System Network Modeling for “SoS Attack” Use Case

Jiang ZHU\textsuperscript{a,}\textsuperscript{*}, Wei CHEN, Ying-chun WANG and Yu-chun FEI
Nanjing Army Command College, Nanjing, China
\textsuperscript{*}pearlriver_1981@163.com
\textsuperscript{*}Corresponding author

Keywords: SoS combat, Combat Simulation, Complex Network, Network modeling.

Abstract. Network plays a dominated role in information war. To validate network-driven fighting methods, a high fidelity network model is indispensable. In this article, applying a layering idea, the designed model respectively embodied neighbor effect in communication network and social relation effect in command and control network. As a result, it can reflect the physical feature of the practical network and can be seemed as an updating of traditional BA model. After this network model was constructed, it was put in a simulation platform, by which, some experiments could be done to testify any military hypothesis. As a example, “SoS attack fighting method” case is performed and the results illustrated that the proposed network model is quite useful and benefits doing related research.

Introduction

In recent era, network technologies have predominated in military area and many aspects of war encircle acquisition of the preponderance in network. SoS(System of system) attack and defense is a typical fighting method. Yet, lacking of suitable network model and proper experiment platform restricts the performance of validating SoS concept. In order to overcome such deficiency, researchers have done some related research in following area:

(1) Military network description.

Military network have multi-layers, and composed of diversiform nodes and edges, that is quite dissimilar with other types of network. Jeffery R. Cares took the network method into account, and brought in network attributes when modeling combat system [1]. General researches simplified the military network and taken it a homogeneous network or segregated network to be convenient for study. In 2015, Complex network theory was proved to be suitable for describing SoS in the “Network Science” report.

(2) Network model

According to complex network theory, Attorney Dekker [2] constructs a C2 network model based on the nonlinear preference attachment method like Kawachi’s method. In this method, regular network (\( p = 0 \)), small word network (\( 0.02 \leq p \leq 0.1 \)), random network (\( 0.5 \leq p \leq 1 \)) and scale-free network (\( p \geq 2 \)) can be generated by regulating parameter \( p \). But these methods are proved to be effective for homogeneous complex work, such as certain traffic network, communication network, not so suited for C2 network and therefore the model is lack of practicability.

Considering the realistic thing, XiuLi Ma provides an idea of integrating the detection network and information network into a unity [3], Peng Di differentiated four types of nodes and creates edges according to the statistic. But, probability function in
this method is too static and not fittingly for evolving network [4]. Jun Li put emphasis on communication network, and adopt different creation mechanism for backbone nodes and access nodes respectively. He also taken the node position into account [5]. Weixin Jin, gave an novel idea. In the method, after constructing a layered C2 network and a local-world based communication network, some mapping and connection are erected to interconnect two networks [6]. These methods began to focus on the diversification of network and lay a good background for further research.

In this article, the work is as follows: firstly, a network model is proposed to meet the requirements of military practice, secondly, a simulation system embodied the network model and its driving mechanism is discussed, at last, “SoS attack” fighting method as a use case is illustrated. All by all, how to model network and how to use that model is the concern of this paper.

**Network Model**

In realistic communication network, the position and veracity of nodes should be considered, actually, attack node is always linked to an adjacent communication node, while the reconnaissance node is always connected to several communication nodes. Moreover, the communication nodes could be classed into two types: kennel and ordinary. The former nodes interconnected with each other by fiber network, and the later nodes joined a tactic mobile network, whose domain is restrained by situation and the signal power of sender.

In this approach, taken command units as nodes, the relations as edge, network construction process, firstly Set the span of Hi level and span value is Si, create subgroups according to commander span (value is Si). In each subgroup, a commander is designated and set up a link to the commander in higher hierarchy, moreover, add some random links representing ad-hoc support and coordination relationship. Like BA, random adding links until each node have at least two links, so as to enhance the bypass of the communication.

It has many steps as follows:

S1: Set an initial network topology according to preset level and span of C2. This network is completely composed of command nodes and acquired the hierarchy modality.

S2: Replicate the communication nodes with the same number of above command nodes, and set a backbone topology made of those communication nodes.

S3: Produce a node to be added in topology by differentiated ratio of different node type, and glean the nodes in his neighborhood.

S4: Compute the link probability from the adding new node to his neighborhood. If the new node is a communication node, the link probability is computed by formula 1:

\[ p_j = \frac{u_i}{\sum_{i \in V} u_i} \sim \varepsilon_i d_i \]  

(1)

In Eq.1, V is the node set in existed topology, \( u_i \) is attractive coefficient of node i, \( \varepsilon_i \) is influential coefficient of node i; \( d_i \) is degree value of node i( if j is a communication
node and seated in the neighbor set of \( i \), then \( \varepsilon^i = 2 \) ; if \( j \) is a communication node out of the neighbor set, \( \varepsilon^i = 1 \); if \( j \) is not a communication node, \( \varepsilon^i = 0 \).

If the node is a reconnaissance node, then the link probability is computed by Eq.2.

\[
p_j = \begin{cases} 
  \frac{d_i \ln d_j}{\sum_{i \in S} d_i \ln d_j} & j \in V_s \\
  0 & j \notin V_s 
\end{cases}, \quad V_s = \{ j | j \in M_2 \land j \notin M_1 \}. 
\]

In formula 2, \( d_i \) is the degree of node \( i \), \( M_1 \) is the neighbor set of new coming communication nodes, \( M_2 \) is the iterative nearer neighbor set whose node is in the neighbor set of nodes in \( M_1 \). \( \delta \) equals 0.048.

If the node is an attack node, then the link probability is computed by Eq.3.

\[
p_j = \begin{cases} 
  \frac{d_i \ln d_j}{\sum_{i \in S} d_i \ln d_j} & j \in V_c \\
  0 & j \notin V_c 
\end{cases}. 
\]

In formula 3, \( d_i \) is the degree of node \( i \), \( V_c = \{ j | j \in M_1 \} \) is the node set of \( M_1 \), \( M_1 \) is the neighbor set of new coming communication node.

S5: Add the new node into the topology. For every \( j \) in topology, compute a random number, if its value is less than the link probability computed from step S4, then connect node \( i \) with node \( j \).

S6: Perform the step S3, S4 and S5 repeatedly, until the count of the topology reached a threshold presented.

In more detail, Presuming the level and span of each level \( i \) is defined as \( A, B_i(1 < i < A) \), S1 has following steps:

S1-1: for the highest level (\( i = 1 \)), add command nodes (count number is \( B_1 \)), and create a fully connected network;

S1-2: set \( i = i+1 \), each node in level \( i \), taken as a father node, add its son nodes (count number is \( B_{i+1} \)) and the link the father node with son nodes;

S1-3: repeat S-2, until all nodes in level \( i \) have been traversed over;

S1-4: repeat S-1 and S-2, until \( i \) reaches \( A \);

S2 has the following steps:

S2-1: Replicate the communication nodes with the same number of command nodes, and map each other by adding a link;

S2-2: if there has a link between command nodes, there should add a link between corresponding communication kennel nodes.

S2-3: add a link as redundancy from above communication kennel nodes to other ordinary nodes.

S2-4: calculate the position of communication kennel node by node distribution function. if there has a node already existed, redo the calculate process.

S2-5: Allocate the node at the position calculated.

S3 has the following steps:

Produce a node to be added in topology by differentiated ratio of different node type, and glean the nodes in his neighborhood.
S3-1: classify the nodes into communication node, reconnaissance node and attack node with respective proportion \( r_c, r_r, r_s \) \((r_c + r_r + r_s = 1)\);

S3-2: calculate the position of communication kennel node by node distribution function. If there has a node already existed, redo the calculate process.

S3-3, sort out those nodes which satisfied \( d(v_i, v_j) < \text{Threshold} \) into a neighbor set, \( d(v_i, v_j) \) is the Euclidean distance between node i and node j.

**Simulation Platform**

In Fig.1, simulation platform, incorporated the network model with MAS(multi-agent system) modeling method, is able to regulates and reflects the interaction and dynamics of network with combination of emerge behavior from entity relationship to network, and driving efficiency from overall network characteristic to entity, it is very fit for command and control testing experiment.

Researchers of Complex network, used to investigate the networks characteristic by the way of computing topology statistically, and put forward a bunch of representative index, such as average distance, convergence coefficient, and the degree distribution. Those index of network, can represent the idea of span, hierarchy, process, cooperative, adaption of C2. The possible mapping between them are concluded in table 1.

| Index            | Physical meaning                                                                 | Military meaning   |
|------------------|----------------------------------------------------------------------------------|--------------------|
| Degree(k)        | The number of links link to a certain node k                                     | C2 Span            |
| Shortest Path    | Refer to the shortest path between given two nodes                              | C2 Process agility |
| Degree Distribution | Refer to the structure of network. If satisfied with the Poisson Distribution, nodes are in same position; otherwise, some node are privileged. | C2 centricity      |
| Cluster convergence coefficient | Group feature of network, reflecting a phenomena for individual to join a group. Cluster contains most of link, Big value means good connectivity. | C2 synchronization |
| Eigen value \( \lambda_{PFE} \) | Eigen value computed from an adjacent matrix which states topology. If eigen value=0, there is no connection in network, if eigen value=1 the topology is loop, if >1, the network contains feed back. | C2 cooperation     |
| Neutral Sub-structure pattern | Refer to a potential sub-structure, in where nodes. The sub-structure pattern emerged numerous times in a graph. In fact, the same structure always have a same function and the same status in the network. | C2 adaptability    |
“SoS Attack” Case

“SoS attack” is a typical use case. As to military domain, traditional fighting method aims at annihilating enemy piecemeal is obviously behind times. Now, various ties in real or virtual network have integrated all atomic units into a unified one, even a trivial event or a small unit may play a decisive role in full-scale. So, a “network-relation concerned” paradigm play a more import role and a new fighting method called “SoS combat” is put forward, which can led to disorder and disintegrated of enemy by attacking important junctions of enemy’s system and giving structural damage.

As network model could produce a created network profile, it can be detailed analyzed based on network science. Object selection is the key problem in SoS attacking. Network graph can be analyzed with diversified tools that Complex Network tool box provided.

In this case, this simulation platform can provide a virtual network of enemies, for our troop doing object selection. Prepare for modeling, we classified the node into six categories, each categories represents different object type, according to object feature. Secondly, we should set the parameters in networking in model. As a example, the parameter is set as follows: the covering area is 10*10 sq.mi. The total number of simulation nodes is 1000; the distance threshold is 500 feet; the command span of initial network is 3; the network layer is 3; nodes ratio is $r_c = 0.5$, $r_r = 0.4$, $r_s = 0.1$.

As a result, the enemy’s object network graph was demonstrated in Fig.2.

![Figure 2. The graph of enemy object network in situation in platform.](image)

The left sub-graph is the topology created after S1 and S2 step, which can be seemed as a physical domain network. The aggregation effect and social group characteristic can be discerned from the graph. It illustrates a community circling around certain core communication nodes, and divided by nodes’ geographic position. The right sub-graph is the whole network by our model, and the hierarchy between physical domain network and task domain network is obvious.

After inputting the scenario data and bilateral forces into the simulation system, the dynamic simulated battlefield situation come into being and the status data can be observed. Fig.3 is the visualization of simulation platform. And the right panel is the output data.
Conclusions

1. Network modeling method designed has effectiveness and advantage, and its aggregation coefficient, average path length, and the distribution of degree more approachable to reality network.
2. This model is always embedded into an experiment system and can benefit combat experiment then.
3. In use case, after carefully chosen network index, and applied into object selection algorithm, “SoS” attacking proved to be more effective than traditional ones.

Acknowledgement

This research was financially supported by the National Science Foundation (No.71401177) and Post-Doctoral Foundation (No.2016m603049).

References

[1] Jeffrey R. Cares. An Information Age Combat Model. 9th International Command and Control Research and Technology Symposium, 2004:166-193.
[2] Dekker A. H. Network Topology and Military Performance. International Congress on Modelling and Simulation, Modeling and Simulation Society of Australia and New Zealand, 2005: 2174-2180.
[3] Xiu-li Ma, Ke-xin Sun, Hong-xia Wang, Fire Control & Command Control, 2010,35(2):69-71 (In Chinese)
[4] Di Peng, Li Fang, Hu Bin, journal of naval university of engineering, 2010, 22(6):107-112 (In Chinese)
[5] Li Jun, Lu Xin, Tan Yue-jin, System Engineering and Electronics, 2010, 7:1456-1460 (In Chinese)
[6]Wang Zai-kui, Ma Ya-ping, Sang jin-rui, Command control & simulation, 2011, 33(2):8-11 (In Chinese)