ELECTRONICS AND ELECTRICAL ENGINEERING
ISSN 1392 – 1215 2011. No. 4(110)
ELEKTRONIKA IR ELEKTROTECHNIKA

TELECOMMUNICATIONS ENGINEERING
T 180
TELEKOMUNIKACIJŲ INŽINERIJA

Estimation of Critical Components of Internet Infrastructure

A. Kajackas, R. Rainys
Telecommunications Engineering Department, Vilnius Gediminas Technical University,
Naugarduko str. 41, LT-03227, phone: +370 5 2744976; e-mails: algimantas.kajackas@el.vgtu.lt, rytis.rainys@elst.vgtu.lt

Introduction

Electronic communications and Internet plays a significant role in the current public life. Beside energy, transport, water supply and other sectors, Internet is considered to be an especially important infrastructure. Currently, more and more users, service providers and public institutions rely on security of Internet network.

Network accessibility can indeed determine the parameters of quality service supply. A failure in network supply due to e.g. cyber attacks, results in service unavailability. As a result, the studies on the reliability and safety of Internet network infrastructure operation, and their continuity remain topical.

The article [1] analyses regional Internet network as an integrated system formed of stochastically connected subnets, and suggests methods for analyzing the topology of such system. The article further analyses one of the fundamental characteristics of a network – Internet network connectivity – on the basis of network topology analysis. The methods suggested in the article are aimed at identifying the critical elements of network infrastructure. Eventually, constant monitoring of such elements would allow real-time assessment of network status.

Problem identification

Cyber attacks have been classified by different impact aspects and some of them have a direct effect on the stability and reliability of Internet network. The number of such attacks on the Internet is increasing, which results in an increased effect on the normal network operation. The network has to process the flows generated by the attacks; and very often such attacks are targeted at the elements of network infrastructure [2]. Normally, as a response to such attacks, an incident management model (a.k.a. detect-clean-recover) – Computer Emergency Response Team (CERT) – is used [3]. The nature of such model operation is exceptionally reactive, i.e. an action is generated upon the fact of an attack. CERT has a short-term effect, i.e. dealing with a specific attack, and responding to the outcomes [4, 11]. Due to anonymity on the Internet, the identification of the source of an attack is not always possible using CERT, therefore, attacks from the same source may recur. Therefore, we presume a need for new proactive (preventive) measures to be employed directing them rather towards protection than towards defense as in the case of using CERT.

Another very important aspect is telecommunication. Internet Service Providers (ISP) forms their network infrastructures individually according to their business objectives, network expansion possibilities and user needs. Each ISP has its own routers and inter-network formation policy. Every ISP monitors its network perimeter, and controls the network security as well as its operation reliability. Connections to other networks are also arranged under the initiative of the very ISP using Border Gateway Protocol (BGP) for compiling Autonomous System (AS) routing tables. Such inter-network connections form a hierarchical structure of the Internet network [5]. The general reliability of stochastically formed Internet network segment depends on various factors, including the reliability and topology of separate AS elements.

This article is aimed at shaping the methodology for analyzing the Internet network infrastructure identifying the critical elements of the infrastructure the disturbances of which are influencing functionality of the entire network operation.

Methodology and Criteria

When analyzing the Internet network, a graph theory is usually applied [6]. Works [7, 8] demonstrates the adoption of graph theory for networks traffic analysis and traffic engineering while practice for Internet interconnections assessments is still lacking.

A segment of Internet network is represented by a graph G_{net}, at the vertexes of which are Autonomous Systems (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 [1] presents the topology and the respective graph of the Lithuanian National Internet Network infrastructure.

The following elements of graph are of especially high importance: *critical node* – V_c and *critical link* – E_c.

The descriptions of these critical elements vary among authors.

By the strict rules node is critical if its removal will disconnect the graph into two components. Extended characterisation of ***critical node*** presented in paper [9] as a node V_c whose failure or malicious behaviour disconnects or significantly degrades the performance of the network.

The vague dual definition of node criticality aggravates the identification of critical nodes. In reality, the variations defined as "disconnecting or significantly degrading the performance" are identified using different methods. Therefore the following definitions are used in this article: 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 disconnected graph.

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

The nodes defined as matching the first 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.

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

$$\eta_i = \frac{A_i}{\sum A_j}; \qquad (1)$$

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 also vary. One of the definitions is as follows: "a link AB is critical if both endpoints A and B are critical nodes". Broader E_c description is the link connecting two critical nodes so that, when this link is eliminated from the graph, the graph becomes disconnected [9].

When identifying E_c, G_{net} is considered to be formed of all the ISPs operating on the Internet network corresponding to the node vertices. It is important to note the links the eliminations of which would disconnect small ISP (having no AS) from the National Internet network.

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).

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

Identification of E_c according to the first definition 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. The graph in question corresponds to the regional Internet network with N_{int} connections [1]. 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, we suggest 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}

$$\eta_{AS} = \frac{\Delta_{\max}}{\sum Bw}; \qquad (2)$$

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, Gb/s.

The estimation of η_{AS} shows the criticality of the link for the i^{th} AS connectivity compared to other links of i^{th} AS. κ-critical link shall be divided into two categories: $\eta_{AS} \geq 0.9$ and $\eta_{AS} < 0.9$. Respectively, the criticality $\eta_{AS} \geq 0.9$ (criticality) of the lines shall be considered to be the highest for the total connectivity of i^{th} AS. Essentially, the presence of the above-mentioned condition shows disproportionate distribution of i^{th} AS resources.

Analyzing κ-critical links ($E_{c\kappa}$), their traffic (bandwidth) intensity is also important to consider. The relation of the data flow $\Delta_{traffic}$ (Gb/s) of the n^{th} link (n = 1, 2, ..., $E_{c\kappa}$) and Δ_{max} shows the line traffic expressed by the traffic coefficient λ_n, $\lambda_n = \Delta_{\text{traffic}}/\Delta_{\max}$. It is a dynamic parameter different from the above-mentioned parameters which are more or less static. $\Delta_{traffic}$ is one of the most significant network parameters often monitored by ISP.

In a real network, given the normal status, connection links are not overloaded and usually have some reserves. However, subject to data flows generated due to user activeness or cyber attacks, traffic intensity may exceed the installed bandwidth. When $\lambda_n \geq 0.8$, it alerts the critical level of resources used of the link, the critical bandwidth limit reached by more than one line may signal a cyber attack, which in turn may result in significant degradation of the whole network connectivity.

Application

The above-described metrics were applied to identify the critical nodes and lines of the Lithuanian national Internet network [1].

Having completed the experiment 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.

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 $E_{c\kappa}$.

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

Monitoring

We 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. For the troubleshooting, we shall use detectors in the subgraph G_c consisting of vertices and edges E_c. These detectors perform network monitoring through constant intercommunication.

The simple way to perform monitoring would be routine checks carried on network switching nodes (V_c). Those could be simple *ping, tracepath, pathping* or *traceroute* commands, which would continuously (for instance, at 1-5 minutes intervals) check the response from all the critical nodes and the process itself would be automated and screened on the network topology map. The positive characteristic of such a method is its independence, since there would be no need for agreements with router administrators regarding placement of sensors. However, the method itself lacks flexibility. In addition, some ISP prohibits reception of the said commands in their networks.

Our approach is to use for monitoring purposes the Simple Network Management Protocol (SNMP). SNMP is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems. As most ISPs use SNMP as de facto standard for network supervision, idea is to monitor some parts of national network identified as critical nodes of network infrastructure.

To get information about critical nodes functionality, dedicated cyclical algorithm invented and presented at Fig. 1.

Generally, monitoring needs to follow several major steps:

1. Send request using SNMP protocol to V_c (SNMP Agent).
2. Get response to monitoring system (SNMP Manager) using SNMP protocol from V_c (SNMP Agent).
3. Calculate and store that data using scripts or tools in central monitoring server with database.

We suggest selecting the Ethernet Statistics Group MIB necessary for λ_n evaluation at SNMP Agent [10]. To calculate λ_n for full−duplex connections, we propose formula taking the largest of the *in* and *out* traffic values

$$\lambda_n = \frac{\max(\Delta_{in}, \Delta_{out}) \times 8}{\Delta t \times \Delta_{\max}}; \quad (3)$$

where Δ_{in} – the difference between two poll cycles of collecting the SNMP *ifInOctets* objects, which represents the count of inbound octets of traffic in bytes [10]; Δ_{out} – the difference between two poll cycles of collecting the SNMP *ifOutOctets* objects, which represents the count of outbound octets of traffic in bytes [10]; $\Delta_{\max}$ – the speed of the interface, as reported in *snmpifSpeed* object in bits/s [10]; Δt – time period. Time period Δt = 60 s.

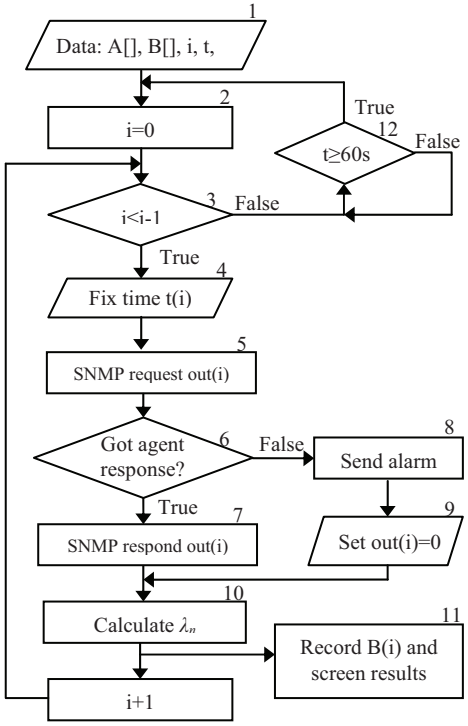

Fig. 1. Algorithm for monitoring with SNMP agents.

Implementation of the structural algorithm presented in Fig. 1 could be performed by the pseudo code algorithm:

```
1    t, id_A, out ∈ B[];
     i ∈ [0, n-1];
     read ID, IP_address ∈ A[];
2    set i = 0;
3    for each ID ∈ A[i] do
4       fix local system time t(i);
5       send SNMP request IP_address ∈ A[i];
6          if IP_address ∈ A[i] responded then;
7             get out(i);
            else
8             send alert notification;
9             set out(i) = 0;
```

```
10          calculate λn;
          endif;
11      write id_A, t(i), out(i) ∈ B[];
      end;
12    wait 60s.
      return.
```

SNMP agents can be software-configured so that *alarm* messages are sent to the monitoring system not only in the case of total failure of the line (Fig. 1) but also when the critical limit of line traffic is reached, i.e. when $\lambda_n \geq 0.8$. Thus the monitoring is performed even more expeditiously.

Conclusions

The assessment of an infrastructure of a network consisting of a large number of stochastically connected subnets (e.g. Internet) in an aspect of reliability is a difficult task due to network complexity. The metrics compiled during the study allows identifying the critical elements of such network: critical and η-critical nodes and critical as well as κ-critical links. The analysis of these elements simplifies the above-mentioned task.

Having applied the above-described metrics to the Lithuanian Internet Network infrastructure, 4 critical nodes (V_c) were identified, whereas the number of η-critical nodes satisfying the condition $\eta_i \geq 0.1$ was 3. Also, 26 critical links and 2 ISPs, including κ-critical links satisfying the condition $\eta_{AS} \geq 0.9$, were identified. Thus we can make a conclusion that the majority of subnets in the infrastructure of the national internet network distribute their resources proportionally. In this way the risk of being dependant on the reliability of κ-critical links' operation is reduced.

We have proved that monitoring of critical network elements is possible 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. All this allows for a real-time centralized monitoring of network status, analysis of network operation failures, etc. We suggest implementing such model, e.g. at the institutions managing electronic communication.

References

1. **Kajackas A., Rainys R.** Internet Infrastructure Topology Assessment // Electronics and Electrical Engineering. – Kaunas: Technologija, 2010. – No. 7 (103). – P. 91–94.
2. **Knight S., Leblanc S.** When not to pull the plug – the need for network counter–surveillance operations // Cryptology and information security series, 2009. – Vol. 3. – P. 226–237.
3. **West–Brown M. J., Stikvoort D.** Handbook for Computer Security Incident Response Teams (CSIRTs), 2003.
4. **Rainys R.** Network and Information Security. Assessments and Incidents Handling // Electronics and Electrical Engineering. – Kaunas: Technologija, 2006. – No. 6(70). – P. 69–74.
5. **Gao L., Rexford J.** Stable Internet Routing Without Global Coordination // ACM SIGMETRICS, 2000.
6. **Ekmanis M.** Graph Mining for Traffic Source Similarity Search // Electronics and Electrical Engineering. – Kaunas: Technologija, 2010. – No. 5(101). – P. 39–42.
7. **Lauks G., Jeļinskis J.** Metamodelling of Queuing Systems using Fuzzy Graphs // Electronics and Electrical Engineering. – Kaunas: Technologija, 2009. – No. 4(92). – P. 61–64.
8. **Jeļinskis J., Lauks G.** Detection of Trends of Internet Traffic using Sequential Patterns // Electronics and Electrical Engineering. – Kaunas: Technologija, 2009 – No. 5(93). – P. 3–6.
9. **Karygiannis A., Antonakakis, E. Apostolopoulos A.** Detecting Critical Nodes for MANET IDS // IEEE Computer Society, 2006.
10. **Waldbusser S.** Network Monitoring Management Information Base // Carnegie Mellon University, 1995.
11. **Thonnard O.** A multi–criteria clustering approach to support attack attribution in cyberspace, PhD Thesis. – Ecole Nationale Supérieure des Télécommunications, 2010.

Received 2011 01 15

A. Kajackas, R. Rainys. Estimation of Critical Components of Internet Infrastructure // Electronics and Electrical Engineering. – Kaunas: Technologija, 2011. – No. 4(110). – P. 35–38.

The article analyses the connectivity of Internet – one of the fundamental network characteristics – on the basis of network topology analysis. The metrics compiled allows identifying the critical elements of Internet network infrastructure: critical and η-critical nodes and critical as well as critical and k-critical links. The model of monitoring the critical network elements was created, and the algorithm of realizing was described. Ill. 1, bibl. 11, tabl. 1 (in English; abstracts in English and Lithuanian).

A. Kajackas, R. Rainys. Interneto infrastruktūros kritinių elementų tyrimas // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2011. – Nr. 4(110). – P. 35–38.

Straipsnyje, remiantis tinklo topologijos analizės duomenimis, nagrinėjima fundamentali tinklo savybė – interneto tinklo junglumas. Sudaryta metrika, kuri leidžia nustatyti kritinius interneto infrastruktūros elementus: kritinius ir η-kritinius mazgus bei kritines ir k-kritines linijas. Suformuluotas kritinių tinklo elementų stebėsenos modelis, aprašytas stebėsenos atlikimo algoritmas. Il. 1, bibl. 11, lent. 1 (anglų kalba; santraukos anglų ir lietuvių k.).