Complex & Intelligent Systems (2024) 10:3197–3211
https://doi.org/10.1007/s40747-023-01316-9

ORIGINAL ARTICLE

A communication-based identification of critical drones in malicious drone swarm networks

Min Teng[1] · Chao Gao[2] · Zhen Wang[2] · Xuelong Li[2]

Received: 27 June 2023 / Accepted: 7 December 2023 / Published online: 17 January 2024

Abstract

Accurate identification of critical malicious drones is crucial for optimizing directed energy attacks and maximizing their effectiveness. However, current studies on critical drone identification are still in the preliminary stage and almost rely on the traditional centrality methods that do not address the distributed features of drone swarms. This leads to inaccurate identification of critical drones, resulting in the low efficiency of directed energy attacks. Therefore, this paper proposes a new critical drone identification method based on the distributed features, communication intensity, and communication scale of drones. Specifically, this paper first constructs a dynamic communication prediction network (DCPN) of drone swarms based on the 3D position and interaction range, which predicts the dynamic communication between drones. Then, this paper proposes a new method called dynamic giant connected component (GCC)-based scale-intensity centrality (DGSIC) that combines the local, global, and community structure of DCPN to identify critical nodes with stronger communication capabilities. The dynamic strategy involves the iterative identification of one critical node at each step, considering the evolving network configuration and ensuring the identified node remains the most critical in the present network. Additionally, the prioritization strategy is employed to identify the nodes within the GCC, which can significantly impact the network connectivity and communication. DGSIC optimizes the attack sequence for directed energy attacks, facilitating the rapid dissolution of malicious drone swarms. Extensive experiments in four simulated networks and eight real-world networks demonstrate the superior robustness and cascading failure performance of DGSIC.

Keywords Malicious drone swarm · Dynamic communication · Community structure · Critical drone

Introduction

The rapid development of micro drone swarms has brought convenience to areas such as urban planning and disaster management [1]. Meanwhile, it has also provided new means for terrorist and military activities, including surveillance and attacks [2]. These malicious incidents have demonstrated the significant threat posed by drone swarms, which seriously endanger the privacy, property, and even the safety of residents, sounding the alarm for low-altitude defense. From then on, research on anti-drone swarms has gradually gained attention.

The anti-drone swarm system consists of two primary components: drone detection and drone attack. Drone detection research has reached a relatively mature stage and can achieve precise detection [3]. Research on drone attacks can be categorized into three main types: non-kinetic energy interference, intensive firepower attack, and directed energy attack [4]. Among them, directed energy attacks are particularly well-suited for low-altitude battlefield defense due to the advantages of precise targeting, low cost, quick response, and minimal environmental interference [2]. Consequently, they have become the mainstream equipment and key focus of anti-drone swarm researches [5, 6]. However, the current

✉ Chao Gao
cgao@nwpu.edu.cn

✉ Zhen Wang
w-zhen@nwpu.edu.cn

Min Teng
ttengmin@mail.nwpu.edu.cn

Xuelong Li
li@nwpu.edu.cn

[1] School of Cybersecurity, Northwestern Polytechnical University(NWPU), Xian 710072, Shaanxi, China

[2] School of Artificial Intelligence, Optics and Electronics (iOPEN), Northwestern Polytechnical University(NWPU), Xian 710072, Shaanxi, China

research on directed energy attacks predominantly concentrates on optimizing the hit rate when targeting specific drones [7–9], often overlooking the optimization of attack sequences. Additionally, the adaptive cooperation of malicious drone swarms following each directed energy attack is underexplored [10, 11]. Therefore, capturing the dynamic collaboration of malicious drones, achieving the precise identification of critical drones, and devising efficient sequences for directed energy attacks are of utmost importance in significantly countering malicious drone swarms.

Communication plays a vital role in facilitating information exchange among drones, and it is influenced by factors such as the interaction range and positional relationship [12]. Considering the high mobility of drones, it becomes necessary to establish a dynamic communication model that can capture the changing communication in drone swarms. Traditional models such as agent-based models [13, 14], Bayesian network-based models [15, 16], and system dynamics [17, 18] have limitations in effectively representing the dynamic communication of drone swarms [19]. However, the development of complex network theory provides a new perspective for complex system modeling, where drones can be abstracted as nodes and communication between drones can be represented as edges [20, 21]. The dynamic communication prediction network (DCPN) model of a drone swarm can be established by tracking the changes in edges. Utilizing the DCPN, critical drones can be identified using critical node identification algorithms. In this paper, critical drones refer to nodes that are significant to the structure and function of DCPN, and their failure can damage the connectivity, communication intensity, and communication scale of the network. However, few studies focus on critical node identification in DCPN, and less attention has been simultaneously given to the distributed features, communication intensity, and communication scale of drones. Consequently, the accuracy of critical drone identification is limited.

To address the limitation, this paper focuses on distributed and dynamic communication features and proposes a new method for identifying critical drones. Specifically, this paper first constructs a communication prediction network model to capture the dynamic communication among drones. Then, considering the distributed features, communication intensity, and communication scale of drones, a new critical node identification method incorporating the local, global, and community structure is proposed to enhance the effectiveness of directed energy attacks.

The main contributions are as follows:

1. A newly extended dynamic communication prediction network (DCPN) model for drone swarms is proposed based on the spatial position relationship, which captures the dynamic changes in drones and their communication. The node features record the 3D positions of drones, and the edge features characterize the dynamic communication between them. DCPN can effectively capture the spatial position changes of drones, enabling dynamic communication prediction and automatic updates of malicious drone swarms.
2. A newly critical node identification method named dynamic GCC-based scale-intensity centrality (DGSIC) is further proposed, in combination with community structure, communication scale, and communication intensity. Additionally, dynamic and prioritization strategies are incorporated. Specifically, the network structure is dynamically updated after each directed energy attack, and the nodes within GCC are given higher priority. DGSIC optimizes the attack sequence for directed energy attacks, facilitating the rapid dissolution of malicious drone swarms.

The rest of this paper is as follows. “Related work” overviews the existing work of malicious drone swarm and critical node identification. “Proposed method” details the proposed method. “Experiments” shows the experiment results and analysis. Finally, the subsequent section shows the conclusion and future work.

Related work

In recent years, the increasing occurrence of malicious drone swarm attacks has posed a significant threat to the privacy, property, and even the safety of individuals. Therefore, it is imperative to propose a method for identifying critical drones to efficiently and accurately counter these attacks using directed energy attacks. While previous research on anti-drone metrics has mainly focused on areas such as malicious drone detection [22–24], trajectory tracking [25–27], interference [28, 29], and swarm robustness analysis [30], less attention is paid to the identification of critical drones [31]. Moreover, traditional models fail to effectively capture the dynamic communication between drones [19], leading to a scarcity of references for the identification of critical drones.

Fortunately, the complex network theory offers a new perspective for identifying critical drones [31], treating the drone swarm as a network and the drones as nodes. Existing literature primarily introduce critical node identification methods based on the complex network theory, which can be divided into three main categories, i.e., local structure-based, global structure-based, and community structure-based methods.

Local structure-based methods mainly focus on the local information of the network. For instance, the degree centrality (DC) [32], a classic method, measures the connection strength between a node and its immediate neighbors, providing a simple and effective metric of node importance [33]. To broaden the scope of local information, Chen et al. proposed an extension of DC called local centrality (LC), which takes into account the influence of third-order neighboring nodes [34]. Tee et al. introduced a local metric called vertex entropy (VE), which has demonstrated effectiveness in large commercial networks [35]. Lei et al. approached critical node identification from the perspective of Tsalli entropy and presented a new method called LSE, considering the influence of first-order and second-order neighboring nodes [36]. The results indicate that LSE exhibits improved information dissemination ability and robustness. Additionally, Wang et al. proposed a method named ALSI based on the aggregated local structure, which combines the degree and the number of layers of a node [37]. Extensive results demonstrate the superiority of ALSI in identifying critical nodes. However, these algorithms only consider the influence of a node and its neighbor nodes, without taking into account the impact of distant nodes, thereby limiting the accuracy of critical node identification.

Global structure-based methods primarily aim to capture the overall network information and can be categorized into two categories: iteration-based and path-based methods. Iteration-based methods, such as HITs [38], PageRank [39] and their variants [40, 41], consider the positional features of nodes and iteratively obtain the global information of networks. These methods effectively characterize the critical nodes with structural advantages. For instance, Jiang et al. proposed BMRank, a new critical node identification method based on the HITs, which outperforms other methods in terms of network structure [40]. Li et al. designed APAMGM, an improved centrality metric based on the PageRank, which can effectively identify the critical nodes with high interpretability [41]. However, these methods heavily rely on the iterative process, resulting in unstable performance as they often converge to the local optima. Path-based methods, such as betweenness centrality (BC) [42] and closeness centrality (CC) [43], effectively characterize the impact of distant nodes based on the shortest path and perform well in characterizing the information diffusion of nodes [44]. Besides, Zhao et al. proposed GIN, a novel method that combines DC and the shortest path algorithm to evaluate node importance [45]. Zareie et al. introduced ECRM, a method that utilizes DC and the similarity between nodes and their neighbor nodes to quantify node importance [46]. The results of GIN and ECRM demonstrate that coupling metrics are more effective than single metrics. Therefore, coupling metrics have gained attention among researchers, providing a new perspective for critical node identification.

In recent years, there has been increasing evidence linking the function of networks to community structure [47, 48]. Consequently, researchers have focused on critical node identification methods that leverage community structure to improve the accuracy of identification [49–54]. For instance, Tutu et al. designed CbM, a community-based metric that considers the entropy of a random walk from a node to each community. Simulation results have shown that nodes identified by CbM accelerate the dissemination of information [50]. Additionally, Liu et al. proposed GDF-ICN, a group-driven framework that leverages community structure to enhance the performance of critical node identification. Comprehensive experiments have confirmed the effectiveness of this approach [53]. Similarly, exploring community structure can gain insights into the organization and interactions of drone swarms, enabling the identification of critical drones that play significant roles in network communication.

In summary, the complex network theory provides a new perspective for identifying critical drones in drone swarms. Building upon this theory, this paper proposes a new method named DGSIC to accurately identify critical nodes with stronger communication capabilities in DCPN.

Proposed method

The proposed method for identifying critical nodes consists of two main parts, as depicted in Fig. 1. Initially, the drone swarm dynamic communication prediction network model is introduced in "Drone swarm dynamic communication prediction network model". Then, the formulation of DGSIC is introduced in "Formulation of the DGSIC ".

Drone swarm dynamic communication prediction network model

Amidst limited information about drone communication protocols, the accurate detection and acquisition of communication between drones pose significant challenges [55]. However, research has shown that the communication between drones is influenced by their distance and interaction range, and they cannot communicate beyond this range [56]. Additionally, considering the high mobility of drones, their distances and communications undergo frequent changes [10]. To address these challenges, this paper proposes a dynamic communication prediction network (DCPN) model based on distance. DCPN can capture the evolving communication within the drone swarm and is designed to address the communication challenges in drone swarms, particularly in cases where the communication is based on technologies like Flying Ad-Hoc Network (FANET) [57] instead of relying on ground control stations.

DCPN: The communication between drones is considered to be bi-directional, and it dynamically changes with the movement of drones. Therefore, DCPN is represented as an undirected and node load graph $G=< V, E, M >$. V is a set of nodes, where each node represents a drone, and $N=|V|$ represents the size of networks. E is a set of edges, which represents the communication between nodes. The construction

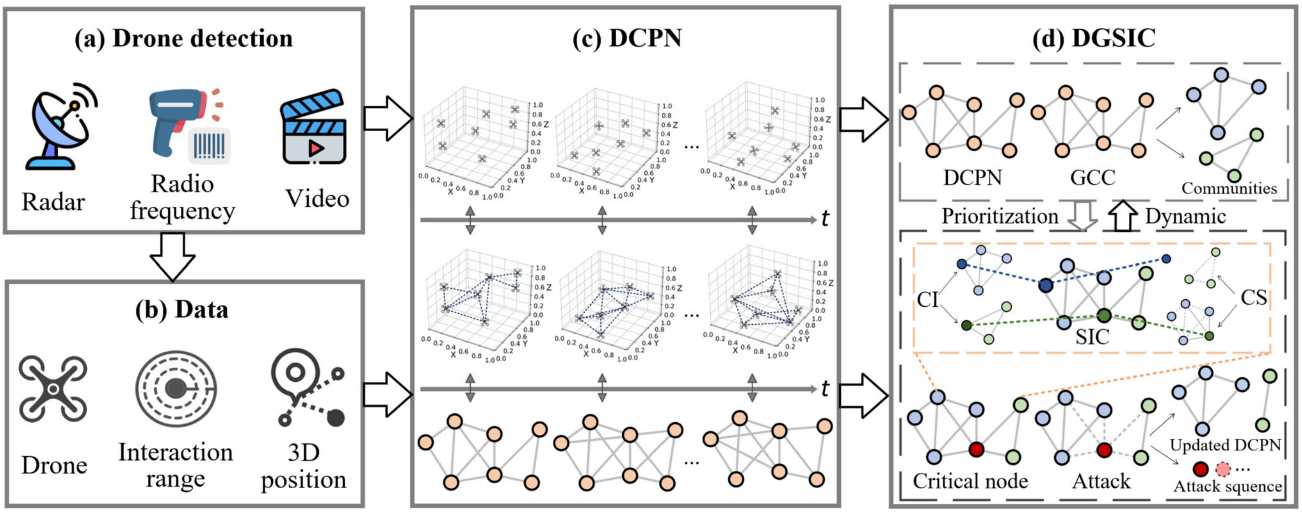


Fig. 1 The framework of DGSIC. **a** Drone detection techniques. DGSIC employs various drone detection methods to collect data from malicious drone swarms. **b** Drone swarm data. The 3D position data records the 3D positions of drones over n consecutive steps. **c** DCPN construction. DGSIC constructs the DCPN, effectively capturing the dynamic communication of malicious drone swarms. **d** Critical node identification. Firstly, DGSIC identifies the GCC of DCPN. Then, DGSIC prioritizes the most critical node within GCC based on the proposed scale-intensity centrality (SIC). Finally, DGSIC attacks the node and updates DCPN. This dynamic process continues until the DCPN is completely disintegrated

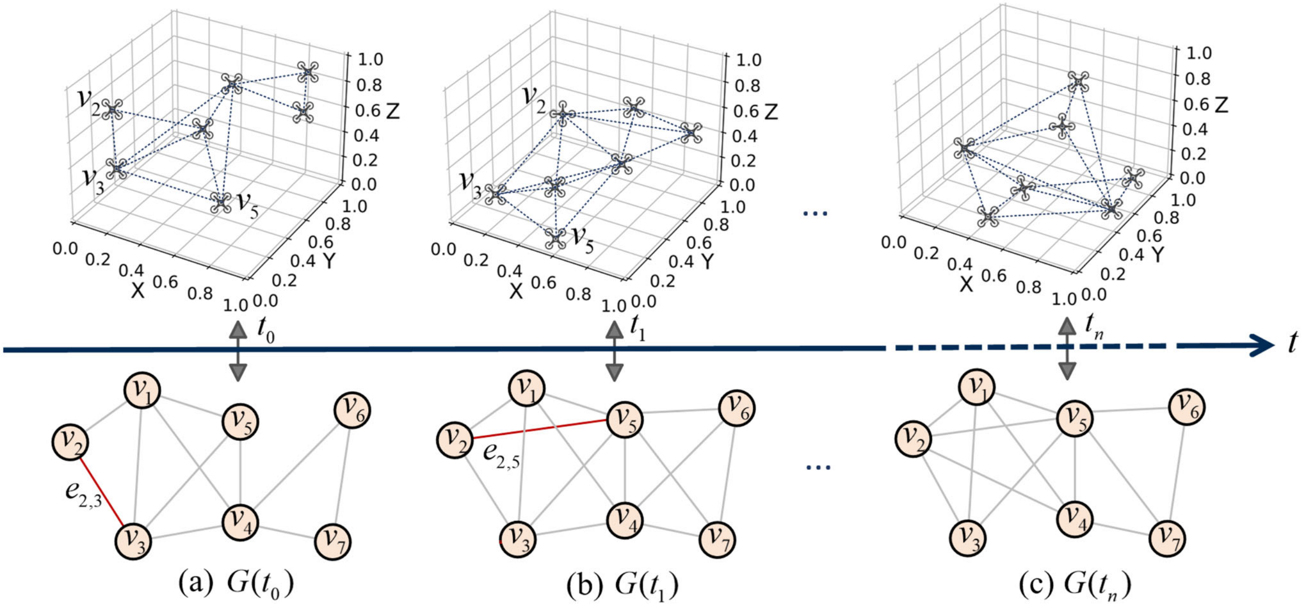


Fig. 2 An example of the dynamic topology of DCPN. **a–c** show the topology at times t_0, t_1, and t_n, respectively. The congregation area of drone swarms is set as $1 \times 1 \times 1$, the drone number N=7, and the interaction range D=0.6

of edges is based on the distance between drones and their interaction range. If the Euclidean distance $d_{i,j}$ between v_i and v_j is less than the interaction range D, whose value is variable and limited by the hardware, there is an edge $e_{i,j}$, otherwise, there is no edge. Fig. 2 shows an example of the topology of DCPN. As shown in Fig. 2(a), $d_{2,3}$ is lower than D at time t_0, that is $d_{2,3}<0.6$, so there exists $e_{2,3}$. $d_{2,5}$ is higher than D, that is $d_{2,5}>0.6$, so there is no $e_{2,5}$. To facilitate the prediction of drone positions and communication, the node feature set M is introduced. Each v_i is associated with a $n \times 3$ dimensional matrix m_i, which records the 3D position of v_i at n consecutive time steps. This information helps in predicting the future positions and communication patterns of drones. The network topology of DCPN is updated based on the real-time positions of drones. As the positions of drones change, the distances between them are updated, and the edges in DCPN are dynamically added or removed. As shown in Fig. 2(a), since $d_{2,5}$ becomes lower than D at time t_1, an edge $e_{2,5}$ is added to represent the communication between them.

Overall, DCPN provides a representation of the dynamic communication within a drone swarm by considering the distances between drones and their interaction range. It enables the prediction and analysis of communication dynamics, which is essential for identifying critical drones and optimizing the efficiency of directed energy attacks against malicious drone swarms.

Formulation of the DGSIC

The new node importance metric named SIC is introduced in "The proposed node importance metric". The dynamic and prioritization strategies are introduced in "The dynamic strategy" and "The prioritization strategy", respectively.

The proposed node importance metric

In a multi-task-oriented and distributed drone swarm, the network community structure provides a valuable framework for describing its distributed features. By identifying the community structure of DCPN, the collaborative relationship among nodes can be captured, reflecting the distributed features within malicious drone swarms. Nodes within the same community engage in frequent communication to accomplish shared tasks, while nodes bridging different communities also communicate to exchange the task-related information and expand the communication scale. Moreover, previous studies have demonstrated that critical nodes identified based on the community structure can significantly enhance information dissemination within the network. Taking inspiration from the distributed features, communication intensity, and communication scale of drones, this paper first proposes a new communication-based node importance metric called scale-intensity centrality (SIC), whose time complexity is $O(N^3)$. This metric incorporates the community structure, local information, and global information of DCPN to assess the importance of nodes.

As shown in Fig. 1(d), the first step is to identify the community structure of DCPN. More specifically, this paper employs the Louvain algorithm [58], an effective community detection method, to obtain a set of communities that capture the distributed features of drone swarms.

$$C = \{c_1, c_2, ..., c_q\} \tag{1}$$

where c_q represents the q^{th} community. Each community consists a group of nodes that exhibit strong internal connections and weaker connections with nodes outside the community. This community structure information serves as a foundation for our subsequent analysis and identification of critical nodes in DCPN.

The communication scale represents the capability of a node to communicate with other nodes from different communities, signifying its potential to expand communication beyond its own community. To quantify the communication scale of a node, this paper considers the connections with its neighbor nodes in other communities The communication scale of v_i is defined as:

$$CS(i) = \sum_{v_j \in \Gamma(i)} \delta(i, j) \tag{2}$$

where $\Gamma(i)$ represents the set of neighbor nodes of v_i, and $\delta(i, j)$ is an indicator function that returns 1 if v_j and v_i belong to different communities, and 0 otherwise. A higher value of $CS(i)$ that v_i has a larger influence on the overall communication and connectivity of DCPN by establishing connections with nodes from different communities. By incorporating the communication scale, this paper captures the distributed features and communication abilities of drones in DCPN.

The communication intensity refers to the capability of a node to communicate with other nodes within the same community. The ratio of the shortest path reflects the efficiency of node communication and information exchange within the community. Therefore, this paper quantifies the communication intensity of a node by the proportion of shortest paths that pass through the node within the community. The communication intensity of v_i is defined as:

$$CI(i) = \sum_{\substack{s \neq t \\ v_s, v_t \in C(i)}} \frac{n_{st}^i}{n_{st}} \tag{3}$$

where $C(i)$ represents the community to which node v_i belongs, n_{st}^i represents the number of shortest paths passing through v_i between v_s and v_t. n_{st} represents the total number of shortest paths between v_s and v_t. A higher value of $CI(i)$ indicates a stronger and more direct communication capability within the community. By incorporating the communication intensity, this paper captures the communication efficiency and effectiveness of drones within their respective communities.

The communication capability of a drone is mainly determined by its communication scale, and the communication intensity can promote information exchange between drones, thereby improving communication capability. Based on the above analysis, this paper takes into account the community structure, communication scale, and communication intensity of the network, and then proposes a new critical drone metric called SIC based on the communication, which is defined as Eq. (4).

$$SIC(i) = CS(i)^{1+CI(i)} \tag{4}$$

The dynamic strategy

To achieve the precise identification of critical drones, the dynamic strategy is incorporated into SIC, which addresses the adaptive communication of malicious drones. The dynamic scale-intensity centrality (DSIC) allows for the adaptation of the network topology in response to attacks, simulating the changing communication and connectivity patterns within the drone swarm.

Algorithm 1 DSIC

```
Input: Drone swarm dynamic communication prediction network DCPN, Parameter $H$;
Output: The directed energy attack sequence $A$;
Initial the $A$;
while $N>H$ do
    Detect the community structure $C = \{c_1, c_2, ..., c_q\}$ of DCPN based on Louvain algorithm;
    Initial the $CS$, $CI$, and $SIC$;
    for $i$=1 to $N$ do
        Calculate the $CS(i)$ based on Eq. (2);
        Calculate the $CI(i)$ based on Eq. (3);
        Calculate the $SIC(i)$ based on Eq. (4);
    end for
    Rank the $V$ based on the decreasing order of $SIC$;
    Add the top-1 node into $A$;
    Update the DCPN, removing the top-1 node and its associated edges;
end while
return $A$.
```

The process of DSIC to identify the critical nodes in DCPN is shown in Algorithm 1, whose time complexity is $O(N^4)$. When v_i is identified as the top-1 node, both v_i and associated edges E_i=$\{e_{i,j}|i \neq j \in [1, N]\}$ are removed from DCPN, representing the attack impact on the network topology. This process simulates the updated DCPN after each attack and is stopped when $N \leq H$. In this paper, the value of H is set as 0, thereby considering the complete disintegration of networks. In practical scenarios, H can be adjusted to other values based on the network disintegration extent. On this basis, DSIC ensures the identified node is the most critical in updated DCPN. This dynamic and iterative strategy captures the evolving features of drone swarms, thereby optimizing the attack sequence A.

Overall, DSIC empowers the identification of critical drones within dynamic drone swarms, accounting for the evolving network topology and adaptability of drone swarms.

The prioritization strategy

To further improve the efficiency and reduce the time overhead of DSIC, the prioritization strategy is incorporated. By prioritizing the identification and destruction of critical nodes within GCC, dynamic GCC-based scale-intensity centrality (DGSIC) focuses on the most influential and interconnected part of networks, thereby improving the efficiency of critical node identification.

As shown in Fig. 1(d), DGSIC solely computes the SIC values for the node set within GCC V_G=$\{v_i|v_i \in$GCC$\}$, which typically plays a crucial role in maintaining network connectivity and facilitating information exchange. N_G=$|V_G|$ is the size of GCC. Firstly, DGSIC sorts the V_G in decreasing order based on their SIC values and forms the sorted list L. Then, DGSIC selects the top-1 node from L and adds it to A. After the top-1 node is added to A, DCPN is updated. This iterative process continues until $N_G \leq H$.

Algorithm 2 DGSIC

```
Input: Drone swarm dynamic communication prediction network DCPN, Parameter $H$;
Output: The directed energy attack sequence $A$;
Initial the $A$
Identify the GCC of DCPN;
while $N_G>H$ do
    Detect the community structure $C = \{c_1, c_2, ..., c_q\}$ of GCC based on Louvain algorithm;
    Initial the $CS$, $CI$, and $SIC$;
    for $i$=1 to $N_G$ do
        Calculate the $CS(i)$ based on Eq. (2);
        Calculate the $CI(i)$ based on Eq. (3);
        Calculate the $SIC(i)$ based on Eq. (4);
    end for
    Rank the $V_G$ based on the decreasing order of $SIC$;
    Add the top-1 node into $A$;
    Update the DCPN, removing the top-1 node and its associated edges;
    Identify the GCC of updated DCPN;
end while
return $A$.
```

The process of DGSIC to identify the critical nodes in DCPN is shown in Algorithm 2, whose time complexity is $O(N \cdot N_G^3)$. By further incorporating the prioritization strategies into DSIC, the time overhead is significantly reduced. Compared to DSIC, DGSIC only necessitates the computation of node importance within GCC rather than across all nodes in the network, leading to a decrease in time overhead. Moreover, as the network gets fragmented into multiple smaller connected components due to attacks, the advantages of DGSIC become even more pronounced. Additionally, attacking the critical nodes according to DGSIC can significantly disrupt the connectivity and communication of the network. Fig. 3 provides a comparison of the top-3 and top-4 critical nodes identified using SIC and DGSIC. As shown in Fig. 3(a), when attacking the top-3 critical nodes identified by SIC and DGSIC, the damage to the network structure is the same. However, when the network becomes disconnected after attacks, the critical nodes identified by DGSIC demonstrate superior performance in terms of network disruption. In Fig. 3(b), when attacking the top-4 critical nodes identi-

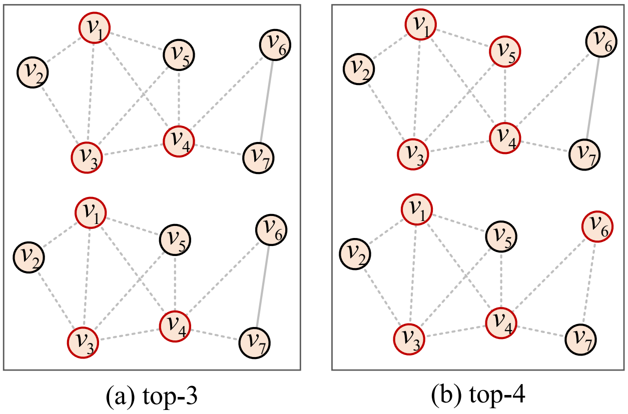


Fig. 3 The damage comparison of two methods. **a** and **b** show the damage to DCPN when attacking the top-3 and top-4 critical nodes identified by SIC and DGSIC. The upper two figures are the results based on SIC, and the lower two figures are based on DGSIC. The red circles represent the attacked nodes, and the dotted lines represent the affected communication

fied by DGSIC, DPCN is completely destroyed. In contrast, it would require attacking more nodes identified by SIC to achieve the same level of damage. These results demonstrate the effectiveness of the prioritization strategy in DGSIC, as it allows for the identification and attack of critical nodes that have a greater impact on network communication and connectivity, leading to more significant network disruption with fewer attacks.

Overall, the dynamic and prioritization strategies of DGSIC provide an efficient and effective approach for identifying critical nodes in dynamic drone swarms.

Experiments

To verify the performance of DGSIC, it has been compared with several existing methods that are based on the different types of information and centrality metrics. The comparison includes the classical local information-based methods such as DC [32] and LC [34], global information-based methods such as BC [42], coupling metric-based methods such as GIN [45] and ECRM [46], classical network dismantling methods such as KS [59] and GND [60], as well as community-based methods such as NEES [52].

The datasets are shown in “Datasets”, and evaluation metrics are shown in “Evaluation metrics”. The results of experiments along with analysis are discussed in “Results and analysis”. The ablation experiments are introduced in “Ablation experiments”. Finally, the time complexity of nine critical node identification methods is discussed in “Time over head analysis”.

Table 1 The details of simulated networks

Network	N	E	D	$< k >$	$< d >$	c
SimNet10	10	18	0.6	3.60	1.96	0.69
SimNet20	20	48	0.5	4.80	2.58	0.66
SimNet40	40	83	0.4	4.15	3.76	0.51
SimNet80	80	196	0.3	4.90	4.22	0.47

Datasets

To address the lack of standard drone datasets, the researchers utilized AirSim, a popular drone simulator, to simulate the DCPN. Four simulated networks were created, each with a different size. The map size for the simulations was set to $1 \times 1 \times 1$ $(km \times km \times km)$, and the specific parameter settings are shown in Table 1. In addition, this paper not only used simulated networks but also incorporated eight real-world networks to further evaluate the performance of DGSIC. These real-world networks encompass various domains and types of social and infrastructure networks. Here are the specific networks used:

Raccoon-proximity: An animal social network representing the proximity relationships among a group of raccoons.

Aves-weaver-social: Another animal social network depicting the social interactions among a group of weaver birds.

Karate: A human social network that captures the interactions among members of a university karate club.

Rt-retweet: A human social network derived from Twitter, focusing on retweet interactions among users.

Road-chesapeake: A road network representing the road connections in Chesapeake, Virginia, USA.

Bcspwr: An electrical grid network modeling the power transmission system of British Columbia, Canada.

Ca-sandi-auths: A collaboration network among authors in the field of computer science, specifically in the area of San Diego, California, USA.

Adjnoun: A keyword network extracted from the British National Corpus, where nodes represent adjectives and nouns that co-occur frequently.

These real-world networks, which span across various domains, provide representative examples that facilitate a comprehensive evaluation of DGSIC. Partial details of these networks are presented in Table 2, and additional information can be obtained from the network repository. [1]

[1] https://networkrepository.com/networks.php.

Table 2 The details of real-world networks

Network	N	E	$\langle k \rangle$	$\langle d \rangle$	c
Raccoon-proximity	19	57	6.00	2.03	0.68
Karate	34	78	4.59	2.41	0.57
Road-Chesapeake	39	170	8.71	1.84	0.45
Bcspwr	49	59	2.41	4.59	0.05
Aves-weaver-social	64	177	5.53	3.04	0.60
Ca-sandi-auths	86	123	2.86	4.84	0.40
Rt-retweet	96	117	2.44	4.31	0.06
Adjnoun	112	425	7.59	2.54	0.17

Evaluation metrics

Critical nodes are highly influential nodes for maintaining the network structure and function. Evaluating diverse critical node identification methods necessitates a thorough analysis of both structural and communication metrics. Therefore, robustness and cascading failure metrics are introduced in “Roubustness” and “Cascading failure”, respectively.

Robustness

Robustness refers to the ability of the network to resist deliberate damage. The robustness of the network decreases as the degree of the damage, and the importance of nodes is the opposite. The relative size of the giant connected component (S) and network efficiency (E) are two classical robustness metrics used to quantify the impact of critical node failures on network connectivity and efficiency, which are defined as follows:

$$S = \frac{N^{'}}{N} \tag{5}$$

where $N^{'}$ represents the size of GCC after direct energy attacks.

$$E = \frac{1}{N(N-1)} \sum_{i \neq j}^{N} \frac{1}{d_{ij}} \tag{6}$$

where N is the size of the network, d_{ij} is the length of the shortest path from v_i to v_j. If there is no path, $1/d_{ij}$=0. By comparing these metrics across different critical node identification methods, this paper can assess the effectiveness of DGSIC in identifying critical nodes that significantly affect the robustness of the network (Fig. 4).

Cascading failure

The state of each node is divided as either normal or failed. The normal node will fail if it is directly attacked, or if most of its neighbor nodes fail. More specifically, when v_j in $\Gamma(i)$ is attacked, the communication of v_i will also be impacted. If the communication loss of v_i exceeds its adjustable threshold θ_i, tasks cannot be carried out, and v_i is considered failed. Due to the tight connection between nodes, the failure of a node will not only affect the communication of its neighbor nodes but also has a cascading effect on information transmission of the entire network.

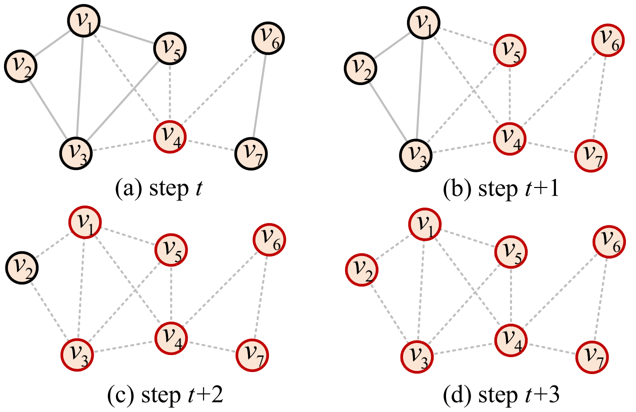
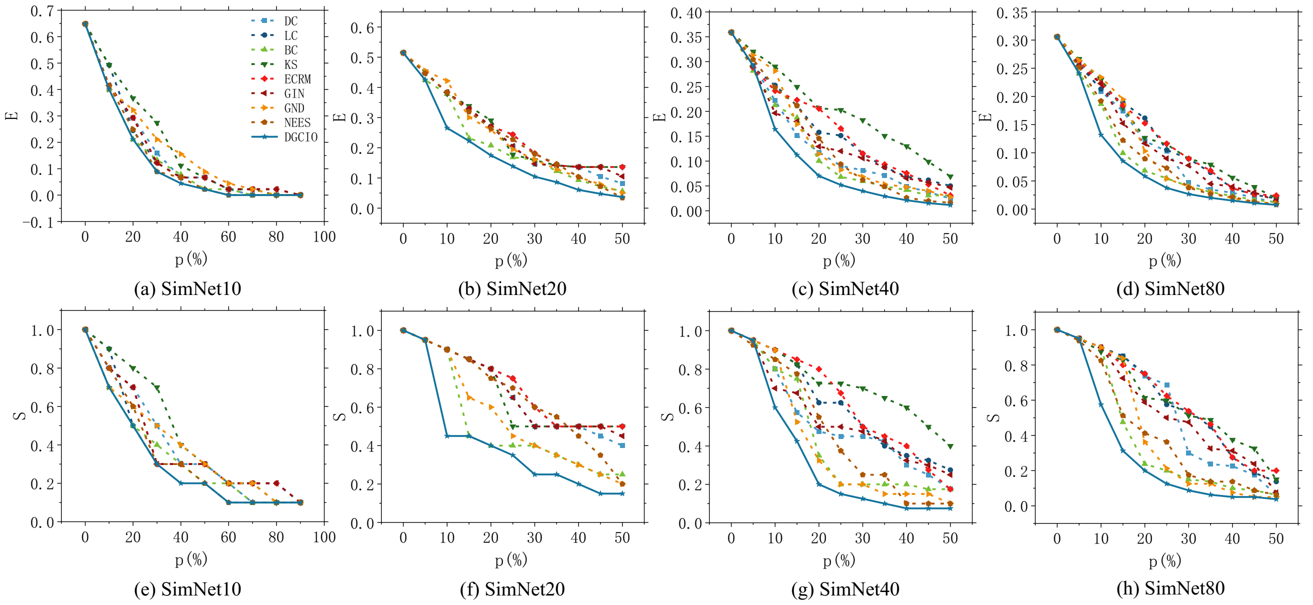


Fig. 4 An example of the cascading failure. The black circles and red circles represent normal nodes and failed nodes, respectively. The adjective threshold θ_i of v_i is consistently set as 0.3. **a** The initially failed node is v_4. **b** The effect of v_4 on v_5, v_6, and v_7 is bigger than θ_5, θ_6, and θ_7, respectively. Therefore, v_5, v_6 and v_7 fail at step $t + 1$. **c** The effect of v_5 on v_1 and v_3 is respectively bigger than θ_1 and θ_3, thus they fail at step $t + 2$. **d** Similarly, v_1 and v_3 make v_2 failed at step $t + 3$. The propagation terminates since all nodes fail at step $t + 3$

To simulate these dynamic impacts, the Linear Threshold model (LT) [61] is used, which is a classic cascading failure model. In this model, each normal node v_i is assigned a random θ_i. The effect of a failed node $v_j \in \Gamma(i)$ on v_i is determined by the parameter c_{ji}=$1/k_i$, where k_i represents the degree of node v_i. If the sum of effects from all failed nodes in $\Gamma(i)$ exceeds θ_i at step t, v_i will fail at step $t + 1$. The cascading failures continue as long as there are no newly failed nodes. To quantify the cascading communication loss in the network, the cascading failure scale (F) is defined as a metric, which is calculated as follows:

$$F = \frac{N_f}{N} \tag{7}$$

where N^f is the number of failed nodes in the network, and the results are the average of 1000 experiments due to the randomness of θ_i. By analyzing F, this paper can evaluate the extent of cascading communication loss and assess the effectiveness of different critical node identification methods in terms of cascading failure.



(a) SimNet10 (b) SimNet20 (c) SimNet40 (d) SimNet80

(e) SimNet10 (f) SimNet20 (g) SimNet40 (h) SimNet80

Fig. 5 The robustness experiment results in four simulated networks. **a**–**d** and **e**–**h** show the network efficiency E and the relative size of the giant connected component S with the node attack ratio p in four simulated networks, respectively

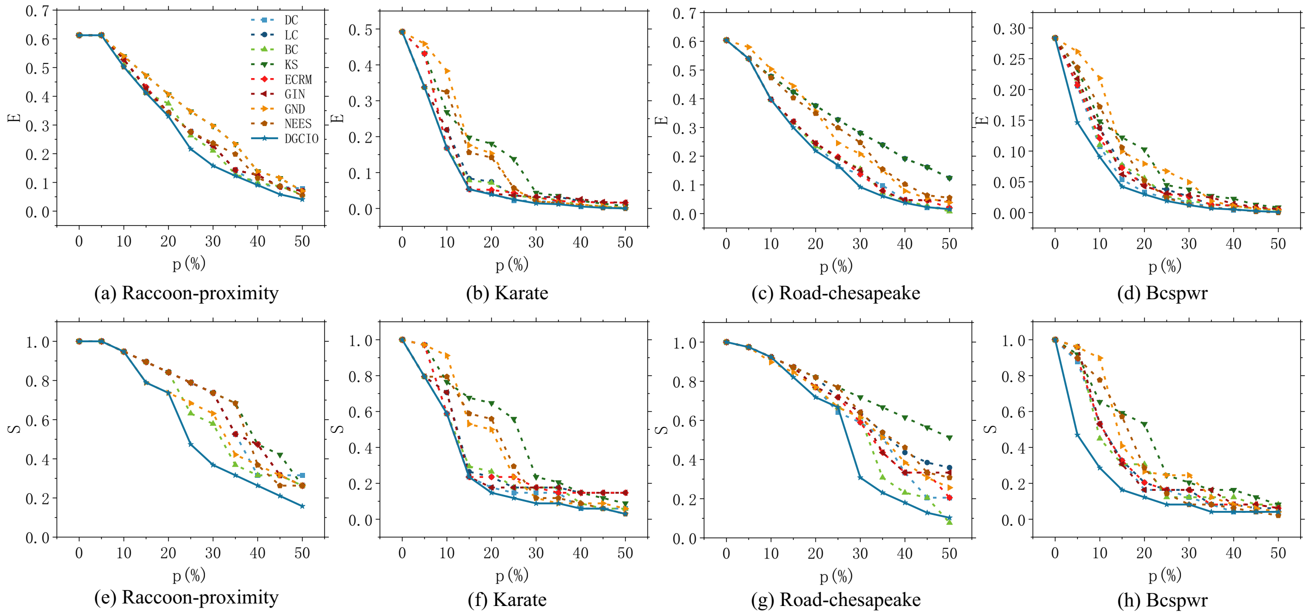
Results and analysis

Extensive experiments validate the effectiveness of the proposed method. The results of robustness and cascading failure experiments are analyzed in "Robustness experiments" and "Cascading failure experiments", respectively.

Robustness experiments

In the experiments conducted in this paper, the deliberate attacks are performed on DCPN. Specifically, the process begins with the detection of malicious drone swarms, followed by the construction of DCPN. Subsequently, various methods for critical node identification are employed to identify critical drones, resulting in different A based on the node importance. Finally, the directed energy attacks are performed against the identified critical drones to assess the impact of their failures on the structure and functionality of drone swarms. In the event of an attack on a drone, the corresponding node itself and its associated edges are removed from DCPN. This removal simulates the damage incurred by the attack, disrupting the communication and connectivity among nodes within DCPN. By analyzing the changes in network structure and function after deliberate attacks, this paper aims to evaluate the impact of critical node failures on DCPN and assess the efficacy of various methods for identifying critical nodes.

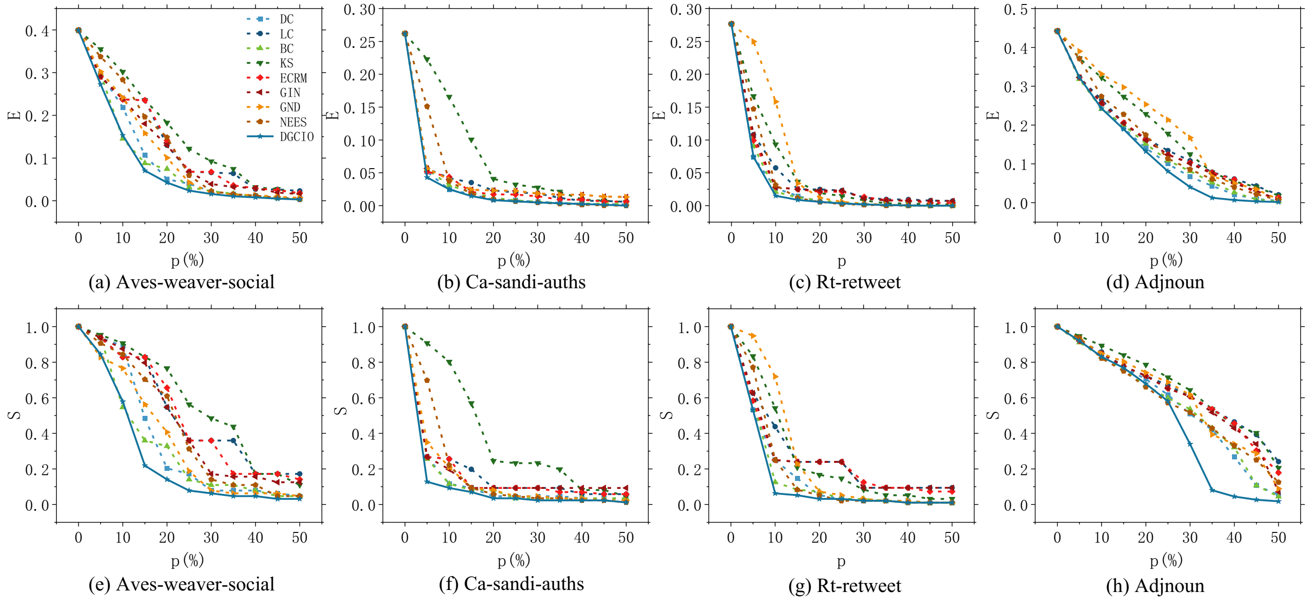
Fig. 5 shows the robustness results of DGSIC and other eight critical node identification methods in four simulated networks. The results demonstrate that DGSIC exhibits a significant advantage in terms of network efficiency and connectivity, particularly in the early stages. Regardless of the node ratio p, DGSIC consistently achieves the best results and causes substantial damage to network efficiency and connectivity. For instance, in Fig. 5(b)–(d), DGSIC outperforms the suboptimal method by 86.02%, 20.04%, and 45.91% in terms of damaging the E when p=10%. Similarly, in Fig. 5(f)–(k), DGSIC surpasses the suboptimal method by 450%, 33.33%, and 142.86% in terms of damaging S when p=10%. Although DGSIC does not exhibit a significant advantage in SimNet10, it consistently achieves the best results across different values of p. Notably, KS performs poorly in these experiments, indicating that coarse-grained methods are not suitable for small and sparse networks. Among the compared methods, LC expands on DC by considering the third-order neighbor nodes. ECRM and GIN combine DC with other global indicators. However, the performance of LC and ECRM is similar to or even worse than DC. This suggests that the extension metric of LC and the similarity metric of ECRM do not have a positive impact and may even have an opposite effect in small networks. On the other hand, GIN performs better than DC in the early stages, indicating that the shortest path strategy employed by GIN contributes to its performance improvement. GND focuses on the partial dismantling of GCC. NEES is a machine learning-based critical node identification method that takes into account both neighbor nodes and multi-scale community structures. As shown in Fig. 5, the performance of NEES and GND has been significantly improved when $p>10\%$, and the performance is further improved with the increase of p. Addi-



(a) Raccoon-proximity (b) Karate (c) Road-chesapeake (d) Bcspwr

(e) Raccoon-proximity (f) Karate (g) Road-chesapeake (h) Bcspwr

Fig. 6 The robustness experiment results in four smaller real-world networks. **a**–**d** and **e**–**h** show the network efficiency E and the relative size of the giant connected component S with the node attack ratio p in four smaller real-world networks, respectively



(a) Aves-weaver-social (b) Ca-sandi-auths (c) Rt-retweet (d) Adjnoun

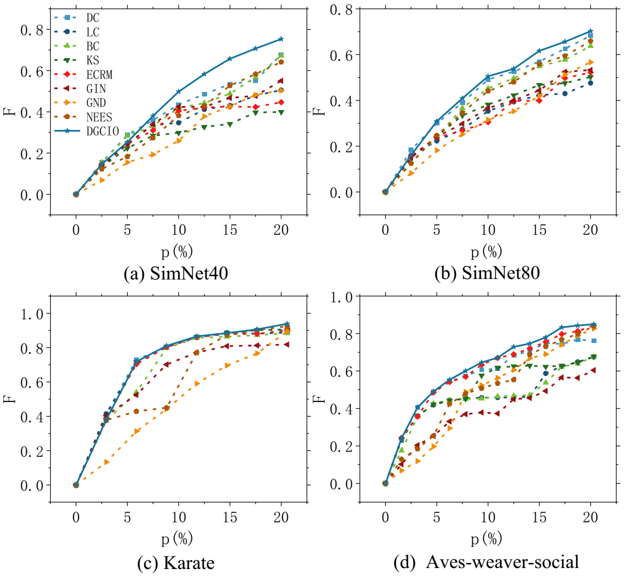
(e) Aves-weaver-social (f) Ca-sandi-auths (g) Rt-retweet (h) Adjnoun

Fig. 7 The robustness experiment results in four bigger real-world networks. **a**–**d** and **e**–**h** show the network efficiency E and the relative size of the giant connected component S with the node attack ratio p in four bigger real-world networks, respectively

tionally, BC also shows superior performance, which is only inferior to DGSIC.

However, none of the above methods can achieve the same performance as DGSIC. This is attributed to the effective integration of communication intensity and scale in DGSIC, taking into account the distributed nature of drones. Furthermore, DGSIC incorporates the dynamic and prioritization strategies to improve the accuracy of critical node identification.

Figures 6 and 7 show the robustness results in eight real-world networks, and the results are almost consistent with those from the simulated networks. It can be observed that DGSIC consistently achieves optimal results across the majority of the networks, especially in Bcspwr. Additionally, DGSIC also demonstrates good performance in animal social networks such as Raccoon-proximity and Aves-weaver-social. These networks exhibit clear community structures and sparse connections between communities,



(a) SimNet40

(b) SimNet80

(c) Karate

(d) Aves-weaver-social

Fig. 8 The cascading failure experiment results. **a**–**b** and **c**–**d** show the cascading failure scale F with the node attack ratio p in simulated and real-world networks, respectively

which aligns well with the strengths of DGSIC. While the advantage of DGSIC may not be particularly significant in other networks, it still outperforms the compared methods, showcasing its effectiveness in critical node identification.

Cascading failure experiments

Figure 8 shows the cascading failure scale F corresponding to different node attack ratios p. From the results, we can observe that as the p increases, the F shows an upward trend, indicating a higher level of damage to the network. Among the compared methods, DGSIC exhibits a more significant increasing trend in F, indicating its superior performance in causing cascading failures. Interestingly, GND achieves the worst results in terms of cascading failure, suggesting that the critical nodes identified by GND do not possess an advantage in terms of cascading failure. This finding indirectly suggests that the prioritization strategy of GND does not play a crucial role in causing cascading failures.

The analysis reveals that when $p<5\%$, the failure of critical nodes has a relatively small impact on the network. This suggests that the network possesses a certain level of resilience against external damage. In addition, DC exhibits better performance in the early stages, especially in SimNet40. This suggests that in small networks with higher clustering coefficients, attacking nodes with the highest degree will cause more significant damage to network communication.

When $p>5\%$, BC also shows excellent performance in simulated networks. Moreover, ECRM demonstrates significantly superior performance in real-world networks, almost approaching DGSIC. This suggests that while ECRM may not effectively identify nodes with high robustness, it can identify nodes crucial for cascading failure. However, DGSIC always achieves the maximum F across different values of p, and the advantage becomes more pronounced as p increases. This can be attributed to the dynamic strategies incorporated in DGSIC, which ensure that the identified critical node is the most crucial node in the current network topology. By considering the dynamic feature of the network and incorporating prioritization strategies, DGSIC effectively identifies nodes that have the highest impact on the network communication, leading to the highest cascading failure scale. For example, as shown in Fig. 8(a) and at p=15%, the F of DGSIC increased by 14.43% and 18.79% compared to DC and BC, respectively. Similarly in Fig. 8(d) and at p=15%, the F of DGSIC increased by 5.58% and 3.62% compared to DC and ECRM, respectively. Moreover, the F of NEES is significantly improved as p increases. This suggests that the community structure plays a crucial role in identifying critical nodes, particularly when the network becomes sparse. For example, as shown in Fig. 8(b), when p=10%, the F decreased by 14.59% compared to DGSIC. When p=20%, the F decreased by 6.52% compared to DGSIC. As shown in Fig. 8(c), when p=10%, the F decreased by 27.12% compared to DGSIC. When p=20%, the F decreased by 1.56% compared to DGSIC. These results highlight the superiority of DGSIC in identifying critical nodes and its ability to maintain high cascading failure scales, even as the node attack ratio p increases. The incorporation of dynamic strategies in DGSIC contributes to its robust performance in the face of deliberate attacks.

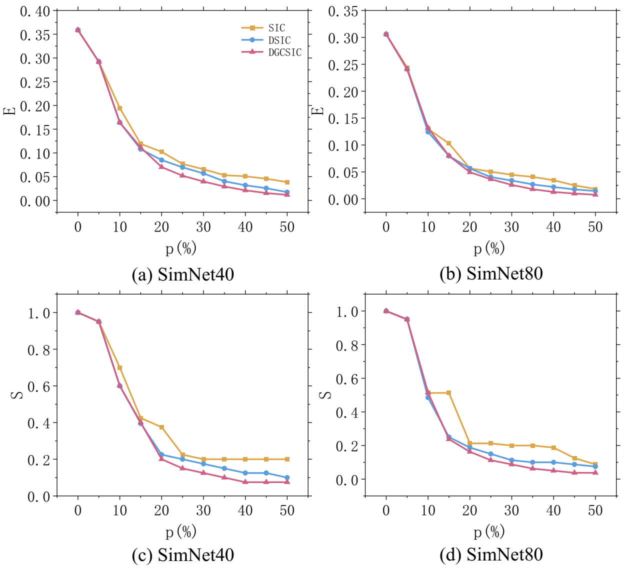
From the above analysis, it can be concluded that DCPN has a certain ability to resist external damage. In addition, attacking the critical nodes identified by DGSIC cannot only quickly disrupt the connectivity and efficiency, but also cause the maximum dynamic cascading impact on DCPN.

Ablation experiments

To further validate the effectiveness of the dynamic and prioritization strategies, this paper conducts ablation experiments comparing SIC, DSIC, and DGSIC in terms of robustness and cascading failure, as introduced in "The comparison of three methods in robustness" and "The comparison of three methods incascading failure", respectively.

The comparison of three methods in robustness

The comparison of their robustness performance is depicted in Fig. 9 for simulated networks and in Fig. 10 for real-world social networks. The experimental results demonstrate that there is virtually no distinction in the robustness performance



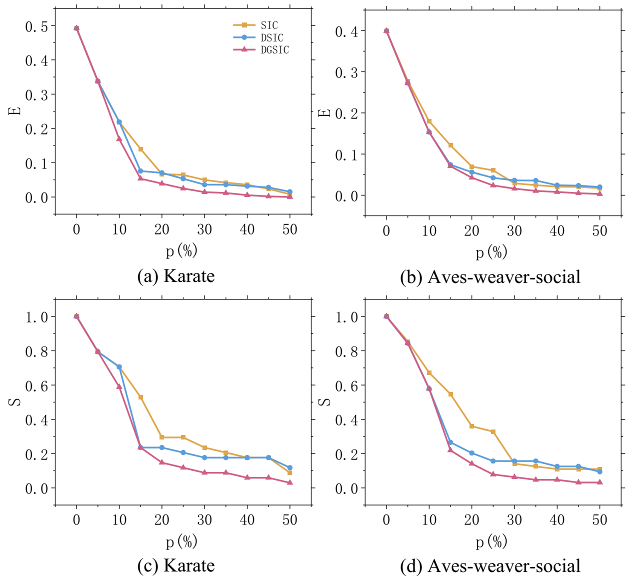
(a) SimNet40

(b) SimNet80

(c) SimNet40

(d) SimNet80

Fig. 9 The robustness experiment results in two simulated networks. **a**–**b** and **c**–**d** show the network efficiency E and the relative size of the giant connected component S with the node attack ratio p in two simulated networks, respectively



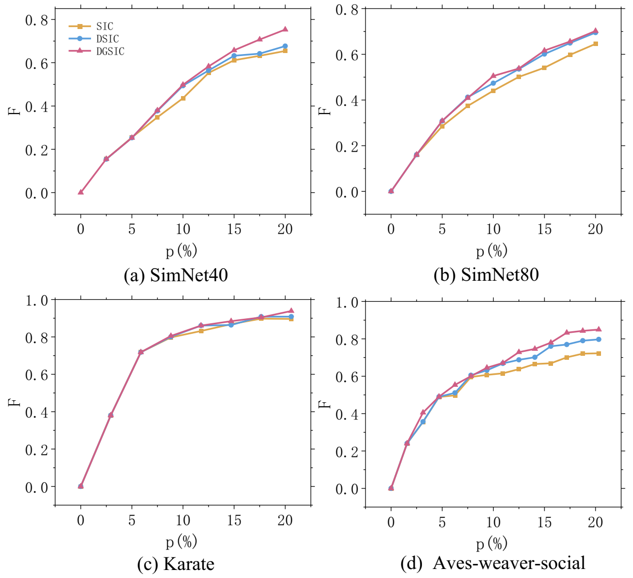
(a) Karate

(b) Aves-weaver-social

(c) Karate

(d) Aves-weaver-social

Fig. 10 The robustness experiment results in two real-world networks. **a**–**b** and **c**–**d** show the network efficiency E and the relative size of the giant connected component S with the node attack ratio p in two real-world networks, respectively



(a) SimNet40

(b) SimNet80

(c) Karate

(d) Aves-weaver-social

Fig. 11 The cascading failure results in four networks. **a**, **b** and **c**, **d** show the cascading failure scale F with the node attack ratio p in simulated and real-world networks, respectively

among the three methods when p<5%. This can be attributed to the network's capacity to maintain its connectivity when only a marginal fraction of nodes are attacked. In such circumstances, the most critical nodes identified by the three methods are almost the same. Furthermore, SIC consistently exhibits the poorest performance when p>5%. The integration of the dynamic strategy has substantially enhanced the performance of DSIC. For instance, as shown in Fig. 9(b) and (d), when p=15%, DSIC outperforms SIC by 11.36% and 54.86% in terms of damaging the E and S, respectively. This trend is consistent across real-world networks, as evident in Fig. 10(b) and (d), where at the same p=15%, DSIC continues to outperform SIC by 16.97% and 31.61% in terms of damaging the E and S, respectively. This consistent trend stems from the dynamic strategy's integration in DSIC. Following each critical node identification, DSIC updates the network topology, ensuring the perpetuation of the identified node's paramount significance within the network structure at that precise moment.

By further incorporating the prioritization strategy, DGSIC gives priority to critical nodes within GCC when the network becomes disconnected. Furthermore, as p increases, the advantages of DGSIC become even more pronounced. As shown in Figs. 9(a) and (c), 10(a) and (c), when p=15%, DGSIC and DSIC demonstrate nearly the same performance. However, when p=30%, DGSIC outperforms DSIC by 5.64% and 6.06% in terms of damaging the E and S as shown in Fig. 9(a) and (c), respectively. Similarly in Fig. 10(a) and (c), DGSIC outperforms DSIC by 4.76% and 10.71% in terms of damaging the E and S, respectively. This is because as p increases, the network becomes more disconnected, resulting in more numerous connected components. Among them, GCC assumes a greater portion of the communication load. Consequently, prioritizing the disruption of GCC would lead to more significant communication losses within the network.

Table 3 The time complexity of methods

Methods	DC	LC	BC	KS	ECRM	GIN	GND	NEES	SIC	DSIC	DGSIC
Complexity	$O(N)$	$O(N \cdot \langle k \rangle^2)$	$O(N^3)$	$O(N)$	$O(N)$	$O(N^3)$	$O(N \cdot logN)$	$O(N \cdot N_G^2)$	$O(N^3)$	$O(N^4)$	$O(N \cdot N_G^3)$

Among them, N and $\langle k \rangle$ are the size and the average degree of a network. N_G is the size of GCC

The comparison of three methods in cascading failure

Figure 11 illustrates the results of cascading failure experiments in two simulated networks. These results almost align with the robustness experiments, affirming that DGSIC not only has superior performance in robustness but also in cascade failures. Particularly noteworthy is the sharp increase in the value of F with the rise of p in the Karate network, where the distinctions between the three algorithms are less pronounced. This phenomenon is attributed to the small size of the Karate network, where the failure of even a few nodes will gradually impact the whole network. As the network size expands, DGSIC's advantage becomes increasingly evident.

Hence, when countering malicious drone swarms, the sequence of critical nodes provided by DGSIC can be utilized to target these drones using directed energy attacks. This directed attack strategy enables the systematic disruption of critical drones with great communication significance, thereby achieving an efficient neutralization of malicious drone swarms.

Time overhead analysis

Table 3 shows the time complexity of different critical node identification methods. Compared to SIC, DSIC increases the time complexity from N^3 to N^4. It's evident that the dynamic strategy, while significantly enhancing DGSIC's performance, also introduces the substantial time overhead. DGSIC addresses this challenge by prioritizing the nodes in GCC rather than all nodes in DCPN. Additionally, as the network is disintegrated into smaller connected components, the advantages of DGSIC become more pronounced. However, despite the introduction of prioritization strategies, reducing the complexity to $N \cdot N_G^3$, it remains higher than the comparison methods.

Currently, the size of malicious drone swarms is manageable, and the computational overhead introduced by DGSIC remains reasonable. Nonetheless, as the size of drone swarms grows to thousands or even more, the computational burden of DGSIC escalates considerably. We hope future research can address this challenge and provide efficient solutions for handling larger-scale drone swarms.

Conclusion and future work

To enhance the efficiency of directed energy attacks on malicious drone swarms, this paper proposes a new critical drone identification method named dynamic GCC-based scale-intensity centrality (DGSIC). The method is based on the communication analysis and aims to identify critical drones for targeted attacks, thereby maximizing the disruption caused to the malicious swarm. More specifically, an extended dynamic communication prediction network (DCPN) model is first constructed to predict the dynamic communication of drones. On this basis, DGSIC is further proposed to identify critical drones for targeted attacks, enhancing the efficiency of directed energy attacks and maximizing the disruption of malicious drone swarms. DGSIC optimizes the drone attack sequence for directed energy attacks, ensuring that each attack inflicts more damage to the robustness and triggers larger-scale cascading failures of malicious drone swarms. This improvement contributes to the effectiveness of directed energy attacks, facilitating the rapid dissolution of malicious drone swarms while minimizing cost. However, while DGSIC enhances the performance of critical drone identification, it also introduces a significant time overhead. This temporal cost becomes particularly pronounced when dealing with large-scale swarms comprising thousands of drones. We hope that these issues will be addressed in future research.

Moreover, future research can integrate trajectory prediction methods for the automatic predictions of DCPN. Advancements in drone detection technology enable the direct detection of communication protocols embedded in malicious drone swarms, thereby enhancing the accuracy of DCPN construction and further improving the accuracy of DGSIC. These advancements would contribute to more effective approaches for countering malicious drone swarms.

Acknowledgements This work was supported by the National Science Fund for Distinguished Young Scholars (No. 62025602), the National Natural Science Foundation of China (Nos. 61976181, 62261136549, U22B2036, 11931015), Technology-Scientific and Technological Innovation Team of Shaanxi Province (No. 2020TD-013), Fok Ying-Tong Education Foundation, China (No. 171105), and Tencent Foundation and XPLORER PRIZE.

Data availability The real-world network datasets supporting this study are openly available at https://networkrepository.com/networks.php.

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. Wu Y, Wu S, Hu X (2021) Multi-constrained cooperative path planning of multiple drones for persistent surveillance in urban environments. Comp Intell Syst 7:1633–1647
2. Yaacoub JP, Noura H, Salman O, Chehab A (2020) Security analysis of drones systems: Attacks, limitations, and recommendations. Internet Things 11:100218
3. Chamola V, Kotesh P, Agarwal A, Naren Gupta N, Guizani M (2021) A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques. Ad hoc Netw 111:102324
4. Lyu C, Zhan R (2022) Global analysis of active defense technologies for unmanned aerial vehicle. IEEE Aerosp Electron Syst Mag 37(1):6–31
5. Lyu CY, Zhan RJ (2020) Research on the cutting-edge application of high energy laser c-uas technology. International Conference on Optoelectronic and Microelectronic Technology and Application 11617:291–304
6. Tianfeng F, Xiaojing M, Chi Z (2023) Development status of anti uav swarm and analysis of new defense system. In: Proceedings of the Journal of Physics: Conference Series, vol 2478, p 092011
7. Min SH, Jung H, Kwon O, Sattorov M, Kim S, Park SH, Hong D, Kim S, Park C, Hong BH, Cho I, Ma S, Kim M, Yoo YJ, Park SY, Park GS (2021) Analysis of electromagnetic pulse effects under high-power microwave sources. IEEE Access 9:136775–136791
8. Billaud A, Le Guennic T, Allioux D, Jian P, Pinel O, Labroille G (2020) Optimal coherent beam combining based on multi-plane light conversion for laser directed energy weapons and countermeasure. In: Proceedings of the Technologies for Optical Countermeasures XVII; and High-Power Lasers: Technology and Systems, Platforms, Effects IV, vol 11539, p 115390F
9. Kracman M (2023) Optimisation of directed energy systems' positions subject to uncertainty in operations. Progress Electromagn Res Lett 110:47–53
10. Wang J, Jiang C, Han Z, Ren Y, Maunder RG, Hanzo L (2017) Taking drones to the next level: Cooperative distributed unmanned-aerial-vehicular networks for small and mini drones. IEEE Veh Technol Magaz 12(3):73–82
11. Wang F, Huang J, Low KH, Nie Z, Hu T (2023) AGDS: adaptive goal-directed strategy for swarm drones flying through unknown environments. Complex Intell Syst 9(2):2065–2080
12. Jin X, Wang Z, Zhao J, Yu D (2022) Swarm control for large-scale omnidirectional mobile robots within incremental behavior. Inform Sci 614:35–50
13. Fan DD, Theodorou EA, Reeder J (2018) Model-based stochastic search for large scale optimization of multi-agent uav swarms. In: Proceedings of the 2018 IEEE Symposium Series on Computational Intelligence, pp 2216–2222
14. Li J, Rombaut E, Vanhaverbeke L (2021) A systematic review of agent-based models for autonomous vehicles in urban mobility and logistics: Possibilities for integrated simulation models. Comput Environ Urban Syst 89:101686
15. Wang J, Wang X, Wang L (2017) Modeling of BN lifetime prediction of a system based on integrated multi-level information. Sensors 17(9):2123
16. Ren Z, Zhang D, Tang S, Xiong W, Yang Sh (2022) Cooperative maneuver decision making for multi-UAV air combat based on incomplete information dynamic game. Defence Technol. https://doi.org/10.1016/j.dt.2022.10.008
17. Elsawah S, Pierce SA, Hamilton SH, Van Delden H, Haase D, Elmahdi A, Jakeman AJ (2017) An overview of the system dynamics process for integrated modelling of socio-ecological systems: Lessons on good modelling practice from five case studies. Environ Modell Softw 93:127–145
18. Yehui S, Guoru D, Jiachen S, Jinghua L, Yitao X (2022) Topology tracking of dynamic UAV wireless networks. Chin J Aeronaut 35(11):322–335
19. Xiaohong W, Zhang Y, Lizhi W, Dawei L, Guoqi Z (2020) Robustness evaluation method for unmanned aerial vehicle swarms based on complex network theory. Chin J Aeronaut 33(1):352–364
20. Yu D, Chen CLP, Ren CE, Sui S (2019) Swarm control for self-organized system with fixed and switching topology. IEEE Trans Cybern 50(10):4481–4494
21. Chen Y, Zhang H, Fu X, Xu J (2022) Robustness analysis and modeling of UAV cluster system based on complex network. In: Proceedings of the International Conference on Computer Science, Electronic Information Engineering and Intelligent Control Technology, pp 743–748
22. Bisio I, Garibotto C, Haleem H, Lavagetto F, Sciarrone A (2021) On the localization of wireless targets: A drone surveillance perspective. IEEE Netw 35(5):249–255
23. Li Y, Fu M, Sun H, Deng Z, Zhang Y (2022) Radar-based UAV swarm surveillance based on a two-stage wave path difference estimation method. IEEE Sensors J 22(5):4268–4280
24. Yan J, Xie H, Li J (2021) Modeling and optimization of deploying anti-UAV swarm detection systems based on the mixed genetic and monte carlo algorithm. In: Proceedings of the IEEE International Conference on Unmanned Systems, pp 773–779
25. Zhao J, Zhang J, Li D, Wang D (2022) Vision-based anti-UAV detection and tracking. IEEE Trans Intell Transp Syst 23(12):25323–25334
26. Cheng F, Liang Z, Peng G, Liu S, Li S, Ji M (2022) An anti-UAV long-term tracking method with hybrid attention mechanism and hierarchical discriminator. Sensors 22(10):3701
27. Valianti P, Kolios P, Ellinas G (2022) Energy-aware tracking and jamming rogue uavs using a swarm of pursuer UAV agents. IEEE Syst J 17(1):1524–1535
28. He D, Yang G, Li H, Chan S, Cheng Y, Guizani N (2020) An effective countermeasure against UAV swarm attack. IEEE Netw 35(1):380–385
29. Lee CH, Thiessen C, Van Bossuyt DL, Hale B (2022) A systems analysis of energy usage and effectiveness of a counter-unmanned aerial system using a cyber-attack approach. Drones 6(8):198
30. Wu H, Li W, Li W, Liu G (2020) A real-time robust approach for tracking uavs in infrared videos. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, pp 1032–1033

31. Chen W, Meng X, Liu J, Guo H, Mao B (2022) Countering large-scale drone swarm attack by efficient splitting. IEEE Trans Veh Technol 71(9):9967–9979
32. Freeman LC (2002) Centrality in social networks: Conceptual clarification. Social network: critical concepts in sociology Londres: Routledge 1:238–263
33. Gao C, Su Z, Liu J, Kurths J (2019) Even central users do not always drive information diffusion. Commun ACM 62(2):61–67
34. Chen D, Lü L, Shang M, Zhang Y, Zhou T (2012) Identifying influential nodes in complex networks. Phys A 391(4):1777–1787
35. Tee P, Parisis G, Wakeman I (2017) Vertex entropy as a critical node measure in network monitoring. IEEE Trans Netw Service Manage 14(3):646–660
36. Lei M, Cheong KH (2022) Node influence ranking in complex networks: A local structure entropy approach. Chaos, Solitons & Fractals 160:112136
37. Wang F, Sun Z, Gan Q, Fan A, Shi H, Hu H (2022) Influential node identification by aggregating local structure information. Phys A 593:126885
38. Fang J, Partovi FY (2020) A HITS-based model for facility location decision. Expert Syst Appl 159:113616
39. Page L, Brin S, Motwani R, Winograd T (1999) The PageRank citation ranking: Bringing order to the web. Tech. rep, Stanford InfoLab
40. Jiang S, Luo Z, Yin Z, Wang Z, Wang S, Gao C (2021) Identification of Critical Nodes in Urban Transportation Network Through Network Topology and Server Routes. In: Proceedings of the International Conference on Knowledge Science, Engineering and Management, pp 395–407
41. Li Z, Tang J, Zhao C, Gao F (2023) Improved centrality measure based on the adapted PageRank algorithm for urban transportation multiplex networks. Chaos, Solitons & Fractals 167:112998
42. Freeman LC (1977) A set of measures of centrality based on betweenness. Sociometry pp 35–41
43. Sabidussi G (1966) The centrality index of a graph. Psychometrika 31(4):581–603
44. Gao C, Liu J, Zhong N (2011) Network immunization and virus propagation in email networks: experimental evaluation and analysis. Knowl Inform Syst 27:253–279
45. Zhao J, Wang Y, Deng Y (2020) Identifying influential nodes in complex networks from global perspective. Chaos, Solitons & Fractals 133:109637
46. Zareie A, Sheikhahmadi A, Jalili M, Fasaei MSK (2020) Finding influential nodes in social networks based on neighborhood correlation coefficient. Knowl Based Syst 194:105580
47. Zhang G, Bai J, Tebbe CC, Zhao Q, Jia J, Wang W, Wang X, Yu L (2021) Salinity controls soil microbial community structure and function in coastal estuarine wetlands. Environ Microbiol 23(2):1020–1037
48. Gao C, Yin Z, Wang Z, Li X, Li X (2023) Multilayer network community detection: A novel multi-objective evolutionary algorithm based on consensus prior information [feature]. IEEE Comput Intell Mag 18(2):46–59
49. Wang Z, Wang C, Li X, Gao C, Li X, Zhu J (2020) Evolutionary markov dynamics for network community detection. IEEE Trans Knowl Data Eng 34(3):1206–1220
50. Tulu MM, Hou R, Younas T (2018) Identifying influential nodes based on community structure to speed up the dissemination of information in complex network. IEEE Access 6:7390–7401
51. Yu EY, Wang YP, Fu Y, Chen DB, Xie M (2020) Identifying critical nodes in complex networks via graph convolutional networks. Knowl Based Syst 198:105893
52. Liu Q, Wang B (2022) Neural extraction of multiscale essential structure for network dismantling. Neural Netw 154:99–108
53. Liu Y, Song A, Shan X, Xue Y, Jin J (2022) Identifying critical nodes in power networks: A group-driven framework. Expert Syst Appl 196:116557
54. Gao C, Zhu J, Zhang F, Wang Z, Li X (2023) A novel representation learning for dynamic graphs based on graph convolutional networks. IEEE Trans Cybern 53(6):3599–3612
55. Sharma A, Vanjani P, Paliwal N, Basnayaka CMW, Jayakody DNK, Wang HC, Muthuchidambaranathan P (2020) Communication and networking technologies for UAVs: A survey. J Netw Comput Appl 168:102739
56. Vásárhelyi G, Virágh C, Somorjai G, Nepusz T, Eiben AE, Vicsek T (2018) Optimized flocking of autonomous drones in confined environments. Sci Robot 3(20):3536
57. Colajanni G, Daniele P, Galluccio L, Grasso C, Schembra G (2022) Service chain placement optimization in 5G FANET-based network edge. IEEE Commun Magaz 60(11):60–65
58. Blondel VD, Guillaume JL, Lambiotte R (2008) Lefebvre E (2008) Fast unfolding of communities in large networks. J Statis Mech 10:P10008
59. Kitsak M, Gallos LK, Havlin S, Liljeros F, Muchnik L, Stanley HE, Makse HA (2010) Identification of influential spreaders in complex networks. Nat phys 6(11):888–893
60. Ren XL, Gleinig N, Helbing D, Antulov-Fantulin N (2019) Generalized network dismantling. Proc Natl Acad Sci 116(14):6554–6559
61. Chen W, Yuan Y, Zhang L (2010) Scalable influence maximization in social networks under the linear threshold model. In: Proceedings of the IEEE International Conference on Data Mining, pp 88–97