ELECTRONICS AND ELECTRICAL ENGINEERING
ISSN 1392 – 1215 *2011. No. 7(113)*
ELEKTRONIKA IR ELEKTROTECHNIKA

TELECOMMUNICATIONS ENGINEERING
T 180
TELEKOMUNIKACIJŲ INŽINERIJA

Assessment of Cyber Attacks Influence over Internet Network

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

crossref http://dx.doi.org/10.5755/j01.eee.113.7.619

Introduction

Cyber attack is an attempt to damage computer system or disturb its operation, or an attempt to manipulate the information on the Internet. Lately, cyber attacks of large scope have a negative effect on the functionality of Internet network. In 2007, a major cyber attack was launched against Estonian information systems. The internet resources of banks, various ministries, government, and other important institutions were compromised during the attack. 128 distributed denial of service (DDoS) has been found that practically damaged Estonian Internet network for some time period [1]. A similar cyber attack was detected in Georgia as well in 2008 [1].

The article discusses the main types of cyber attacks targeting Internet network. It also presents the results of the study aimed at identifying the effects of cyber attacks on the functionality of Lithuanian Internet network infrastructure. The objective of the study is to prepare model to measure the impact of a hypothetical cyber attack on the Lithuanian Internet Network infrastructure, and identify the weakness components of network.

Methodology

Cyber attacks directed towards Internet network resources cause large-scale damage and affect the majority of users. Having performed the analysis of works [2, 3], three network protocols BGP, TCP and DNS were identified as being the most hazardous when used during the cyber attack to Internet network. BGP protocol has vulnerabilities that could be used to design false Autonomous Systems (AS) routing tables for traffic redirecting. Using botnet (controlled network of large number of compromised computers) a large number of SYN and SYN-ACK (no-reply) messages could be generated within TCP protocol to overload system resources and interrupt functionality of the system. Similarly, DNS (Domain Name System) servers could be overloaded by the cyber attacks that their functioning would be disturbed.

This work is intended to simulate and measure the impact of cyber attacks and congestions [4] 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 [5]. To reach the objective, two following tasks need to be fulfilled.

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

ii. Create and test hypothetical *cyber attacks scenarios* on the simulated network topology measuring the impact and consequences.

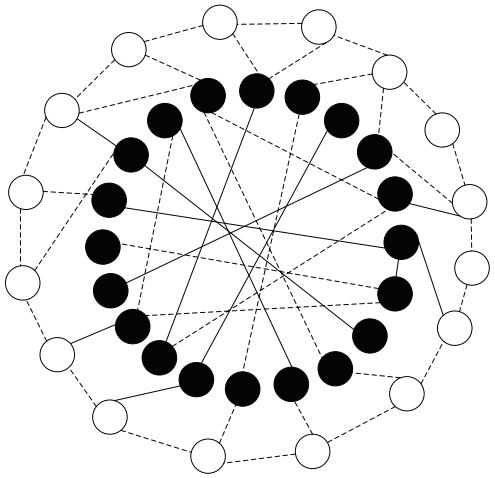

Fig. 1. Graph of the state Internet network topology: national AS represented in black nodes; international AS in white; *peering* interconnections type – dotted lines; *transit* – solid lines

The object of the assessment (Fig. 1) represents Lithuanian Internet network topology. It is a graph consisting of 37 AS related to the national network and 7 international AS that are densely interconnected with *peering* and *transit* types of links [5]. For the sake of security and information confidentiality, the real names of the AS in the model were encoded with certain numbers.

OPNET Modeler application was selected to simulate described network infrastructure topology. Practice of

OPNET usage for network performance measurements demonstrated in works [6, 7]. OPNET Modeler used to simulate network close to real, including nodes and links technical specifications.

We assume Internet or part of the network could be disturbed by cyber attack(s). Attacks profiles selected according to the descriptions of cyber attacks impact to the Internet mentioned above in this chapter. In practice attacks could be realised as a data traffic flood or nodes (routers) failure due to the e. g. BGP misconfiguration. According to that, several scenarios were tested:

1. The attack generating traffic flood from international AS to the Lithuanian network infrastructure;
2. Major transit type interconnections with the international AS nodes failure;
3. Central network peering-type interconnection node failure.

Cyber attack, according to first scenario, was executed in the simulated network model by creating larger than normal data flow from different AS subnets imitating DDoS. Next two scenarios executed by alteration of BGP protocol configuration imitating network nodes random failures and configuration errors. Generally, the cyber attacks were assessed on the basis of variations in the data compared to normal network operation.

Study results

The virtual network with OPNET constructed from 37 AS, 7 international AS and 548 interconnection links, including 424 *peering* and 124 *transit* links [9, 10]. It is identical to the real Lithuanian Internet topology, data of which were collected during the work [5].

The BGP protocol was used for exchanging the routing data among AS since it is currently the main routing protocol within the Internet. An AS in the OPNET Modeler was represented by one Ethernet router with the BGP protocol support. For the interconnection of AS in the network, 10GBaseX and 1000BaseX technologies were used. The types of technologies were chosen with respect to the bandwidth used across the real AS in the Lithuanian Internet infrastructure [5].

Three different data flows were generated within the simulated network. The main data flow was generated inside the state network between national AS; another data flow was created from the national AS to the international AS; and the third data flow created was from the international AS to the national AS.

Using OPNET an ordinary network operation was simulated setting the network operation conditions that were generating the data flows, the FTP, HTTP, E-mail services. This has allowed setting the limits with reference to which entry values are changed for attack simulation. The data transfer line throughput was obtained and measured during the network operation.

During the above-mentioned scenarios, different parts of Internet network were compromised in order to estimate the effect of the attack for the functionality of the whole network.

1. In the first scenario, a cyber attack was launched generating traffic flood from international AS to the Lithuanian network infrastructure (national AS) (Fig. 2). The aim of the attack was to interrupt data transfer in all national AS network. For example this scenario in practice could coincide with botnet located outside Lithuanian network that generates DDoS attack to the national Internet.

Computer resources were limited to operate attacks scenarios at maximum scfig.ale on the OPNET simulated network topology (Fig. 1). In this case, a coefficient k = 1000 was introduced that is applicable to following throughput measurements.

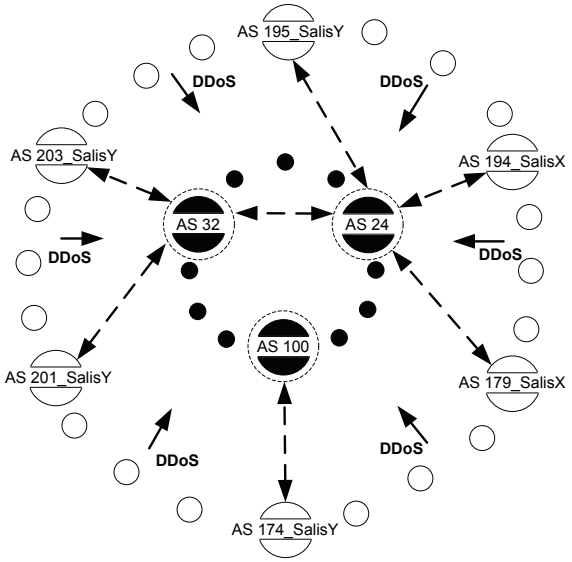

Fig. 2. Part of the network topology illustrating type of attack from international AS to the national AS infrastructure (attack vector represented by *DDoS*)

As a result, after the simulation of the scenario, it was found that 3 AS (numbers 24, 32 and 100) had the maximum subsequences. It means that within the network topology those nodes will accumulate the biggest amount of DDoS traffic. Determining the main interconnections, which will have major traffic load, may help to visualize the real behavior of cyber attack in Lithuania Internet infrastructure.

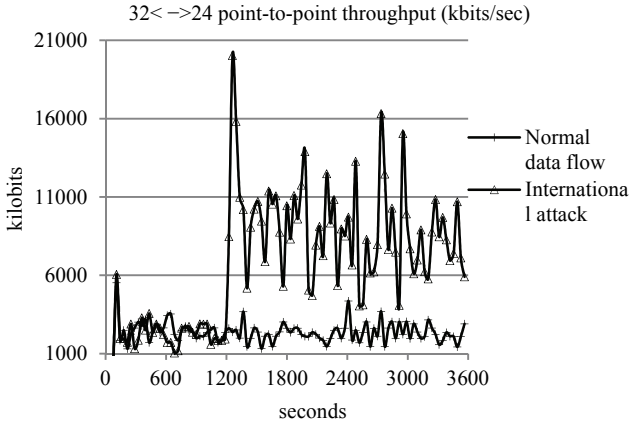

Fig. 3. Throughput measurement during the attack scenario 1

Having analyzed throughput measurement of all those AS interconnections, it was found 4 interconnection lines that had the major (maximum throughput) traffic load. The

graph (Fig. 3) shows interconnection that faced with the greatest traffic load.

The graph (Fig. 3) shows that during the 20th minute from the start of the attack, the bandwidth in the link has increased up to 3 times. The effect of this link failure was observed during this scenario with coefficient *k* estimation. It was found that this factor will affect 2 others interconnections of this AS as well.

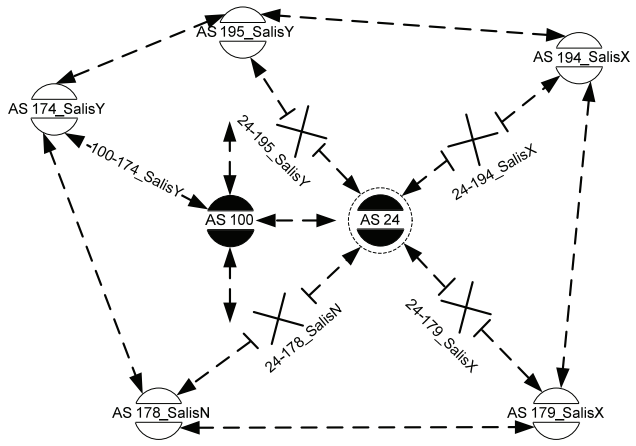

Fig. 4. Part of the network topology illustrating the attack on interconnections node (attack vector represented by broken node/lines)

2. In the second scenario, we selected the AS (No. 24) in order to assess the possible outcomes in case all the *transit* interconnections of this AS, connecting it directly to the international ISP, are lost (network node breakdown). With the work [8] we have identified this AS as a critical node. The attack was realized by altering the AS BGP protocol configurations. Due to altered BGP protocol configuration, data transfer through *transit* interconnections was interrupted (Fig. 4).

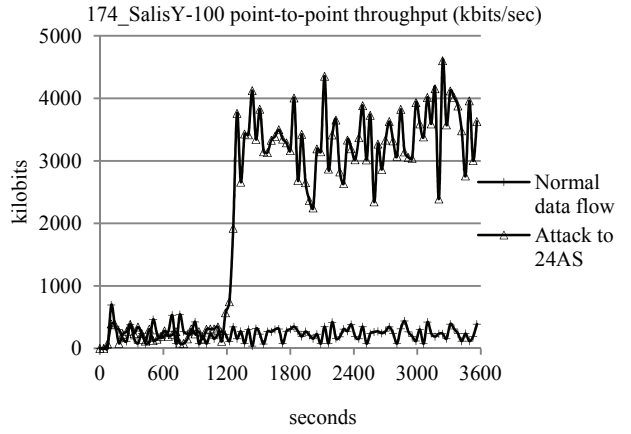

Fig. 5. Throughput measurement during the attack scenario 2

The test has revealed what alternative routes could be used by users to access Internet outside the national network in case the single direct route to these AS is eliminated. It has been established that as a result of the cyber attack, the entire data flow from the international AS has to be directed to the other AS and only then access to the Lithuanian networks. The main alternative route has been established in the OPNET model having analyzed the AS BGP routing tables.

The graph (Fig. 5) presents the throughput of the interconnection on which traffic was redistributed because of node breakdown. During the 20th minute, there was an increase up to 8 time observed in the traffic through this interconnection. Such increase in the traffic exceeded the limits of the bandwidth of this interconnection.

3. In the last scenario, a cyber attack was launched targeting all the *peering* interconnections to central peering node IXP (Internet eXchange Point). During the attack, the AS BGP protocol configurations were altered. Due to altered BGP protocol configuration, data transfer through *peering* interconnections was interrupted (attack process the same as in Fig. 4). The test showed that in such case the entire flow was redistributed across the *transit* interconnections of ASs thus resulting in the increased traffic through the *transit* interconnections. Having analyzed all the *transit* interconnections with respect to the number of times the traffic changed, the interconnections receiving the most of the traffic were identified. The graph (Fig. 6) presents traffic dynamics at one of those interconnections. Generally in the OPNET model observed that due to the damaged IXP node, national internet network was able to manage operations because of traffic redirections to the *transit* type of connections. The graph shows that during the 10th minute, the traffic through this interconnection has increased by three times. This was the interconnection receiving the major traffic load.

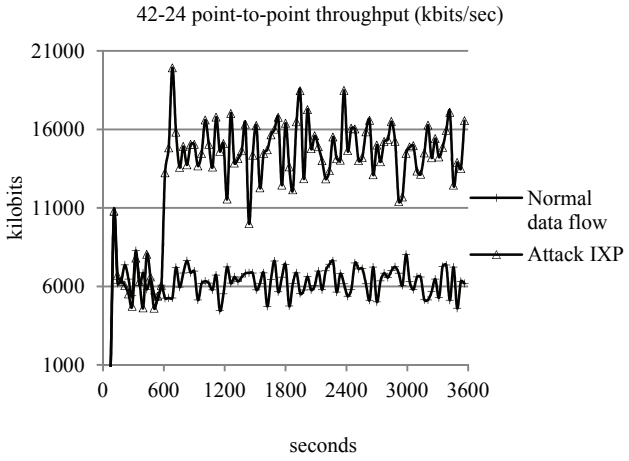

Fig. 6. Throughput measurement during the attack scenario 3

Conclusions

The growing Internet interconnections complexity and increasing cyber attacks impact to the Internet and its users made Internet network infrastructure resilience relevant research topic. This article is continues work of [5, 8] that investigated Internet network topology and identified Internet network infrastructure critical components. It is an approach to verify and measure possible impact of cyber attacks or critical nodes failures to the functionality of the network infrastructure.

Virtual Lithuanian Internet network model created for a first time using the OPNET and data related to the Internet network topology. Having analyzed the TCP and BGP protocols as well as the DNS system, the security gaps used by cyber offenders were identified. According to that, several different scenarios of cyber attacks created to be tested on the created virtual network topology.

As a result of the study of the attack that generated traffic flood from international AS to the Lithuanian national AS infrastructure, 3 AS (nodes) and 4 interconnection lines was found that had the maximum subsequences. 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 work [8]. It proved the theoretical model reliability 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 that.

The results obtained could be useful when predicting possible outcomes of a real cyber attack against the infrastructure of the state Internet network. The model created could be used for strengthening the Lithuanian or other countries Internet network infrastructures.

Acknowledgment

Authors express gratitude to Dr. Antanas Vindašius for his efforts during evaluation of this work.

References

1. **Nazario J.** Politically Motivated Denial of Service Attacks // CCDCOE, 2010.
2. **Mirkovic J., Martin J., Reiher P.** A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms // UCLA CSD Technical Report, 2004. – No. 020018.
3. **Chandramouli R., Rose S.** Secure Domain Name System (DNS) Deployment Guide. – Recommendations of the National Institute of Standards and Technology, 2009. – 118 p.
4. **Pavilanskas L., Statkus A.** Evaluation of TCP Acknowledgment Mechanism Influence on Router Performance // Electronics and Electrical Engineering. – Kaunas: Technologija, 2010. – No. 7(103). – P. 95–100.
5. **Kajackas A., Rainys R.** Internet Infrastructure Topology Assessment // Electronics and Electrical Engineering. – Kaunas: Technologija, 2010. – No. 7 (103). – P. 91–94.
6. **Kulikovs, M. Petersons E.** Modeling the On–line Traffic Estimator in OPNET // Electronics and Electrical Engineering – Kaunas: Technologija, 2009. – No. 7(95). – P. 82–86.
7. **Kajackas A., Pavilanskas L., Vindašius A.** Synchronous Voice Applied Customer Access based on IEEE 802.11 // Electronics and Electrical Engineering. – Kaunas: Technologija, 2007. – No. 8 (80). – P. 23–28.
8. **Kajackas A., Rainys R.** Estimation of Critical Components of Internet Infrastructure // Electronics and Electrical Engineering. – Kaunas: Technologija, 2011. – No. 4(110). – P. 35–38.
9. **Dhamdhere A., Dovrolis C.** The Internet is Flat: Modeling the Transition from a Transit Hierarchy to a Peering Mesh // CAIDA Georgia Tech. – Philadelphia, USA, 2010.
10. **Luckie M., Dhamdhere A., Murrell D.** Measured Impact of Crooked Traceroute // ACM SIGCOMM Computer Communication Review, 2011. – Vol. 41. – No. 1.

Received 2011 05 02

A. Kajackas, R. Rainys, A. Aputis. Assessment of Cyber Attacks Influence over Internet Network // Electronics and Electrical Engineering. – Kaunas: Technologija, 2011. – No. 7(113). – P. 89–92.

The objective of the study is to prepare model to measure the impact of a cyber attack on the Internet network infrastructure, and identify the weakness components of network. As a result of the study virtual Lithuanian Internet network model created and several different scenarios of cyber attacks prepared and tested. 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. Other attacks targeting separate interconnection node of the network infrastructure, resulted that network was able to reroute the traffic. Ill. 6, bibl. 10 (in English; abstracts in English and Lithuanian).

A. Kajackas, R. Rainys, A. Aputis. Kibernetinių atakų įtakos interneto tinklui tyrimas // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2011. – Nr. 7(113). – P. 89–92.

Tyrimo tikslas – parengti modelį, kuriuo būtų galima įvertinti kibernetinių atakų poveikį Lietuvos interneto tinklo infrastruktūrai ir nustatyti labiausiai pažeidžiamus mazgus ir linijas tinkle. Sudarytas virtualus Lietuvos interneto tinklo modelis bei paruošti ir išbandyti skirtingi kibernetinių atakų scenarijai. Atliekant bandymus generuojant duomenų srautų ataką iš tarptautinių AS nukreiptą į Lietuvos tinklo infrastruktūrą, nustatyti trys AS (mazgai) ir keturios jungiamosios linijos, kurios pasiekė galimybių ribas. Kiti atakų scenarijai, nukreipti į atskirus tinklo infrastruktūros mazgus, lėmė, kad tinklas sugebėjo akumuliuoti duomenų srautus. Il. 6, bibl. 10 (anglų kalba; santraukos anglų ir lietuvių k.).