An integrated network/firepower operation model based on Lanchester equation

Jin Xing Liu[1], **Shi Hong Xu**[2], **Jin Song Gao**[3], **Yi Qin Yuan**[4]
[1, 2]The First Aeronautical College of Air Force, Xinyang, 464000, P. R. China
[1, 3, 4]Science and Technology on Electro-Optic Control Laboratory, Luoyang, 471009, P. R. China
[2]Corresponding author
E-mail: [1]*drljx@163.com*, [2]*lixiang8488@sina.com*, [3]*jsgao@263.net*, [4]*shadow_YYQ@126.com*

Received 9 January 2018; accepted 19 February 2018
DOI https://doi.org/10.21595/vp.2018.19620

Abstract. In this paper, an analysis is made to the network/firepower integrated combat mode based on the development trend of future combat equipment and existing combat cases. Then, the system dynamics model of network/firepower integrated strike is established based on the mechanism of network reconnaissance/attack and firepower attack. The Attrition-Rate Coefficients model of network/firepower combat is established by studying the effectiveness evaluation method of network attack and firepower attack. The Lanchester model of network/firepower integrated confrontation covering normal nodes, infected nodes and all infected nodes is established. In order to study the dynamic, uncertain network counter process, a type of the vibration network attack is introduced to Lanchester equation and its effectiveness in network attack process is discussed by means of the simulation results.

Keywords: network attack, firepower attack, integrated operation, Lanchester equation, performance analysis.

1. Introduction

In the future wars, the cooperative combat with the integration of network reconnaissance, network attacking, electronic attacking, and firepower attacking will become the main combat mode [1]. Therefore, with the development of the equipment for network and electronic attacking, it is necessary to study the simulation and the resource planning methods of the integrated combat of network attack, electronic attack, firepower and other different types of forces, so as to use the resources reasonably [2-8]. With the arrival of information war, the classical Lanchester equation is difficult to adapt to the modern information war and meet the demand of the war. In recent years, scholars studied the Lanchester equation under the condition of information [5-10]. In the literature [5], the Lanchester equation of the electronic counter/fire model and force assignment algorithm is studied based on Cooperative combat of electronic warfare and fire strike force. Literature [6-8] focuses on the influence of information on operational effectiveness from the aspect of information support. Literature [9] makes improvement to the classic Lanchester equation and establishes the model of a network attack process. Based on the virus-spread ideas, the network attack effect on combat firepower of war between entities is studied in [10], which ignore the dependency of effectiveness of network attacks on network reconnaissance. In order to evaluate the network/firepower integrated attack effectiveness, in this paper, the combat mode of the network/firepower attack integrated operation is put forward, and its dynamics are given, a method for calculating the force attrition is presented, and a cooperative combat model of network /firepower attack is built based on Lanchester equation.

2. Integrated network/firepower attack operation modeling

2.1. Integrated network/firepower attack operation process

An integrated network/firepower strike situation is given in Fig. 1. The role of the Red side is executor of the integrated network /firepower attack, and that of the blue is air defense. The red force includes: network reconnaissance, network attack, aerial escort, air strike formation. The

Blue includes sensor, control center, anti-aircraft weapons, and interceptor aircraft. Each combat unit of the Blue side is connected through the network. The red network reconnaissance unit receives the enemy radiation signal for recognition, positioning, and analyzing, gets the enemy command and control network topology and the weak point, makes combat decisions for network attacks and firepower attacks, and distributes the decisions to the attacking units. The network attack unit fight against the enemy network to paralyze the enemy command and control network. After the enemy network get paralysis, the firepower attacking unit will fire at the pre-assigned target. The escort airplane formation will escort the network reconnaissance and attack unit. Sensors of the Blue side detect the intrusion of the red side, and report to the allegations center, and the command center will guide ground anti-aircrafts fire and interceptor aircrafts to intercept the invasion forces of the red.

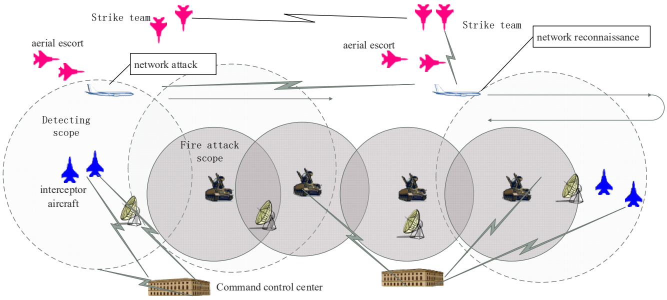


Fig. 1. Network / firepower integrated combat situation

2.2. System dynamics model

System dynamics is an influence diagram for describing mutual destruction of the two sides (Fig. 2), which is the foundation of Lanchester equation. The network attack makes soft killing to the enemy combat unit, through virus infection of the enemy software system, tampering with the command control commands, and other methods of false target deception. Soft killing cannot lead to the decrease of the number of enemy combat platforms, but can directly or indirectly lead to loss or degraded combat effectiveness of the enemy combat platform in a certain period of time or in the whole course of war.

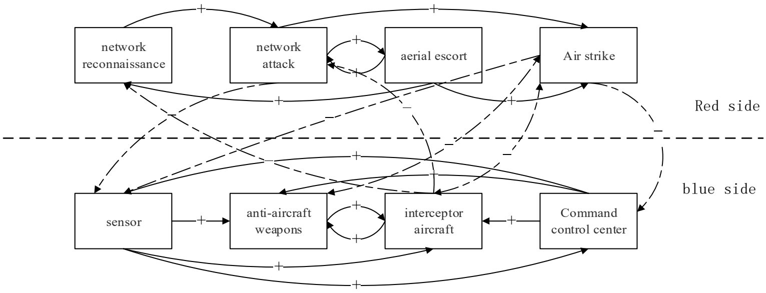


Fig. 2. System dynamics description

2.3. Lanchester equation modeling

The necessary condition for launching the guided weapons is that the target is captured by sensor and enter the effective firing range. The fire between the guided weapons can be described by Lanchester square law. The implementation of a network attack is to enter an effective range of enemy wireless energy radiation and to obtain enemy information. Therefore, the Lanchester square law [8] is applied to describe the network operation between ourselves and the enemy.

2.3.1. Model of attrition-rate coefficients under network attack

In order to simplify the research, the working condition of each unit in the enemy's command and control system after a cyber-attack is classified into three states: the normal state, the state of operational efficiency decline, and the loss of combat effectiveness. For example, after our implementation of virus attacks on the enemy's command and control network, one of the following effects will appear: the enemy's command and control network is not infected, or some computers in one system of the network are infected, or the entire computer system is infected, resulting in a complete paralysis of the system. Therefore, the three states are introduced to connote the states of the computers in the enemy's command and control system after cyber-attack. After the cyber-attack, the enemy may use antivirus software to kill virus, or use the backup system to restore the computer system. Therefore, these three states can be converted to each other.

When the computer virus is injected into the command and control network, the virus can be transmitted in the command and control network. The influence of the command and control network on the enemy can be expressed in the following formula:

$$\begin{cases}\dot{y}_0(t)=-\lambda_1 y_0(t)+\lambda_4 y_1(t)+\lambda_6 y_2(t),\\ \dot{y}_1(t)=-\lambda_3 y_1(t)+\lambda_1 y_0(t)+\lambda_5 y_2(t),\\ \dot{y}_2(t)=\lambda_3 y_1(t)+\lambda_2 y_0(t)-\lambda_5 y_2(t)-\lambda_6 y_2(t),\end{cases} \tag{1}$$

where, y_0, y_1 and y_2 is the infection status of the computer, i.e. normal, partial infection, all infection; λ_1, λ_2,…, λ_6 are the transition probability of the infection state of the computers respectively.

2.3.2. Lanchester equation for network / firepower integrated strike

Suppose, x_d is the network reconnaissance unit of the Red side, x_{na} is the network attack unit of the Red side, x_{hh} is the escort team, x_a is the attack team; y_r is the radar of the Blue side, y_{aam} is the anti-air missile; y_{lj} is the intercept team, y_{comm} is the command and control unit. The Lanchester model is show as following:

$$\begin{cases}\dot{x}_d(t)=-a_{lj}\sum_{k=0}^{k}\mathrm{a_i}y_{ljk}(t),\\ \dot{x}_{na}(t)=-a_{lj}\sum_{k=0}^{k}\mathrm{a_i}y_{ljk}(t)-a_{aam}\sum_{j=0}^{m}a_j y_{aam_\mathrm{j}}(t)+Rif(t),\\ \dot{x}_{hh}(t)=-a_{lj}\sum_{k=0}^{k}\mathrm{a_i}y_{ljk}(t)-a_{aam}\sum_{j=0}^{m}a_j y_{aam_\mathrm{j}}(t),\\ \dot{x}_a(t)=-a_{lj}\sum_{k=0}^{k}\mathrm{a_i}y_{lji}(t)-a_{aam}\sum_{j=0}^{m}a_j y_{aam_\mathrm{j}}(t),\\ \dot{y}_{ri}(t)=-b_{hh}d_i x_{hh}(t)-\sum_{i=0}^{m}\lambda_{ik}y_{ri}(t),\\ \dot{y}_{aamj}(t)=-b_{hh}e_i x_{hh}(t)+\sum_{i=0}^{m}\lambda_{jk}y_{aami}(t),\\ \dot{y}_{ljk}(t)=-b_{hh}f_i x_{hh}(t)+\sum_{k=0}^{m}\lambda_{kk}y_{ljk}(t),\\ \dot{y}_{commi}(t)=-b_a g_i x_a(t)+\sum_{i=0}^{m}\lambda_{ik}y_{lji}(t),\end{cases} \tag{2}$$

where a_i is the efficiency discount factor, represents the decline in the effectiveness of the Blue weapon system after a cyberattack; d, g, f, h are the red factor firepower distribution of weapon systems to cyber-attacks the enemy nodes; λ_i represents the state transfer factor for each part of the Blue weapon system after the network attack. The reinforcement force of the network attack can be described as a vibration type, and described as follow:

$$Rif = et\sin(\omega t), \tag{3}$$

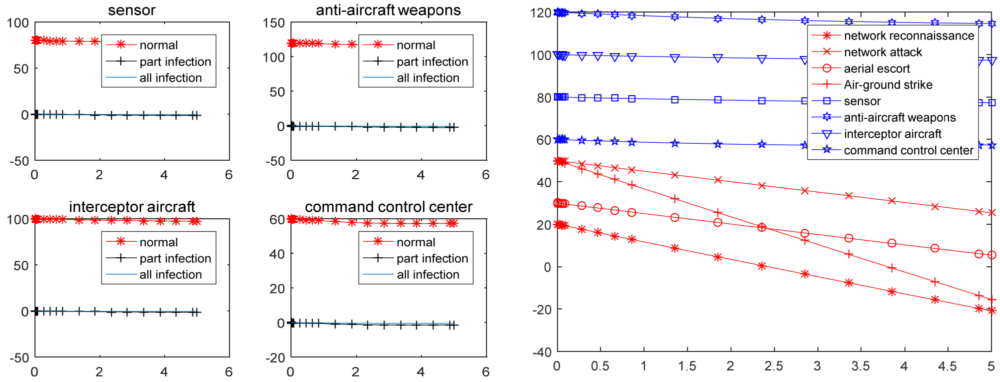
where e is the amplitude, t is the time, ω is the frequency of the vibration which is represent the uncertainty of the network.

3. Simulation analysis

Suppose the quantities of Red side participating platforms are respectively: network reconnaissance 20, network attack 30, escort 30, assault 50. The quantities of Blue side platforms are: sensor 80, air defense firepower 120, air interception 100, command platform 60. Before the start of the fighting, the number of virus infection of all kinds of platforms of the Blue side is 0.

3.1. Network reconnaissance and attack of Red side is invalid

Suppose that the Red side network reconnaissance unit fail to effectively detect the vulnerable points in the Blue command system, the Blue platforms are all in normal working condition (Fig. 3(a)). Attacked by Blue side, the units of the Red side are rapidly consumed (Fig. 3(b)).



a) b)

Fig. 3. Simulation results of Blue units working effectively

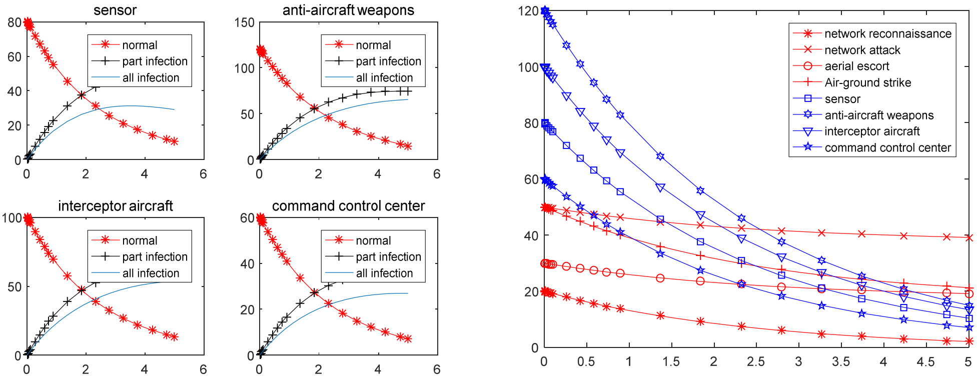
3.2. Network reconnaissance and attack of Red side is effective

Suppose that the Red side makes effective network reconnaissance and network attack, the Blue side has its nodes attacked by network, the number of normal nodes decreases, the number of partially infected and completely infected nodes increases (Fig. 4(a)), which results in decline of effectiveness of Blue sensor platform, air defense firepower, interceptor aircraft and command platform. The number of interceptors and command platforms will drop rapidly under the attack of red assault force, losing the advantage of number of battlefields (Fig. 4(b)).

3.3. Dynamic type network attack and the proposed reinforcement

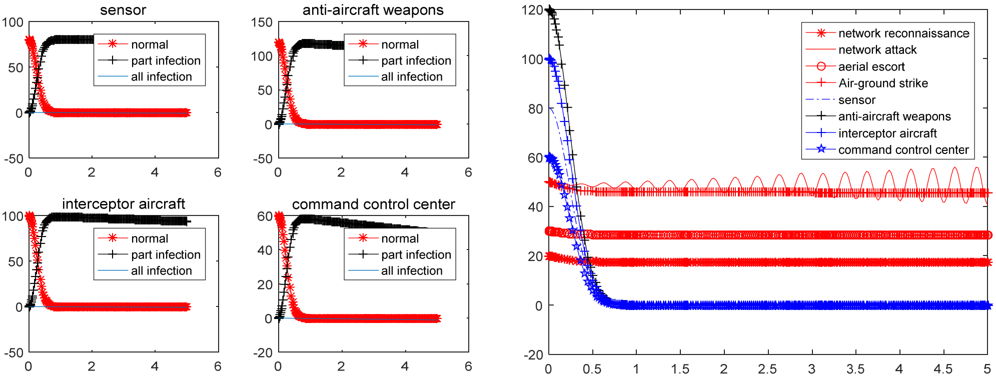
Under the attack of the reinforcement of the network, the combat result will be changed (Fig. 5).

As in Fig. 5, the number of the normal nodes of Blue side under the vibration type network attack reinforcement, decreases faster than that of the normal network attack shown in Fig. 4, and each part of the Blue decreases to about zero within 1 second. The simulation results show that the vibration type network attack has higher effectiveness than that of the stable network attack.



a) b)

Fig. 4. Simulation results of no reinforcement



a) b)

Fig. 5. Simulation results under the vibration type of reinforcement

4. Conclusions

This paper focuses on the modeling of network /firepower integrated combat. The influences of partial and complete virus infection modes of network attacking on operational effectiveness of the engagement platform are described. The Lanchester equation is used as the basis for establishing the simulation model of integrated network/firepower combat. The results of this study can be used as a reference for further studies on such decision-making as effectiveness evaluation, and force assignment of the integrated network/fire combat. The simulation results and practical examples show that the uncertain network attack power has the higher effectiveness. If the vibration frequency and the amplitude are changed at the same time, the effective of the network attack and the integrated combat effectiveness will be increased further.

Acknowledgement

The National Natural Science Foundation of China (No. 61672206), and Aviation Science Foundation (20165197001) support the research work.

References

[1] **Enn Tyugu** Command and Control of Cyber Weapons. 4th International Conference on Cyber Conflict, Tallinn, 2012.

[2] **Huang Ren Quan, et al.** UML and petri net model of the air defense system countering the cyber attack. Modern Defense Technology, Vol. 40, Issue 2, 2012, p. 17-23.

[3] **Johnson I. R., Mackay N. J.** Lanchester models and the battle of Britain. Naval Research Logistics, Vol. 58, Issue 3, 2011, p. 210-222.

[4] **Li Bo, Gao X. G.** Algorithm of power allocation for cooperative electronic jamming in air combat of formation. Systems Engineering and Electronics, Vol. 30, Issue 7, 2008, p. 1298-1300.

[5] **Wan Kia Fang** Optimal power partitioning for cooperative electronic jamming based on Lanchester with variable efficiency factors. Systems Engineering and Electronics, Vol. 33, Issue 7, 2011, p. 1544-1552.

[6] **Gao Chun Rong, Ben Ke Rong** An advanced Lanchester equation-based attrition model in communication countermeasures simulation system. Journal of Hefei University of Technology, Vol. 33, Issue 2, 2010, p. 193-196.

[7] **Niu D., et al.** Modeling and reinforcement decision analysis in air force combat based on data link. Journal of Beijing University of Aeronautics and Astronautics, Vol. 41, Issue 1, 2015, p. 102-109.

[8] **Chen Chang Xing, Al** Modeling of air combat based on effectiveness evaluation. Systems Engineering and Electronics, Vol. 37, Issue 1, 2015, p. 79-84.

[9] **Jin Xing Liu, et al.** Networks attack-defense model based on the improved Lanchester equation. Proceedings of the International Conference on Machine Learning and Cybernetics, Tianjin, 2013, p. 1083-1086.

[10] **Fatih Yildiz** Modeling the Effects of Cyber Operations on Kinetic Battles. Naval Postgraduate School Monterey, California, 2014.