Combination of Simulation and Formal Methods to Analyse Network Survivability

Petr Matoušek
Brno University of Technology
Bozetechova 2, 612 66 Brno
Czech Republic
matousp@fit.vubr.cz

Ondřej Ryšavý
Brno University of Technology
Bozetechova 2, 612 66 Brno
Czech Republic
rysavy@fit.vubr.cz

Gayan de Silva
Brno University of Technology
Bozetechova 2, 612 66 Brno
Czech Republic
xdesil00@fit.vubr.cz

Martin Danko
Brno University of Technology
Bozetechova 2, 612 66 Brno
Czech Republic
xdanko00@fit.vubr.cz

ABSTRACT

Modern computer networks are complex and their topology can dynamically change when links go down. It is difficult to predict behaviour of a large network with dynamic routing protocols. To automatically prove survivability and reliability of an end-to-end connection, formal analysis combined with simulation can be exploited. In this paper, an approach based on detection of critical elements using formal analysis and subsequent simulation of time related properties is introduced. Our network model is automatically extracted from configurations of network devices. Then, critical network elements are detected using graph search algorithms. After that, several simulation scenarios are executed over a model in order to detect time dependencies. Modelling and simulation is done in OMNeT++ simulator, formal analysis is computed using scripting. The first results of this combined analysis show feasibility of this approach and help to reveal both qualitative parameters (status of links and nodes), and quantitative parameters (timers, routing protocols) that influence reliability and survivability of the network. The approach is demonstrated on a simplified topology of Czech Academic Network (CESNET).

Keywords

formal analysis, dynamic networks, simulation, reliability

1. INTRODUCTION

Current network communication moves from a simple data exchange to integration of different services transmitting data, voice, and video. Design of scalable converged networks includes physical paths topology, bandwidth requirements, high-availability backup lines, security of valuable assets, etc. Network design is usually split to several OSI layers—a plan of link topology and L2 devices, L3 design with addressing and routing, security measures, network services and applications on higher levels. Having such complex network design with separated layers, it is difficult to analyze network behavior when changes occur.

There is a need for an a-priory analysis in order to detect bottlenecks of the design. Such analysis helps to design a reliable network with failure recovery. Failures can outcome of unstable wireless connection, temporarily overloaded links, or slow convergence of routing protocols. Failures on lower layers may affect higher layer services.

The goal of network administrators is to guarantee maximum service availability and survivability. The term *availability* means readiness for correct services [1], *survivability* refers to a system's capability to fulfill its mission in the presence of failures or accidents [9].

This paper focuses on semi-automatical analysis of a real network with dynamic routing in order to detect potential points of failure. Our approach is based on combination of formal methods and simulation. Using formal methods, obvious critical parts of the network are detected, marked and excluded from the further analysis. Then, a set of typical failure scenarios is simulated on the network and time related behaviour is examined.

Network topology with IP addresses, routing protocols and firewall rules is automatically extracted from configuration files of network devices. This XML description is then turned into formal model for formal analysis and into the simulation model in OMNeT++ specification [8], see Figure 1. Using formal analysis, two sets of network elements are computed—critical points and universal points. Critical points specify links and nodes whose failure always prevent service availability. Universal points define links and nodes whose failure has no effect on service availability. Both sets are independent on routing protocols.

Simulation analyzes network elements that are neither of the two sets. In addition, time parameters like delays between consequent failures or convergence delay, is examined. Using combination of both approaches more precise model of network survivability can be obtained.

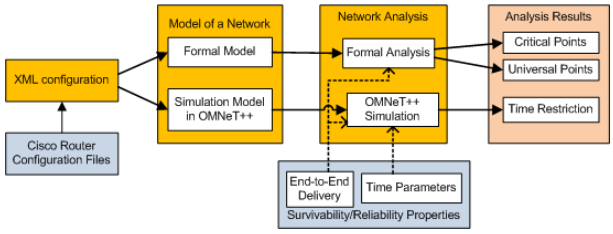

Figure 1: Structure of the Analysis

1.1 Motivation

Many current networks use dynamic routing protocols to find the best path through changing topology. When network topology changes due to link or device failure, new paths can have different bandwidth and delay parameters comparing to the original ones. Further, different security restrictions may block original traffic over a rerouted path.

Our goal is to develop an automated tool that will read the actual network configuration (e.g., configuration files of routers and switches on the network) and convert it into an analytical and simulation model. Upon the models, the reachability analysis will be done in order to prove survivability of end-to-end connections under network topology changes. Using this tool, important Service Level Agreement (SLA) parameters (bandwidth, delay, loss) will be checked using a combination of formal verification and simulation scenarios. In this paper, we show our preliminary results and steps for future work.

1.2 Structure of the paper

The paper is structured into four main parts. The first part gives an overview of the state of the art in the area of network analysis and presents our motivation for the research. The second part shows how to build simulation model based on configuration files of network device. The third section describes formal analysis approach that is used to detect critical elements of the network. The fourth section deals with simulation and describes analysis of convergence delay on the case study. Our results are summarized in the last parts, where future work is discussed.

1.3 State of the Art

The issue of reliability and survivability of computer networks has been discussed since the birth of the Internet. There are several works that try to classify network survivability components. In [13], taxonomy based on physical and logical survivability is proposed. The authors cite tens of research papers dealing with different layers or parts of networking. Their work mostly present heuristic solutions. In his dissertation [6], R. Mortier describes important issues related to traffic engineering (including reliability) and builds simulation models of networks using network simulator NS2 [15]. Analysis and simulation of IGP routing protocols using OPNET simulator is presented in [17]. Many of these approaches are demonstrated on small networks and observe a few routing properties. There are also works dealing with formal modeling and analysis of dynamic networks. In [16], Geoffrey G. Xie et al. show how dynamic routing information can be added to the static model with filtering rules. Their approach was extended by our previous work [5, 2]. In this paper, we introduce the combination of formal analysis and simulation over an abstract model that is automatically extracted from a real network configuration.

1.4 Contribution

Contribution of the paper includes (i) extension of formal analysis for network reliability. Unlike [5], no need to precompute routing tables for all states of the topology is required. In addition to [4], this paper introduces (ii) notion of *criticalness* as an important property related to survivability and shows how to use it to detect possible weaknesses in the topology. Another contribution of this paper is (iii) simulation approach applied to the results of formal analysis. We implemented an improved model of router and models of routing protocols for simulation tool OMNeT++[1] and (iv) created a tool that automatically translates Cisco configuration files into OMNeT++ models. Using simulation, we can observe network survivability when links go down and up. Our approach is (v) demonstrated on the topology of Czech Academic Network (CESNET).

2. BUILDING MODELS UPON CONFIGURATION FILES

The first step that precedes network analysis consists of a model definition. The model can be either generated from an existing network configuration or developed by a network designer according to the expected network behaviour.

We developed a tool that can automatize model generation. It reads configuration files of network devices and produces a vendor neutral configuration represented in XML format. Currently, the tool understands Cisco configuration files, but it is not difficult to extend it to accept other formats. The intermediate XML representation of the network model is then used as an input for analytical tools or simulator OMNeT++ [11]. This tool also generates network description file (NED) that shorten the time needed to set up the simulation model.

The example of the translation is shown bellow. A fast Ethernet interface of router R1 has specified IP address and bandwidth. Other configuration is default.

```
interface FastEthernet0/0
  ip address 192.168.1.1 255.255.255.0
  bandwidth 64
!
```

The corresponding XML representation includes name of the interface and link speed (100 Mbps) derived from the type of the interface (FastEthernet). Explicit definition of default options (e.g., Duplex) is necessary to produce vendor and IOS version independent XML intermediate configuration.

```
<Interface name="eth0">
  <IPAddress>192.168.1.1</IPAddress>
  <Mask>255.255.255.0</Mask>
  <Duplex>auto</Duplex>
  <Speed>100</Speed>
  <Bandwidth>64</Bandwidth>
</Interface>
```

The simulation model consists of XML representation and the NED file that describes the network topology. The NED

[1]see http://www.omnetpp.org

file can be generated from the XML file considering IP addresses to be consistent. Our improved implementation of the OMNeT++ router is able to download its configuration directly from XML configuration file. An XPath pointer connects the relevant XML subsection with the given router. For instance, to set up interface `eth0` on router `R1` using global XML configuration file, the following XPath pointer is used:

```
/Routers/Router[@id="R1"]/Interfaces/Interface[@id="eth0"]
```

The new simulation module of a router [12] integrates OSPF and RIP routing processes with packet filtering using ACLs. The router is built on the top of `OSPFRouter` module available in INET Framework of OMNeT++ tool. Additionally, it contains methods allowing to instrument the simulation with new events like interface or router failure. It is expected to extend the router simulation model with a cost model and advanced features, e.g. policy based routing.

3. DETECTING CRITICAL ELEMENTS

This section describes formal approach to the analysis. The used approach is based on detection of two sets of network devices–critical points (CP) and universal points (UP) on the connection between two end points. Because of link redundancy, there can be several physical paths forming connection between end points. We will demonstrate how UPs and CPs can be used for survivability and reliability analysis of the network. The critical points are routers and links that are always present on every path between end points. If any of them fails no connection is available. Universal points are routers and links that are not used for data transmission between analyzed end points in any case. They are not part of any possible path.

Definition 1. Let R be a set of network devices, L be a set of links, π^k is a k^{th} path between source and destination, $C(l)$ be a cost function over link l such that cost of the path is the total cost of each link along the path, and P be a set of paths evaluated by cost function. *Critical Points (CP)* is a subset of routers and links which are present along every possible path between the end points. $CP = \{R^c, L^c\}$ where $R^c = \{r|\forall\pi \in P : r \in \pi\}$ represents critical nodes and $L^c = \{l \mid \forall\pi \in P : l \in \pi\}$ represents critical links. *Universal Points (UP)* is a subset of routers and links which are not present along any available path, that is $UP = \{R^u, L^u\}$, where $R^c = \{r|\forall\pi \in P : r \notin \pi\}$ represents universal nodes, and $L^c = \{l|\forall\pi \in P : l \notin \pi\}$ represents universal links.

The UP set can also be defined using complementary sets R' and L'. Let R' and L' be sets such that $R' = \{r \mid \exists\pi \in P : r \in \pi\}$, and $L' = \{l \mid \exists\pi \in P : l \in \pi\}$. The universal devices and links build complement sets to R', resp., L', i.e., $R^u = R - R'$, resp. and $L^u = L - L'$.

3.1 Formal Model of the Network

We assume the network is correctly configured for OSPF routing. The relation between the cost function $C(l)$ and the bandwidth $BW(l)$ for OSPF is given by formula $C(l) = [10^7/BW(l)]$ [7]. Formal specification of our network model can be applied for static routing, RIP, or EIGRP with different cost functions. Static routing is considered as a special dynamic routing protocol which has the highest priority over

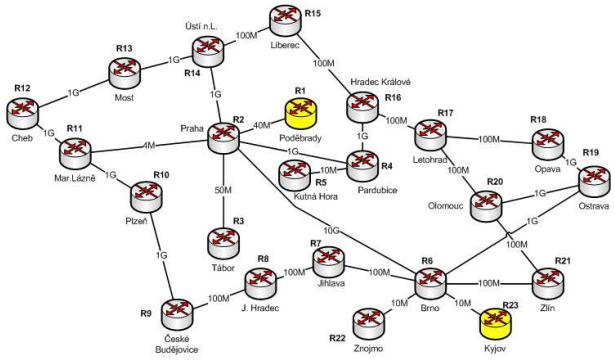

Figure 2: Modelling Network CESNET

network and omits all other physical links from that device to the end point. The same approach can be extended to BGP by treating one AS as a single device and computing a different cost function.

A formal model of CESNET topology as shown in Fig. 2 is composed of routers and links evaluated by cost functions for OSPF, see Table 1.

Device R_i	NextHop R_j	BW (Mbps) $BW(l_{ij})$	Cost $C(l_{ij})$
R1	R2	40	0.25
R2	R3	50	0.2
R2	R4	1000	0.01
R2	R6	10000	0
R2	R11	4	2.5
R2	R14	1000	0.01
R4	R5	10	1
R4	R16	1000	0.01
...	...	...	...
R18	R19	1000	0.01
R19	R20	1000	0.01
R20	R21	100	0.1

Table 1: Cost Function for CESNET Network

3.2 Reachability Analysis

Verification of reachability property is used to analyse survivability of network connections. Dynamic routing protocol searches for the best available path for data transfer. Since routing protocols cannot establish a virtual path without a physical connection, the methods based on computation of routing tables and consequent analysis of the best path for every combination of links state (up and down) as proposed in [5] and [16] is inefficient and unfeasible for larger networks. Here, all available physical paths are examined and the best path is selected using the cost function.

Current network state is described by states of links and routers. In a single failure model, we consider that a link

No. k	Path Cost $C(\pi^k)$	Path π^k
1	1.25	$R_{23}, l_{23,6}, R_6, l_{6,2}, R_2, l_{2,1}, R_1$
2	11.57	$R_{23}, l_{23,6}, R_6, l_{6,7}, R_7, l_{7,8}, R_8, l_{8,9}, R_9, l_{9,10}, R_{10}, l_{10,11}, R_{11}, l_{11,2}, R_2, l_{2,1}, R_1$
3	1.61	$R_{23}, l_{23,6}, R_6, l_{6,7}, R_7, l_{7,8}, R_8, l_{8,9}, R_9, l_{9,10}, R_{10}, l_{10,11}, R_{11}, l_{11,12}, R_{12}, l_{12,13}, R_{13}, l_{13,14}, R_{14}, l_{14,2}, R_2, l_{2,1}, R_1$
4	1.81	$R_{23}, l_{23,6}, R_6, l_{6,7}, R_7, l_{7,8}, R_8, l_{8,9}, R_9, l_{9,10}, R_{10}, l_{10,11}, R_{11}, l_{11,12}, R_{12}, l_{12,13}, R_{13}, l_{13,14}, R_{14}, l_{14,15}, R_{15}, l_{15,16}, R_{16}, l_{16,4}, R_4, l_{4,2}, R_2, l_{2,1}, R_1$
5	1.58	$R_{23}, l_{23,6}, R_6, l_{6,19}, R_{19}, l_{19,18}, R_{18}, l_{18,17}, R_{17}, l_{17,16}, R_{16}, l_{16,4}, R_4, l_{4,2}, R_2, l_{2,1}, R_1$
...	...	...
16	11.91	$R_{23}, l_{23,6}, R_6, l_{6,21}, R_{21}, l_{21,20}, R_{20}, l_{20,19}, R_{19}, l_{19,18}, R_{18}, l_{18,17}, R_{17}, l_{17,16}, R_{16}, l_{16,15}, R_{15}, l_{15,14}, R_{14}, l_{14,13}, R_{13}, l_{13,12}, R_{12}, l_{12,11}, R_{11}, l_{11,2}, R_2, l_{2,1}, R_1$

Table 2: Computing paths π^k between R_{23} and R_1

can be either up or down, or device can be either functioning or broken. We define a set of failed devices and links, R^f and L^f, respectively. There are three general cases:

1. If $\exists r \in R^f$ such that $r \in R^c$ or $\exists l \in L^f$ such that $l \in L^c$, then destination is always unreachable.

2. If $R^f \subseteq R^u$ and $L^f \subseteq L^u$, then network survives and the path with the best cost $C(\pi^k)$ is used.

3. Otherwise, from Table 2 select all paths $\pi^k \in P$ such that $\forall r \in R^f, \forall l \in L^f : (r,l) \notin \pi^k$. Then, the best path is $\pi = \{\pi^k \in P | \ \forall r \in R^f, \forall l \in L^f, \forall i \in < 0, n >: r \notin \pi^k \wedge l \notin \pi^k \wedge C(\pi^k) \leq C(\pi^i)\}$.

First two limiting cases are easy to find. The most interesting is the third case, which suggests further analysis using the simulation technique or refinement considering routing models as in [5].

To demonstrate the approach, we analyze the communication path between source $R23$ and destination $R1$, see Fig. 3. Table 2 shows all available physical path with their costs. When all devices and links are up, the path used to communicate from R_{23} to R_1 is the least cost path ($k = 1$). The computation of CP and UP gives following results:

$$\mathbf{CP} = \{R_1, R_2, R_6, R_{23}, l_{1,2}, l_{6,23}\}$$

$$\mathbf{UP} = \{R_3, R_5, R_{22}, l_{2,3}, l_{4,5}, l_{6,22}\}$$

This approach gives the first approximation that may be further analyzed in detail [4]. The cost function is used to select the best path among all available physical paths. Such best path corresponds to the path determined by dynamic routing protocols.

The result of analysis can determine *criticalness* of a given device or link. Criticalness is a property that describes how many paths exploit the device as primary connection. Higher number of paths is, higher the value of criticalness appears. This is very useful for network administrators to detect first-level and second-level critical devices on the network and implement high-available redundancy to provide better reliability. Criticalness can be computed as a percentage of a number of paths over which devices appear to the total number of paths. For example, consider $_{R16}$ having criticalness of $(13/16) * 100 = 81.25$. This implies its importance in case of failure. Buy a single failure that device can be a part of newly computed CP. Analysis of criticalness performed over our simplified model of Czech Academy Network CESNET is depicted in Fig. 3.

4. ANALYZING CONVERGENCE DELAYS USING OMNET++

While formal analysis reveals rather qualitative aspect of the network, simulation provides quantitative information on the network's dynamics. There are several simulation scenarios that can provide information on the specific properties of the network. As we are interested in the impact of dynamic routing on the quality of the specific traffic we focus on measuring packet delay and packet loss under different network conditions. To clarify contribution of routing process mechanisms we can also measure convergence time required to reach a stable state by routing protocols employed.

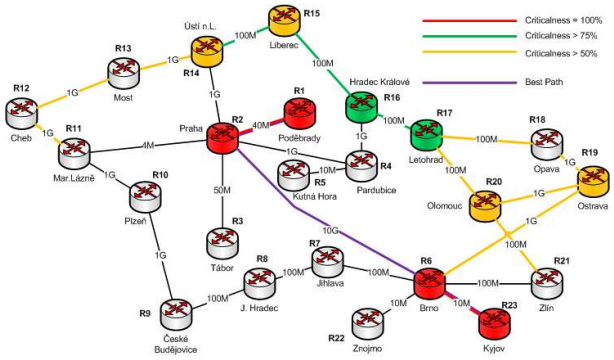

Figure 3: Network CESNET with critical links

We chose OMNeT++ as the simulation environment for our exercises on combination of formal methods and simulation techniques. Simulation model for OMNeT++ was automatically extracted from XML configuration of real network devices. Our translating tool is able to setup all devices and links, provide initialization information, and run simulation scenarios. To accomplish this task, new modules to INET Framework were developed: a module for general router, a module for advanced OSPF routing, a module for RIP routing with redistribution, and a model for filtering using Cisco Access Control Lists (ACLs). Following simulation experiment demonstrates our approach and give data that may be further analysed.

We are aware of the limited scope of the simulation experiment presented in this section. It serves only to demonstration purposes showing the nature of the technique being developed and is restricted only to three selected scenarios out of many possible. To gain the full power of the simulation approach we are developing a method for automatic designing and executing simulation scenarios according to the defined parameters, which come from user suggestions and formal method findings.

The simulation scenarios are managed in a common environment that provides the basic settings, such as network topology, device configuration, definition of interesting traffic, and basic simulaton parameters. Each scenario consists of a different sequence of intervention actions, which change the network considitions. In the simplest case as presented in this section, an intervention consists of alternating link states.

4.1 Setting Simulation Environment

An example of simulation environment captures 600 seconds of data communication within the network. The interesting traffic is defined to be a sequence of non-reliable packets of two sizes 200 bytes and 60 bytes sent every 20 ms. These flows correspond to voice streams encoded by G.711 and G.729 standards, respectively.

The OSPF routing protocol was configured on all routers in the network from Fig. 2. The routers belong to the same area. To approximate real network conditions, the link error model was employed. The error model can simulate not only link errors, but can also mimic packet loss because of buffer overflow problems. We are aware that our simulation environment is far from real conditions, but to demonstrate our approach it seems to be sufficient. To increase the precision of the results the simulation model should capture other

parameters that can significantly influence the transmission delay and packet loss.

4.2 Simulation Scenarios

We describe only three different scenarios. Each scenario is defined as a sequence of events in time that corresponds to link failures—a link goes from up state to down state and vice versa. In each scenario all links are also parameterized with packet loss ratio. These values are equal for all links and constant during the whole simulation. In our example, the best path between R_{23} and R_1 includes link $l(R_2, R_6)$. Simulation scenarios consider varying state of this link in different times. We run the simulation many times with randomized simulation parameters to get results in the form of mean values. It is our intention to develop a systematic method for synthesizing scenarios for user given inputs to scale the method. At the moment we need to generate scenarios manually that prevents us to setup larger experiments providing complex outputs.

The formal method proposed in previous sections helps to reduce the number of interesting scenarios by eliminating those that do not affect the path used by the interesting traffic. It is done by classifying nodes and links of the network to those affecting the transmission and those that have no significant contribution to delivery of interesting data.

Our simulation is focused on analysis of service reliability as expressed by number of lost packets and network survivability that is measured using convergence time of routing protocol. Simulation was run in simulation tool OMNeT++ (version 4). The scenario definitions and results are shown in Table 3.

4.3 First Approach Results and Discussion

As expected the OSPF is a robust protocol that for default parameters quickly finds an alternate path in the network causing little or no service disruption. Difficulties emerge if we consider significant packet loss, which leads to OSPF instability.

1. Convergence time in OSPF network is very small. Although the simulation does not include CPU time on routers needed to re-calculate an SPF tree the results specify the amount of time required to disseminate updates to all network OSPF nodes. To refine the results the computation model of router needs to be considered. The OSPF simulation does not include SPF delay, which is a standard mechanism in most real devices to prevent excessive SPF calculation.

2. With small link packet loss rate (less than 10%), there is not observed significant convergence delay to the loss-less case. The convergence delay was in between 0.3–0.7 ms. It is because that in case of loss of an update packet another update packet with the same information comes from the different neighbor. In this cases, packets are lost mostly due to error rate on the link. If the link error rate is higher (10%+) the update packets get lost more often from all neighbors and the convergence time is prolonged, which results in a situation that the network was unable to reach convergence state between two consecutive events.

3. Ratio of lost data packets depends naturally on the link error rate. In case of dynamic routing this ratio depends also on the actual path used to deliver such traffic. Considering the network from running example, the shortest path consists of three links. If each link has error rate 2% than the overall path lost rate is roughly 6%. However in case of link failures the data can travel using different paths with overall bigger error rate.

The present experiment aims at showing the impact of link dynamic parameters on performance of OSPF routing protocol and the overall network behavior. We present only limited amount of results that may be obtained from this class of experiments. More results can be found in [3]. The further work is oriented to provide more accurate models of links dynamics. We will also include data communication patterns based on real network load to a link description, and will automate the simulation scenarios design and result analysis.

We also conducted the same experiments with routing protocol RIP [10]. The RIP implementation conformes to RFC1058, which contains basic specification without any extensions such as triggered updates, split horizon with poison reverse, etc. This contributes to the convergence issues of the simulated network. In some case the network with RIP was unable to reach the stable state between the changes specified by the scenarios. It is because link changes occur more often than the periodic updates are issued. By repeating the experiments with randomized divergence of event occurrence time to periodic update time, it is possible to obtain mean convergence time and corresponding mean packet loss. However, it is not possible to guarantee the convergence.

5. CONCLUSION

In the present paper, we unveil some issues related to automated analysis of dynamic networks. The case study of larger network and an approach based on combination of formal analysis that points out the interesting places in the network and consecutive simulation that aims at providing more refined view on the problem were presented. The idea behind seems right placed since the full scale simulation in order to obtain the precise model of network behavior is impossible because of time and size complexity. The formal method and static analysis can identify problematic network components from the qualitative viewpoint. For these particular components the simulation can provide missing quantitative data. The present simulation experiments were focused only on few metrics out of many that can be explored. We believe that the other quantitative properties can be extracted without significant changes of the simulation model.

5.1 Future work

The intensive research needs to be done to fill in all the necessary technical details that have not been addressed yet. In the current state, we defined the overall idea of the work and implemented some supporting tools and models. To fulfill the objective of the project, the future research should be oriented to:

- Automatize the process of simulation scenarios definitions and result presentation. The tool that would generate and govern the execution of simulation scenarios according to the specified properties helps to obtain

Scenario definitions

Scenario 1	$\downarrow(R_2, R_6)$	$\downarrow(R_{16}, R_{17})$	$\uparrow(R_{16}, R_{17})$	$\downarrow(R_{16}, R_{17})$	$\uparrow(R_{16}, R_{17})$	$\downarrow(R_{16}, R_{17})$	$\uparrow(R_{16}, R_{17})$	$\uparrow(R_2, R_6)$
Scenario 2	$\downarrow(R_2, R_6)$	$\downarrow(R_{16}, R_{17})$	$\downarrow(R_{13}, R_{14})$	$\uparrow(R_{16}, R_{17})$	$\uparrow(R_{13}, R_{14})$	$\uparrow(R_2, R_6)$	$\downarrow(R_2, R_6)$	$\uparrow(R_2, R_6)$
Scenario 3	$\downarrow(R_{16}, R_{17})$	$\downarrow(R_2, R_6)$	$\uparrow(R_{16}, R_{17})$	$\downarrow(R_{16}, R_{17})$	$\uparrow(R_2, R_6)$	$\uparrow(R_{16}, R_{17})$	$\downarrow(R_2, R_6)$	$\uparrow(R_2, R_6)$

Total number of packet loss

Error Rate	Scenario 1	Scenario 2	Scenario 3
0%	0	0	0
2%	5311	4806	4059
5%	11466	10628	8895
10%	24941	28554	27462

Total convergence delay [ms]

Error Rate	Scenario 1	Scenario 2	Scenario 3
0%	0.364	0.351	0.402
2%	0.561	0.353	0.425
5%	0.429	0.448	0.697
10%	-	-	-

Table 3: Scenario definitions and meassured values

valid simulation results for further analysis. Without that the manual setting of simulations is very time consuming.

- Refine the simulation models to provide more accurate results. Currently, the simulation environment contains basic models of networking components that in many cases lack some important properties.

- Extend the formal analysis phase with more advanced techniques able to determine network components according to various qualitative parameters. The presented formal method is able to find out points in the network that are crucial for the data transmission. However, the potential of formal methods is much larger and it should be adequately exploited.

- Collect information on typical network design issues and identify key properties and network design patterns. The importance of adequate support during network planning and design is evident and was observed by industrial leaders [14]. The automated tools that would assist the designer must be customized such that they provide relevant information and techniques to accomplish the required tasks. To support this, we aim at studying the typical issues and their solutions to fit the tools to these needs.

6. ADDITIONAL AUTHORS

Simulation results are also based on work done by Veronika Rybová (RIP simulation), Peter Scherfel (configuration reading), and Vladimír Sivák (router model), students of Brno University of Technology. Authors also appreciate important contribution by Martin Tlolka (EIGRP modeling) and Tomáš Suchomel (ACLs) in OMNeT++ module extension.

7. ACKNOWLEDGMENTS

The research is supported by the Czech Ministry of Education in frame of the Research Intention MSM 0021630528: Security-Oriented Research in Information Technology and by ESF project CZ.1.07/2.3.00/09.0067 "TeamIT—Building Competitive Research Teams in IT".

8. REFERENCES

[1] A. Avižienis, J.-C. Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 1:11–33, 2004.

[2] R. Cejka, P. Matoušek, J. Ráb, O. Ryšavý, and M. Švéda. A formal approach to network security analysis. Technical report, 2008.

[3] M. Danko. Modelling ospf routing protocol using omnet++ simulator. Bachelor's thesis, Brno University of Technology, 2009.

[4] G. de Silva. Using formal analysis approach on networks with dynamic behaviors. In *5th EEICT student conference*, volume 4, pages 390–394, April 2009.

[5] P. Matoušek, J. Ráb, O. Ryšavý, and M. Švéda. A formal model for network-wide security analysis. In *15th IEEE Symposium and Workshop on ECBS*, 2008.

[6] R. Mortiere. Internet traffic engineering. Technical Report UCAM-CL-TR-532, University of Cambridge, 2002.

[7] J. Moy. *OSPF Version 2*. RFC 2328, April 1998.

[8] Omnest Global, Inc. OMNeT++ *User Manual*, 2008. http:// www.omnetpp.org/doc/manual/usman.html.

[9] R.J.Ellison, D. Fisher, R.C.Linger, H.F.Lipson, T.Longstaff, and N.R.Mead. Survivable network systems: An emerging discipline. Technical Report CMU/SEI-97-TR-013, Carnegie Mellon University, 1997.

[10] V. Rybová. Modelling and simulation of network design guides for ip routing. Bachelor's thesis, Brno University of Technology, 2009.

[11] P. Scherfel. Simulation of network behaviour based on analysis of configuration of active network devices. Bachelor's thesis, Brno University of Technology, 2009.

[12] V. Sivák. Modelling cisco router in simulation tool omnet++. Bachelor's thesis, Brno University of Technology, 2009.

[13] S. Soni, R. Gupta, and H. Pirkul. Survivable network design: The state of the art. *Information Systems Frontiers*, 1(3):303–315, 1999.

[14] C. Systems. Cisco validated design program. `http://www.cisco.com/en/US/netsol/ns741/networking_solutions_program_home.html`.

[15] The VINT Project. *The* ns *Manual*, Last checked: 02-01-2010. http://www.isi.edu/nsnam/ns/doc/.

[16] G. Xie, J. Zhan, D. Maltz, H. Zhang, A. Greenberg, G. Hjalmtysson, and J. Rexford. On static reachability analysis of ip networks. In *INFOCOM*, pages 2170–2183, 2005.

[17] A. Zaballos and C. Seguí. Analysis and simulation of igp routing protocols. Technical report, University of Ramon Llull, Barcelona, 2006.