Contribution ID: **4** Type: **not specified**

Fermilab Network Modeling & Simulation Efforts

Tuesday, September 11, 2012 2:48 PM (12 minutes)

We have two previous projects that are related to network modeling and simulation. In these projects, we used the modeling & simulation methodology to study and analyze network functions and performance.

(1) The Modeling Process and Analysis of Virtual GMPLS Optical Switching Routers

Generalized multi-protocol label switching (GMPLS) has emerged as a very promising protocol technology for the next generation optical networks. GMPLS successfully combines the best features of IP and optical networks in terms of quality of service (QoS), privacy, flexibility and scalability. GMPLS introduces enhancements to the existing IP routing and signaling protocols by supporting not only networks that perform packet switching (IP), but also networks that perform switching in the time (TDM), wavelength (DWDM), and space domain (circuit switching). This project designed and implemented a modeling tool for analysis of GMPLS optical switching routers (GOSR). A model of the GOSR has been built using OPNET modeling and simulation platform, in lieu of a prototype. The virtual model contains all the necessary GMPLS functions of an optical backbone router. The virtual model of the GOSR has the capability of giving a more integrated and realistic simulation on wavelength routing, wavelength assignment, wavelength switching, dynamic label switching path (LSP) setup and tear down, and blocking mechanism of GMPLS light paths. The OPNET process modeling methodology was used to develop the virtual GOSR models. The simulation results obtained include the blocking rate, OSPF-TE bandwidth analysis, and CPU utilization. The modeling environment developed in this project provides a simulation platform for further development and future enhancement of GMPLS protocols, routing protocols, and optical switching router implementations.

(2) Development of Modeling Cyber-attack Scenarios for JTRS IW Threat Analysis Using OPNET Modeler

The Joint Tactical Radio System (JTRS) program intends to develop a family of communications devices that support reliable multi-channel voice, data/imagery, and video communications for battlefield communications. The JTRS devices use Software Defined Radio (SDR) technology based on the Software Communications Architecture (SCA). Ultimately JTRS will extend the information infrastructure supporting Network-centric Warfare to the last "tactical" mile, enabling the warfighter to gain access to real-time information. Under the JTRS program the role of the radio changes from network "terminal" to network node. This role includes behaviors similar to a router in a packet-switched network based on Internet protocols. Therefore, these network nodes will be susceptible to the types of attacks generally referred to as "cyber-attacks" that generate information processing faults. In this project we investigated classes of cyber-attacks with respect to the feasibility of modeling attack behaviors in OPNET Modeler, as well as the development of an attack library. The purpose of the development was to validate and demonstrate the effectiveness of the JTRS mobile nodes under a wide range network attacks. We specifically developed generic models for ICMP-based Distributed Denial of Service (DDOS) and attacks oriented to MANET protocols. The design objectives were structured around a concept of a "fault insertion node" that can incorporate fault functionality based on pluggable "fault modules" with configurable interfaces. A fault insertion node is capable of generating the necessary communication fault insertion frames generated as a function of fault modules hosted within the node. Fault insertion node modules were developed with the Ethernet data link interface; IEEE 802.11b Ad-hoc interface; and a capability to incorporate other link interfaces.

Primary author: Dr WU, Wenji (Fermilab)

Co-author: DEMAR, Phil (Fermilab)

Presenter: Dr WU, Wenji (Fermilab)