Y9.ET1.3 Secure Communications for RSC/DGI Testbed

Jonathan Ng, Ming Yu

Overview

Background

- Improve the OPNET network simulator's scalability by connecting the OPNET simulator to a second OPNET simulator that runs in another machine

The performance of the Smart Grid depends greatly on the underlying network that supports the communications between the grid devices. Metrics such as link availability and latency need to be studied thoroughly before the Smart Grid is deployed in the real world to reduce the total cost and to reduce the damage when possible communications outages happen. OPNET is introduced to simulate various real world communications scenarios so as to improve the system reliability and to reduce losses in unexpected situations. As the scale of the simulated network increases, it also poses greater requirements for the simulation scalability for the OPNET system. Slower simulators can lead to packet dropping in a large scale simulation, which will lead to non-realistic simulation results. To lessen the impact of such negative situations, multiple simulators are introduced to divide to work load imposed on such scenarios.

- Develop the secure firmware updating mechanism for DGIs

Most of the communications the Smart Grid takes place on the TCP/IP based Internet. However, ever since its emergence, the Internet is not designed to guarantee the security and reliability as the most important privileges. On the other hand, without proper consideration of security and reliability, information can be eavesdropped and forged during transmission, which can lead to privacy leakage and malfunction of part or the whole Smart Grid system, if a forged control code block spreads to a wide area of the grids. The danger is especially noticeable when new firmware is updated to devices throughout the network to enhance their functions, to improve their performance, or to correct found bugs. Therefore, the requirements arise for a secure firmware update mechanism.

Method

- Scalable OPNET network

An additional simulation computer is connected to the existing one with the topology on the right.
A straight through patch cable connects the two simulator computers together on their Ethernet ports.
Routing tables are configured to forward network traffic from one computer to the other and vice versa.

mamba1 - mamba 6 routing table

Destination	Gateway	Genmask	Flags	Iface
192.168.170.0	*	255.255.255.0	U	eth0

netsim routing table

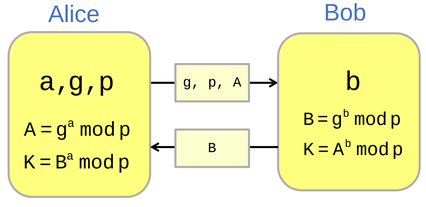
Destination	Gateway	Genmask	Flags	Iface
192.168.170.0	0.0.0.0	255.255.255.0	U	p2p3
192.168.170.0	0.0.0.0	255.255.255.0	U	p1p1
192.168.170.0	0.0.0.0	255.255.255.0	U	p1p2
192.168.170.0	0.0.0.0	255.255.255.0	U	p1p3

newsim routing table

Destination	Gateway	Genmask	Flags	Iface
192.168.170.0	0.0.0.0	255.255.255.0	U	p5p4
192.168.170.0	0.0.0.0	255.255.255.0	U	p6p1
192.168.170.0	0.0.0.0	255.255.255.0	U	p6p2
192.168.170.0	0.0.0.0	255.255.255.0	U	p6p3

- Secure DGI updating

Use the sftp protocol for DGI software delivery between the administration computer and the mambas, which prevents eavesdropping. The encryption strength of sftp can be up to triple DES and AES-256.
Combining an additional nonce to generate the SHA-256 checksum for the DGI to prevent any data corruption during transmission.



$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B \bmod p$

Diffie-Hellman key exchange is used to negotiate an ephemeral shared key between the client and the server for SSH/SFTP

Results

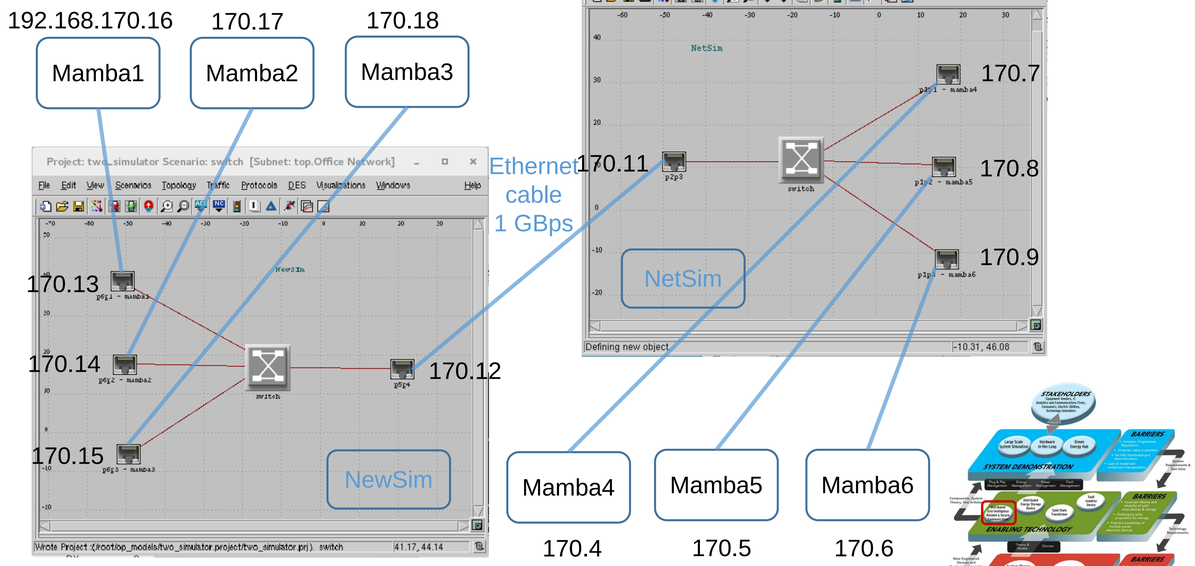


Fig. 1. Multiple OPNET simulators

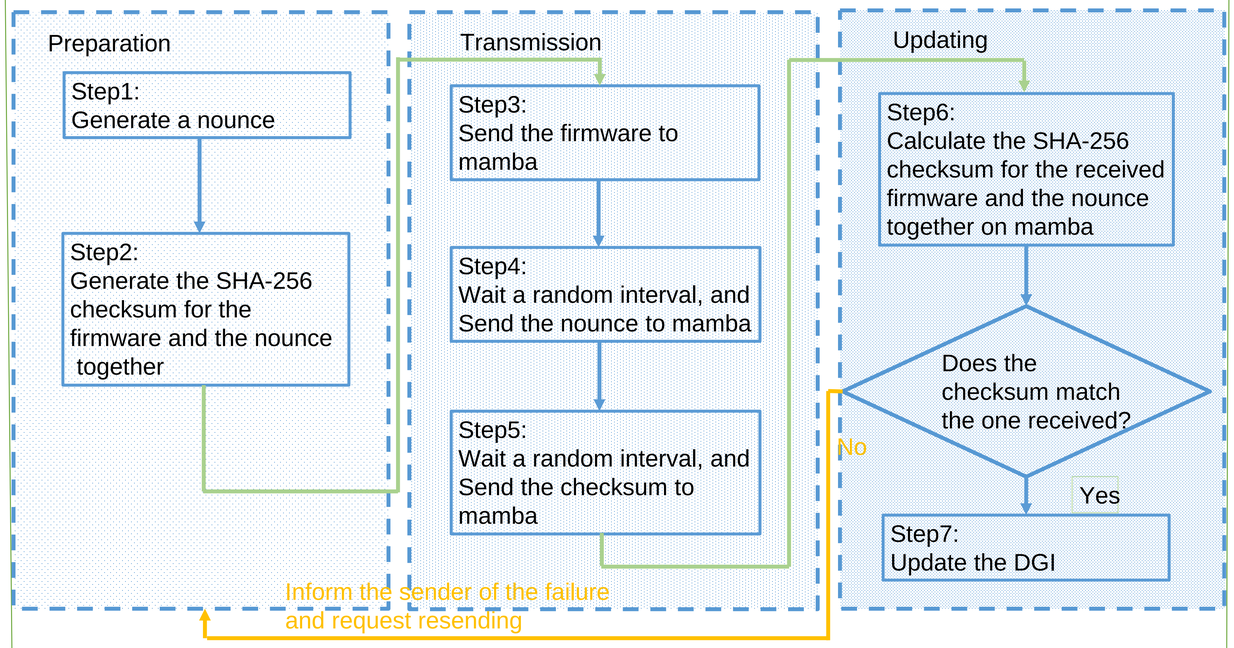


Fig. 2. Flowchart of DGI updating