

Research on “Real-Network-in-the-Loop” Simulation Based on OPNET

Jian-jun Shen^{1,a}, Kai Li^{1,b}, Yu-qing Xu^{1,c}

1Academy of National Defense Information, Wuhan, Hubei, China

ashjj06@sina.com, b307482359@qq.com, cqjl44@163.com

Abstract

As for communication network simulation, embedding real network into simulation loop can bring lots of advantage. However, there are some problems waiting to be addressed. Targeting the application of communication network training, this paper firstly put forward a simulation structure of “Real-Network-in-the-Loop”, which can connect the real communication network with the simulated communication network and implement the data packet interaction between two. Secondly, this paper designed the internal structure of IP/HLA Converter, which can complete the conversion between the IP-format data packet and HLA-format data packet. Finally, this paper put forward some ways for realization of key techniques such as IP packet intercepting, raw IP packet sending and etc. With above schemes, paper solved the simulation issue of “Real-Network-in-the-Loop” fully.

Keywords: Simulation, Real-Network-in-the-Loop, OPNET, HLA, Format Conversion

Introduction

In information age, with the arising of new operation patterns such as information operation, network-centric warfare and etc, the network are playing an increasingly important role in modern warfare [1]. Since some tactics communication networks have employed many novel techniques and feature more complex network structure and larger network scale, the method of simulation is often adopted to verify these networks characteristics.

As an excellent simulation platform, OPNET is widely adopted for the modeling and simulation of the communication network [2]. On general conditions, it should firstly conduct network modeling, node modeling and process modeling and then gain the simulation result through the computer execution. However, in practical applications, mainly in the simulative training of the communication network [3], besides the simulated network, the real communication network should be connected to OPNET sometimes in order to gain better training results.

In the simulative training, the advantages of the real communication network connecting to OPNET are as follows: 1) improving the fidelity of the upper

training application because of the real communication network operation, such as message transmission; 2) conducting the real combat operation to the communication network, such as electronic interference; and 3) reducing the simulated network scale of OPNET, then improving the timeliness of simulation execution.

The combination of the simulated network and real network calls for the solution of some issues related to the design of simulation structure and the realization of some techniques. Aiming at these issues, the paper will conduct research and put forward solutions in the following parts.

Simulation Structure

In the information age, distributed interactive simulation is the development trend, thus the simulation structure of communication network should tally with this requirement. As a standard distributed interactive simulation architecture, HLA (High Level Architecture) has been used world widely [4]. Thus, the simulation structure of “Real-Network-in-the-Loop” for communication network simulative training should adopt the architecture based on HLA, shown as Fig.1.

In Fig.1, all training seats, IP/HLA Converter and OPNET Simulator constructed a simulation federation. All of them join in the federation as federates and carry out information interaction among them through HLA standards, for example, the training seats send the device operation parameters or message data to OPNET Simulator, etc.

OPNET Simulator is applied to the running of the simulated network. Real Network represents the actual communication network, which access to LAN through Router. Real Network realizes its information interaction with OPNET Simulator through IP/HLA Converter, thus the information interaction between the simulated network and the real network is achieved.

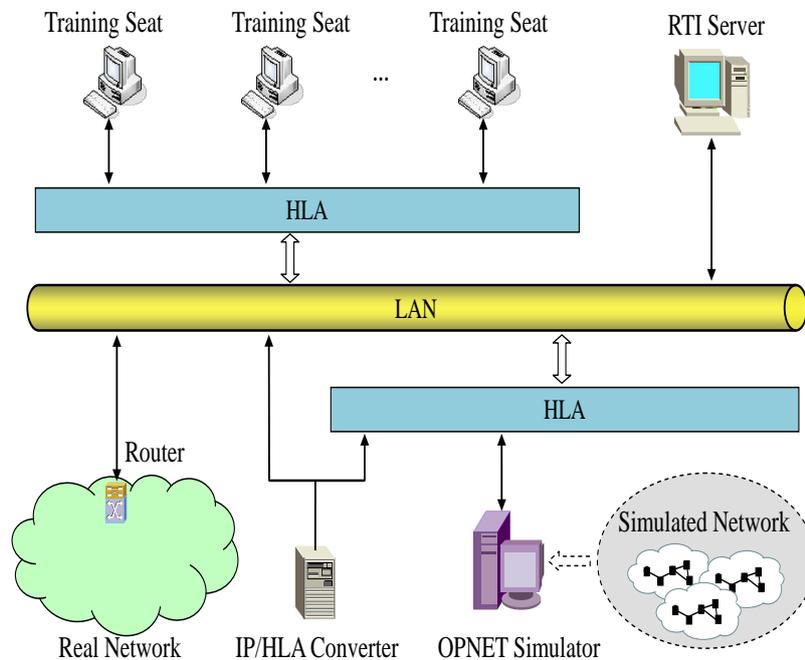


Fig.1. The “Real-Network-in-the-Loop” simulation architecture based on HLA.

Apart from joining in the federation with HLA standards, IP/HLA Converter can implement direct network communication. IP/HLA Converter is used for achieving data conversion of IP-format data packet and HLA-format data packet, thus becomes the communication bridge between the simulated network and the real network.

All the training seats are mapped to one node in the simulated network. When the training seat A sends a data packet to the training seat B, the data packet is firstly sent to the corresponding node A' of the simulated network within OPNET Simulator. Then, OPNET Simulator simulates the route and data transmission process from A' to B', and after the simulation is finished, the data packet is sent from B' to B. Since all training seat adopt LAN IP address, while the simulated network within OPNET Simulator adopts the IP address similar to that of the actual communication network, the address should be converted when the training seat communicates with the Real Network, that is, the LAN IP address should be converted into that of the simulated network.

The Structure of IP/HLA Converter

IP/HLA Converter is used for achieving the format conversion between the IP data packet and the HLA data packet. Its internal structure was shown as Fig.2.

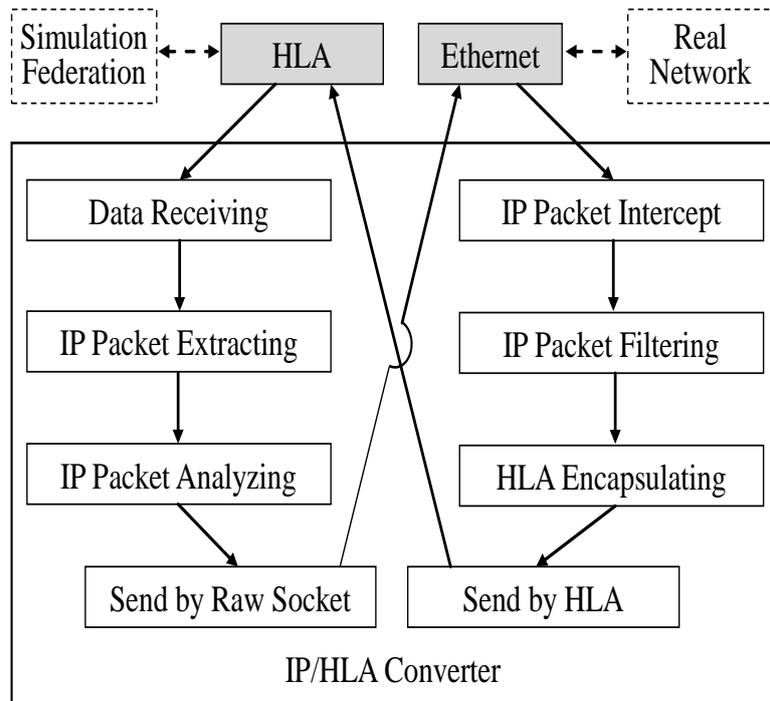


Fig.2. The structure of IP/HLA Converter.

In Fig.2, the “IP Packet Extractor” module is used for extracting IP packet from the HLA-format data packet. Here, the IP packet is the data such as writ data and etc sent from the training seat to the Real Network. The “IP Packet Analyzing” module is used for judging whether the destination address of IP packet is located in the Real Network. If not, it will be discarded. The “Send by Raw Socket” module is used for sending IP packet to the Router of Real Network in the form of “Raw Socket”, then, the Router sends IP packet to the real communication network.

The “IP Packet Intercept” module is used for intercepting the data packet in IP Protocol Layer. The “IP Packet Filtering” module is used for judging whether the destination address of IP packet is located in the simulated network. If not, the data packet will be handed intact over to the IP protocol layer for further handling. The “HLA Encapsulating” module is used for encapsulating the IP packet into the HLA format data packet. The “Send by HLA” module is used for sending HLA data packet according to the HLA standards. The HLA data packet will be received by OPNET Simulator.

The Data Exchange Procedure

After the connection of the simulated network and the real network, the data communication between the two networks poses a problem due to their different

operation mechanisms. It calls for resolution through some measures. In the following part, the data exchange procedure between the simulated network and the real network is firstly given. In the next section, the paper will give the relevant key techniques.

Since all training seats are mapped to the nodes in the simulated network, the data sending from the simulated network to the real network actually means the data sending from the training seats to the real network, this procedure was shown as Fig.3.

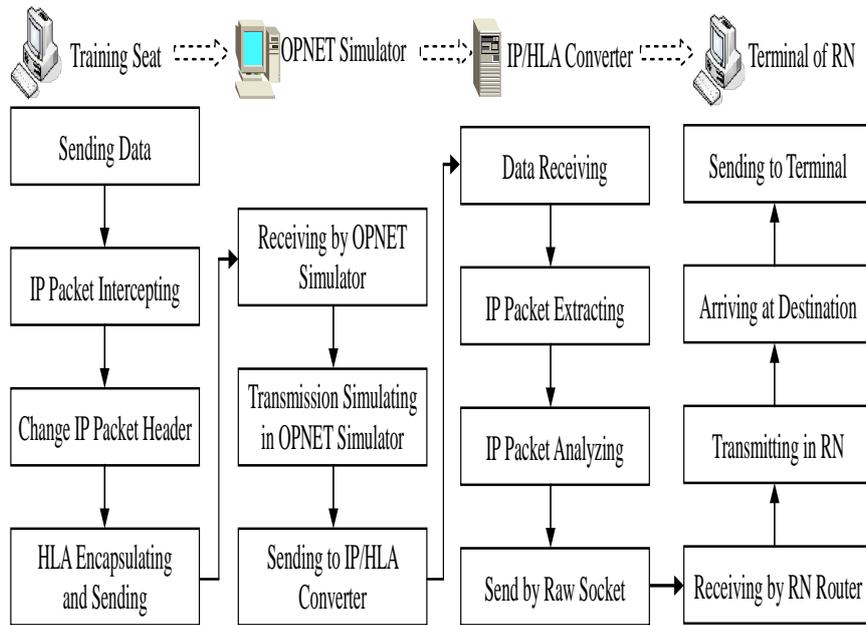


Fig.3. The data exchange procedure from training seat to real network.

In Fig.3, RN stands for Real Network. The “Change IP Packet Header” module is used for changing the source address (it is the LAN address) of IP packet to the IP address of the corresponding node in simulated network, and then checksum work is conducted. The “Transmitting in RN” module stands for the transmission of IP data packet in the real network, i.e. the transmission between the real devices through the real communication channel.

Realization of Key Techniques

A. Data Packet Intercepting. In the training seat and IP/HLA Converter, in order to convert IP data sent from the application software (such as writ software) or received by the Ethernet port to the data of HLA format, it is necessary to intercept the IP data firstly, however it needs employing the core programming techniques of the operation system.

There are three frequently used IP data intercepting techniques, namely the techniques based on API hook, based on IP filtering hook and based on the interlayer driving of NDIS [5]. After comparing the three techniques, this paper finds out that the second technique is feasible in terms of its difficulty and can also intercept TCP link-building and other data. Therefore, this paper adopts this technique to intercept the IP data.

The procedure to realize IP Filtering Hook technique is: 1) write a filtering hook function PF_FORWARD_ACTION (*PacketFilterExtensionPtr) (...), where the analyzing and processing of IP packet is conducted; 2) invoke the function IoGetDeviceObjectPointer(...) for getting the pointer of IP filtering drive device to install hook function; 3) invoke IoBuildDeviceIoControlRequest(...) and IoCallDriver(...) to finish the installation of IP filtering hook function.

B. Conversion of Data Packet Format. The data packets operated by real network, the federate and the OPNET simulation are different formats [6]. To ensure the normal operation of whole simulation system, the data packets of different formats should be converted. The format conversion includes two parts. The first is converting the IP data to HLA data, and the second is converting the HLA data to simulation data of OPNET. As to the first, it only requires the HLA FOM (Federation Object Model) to be designed and then the conversion to be conducted. As to the second, it requires OPNET-HLA module to be placed in the simulation scenario and the map file configured during the OPNET modeling. Since map file defines the conversion relationship between the HLA data packet and the simulation packet of OPNET, OPNET-HLA module will conduct format conversion based on that and send the converted simulation packet to the specified process module, shown as Fig.4.

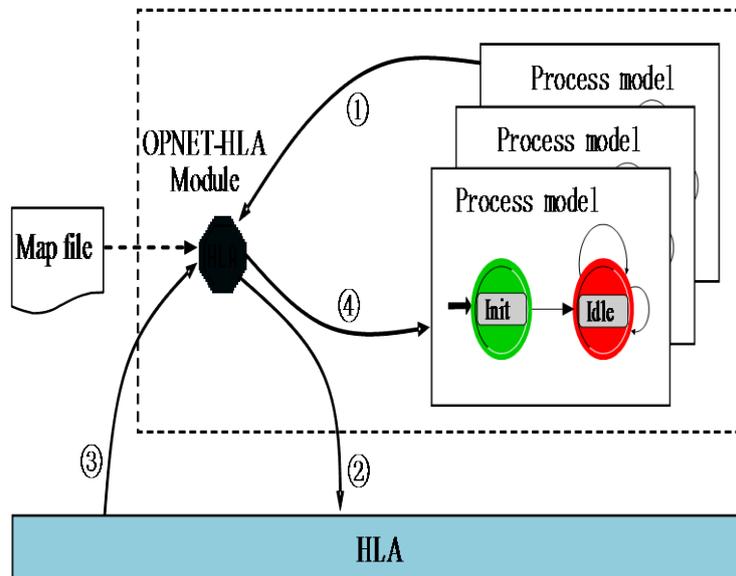


Fig.4. The conversion between HLA data packet and OPNET simulation packet.

C. Raw IP Packet Sending. In the IP/HLA Converter, since the extracted IP packet (made up of IP header, TCP/UCD header and application data) is raw IP packet, the IP data packet should be directly sent out without making any changes. It needs raw socket technique. The establishment method of the raw socket technique is “SOCKET sRaw = ::socket(AF_INET, SOCK_RAW, IPPROTO_RAW)”. After the raw socket is created, it can be used to send out IP data packet through Ethernet port.

References

- [1] Jianjun Shen. Research on Operation Simulative Training in Information Age, Applied Mechanics and Materials, Vols. 411-414 (2013), pp.2860~2864.
- [2] Youcef Atamna. OPNET-based Modeling and Simulation of C4 System[DB/OL]. <http://www.modelingandsimulation.org/MandS010part3.pdf>,2004-02-12.
- [3] Jianjun Shen, Zhichun Gan, Xiaohu Yu. The Research on Tactical Internet Simulative Training and its Dynamic Real-time Network Simulation, International Conference on Information Management and Engineering, Beijing, 2010, pp.354~358.
- [4] Yan Zhou, Jianwei Dai. The Simulation Program Design of HLA, Publishing House of Electronics Industry, Beijing, 2002. (in chinese)
- [5] Zhaoyong Fan. Research on Overall and Key Problems of Tactical Internet Training Simulation System, Communication Commanding Academy, Wuhan, 2009. (in chinese)
- [6] Hongxin Li. Research on Hardware-in-the-Loop Simulation Mechanism in OPNET, Journal of Information Engineering University, Vol.12, No.4 (2011), pp.509~512. (in chinese)