Journal of Systems Engineering and Electronics
Vol. 35, No. 2, April 2024, pp.430 – 443

A framework of force of information influence and application for C4KISR system

MAO Shaojie[1], DIAO Lianwang[1], SUN Yu[1,2], WANG Heng[1], YI Kan[1], XU Xin[1], MAO Xiaobin[1], ZHANG Kecheng[1,*], and SHENG Long[1]

1. Science and Technology on Information Systems Engineering Laboratory, The 28th Research Institute of China Electronics Technology Group Corporation, Nanjing 210007, China; 2. Unit 94860 of the PLA, Nanjing 210008, China

Abstract: The subversive nature of information war lies not only in the information itself, but also in the circulation and application of information. It has always been a challenge to quantitatively analyze the function and effect of information flow through command, control, communications, computer, kill, intelligence, surveillance, reconnaissance (C4KISR) system. In this work, we propose a framework of force of information influence and the methods for calculating the force of information influence between C4KISR nodes of sensing, intelligence processing, decision making and fire attack. Specifically, the basic concept of force of information influence between nodes in C4KISR system is formally proposed and its mathematical definition is provided. Then, based on the information entropy theory, the model of force of information influence between C4KISR system nodes is constructed. Finally, the simulation experiments have been performed under an air defense and attack scenario. The experimental results show that, with the proposed force of information influence framework, we can effectively evaluate the contribution of information circulation through different C4KISR system nodes to the corresponding tasks. Our framework of force of information influence can also serve as an effective tool for the design and dynamic reconfiguration of C4KISR system architecture.

Keywords: information warfare, command, control, communications, computer, kill, intelligence, surveillance, reconnaissance (C4KISR) system, information circulation, force of information influence, information entropy.

DOI: 10.23919/JSEE.2024.000011

1. Introduction

From the end of the last century to the beginning of the 21st century, human society began to enter the information age. And the mechanized warfare gave way to the information warfare [1]. The winning mechanism of information warfare is to seize battlefield information superiority [2−4] and turn it into decision-making and action superiority [5]. Information superiority has become the key to the victory of information war [6−8]. However, how can we transform the information superiority into the decision-making and action superiority in the dynamic battlefield environment? What is the intrinsic mechanism of action? So far, how to characterize and evaluate the information circulation between command, control, communications, computer, kill, intelligence, surveillance, reconnaissance (C4KISR) system [9,10] nodes of sensing, intelligence processing, decision making and fire attack has remained an open problem in military research.

In the field of information science research, Zhang put forward the concept of "information power", which mainly referred to the ability of individuals and organizations to analyze, process and utilize information [11]. Zhang pointed out that information power was the product of information and information acceleration [11]. However, they have not considered the effect of information transmission. Ciftcioglu et al. [12] and Bar-noy et al. [13] put forward the concept of "information quality" for the evaluation of information accuracy, precision, reliability, credibility, corroboration and timeliness. As can be seen, the information quality can be effectively represented by the above dimensions and the corresponding dimension values. However, it does not work for C4KISR system as the same information may have different values at different C4KISR nodes. This is because the concept of "information quality" ignored the information context, such as the related task in C4KISR system. To address the above problem, Cansever put forward the concept of "information value", which was defined as "the difference in task quality when the same task was completed with or without this information" [14]. In this concept, the task quality was expressed by the expected value of a utility function, but the contribution of infor-

Manuscript received February 14, 2022.
*Corresponding author.
The work was supported by the Natural Science Foundation Research Plan of Shanxi Province (2023JCQN0728).

mation to the task quality has not been evaluated. Kong et al. established an analysis framework of "objective/task-information subject/subject factor-probability distribution-information value" [15]. Within this framework, the value of information was evaluated based on the theory of information entropy and Bayesian theory, similar to the concept of "information value" put forward by Cansever. Again, the framework ignored the information context and failed to evaluate the contribution of information to decision making. He et al. put forward the theory of "transfer entropy" to evaluate the value of information [16]. This theory extended the traditional information entropy from the evaluation of information itself to the evaluation of its contribution to decision making. The main contribution was that it not only considered the utility of information but also the information usage cost. However, it was not applicable for evaluating the process of information circulation. In summary, none existing work has taken the value of information circulation between C4KISR system nodes into consideration yet.

In order to evaluate and model the influence (i.e., information value) of information circulation between C4KISR system nodes, we put forward a novel framework of force of information influence between C4KISR system nodes, based on the theories of operational command science [17] information entropy, fuzzy mathematics, C4KISR system design, etc. To our knowledge, this is the first concept for information circulation evaluation. Upon that, we further established the models of force of information influence between typical C4KISR system nodes. We have validated our framework of force of information influence under a simulated air defense and attack scenario. Our framework is applicable for both C4KISR and civilian information systems. It has also provided a quantitative analysis approach for the architecture design and dynamic reconfiguration for both military and civilian information systems.

2. Framework of force of information influence for C4KISR system

In this section, we propose the novel framework of force of information influence for the nodes of C4KISR system in information warfare. The force of information influence from the source node to the recipient node in the C4KISR system is defined as the average change of task-related knowledge level of the recipient node for each bit of transmitted information, as shown in

$$F_{XY} = \frac{K_Y}{I_{XY}} \tag{1}$$

where F_{XY} denotes the force of information influence from source node X to recipient node Y, I_{XY} denotes the amount of information provided by source node X to recipient node Y and K_Y denotes the change of task-related knowledge level of recipient node Y after receiving the information. In practical applications, the force of information influence F_{XY} implies that, given a fixed amount of information I_{XY}, the larger change in the task-related knowledge level K_Y of recipient node Y, the larger value F_{XY} tends to have.

The source and recipient nodes in our definition of force of information influence refer to the nodes with different functions in C4KISR system. The typical functions include sensing, intelligence processing, decision making and fire attack. Each node in C4KISR system is capable of sending, receiving, processing and utilizing information independently. The information is transmitted between different nodes according to their collaboration relationships, such as information support, command, cooperation, etc. [18]. The type of transmitted information is dependent on the collaboration relationships between the nodes. For instance, the information provided by a sensing node is usually related with the observations and measurements of target status and behaviors. As another instance, the information sent from an intelligence processing node to a decision-making node is usually related with the attributes, types, positions, speed and headings of targets.

Our definition of force of information influence also involves the concept of task-related knowledge. According to [19], knowledge is the product of information analysis and understanding, such as the inferred relationships between objects, the summarized object characteristics and the identified behavior patterns. From another point of view, knowledge is a special type of information to support decision making after interpretation and understanding. From the perspective of C4KISR system, the task-related knowledge is mainly about the relationships, behavior characteristics and patterns of the targets involved in C4KISR tasks. The task-related knowledge of a C4KISR node is closely related with its associated task as well as the associated targets, process and environments. The task-related knowledge is crucial for the operational capacity of the node. For example, the task-related knowledge for a decision-making node includes the relationships, behavior characteristics and patterns of adversarial targets as well as the meteorological and hydrological forecast of battlefield. The more accurate and more timely the knowledge, the more efficiently and effectively the commander is capable of completing the missions.

The force of information influence proposed in this paper has four main characteristics. Firstly, the definition

of force of information influence provided in (1) is just theoretical. In practical cases, it has to be refined according to the associated tasks and transmitted information. The key is how to extract and represent the task-related knowledge. Secondly, the concept of force of information influence reflects the value-enhancing role of information and is independent with the task-related processes, personnel and equipment. This indicates that our framework of force of information influence is adaptable in various scenarios. This is especially valuable for designing, evaluating and optimizing military information systems and architectures. Thirdly, the force of information influence is temporal in nature as it is closely related with the dynamic information and task-related knowledge the recipient node has. These dynamic factors could be modeled with a function of the situational awareness of the dynamically changing battlefield. The temporal characteristic complies with the basic theory that the information timeliness affects its effectiveness. Finally, the value of force of information influence could be negative, implying that it may result in negative effect. Under the complex and adversarial battlefield environment, the false, messy, faked and incomplete information could result in an aggravation of fog of war and an increase in the knowledge uncertainty for the nodes of C4KISR system. It could also result in a decrease in the task efficiency and effectiveness. This complies with the basic principles of information confrontation [20−22].

There are generally three different application modes for force of information influence. Firstly, in the process of system architecture design, the system architecture can be optimized by evaluating the change of force of information influence when exploring combinations of system units. Secondly, in the process of system operation, the system architecture may need to be adjusted due to the failure of a system unit or the task change. In that case, the force of information influence can serve as a guideline for the adjustment in information relationships between system units. Thirdly, for the mission of striking time sensitive targets, the sensor with the optimized value of force of information influence can be screened out quickly for the agile construction of kill chain, a tightly woven fabric of sensors, shooters and command and control.

3. Model of force of information influence for C4KISR system

We assume that the sensing node in C4KISR system is represented by node O, the intelligence processing node by node P, the decision-making node by node D and the fire attack node by node A. According to the basic definition and mathematical expression of force of information influence, we model the force of information influence from node O to node P, node P to node D and node D to node A respectively within the operational process of "sensing→intelligence processing→decision making→fire attack" for C4KISR system.

3.1 Force of information influence from node O to node P

The force of information influence from node O to node P has been a hotspot in C4KISR system field. Long et al. [2] summarized three methods of measuring information superiority with different characteristics and application scopes, based on information flow, knowledge gain and information quality respectively. Li et al. [3] pointed out that information superiority was indispensable for the evaluation index system of command and control. He established a framework with quantifiable mathematical models to evaluate information superiority from three aspects: information completeness, accuracy and timeliness. Zibetti et al. [4] studied the concept connotation, evaluation framework and method of information superiority for network information system. He pointed out that a comprehensive evaluation of information superiority of network information system should be carried out from sensor domain, fusion domain and cooperation domain simultaneously. Within the C4KISR system operational process, the main role of node P is to associate and fuse the target measurement information from one or more sensing nodes, generate complete intelligence products and send them to node D. The intelligence products mainly include the attribute, type, location, moving state and quantity of targets. According to the theory and methodology of information fusion [23], the efficiency and quality of intelligence products generated by node P depend on the knowledge level about adversary target status. The latter is closely related with the accuracy, timeliness and continuity of the target information sent from node O to node P. Of course, there is also static knowledge such as intelligence processing rules/processes, enemy equipment and operational regulations, but it has nothing to do with the target information sent from node O. For this reason, the awareness of adversary target status is chosen as the task-related knowledge for node P.

In this case, the force of information influence from node O to node P is calculated as the average change of knowledge level about adversary target status after node P receives the target information from node O. Suppose

the amount of target information sent from node O to node P is denoted as I_{OP}, the set of adversary targets to be aware of is denoted as $S_{OP}=\{\mathrm{at}_1,\mathrm{at}_2,\cdots,\mathrm{at}_n\}$, where n denotes the number of adversary targets, and the set of adversary targets that node P is truly aware of is denoted as S_{OP}'.

For node P, the knowledge level about target at_i is modeled as an uncertain fuzzy concept. Based on the fuzzy set theory, the following membership functions $U_{S_{OP}'}(\mathrm{at}_i)$ are constructed:

$$U_{S_{OP}'}(\mathrm{at}_i)=\begin{cases}1, & \mathrm{at}_i\in S_{OP}'\\ 0, & \mathrm{at}_i\notin S_{OP}'\end{cases} \tag{2}$$

where $U_{S_{OP}'}(\mathrm{at}_i)\in[0,1]$. The value of $U_{S_{OP}'}(\mathrm{at}_i)$ indicates the membership probability of target at_i for the set S_{OP}', thus representing the knowledge level of node P about target at_i. In the case that $U_{S_{OP}'}(\mathrm{at}_i)=1$, node P is completely aware of the status of target at_i, whereas in the other case, node P is not aware about the status of target at_i. The value of $U_{S_{OP}'}(\mathrm{at}_i)$ is related with I_{OP}, the amount of information sent to node P from node O. The awareness level about target at_i for node P can also be calculated according to the different propertiesof target at_i. It includes the IFF property knowledge level x_{i1}, quantity knowledge level x_{i2}, type knowledge level x_{i3}, position knowledge level x_{i4}, course knowledge level x_{i5}, speed knowledge level x_{i6} and damage status knowledge level x_{i7}. The overall knowledge level can be inferred as $U_{S_{OP}'}(\mathrm{at}_i)=\sum_{j=1}^{7}w_jx_{ij}$, where w_j is the weight of corresponding property j $(1\leqslant j\leqslant 7)$. It should be pointed out that the calculation of $U_{S_{OP}'}(\mathrm{at}_i)$ varies for different sensors and different combat scenarios.

Given the target set S_{OP}, the knowledge level about the target status can be represented with the fuzzy information entropy (denoted as H_{OP}):

$$\begin{aligned}H_{OP}=-k\sum_{i=1}^{n}&(U_{S_{OP}'}(\mathrm{at}_i)\cdot\log_2U_{S_{OP}'}(\mathrm{at}_i)+\\&(1-U_{S_{OP}'}(\mathrm{at}_i))\cdot\log_2(1-U_{S_{OP}'}(\mathrm{at}_i)))\end{aligned} \tag{3}$$

where k is a normalizing constant.

The smaller the value of fuzzy information entropy, the higher knowledge level about the adversary target status for node P. Suppose t_1 is the time before node O sends target information to node P, and t_2 is the time after node O sends the information to node P. According to (1) and (3), the force of information influence from node O to node P within the time interval $[t_1,t_2]$ (denoted as F_{OP}) is calculated as

$$F_{OP}=-\frac{H_{OP}(t_2)-H_{OP}(t_1)}{I_{OP}} \tag{4}$$

where $H_{OP}(t_1)$ refers to the knowledge level about target statusattime t_1, $H_{OP}(t_2)$ refers to the knowledge level about target status at time t_2, and I_{OP} refers to the average amount of information sent from node O to node P within the time interval $[t_1,t_2]$.

3.2 Force of information influence from node *P* to node *D*

Within the operational process of C4KISR system [24–27], the major role of node D is to conduct situational awareness according to the information sent from node D and develop military plans and orders based on the obtained knowledge about adversarial troop deployment, course of action and combat intention. According to operational command theory, C4KISR system design methodology and engineering practice [28,29], the inferred adversary intent is critical for commander to build up combat determination and develop military plans. For this reason, the inferred adversary intent is considered as the task-related knowledge for node D. Other knowledge about warfare regulations, combat tactics, equipment, troop deployment and battlefield environment is also related with decision making. However, it has little to do with the intelligence information sent from node P to node D. Of course, other knowledge closely related with the intelligence information also can be considered as the task-related knowledge for node D in different decision-making domains and at different command levels.

As a result, the force of information influence from node P to node D is calculated as the average change of knowledge level about adversary's intention given the amount of intelligence information sent from node P to node D.

Suppose that an adversary target is moving towards our control area from far to near, and the amount of intelligence information sent by node P to node D is denoted as I_{PD}. The information is about adversary target's attribute, subordinate relationship, type, location, course of action, etc. Suppose the set of all possible adversary intentions to be identified for node D is denoted as $S_{OP}=\{e_1,e_2,\cdots,e_m\}$, where m refers to the number of possible adversary's intentions. We assume only one adversary's intention is true. The adversary may intend to attack on our key defensive assets, attack and occupy strategic sites, conduct reconnaissance/harassment, conduct deterrence, etc.

With the adversarial target getting closer to our strategic location, defensive asset, important facility, etc., its

operational intention become sclearer and clearer for node D. It means that the possibility of a certain operational intention is getting higher. Therefore, the knowledge level of adversary's operational intention can be represented with the probabilities of adversary's operational intentions, denoted as $P(e_i)\,(1 \leqslant i \leqslant m)$. The inferred probabilities are related with the intelligence support ability, the operational scenarios, the status of target under attack, etc. The information entropy is used to measure the overall knowledge level about adversary's intentions as below:

$$H_{PD} = -k \sum_{i=1}^{m} P(e_i) \cdot \log_2 P(e_i) \tag{5}$$

where $k \geqslant 0$ is a normalizing constant.

The smaller the value of information entropy H_{PD}, the less uncertainty of adversary's operational intention for node D, and the higher possibility of a certain operational intention. Suppose t_1 denotes the time before node P sends intelligence information to node D and t_2 denotes the time after node P sends the information to node D. According to (1) and (5), the force of information influence from node P to node D within the time interval $[t_1, t_2]$ (denoted as F_{PD}) is computed as

$$F_{PD} = -\frac{H_{PD}(t_2) - H_{PD}(t_1)}{I_{PD}} \tag{6}$$

where $H_{PD}(t_1)$ denotes the knowledge level about the adversary's operational intention at time t_1 for node D, $H_{PD}(t_2)$ denotes the knowledge level about adversary's operational intention at time t_2 and I_{PD} denotes the average amount of information sent from node P to node D within the time interval $[t_1, t_2]$.

3.3 Force of information influence from node *D* to node *A*

Fire attack is the last step of the operational process for C4KISR system. The major role of node A is to use the fire control radar or guidance radar to identify, track, lock on and attack the adversary target according to the striking command sent by node D, including the target indication information. When the weapon launch conditions are met, the fire attack starts. Besides the factors related with the weapon platform and performance, the time interval between turning on the radar and meeting the condition is crucial for the strike effect. In a dynamic changing, complex and highly adversarial environment, the fire attack may be exposed due to electromagnetic radiation if the time interval is too long. It may provide the adversary a chance to escape or fire first. Therefore, the awareness of the immediate strike readiness is considered as the task-related knowledge for node A. It implies that the time interval between turning on the radar and meeting weapon launch conditions should be within a certain threshold. Other knowledge about weapon platform and performance, operational tactics, etc. is not considered as it is not directly related with the information sent from node D to node A.

For this reason, the force of information influence from node D to node A is calculated as the average change of knowledge level for node A about the immediate strike readiness when given the transmitted striking command information. The change of the knowledge level is caused by the striking command information sent from node D to node A. The similar approach could be applied for calculating the force of information influence from node O to node A for the transmitted target indication information.

Suppose the amount of striking command information sent from D node to node A is denoted as I_{DA}, the target to be struck by node A is denoted as T_{st}. It is considered as a random event that whether the fire control radar or guidance radar of node A is able to detect target T_{st} immediately after the radar is turned on. The random event is represented with a random variable X, with $X = 1$ indicating that the event occurs and $X = 0$ indicating that the event does not occur. The knowledge level for node A about immediate strike readiness is modeled with the information entropy. The information entropy is calculated as

$$\begin{aligned} H_{DA} = &-P(X=1) \cdot \log_2 P(X=1) - \\ &P(X=0) \cdot \log_2 P(X=0). \end{aligned} \tag{7}$$

The values of $P(X = 1)$ and $P(X = 0)$ are related with radar capabilities as well as the accuracy and timeliness of target indication information, operational scenarios and so on. The smaller value of information entropy H_{DA}, the less uncertainty about adversary target for immediate strike node A tends to have.

Suppose t_1 denotes the time before node D sends intelligence information to node A and t_2 denotes the time after node D sends the information to node A. According to (1) and (7), the force of information influence from node D to node A within the time interval $[t_1, t_2]$ is computed as

$$F_{DA} = -\frac{H_{DA}(t_2) - H_{DA}(t_1)}{I_{DA}} \tag{8}$$

where $H_{DA}(t_1)$ denotes the knowledge level for node A about immediate strike readiness at time t_1, $H_{DA}(t_2)$ denotes knowledge level about immediate strike readiness at time t_2 and I_{DA} is the amount of striking command information sent from node D to node A within the time interval $[t_1, t_2]$.

4. Simulation experiments

We simulated the scenarios of air attack and defense between the red and blue forces in key areas, as shown in Fig. 1. The red force has an air defense command post D1, an intelligence processing center P1, four ground-based air defense radars O1 – O4 and four fighters on patrol A1 – A4. The mission of the red force is to defend its key assets E1 – E5. The blue force has a fighter-bomber T1 and two escort fighters T2 and T3. The mission of the blue force is to destroy the key asset E3. After that, the blue force will stop attacking other assets of the red force and return. During the confrontation, the fighters of the blue force follows the predetermined route as shown in Fig. 1, and the ground-based radars of the red force send the information to the intelligence processing center after detecting the adversary fighters. The intelligence processing center P1 then sends the fused information to the command post D1. The command post will conduct its own fighters A1 – A4 to intercept the adversary fighters after discerning their intentions according to the received information.

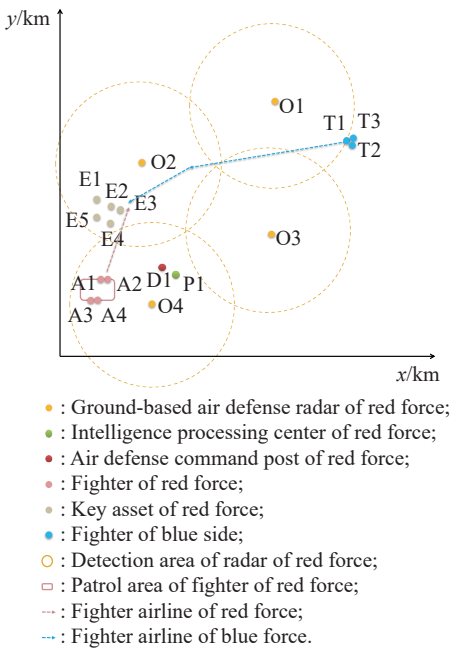


Fig. 1 Schematic diagram of simulation of air attack and defense scenarios

4.1 Simulation of force of information influence from node *O* to node *P*

According to (3) and (4), the force of information influence from the air defense radars to the intelligence processing center was calculated as the average change of knowledge level about the adversary target status for node P given the information sent from node O. The knowledge level about the adversary target status was calculated according to the recognition accuracy of six target properties as below.

(i) Recognition accuracy of IFF property

We assumed the IFF property of adversary target is either unknown, or adversary, or ours, or friend's, then the knowledge level about target IFF property is calculated as the corresponding recognition accuracy. During the process of target tracking, the IFF property for each target track in the same batch is evaluated. Suppose the number of target tracks with correct IFF attribute is denoted as N_a and the total number of evaluated target tracks is denoted as N_T, then the recognition accuracy of IFF property P_a can be calculated as

$$P_a = N_a / N_T. \tag{9}$$

(ii) Recognition accuracy of target type

We assumed the type of adversary fighter is either unknown, or large, or medium, or small. During the process of target tracking, the target types for each track obtained before and after information fusion are compared. Suppose the number of target tracks with correct types is denoted as N_C and the total number of evaluated target tracks is denoted as N_T, then the recognition accuracy of target type P_C can be calculated as

$$P_C = N_C / N_T. \tag{10}$$

(iii) Recognition accuracy of target number

We assumed that the number of adversary targets in a formation is generally one, two, three, four or fleet and the knowledge level about target number in a formation is calculated as the corresponding recognition accuracy. The number of adversary targets is evaluated for target tracks in the same batch. We denoted the number of target formations with correct target number as N_n and the total number of evaluated target formations as N_T. In this way, the recognition accuracy of target number P_n could be calculated as below:

$$P_n = N_n / N_T. \tag{11}$$

(iv) Recognition accuracy of target tracks

At first, all the points of a target track to be evaluated are aligned with the corresponding standard target tracks in time and space. Then, the standard target tracks are aligned to the target track to be evaluated and the positional difference is calculated. The evaluation proceeded from the start of target tracking to the end of target identification, during which the discarded target points are no longer considered. It is assumed that the threshold of distance measurement deviation for target tracks is σ_r.

According to the 3σ criteria, the deviation of distance measurement data will not exceed $[-3\sigma_r, 3\sigma_r]$ generally. Therefore, the knowledge level about target tracks could be calculated by the following equation:

$$\int_{-3\sigma_r}^{3\sigma_r} \frac{1}{\sqrt{2\pi}} \exp\left\{-\frac{1}{2\sigma_i{}^2}x^2\right\} \mathrm{d}x, \quad i = 1,2,3 \tag{12}$$

where σ_1, σ_2, and σ_3 are the distance measurement deviations of target tracks for the three air-defense radars respectively.

(v) Recognition accuracy of target speed and heading

The knowledge level about the target speed and heading are evaluated by comparing the detected target speed and heading against those of standard target tracks. Again, the evaluation proceeded from the start of target tracking to the end of target identification, during which the discarded target points are no longer considered. Therefore, the knowledge level about the target speed and heading are calculated by the following equation:

$$\int_{-3\sigma_l}^{3\sigma_l} \frac{1}{\sqrt{2\pi}} \exp\left\{-\frac{1}{2\sigma_{lj}{}^2}x^2\right\} \mathrm{d}x, \quad l = v,c; j = 1,2,3 \tag{13}$$

where σ_{v1}, σ_{v2} and σ_{v3} are the standard deviations of speed measurements for air defense radars O_1, O_2 and O_3 respectively; σ_{c1}, σ_{c2}, and σ_{c3} are the standard deviations of heading measurements for air defense radars O_1, O_2, and O_3, respectively; σ_v, σ_c are the required measurement deviations for target speed and heading respectively.

(vi) Knowledge level about target status

Based on the above calculation, the weights fortarget IFF properties, quantities and types as well as their positions, speeds and headings are calculated according to the advice from consulted experts with rich engineering experience, as shown in Table 1.

Table 1 Weight distribution

Status index	Weight
IFF	0.25
Quantity	0.15
Type	0.10
Position/km	0.25
Speed/(km/h)	0.15
Heading/radian	0.10

Then knowledge level about the overall target status is calculated as below:

$$U_{S_{OP}}(\mathrm{at}_i) = \sum_{j=1}^{6} w_j \cdot x_{ij} \tag{14}$$

where w_j is the weight of IFF, quantity, type, position, speed, heading, and x_{ij} is the recognition accuracy of IFF, quantity, type, position, speed, heading at time t_i.

According to (14), the force of information influence from the ground-based air defense radars to the intelligence processing center is calculated for the red force after the fighters of the blue force entered the detection range of the red force. The experimental results are shown in Fig. 2.

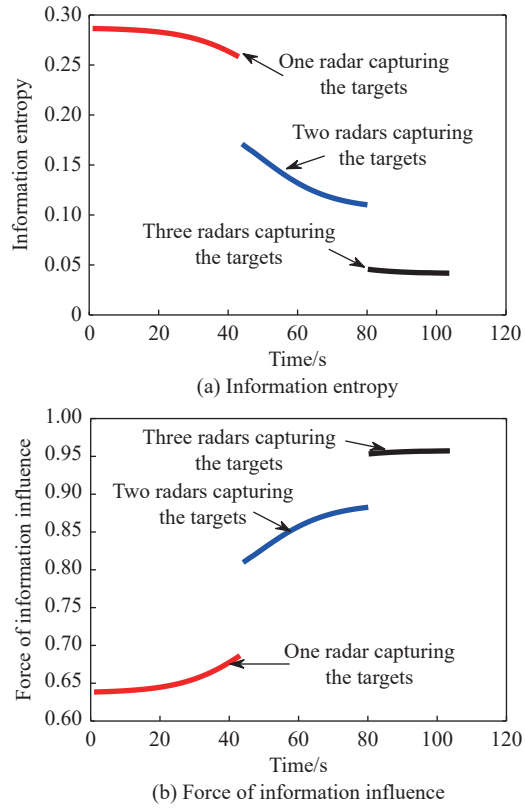
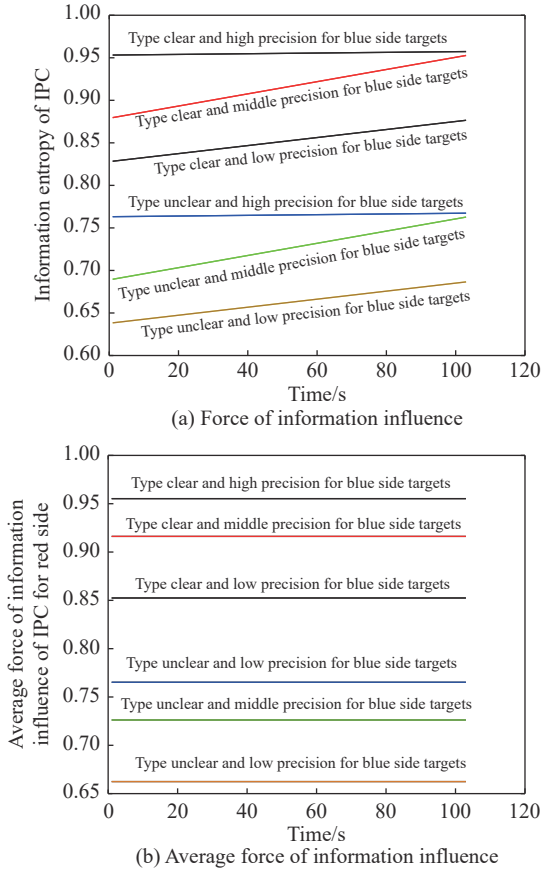


Fig. 2 Evaluation of the information entropy and force of information influence from the air defense radars to the intelligence processing center

As the fighters of the blue force go deeply into the red force square, the number of detected fighters by the red-force increased. As can be seen, the value of information entropy for the intelligence processing center of the red force decreased with time as shown in Fig. 2(a), while the value of force of information influence from the air defense radars to the intelligence processing center increased with time as shown in Fig. 2(b). This implied that the target status information about the adversary fighters of the blue force provided by the air defense radars increases the knowledge level about the adversary target status for the intelligence processing center significantly.

We also evaluate the force of information influence from the air defense radars to the intelligence processing

center for the red force in cases with different information accuracy and integrity. The corresponding experimental results are provided in Fig. 3.



(a) Force of information influence

(b) Average force of information influence

Fig. 3 Evaluation of force of information influence from air defense radars to intelligence processing center when varying the information accuracy and integrity

As can be seen from Fig. 3, the higher the information accuracy and integrity, the larger value of force of information influence the intelligence processing center tendes to have. This indicates that there is a positive correlation between the information quality and the force of information influence from the air defense radars to the intelligence processing center.

4.2 Simulation of force of information influence from node *P* to node *D*

To infer the force of information influence from the intelligence processing center P1 to the command post D1 as illustrated inequation (6), we calculate the probabilities of being attacked for defensive assets E1 – E5 first. Given the information sent from the intelligence processing center P1, the probability of being attacked for each defensive asset is calculated based on the information about its type, position, course and importance. The calculation included the following steps.

(i) We judged whether the incoming adversary target had the ground attack capability according to its type. If that is not the case, the probability of being attacked for the defensive assets would beset as zero, and the calculation finished.

Specifically, in case that the incoming targets are identified as reconnaissance aircraft, transport aircraft, electronic jammers, early warning aircraft, etc., the probability of being attacked for each defensive asset is set as zero. In case that the incoming targets are identified as fighters, attack aircraft, bombers, etc., the probability of being attacked for each defensive asset needs further inference. In the case that the type of incoming target could not be identified, it would be treated as a fighter.

(ii) According to the type of the incoming target, we inferred its attack range, including long-range, medium-range and short-range. If the target type could not be identified, its attack range will be set as the average range of all possible target types. Specifically, if the target type is known, its attack range will be calculated according to its conventionally equipped weapons. On the other hand, if the target type is unknown, the average range of all possible target types will be used for that target.

(iii) According to the position, course and attack range of the incoming target, the different attack areas of the incoming target are obtained, as shown in Fig. 4.

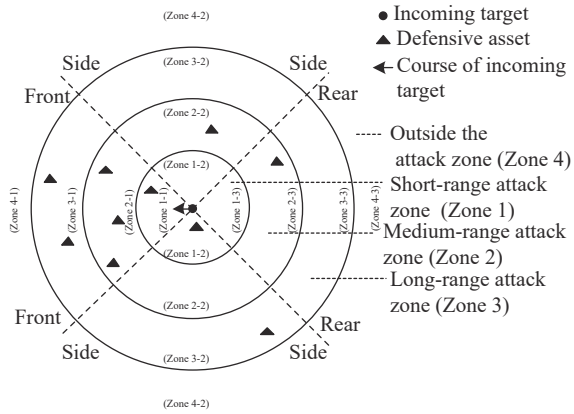


Fig. 4 Schematic diagram of attack areas of the incoming target

Specifically, as the incoming target might carry short-range, medium-range and long-range surface-to-air missiles, we divide the possible attack area of the incoming target into four zones, including the short-range attack zone (Zone 1), medium-range attack zone (Zone 2), long-range attack zone (Zone 3), and outside zone (Zone 4) accordingly. Based on the front, side and rear position relative to the incoming target, we further partition the short-range attack zone (Zone 1) into Zone 1-1, Zone 1-2 and Zone 1-3 respectively, the middle-range attack zone

(Zone 2) into Zone 2-1, Zone 2-2 and Zone 2-3 respectively, the long-range attack zone (Zone 3) into Zone 3-1, Zone 3-2 and Zone 3-3 respectively and outside zone (Zone 4) into Zone 4-1, Zone 4-2 and Zone 4-3 respectively.

(iv) We assume that all the defensive assets in an attack zone are considered as a defensive asset group as a whole. The probability of being attacked for each defensive asset group is calculated as follows.

In case that there was only one defensive asset group in a zone among Zone 1, 2, 3 and 4, the probability of being attacked for the defensive asset group is set as 1. In case that the defensive asset groups are distributed across two zones, the probabilities of being attacked for the defensive asset group in the inner zone and outer zone are set as $\alpha\ (0<\alpha<1)$ and $1-\alpha$ respectively. When the defensive asset groups are distributed across three different zones, the probabilities of being attacked for the defensive asset groups are specified as α, $\alpha(1-\alpha)$ and $1-\alpha-\alpha(1-\alpha)$ for the inner, middle and outer zones respectively. In the other case that the defensive asset groups are distributed across all the four zones, the probabilities of being attacked are specified as α, $\alpha(1-\alpha)$, $\alpha(1-\alpha-\alpha(1-\alpha))$ and $1-\alpha-\alpha(1-\alpha)-\alpha(1-\alpha-\alpha(1-\alpha))$ for Zone 1, 2, 3 and 4 respectively.

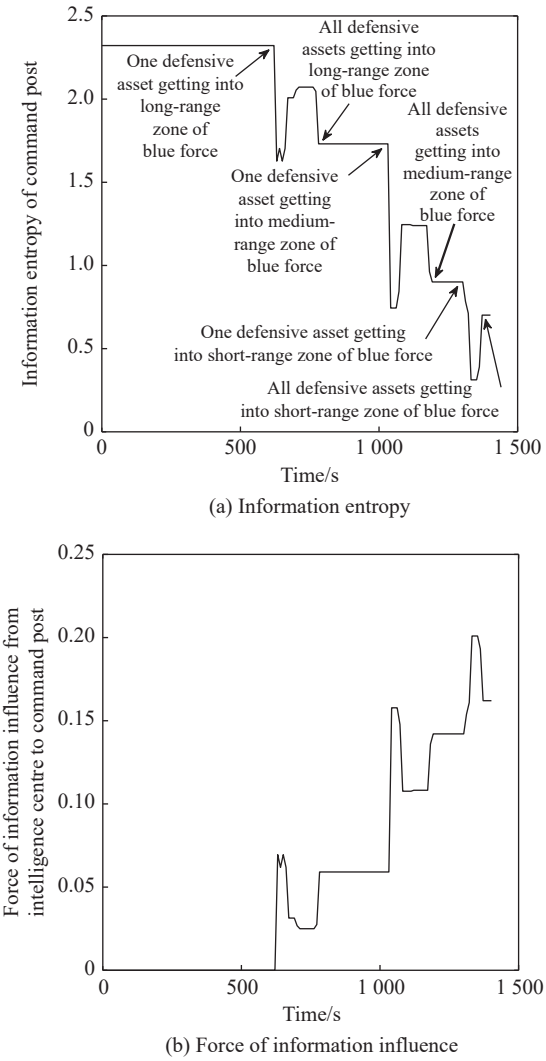
If there is a defensive asset group in Zone i $(1\leqslant i\leqslant 4)$, then the probability of being attacked for this defensive asset group is denoted as p_i. When the defensive asset group is distributed in only one zone among Zone i−1, i−2 and i−3, the probabilities of being attacked for the defensive asset group is set as p_i. When the defensive asset groups are distributed across two zones among Zone i−1, i−2 and i−3, the probabilities of being attacked for the defensive asset group in the inner and outer zone are set as $\beta p_i\ (0<\beta<1)$ and $(1-\beta)p_i$ respectively. When the defensive asset groups are distributed across all the three zones of Zone i−1, i−2 and i−3, the probabilities of being attacked for the defensive asset group in Zone 1, 2 and 3 are set as βp_i, $\beta(p_i-\beta p_i)$ and $p_i-\beta p_i-\beta(p_i-\beta p_i)$ respectively.

(v) We calculated the probability of being attacked for each defensive asset according to the importance level of defensive assets. Suppose there is a defensive asset group in Zone n−m $(1\leqslant n\leqslant 3, 1\leqslant m\leqslant 3)$, the probability of being attacked for the group is denoted as p_{nm} and the number of defensive assets in the group is denoted as N, then the N defensive assets will be sorted in descending order of importance level, denoted as $g_1\prec g_2\prec\cdots\prec g_N$ and the probability of being attacked for each asset $P(g_i)$ will be calculated as

$$P(g_i)=\begin{cases}\gamma p_{nm}, & i=1\\ \gamma\left(p_{nm}-\sum\limits_{j=1}^{i-1}P(g_j)\right), & 2\leqslant i\leqslant N-1\\ p_{nm}-\sum\limits_{j=1}^{i-1}P(g_j), & i=N\end{cases}\tag{15}$$

where γ is a constant within interval $(0,1)$. Suppose there is a defensive asset group in Zone 4−m $(1\leqslant m\leqslant 3)$ and its probability of being attacked is denoted as $p_{4,m}$, the number of defensive assets in the group is N, then the probability of being attacked for each asset in the group is calculated as $p_{4,m}/N$.

According to (6), the force of information influence from the intelligence center to the command post of the red force in the simulation experiment is calculated, as shown in Fig. 5.



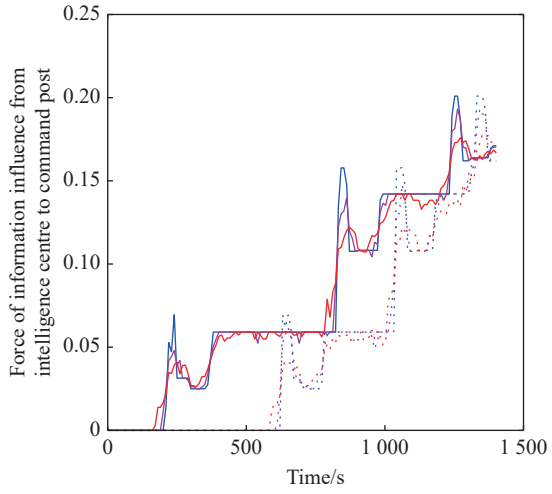
(a) Information entropy

(b) Force of information influence

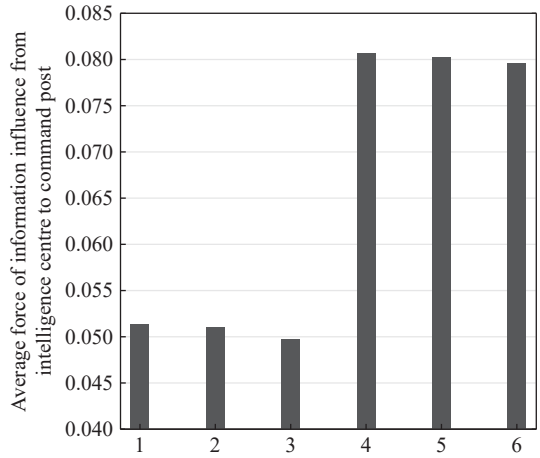
Fig. 5 Evaluation of the force of information influence from the intelligence processing center to the command post for the red force

As can be seen from Fig. 5(a), the information entropy of the command post of the red force for adversary's intention decreased with time. That is, the adversary's intention is getting more and more obvious. With only one defensive asset of the red force getting into a certain attack range of an adversary target of the blue force, the information entropy decreased significantly. This indicates the command post tended to think the adversary's intention is to attack the asset. With the defensive assets getting into a certain attack range of the adversary target of the blue force one by one, the value of information entropy fluctuated sharply. This indicates that there is a certain degree of ambiguity about the adversary's intention. With all the defensive assets getting into a certain attack range of the adversary target, the information entropy decreased again and remained stable afterwards. This indicates that the awareness level about the adversary intention for the command post of the red force is getting higher. As shown in Fig. 5(b), we can see that the force of information influence from the intelligence center to the command post is on a rise, indicating that the information sent from the intelligence center increased the knowledge level of the command post significantly.

Then we evaluate the force of information influence from the intelligence center to the command post when varying the information accuracy and integrity. The experimental results are illustrated in Fig. 6.



(a) Force of information influence



1: Low information integrity and high information accuracy;
2: Low information integrity and medium information accuracy;
3: Low information integrity and low information accuracy
4: High information integrity and high information accuracy;
5: High information integrity and medium information accuracy;
6: High information integrity and low information accuracy.

(b) Average force of information influence

Fig. 6 Evaluationof force of information influence from the intelligence processing center to the command post for the red force when varying information accuracy and integrity

As can be seen from Fig. 6, the higher level of the accuracy and integrity of the information sent from the intelligence processing center to the command post, the larger value the corresponding force of information influence tended to have. This indicates that there is a positive correlation between the information quality and the force of information influence-from the intelligence processing center to the command post.

4.3 Simulation of force of information influence from node *D* to node *A*

To calculate the force of information influence from the command post D1 to its fighter A1 according to (8), we compute the detection probability of adversary target by fighter A1 first, assuming fighter A1 is under the command of the command post of the red force.

Firstly, we only consider the position measurement error of adversary fighter T1 of the blue force and the transmission delay of the target indication information sent from command post D1 to fighter A1 while the measurement error of the speed and course of the adversary fighter T1 are ignored. At time t, the reported position and the true position of the adversary fighter T1 are shown in Fig. 7 after fighter A1 received the target indication information from command post D1.

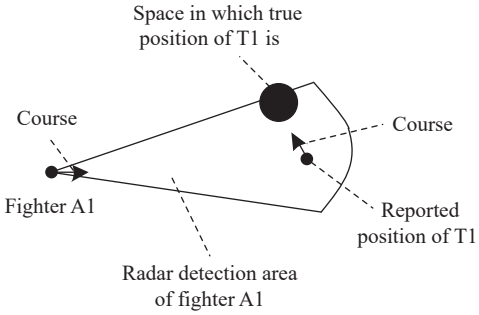


Fig. 7 Reported and true positions of adversary fighter T1 at time t

We denote the true polar-coordinate position of adversary fighter T1 as (r,α,β) and calculated the corresponding detection probability $P(r,\alpha,\beta)$ of fighter T1 by fighter A1 with its fire control radar turned on as follows:

$$P(r,\alpha,\beta)=\begin{cases}0, & (r,\alpha,\beta)\notin S_A\\ f(d), & (r,\alpha,\beta)\in S_A\end{cases} \tag{16}$$

where S_A indicates the cone area of radar detection of fighter A1, d indicates the distance from fighter A1 to the true position of adversary target T1 and $f(d)$ indicates the function of detection probability, which is calculated based ondistance d. Function $f(d)$ is related with the characteristics of the radar itself. Considering that the true position of adversary fighter T1 is in a spherical space, the detection probability of adversary fighter T1 at time t by fighter A1 is calculated as follows:

$$P(t)=\frac{\int_0^{2\pi}\int_0^{2\pi}\int_0^{l}P(r,\alpha,\beta)\mathrm{d}r\mathrm{d}\alpha\mathrm{d}\beta}{4\pi l^3/3} \tag{17}$$

where l indicates the position measurement error of adversary fighter T1. Assume the fire control radar of fighter A1 was turned on at time t. Then the condition of the radar to lock the adversary fighter is that the adversary fighter can be detected by the radar continuously from time t to $t+T$, where T is a constant whose value is related with the radar itself. The lock probability of adversary fighter by fighter A1 is calculated as follows:

$$P_{\mathrm{A}}=\frac{\int_t^{t+T}P(t)\mathrm{d}t}{T}. \tag{18}$$

It should be noted that the relative positions between fighter A1 and adversary fighter T1 during the time interval $[t,t+T]$ needed to be considered when calculating the probability P_{A}. Since the time interval is relatively short, we assume that the speed and course of adversary fighter T1 as well as the speed of fighter A1 remain unchanged while fighter A1 turns to the front of the adversary fighter at a uniform angular velocity.

Secondly, we further take the measurement error of the speed and course of the adversary fighter into consideration. The reported position and course of adversary fighter T1 are shown in Fig. 8. We represent its ground-truth course with an arrow pointing from the reported position to a polar-coordinate point (λ,γ) on a unit circle with its center as the origin point. The circle plane is perpendicular to the reported course of the adversary fighter and the intersected point is the center of the unit circle.

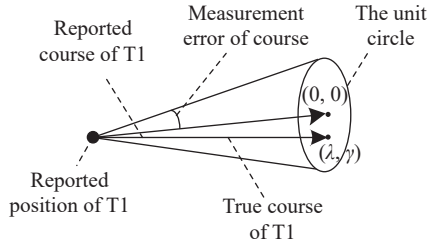
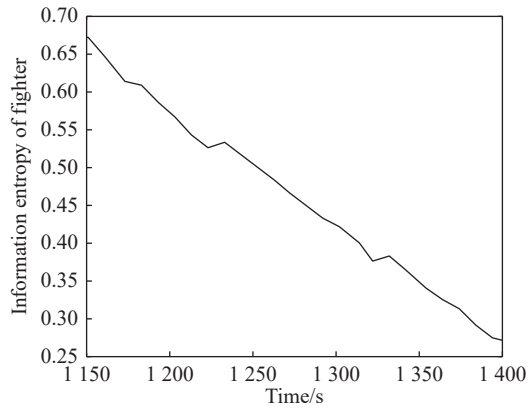


Fig. 8 Reported position and course of the adversary fighter of the blue force

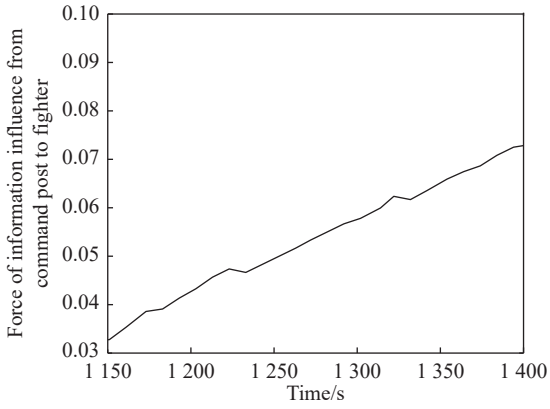
Recall that the detection probability of the adversary fighter at time t is P_{A} in (18) when the measurement errors of its speed and course are not considered. As the value of P_{A} is affected by factors v,λ and γ, we denoted it as $P_{\mathrm{A}}(v,\lambda,\gamma)$, where v indicates the speed of the adversary fighter. The measurement error of speed is noted as Δv and the measurement error of course is represented with a unit circle plane above. In this way, the average detection probability $P_{\mathrm{A}}^{\mathrm{Avg}}$ of adversary fighter T1 by fighter A1 could be calculated as follows:

$$P_{\mathrm{A}}^{\mathrm{Avg}}=\frac{\int_0^{2\pi}\int_0^{1}\int_{v-\Delta v}^{v+\Delta v}P_{\mathrm{A}}(v,\lambda,\gamma)\mathrm{d}v\mathrm{d}\lambda\mathrm{d}\gamma}{2\Delta v\pi}. \tag{19}$$

According to (8), the force of information influence from the command post D1 to fighter A1 of the red force was calculated. The experimental results are shown in Fig. 9, assuming the adversary fighter T1 already entered the radar detection area of fighter A1.



(a) Information entropy

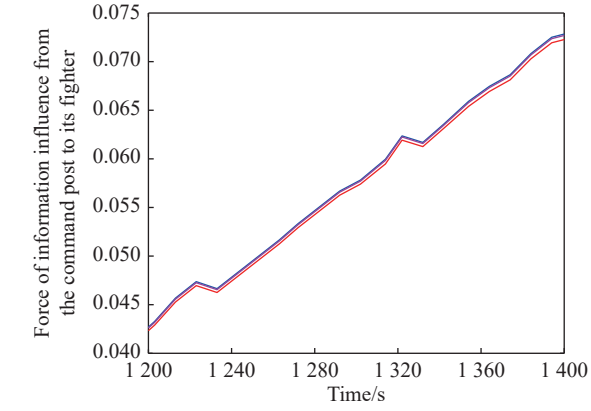


(b) Force of information influence

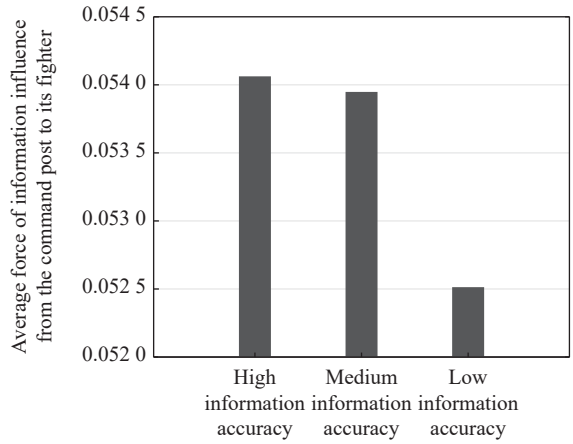
Fig. 9 Evaluation of force of information influence from command post D1 to fighter A1

As can be seen from Fig. 9, after adversary fighter T1 entered the radar detection area of fighter A1, the information entropy of fighter A1 exhibited a downward trend while the force of information influence from command post D1 to fighter A1 exhibited an upward trend. This indicates that the target indication information sent from command post D1 contributed significantly to the detection of adversary fighter T1. Next, we evaluated the force of information influence from command post D1 to fighter A1 when varying the information accuracy. The experimental results are shown in Fig. 10.

As can be seen from Fig. 10, the higher the information accuracy, the larger value the average force of information influence tends to have. The result indicates that there is a positive correlation between the information accuracy and the force of information influence from command post D1 to fighter A1.



(a) Force of information influence



(b) Average force of information influence

Fig. 10 Evaluation of the force of information influence from command post D1 to fighter A1 when varying the information accuracy

5. Conclusions

This paper studies how to evaluate the information circulation between C4KISR system nodes of sensing, intelligence processing, decision making and fire attack in the dynamic battlefield environment. We propose a framework of force of information influence for the four types of nodes in C4KISR system. Firstly, we propose the basic framework of force of information influence force between nodes and the corresponding mathematical definition. Secondly, based on the theory of information entropy, the models of force of information influence between nodes of sensing (O), intelligence processing (P), decision making (D) and fire attack (A) are established. Thirdly, the feasibility and effectiveness of our framework of force of information influence are evaluated under a simulated air defense and attack scenario. Our future work is to evaluate our framework of force of information influence in practical systems and apply it for the design and optimization of C4KISR system.

References

[1] GAO J R, LIAO Y Y, GAO J. The connotation of information warfare. Electronic Information Warfare Technology, 2020, 35(3): 50–53. (in Chinese)

[2] LONG J, LIU D S. Overview of information superiority measurement methods. Journal of Ordance Equipment Engineering, 2018, 39(10): 168–172. (in Chinese)

[3] LI L L, LU Y F, ZHUANG Z, et al. Construction and modeling of indicator system of accusation system based on information superiority. Systems Engineering and Electronics, 2018, 40(3): 577–582. (in Chinese)

[4] ZIBETTI G R, WICKBOLDT J A, FREITAS E P D. Context-aware environment monitoring to support LPWAN-based battlefield applications. Computer Communications, 2022, 189: 18–27.

[5] ALBERT D, GARSTKA J. The basic principles and measurement of network centric operations. LANCO research center. Trans. Beijing: National Defense Industry Press, 2007. (in Chinese)
[6] SOPILKO I, SVINTSYTSKYI A, KRASOVSKA Y, et al. Information wars as a threat to the information security of Ukraine. Conflict Resolution Quarterly, 2021, 39(3): 333–347.
[7] ZHANG J G. Mobilization of the technique and information resources in the information war. Journal of Academy of Equipment, 2012, 23(2): 22–27.
[8] LIANG S, SHI H, LI Z D, et al. Generalized Lanchester war model for information warfare. Mathematics in Practice and Theory, 2017, 47(9): 291–296.
[9] WAGENHALS L W, SHIN I, KIM D, et al. C4ISR architectures: II. A structured analysis approach for architecture design. Systems Engineering, 2000, 3(4): 248–287.
[10] LI X M, LI Z F, DAI J J, et al. Research on architecture of networked targeting system based on C4KISR. Electronics Optics & Control, 2012, 19(1): 1–4, 37. (in Chinese)
[11] ZHANG J G. Information entropy-theory and application. Beijing: China Water Resources and Hydropower Press, 2021. (in Chinese)
[12] CIFTCIOGLU E N, YENER A, GOVINDAN R, et al. Operational information content sum capacity: from formulation and examples. Proc. of the 14th International Conference on Information Fusion, 2011: 5−8.
[13] BAR-NOY A, CIRINCIONE G, GOVINDAN R, et al. Quality-of-information aware networking for tactical military networks. Proc. of the IEEE International Conference on Pervasive Computing and Communications Workshops, 2011: 2−7.
[14] CANSEVER D. Value of information. Proc. of the IEEE Military Communications Conference, 2013: 1105−1108.
[15] KONG R Y, SHEN Y L, XIAO T S, et al. Research on battlefield information value measurement model based on information entropy. Journal of China Institute of Electronic Science, 2019, 2: 139–145. (in Chinese)
[16] HE Y, NIU R X, TONG L Z. Value analysis and application of decision information based on transfer entropy. Value Engineering, 2013, 15: 159–160.
[17] LIU W G, ZHANG G A, WANG W, et al. Research on digital operational command. Beijing: PLA Press, 2012. (in Chinese)
[18] JIA G H, ZHOU J, LI J Y. Reliability evaluation of command information system under different attack modes. IOP Conference Series: Materials Science and Engineering, 2021, 1043(3): 032051.
[19] EDWARD W. Information warfare: principles and operations. Norwood: Artech House, 1998.
[20] HU X F. War engineering theory-war methodology towards the information age. Beijing: Science Press, 2017. (in Chinese)
[21] TIMOTHY L T. Kosovo and the current myth of information superiority. Parameters, 2020, 30(1): 13−29.
[22] HYUN S Y, LEE D H, LEE G, et al. A study on the information superiority of network centric warfare of future battlefield. Proc. of the International Conference on information Science and Security, 2008: 224−231.
[23] ZHANG Y, XIAO Q L, DENG X Y, et al. A multi-source information fusion method for ship target recognition based on Bayesian inference and evidence theory. Journal of Intelligent & Fuzzy Systems: Applications in Engineering and Technology, 2022, 42(3): 2331–2346. (in Chinese)
[24] LI Y F, HUANG H Z, ZHANG T Y. Reliability analysis of C4ISR systems based on goal-oriented methodology. Applied Sciences, 2021, 11(14): 6335.
[25] ARIFIN H, IWAN N, LAILATUL Q, et al. Evaluating the interoperability of C4ISR system using cyber six-ware framework. Proc. of the International Conference on Advanced Computer Science and Information Systems, 2021: 1−7.
[26] JIAO Z Q, ZHANG J Y, YAO P Y, et al. C4ISR service deployment based on an improved quantum evolutionary algorithm. IEEE Trans. on Network and Service Management, 2021, 18(2): 2405–2419.
[27] LAN Y S, YI K, WANG H, et al. Delay assessment method for networked C4ISR system architecture. Systems Engineering and Electronics, 2013, 35(9): 1908–1914. (in Chinese)
[28] DONG Q C, WANG Z X, CHEN G Y, et al. Domain-specific modeling and verification for C4ISR capability requirements. Journal of Central South University of Technology, 2012, 19(5): 1334–1340. (in Chinese)
[29] LAN Y S, DENG K B, MAO S J, et al. Adaptive evolvement of information age C4ISR structure. Journal of Systems Engineering and Electronics, 2015, 26(2): 301–316.

Biographies

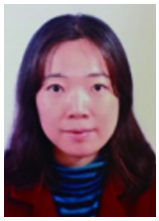
MAO Shaojie was born in 1963. He received his M.S. degree from Nanjing University, China. He is a senior engineer working in Science and Technology on Information Systems Engineering Laboratory. His research interest is information systems engineering.
E-mail: maoshaojie@163.com

DIAO Lianwang was born in 1965. He received his Ph.D. degree from Nanjing University of Science and Technology, China. He is a senior engineer working in Science and Technology on Information Systems Engineering Laboratory. His research interests include command information system and optimization theory.
E-mail: diaolw@sina.com

SUN Yu was born in 1989. He received his Ph.D. degree from Air Force Engineering University, China. He is an engineer working in Information Systems Engineering Laboratory of Science and Technology. His research interest is information systems engineering.
E-mail: suny.z@qq.com

WANG Heng was born in 1977. He received his Ph.D. degree from Nanjing University of Science and Technology, China. He is a senior engineer working in Science and Technology on Information System Engineering Laboratory. His research interest is information systems engineering.
E-mail: wangheng@gmail.com

YI Kan was born in 1981. He received his Ph.D. degree from Nanjing University of Posts and Telecommunications, China. He is a senior engineer working in Science and Technology on Information System Engineering Laboratory. His research interest is information systems engineering.
E-mail: yikan@gmail.com



XU Xin was born in 1978. She received her Ph.D. degree in data mining at the School of Computing from National University of Singapore. She is currently a senior engineer working in Science and Technology on Information System Engineering Laboratory. Her research interests include machine learning, unmanned autonomous system and intelligent decision making.
E-mail: xinxu_nriee@sina.com

MAO Xiaobin was born in 1981. He received his Ph.D. degree from Nanjing University of Aeronautics and Astronautics. He is currently a senior engineer working in Science and Technology on Information System Engineering Laboratory. His research interest is information systems engineering.
E-mail: maoxiaobin@cetc.com.cn

ZHANG Kecheng was born in 1990. He received his Ph.D. degree in data mining from Beijing University of Posts and Telecommunications. He is currently an engineer working in Science and Technology on Information System Engineering Laboratory. His research interest is on information systems engineering.
E-mail: buptzkc@163.com

SHENG Long was born in 1989. He received his Ph.D. degree from Nanjing University of Aeronautics and Astronautics. He is currently an engineer working in Science and Technology on Information System Engineering Laboratory. His research interest is information systems engineering.
E-mail: shenglong@cetc.com.cn