VILNIUS GEDIMINAS TECHNICAL UNIVERSITY

Rytis RAINYS

INVESTIGATION OF THE REGIONAL INTERNET NETWORK INFRASTRUCTURE DEPENDABILITY

SUMMARY OF DOCTORAL DISSERTATION

TECHNOLOGICAL SCIENCES,
ELECTRICAL AND ELECTRONIC ENGINEERING (01T)

VGTU
LEIDYKLA
Vilnius TECHNIKA 2011

Doctoral dissertation was prepared at Vilnius Gediminas Technical University in 2007–2011.
Scientific Supervisor
Prof Dr Habil Algimantas KAJACKAS (Vilnius Gediminas Technical University, Technological Sciences, Electrical and Electronic Engineering – 01T).
The dissertation is being defended at the Council of Scientific Field of Electrical and Electronic Engineering at Vilnius Gediminas Technical University:
Chairman
Prof Dr Dalius NAVAKAUSKAS (Vilnius Gediminas Technical University, Technological Sciences, Electrical and Electronic Engineering – 01T).
Members:
Prof Dr Habil Antanas ČENYS (Vilnius Gediminas Technical University, Technological Sciences, Informatics Engineering – 07T),
Prof Dr Habil Gintautas DZEMYDA (Vilnius University, Technological Sciences, Electrical and Electronic Engineering – 01T),
Prof Dr Habil Romanas MARTAVIČIUS (Vilnius Gediminas Technical University, Technological Sciences, Electrical and Electronic Engineering – 01T),
Assoc Dr Jonas RIMAS (Kaunas University of Technology, Technological Sciences, Informatics Engineering – 07T).
Opponents:
Assoc Prof Dr Šarūnas PAULIKAS (Vilnius Gediminas Technical University, Technological Sciences, Electrical and Electronic Engineering – 01T),
Prof Dr Habil Rimantas ŠEINAUSKAS (Kaunas University of Technology, Technological Sciences, Informatics Engineering – 07T).

The dissertation will be defended at the public meeting of the Council of Scientific Field of Electrical and Electronic Engineering in the Senate Hall of Vilnius Gediminas Technical University at 10 a. m. on 12 of December 2011.
Address: Saulėtekio al. 11, LT-10223 Vilnius, Lithuania.
Tel.: +370 5 274 4952; fax +370 5 270 0112. e-mail: doktor@vgtu.lt
The summary of the doctoral dissertation was distributed on 11 of November 2011.
A copy of the doctoral dissertation is available for review at the Library of Vilnius Gediminas Technical University (Saulėtekio al. 14, Vilnius, Lithuania).
© Rytis Rainys, 2011

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Rytis RAINYS

REGIONŲ INTERNETO TINKLO INFRASTRUKTŪROS PATIKIMUMO TYRIMAI

DAKTARO DISERTACIJOS SANTRAUKA

TECHNOLOGIJOS MOKSLAI,
ELEKTROS IR ELEKTRONIKOS INŽINERIJA (01T)

VGTU
LEIDYKLA
Vilnius TECHNIKA 2011

Disertacija rengta 2007–2011 metais Vilniaus Gedimino technikos universitete.
Mokslinis vadovas

prof. habil. dr. Algimantas KAJACKAS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, elektros ir elektronikos inžinerija – 01T).

Disertacija ginama Vilniaus Gedimino technikos universiteto Elektros ir elektronikos inžinerijos mokslo krypties taryboje:

Pirmininkas

prof. dr. Dalius NAVAKAUSKAS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, elektros ir elektronikos inžinerija – 01T).

Nariai:

prof. habil. dr. Antanas ČENYS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, informatikos inžinerija – 07T),

prof. habil. dr. Gintautas DZEMYDA (Vilniaus universitetas, technologijos mokslai, elektros ir elektronikos inžinerija – 01T),

prof. habil. dr. Romanas MARTAVIČIUS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, elektros ir elektronikos inžinerija – 01T),

doc. dr. Jonas RIMAS (Kauno technologijos universitetas, technologijos mokslai, informatikos inžinerija – 07T).

Oponentai:

doc. dr. Šarūnas PAULIKAS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, elektros ir elektronikos inžinerija – 01T),

prof. habil. dr. Rimantas ŠEINAUSKAS (Kauno technologijos universitetas, technologijos mokslai, informatikos inžinerija – 07T).

Disertacija bus ginama viešame Elektros ir elektronikos inžinerijos mokslo krypties tarybos posėdyje 2011 m. gruodžio 12 d. 10 val. Vilniaus Gedimino technikos universiteto senato posėdžių salėje.

Adresas: Saulėtekio al. 11, LT-10223 Vilnius, Lietuva.

Tel.: (8 5) 274 4952; (8 5) 274 4956; faksas (8 5) 270 0112.

el. paštas doktor@vgtu.lt

Disertacijos santrauka išsiuntinėta 2011 m. lapkričio 11 d.

Disertaciją galima peržiūrėti Vilniaus Gedimino technikos universiteto bibliotekoje (Saulėtekio al. 14, LT-10223 Vilnius, Lietuva).

VGTU leidyklos „Technika“ 1927-M mokslo literatūros knyga.

© Rytis Rainys, 2011

Introduction

Scope of the problem. Information and communication technologies (ICT) are a significant tool for development of innovation and the social and economic wellbeing of a country. The ICT and specifically Internet innovations are widely utilized in e. business, e. banking, e. governance services, etc. The Internet network becomes a national infrastructure of utmost importance. Therefore the increasing intensity of cyber-attacks and the potential technological disruptions of the Internet raise the demand for active studying of the Internet security and operational dependability. In a scope of this work Internet network dependability is the topic of Electrical and Electronic Engineering science.

The existing Internet network infrastructure has formed stochastically, without any systematic analysis of data flows and throughputs and without any systematic network project. The regional Internet networks consist of randomly interconnected sub-networks, which form a complex interconnected communications scheme with a big number of nodes. It is not known whether the throughputs of network nodes and connecting cables are sufficient in case of faults of individual nodes and channels or in case of accidental increase of data flows or cyber attacks. For the purpose of evaluating the possibilities and dependability of the Internet network on the national level, it is necessary to perform comprehensive systematic examination of the entire network infrastructure.

For many years the Internet network has been operated in the increasing cyber attacks and security incidents conditions. With the first serious threats to security of the Internet the Computer Emergency Response Team (CERT) model was developed. The model is still being improved. However it was noticed that the CERT model, being efficient for resolving individual security incidents, is not the absolute method for resolution of the Internet network security and dependability issues.

Topicality of the work. The research of the global Internet has been performed continuously since the very creation of the network. The studies cover the analysis of the network elements, i. e. the autonomous systems and methods for optimization of the networks interconnection topology. However there have not been any systematic studies of the ways for researching and analyzing the Internet network of the state or a region, formed of stochastically interconnected sub-networks, as one common system. The study attempts to resolve the problem and develop a new direction for the Internet studies. The

performed research and developed methodologies supplement the Internet studies tools and methodologies.

The aim of the study is to search for the ways for evaluation of the dependability of a regional Internet network and to develop a methodology for identification of the indicators of continuity and retaining of quality of the Internet activities. The results of solution of the problem have a great significance for development of the practice of evaluation of dependability of the Internet network activities.

The studies of the Internet network infrastructure were performed and the metrics for evaluation of dependability of the Internet network were developed. The methods, based by the column theory, network modeling and statistical analysis, allow for resolving the network analysis tasks in cases where the model of the object is complex or its sub-networks are interconnected randomly and where the statistical characteristics of the network are not fully known.

The results are relevant for the national and international telecommunications supervision and regulatory institutions, since they help to evaluate the existing dependability of the Internet network infrastructure and create the preconditions for the telecommunications regulatory institutions to apply scientific methods for controlling the dependability of the Internet network infrastructure.

The study is also relevant for the national defense institutions. Telecommunications and the Internet are a national resource. Since the impact of cyber-attacks on the functioning of the Internet network has been increasing and the NATO electronic space has announced the fifth defense dimension, the issue of ensuring the Internet security must become a part of the national defense plan.

Object of the research. The object is the regional Internet network infrastructure (geographically described combination) composed of interconnected autonomous systems (AS) and local networks. Investigated real Lithuanian Internet network consist of 40 AS, 27 local networks, 7 International AS and 490 interconnection lines (including 373 peering and 117 transit types of connections).

Aim of the work. The objective is to study and analyze the Internet network of the state or a region, formed of the stochastically interconnected sub-networks, as one common system and search for the ways for identification of the indicators of dependability of the system and continuity of services.

Tasks of the work. In order to reach the goal the following tasks attempted to resolve:

1. To develop a topological scheme of the Internet network and to formulate the model and tools for the topological analysis.
2. To identify the critical elements of the Internet network infrastructure, whose violations would result in a significant degradation of network functionality.
3. To develop a model for monitoring of the critical elements of the Internet network infrastructure and its operation algorithm.
4. To model the topology of the state Internet network infrastructure and to test it vulnerability by simulating cyber-attacks.
5. To formulate the methodical recommendations for strengthening the dependability of the Internet network infrastructure.

Methodology used in the research. Graph theory, statistical analysis, network modeling and simulation and experimental methodology approaches were used.

Scientific novelty. The following results, important for telecommunications were obtained:

1. The methodology for analyzing the Internet network topology in terms of dependability of the network infrastructure activities was developed. The topology of Lithuania's Internet network was outlined and the vulnerability indicators were evaluated.
2. The metrics for identification of the critical elements of the Internet network infrastructure were developed. By applying the said metrics the region's Internet networks results were obtained.
3. The model of the Internet network infrastructure topology was analyzed by applying cyber-attack simulation experiments.
4. The model for monitoring the critical elements of the Internet network infrastructure and its operation algorithm were proposed.

Practical value. The developed metrics is universal and can be used for studies of dependability of the infrastructure of different Internet network areas/regions, identification of the critical elements within the Internet network infrastructures and their further monitoring. The national telecommunications networks regulatory and supervising authorities, referring to the methods, described in the study, can practically evaluate the dependability and security of the Internet network.

The results of studies were analyzed at the Communications Regulatory Authority of the Republic of Lithuania (RRT) and are planned to be used for performing the national regulation of electronic communications. The model for monitoring the critical elements of the Internet network infrastructure has been tested by RRT and an operational demo version was developed.

Summaries of the results were provided to the International Telecommunication Union (ITU), the European Networks and Information Security Agency (ENISA), European countries' regulatory authorities and the Ministry of National Defense of the Republic of Lithuania.

Defended propositions

1. The real regional Internet networks are, in essence, a totality of stochastically interconnected autonomous systems and the throughput of their lines and nodes do not always correspond to the information traffic flows.
2. The vulnerability of the Internet network infrastructure better could be described by critical elements: the critical and η-critical nodes and critical and κ-critical lines.
3. Because of dynamic Internet infrastructure, constantly updated regional network structure model is necessary for internet monitoring and dependability evaluation.
4. Real time monitoring of critical network elements and cyber attacks simulation experiments are complimentary methods for the supervision of the status of the regional internet network and analysis of cyber attacks influence.

The scope of the scientific work. The scientific work consists of the general characteristic of the dissertation, 5 chapters, conclusions, list of literature, list of publications and annexes. The total scope of the dissertation – 84 pages, 9 formulas, 21 pictures, 7 tables, 91 references and 2 annexes.

1. Overview of the Security Incidents Management Model

The Internet, which is one of the most developed ICT networks, is also the one most susceptible to cyber-attacks. The CERT model, developed for the purpose of performing studies of security incidents and responding to incidents, occurring in electronic communications networks, especially in case of a potential risk to functioning of the network or security of the data is overviewed. The role of CERT for the purpose of managing security incidents

on the Internet is evidenced both by other authors and within the framework of the present study.

West-Brown, Killcrece, Alberts, Wii, Kossakowski and many others researches are continuously working in the field of development of the CERT model. As cyber incidents are changing as well as Internet is growing, researches seek to invent new variants or improve CERT model. Carnegie Mellon University (US) stands as a centre of investigations of the CERT model already for several decades.

Academia in Lithuania has also experience in the field of cyber security researches. Research Laboratory of Security of Information Technologies established by the lead of prof. A. Čenys within the Vilnius Gediminas Technical University (VGTU). Kaunas University of Technology does investigations of security incidents and vulnerabilities through the implemented CERT team at the academia network. Prof. A. Kajackas (VGTU) is leading researches of Internet infrastructure resilience and quality of service while prof. J. Skudutis (VGTU) works in the field of cyber incidences defensive measures.

In this study an optimized CERT model for a regional Internet network is outlined. Proposed model developed for security incidents management on the national level, in the conditions with no direct relation to networks administration.

The use of the CERT model, which can be characterized as a detect-clean-recovery system is purely responsive, i. e. the action is performed against the incident fact. Therefore the effect of CERT is short-term. The CERT model, being an efficient tool for resolving incidents, does not create the necessary preconditions for the resolution of the overall issue of evaluation of security and dependability of the Internet network. There comes a need to develop new, proactive/preventive measures, which would create the conditions for minimizing or neutralizing the impact of cyber incidents on the Internet.

Further on, the task of resolution of the Internet security and dependability analysis issue by examining the Internet network infrastructure itself is to study and analyze the Internet network of the state or a region, formed of stochastically interconnected sub-networks, as one common system and search for the ways for identification of the indicators of dependability of the system, continuity of activities and retaining of quality of the services.

In order to reach the said goal, first of all, it is necessary to outline the scheme of the Internet network topology and select the models and tools for analysis. Upon evaluating the topology, the next task is the analysis of connectivity of the Internet network in order to identify the critical network elements, whose violations would result in the loss of functionality of the entire network. After the critical elements of the Internet network are established,

attempts will be made to develop the model for their monitoring and perform cyber-attack simulation tests. The experience, accumulated when performing the studies and the obtained results will create the preconditions for formulation of methodological recommendations for strengthening the dependability of the Internet network infrastructure.

2. Internet Infrastructure Topology Assessment

For the purpose of a further analysis each AS_i is formally described by graph $G_i(V, U)$, comprising a set V of vertices together with a set U of edges. The vertices correspond to the nodes of a real Autonomous Systems (AS) and the edges correspond to the connecting communication lines.

The initial analysis of the topological structure of the Internet can be performed by employing the graphs metrics: node degree, node degree distribution and clustering.

Node degree. The degree of a vertex deg(v) of a graph is the number of edges incident to the vertex. The degree of vertex of the graph is the number k of the communication lines between AS_i and other AS.

Node degree distribution. It is the probability distribution of nodes degrees over the whole network. The degree distribution P(k) of a network is then defined to be the fraction of nodes in the network with degree k. Thus if there are n nodes in total in a network and n_k of them have degree k, we have $P(k)=n_k/n$. When dividing the constituents of the network into the hierarchical structure, there is a need for initial data on each Internet Service Provider (ISP) and the graph $G_i(V,U)$, characterizing its network, specifying N_i and M_i and evaluating the parameters of the lines, connecting the AS.

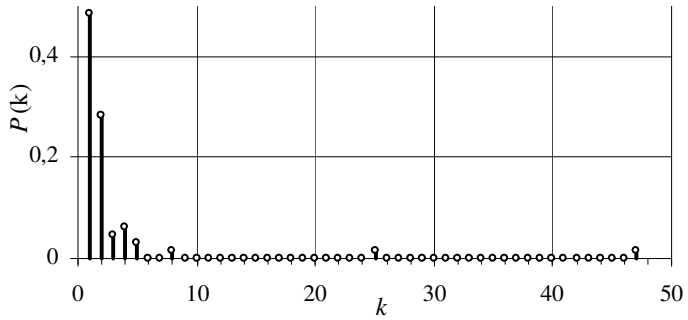


Fig. 1. Nodes degree distribution for transit types of connections

Clustering. If the i^{th} edge of graph and all its direct edges neighbors k_i are taken, connected nodes network could have maximum links equal $k_i(k_i–1)/2$. If graph vertex between edges k_i number is E_i, clustering coefficient for i^{th} edge is C_i. For the regional Internet network C_i should be calculated as average of all nodes within network C_i.

$$C_i = \frac{2E_i}{k_i(k_i - 1)}. \quad (1)$$

The identification of the region Internet AS topology is the necessary approximation towards the evaluation of dependability of the network infrastructure. When describing the hierarchical structure of the Lithuanian Internet network, the Customer type AS identified as most spread (81 %). The classification of types of communications has shown that Peering type connections between the AS prevail in the infrastructure (76 %).

Nodes degree distribution in Fig. 1 shows that 48% of nodes has only 1 Transit type connection $P(k)=0.48$ and 28 % has 2 $P(k)=0.28$. We observed two outstanding nodes with 25 and 47 Transit type connections. It allows for the conclusion that the AS topology of Lithuanian Internet network contains small number of nodes with sufficient connections of the Transit type. We assume that the node with dominant connections amount has great influence on the network topology and has impact to the dependability of the region internal interconnection.

Clustering coefficient for Lithuanian Internet network calculated to be $C_{LT}=0.23$. Dividing to Transit type interconnections network is $C_{transit}=0.05$ and for Peering $C_{peering}=0.17$. As fully connected graph should have $C_i=1$, Lithuanian Internet network connectivity should be improved to achieve better dependability level.

3. Estimation of Critical Components of Internet Infrastructure

When analyzing the Internet network, a graph theory is usually applied. A segment of Internet network is represented by a graph G_{net}, at the vertex of which is AS. A stationary network status is represented by a connected graph. Such graph contains at least one route between the i^{th} AS and any other AS belonging to G_{net}. The article published presents the topology and the respective graph of the Lithuanian National Internet Network infrastructure.

By the rule node characterisation as ***critical node*** (V_c) whose failure or malicious behavior disconnects or significantly degrades the performance of the network.

The vague definition aggravates the identification of critical nodes. The variations defined as "disconnecting or significantly degrading the performance" are identified using different methods. Therefore the following definitions are used in the study: critical node and η – critical node.

A node shall be considered to be critical when its elimination or disturbance dissolves the original graph into two or more separate subgraphs having no interconnection. The nodes defined as matching the description are applied the formal method of removing graph vertices. In case the elimination of i^{th} AS creates separate subgraphs having no interconnection, such AS is considered to be V_c.

η – node shall be considered to be critical when its elimination significantly degrades the network performance for the majority of users (ηA).

On the purposes of this article and specifying the definition of η – critical node, the criticality of a node shall be assessed in relation to the number of users A_i connected to the i^{th} AS. The criticality index of a node η is a relative value:

$$\eta_i = \frac{A_i}{\sum_{j=1}^{J} A_j}. \tag{2}$$

Where A_i is the number of users of the i^{th} AS; ΣA_j is the total number of Internet users in the network.

For convenience, the expression of η – critical node shall be divided into two categories: $\eta_i \geq 0.1$ and $\eta_i < 0.1$. Respectively, the criticality $\eta_i \geq 0.1$ shall be considered to be the highest in the general network infrastructure.

The definitions of a ***Critical link*** E_c is the link connecting two critical nodes so that, when this link is eliminated from the graph, the graph becomes disconnected.

By analogy with the concepts of a critical node used in this article, the following definitions are used: critical link and κ – critical link.

A link shall be considered to be critical when its elimination or disturbance forms several subgraphs having no interconnection (edges). Identification of E_c is performed by the analogous V_c principle – method of removing graph edges. In case the elimination of n^{th} creates separate subgraphs having no interconnection, such line is considered to be E_c.

κ – critical link shall be considered to be critical when its elimination or disturbance significantly degrades network connectivity.

The graph in question corresponds to the regional Internet network with N_{int} connections. N_{int} are the links connecting the AS of the regional network

with the AS of the International Internet network provider. In such case, applying the method of removing, N_{int} shall correspond to E_c.

Specifying the concept of κ – critical link, suggested linking it with the interconnection bandwidth Δ. The maximum installed bandwidth Δ_{max} of the link belonging to the i^{th} AS shall be assessed in relation to the total bandwidth ΣBw of connections managed by i^{th} AS. This relation is expressed by the capacity coefficient η_{AS}:

$$\eta_{AS} = \frac{\Delta_{max}}{\sum_{k=1}^{K} Bw}. \quad (3)$$

Where Δ_{max} is installed connections capacity of the i^{th} AS, Gb/s; ΣBw is the overall bandwidth of the i^{th} AS for all connections of this particular AS.

Having completed the experiment, results of which presented at table 1, using the method of removing the vertices, 4 critical nodes were identified (V_c), whereas the number of η – critical nodes satisfying the condition $\eta_i \geq 0.1$ was 3. Increasing the η_i (presented at table 1) will result in to the increase of number of V_c respectively. It should be noted that one of that 3 nodes coincides with the respective critical node.

Table 1. Critical elements calculation results

Critical element	Criteria	Conditions	Results
V_c	Nodes elimination method		4
	η – critical node	$\eta_i \geq 0.1$	3
		$\eta_i \geq 0.2$	11
		$\eta_i \geq 0.3$	25
E_c	Links elimination method		26
	κ – critical link	$\eta_{AS} \geq 0.9$	2
		$\eta_{AS} \geq 0.8$	13
		$\eta_{AS} \geq 0.5$	33

The identification of critical lines (E_c) in the graph representing the Lithuanian Internet network was slightly more complicated since E_c search must take place among several hundreds of connection lines. Using the method of line removal, 26 critical lines were identified. The search of κ – critical lines ($E_{c\kappa}$) was performed for every ISP separately. Only 2 ISP (independent from E_c), including $E_{c\kappa}$, were identified as satisfying the condition $\eta_{AS} \geq 0.9$. Decreasing the level of η_{AS} will result the increase of number identified $E_{c\kappa}$.

Suggest monitoring the above-mentioned V_c and E_c in order to identify the failures of the critical elements of the network or critical levels of link traffic resources. Monitoring is very important for timely identification of the failures of the critical elements since the loss of such elements affects the whole network performance. Monitoring of critical network elements is investigated on the basis of SNMP protocol using detectors in the critical network nodes and a monitoring system. Since SNMP is commonly used among ISP, there is no need to install a new system; an additional software installation is enough. The algorithm of network monitoring and its realization code were composed.

4. Cyber attacks influence to the Internet functionality

Experiments were intended to simulate and measure the impact of cyber attacks and congestions to the functionality of the infrastructure of the Internet network. In our case the network under this investigation is limited by the interconnected AS operating in the region. To reach the objective, two following tasks fulfilled.

i. Simulate virtual network topology using the real network data available.

ii. Create and test hypothetical cyber attacks scenarios on the virtual network topology measuring the impact and consequences. Experiments made with attack vector represented by: a) the attack generating traffic flood from international AS to the region network infrastructure; b) major transit type interconnections with the international AS nodes failure; c) central network peering-type interconnection node failure.

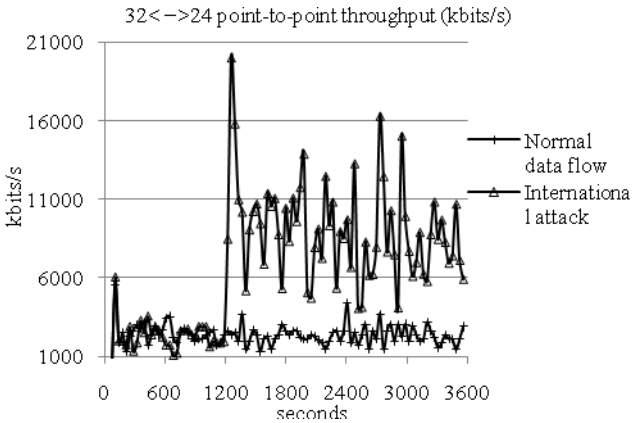


Fig. 2. Throughput measurement during the attack scenario

Virtual Lithuanian Internet network model created for a first time using the OPNET and data related to the Internet network topology.

As a result of the study of the attack (attack vector represented by distributed denial of service attack from outside the region network perimeter), 3 AS (nodes) and 4 interconnection lines was found that had the maximum subsequences (example in Fig. 2). In practice those elements could became "bottle neck" of the network performance and congestions. Estimated that mentioned ASs and lines matches the critical components of Internet network infrastructure defined by the metrics compiled in this work. It proved the theoretical model dependability to the test results.

As a result of the scenarios of the attacks targeting separate interconnection node of the network infrastructure, resulted that network was able to reroute the increase of traffic. Estimated that network node failure due to the cyber attack influenced the traffic increase on other lines but network itself was able to accumulate flows.

5. Dependability consolidation for regional internet network

The stochastic Internet network evolution is based on network neutrality principle that is enough to guaranty its dependability. Additional proactive measures are necessary to introduce to consolidate network dependability.

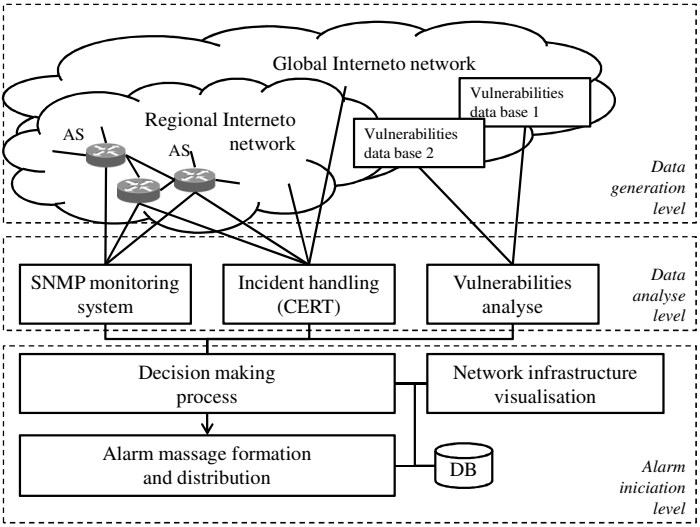


Fig. 3. Conceptual implementation of early warning system

Internet topology assessment, monitoring of network critical elements and virtual cyber attacks simulation systems was accumulated to develop an early warning system (EWS). Vulnerabilities analyses and CERT model complimentary added to the EWS to form EWS as preventive organizational measure dedicated to the regional Internet dependability presented in Fig. 3.

The effectiveness of the decision reception procedure object to initiate the alarm depends on time t necessary for information to reach the target (short t gives more chances for reaction measures), alarm dependability (eliminate false positive by seeking for the minimum error probability $\varepsilon(t)$) and quality of preventive measures.

General conclusions

After developing the model of Internet topology assessment and identification of critical network elements and after verifying and checking it in a nature, as well as after performing a computer experiments with cyber attacks simulation there were formulated the following scientific and practical conclusions:

1. While CERT model stands as an effective tool for the response to the incidents, it can't compose enough preconditions to solve internet network security and resilience problem. Therefore, there is a need for new proactive (preventive) measures to be employed for internet resilience directing them rather towards control and neutralisation of cyber attacks and casual faults.
2. Definitive way of analysis of the internet network topology resilience could be done with graph metrics for interconnected networks applying to node degree, node degree distribution and clustering.
    2.1. According to the formed classification of the autonomous systems (AS) and connections links, type of Customer AS (81 %) and peering links between AS (76 %) identified as most spread within Lithuanian internet network;
    2.2. According to the node degree distribution only one node within Lithuanian internet network has 47 transit type connections and majority of nodes (76 %) use 1-2 transit links with other AS.
3. During the analysis of the regional internet network infrastructure resilience, critical elements were identified using the criteria of critical and η-critical nodes and critical as well as κ-critical links. Model prepared for centralised network supervision over monitoring of critical elements via SNMP protocol. Having applied the above-described metrics to the

Lithuanian internet network infrastructure, 4 critical and 3 η-critical nodes were identified, also as 26 critical links were found that had κ-critical links as well.

4. Virtual Lithuanian Internet network model created dedicated to test network vulnerabilities performing experiments with different scenarios of cyber attacks. During the tests of the attack that generated traffic flood from international AS to the Lithuanian network infrastructure, 3 AS (nodes) and 4 interconnection lines was found that had the maximum subsequences. Violated nodes and links coincide with critical elements identified by theoretical model.
5. To strengthen the resilience of regional internet network infrastructure, early warning system and balancing network topology measures proposed.

List of Published Works on the Topic of the Dissertation
In the reviewed scientific periodical publications

Kajackas A.; Rainys R.; Aputis A. 2011. Assessment of Cyber Attacks Influence over Internet Network, *Electronics and Electrical Engineering*. – No. 7(113). – P. 89–92 ISSN 1392 – 1215 (Thomson ISI Web of Sience).

Kajackas A.; Rainys R. 2011. Estimation of Critical Components of Internet Infrastructure, *Electronics and Electrical Engineering* 4(110): 35-38. ISSN 1392 – 1215 (Thomson ISI Web of Sience).

Kajackas A.; Rainys R. 2010. Internet Infrastructure Topology Assessment, *Electronics and Electrical Engineering* 7(103): 91–94. ISSN 1392 – 1215 (Thomson ISI Web of Sience).

Rainys R. 2006. Network and Information Security. Assessments and Incidents Handling, *Electronics and Electrical Engineering* 6(70): 69–74. ISSN 1392 – 1215 (Thomson ISI Web of Sience).

In the other editions

Rainys R. 2007. Enterprises wireless networks security, in *Proceedings of the International Scientific Conference* „Information technologies“. Kaunas, 234-239. ISSN 1822-6337.

Rainys R. 2006. How Can NRA Contribute to the Improvement of IT Security, in *Proceedings of the International Scientific Conference* „Information Security Solutions Europe“. Roma, 426-432.

About the author

Rytis Rainys was born on 24 of June 1976 in Varėna, Lithuania. He obtained Bachelor of Sciences degree, 1999 and Master degree, 2006 in electronics engineering, Faculty of Electronics, Vilnius Gediminas Technical University. Doctoral dissertation was prepared at Vilnius Gediminas Technical University in 2007–2011. In 1998–1999 was working at Vilnius Metrology Center. At present – director of Network and Information Security Department of Communications Regulatory Authority of the Republic of Lithuania.

REGIONŲ INTERNETO TINKLO INFRASTRUKTŪROS PATIKIMUMO TYRIMAI

Problemos formulavimas. Informacijos ir ryšių technologijos (IRT) yra reikšmingas įrankis kuriant inovacijas, socialinę ir ekonominę šalies gerovę. IRT ir konkrečiai interneto technologijos plačiai išnaudojamos e. versle, e. bankininkystėje, e. valdžios paslaugose. Visuomenė tapo priklausoma nuo IRT ir interneto dėl visapusiškos jų integracijos į socialinius piliečių santykius. Interneto tinklas yra ypatingos svarbos nacionalinė infrastruktūra, todėl didėjantis kibernetinių atakų intensyvumas bei technologinių tinklo grandžių sutrikimai kelia poreikį ištirti interneto saugumą ir jo veiklos patikimumą.

Esama interneto tinklo infrastruktūra susiformavo ir toliau vystosi stochastiškai, be sistemingos duomenų srautų bei pralaidumų analizės, be sistemingo tinklo projekto. Regionų interneto tinklus sudaro atsitiktinai sujungti potinkliai, kurie formuoja komplikuotą tarptinklinių ryšių topologiją su dideliu skaičiumi mazgų ir jungčių tarp jų. Nėra žinoma ar pakankami tinklo mazgų bei jungiamųjų kanalų pralaidumai, ar tie pralaidumai pakankami esant atskirų mazgų bei kanalų gedimams, ar jie pakankami atsitiktinai padidėjus duomenų srautams ir kibernetinių atakų atvejais. Siekiant valstybės mastu įvertinanti interneto tinklo galimybes, jo patikimumą, būtina atlikti išsamius viso tinklo infrastruktūros tyrimus.

Interneto tinklas veikia didėjančioje kibernetinių atakų ir saugumo pažeidimų aplinkoje. Kartu su pirmomis rimtomis grėsmėmis interneto saugumui, sukurtas reagavimo į saugumo incidentus kompiuterių tinkluose CERT modelis, kuris tobulinamas iki šiol. Tačiau pastebėta, kad CERT modelis, būdamas efektyvus sprendžiant atskirus saugumo incidentus, nėra tinkamas metodas spręsti sisteminius interneto tinklo saugumo ir patikimumo klausimus. Kyla poreikis pasirinkti ir vystyti naujas, pro-aktyvias (prevencines) priemones, kurios sudarytų sąlygas mažinti interneto pažeidžiamumą ar neutralizuoti kibernetinių incidentų įtaką internetui.

Mokslo problemos aktualumas. Globalaus interneto moksliniai tyrimai vykdomi nuo tinklo sukūrimo pradžios. Šie tyrimai apima tinklo dedamųjų – autonominių sistemų analizę, tarptinklinių sujungimų topologijos optimizavimo metodus. Tačiau nėra sistemingų tyrimų kaip tirti ir analizuoti iš stochastiškai sujungtų potinklių susiformavusį regiono ar valstybės interneto tinklą kaip bendrą vientisą sistemą. Pristatomoje disertacijoje sprendžiama įvardinta problema ir tuo sukuriama nauja interneto tyrimų kryptis. Darbe atlikti tyrimai ir sukurtos metodikos papildo interneto tyrimų metodikas bei priemones.

Šiuo darbu ieškoma būdų, kaip galima objektyviai vertinti regiono interneto tinklo patikimumą, kuriama metodika, skirta nustatyti interneto veiklos nenutrūkstamumo bei kokybės palaikymo rodiklius. Šios problemos sprendimo rezultatai turi didelę reikšmę kuriant interneto tinklo veiklos patikimumo vertinimo praktiką.

Disertacijoje atlikti interneto tinklo infrastruktūros pažeidžiamumo tyrimai ir sudaryta metrika interneto tinklo patikimui vertinti. Metodai, paremti grafų teorija, tinklo modeliavimu, statistine analize bei eksperimentiniais bandymais, leidžia spręsti tinklo analizės uždavinius tais atvejais, kai objekto modelis yra sudėtingas arba jo potinkliai sujungti atsitiktinai, kai nėra pilnai žinomos tinklo statistinės charakteristikos.

Darbo rezultatai yra aktualūs šalies ir tarptautinėms telekomunikacijų priežiūros ir reguliavimo institucijoms, nes padeda įvertinti esantį interneto tinklo infrastruktūros pažeidžiamumą. Taip pat sudaro prielaidas telekomunikacijų reguliavimo institucijoms pritaikyti mokslinius metodus interneto tinklo infrastruktūros patikimumo kontrolei bei ateities interneto patikimumo stiprinimui.

Darbas taip pat aktualus krašto apsaugos tarnyboms. Telekomunikacijos ir internetas yra nacionalinis resursas. Kadangi auga kibernetinių atakų įtaka interneto tinklo funkcionalumui, o NATO elektroninę erdvę paskelbė penktąja gynybos dimensija, interneto saugumo užtikrinimas yra ir šalies gynybos plano dalis.

Tyrimų objektas. Darbo tyrimų objektas – iš anksto apibrėžto (geografiškai išreiškiamo grafo briaunų ir viršūnių visuma) interneto tinklo regiono infrastruktūra, sudaryta iš tarpusaviu sujungtų autonominių sistemų (AS) ir lokaliųjų tinklų. Praktiškai ištirtas Lietuvos interneto tinklas sudarytas iš 40 AS, 27 lokalių potinklių, 490 tarptinklinių jungčių (tarp jų 373 lygiaverčių mainų tipo ir 117 tranzitinės jungtys).

Tyrimų metodikos. Taikyti grafų teorijos, statistinės analizės, tinklo modeliavimo ir simuliavimo bei eksperimentinio taikymo tyrimų metodai.

Darbo tikslas. Darbo tikslas – ištirti ir išanalizuoti iš stochastiškai sujungtų potinklių susiformavusį regiono ar valstybės interneto tinklą kaip bendrą sistemą ir pasiūlyti būdus kaip nustatyti ir stebėti tokios sistemos patikimumo bei veiklos nenutrūkstamumo rodiklius.

Darbo uždaviniai. Darbo tikslui pasiekti siekiama spręsti sekančius uždavinius:

1. Sudaryti interneto tinklo topologijos analizės modelį bei priemones.
2. Sukurti metodus interneto tinklo infrastruktūros kritiniams elementams, kurių pažeidimai būtų susiję su ženkliu tinklo funkcionalumo praradimu, nustatyti.
3. Sudaryti kritinių interneto tinklo infrastruktūros elementų stebėsenos modelį ir jo veiklos algoritmą.
4. Sumodeliuoti virtualų regiono interneto tinklą bei išbandyti jo pažeidžiamumą simuliuojant kibernetines atakas.
5. Suformuluoti priemones interneto tinklo infrastruktūros patikimumui stiprinti.

Mokslinis naujumas. Rengiant disertaciją buvo gauti šie telekomunikacijų inžinerijos mokslui reikšmingi rezultatai:

1. Sukurta metodika Interneto tinklo topologijos analizei tinklo infrastruktūros veiklos patikimumo aspektu. Sudaryta Lietuvos Interneto tinklo topologija, įvertinti pažeidžiamumo rodikliai.
2. Sudaryta metrika kritinių Interneto tinklo infrastruktūros elementų identifikavimui. Taikant šią metriką gauti rezultatai regiono Interneto tinklui.
3. Atlikta Interneto tinklo infrastruktūros topologijos modelio analizė taikant kibernetinių atakų simuliacijos eksperimentus.
4. Pasiūlytas kritinių Interneto tinklo infrastruktūros elementų stebėsenos modelis ir jo veiklos algoritmas.

Praktinė vertė. Darbe sukurta universali tyrimų metodika ir metrika gali būti naudojamos įvairių interneto tinklo sričių (regionų) infrastruktūros patikimumo tyrimams, kritinių interneto tinklo infrastruktūrų elementams identifikuoti ir jų tolesnei stebėsenai atlikti. Nacionalinės elektroninių ryšių reguliavimo ir priežiūros institucijos, remiantis darbe aprašytais metodais, praktiškai vertina interneto tinklo patikimumo bei saugumo rodiklius.

Tyrimų rezultatai įvertinti Lietuvos Respublikos ryšių reguliavimo tarnyboje ir naudojami vykdant nacionalinį elektroninių ryšių reguliavimą. Išbandytas darbe pasiūlytas kritinių interneto tinklo infrastruktūros elementų stebėsenos modelis laboratorijos sąlygomis.

Darbo rezultatų santraukos ir vaizdiniai pristatymai demonstruoti Tarptautinei Telekomunikacijų Sąjungai (ITU), Europos tinklų ir informacijos saugumo agentūrai (ENISA), Europos šalių reguliavimo institucijoms bei Lietuvos Respublikos krašto apsaugos ministerijai.

Ginamieji teiginiai

1. Realūs interneto regionų tinklai susidaro stochastiškai sujungiant autonomines sistemas, todėl jų linijų bei mazgų pralaidumų charakteristikos ne visada atitinka informacinių srautų intensyvumus.
2. Interneto tinklo infrastruktūros patikimumui vertinti reikalinga sudaryti analizuojamo tinklo topologijos modelį.
3. Interneto tinklo infrastruktūros grandžių pažeidžiamumą gerai atspindi kriterijai: kritiniai ir η-kritiniai mazgai kartu su kritinėmis ir κ-kritinėmis linijomis.
4. Regioninio interneto tinklo būsenos bei kibernetinių atakų įtakos analizei geriausiai tinka kritinių tinklo elementų stebėsenos realiuoju laiku modelis bei kibernetinių atakų simuliacijos eksperimentai.

Darbo apimtis. Darbą sudaro bendra darbo charakteristika, 5 skyriai, išvados, literatūros sąrašas, publikacijų sąrašas ir priedai. Bendra disertacijos apimtis – 84 puslapiai, 21 iliustracija, 7 lentelės, 9 formulės, 91 literatūros šaltiniai ir 2 priedai.

Pirmasis skyrius skirtas tinklų ir informacijos saugumo incidentų valdymo modelio (CERT) apžvalgai bei jo optimizavimui regiono interneto tinklo aprėptyje. Skyriaus pabaigoje formuluojamos išvados ir uždaviniai.

Antrajame skyriuje analizuojama interneto tinklo topologija taikant grafų teoriją, pasiūlytas autonominių sistemų ir jų sujungimo linijų klasifikavimas, nustatytas regiono interneto patikimumas.

Trečiasis skyrius skirtas kritinių interneto tinklo infrastruktūros elementų paieškos metodikos sudarymui ir taikymui. Pasiūlyta metodika bei algoritmas tokių elementų stebėsenai.

Ketvirtajame skyriuje modeliuojama ir tiriama kibernetinių atakų įtaka interneto tinklo infrastruktūros funkcionalumui.

Penktajame skyriuje formuluojamos priemonės regiono interneto tinklo patikimumui stiprinti.

Bendrosios išvados

Sudarius interneto tinklo topologijos analizės modelį bei kritinių tinklo elementų paieškos metodiką, atlikus praktinius skaičiavimus Lietuvos interneto tinklo infrastruktūrai bei kompiuterinius kibernetinių atakų eksperimentus, suformuluotos šios mokslinės ir praktinės išvados:

1. CERT modelis, efektyvus atskirų incidentų tyrime, nesudaro reikiamų prielaidų bendram interneto tinklo saugumo ir patikimumo klausimui išspręsti. Interneto pažeidžiamumas iškelia poreikį kurti ir vystyti naujas, pro-aktyvias (prevencines) priemones, kurios sudarytų sąlygas kontroliuoti bei neutralizuoti kibernetinių incidentų bei atsitiktinių gedimų įtaką interneto veiklos patikimumui.
2. Interneto tinklo topologinės struktūros patikimumo analizei geriausiai tinka ryšių grafų sudarymo metodai, išskiriant mazgų laipsnius, mazgų laipsnių pasiskirstymą ir grupavimą.
   2.1. Pagal sudarytą autonominių sistemų (AS) ir jungčių klasifikaciją, Lietuvos interneto tinklo infrastruktūroje dominuoja Vartotojiško tipo AS (81 %) ir lygiaverčių mainų tipo sąryšiai tarp AS (76 %);
   2.2. Pagal mazgo laipsnių pasiskirstymą, Lietuvos interneto tinklo topologijoje yra tik vienas mazgas valdantis 47 tranzitinių jungčių, o 76 % mazgų valdo tik 1–2 tranzitines jungtis su kitomis AS.
3. Interneto tinklo infrastruktūros pažeidžiamumo analizė pagal kritinių ir η-kritinių mazgų, kritinių ir κ-kritinių linijų paieškos metodiką identifikuoja regiono interneto tinklo kritinius elementus. Šių elementų stebėsena paremta modeliu, naudojančiu SNMP protokolą, užtikrina centralizuotą tinklo infrastruktūros junglumo stebėseną. Sudarytą metriką pritaikius Lietuvos interneto tinklo infrastruktūrai, identifikuoti 4 kritiniai mazgai ir 3 η-kritiniai mazgai, bei nustatytos 26 kritinės linijos ir 2 regiono interneto potinkliai, kurių tarpe yra κ-kritinės linijos,
4. Sukurtas virtualus Lietuvos interneto tinklo modelis, kurio pagrindu, eksperimentiškai vertinamas tinklo patikimumas naudojant kibernetinių atakų scenarijus. Bandyme (kibernetinės atakos vektorius iš tarptautinių AS į nacionalinį regiono tinklą) nustatyta 3 AS (tinklo mazgai) ir 4 tarptinklinių sujungimų linijos, kurios patyrė maksimalias srautų apkrovas. Pažeistos jungtys ir AS sutampa su kritiniais mazgais ir kritinėmis linijomis nustatytais pagal teorinį modelį.
5. Išankstinio įspėjimo sistema ir tinklo topologijos balansavimo priemonės sudaro prielaidas sustiprinti regiono interneto tinklo infrastruktūros patikimumą.

Trumpos žinios apie autorių

Rytis Rainys gimė 1976 m. birželio 24 d. Varėnoje. 1999 m. įgijo elektronikos inžinerijos bakalauro, o 2006 m. magistro laipsnį Vilniaus Gedimino technikos universiteto Elektronikos fakultete. 2007–2011 m. – Vilniaus Gedimino technikos universiteto doktorantas. 1998–1999 m. dirbo metrologu Vilniaus metrologijos centre. Nuo 1999 m. iki šiol dirba Lietuvos Respublikos ryšių reguliavimo tarnyboje, užimamos pareigos – Tinklų ir informacijos saugumo departamento direktorius.

Rytis RAINYS

INVESTIGATION OF THE INTERNET NETWORK INFRASTRUCTURE DEPENDABILITY

Summary of Doctoral Dissertation
Technological Sciences, Electrical and Electronic Engineering (01T)

Rytis RAINYS

REGIONŲ INTERNETO TINKLO INFRASTRUKTŪROS PATIKIMUMO TYRIMAI

Daktaro disertacijos santrauka
Elektros ir elektronikos inžinerija (01T)

2011 11 11. 1,5 sp. l. Tiražas 70 egz.
Vilniaus Gedimino technikos universiteto
leidykla „Technika“,
Saulėtekio al. 11, 10223 Vilnius,
http://leidykla.vgtu.lt
Spausdino UAB „Ciklonas“
J. Jasinskio g. 15, 01111 Vilnius