Journal of Network Intelligence
Taiwan Ubiquitous Information
 ISSN 2414-8105 (Online)
Volume **8**, Number **3**, August **2023**

Battlefield Network Topology Inference and Feature Analysis Based on OPNET

Lu Xu, Wan-Xin Yao, Yi-Jia Zhang

School of Information Science and Engineering
Zhejiang Sci-Tech University
No. 928, 2 Street, Hangzhou 310018, China
xlhit@126.com, wanxin_67@sina.com, waiting@zstu.edu.cn

Zhe-Ming Lu*

School of Aeronautics and Astronautics
Zhejiang University
No. 38, Zheda Road, Hangzhou 310027, P. R. China
zheminglu@zju.edu.cn

Hao-Lai Li

EFORT Intelligent Equipment Co., Ltd.
Shanghai 201600, P. R. China
lihaolai@efort.com.cn

*Corresponding author: Zhe-Ming Lu

Received November 30, 2022, revised January 15, 2023, accepted March 14, 2023.

Abstract. *With the rapid development of wireless networks, more and more wireless communication technologies are applied to the battlefield. Among various wireless communication protocols, Ad Hoc protocol is a widely used and stable communication protocol. Even if one of the communication nodes is destroyed, it will not affect the mutual communication of other communication nodes, so this paper chooses the Ad Hoc system as the communication protocol of the wireless network. OPNET is a powerful network simulation software that can accurately analyze the performance and behavior of complex networks. Use OPNET simulation software to build communication scenarios, generate communication animations and network service data. Based on the business data generated by OPNET, this paper uses the theoretical knowledge of complex networks to perform topology inference and feature analysis on the generated data through the VS2017 simulation platform. In order to make the network topology expression more intuitive, Pajek software was used to read net files to generate a visual topology map. The static characteristics of the network are analyzed by using the relevant knowledge of the complex network, including the degree, the clustering coefficient, the shortest path of the network, the betweenness and other characteristics.*
Keywords: OPNET, Ad Hoc Protocol, Topology Inference, Static Characteristics of Complex Networks, VS2017

1. **Introduction.** The rapid development of information technology promotes a new military revolution. The battlefield is not only an attack between physical weapons, but also a new battlefield dominated by information. At present, electronic warfare has become a crucial combat method on the battlefield. Mastering more information and being able to analyze it effectively is the key to winning electronic warfare [1]. The battlefield network is the foundation of the information battlefield. With the development of network

technology, a variety of wireless network technologies have appeared, such as WLAN, CDMA, GSM, Ad Hoc and so on. Ad Hoc network, as a multi-hop wireless communication network that can automatically establish communication links, has no center and highly invulnerable, has always been the preferred technology for digital battlefield.

OPNET is a very mature network simulation software. It has perfect simulation and analysis capabilities and has been widely used in wireless communication networks. OPNET can accurately analyze the performance and behavior of complex networks. Many scholars use OPNET to conduct research and analysis on the performance of battlefield networks, especially Ad Hoc networks. Nie mainly used OPNET to simulate the typical protocol AODV in the tactical radio network. By simulating the interference devices added to the network, analyzing indicators such as throughput and packet loss rate, obtained the performance of the entire network and a single node after interference [2]. Zhang proposed a reliability assessment method for Tactical Internet (TI) based on OPNET, which has certain effectiveness and feasibility [3]. Nisar used OPNET to test the network performance under the three most common protocols AODV, DSR and OLSR of Mobile Ad Hoc Network (MANET). By comparing the indicators after the simulation, finally find the most suitable routing protocol OLSR [4]. Bi used the OPNET platform to simulate four communication protocols, and proposes a new Cluster Routing Protocol (CRP) based on the AODV protocol, which can significantly reduce the network end-to-end delay [5]. Lim used OPNET to design several tactical sensors and evaluate the reliability of the network [6].

In conclusion, their research only analyzes the network performance parameters provided by OPNET software, and does not use OPNET and other software to co-simulate. In this paper, the OPNET simulation model is combined with the complex network theories. Use OPNET to build wireless communication scenarios and generate network service data and simulation animation. Visual Studio 2017 is used to implement network topology inference based on network business data, and on this basis, various characteristics of the resulting network are analyzed. Finally, use MFC to design a battlefield network analysis software based on the above data. The overall technical route is shown in Figure 1.

2. **Building of OPNET Simulation Model.**

OPNET adopts a three-layer modeling architecture, which are process layer, node layer and network layer [7]. These three-layer structures correspond to the layer-by-layer modeling process of networks, devices, and protocols in reality. The network layer is mainly for planning and deploying the network structure. Different network topologies can be built by placing different network models. The specific function of each node is realized by building a protocol stack at the node layer. The protocol stack adopts the OSI seven-layer standard protocol structure, which is built from the physical layer to the protocol layer. Entering the next layer of each module is the process layer. By editing the process state transition diagram and modifying the process code, algorithms and protocols can be written. This paper mainly uses the network editor to build the wireless communication model, and the whole network adopts the AODV protocol for simulation.

2.1. **AODV Routing Protocol.**

A wireless Ad Hoc network refers to a multi-hop, temporary, non-central network without infrastructure support, which is composed of a group of wireless mobile nodes. All nodes in the Ad Hoc network have equal status and highly survivable. Any node failure will not affect the operation of the entire network. The network adopts Ad Hoc On-Demand Distance Vector Routing (AODV) Protocol, which is a very typical network protocol in Ad Hoc network.

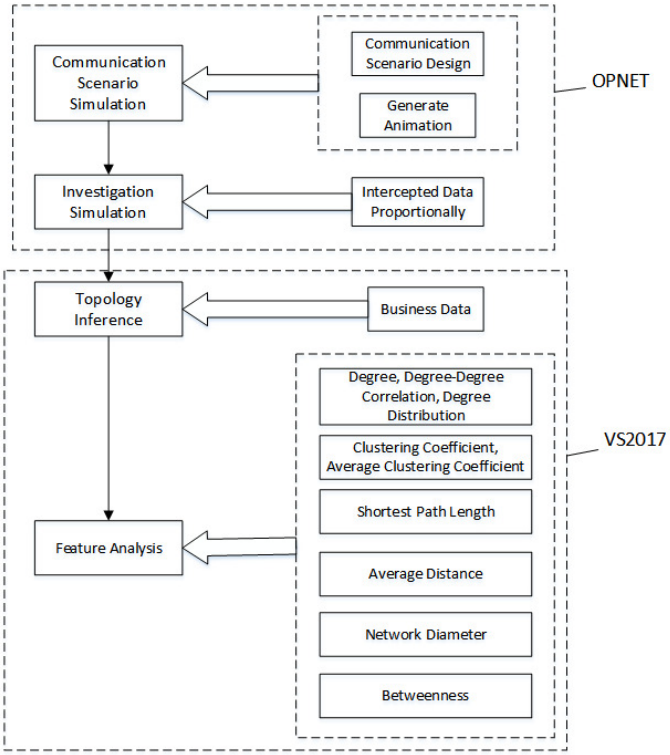


FIGURE 1. Overall technical route

AODV is a routing protocol that finds the path on demand. It does not record the paths of all nodes, but only records the path to be found by the target node [8]. Each node will have a sequence number, and the sequence number is incremented in order to avoid the search path being a circuit. AODV can implement unicast and multicast routing, and can store the routing table of unicast routing and multicast routing to the target node [9]. The record content of the routing table includes the destination node number, the next node number, the serial number, and the validity period. The validity period is used to record the real-time nature of the path. The value of the path increases by one each time it passes through. If the path is not passed for a long time, the path will be destroyed. When a node wants to send a packet to a certain target node, it first needs to check whether its own routing table has established a path to the target node [10]. If the path has been established, the data packet is sent directly, otherwise the path needs to be found. The source node sends a Route Request (RREQ) packet when finding a path for the first time. This packet contains the IP address of the source node, the current sequence number of the source node, the IP address of the destination node, the current sequence number of the destination node, and the broadcast ID number. The broadcast ID number and the IP address of the source node mark the packet as an RREQ and also make the packet unique.

2.2. **Communication Scenario Design.**

2.2.1. *Network Model Construction.* In this paper, a wireless network communication scenario with 30 nodes is designed. The scenario is deployed within a range of $200km \times 100km$, including one workstation, one router node, four sensor nodes, nineteen common forwarding nodes, and five attack platform nodes. Figure 2 shows the scenario deployment solution based on OPNET.

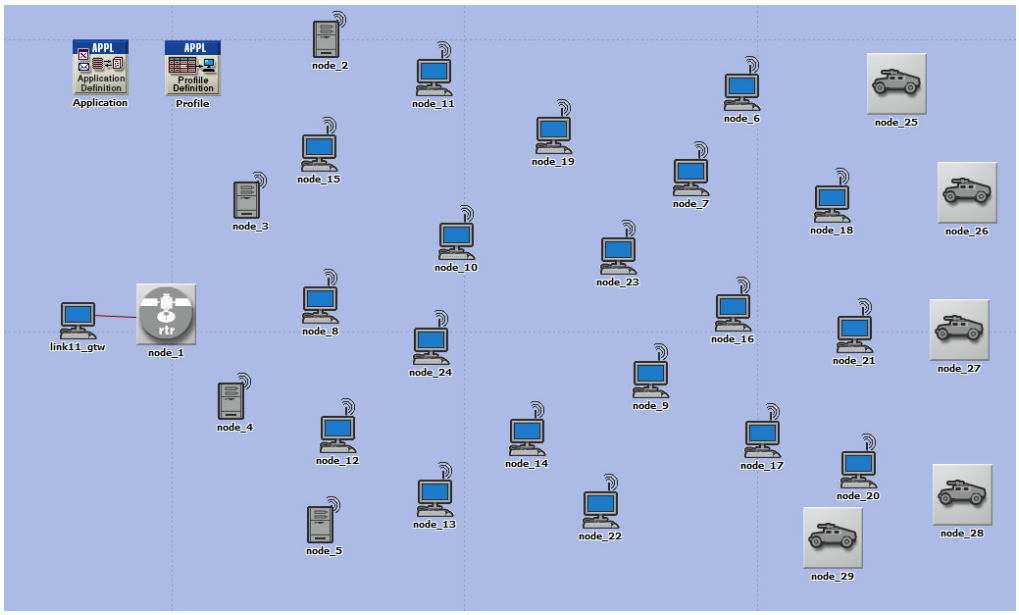


FIGURE 2. Schematic diagram of OPNET scenario deployment scheme

In the figure, link11_gtw and the connected node_1 are the simulation of the Network Control Station (NCS), which can be understood as one node in the simulation. 10BaseT is used for connection between link11_gtw and node_1, and the AODV protocol is mainly used for data broadcasting between the backend networks. The four nodes node_2, node_3, node_4 and node_5 to the right of the node_1 node are modeling sensor nodes. They are responsible for collecting other intelligence information on the battlefield, and transmit their own information according to the request of other nodes. Nodes from node_6 to node_24 on the right side of the sensor nodes are modeling of a series of forwarding nodes in the battlefield. Such nodes do not generate information by themselves, but only forward information from other nodes. The five nodes node_25 to node_29 on the right are modeling the attack platform.

2.2.2. *Network Business Configuration.* Configuring a simulation system to run an application model is a multi-step process. The detailed flow chart is shown in Figure 3.

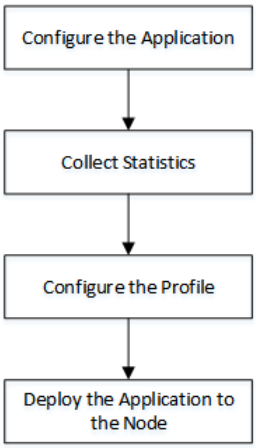


FIGURE 3. OPNET business configuration flow chart

In the process of configuring traffic, pay attention to distinguish the difference between application model and user profile. Application model specify the nature of the traffic generated by an application, and user profile describe how the application will be used. The application model defines information such as message interval and size, while the user profile specifies which applications to use, the start time and execution time of the application, whether the execution mode within the profile is serial or parallel, also include the start time and end time for the entire profile [11]. In OPNET, after the application model and user profile are properly configured, it is necessary to specify the node on which the profile will be executed and the node that will serve the application of the profile. A node is called a source node or client if it is used to run a user profile, and a destination node or server if it serves an application. OPNET offers eight standard applications including database, E-mail, FTP, HTTP, print, remote login, video conferencing and voice.

The application configured in this article is Database, and the application executes two database operation protocols, namely the query and the entry. The database query operation consists of a query message carrying a database request and a response message carrying the data, and completes the task of retrieving data from the database. A database input operation consists of an input message that carries data and a database response message that carries the operation. The application contains three presets low load, medium load and high load. The value set in this paper is low load. The specific settings of the application configuration model are shown in Figure 4.

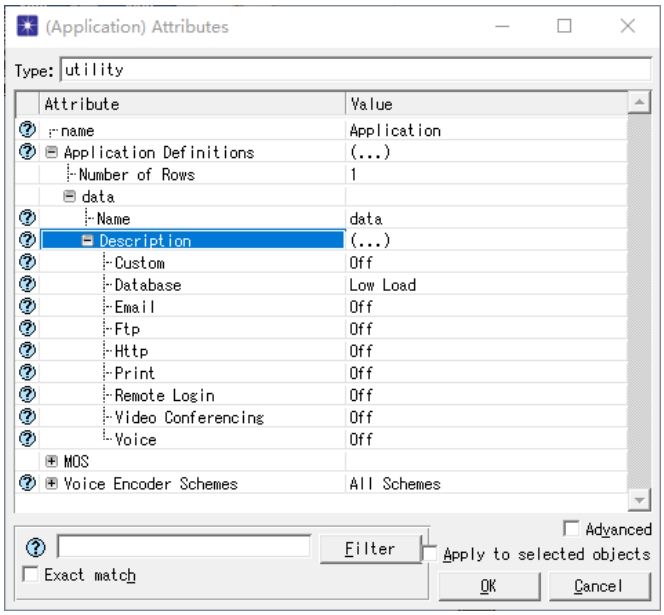


FIGURE 4. Configure the Application Definitions attributes

Since this paper does not involve OPNET statistical analysis, it does not involve the statistical collection step. Next deploy the profile definition. The information specified by the user profile definition includes the start time and duration of the application, the number of applications executed by a single user, and the order in which these applications are executed. This paper defines a user profile named BATMessage. The profile start time is uniformly distributed, the minimum value is 100s and the maximum value is 110s. The user profile does not end until the end of the simulation, and the number of repetitions is once. The application is launched serially, placing the application set above into the profile. The application start time refers to the time from the start of the configuration

file to the start of the first application. It is set to a normal distribution, the minimum value is 5s and the maximum value is 10s. The end time is the end time of the user profile and the number of repetitions is not limited. Figure 5 shows the specific settings for the application configuration model.

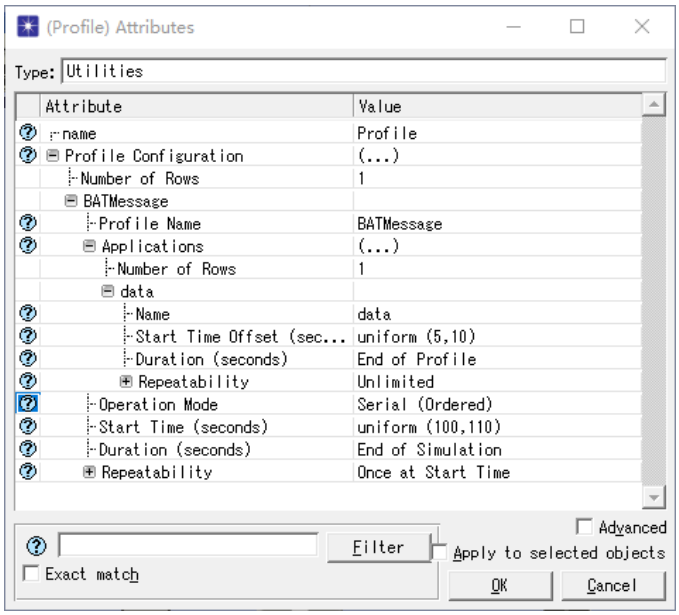


FIGURE 5. Configure the Profile Definitions attributes

With the application and user profiles defined, the next step is to deploy the defined application inside the simulation system. In general, the supported applications and profiles need to be deployed separately for each node, which is time-consuming and error-prone during the configuration process. Therefore, this paper adopts the Application Deployment Wizard to collectively deploy the specified application for each node. Figure 6 shows the Deploy Application window. The Network Tree Browser shows the objects available in the simulation system, and the Deploy Application option is used to deploy the application. Among them, node_2-node_5 is configured as a server node, supporting data application services, node_9-node_24 is configured as a client, supporting BATMessage user profiles. The specific configuration steps are displayed with help at the bottom of the window.

3. **Battlefield Network Reconnaissance Simulation.**

3.1. **Topology Inference Based on Network Business Data.** Network topology inference is the process of analyzing the connection relationship of the target network and drawing a topology map according to the detection results of wireless signals. The wireless network topology inference steps include signal detection, set the signal detection ratio, communication link identification, calculation link weight and draw topology. Figure 7 shows the basic flow of topology inference.

This paper does not study the specific physical reconnaissance method, but only studies how to simulate the effect of the reconnaissance method in the simulation platform [12]. The method deduces the topology of the network through the business data in the network, and counts the communication frequency between two nodes, finally obtaining a weighted topology. The original communication data comes from OPNET, and the data is exported and put into VS2017 for analysis. Since the battlefield environment

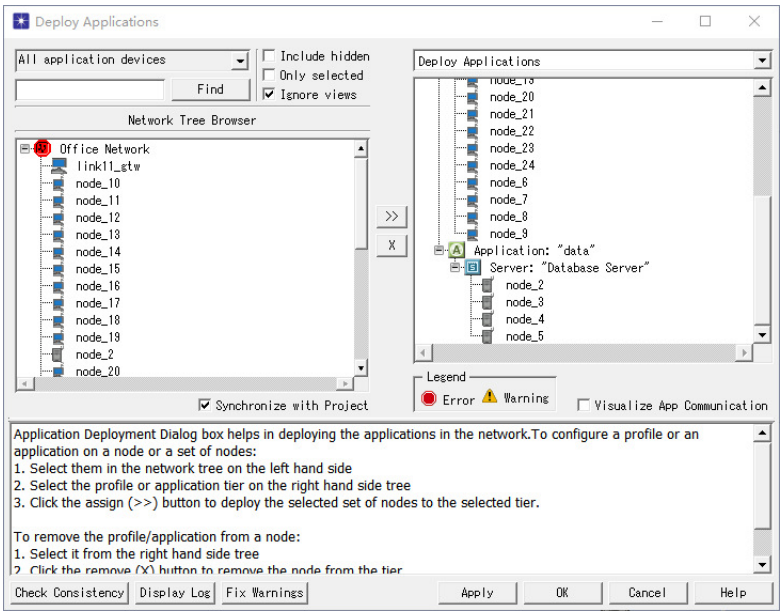


FIGURE 6. Deploy Application window

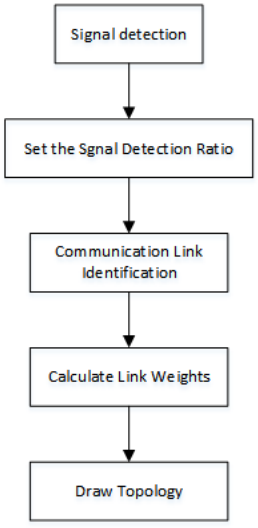


FIGURE 7. Basic flow of topology inference

is non-cooperative, the communication data is firstly intercepted in proportion, and the interception proportion is 70%, 80%, and 90%. According to the intercepted communication data, the communication status of each node can be obtained, and the data can be put into VS2017 for further analysis, and the results can be saved in the Pajek net file format. Finally, put the obtained .net file into Pajek software to read and generate a visual topology map.

Pajek's net file format defines all points and edges in a network. Points are defined under the label *Vertices n, and edges are defined under the label *Edges [13]. *Vertices n defines the node, n is the specific number of nodes, and the parameters are separated by spaces. The description format of node is shown in Figure 8. It should be noted that if parameter 2 is a label composed of multiple words, it must be enclosed in double quotation marks, and parameter 3 is a non-essential node whose coordinate value is the ratio of the

relative drawing area, ranging from 0 to 1 [14]. The edge of the node is defined under the *Edges tag, the format is shown in Figure 9. These three parameters are required. If no other parameters are specified, the default edge will be a solid line. If the value is negative, the solid line will become a dotted line.

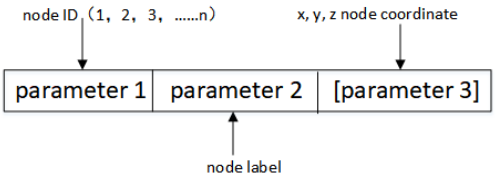


FIGURE 8. Vertices label description

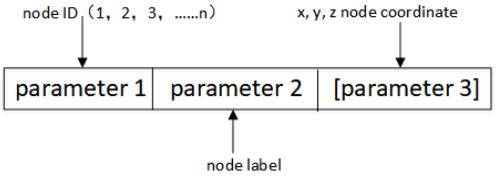


FIGURE 9. Edges label description

3.2. **Main Static Features of Communication Networks.** After the topology structure is obtained through topology inference, the feature analysis of the obtained topology can be performed. In order to characterize the comprehensive properties of complex networks, scientists have proposed many basic concepts, feature quantities and measurement methods of complex networks to represent the topological properties of complex networks [15]. Read the net file obtained above and convert it into a right undirected adjacency matrix for subsequent calculations, defined as:

$$A[i,j] = \begin{cases} W_{i,j}, if(v_i, v_j) or < v_i, v_j > \in E(G) \\ \infty, if(v_i, v_j) or < v_i, v_j > \notin E(G) \end{cases} \tag{1}$$

(1) Degree, degree distribution, degree-degree correlation. Degree is the basic parameter of network topology, mainly used to describe the influence of nodes in the network, and its value is the number of nodes connected to this node [16]. Assuming that the network has N nodes, the degree of the node is defined as:

$$C_d(v_i) = k_i \tag{2}$$

k_i denotes the number of nodes directly connected to the node. For an adjacency matrix A, the sum of each row or column element is the degree. By averaging the degrees of all nodes in the network, the average degree of the network can be obtained as follows:

$$< k >= \frac{1}{N} \sum_{i=1}^{N} k_i \tag{3}$$

The degree distribution is defined as the probability of randomly selecting a node in the network with degree value k:

$$P(k) = N(k)/N \tag{4}$$

Among them, $N(k)$ is the number of degree k, and N is the number of nodes.

Degree-degree correlation describes the relationship between nodes with large degrees and nodes with small degrees in the network [17]. The network is positively correlated if nodes with large degrees tend to be connected to nodes with large degrees, otherwise it is negatively correlated. This paper uses the Person correlation coefficient r to describe the degree-degree correlation of the network, which is defined as follows:

$$r = \frac{M^{-1}\sum\limits_{e_{i,j}} k_i k_j - [M^{-1}\sum\limits_{e_{i,j}} \frac{1}{2}(k_i + k_j)]^2}{M^{-1}\sum\limits_{e_{i,j}} \frac{1}{2}(k_i^2 + k_j^2) - [M^{-1}\sum\limits_{e_{i,j}} \frac{1}{2}(k_i + k_j)]^2} \tag{5}$$

The absolute value of r ranges from 0 to 1. When $r > 0$, the network is positively correlated, otherwise it is negatively correlated.

(2) Aggregation coefficient, average aggregation coefficient. For an undirected network, the local clustering coefficient of a node is the ratio of the actual number of edges between the neighbors of the node to the total possible number of edges [18]:

$$C_i = \frac{2M_i}{k_i(k_i - 1)} \tag{6}$$

(3) Shortest path length, average distance, network diameter. In this paper, the Floyd algorithm is used to solve the shortest path length of any two points [19]. The main idea of this algorithm is to compare all paths with the same start and end nodes but pass through other nodes with the current shortest path, If the new path has a smaller weight, update the weight of the path. The recursive formula is:

$$d_{i,j}^{\ k} = \begin{cases} W_{i,j}, k = 0 \\ min(d_{i,j}^{\ k-1}, d_{i,k}^{\ k-1} + d_{k,j}^{\ k-1}), k \geq 1 \end{cases} \tag{7}$$

$d_{i,j}$ is the distance between two nodes v_i and v_j.

The diameter D of the network is defined as the maximum of all distances $d_{i,j}$:

$$D = \max_{l \leq i,j \leq N} d_{i,j} \tag{8}$$

The average distance L is defined as the average of the distances between all node pairs. It describes the average degree of separation between nodes in the network. The formula is as follows:

$$L = \frac{1}{N^2}\sum_{j=1}^{N}\sum_{i=1}^{N} d_{i \cdot j} \tag{9}$$

(4) Betweenness. Betweenness is divided into point betweenness and edge betweenness. It is a global feature quantity, which reflects the role and influence of a node or edge on the entire network [20]. The betweenness of a node is defined as:

$$B_k = \sum_{\substack{all\, i,j \\ i \neq k \neq j}} [N_{i,j}(k)/N_{i,j}] \tag{10}$$

$N_{i,j}$ is the number of shortest paths between nodes v_i and v_j, $N_{i,j}(k)$ represents the number of shortest paths between nodes v_i and v_j passing through node v_k. The betweenness of an edge is defined as:

$$B_k = \sum_{\substack{all\, m,n;m \neq n \\ m,n \neq i,j}} [N_{m,n}(e_{i,j})/N_{m,n}] \tag{11}$$

$N_{m,n}$ is the number of shortest paths between nodes v_m and v_n, $N_{m,n}(e_{i,j})$ represents the number of shortest paths between nodes v_m and v_n through edge $e_{i,j}$.

When calculating the length of the shortest path, whenever the new path length is the same as the shortest path, add one to the number of shortest paths, so the length of the shortest path and the number of shortest paths can be calculated at the same time. The idea of calculating the number of shortest paths through v_i is that when the distance between nodes v_i and v_j is equal to the distance between nodes v_i and v_k and the distance between nodes v_k and v_j, the shortest path between v_i and v_j goes through v_k. Because when the shortest path of nodes v_i and v_j passes through v_k, both v_i to v_k and v_k to v_j must be the shortest path. Similarly, the edge betweenness is also calculated based on the above algorithm.

4. **Experiment Simulation.**

4.1. **OPNET Results Generation.**

After building the model, use OPNET software to export communication data and generate communication animations. The network simulation time is 5 minutes, and the data information in the network is intercepted as the original data to be analyzed, as shown in Figure 10. The data mainly shows the communication status of each node. Save the exported data in txt and read it into VS2010 for further analysis. To generate a communication animation, the ODB debugger needs to be opened. By default, the simulation core is Optimized. In order to speed up the simulation, optimized does not generate ODB debug information, so it is necessary to set the simulation core type to Development. After the simulation, open the Model tab to watch the communication animation. Figure 11 shows the screenshot of the animation video of data transfer.

Flow type: ip_traffic_flow_with_socket

#Source Name	Source IP Address	Source Port	Destination Name	Destination IP	Address	Destination Port	Protocol	Type of Service	Flow Name	Avg Pkt Size (Bytes)
top.Office Network.node_1	default	default	top.Office Network.node_10	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_11	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_12	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_13	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_14	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_15	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_16	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_17	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_18	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_19	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_2	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_20	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_21	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_22	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_23	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_24	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_25	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_26	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_27	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_28	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_29	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_3	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_4	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_5	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_6	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_7	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_8	default	default	default	default	default	0	End Data
top.Office Network.node_1	default	default	top.Office Network.node_9	default	default	default	default	default	0	End Data
top.Office Network.node_10	default	default	top.Office Network.node_1	default	default	default	default	default	0	End Data
top.Office Network.node_10	default	default	top.Office Network.node_11	default	default	default	default	default	0	End Data
top.Office Network.node_10	default	default	top.Office Network.node_12	default	default	default	default	default	0	End Data
top.Office Network.node_10	default	default	top.Office Network.node_13	default	default	default	default	default	0	End Data
top.Office Network.node_10	default	default	top.Office Network.node_14	default	default	default	default	default	0	End Data
top.Office Network.node_10	default	default	top.Office Network.node_15	default	default	default	default	default	0	End Data
top.Office Network.node_10	default	default	top.Office Network.node_16	default	default	default	default	default	0	End Data

FIGURE 10. Original communication data content read by OPNET

4.2. **Network Analysis Based on VS2010.**

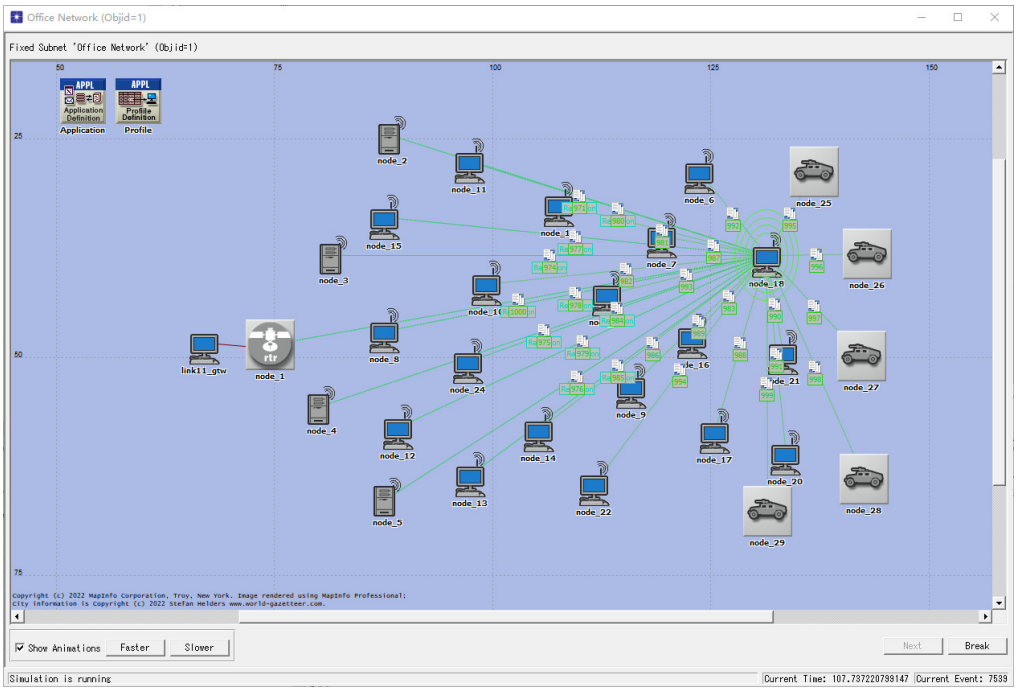


FIGURE 11. OPNET communication animation

4.2.1. *Topology Inference.* This paper randomly intercepts and generates reconnaissance data from the original communication data in proportion, and generates three types of reconnaissance data files with proportions of 70%, 80%, and 90%. VS2017 reads the reconnaissance data file generated by OPNET and saves the result as a net file. Figure 12 shows the net file at 80% interception probability. Vertices 29 indicates that there are 29 nodes in the network. The first column is the ID number of the node, which is arranged in order from 1. The second column is the name of the node, and the third and fourth columns are the relative positions of the node in the x and y coordinates. The Edges label indicates the connection status of the nodes. The first two columns indicate that the nodes in the first column communicate with the nodes in the second column, and the third column indicates the weight of the link, and the weight is increased by one for each communication.

Use Pajek software to read the obtained net file, and get the visualized topology inference results when the interception probability is 80%, as shown in Figure 13. This figure can reflect all the information in the net file. Including node name, node location, link connection and weight.

4.2.2. *Feature Analysis.* This paper mainly focuses on the static characteristics of complex networks, and uses complex network theory and graph theory to integrate parameters or characteristics such as degree, average degree, degree-degree correlation, degree distribution, aggregation coefficient, average aggregation coefficient, average distance, network diameter and betweenness. The information is analyzed in the simulation platform together.

The interception ratio is 70%, 80% and 90%. The degree and average degree of each node are shown in Figure 14. The degree distribution is shown in Figure 15, The aggregation coefficient and average aggregation coefficient are shown in Figure 16, The degree-degree correlation, average distance, and network diameter are shown in Table 1. The point betweenness of the network is shown in Figure 17.

*Vertices 29	*Edges
1 node1 0.3725 0.4860	1 2 2
2 node2 0.4423 0.2466	1 3 1
3 node3 0.4088 0.3844	1 4 2
4 node4 0.4020 0.5560	1 6 2
5 node5 0.4400 0.6615	1 7 1
6 node6 0.6185 0.2885	1 8 2
7 node7 0.5968 0.3616	1 10 2
8 node8 0.4382 0.4706	1 11 2
9 node9 0.5795 0.5344	1 12 2
10 node10 0.4965 0.4160	1 13 2
11 node11 0.4868 0.2763	1 14 2
12 node12 0.4460 0.5810	1 15 2
13 node13 0.4872 0.6356	1 16 2
14 node14 0.5265 0.5839	1 17 1
15 node15 0.4380 0.3410	1 18 2
16 node16 0.6145 0.4773	1 19 2
17 node17 0.6273 0.5854	1 21 2
18 node18 0.6570 0.3844	1 22 2
19 node19 0.5378 0.3258	1 23 1
20 node20 0.6680 0.6110	1 24 2
	1 25 2
	1 27 2

FIGURE 12. 80% interception probability of net files

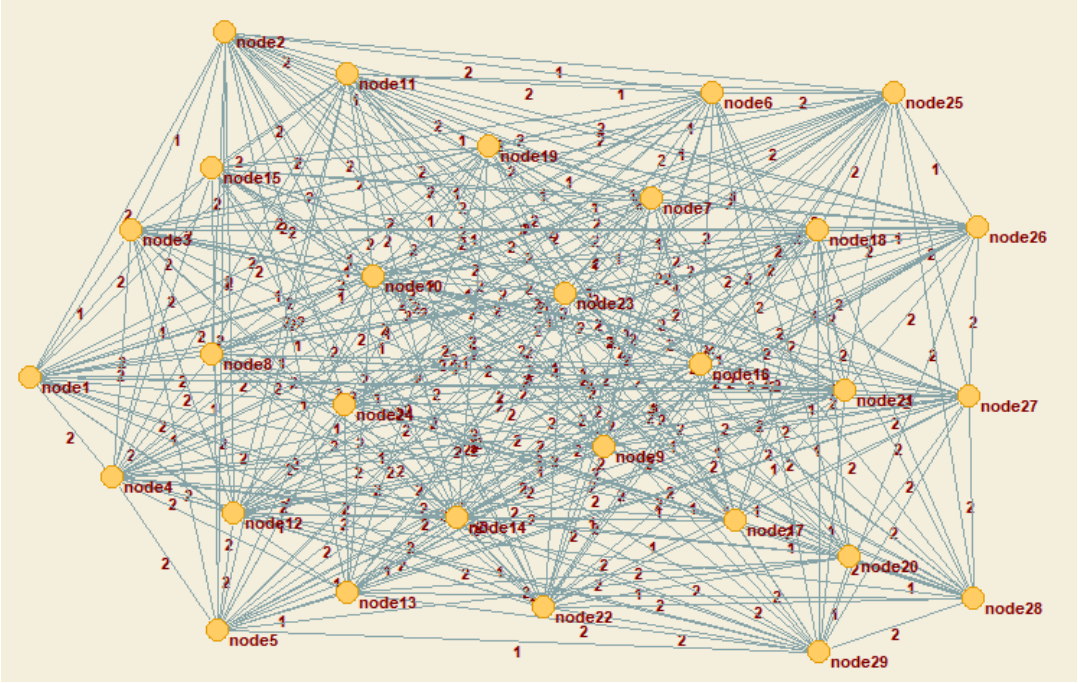


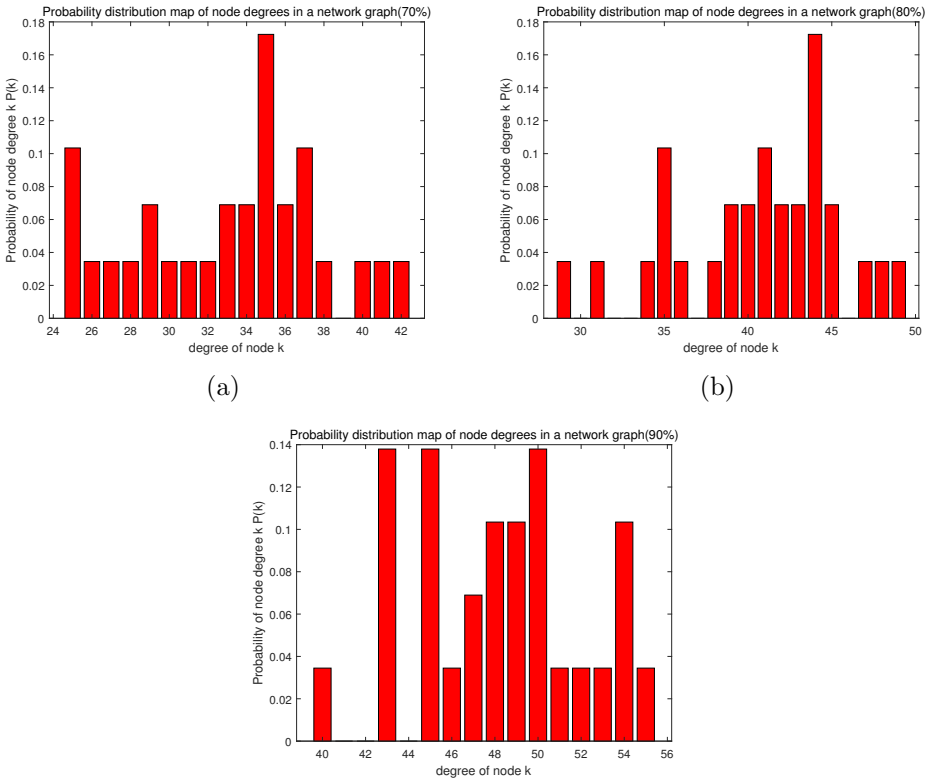
FIGURE 13. Topological result with 80% intercept probability

TABLE 1. Degree-degree correlation, average distance, network diamete

Feature	70%	80%	90%
Degree-degree Correlation	Negative Correlation	Negative Correlation	Negative Correlation
Average Distance	1.78597	1.81451	1.88823
Network Diameter	3	3	3

degree(70%):	degree(80%):	degree(90%):
k1 = 36	k1 = 42	k1 = 50
k2 = 42	k2 = 49	k2 = 55
k3 = 28	k3 = 35	k3 = 45
k4 = 34	k4 = 47	k4 = 54
k5 = 29	k5 = 35	k5 = 43
k6 = 35	k6 = 41	k6 = 45
k7 = 27	k7 = 38	k7 = 46
k8 = 35	k8 = 44	k8 = 49
k9 = 41	k9 = 45	k9 = 52
k10 = 38	k10 = 44	k10 = 49
k11 = 33	k11 = 41	k11 = 48
k12 = 40	k12 = 48	k12 = 54
k13 = 35	k13 = 41	k13 = 45
k14 = 37	k14 = 45	k14 = 54
k15 = 25	k15 = 31	k15 = 40
k16 = 32	k16 = 44	k16 = 51
k17 = 26	k17 = 39	k17 = 45
k18 = 35	k18 = 40	k18 = 48
k19 = 34	k19 = 39	k19 = 47
k20 = 25	k20 = 29	k20 = 43
k21 = 37	k21 = 44	k21 = 53
k22 = 37	k22 = 43	k22 = 48
k23 = 31	k23 = 43	k23 = 50
k24 = 33	k24 = 34	k24 = 50
k25 = 36	k25 = 42	k25 = 49
k26 = 29	k26 = 40	k26 = 50
k27 = 35	k27 = 44	k27 = 47
k28 = 30	k28 = 36	k28 = 43
k29 = 25	k29 = 35	k29 = 43
<k> = 33.1034	<k> = 40.6207	<k> = 48.1379

FIGURE 14. Degree of network



(a) (b) (c)

FIGURE 15. Degree distribution. (a) 70%; (b) 80%; (c) 90%.

4.3. **Interface Design Based on MFC.** Due to the complex data results of the experiment, this paper uses the MFC dialog program to build a battlefield network analysis

clustering coefficient(70%):	clustering coefficient(80%):	clustering coefficient(90%):
C1 = 0.047619	C1 = 0.0209059	C1 = 0.00408163
C2 = 0.018583	C2 = 0.0102041	C2 = 0
C3 = 0.0820106	C3 = 0.0285714	C3 = 0.00909091
C4 = 0.0552585	C4 = 0.00740056	C4 = 0.00209644
C5 = 0.0566502	C5 = 0.0369748	C5 = 0.0110742
C6 = 0.0537815	C6 = 0.0280488	C6 = 0.00909091
C7 = 0.0598291	C7 = 0.0256046	C7 = 0.00772947
C8 = 0.0487395	C8 = 0.0232558	C8 = 0.00765306
C9 = 0.0231707	C9 = 0.0151515	C9 = 0.00226244
C10 = 0.0312945	C10 = 0.012685	C10 = 0.00340136
C11 = 0.0568182	C11 = 0.0207317	C11 = 0.0035461
C12 = 0.0269231	C12 = 0.0124113	C12 = 0.00419287
C13 = 0.0605042	C13 = 0.0317073	C13 = 0.0151515
C14 = 0.0285285	C14 = 0.00909091	C14 = 0
C15 = 0.08	C15 = 0.0494624	C15 = 0.00641026
C16 = 0.0544355	C16 = 0.0169133	C16 = 0.00156863
C17 = 0.0769231	C17 = 0.0283401	C17 = 0.00808081
C18 = 0.0487395	C18 = 0.0230769	C18 = 0.00265957
C19 = 0.0499109	C19 = 0.0310391	C19 = 0.00740056
C20 = 0.0966667	C20 = 0.0615764	C20 = 0.0110742
C21 = 0.0405405	C21 = 0.02537	C21 = 0.00217707
C22 = 0.0315315	C22 = 0.0155039	C22 = 0.00443262
C23 = 0.0623656	C23 = 0.0232558	C23 = 0.00326531
C24 = 0.0492424	C24 = 0.0481283	C24 = 0.00408163
C25 = 0.0412698	C25 = 0.0197445	C25 = 0.0042517
C26 = 0.0640394	C26 = 0.0217949	C26 = 0.00489796
C27 = 0.0470588	C27 = 0.0190275	C27 = 0.00555042
C28 = 0.0643678	C28 = 0.0380952	C28 = 0.0110742
C29 = 0.09	C29 = 0.0436975	C29 = 0.013289
C = 0.053338	C = 0.0257852	C = 0.00584775

FIGURE 16. Clustering coefficient

point betweenness(70%):	point betweenness(80%):	point betweenness(90%):
B1 = 2.22448	B1 = 4.02201	B1 = 1.34444
B2 = 3.70618	B2 = 1.01515	B2 = 0.333333
B3 = 7.6728	B3 = 10.8374	B3 = 2.08333
B4 = 1.84848	B4 = 2.87197	B4 = 0
B5 = 33.4038	B5 = 17.1287	B5 = 3.23333
B6 = 0.4	B6 = 1.59215	B6 = 1.61111
B7 = 26.3522	B7 = 14.8063	B7 = 8.60801
B8 = 1.34842	B8 = 0.333333	B8 = 0
B9 = 4.88725	B9 = 1.22077	B9 = 0.833333
B10 = 16.0774	B10 = 7.61705	B10 = 5.62511
B11 = 7.20316	B11 = 3.88189	B11 = 3.83333
B12 = 0.25	B12 = 0.458333	B12 = 0
B13 = 1.06564	B13 = 0	B13 = 0.416667
B14 = 1.72717	B14 = 4.00164	B14 = 0.583333
B15 = 7.67856	B15 = 10.8709	B15 = 9.67857
B16 = 2.15336	B16 = 2.21212	B16 = 2.23333
B17 = 10.5907	B17 = 5.25779	B17 = 2.99167
B18 = 1.49381	B18 = 3.19476	B18 = 4.54286
B19 = 20.5427	B19 = 17.1969	B19 = 1.11111
B20 = 3.72093	B20 = 8.84848	B20 = 3.32071
B21 = 4.64787	B21 = 0.458333	B21 = 0.866667
B22 = 16.2611	B22 = 10.6876	B22 = 0.833333
B23 = 5.07769	B23 = 5.41899	B23 = 4.25051
B24 = 7.4245	B24 = 6.08077	B24 = 1.76111
B25 = 15.3163	B25 = 13.6326	B25 = 5.77983
B26 = 9.77577	B26 = 3.07897	B26 = 0.583333
B27 = 1.66863	B27 = 3.66495	B27 = 7.45758
B28 = 2.31111	B28 = 2.96037	B28 = 2.13889
B29 = 9.54762	B29 = 10.5507	B29 = 6.38182

FIGURE 17. Point betweenness

software [21]. The software consists of a main interface and three sub-interfaces, and the dialog type is modal. The main interface is shown in Figure 18. The interface contains three button controls, which are the guides to each sub-interface. A total of three buttons are included: battlefield network, reconnaissance simulation and feature calculation.

The battlefield network sub-interface is shown in Figure 19. The main content of this interface is to display the communication animation and business data generated by

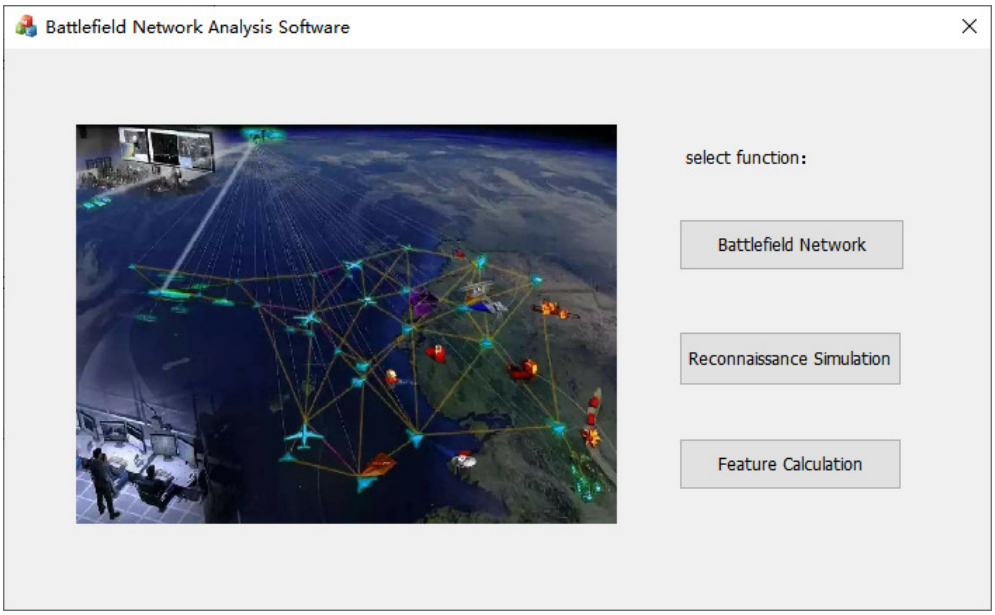


FIGURE 18. Battlefield network analysis software main interface

OPNET. First, click the "Open File" button to select the video file and data file to be played, then click the "Play Animation" button to play the animation on this page. The progress bar and buttons below the video can control the video playback progress. The data file can be opened by clicking the "Data File" button again.

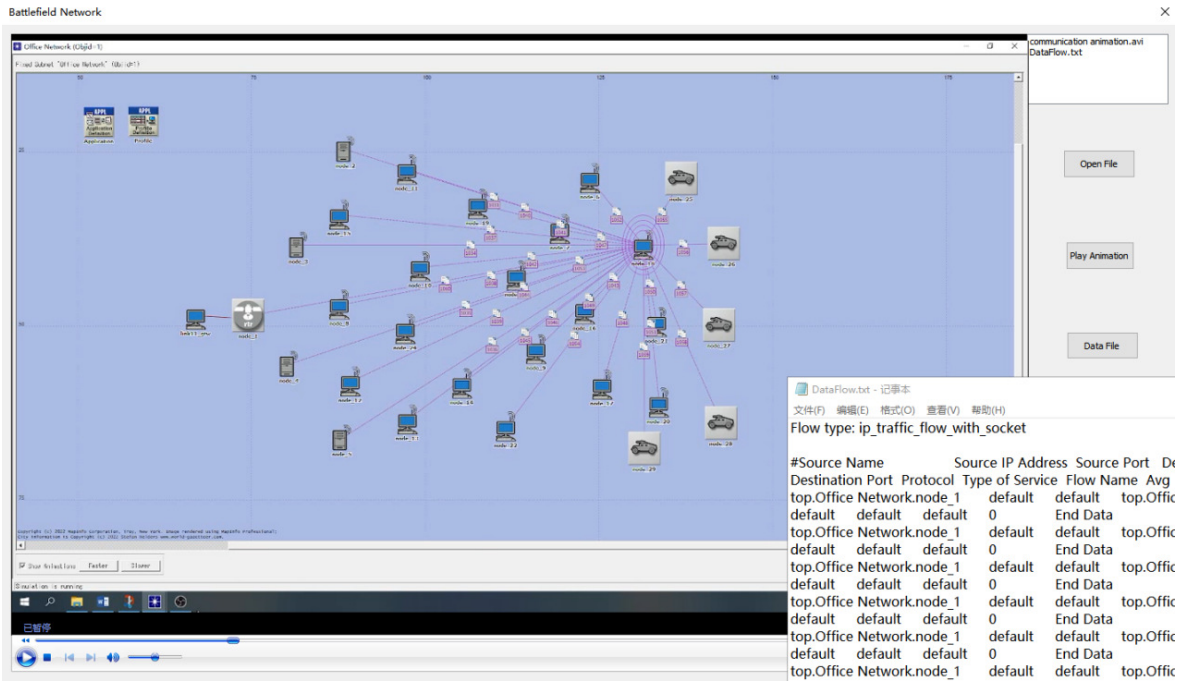


FIGURE 19. Battlefield network sub-interface

The reconnaissance simulation sub-interface is shown in Figure 20. The main content of this interface is to output the point-edge relationship of the network topology. Click the first button to select the scale you want to intercept, and click the ".net file format" button below to get the topology file in that scale.

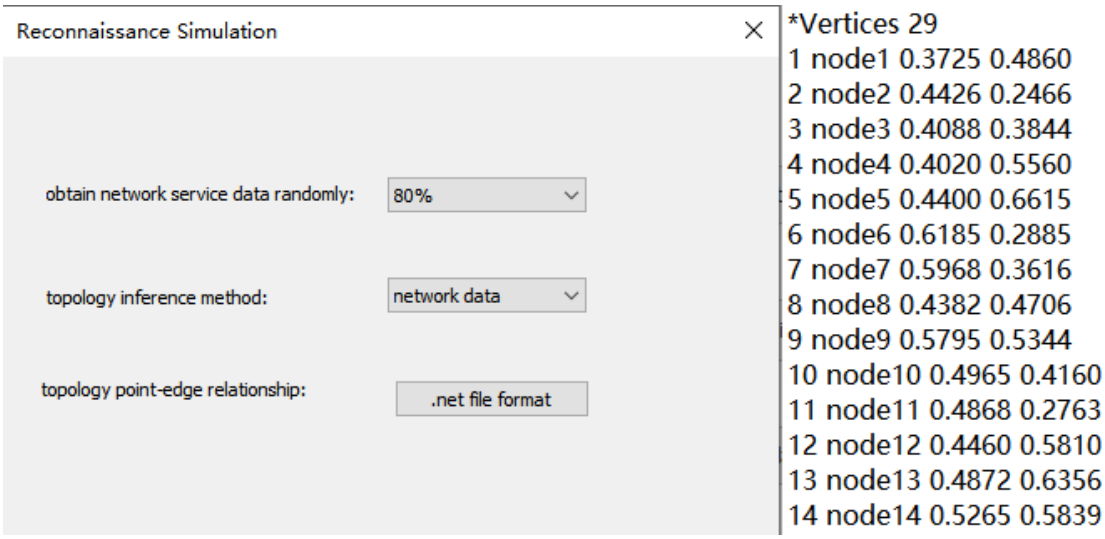


FIGURE 20. Reconnaissance simulation sub-interface

The feature calculation sub-interface is shown in Figure 21. The main content of this interface is to display the static characteristics of the network under different data interception proportions. First, select the scale in the drop-down box of the input topology file, and click the different buttons below according to the corresponding scale to view the corresponding static features. The figure shows the shortest path length when the interception ratio is 80%.

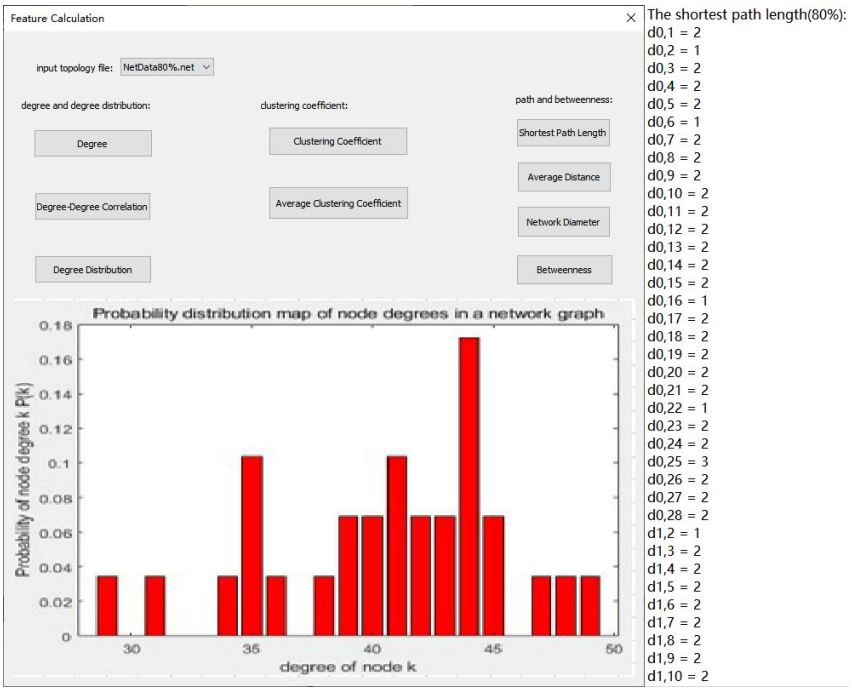


FIGURE 21. Feature calculation sub-interface

5. **Conclusion.** The research in this paper combines OPNET and VS2017 co-simulation to analyze the communication network based on Ad Hoc protocol. The construction and simulation of communication scenarios, topology inference and feature analysis have

been completed, which provides new ideas for battlefield network analysis. This paper firstly uses OPNET to build a simulation scene, generates communication animation and outputs communication data. The generated data is simulated and analyzed using VS2017 to obtain topology inference information and static characteristics of the network. Finally, a battlefield network analysis software is designed based on the above data, which can completely display the network communication animation, business data, network topology information and static characteristics.

Acknowledgment. This work is supported by Science Foundation of Zhejiang Sci-Tech University(ZSTU) under Grant No.19032458-Y. This work is also partially supported by Ningbo Science and Technology innovation 2025 major project under Grants No. 2021Z010 and No. 2021Z063.

REFERENCES

[1] W. Chen, J. Li and J. Jiang, "Research on Disintegration of Combat Networks under Incomplete Information," *2021 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 784–791, 2021.

[2] H. Nie, X. Cai, and H. Chen, "Analysis of interference performance of tactical radio network," *AIP Conference Proceedings*, 020177, 2017.

[3] S. Zhang, N. Huang and X. Sun, "Application Reliability Evaluation for Tactical Internet Based on OPNET," *2015 IEEE 12th International Conference on Ubiquitous Intelligence and Computing and 2015 IEEE 12th International Conference on Autonomic and Trusted Computing and 2015 IEEE 15th International Conference on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom)*, pp. 705–709, 2015.

[4] K. Nisar, I. A. Lawal, U. I. Abdulmalik, A. A. Muazu, BS Chowdhry, S. Khan, S. Memon, "QoS Analysis of the MANET routing protocols with Respect to Delay, Throughput, & Network load: Challenges and Open Issues," *2020 IEEE 14th International Conference on Application of Information and Communication Technologies (AICT)*, pp. 1–8, 2020.

[5] H. Bi and Z. Wei, "Research on route protocols of WiFi-based Ad-hoc network," *2014 IEEE 5th International Conference on Software Engineering and Service Science*, pp. 1154–1157, 2014.

[6] J. Lim, D. Keum, and Y.-B. Ko, "A Stepwise and Hybrid Trust Evaluation Scheme for Tactical Wireless Sensor Networks," *Sensors*, vol. 20, no. 4, 1108, 2020.

[7] D. Chen, J. Y. Khan, J. Brown, M. A. Javed, and Y. Zhuang, "A 6LoWPAN OPNET simulation model for machine-to-machine communications," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 11, e4120, 2020.

[8] A. M. El-Semary and H. Diab, "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map," *IEEE Access*, vol. 7, pp. 95197–95211, 2019.

[9] E. A. Tuli, M. Golam, D.-S. Kim, and J.-M. Lee, "Performance Enhancement of Optimized Link State Routing Protocol by Parameter Configuration for UANET," *Drones*, vol. 6, no. 1, 22, 2022.

[10] D. Ding, F. Bu, and B. Wang, "Modeling and Performance Analysis of OPNET-Based Routing Protocols for Mobile Ad Hoc Networks," *2021 IEEE 9th International Conference on Information, Communication and Networks (ICICN)*, pp. 323–328, 2021.

[11] L. Zhou, Y. Chen, Z. Li, and Z. He, "An Improved Video Monitoring System Based on RSVP Protocol," *2015 International Conference on Intelligent Transportation, Big Data and Smart City*, pp. 94–97, 2015.

[12] Z. Niu, Q. Li, T. Ma, L. Jiang, "Research on Non-cooperative Topology Inference Method Based on Node Location Information," *2018 IEEE 18th International Conference on Communication Technology (ICCT)*, pp. 271—275, 2018.

[13] J. Liu, J. Hao, Z. Shi, "Building the COVID-19 Collaborative Emergency Network: a case study of COVID-19 outbreak in Hubei Province, China," *Nat Hazards 104*, pp. 2687—2717, 2020.

[14] Q. Yu, Z. Wang, Z. Li, X. Liu, F. Oteng Agyeman, and X. Wang, "Hierarchical Structure of Depression Knowledge Network and Co-word Analysis of Focus Areas," *Frontiers in Psychology*, vol. 13, 920920, 2022.

[15] J. Zhu, Y. Jiang, T. Li, H. Li, and Q. Liu, "Trend Analysis of COVID-19 Based on Network Topology Description," *Frontiers in physics*, vol. 8, 564061, 2020.

[16] Y. Wang, Y. Wang, Z. Wang, G. Yang, and X. Yu, "Research cooperations of blockchain: toward the view of complexity network," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, pp. 1339–1352, 2022.

[17] S. Morita, "Solvable epidemic model on degree-correlated networks," *Physica A: Statistical Mechanics and Its Applications*, vol. 563, 125419, 2021.

[18] A. L. Sreenivasulu and P. Chenna Reddy, "NLDA non-linear regression model for preserving data privacy in wireless sensor networks," *Digital Communications and Networks*, vol. 6, no. 1, pp. 101–107, 2020.

[19] R. Awari, "Parallelization of shortest path algorithm using OpenMP and MPI," *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pp. 304–309, 2017.

[20] G. Zhang and W. Zhang, "Protein–protein interaction network analysis of insecticide resistance molecular mechanism in Drosophila melanogaster," *Archives of Insect Biochemistry and Physiology*, vol. 100, no. 1, e21523, 2020.

[21] G.-S. Cho, "Development of an anti-forensic tool for hiding message in a directory index of NTFS," *2015 World Congress on Internet Security (WorldCIS)*, pp. 144–145, 2015.