Review of Dissertation Thesis
Network-Wide Security Analysis
submitted by Gayan Ruchika de Silva
at the Faculty of Information Technology, Brno University of Technology

The thesis has 163 pages (appendices and bibliography included) written in English and has been submitted in 2011.

Subject of the submitted thesis is network-wide security analysis and addresses service reachability, configurations, routing and security filters on dynamic networks in case of device or link failrules. Considering broadening of comupter networks, the subject of the theses is up to date and is a vital part of computer science without doubt.

Author gives two main objectives of the thesis namely to built an effective model for dynamic networks and develop analysis method to predict properties of the network. The first one is logically devided into modelling network topology and modelling device configurations including policy routing, tunneling and hidden paths. The second one aims at reachability, device configurations, routing, filtering and quality of service. Next, the model and the analysis should be embbeded into a simulation tool in order to provide the administrators to analyse the network not disturbing the running network.

State of the art is described in chapter 2, where also the overview of the terminology is given. Firstly, the research on modelling of networks is given including approaches for analyzing reachability, routing behaviours and filtering rules. Next, the related work on automation of the evaluation process of filtering rules is given.

In chapter 3, the proposed approach to network modelling is described. The network topology is converted to a digraph, where the vertices represent the forwarding devices and communications links and the abstract network graph is introduced. Next, the filtering network graph incorporating the device node model is defined.

The reachability analysis is described in chapter 4. Modified topology table containing all paths with costs, network states and path filters is introduced. Modified topology table is used as an input for the reachability analysis.

Chapter 5 introduces a constraint-based model for representation of device configurations and packet transformations. These are transformed to logical formulas and Prolog language is used for their modelling and analysis.

Routing analysis is described in chapter 6. The routing analysis is based on the device configurations and standard graph algorithms are used for the analysis. Applicability of the modified topology table introduced in chapter 3 for expressing the redistribution process between different Interior Gateway Protocol Network proved usefulness of this concept.

Chapter 7 deals with verification of firewall rule sets against the network security policy. Constructing logical formula for the set of rules leads to a SAT based method enhanced by including routing effects.

Finally, in chapter 8 the proposed methods are evaluated using three scenarios and in chapter 9 conclusion and suggestions for future work are given.

Without doubts, de Silva has done a lot of work and covered many issues of network-security analysis. The price for the broad scope of problems is that as mentioned in the end of chapters a lot of work is still to be done. Specifically, I have following questions:

How the parameters for the model from the network under operation will be gathered?

How the consistency of the network parameters will be achieved?

How the simulation scenarios were selected?

Were some experiments on real network performed?

The results of the thesis were published in one journal paper, four conferences and in one student conference. The thesis is well written and can be used as basis for future research. The work of de Silva significantly enhanced methods for network analysis.

I recommend the thesis for the defence.

Plzeň 16.1.2012

Prof. Ing. Jiří Šafařík, CSc.
Faculty of Applied Sciences
University of West Bohemia