain original network reliability \(R_0\).

At the very beginning, BATRA is based on BAT and executes lessening number of impossible solutions (i.e. Fig. 2 is lessened to Fig. 3), listing \(2^5\) all possible state vectors, lessening number of connectivity verifications, verifying connectivity of state vectors, and computing reliability of found 15 connected vectors and the original network in sequence. We can obtain \(R_0 = 0.94168\).

\textbf{STEP A2.} Obtain vulnerability \(R_e\).

Based on binary-addition tree, five scenarios with different one failed arc can be found. Then, continuing to use found 15 connected vectors from \textbf{STEP A1}; the network vulnerability \(R_e\) can be obtained for these five scenarios. Notice that here we only care about one failed arc in the network.

\textbf{STEP A3.} Obtain recoverability \(R_r\).

Based on binary-addition tree, according to scenarios with different one failed arc, there are different recovery strategies that can be generated. That is, for each scenario, there are two related recovery strategies: “not to recover” and “to recover.” The point to note is that if we want to recover the arc, we will incur cost. Therefore, considering the cost, not recovering the arc, and enabling the network to operate normally is also a type of recovery strategy. Via continuing to use found 15 connected vectors from \textbf{STEP A1} and choosing the strategy with the largest ratio of recovery reliability to cost, the network recoverability \(R_r\) can be obtained for these five scenarios.

\textbf{STEP A4.} Calculate importance weight of each arc using equation (1).

After obtaining \(R_0\), \(R_e\), and \(R_r\), the importance weight of each arc can be calculated using equation (1). For example, the detailed numbers to find the importance weight of each arc from \textbf{STEP A2} to \textbf{STEP A4} in \textbf{STEP A} can be summarized as Table 4. The column “I” in Table 4 is the calculation result by equation (1), stands for the importance weight of each arc, and will be used in the following steps.

| a       | \(P(a)\) | \(C_r(a)\) | \(P'(a)\) | \(C_r'(a)\) |
|---------|---------|----------------|-----------|-----------|
| \(a_1 = e_{1,2}\) | 0.8     | 30             | 0.6       | 20        |
| \(a_2 = e_{1,3}\) | 0.9     | 40             | 0.7       | 30        |
| \(a_3 = e_{2,3}\) | 0.7     | 30             | 0.5       | 20        |
| \(a_4 = e_{3,4}\) | 0.8     | 40             | 0.6       | 20        |
| \(a_5 = e_{3,4}\) | 0.9     | 50             | 0.7       | 40        |
is at least 55 in Table 3 by summing variable and fixed protected costs for five arcs. To protect two arcs, the protection cost is determined by equation (6). Also, the sum of recovery variable costs of the five arcs as the constraint in equation (5).

For example, when protecting three arcs, smart protectors will give priority to protecting arcs 2 and 5. When protecting three arcs, smart protectors will give priority to protecting arcs 1, 2, and 3. Therefore, there will be two protection strategies and corresponding protection costs, as shown in Table 5. In Table 5, \( N_p \) is the number of protected arcs, \( X_p \) is the state vector for the protection strategy, and \( \text{sum} \; C_p \) is the total protection cost.

**STEP B.** Decide total number of protected arcs and the protected arcs with protect costs.

Based on binary-addition tree table from STEP A1, we can decide total number of protected arcs and the protected arcs with protect costs. In STEP A1, we can also obtain the least number of arcs to disconnect the network, \( n_e \). Therefore, the protector (our side) will protect the number of arcs greater than or equal to \( n_e \). However, since protecting arcs will incur costs, the smart protector will choose to protect the number of arcs, \( N_p \), which the least sum of protection costs is less than the sum of recovery variable costs of the five arcs as the constraint in equation (5).

For example, \( n_e = 2 \) in Fig. 3, so at least two arcs must be protected by equation (6). Also, the sum of recovery variable costs of the five arcs is 190 in Table 2 by summing full recovery variable costs for five arcs. To protect two arcs, the protection cost is at least 55 in Table 3 by summing variable and fixed protected costs for two arcs. To protect three arcs, the protection cost is at least 105 in Table 3 by summing variable and fixed protection costs for three arcs. To protect four arcs, the protection cost is at least 220 in Table 3 by summing variable and fixed protection costs for four arcs. However, since the minimum cost of protecting four arcs is 220, it is greater than the maximum recovery variable cost, 190, the protector will choose not to protect more than four arcs, but only two or three arcs.

Therefore, here we first list the number of possible protected arcs. Then, according to the number of protected arcs and the importance weight of the arcs, the combination of the protected arcs is listed and the corresponding protection cost is calculated. For example, according to the order of the importance weight of the arcs from high to low, the first three arcs with the highest importance weight are \( a_2 \), \( a_5 \), and \( a_0 \). When protecting two arcs, smart protectors will give priority to protecting \( a_2 \) and \( a_5 \). When protecting three arcs, smart protectors will give priority to protecting \( a_0 \), \( a_2 \), and \( a_5 \). Therefore, there will be two protection strategies and corresponding protection costs, as shown in Table 5. In Table 5, \( N_p \) is the number of protected arcs, \( X_p \) is the state vector for the protection strategy, and \( \text{sum} \; C_p \) is the total protection cost.

**STEP C.** Decide total number of attacked arcs and the attacked arcs.

Based on binary-addition tree table from STEP A1, we can decide total number of attacked arcs and the attacked arcs. In Step A1, we can also obtain \( n_e \). We assume that the attacker (our enemy) is smart and can know the network structure and the number of arcs in the network, but does not know the probability value of the arcs in the network and the protection strategy of the protector. In other words, the attacker does not know the probability of each arc, and therefore cannot know which arc is the most important. However, the attacker can also calculate the value of \( n_e \) by himself to determine the number of attacking arcs.

The main purpose of the attacker is to disconnect the network from the arc with the least attack. We believe that the assumption of a smart attacker is more reasonable.

Both the protector and the attacker know that the protected arc will not be broken when attacked. Therefore, a smart attacker will only attack \( n_e \) arcs as the constraint in equation (7), where \( n_e \) is the number of arcs with the least attack to disconnect the network and \( 2 \times n_e \) means that the attacker believes that the protector will protect the \( n_e \) arcs. In order to increase the success rate of disconnecting the network, the attacker may attack more arcs. Therefore, for the protection strategy found in the previous step, the corresponding attack strategies of various possible combinations will be generated according to the number of attacking arcs of the attacker.

For example, \( n_e = 2 \) in Fig. 3, thus, in Table 5 corresponding to the previous step, the possible attack strategy of the attacker...
is as shown in the gray bottom items in Table 6. Note that Table 6 can be acquired based on the state vectors found by binary-addition tree in STEP A1. With the constraint in equation (7), the number of $X_{aq}$ is reduced from 32 to 25, thus reducing the amount of calculation for subsequent steps.

According to Tables 5 and 6, the protection strategy and the attack strategy can be obtained, respectively. Each protection strategy in Table 5 will correspond to so many attack strategies in Table 6. By “subtracting” the vector values of the protection strategy and the attack strategy, the failed arcs can be obtained. After subtraction, if the vector value obtained is 0, it means that the arc is not broken. If the obtained vector value is 1, it means that the arc is protected and not attacked. If the obtained vector value is −1, it means that the arc is damaged and needs to be recovered in the next step. Notice that the vector value of the protected arc subtracts that of the attacked arc, and the vector value is 0, which means that the protected arc will not fail by the attack.

Then, after converting 0 and 1 to 0, and −1 converts to 1, it can correspond to the calculation result of the failed arc scenario in STEP A. In other words, the previous calculation results can be used to save the time needed to calculate the reliability of the network after the recovery strategy is implemented. For example, under the two protection strategies in the previous step, after facing different attack strategies, the transformed state vector for the network failed status $v$, $X_{d,a'}$, is shown in Table 7. In Table 7, $N_f$ is the number of failed arcs and has the constraint in equation (8).

For example, when protecting two arcs and facing an attack strategy, the number of arcs that may fail is between 0 and 3 as shown in the column “For $X_{p1}$ with all $X_{aq}$” in Table 7. When protecting three edges and facing an attack strategy, the number of arcs that may fail is between 0 and 2 as shown in the column “For $X_{p2}$ with all $X_{aq}$” in Table 7

### Table 6: All the $X_{aq}$ obtained in Fig. 3.

| $j$ | $N_a$ | $X_{aq}$ |
|---|---|---|
| 1 | 0 | (0, 0, 0, 0, 0) |
| 2 | 1 | (0, 0, 0, 0, 1) |
| 3 | 1 | (0, 0, 1, 0, 0) |
| 4 | 2 | (0, 0, 0, 1, 0) |
| 5 | 1 | (0, 1, 0, 0, 0) |
| 6 | 2 | (0, 0, 1, 0, 1) |
| 7 | 2 | (0, 1, 1, 0, 0) |
| 8 | 3 | (0, 0, 1, 1, 1) |
| 9 | 1 | (1, 0, 0, 0, 0) |
| 10 | 2 | (0, 1, 0, 0, 1) |
| 11 | 2 | (0, 1, 1, 0, 0) |
| 12 | 3 | (0, 1, 0, 1, 0) |
| 13 | 2 | (0, 1, 1, 0, 1) |
| 14 | 3 | (0, 1, 1, 1, 0) |
| 15 | 3 | (1, 0, 1, 1, 0) |
| 16 | 4 | (0, 1, 1, 1, 1) |

### Table 7: All the $X_{d,a'}$ obtained in Fig. 3.

| $u$ | $N_f$ | $X_{d,a'}$ |
|---|---|---|
| 1 | 0 | (0, 0, 0, 0, 0) |
| 2 | 1 | (0, 0, 0, 1, 0) |
| 3 | 1 | (0, 1, 0, 0, 0) |
| 4 | 1 | (1, 0, 0, 0, 0) |
| 5 | 2 | (0, 0, 1, 0, 0) |
| 6 | 2 | (0, 1, 0, 1, 0) |
| 7 | 2 | (0, 1, 1, 0, 0) |
| 8 | 3 | (0, 1, 1, 1, 0) |

For $X_{p1}$ with all $X_{aq}$

| $u$ | $N_f$ | $X_{d,a'}$ |
|---|---|---|
| 1 | 0 | (0, 0, 0, 0, 0) |
| 2 | 1 | (0, 0, 0, 1, 0) |
| 3 | 1 | (0, 1, 0, 0, 0) |
| 4 | 1 | (1, 0, 0, 0, 0) |
| 5 | 2 | (0, 0, 1, 0, 0) |
| 6 | 2 | (0, 1, 0, 1, 0) |
| 7 | 2 | (0, 1, 1, 0, 0) |
| 8 | 3 | (0, 1, 1, 1, 0) |

For $X_{p2}$ with all $X_{aq}$

For example, the following the previous STEP C, Tables 8 and 9 are different recovery strategies with changes in network reliability during the recovery process, $R_d(t)$, total recovery costs, $sumCr$, and dynamic network resilience, $\phi$. According to the importance weight of the arc calculated by STEP A, the order of arc recovery is $a_2$, $a_5$, $a_1$, $a_4$, and $a_3$. Table 8 is full recovery strategies, and Table 9 is partial recovery strategies. In Tables 8 and 9, since the total number of failed arcs $N_f$ is 3, the maximum value of $N_{tr}$ and $T_{tr}$ is 3. It can be seen from Tables 8 and 9 that when the number of recovery stages is fewer and the number of recovery arcs is greater, the dynamic network resilience is greater, but the recovery cost is also greater.

At this step, we can obtain different protection strategies, different attack strategies, and dynamic network resilience under different recovery strategies, as well as the cost of our protection and recovery of the network. The decision maker can get the result of the combination of the importance weight of the arcs and all the strategies, and make relevant decisions. For example, if only based on the importance of arcs, decision makers can quickly determine the priority of protecting and recovering arcs. Based on the results of all the strategy combinations, we can look at all strategies and get a strategy combination ($N_{tr}$, $N_f$, and $T_{tr}$) with high dynamic network resilience and low cost.

For example, if the dynamic network resilience is required to be as large as possible, the top 10 full recovery and partial recovery strategies can be obtained as shown in Tables 10 and 11, respectively. It can be seen from Table 10 that only the costs of the 4th, 7th, 8th, and 10th full recovery strategy are less than or equal to 150. From Table 11, it can be seen that only the costs of the 1st, 5th, and 10th partial recovery strategies are greater than 150. It is worth noting that the $\phi = 200$ means that the network is not failed when it is attacked under the protection strategy, so there is no need to recover the network.
If the cost is required to be as small as possible, the top 10 full recovery and partial recovery strategies can be obtained as shown in Tables 12 and 13, respectively. However, in Table 12, the dynamic network resiliencies of the 4th, 5th, 6th, and 9th full recovery strategies are all less than 100. In Table 13, it is obvious that only the dynamic network resiliencies of 8th and 9th partial recovery strategies are greater than 100. Note that $\Psi_D = 100$ means that the network is recovered to an operational state.

If the dynamic network resilience is required to be above 100 and the cost is as small as possible, then the top 10 full recovery and partial recovery strategies can be obtained as shown in Tables 13 and 15, respectively. From the perspective of actual implementation, the strategies in Tables 14 and 15 are more likely to be adopted by decision makers because the dynamic network resilience is acceptable and the cost is low.

### 4. Case Study

This study uses the proposed time-related BATRA to analyse a case: the wildfire wireless detection sensor network, which is an important infrastructure network. The example network in Fig. 2 with only four nodes and five arcs is also called the bridge.
Table 14: Full recovery strategies for all \(X_{d_i}'\) with \(\varphi_D > 100\) and ranked by sumCost.

| Rank | \(X_{d_i}'\) | \(N_p\) | \(N_i, T_i\) | \(\varphi_D\) | sumCost |
|------|-------------|--------|--------|--------|--------|
| 1    | 00000       | 2      | -      | 200    | 55     |
| 2    | 00100       | 2      | (1, 1) | 129.6789 | 105 |
| 3    | 10000       | 2      | (1, 1) | 117.2033 | 105 |
| 4    | 00000       | 3      | -      | 200    | 110    |
| 5    | 00010       | 2      | (1, 1) | 118.2737 | 115 |
| 6    | 10100       | 2      | (2, 1) | 134.8399 | 145 |
| 7    | 00110       | 2      | (2, 1) | 134.8399 | 145 |
| 8    | 10010       | 2      | (2, 1) | 121.7144 | 145 |
| 9    | 10100       | 2      | (2, 2) | 210.322 | 150 |
| 10   | 00110       | 2      | (2, 2) | 210.322 | 160 |

Table 15: Partial recovery strategies for all \(X_{d_i}'\) with \(\varphi_D > 100\) and ranked by sumCost.

| Rank | \(X_{d_i}'\) | \(N_p\) | \(N_i, T_i\) | \(\varphi_D\) | sumCost |
|------|-------------|--------|--------|--------|--------|
| 1    | 00110       | 2      | (2, 1) | 104.6428 | 115 |
| 2    | 10100       | 2      | (2, 1) | 104.6428 | 115 |
| 3    | 00110       | 2      | (2, 2) | 148.2457 | 130 |
| 4    | 10100       | 2      | (2, 2) | 148.2457 | 130 |
| 5    | 10010       | 2      | (2, 2) | 145.5271 | 130 |
| 6    | 10110       | 2      | (3, 1) | 121.0211 | 130 |
| 7    | 10110       | 2      | (3, 1) | 209.4894 | 150 |
| 8    | 00110       | 3      | (2, 1) | 104.6428 | 170 |
| 9    | 10110       | 2      | (3, 3) | 216.3283 | 180 |
| 10   | 00110       | 3      | (2, 2) | 148.2457 | 185 |

The proposed time-related BATRA is applied to analyse the dynamic network resilience. The model was run on a personal computer with an Intel Core-i7 CPU @ 2.20 GHz and 8 GB of RAM. The code was implemented in RStudio Version 1.2.1335. The following is the analysis procedure.

**Input:** \(G(V, E, D)\), arc protect and recovery costs in Fig. 4 and Tables 16 and 17.

**Output:** Network protect, attack, and recovery strategies with dynamic network resilience and costs.

**STEP A.** Apply the BATRA algorithm to find the importance weight of each arc.

**STEP A1.** Obtain original network reliability \(R_0\).

In Fig. 4, there are 2048 different possible state vectors found by binary-division tree. After PLSA, 639 connected state vectors are verified. Then, the original network \(R_0 = 0.99188\) can be acquired by reliability calculation of the connected state vectors. We also can obtain \(n_p = 3\) and \(n_i = 2\) in Fig. 4.

**STEP A2.** Obtain vulnerability \(R_s\).

There are 11 different scenarios with different failed arcs in Fig. 4. By using the connected state vectors derived from **STEP A1**, \(R_s\) for different failed arcs can be obtained and summarized in Table 18.

**STEP A3.** Obtain recoverability \(R_r\).

By considering full or partial recovery variable cost and the largest ratio of recovery reliability to cost, we can obtain \(R_r\) as shown in Table 18.

**STEP A4.** Calculate importance weight of each arc using equation (1).

After obtaining \(R_0\), \(R_s\), and \(R_r\), the importance weight of each arc, \(I_i\), can be calculated using equation (1) and as shown in Table 18. From Table 18, we can obtain the importance of arcs from high to low as: \(a_4, a_8, a_9, a_{10}, a_{11}, a_5, a_1, a_2, a_6, a_7\), and \(a_3\).

**STEP B.** Decide total number of protected arcs and the protected arcs with protect costs.

After obtaining \(I_i\), we can decide total number of protected arcs and the protected arcs with protection costs using equations (5) and (6). Table 19 shows all the \(X_{p_i}\) obtained in Fig. 4. In Table 19, we can find that there are five possible values from 2 to 5 for \(N_p\), their corresponding \(X_{p_i}\), and their related SumCp. For example, according to the order of the importance weight of the arcs from high to low, if \(N_p = 2\), the first two arcs with the highest importance weight are \(a_4\) and \(a_8\). If \(N_p = 3\), the first three arcs with the highest importance weight are \(a_4, a_8, a_9\), and so on.

**STEP C.** Decide total number of attacked arcs and the attacked arcs.

---

**Figure 4:** The wildfire wireless detection sensor network (Su & Yeh, 2020).
Table 16: Arc success probability and recovery variable cost in Fig. 4.

| A       | Pr(a) | Cr(a) | Pr'(a) | Cr'(a) | a       | Pr(a) | Cr(a) | Pr'(a) | Cr'(a) |
|---------|-------|-------|--------|--------|---------|-------|-------|--------|--------|
| a_1 = e_1,2 | 0.98  | 3     | 0.80   | 2.3    | a_7 = e_4,5 | 0.88  | 3.2   | 0.70   | 2.4    |
| a_2 = e_1,4 | 0.95  | 6     | 0.75   | 4.5    | a_8 = e_6,6 | 0.92  | 3.6   | 0.85   | 3.4    |
| a_3 = e_2,3 | 0.90  | 2.4   | 0.70   | 1.6    | a_9 = e_5,8 | 0.90  | 2.9   | 0.85   | 2.7    |
| a_4 = e_2,7 | 0.99  | 4.5   | 0.85   | 4.0    | a_10 = e_6,7 | 0.98  | 6.5   | 0.82   | 6      |
| a_5 = e_3,4 | 0.85  | 3     | 0.75   | 2.2    | a_11 = e_7,8 | 0.95  | 2.8   | 0.88   | 2.1    |
| a_6 = e_3,5 | 0.85  | 2.5   | 0.70   | 1.9    | -       | -     | -     | -      |        |

Table 17: Arc protect variable cost in Fig. 4.

| A   | Cp(a) | Np | Cr(Np) | Tr | Crf(Tr) |
|-----|-------|----|--------|----|---------|
| a_1 | 2.5   | 1  | 1      | 1  | 2       |
| a_2 | 5     | 2  | 3      | 2  | 3       |
| a_3 | 6     | 3  | 5      | 3  | 6       |
| a_4 | 7.2   | 4  | 8      | 4  | 12      |
| a_5 | 5     | 5  | 13     | 5  | 18      |
| a_6 | 3.6   | 6  | 18     | 6  | 26      |
| a_7 | 3.2   | 7  | 22     | 7  | 32      |
| a_8 | 3.6   | 8  | 30     | 8  | 40      |
| a_9 | 4     | 9  | 36     | 9  | 47      |
| a_10| 6.5   | 10 | 45     | 10 | 52      |
| a_11| 5.5   | 11 | 52     | 11 | 56      |

Table 18: Importance weight of each arc in Fig. 4.

| Failed arc | Rd | Rr | I(a_k) | Failed arc | Rd | Rr | I(a_k) |
|------------|----|----|--------|------------|----|----|--------|
| a_1        | 0.01843 | 0.76905 | 0.77109 | a_7        | 0.11768 | 0.75166 | 0.72521 |
| a_2        | 0.04839 | 0.74802 | 0.74153 | a_9        | 0.07899 | 0.99188 | 1       |
| a_3        | 0.09856 | 0.72452 | 0.70071 | a_9        | 0.09462 | 0.99188 | 1       |
| a_4        | 0.00974 | 0.99188 | 1       | a_10       | 0.01974 | 0.99188 | 1       |
| a_5        | 0.14873 | 0.80831 | 0.78228 | a_11       | 0.04337 | 0.84571 | 0.84589 |
| a_6        | 0.14812 | 0.76818 | 0.73488 |            |        |    |        |

Table 19: All the Xp obtained in Fig. 4.

| I | Np  | Xp   | sumCPp |
|---|-----|------|--------|
| 1 | 2   | (0, 0, 0, 1, 0, 0, 1, 0, 0) | 13.8   |
| 2 | 3   | (0, 0, 0, 0, 0, 0, 1, 1, 1) | 19.8   |
| 3 | 4   | (0, 0, 0, 0, 0, 0, 1, 0, 0) | 29.3   |
| 4 | 5   | (0, 0, 0, 1, 0, 0, 0, 1, 1) | 39.8   |
| 5 | 6   | (0, 0, 0, 1, 1, 0, 0, 0, 0) | 49.8   |

Next, we need to decide Na. We can obtain Na = 2, 3, or 4 using equation (7). Then, we can obtain all the Xa in Fig. 4 with n_c and Na as shown in Table 20. Obviously, the number of attack strategies is far more than the protection strategies, because the attacker does not know the importance of the arcs and the protection of the arcs. In order to conform to the position of the attacker, all possible attack strategies of the attacker will be discussed here. It can be seen that when we master the importance weight of arcs, we can greatly reduce the number of strategies that need to be discussed.

According to Tables 19 and 20, the protection strategy and the attack strategy can be obtained, respectively. Each protection strategy in Table 19 will correspond to so many attack strategies in Table 20. By “subtracting” the vector values of the protection strategy and the attack strategy, the failed arcs can be obtained. After subtraction and conversion, we can obtain Xdv' that can correspond to the calculation result of the failed arc scenario in STEP A. There are totally 256 different Xdv'.
**Table 21:** Full recovery strategies for Xd_{66}' under Xp_1 to Xp_5.

| Rank | Xd_{66}' | N_p | N_a | N_f | N_{i}, T_r | v_D | sumCost |
|------|----------|-----|-----|-----|------------|-----|---------|
| 1    | 00001110100 | 2   | 2, 3, or 4 | 4   | (4, 4)     | 400.103 | 43.3    |
| 2    | 00001110100 | 2   | 2, 3, or 4 | 4   | (4, 4)     | 400.103 | 43.3    |
| 3    | 00001110100 | 3   | 2, 3, or 4 | 4   | (4, 4)     | 400.103 | 49.3    |
| 4    | 00001110100 | 3   | 2, 3, or 4 | 4   | (4, 4)     | 400.103 | 49.3    |
| 5    | 00001110100 | 4   | 2, 3, or 4 | 4   | (4, 4)     | 400.103 | 58.8    |
| 6    | 00001110100 | 4   | 2, 3, or 4 | 4   | (4, 4)     | 400.103 | 58.8    |
| 7    | 00001110100 | 5   | 2, 3, or 4 | 4   | (4, 4)     | 400.103 | 69.3    |
| 8    | 00001110100 | 5   | 2, 3, or 4 | 4   | (4, 4)     | 400.103 | 69.3    |
| 9    | 00001110100 | 6   | 2, 3, or 4 | 4   | (4, 4)     | 400.103 | 79.3    |
| 10   | 00001110100 | 6   | 2, 3, or 4 | 4   | (4, 4)     | 400.103 | 79.3    |

**STEP D.** Decide total number of recovered arcs, and the number of arcs recovered per unit time with recovery costs, and then obtain the corresponding network resilience using equation (3).

According to N_{i} obtained in the previous step, we can find N_{i} and T_r using equations (9) and (10), and their combinations by using the multistate binary-addition tree. Then, we can intelligently recover the arcs according to the importance weights of the arcs obtained by STEP A, and calculate the dynamic network resilience according to the proposed formula in equation (3). There are totally 9405 different recovery strategies with their dynamic network resilience, v_D, and total recovery costs, sumCr, from the combinations of N_{i}, N_a, N_f, and T_r. The total CPU running time is 493.44 seconds.

For example, Tables 21 and 22 show the recovery strategies for Xd_{66}' under Xp_1 to Xp_5, where Xd_{66}' = (0, 0, 0, 0, 1, 1, 0, 0, 0) and represents failed a_5, a_6, and a_7, and Xp_1 to Xp_5 are shown in Table 19. Table 21 is full recovery strategies, and Table 22 is partial recovery strategies. Note that to save table space, we abbreviate (0, 0, 0, 0, 1, 1, 0, 0, 0) as 00 001 110 000 in Tables 21 and 22. According to the importance weight of the arc calculated by STEP A, the order of arc recovery for Xd_{66}' is a_5, a_6, and a_7, which can be seen via the changes of Xr_{uv}(t). Also, each Xr_{uv}(t)
Figure 5: Resilience and sumCost with $T_r$, $N_p$, sumCp, $N_r$, sumCr, and $N_f$ in full recovery strategies.

- (a) Resilience, sumCost, and $T_r$
- (b) Resilience, sumCost, and $N_p$
- (c) Resilience, sumCost, and sumCp
- (d) Resilience, sumCost, and $N_r$
- (e) Resilience, sumCost, and sumCr
- (f) Resilience, sumCost, and $N_f$

has its corresponding $R_d(t)$. In Tables 21 and 22, since the total number of failed arcs $N_f$ is 3, the maximum value of $N_r$ and $T_r$ is 3. It can be seen from Tables 21 and 22 that when both $T_r$ and $N_r$ are greater, the dynamic network resilience is greater, but the recovery cost is also greater.

At this step, we can obtain different protection strategies, attack strategies, and dynamic network resilience under different recovery strategies, as well as the cost of our protection and recovery of the network. The decision maker can get the result of the combination of the importance weight of the arcs and all the strategies, and make relevant decisions. For example, if only based on the importance of arcs, decision makers can quickly determine the priority of protecting and recovering arcs. If the dynamic network resilience is required to be as large as possible and the cost is as small as possible, the top 10 full recovery and partial recovery strategies can be obtained as shown in Tables 23 and 24, respectively. It is obvious from Tables 23 and 24 that both $N_r$ and $T_r$ have the largest $\phi_D = 400.103$ or $353.7295$ when the maximum value is 4. Both $N_r$ and $T_r$ are at the maximum value of 4 because in this example, the maximum value
of \( N_f \) is 4. Also, when \( N_f \) and \( T_r \) are both 4, the total cost will vary with \( X_{d_{i}}' \) or \( N_p \), because it is affected by the cost of the arcs that need to be recovered or protected. It can also be found from the table that \( N_f \) is all 2, 3, or 4, because even if \( N_f \) corresponds to different \( N_p \), the same \( X_{d_{i}}' \) may still be obtained. However, just observing at the top 10 in this example can only provide the above discussion. Therefore, then we will present the results of all 9405 strategy combinations via figures and discuss them further.

Figures 5 and 6 provide scatter diagrams of dynamic network resilience \( \phi_D \) and sumCost with \( T_r, N_f, \text{sumCp}, N_r, \text{sumCr}, \text{and } N_f \) in full and partial recovery strategies, respectively. It can be seen from Fig. 5a that when the resilience is above 100, the resilience is obviously affected by \( T_r \). For example, when the resilience is around 100, \( T_r \) is all 1. When the resilience is around 200, \( T_r \) is all 2. When the resilience is around 300, \( T_r \) is all 3. When the resilience is around 400, \( T_r \) is all 4. However, when the resilience is below 100, the effect of \( T_r \) on the resilience is not significant.

![Figure 6](image-url)
Regardless of the value of resilience, the effect of $T_r$ on $\text{sumCost}$ is not significant.

From Fig. 5b and c, we can see that $\text{sumCost}$ is obviously affected by $N_p$ or $\text{sumCp}$. For example, when $\text{sumCost}$ is between about 20 and 40, $N_p$ is 2 and $\text{sumCp}$ is 13.8. When $\text{sumCost}$ is between about 25 and 45, $N_p$ is 3 and $\text{sumCp}$ is 19.8. When $\text{sumCost}$ is between about 35 and 55, $N_p$ is 4 and $\text{sumCp}$ is 29.3. When $\text{sumCost}$ is about 45 to 65, $N_p$ is 5 and $\text{sumCp}$ is 39.8. When $\text{sumCost}$ is between about 55 and 80, $N_p$ is 6 and $\text{sumCp}$ is 49.8. $N_p$ and $\text{sumCp}$ have a high degree of positive correlation, because when $N_p$ is determined, $\text{sumCp}$ will be determined accordingly. Regardless of the value of $\text{sumCost}$, the effect of $N_p$ or $\text{sumCp}$ on resilience is not significant.

From Fig. 5d, e, and f, we can see that resilience is also affected by $N_r$, $N_r$, or $\text{sumCr}$, but it does not have a significant effect on resilience like $T_r$. When $N_r$ is 4, the resilience is significantly higher than that of $N_r$ less than 4. It can be seen that recovering the four arcs can significantly improve resilience. Also, in this example, the protection cost $\text{sumCp}$ affects $\text{sumCost}$ to a greater extent than the recovery cost $\text{sumCr}$. Therefore, for this example, recovering more arcs can cause the resilience greater and the recovery cost will not increase significantly.

$N_p$, $N_r$, and $\text{sumCr}$ have a high degree of positive correlation, because $N_r$ determines the maximum value of $N_r$, and when $N_r$ is determined, $\text{sumCr}$ will also be determined. Regardless of the value of $\text{sumCost}$, the effect of $N_p$, $N_r$, or $\text{sumCr}$ on resilience is not significant. In addition, when the resilience is less than 100, there are many points where $N_r$ is 4. The reason is that at these points, $N_r$ is large but $N_p$ is not large enough. Therefore, the network is not effectively recovered to an operational state, resulting in low resilience.

The relationship between the variables or parameters shown in Fig. 6 can also be echoed with the previous discussion on Fig. 5. Moreover, the top 10 best solutions we found in Tables 23 and 24 are all in Figs 5 and 6 with a maximum resilience of 400.103 and 353.7295, respectively.

5. Conclusion

In this article, we proposed a new performance measure oriented to the degree of network reliability recovery to quantify the resilience of the network system and a dynamic resilient model with more decision variables, parameters, and cost formulations for critical infrastructure network systems against disruptive events. The proposed dynamic resilience performance measure does not need to assume that the system needs to be recovered to the original state, and is more in line with practical applications. In addition, the proposed time-related BATRA was applied to overcome the complexity of the problem model, obtain protection, attack, and recovery strategies, and calculate the final dynamic network resilience and related cost. An example is provided to illustrate the analysis process of the proposed time-related BATRA. This article also provides a case study of the wildfire wireless sensor network. In the illustrated examples or case studies, the proposed time-related BATRA not only assists decision makers in the allocation of protection and recovery resources, but also provides the best solutions, including maximizing resilience, minimizing costs, and maximizing resilience and minimize cost, or maximize resilience or minimize cost under given resilience or cost constraints.

In addition, in the case study, we discussed the impact of decision variables on the development of protection and recovery strategies and on network resilience and costs. Regardless of the protection or recovery strategy, the importance weight of the arcs does determine the priority of the protection or recovery of the arcs. Network resilience is significantly affected by $N_p$, $N_r$, and $T_r$. If $N_p$, $N_r$, and $T_r$ are all large, the network usually has high resilience, because the damaged arcs can be recovered effectively and instantly. If $N_p$ is large but $N_r$ and $T_r$ are not large enough, the network usually has low resilience, because the damaged arcs are not effectively and instantly recovered. The total cost consists of protection and recovery costs. If the decision maker hopes that the cost is as small as possible, and if the proportion of the protection cost is greater than the recovery cost, then the decision maker should focus on the recovery aspect. Conversely, if the proportion of recovery costs is greater than the protection costs, then decision makers should focus on the protection aspect. The results of this study can help decision makers formulate protection and recovery strategies to ensure that the infrastructure is operated to meet the needs of serving society.

For future research, the predictive maintenance for infrastructure can be applied. Then, the computational efficiency of more complex networks can be further improved. Different from the exact solution obtained by this research method, the complex network tends to obtain a better solution close to the exact solution. Because of the huge amount of calculation in complex networks, more advanced algorithms are usually used, such as optimized heuristic algorithms, hidden Markov models, or a more complex and robust percolation theory. In addition, there are too many variables to be considered in the resilient model. Future research can further incorporate all variables or explore the relationship between factors to make the resilient model more complete. Another important issue is the problem of multi-objective planning. Such a resilient infrastructure model may need to consider more goals in the future, such as static network resilience, dynamic network resilience, protection cost, recovery cost, total cost, etc. How to discuss between multiple goals and choose the most suitable solution for decision makers are important issues.

Acknowledgments

We acknowledge the editor and the referees for their constructive comments and recommendations and the support of National Tsing Hua University.

Conflict of interest statement

None declared.

References

Avci, O., & Ozbulut, O. (2018). Threat and vulnerability risk assessment for existing subway stations: A simplified approach. Case Studies on Transport Policy, 6(4), 663–673.
Aven, T. (1988). Some considerations on reliability theory and its applications. Reliability Engineering & System Safety, 21(3), 215–223.
Calvert, S. C., & Snelder, M. (2018). A methodology for road traffic resilience analysis and review of related concepts. Transportmetrica A: Transport Science, 14(1–2), 130–154.
Colbourn, C. J. (1987). The combinatorics of network reliability. Oxford University Press, Inc.
Gomez, C., & Baker, J. W. (2019). An optimization-based decision support framework for coupled pre-and post-earthquake
infrastructure risk management. *Structural Safety*, 77, 1–9.

González, A. D. et al. (2016). The interdependent network design problem for optimal infrastructure system restoration. *Computer-Aided Civil and Infrastructure Engineering*, 31(5), 334–350.

Hajian, M., Melachrinoudis, E., & Kubat, P. (2016). Modeling wildfire propagation with the stochastic shortest path: A fast simulation approach. *Environmental Modelling & Software*, 82, 73–88.

Hao, Z. et al. (2020). A novel convolution-based algorithm for the acyclic network symbolic reliability function problem. *IEEE Access*, 8, 99337–99345.

Hao, Z., Yeh, W.-C., & Tan, S.-Y. (2021). One-batch preempt deterioration-effect multi-state multi-rework network reliability problem and algorithms. *Reliability Engineering & System Safety*, 215, 107883.

Hosseini, S., & Barker, K. (2016). Modeling infrastructure resilience using Bayesian networks: A case study of inland waterway ports. *Computers & Industrial Engineering*, 93, 252–266.

Hosseini, S., & Ivanov, D. (2019). A new resilience measure for supply networks with the ripple effect considerations: A Bayesian network approach. *Annals of Operations Research*, 1–27. doi:10.1007/s10479-019-03350-8.

Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016a). A review of definitions and measures of system resilience. *Reliability Engineering & System Safety*, 145, 47–61.

Hosseini, S., Al Khaled, A., & Sarder, M. D. (2016b). A general framework for assessing system resilience using Bayesian networks: A case study of sulfuric acid manufacturer. *Journal of Manufacturing Systems*, 41, 211–227.

Hosseini, S., Ivanov, D., & Dolgui, A. (2019). Review of quantitative methods for supply chain resilience analysis. *Transportation Research Part E: Logistics and Transportation Review*, 125, 285–307.

Hsieh, C.-H., & Feng, C.-M. (2020). The highway resilience and vulnerability in Taiwan. *Transport Policy*, 87, 1–9.

Hubbard, S. M. L., & Hubbard, B. (2019). A review of sustainability metrics for the construction and operation of airport and roadway infrastructure. *Frontiers of Engineering Management*, 6(3), 433–452.

Jia, C., & Zhang, C. (2020). Joint optimization of maintenance planning and workflow routing for a geographically distributed networked infrastructure. *IISE Transactions*, 52(7), 732–750.

Kabadurmus, O., & Smith, A. E. (2017). Evaluating reliability/survivability of capacitated wireless networks. *IEEE Transactions on Reliability*, 67(1), 26–40.

Levitin, G. (2005). *The universal generating function in reliability analysis and optimization* (Vol. 6). Springer.

Liu, X. et al. (2016). Microgrids for enhancing the power grid resilience in extreme conditions. *IEEE Transactions on Smart Grid*, 8(2), 589–597.

Markolf, S. A. et al. (2019). Transportation resilience to climate change and extreme weather events—Beyond risk and robustness. *Transport Policy*, 74, 174–186.

Monroe, J., Ramsey, E., & Berglund, E. (2018). Allocating countermeasures to defend water distribution systems against terrorist attack. *Reliability Engineering & System Safety*, 179, 37–51.

Pant, R. et al. (2014). Stochastic measures of resilience and their application to container terminals. *Computers & Industrial Engineering*, 70, 183–194.

Perera, C., Liu, C. H., & Jayawardena, S. (2015). The emerging internet of things marketplace from an industrial perspective: A survey. *IEEE Transactions on Emerging Topics in Computing*, 3(4), 585–598.

Poulin, C., & Kane, M. (2021). Infrastructure resilience curves: Performance measures and summary metrics. *preprint arXiv:2102.01009*.

Rocco, C. M. et al. (2018). Community detection and resilience in multi-source, multi-terminal networks. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 232(6), 616–626.

Rose, A. (2007). Economic resilience to natural and man-made disasters: Multidisciplinary origins and contextual dimensions. *Environmental Hazards*, 7(4), 383–398.

Sharma, N., Tabandeh, A., & Gardoni, P. (2020). Regional resilience analysis: A multiscale approach to optimize the resilience of interdependent infrastructure. *Computer-Aided Civil and Infrastructure Engineering*, 35(12), 1315–1330.

Smith, A. M. et al. (2020). Interdependent network recovery games. *Risk Analysis*, 40(1), 134–152.

Su, Yi.-Z., & Yeh, W.-C. (2020). Binary-addition tree algorithm-based resilience assessment for binary-state network problems. *Electronics*, 9(8), 1207.

Szarata, A., & Hoy, K. N. (2019). The impact of road infrastructure failures on traffic conditions and travel behaviour in urban areas—the case of the Lazienkowski Bridge in Warsaw. In *MATEC Web of Conferences* (Vol. 284, pp. 01006). EDP Sciences.

Trotter, M. J., & Ivory, V. (2019). A systems-based framework as an engagement tool: Adaptation for insight on transport network resilience. *Case Studies on Transport Policy*, 7(2), 167–178.

Wikipedia(2021). Xingda power plant shutdown accident in 2021. [https://zh.wikipedia.org/wiki/2021%E5%B9%B4%E8%88%98%E9%94%AE%E7%99%BC%E9%9B%B8%E5%B8%A0%E5%81%9C%E6%A9%9F%E4%BA%8B%E5%95%85], accessed 6, 24.

Xu, Z. et al. (2020). A new resilience-based component importance measure for multi-state networks. *Reliability Engineering & System Safety*, 193, 106591.

Yeh, W.-C. (2020a). Novel binary-addition tree algorithm (BAT) for binary-state network reliability problem. *Reliability Engineering & System Safety*, 208, 107448.

Yeh, W.-C. (2020b). Novel bounded binary-addition tree algorithm for binary-state network reliability problems. *preprint arXiv:2011.14832*.

Yeh, W.-C. (2021). Novel algorithm for computing all-pairs homogeneity-arc binary-state undirected network reliability. *preprint arXiv:2105.01500*.

Yeh, W.-C., & Kuo, C.-C. (2020). Predicting and modeling wildfire propagation areas with BAT and maximum-state PageRank. *Applied Sciences*, 10(23), 8349.

Yeh, W.-C. et al. (2021). Novel binary-addition tree algorithm for reliability evaluation of acyclic multistate information networks. *Reliability Engineering & System Safety*, 210, 107427.

Youn, B. D., Hu, C., & Wang, P. (2011). Resilience-driven system design of complex engineered systems. *Journal of Mechanical Design*, 133(10), 101011.

Zhang, C., Ramirez-Marquez, J. E., & Wang, J. (2015). Critical infrastructure protection using secrecy—A discrete simultaneous game. *European Journal of Operational Research*, 242(1), 212–221.

Zhu, H. et al. (2021). The Integration of protection, restoration, and adaptive flow redistribution in building resilient networked critical infrastructures against intentional attacks. *IEEE Systems Journal*, 15(2), 2959–2970.