18th ICCRTS

The Analysis of Information Exchange Capability for Battlefield Networks using M&S techniques of the NetSPIN

Topics: Networks and Networking
Modeling and Simulation
Experimentation, Metrics, and Analysis

Authors: Sangheun SHIM (PoC), Jaeyoung CHEON, and Myunggil AHN

Organization: Defense Cyber Warfare Technology Center,
Agency for Defense Development

Address: Mt.25, Geoyeo-dong, Songpa-gu, Seoul,
138-110, Republic of KOREA

Telephone: +82-10-5012-4023

E-mail: ssheun@hanmail.net, ssheun7@add.re.kr

The Analysis of Information Exchange Capability for Battlefield Networks using M&S techniques of the NetSPIN

Sangheun SHIM, Jaeyoung CHEON, and Myunggil AHN

ABSTRACT

To achieve information superiority of weapon systems for the NCW, they should have the capability that can give information to elements of a battlefield timely and correctly. To assess it, we have been developing the NetSPIN that is the tool to evaluate the timeliness and correctness of information exchange in the battlefield network, which are modeled and simulated using the OPNET. In this paper, we suggest the analysis method of information exchange capability for battlefield networks using M&S techniques of the NetSPIN. First, its M&S techniques are described. Next, we analyze and evaluate the timeliness of messages for the specific operation when the traffic of the Korea tactical communications system called the SPIDER is increased due to introduction of new systems such as an UAV in a corps and a video conferencing system in a division. Particularly, the battlefield network is composed of simulated models of the SPIDER. Also, equipments and organizations of the ATCIS are modeled and interconnected on the SPIDER grid, and they communicate mutually to exchange simulated traffics. Finally, the end-to-end delay of messages for the specific operation and the throughput of links are computed to assess affects for the existing battlefield network according to introduction of new systems.

Keywords: Information Exchange Capability, NetSPIN, SPIDER, ATCIS, OPNET

1. INTRODUCTION

For the NCW (Network Centric Warfare) that networks of a battlefield are interconnected in real time, the interoperability between C4I (Command, Control, Communications, Computers, Intelligence) & weapon systems is essential. Interoperability is the ability of systems, units or forces to provide data, information, material and services and to accept the same from other systems, units or forces and to use the data, information, material and services so exchanged to enable them to operate effectively together. Especially, information exchange capabilities; the timeliness and correctness of information exchange are needed as key factors of C4I & weapon systems for interoperability [1].

To analyze, test, and evaluate the timeliness and correctness of information exchange between elements of the battlefield, communications systems and weapon systems have to be operated according to various operating scenarios in battlefields. However, to do this, a huge sum of time, cost, and manpower are needed, and it is not easy that various circumstances of battlefields are reflected on.

Therefore, up to now, in the laboratory that has the communication circumstance better than the real battlefield, the information exchange capability has been tested mostly for the developed system that is connected with system in the LAN (Local Area Network). Also, tests in a real environment have been executed using the simple communication network and the test scenario. These are not enough to perform faithfully the analysis of the timeliness and correctness of information exchange between elements in a battlefield.

To solve these problems, developed countries such as USA or EU have been made use of network M&S (Modeling and Simulation) techniques. For example, there are JCSS (Joint Communications Simulation System) of DISA (Defense Information Systems Agency) and NetCOS (Network Centric Operations Simulation) of EADS (European Aeronautic Defense and Space) company that can analyze communication effectiveness in the synthetic battlefield environment [2], [3]. In the similitude of them, we have been developing simulation models of several C4I & weapon systems in Korea. Based on them, we have been researching core technologies to test and evaluate the timeliness and correctness of information exchange. In the concrete, we have been developing the NetSPIN (Network Simulator & Planner for Interoperability) [4], [5]. It is a tool that is able to conduct them based on models of battlefield networks that are simulated using the OPNET [6], and by interlocking external real C4I & weapon systems. Furthermore, it reflects real effects of battlefield networks in the laboratory environment.

The development objectives of the NetSPIN are to develop methods for interoperability T&E (Test and Evaluation) based on the network M&S, and model battlefield communication environments considering IERs (Information Exchange Requirements), communications operation scenarios, network equipment & configuration information, network operation organization information, and terrain & environment information. Furthermore, we build the test scenario using developed models. And using it, the test is executed and its results are evaluated. Also, developed models and test results are managed in the repository.

Figure 1 denotes the overall operation concept of the NetSPIN. It is able to validate the propriety of the IER of each system and verify the timeliness of information exchange for the interoperability T&E of C4I & weapon systems. It can be also utilized to find new requirements for networks and plan the network considering a bandwidth and a topology.

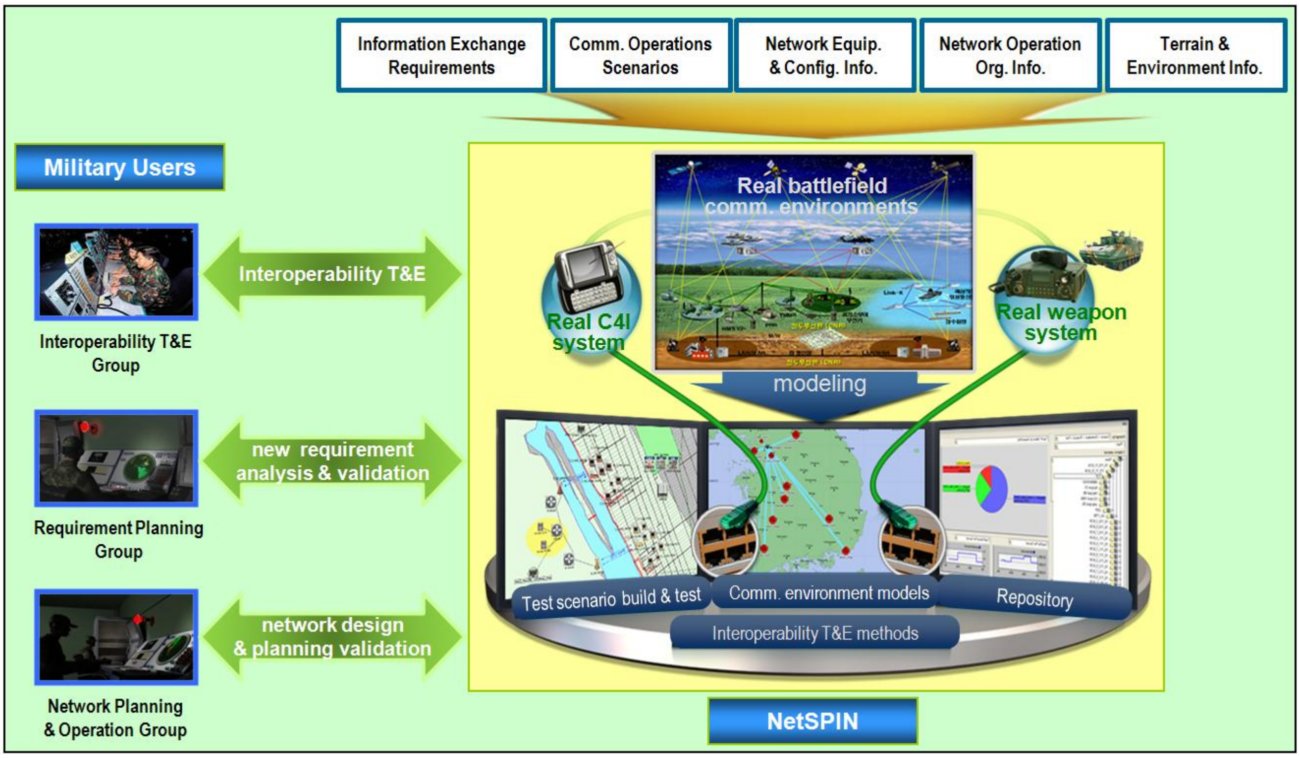

Figure 1. Overall operation concept of the NetSPIN

In this paper, in the situation that traffics in the Korea tactical communications system called the SPIDER [7] are increased because of the introduction of new systems such as the UAV (Unmanned Aerial Vehicle) in a corps and a VTC (Video Tele-Conference) system in a division, the timeliness of messages for the specific simulated operation is analyzed and evaluated.

To do this, the communications network of a corps is composed of simulated models of the SPIDER, and device models and organization models of the ATCIS (Army Tactical C4 Intelligence System) [8] of Korea are interconnected on the simulated SPIDER grid. In particular, simulated models for main units of a corps are placed in the simulated SPIDER network. Therefore, they are able to communicate each other, and exchange simulated traffics through the simulated network. In conclusion, in the simulation, the end-to-end delay of messages for the simulated operation and the throughput of links are outputted, and changes of the existing battlefield network for introduction of new systems are analyzed.

The rest of this paper is organized as follows. Section 2 introduces network modeling of the NetSPIN. Section 3 describes the simulated scenario model related to our analysis, and explains analysis results for the suggested scenario through computer simulations. Finally, Section 4 concludes this paper.

2. NETWORK MODELING OF THE NETSPIN

Figure 2 shows the overall hierarchy of models of the NetSPIN. As shown in the Figure 2, the scenario model consists of several models such as the organization model, the OPFAC (OPerational FACility) model, the device model, the link model, the terrain model, and the traffic model. The OPFAC model is the set of device models, and the traffic model includes IER (Information Exchange Requirement). In particular, to model networks, first, the device model that consists of a network is developed, and the OPFAC model that reflects arrangement and connection of device models is developed. Also, the network of a military organization is modeled as the organization model. Lastly, traffics that are exchanged in the network are simulated as the traffic model.

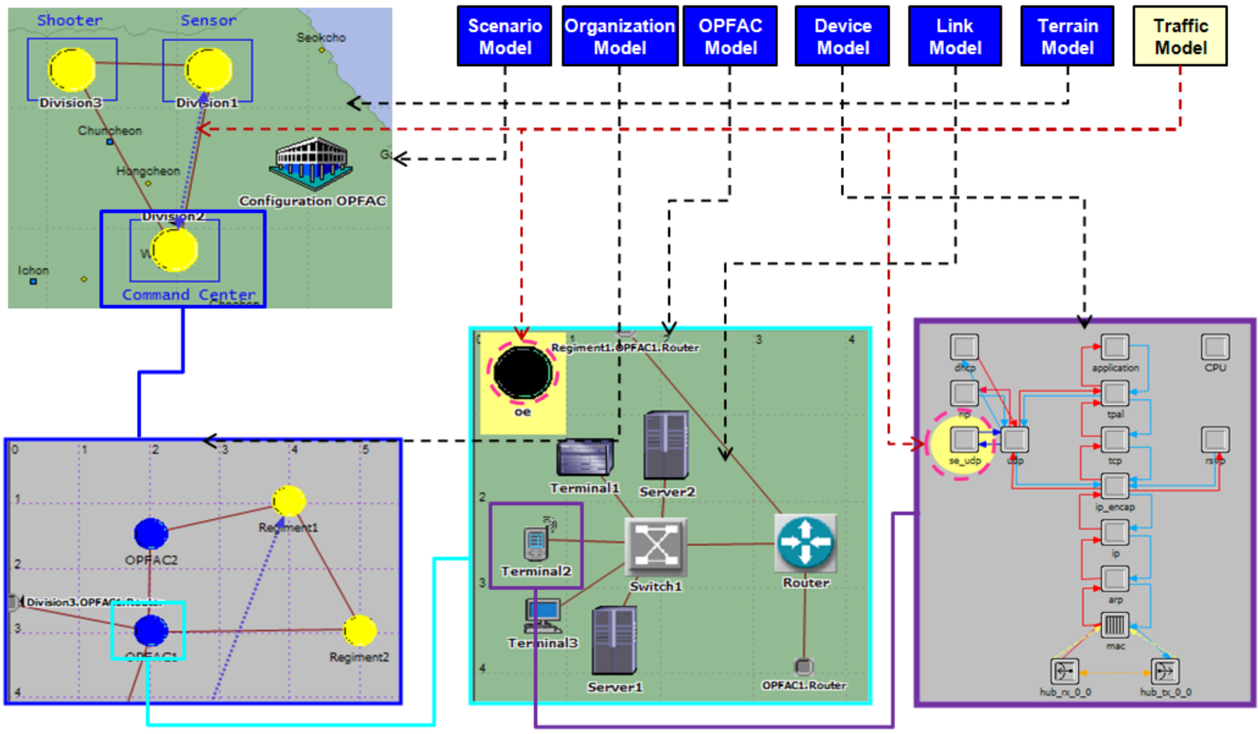

Figure 2. Overall model hierarchy of the NetSPIN

2.1 Device modeling

The device model simulates functions of a communication device, and consists of a node model and a process model. A node model is consisted of processors and queues. A processor is general-purpose building blocks of node models, and is fully programmable. A queue offers all the functionality of processors, and can also buffer and manage a collection of data packets. Next, a process model represents communication protocols and algorithms. Furthermore, it includes shared-resource managers, queuing disciplines, specialized traffic generators, statistic-collection mechanisms, and control processes.

In this paper, we use device models of the ATCIS and the SPIDER in the NetSPIN [7], [8]. The ATCIS of Korea is the tactical command and control system that automates warfighting procedures through integration of C4I between units under the corps of an army, and is interconnected with sensor & striking systems. And, the SPIDER is the army tactical communications system of Korea for real-time command & control of tactical units, and services wired/wireless voice and data communication based on the grid network for a corps. Device models of them are shown in Table 1.

Table 1. Device models of the ATCIS in the NetSPIN

Name	Main functions
Terminal	Functions as the terminal that generates traffics
MFE (Multi-Function accessing Equipment)	Function to transform messages of SST into TCP /IP packets
Terminal_PPP	Functions of the terminal as the commander's laptop to access the ATCIS in the battalion under the direct control of the regiment
DMC (Digital Modem Concentrator)	Function to serve PPP (Point to Point Protocol) services in the battalion under the direct control of the regiment
DLP (Data Link Processor)	Function to transmit data between functional centers and units
ATCIS_SERVER	Functions of the server for data requests between a functional room and a unit
SST (Surveillance & striking System Terminal)	Functions to generate, transmit, and receive traffics
Backbone switching hub	Functions for L2 switching
Workgroup switching hub	Functions for L2 switching

Table 2. Device models of the SPIDER in the NetSPIN

Type	Name	Main functions
Circuit-based switch	TTC-95K (Tactical Switch)	· call processing · circuit switching · flood search routing for searching the position of subscribers · resource management
	PCU (Packet Communication Unit)	
	RSC (Remote Subscriber Concentrator)	
IP router	TDU (Trunk Distribution Unit)	· IP routing function · Integrated multiplexed trunk operation
Mobile communication device	RAU (Radio Access Unit)	· circuit switching · wireless accessing function
	MST (Mobile Subscriber Terminal)	· call processing and data communication function · wireless accessing function
Wireless transmission device	TMR (Tactical Multichannel Radio)	· wireless relay function · wireless accessing function
	RLI (Radio Link Interface)	
Terminal	DMT (Digital Multi-role Terminal)	· call processing · data communication function
	CNRI (Combat Net Radio Interface)	· call processing · interconnection with a FM radio

2.2 OPFAC and organization modeling

The OPFAC model simulates the set of communication devices that are grouped according to the system type and the military organization. For example, because devices of the ATCIS between a corps and a division are different in the respect of composition and specification, it is modeled differently according to the military organization. The example of the OPFAC model and the organization model of the ATCIS for a division is shown in Figure 3.

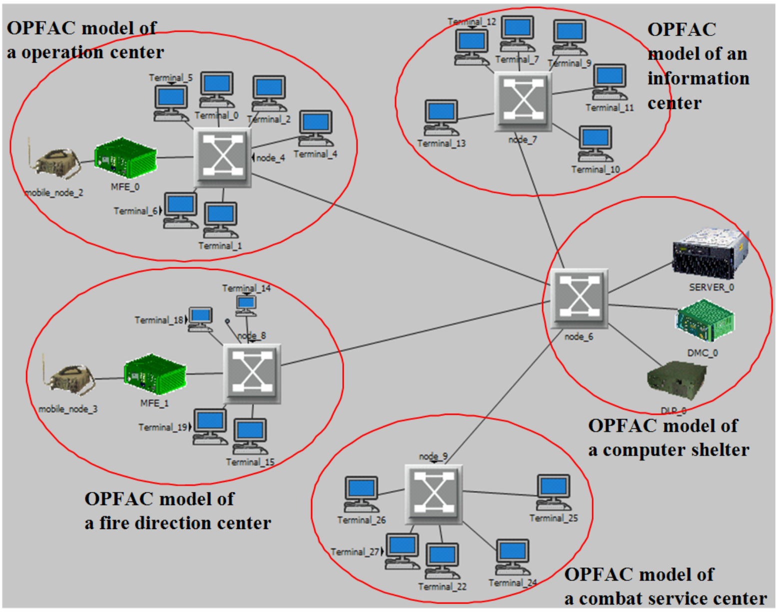

Figure 3. OPFAC models in the organization model of the ATCIS for a division

The organization model that simulates a military organization is the hierarchical combination set of OPFAC models, and is able to include subordinate OPFAC models. Furthermore, the OPFAC and organization model have attributes such as a name, a position, a movement path, and an operating period.

2.3 Traffic modeling

The traffic model simulates information exchange data that are induced to the scenario model. The NetSPIN uses several traffic models. Those are the IER model, the thread model, the application model, the application demand model, and the traffic flow model. The IER and thread model are developed newly, and the other models are COTS (Commercial Off The Shelf) models that are supplied by the OPNET.

The IER model models information to be exchanged between communication devices based on the information exchange list that is provided by the military. It includes attributes such as ID (identification) of Tx (Transmit) & Rx (Receive) devices, traffic generation patterns, and traffic processing characteristics. The attribute of generation pattern has information such as start time, maintenance time, size, and occurrence period. Traffic processing characteristics are like as the retransmission policy, the transmission priority, and the available period.

The thread model is the set of IER models that are generated sequentially between Tx/Rx devices, and is suitable to represent information exchange needed to the military mission. Particularly, for military missions, it is able to have information such as the start condition, the start/end time, the repetition period, the composition IER, the connection between composition IERs, and the mandatory IER.

The application traffic model represents traffics that are composed by COTS applications such as HTTP (Hyper Text Transfer Protocol), E-mail, FTP (File Transfer Protocol), VTC, and VoIP (Voice over Internet Protocol). It has attributes such as the application type, the start time, the operation period, and the repetition period.

The application demand model simulates flows of traffics between a client and a server or between a client and a client. It does not represent the application protocol in detail, and models traffics as transferring defined responses for requests from a client. Furthermore, it characterizes traffics as the size and the request per hour.

The traffic flow model simulates flows of traffics between a client and a server, or between a client and a client, and characterizes traffics as bps (bit per second) and pps (packet per second). Figure 4 shows the modeling procedure for IERs and traffic in the overall modeling and simulation process.

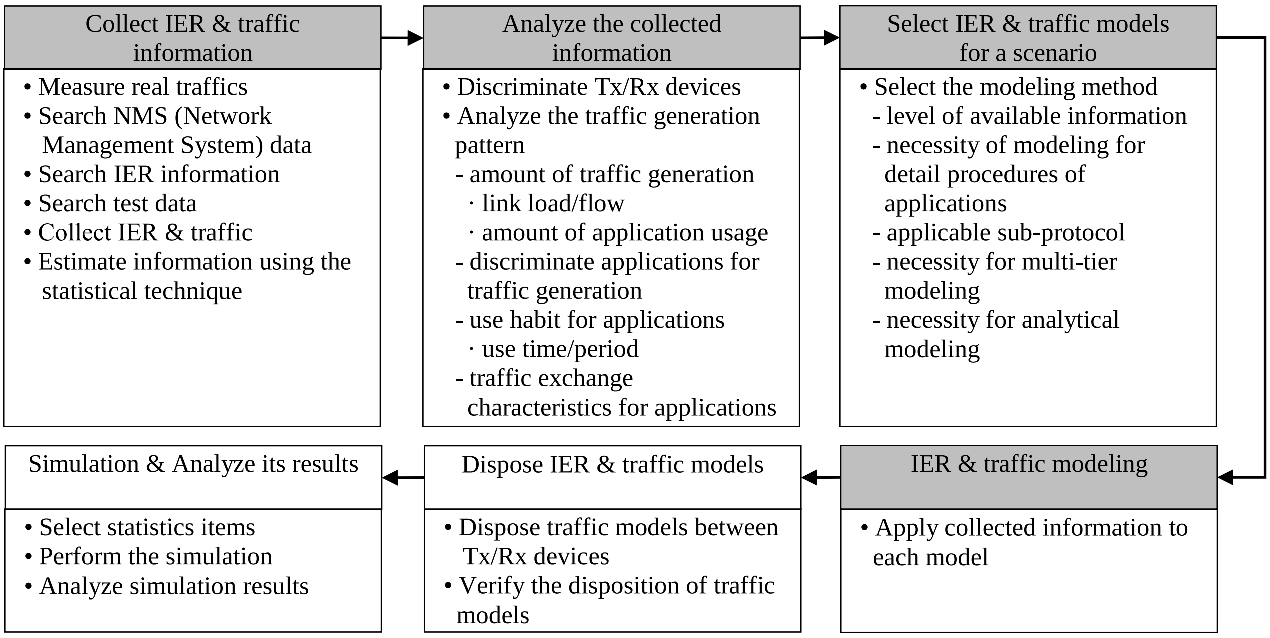

Figure 4. Modeling procedure of IER and traffic in overall simulation process

3. SCENARIO MODELING AND SIMULATION

Based on the network model of the SPIDER of a corps that is simulated in the NetSPIN, we analyze related effects as generating various types of traffics using ATCIS models. In particular, traffics of new systems are added to the SPIDER network of a corps that arbitrary simulated traffics are induced. Simulated new systems are the UAV of a corps and the VTC system in a division. In a situation that traffics are increased due to them, we analyze and evaluate whether messages for the simulated operation are transferred timely or not. The items for analysis are the timeliness of operation messages and traffics, and the utilization of a bottleneck link.

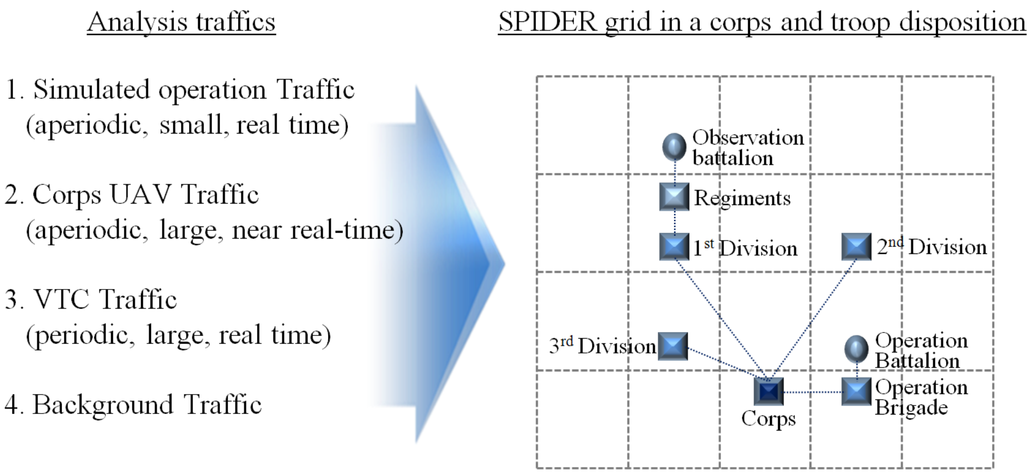

Figure 5. Scenario concept for the analysis of information exchange capability

Figure 5 shows the scenario concept for the analysis of information exchange capability. In the composition of our simulation scenario, a corps and subordinate units of it such as a division, an operation brigade, a regiment, and a battalion are disposed on the SPIDER network grid of a corps. Also, four types of traffics are exchanged in the simulated network model.

3.1 Analysis scenario modeling

In order to analyze information exchange capability, the network model of a corps is made up using device, OPFAC, and organization models of the SPIDER. Furthermore, models of the ATCIS that generate and exchange traffics are linked with it. This simulated scenario model is seen in Figure 6.

As shown in Figure 6, a corps, subordinate divisions, an operation brigade, and regiments under a division are arranged in the simulated scenario model, and these units are linked to communicate each other through the grid network of the SPIDER in a corps. Furthermore, communication networks of each unit are composed of OFAC models in organization models and device models in OFAC models.

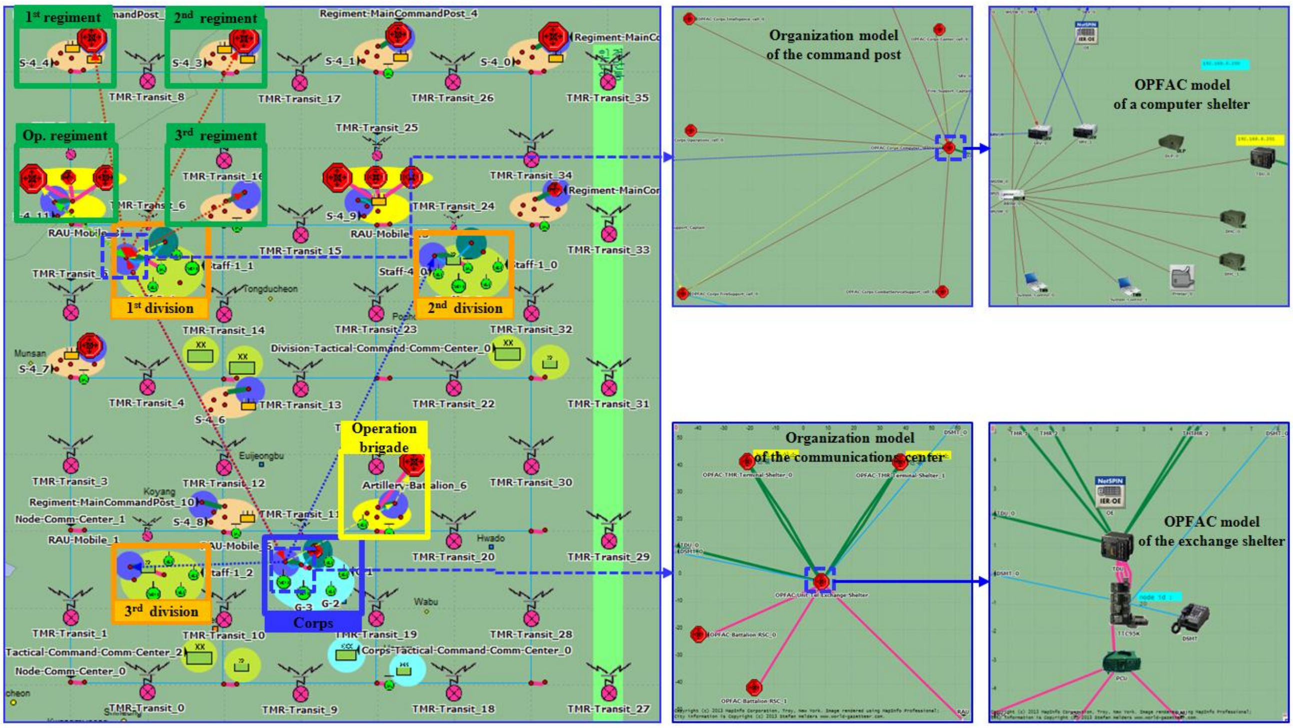

Figure 6. Simulated scenario model for the analysis of information exchange capability

In exchange flows of traffics between these models, the exchange sequence of simulated operation traffics considers the situation that the system in a division transfers operation messages to the system of the battalion under a corps. Messages of simulated operations are transferred using the threaded IER demand model.

As shown in Figure 7, messages of simulated operations are flowed from the operation regiment under a division, followed by the division communications center, the division main command post, the corps communications center, the corps main command post, and the battalion under an operation brigade.

Also, UAV traffics of the corps, and VTC traffics between the corps and the division are exchanged between the corps main command post and the division main command post. Furthermore, VTC traffics between units under the division are exchanged between the division and subordinate regiments.

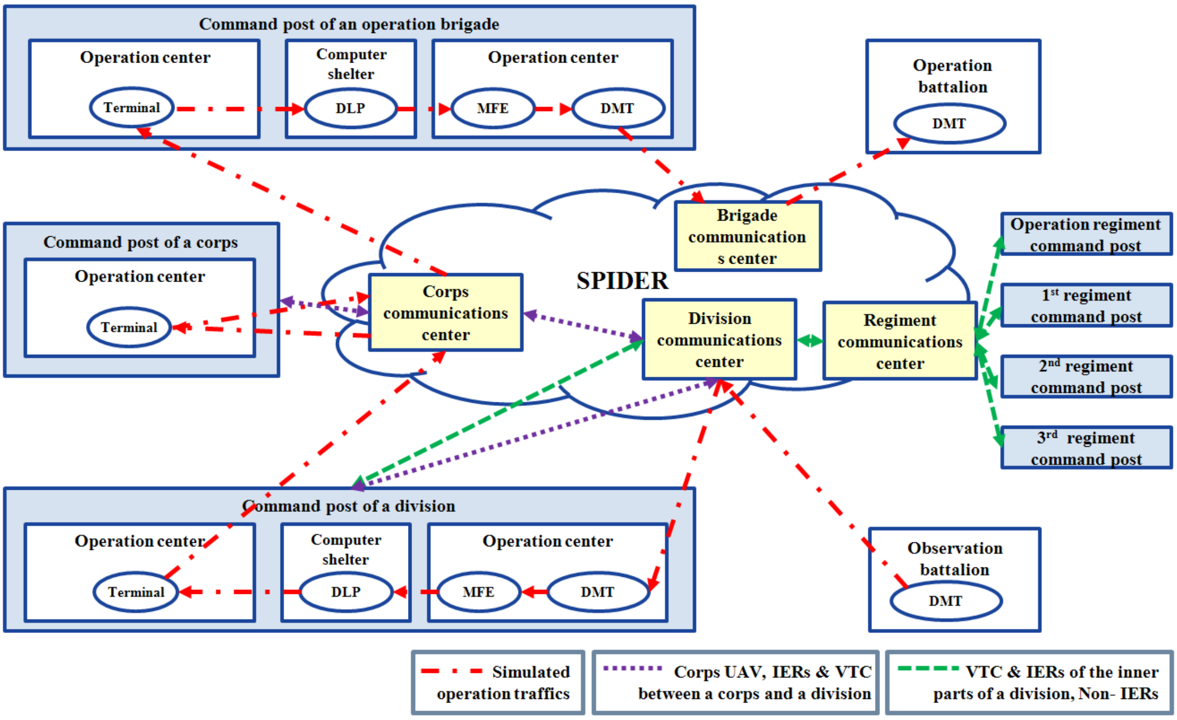

Figure 7. Simulated traffic flows for the analysis of information exchange capability

3.2 Analysis traffic modeling

For the analysis of information exchange capability, exchange traffics are generated based on four types of simulated traffic models. Table 3 describes traffic models that are set up in our analysis scenario for exchange traffics. In Table 3, sizes of traffic models are defined arbitrarily for our simulation and analysis.

Table 3. Definition of analysis traffic models

Types	Description		Size	Modeling method
Traffic for simulated operation	The system in the division transfers information to the system of the battalion under the corps.		600 bps	- IER & Thread modeling · generation period: constant (1) · generation size: constant
Traffic for UAV operation of the corps	main command post of the corps → main command post of the division		400 Kbps	- IP traffic flow modeling · generation period: exponential · generation size: exponential
Traffics for VTC	between the corps and the division	main command post of the corps → main command post of the division	300 Kbps	- Application modeling · standard application: VTC · frame generation characteristics: constant(0.2) · Tx frame: exponential(7500) · Rx frame: exponential(7500)
	the inner parts of the division	main command post of the division → command post of the regiment	300 Kbps	
Background traffics	IER between the corps and the division		80 Kbps	- Application demand modeling · generation period: constant · generation size: exponential (100)
	IER of the inner parts of the division		70 Kbps	
	Other Non-IERs		1200 Kbps	- Application demand modeling · generation period: constant · generation size: exponential (1500)

3.3 Analysis and consideration of simulation results

As main analysis results of our simulation, the end-to-end delay of the simulated operation traffic and the VTC traffic has been analyzed. As shown in Figure 8, the end-to-end delay of simulated operation messages was increased about ten times due to the introduction of new systems. It was because the communication link between the command post and the communications center of the division was saturated, as seen in Figure 9.

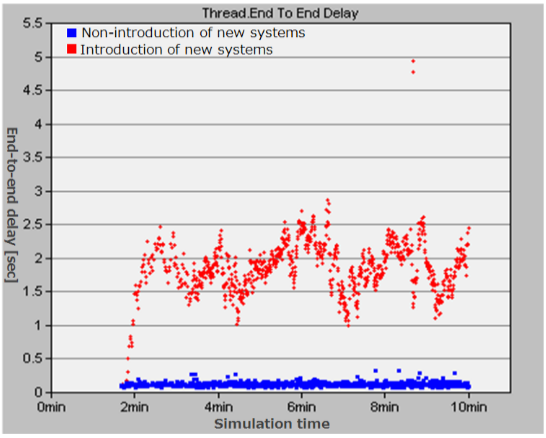

Figure 8. End-to-end delay of simulated operation messages

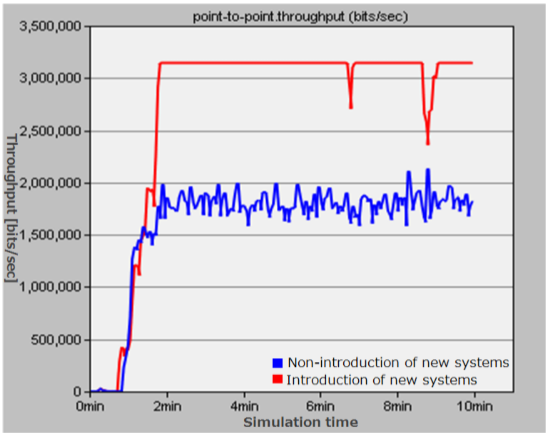

Figure 9. Throughput of the link between the command post and the communications center of a division

Next, Figure 10 and Figure 11 show end-to-end delays of VTC traffics according to the introduction of new systems. That is, the end-to-end delay of the VTC traffic was increased from about 80 milliseconds to about 800 milliseconds. In conclusion, considering these simulation results, the timeliness of information exchange for new systems is not able to be satisfied in the case that they are introduced in existing network of the battlefield.

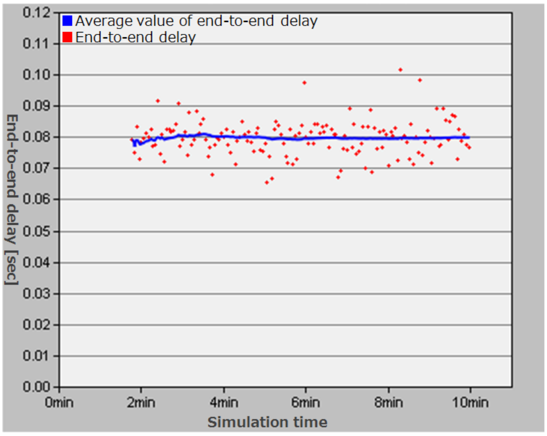

Figure 10. End-to-end delay of VTC traffics in case of the non-introduction of new systems

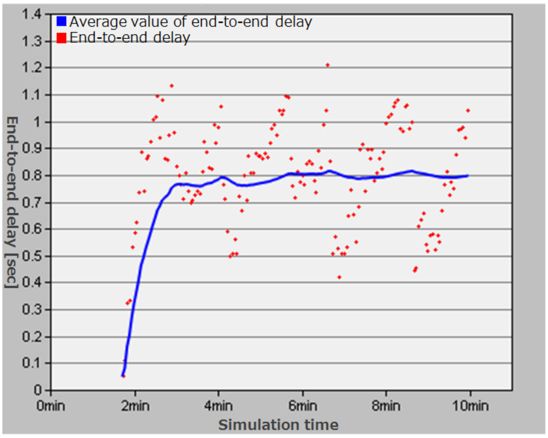

Figure 11. End-to-end delay of VTC traffics in case of the introduction of new systems

4. CONCLUSION

To analyze and evaluate the timeliness and the correctness of information exchange between elements of the battlefield considering effects of real communication environment of it, this paper has presented the modeling of military communications network of the NetSPIN that is able to analyze and evaluate the information exchange capability based on the battlefield communication environment that is simulated using network M&S.

Furthermore, in the situation that traffics of the SPIDER have been increased due to the introduction of new systems such as the UAV in a corps and the video conferencing system in a division, the end-to-end delay of simulated operation messages and the throughput of links have been analyzed. That is, the information exchange capability of existing communications network has been evaluated according to the introduction of the new system.

In conclusion, by analyzing effects of communications network due to the introduction of new systems beforehand utilizing the NetSPIN, causable problems were able to be analyzed and forecasted in advance. Therefore, the NetSPIN will be used effectively for analyzing the information exchange capability of the military and planning the communications network of it.

REFERENCES

[1] Joint Chiefs of Staff, "Interoperability application and evaluation guide", Republic of KOREA 2011. 1.

[2] Defense Information Systems Agency, "JCSS - Joint Communications Simulation System", [Online]. Available: http://www.disa.mil

[3] EADS Defense and Communications Systems, "NetCOS - Network Centric Operations Simulation", [Online]. Available: http://www.eads.net

[4] Sangil LEE, Sangheun SHIM, Myounggil AHN, Dongguk RYU, Jonghyun JIN, and Byoungin CHO, "Network M&S Techniques based on the Interworking of a Real System for the Interoperability T&E", Korea Military Science Technology Conference, 2010.

[5] Jaeyoung CHEON, Sangil LEE, and Byoungin CHO, "Introduction for Network Simulation and Planning for Interoperability Tool", Korea Military Science Technology Conference, 2009.

[6] OPNET Technologies, Inc. "Overview of OPNET Solutions for Network R&D", OPNET Works, Session 1006, 2008.

[7] Jaeyoung CHEON, Sangil LEE, and Byoungin CHO, "Software Design Description for NetSPIN SPIDER Model", Agency for Defense Development, 2011.5.

[8] Sangheun SHIM, Sangil LEE, and Byoungin CHO, "NetSPIN ATCIS Model Design Report", Agency for Defense Development, 2011.5.