RESEARCH REVIEW JOURNALS
Volume-03
Issue-07
July-2018

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

A Critical Study of the Content Analysis on Networks for Monitoring and Security

[1]Devajit Mahanta and [2]Dr. Ashish Chaturvedi

[1]*Research Scholar, Kalinga University, Raipur, Chhattishgarh*
[2]*Associate Professor, Kalinga University, Raipur, Chhattishgarh*

ARTICLE DETAILS

Article History
Published Online: 05 July 2018

Keywords
Domain Name System, Security, network, public domain.

ABSTRACT

This research work can be further applied to algorithms for change-point detection that can be used to identify and isolate the change in a traffic statistic triggered by attacks. Initially, by address, port or protocol, they filter the target traffic data and store the resulting flow as a time series. E.g. E.g. The deviations in the real versus expected local average in the traffic time series can be detected based on known statistics to detect and localise a DoS attack. It can also be used to classify the network worms' standard scanning activities. To evaluate whether network traffic can be repeated by constructing network topologies and collecting data from them, network simulation tools such as GNS3 and ns2/ns3 have been tried. We can telescope the time to create the baseline data for a network and minimize efforts and resources in the gambit, if it is possible to simulate our performance. However, with the present limitations in the simulation software and the replication of network system behaviour, it was possible to reproduce the topologies of the network in part. A new systematic and comprehensive approach to network monitoring has been built from a security perspective. The study defined essential and fundamental parameters of network communication and protocols for consideration from a security perspective for network monitoring.

1. Introduction

Executable files are created and embedded in vulnerability-exploiting documents. With the help of network indicators, these can be identified. By extrapolating techniques and characteristics from known threat contact behaviours, proactive identification of unknown threats can be expanded. C&C domain names and IP addresses will continue to shift in these situations, establishing a defensive posture by blocking them alone. Since network trends are less subject to change. At the network level, the ability to detect APT behaviour is highly dependent on leveraging threat intelligence. The ability to identify them can be compromised by changes made to malware's network communications.

Many of the malware used in targeted attacks interact with the HTTP/HTTPS port since only these ports are firewall-level available. This means that detecting any non-HTTP traffic on port 80 or any non-HTTPS traffic on port 443 can result in further investigation of potentially malicious traffic. It will help to track regular intervals for Domain Name System (DNS) requests for the same URL.

Deep discovery offers the awareness, insight and control required across the network to detect and identify targeted attacks in real time. To remedy threats and avoid further harm, it offers in-depth analysis and actionable intelligence. Malicious information, suspicious contact and attack actions can be identified.

The main objective of the research was to protect the network from vulnerabilities, threats, attacks, flaws in configuration, and weaknesses in security policy. The vulnerabilities are due to improperly configured hardware or software, bad network architecture, intrinsic technological failure or carelessness of the end user, i.e. technical deficiencies, weaknesses in configuration, weaknesses in security policy. An access control policy between networks is implemented by firewall devices, which are software or hardware. Network security applies to all hardware and software functions, features, functional processes, accountability mechanisms, access controls, administrative and management policies needed to provide hardware/software and information with an appropriate degree of protection.

A network must follow three basic principles of honesty, confidentiality and availability to avoid information loss. Prevention, identification and reaction are included in real world defence. Firewall, encryption, and security of passwords are ways to avoid the loss of knowledge. Detection requires tracking.

A test bed has been designed in order to test the security and efficiency of the network. It contains two Cisco routers, a Cisco firewall, a Cisco switch, a AAA server and two workstations (to act as hackers). Using this configuration, the following tests were conducted:-

- Hackers use a network traffic capture and analysis tool (packet sniffer) to access network traffic. Here, encrypted password is configured, so hackers cannot recover the hidden password and because of encrypted transmission, the content loss is prevented.
  To simulate an access attack, a scanner programme is used. Firewall settings, however, prevent open ports from being found.
- Next, it was not possible for NMap and Nessus to collect data for open TCP and UDP ports and other vulnerabilities. This was avoided by disabling excessive route and firewall features and services such as http server, boot server, IP direct broadcast, etc.
- Remote access via Telnet was prevented by disabling non-IP-based remote access protocols.
- By ignoring certain IP addresses that do not

belong to the internal network, the DSniff software was made ineffective.

The test results have therefore shown that such attacks can be prevented by router and firewall settings that are acceptable.

2. Research Methodology

Roadmap

In the current research, the capturing of network packets using software tools is planned and the analysis of network packet movement will be carried out to review communication patterns in a computer network. Network data is deduced from contact patterns.

Protection, since it is a public domain, is a big problem with the network. Sniffing, snooping, eavesdropping, botnets, Distributed Denial of Service (DDoS) attacks, SQL injection and many other kinds of security threats are vulnerable to the cyber world. Stalking and intimidation, identification fraud and theft, technological discovery, standard lead development investigation, anti-pedophile investigation, disciplinary proceedings, company policy breaches, identity checking, alias vetting, development of subject character, discovery of accomplices, violations of probation, other court order violations etc. Content management across the network and correct content flow analysis will identify any unusual behaviour in the cyber world from the point of view of security threats. The area of research for the present study is the control of the network from a safety perspective. For data analysis, various methodologies and techniques are used, including statistics, profiling, behavior-based approach, sampling, visualization and computational infrastructures. Network packet capture can be achieved using different methods. Each instrument has its own applicability and limitations that need to be checked before deciding on the study methodology. As briefly mentioned, the different instruments were studied in terms of data capture and analysis.

The methodology for the conduct of the current research paper was developed on the basis of the above evidence.

- To get an overview of several protocols that make network communication possible, the network traffic will first be analyzed. Traffic capture and review for various traffic comprising wired & wireless traffic will also be carried out.
- Then a wired network will be tested in an internet laboratory using a sniffing technique for the current job. In the network, the usual patterns of packet flow will be studied. In order to evaluate their range values and co-relation between them, variables such as protocol types, packet size, flow rate etc will be studied.
- Experiments will be carried out using third-party instruments and the known common scenarios for cyber attacks will be simulated. During cyber attack situations, the differences in packet flow will be observed and contrasted with the ordinary patterns of communication.
- Using network emulation applications such as NS2/ NS3 and GNS3, network communication will be simulated. From a security viewpoint, this will test our perception of networks and simulation possibilities.

Method

Manual examination being tedious, graphical method using software tools is adopted for examination of network content. A network sniffing and analysis tools can be used for the following:-

- Network administrator to troubleshoot network problems.
- Network security engineer to examine security problems.
- Developers to debug for protocol implementations.
- Learners of network protocol internals and network study.
- Detecting uncommon notable network behavior and for finding probable network problems.

3. Results and Discussion

Experiment - Data Collection from Internet Lab

Data processing is carried out from the University Campus Internet laboratory (lab 1). The University Campus layout consists of a firewall in front of the computer. The internet lab is linked with the server via a switch. For individual computers, where the computers are connected through a switch, the .pcap files are captured to get data from the internet lab. As the gateway, one of the PCs in the internet lab is configured and Wireshark is installed for data collection on it. Using this setup, and also from individual PCs in the lab, about 3 GB of data is obtained.

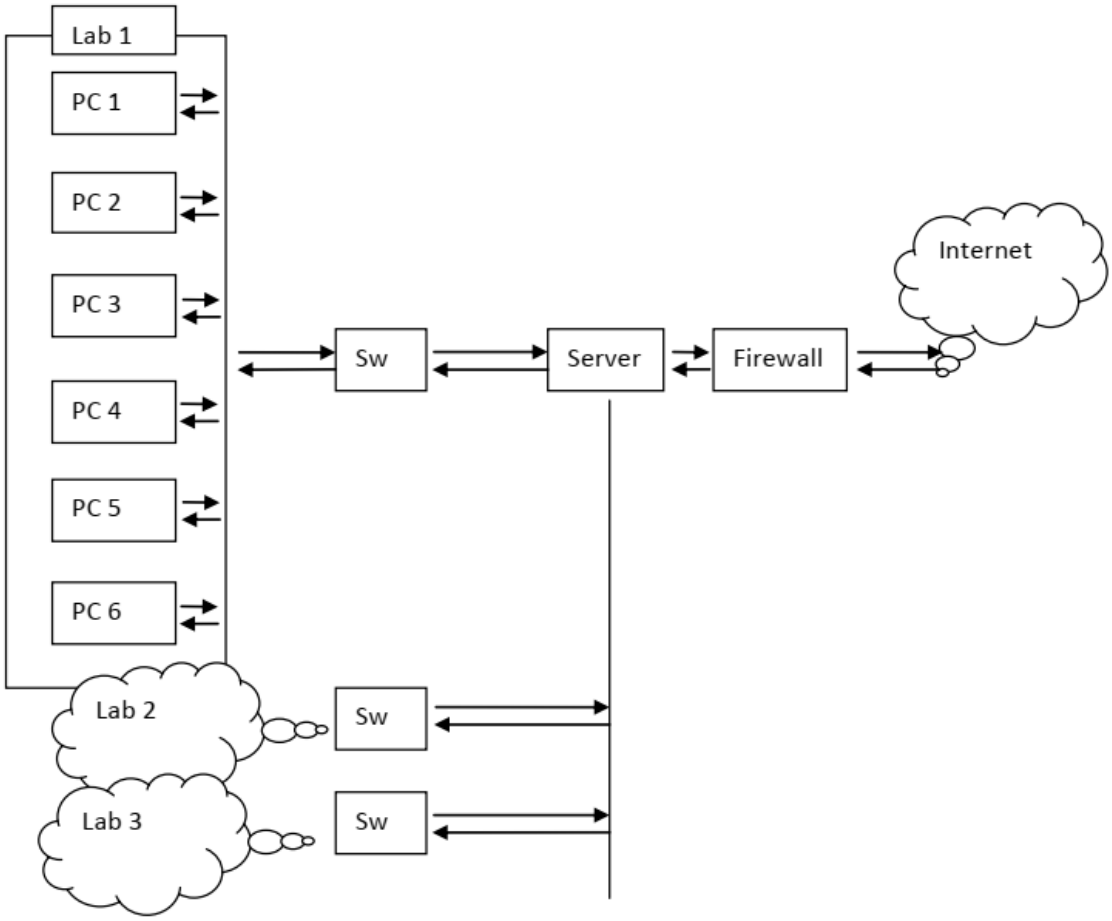

Figure-1 Packet Capture from Internet Lab

Data Collection at the Server

Subsequently, Forti Analyzer software will be used on the University Campus server for a detailed view of network results. Using the app, approximately 65 days of data on the server is analysed. There are 50MBs of report files created using this programme. During normal communication, the data flow rate for the above network of more than 100 packets/sec was observed. The data capture shown in red in Table - 1 indicates network contact when internet access has been interrupted. However, the protocol distribution of various .pcap files that were collected on different computers was pooled for the experiment - data capture, and network configuration was found and also differed between different computers within the University Campus Lab. It is also reiterated that it can be deceptive and should be ignored for studies to record .pcap files that are captured for a very short time.

Table 2 Percentage of Protocols in Various .pcap Files for Experiment

Time Period (s)	Pkts/s	IPv4	TCP	UDP	IPv6
292.415	112.990	59.12%	30.22%	28.30%	22.42%
164.000	57.799	49.76%	15.43%	33.40%	22.70%
2269.578	76.790	39.74%	11.80%	27.47%	20.64%
14.422	50.757	90.85%	84.84%	5.74%	5.05%
112.029	66.358	99.95%	96.95%	2.95%	0.05%
413.338	46.911	63.24%	35.38%	27.77%	19.05%

Scalability Parameter Consideration

The internet has global scalability and smart routing, but it is actually not feasible to capture the entire network graph. This research focuses on the study of packet flow in a network for traffic monitoring from a safety perspective.

For scalability considerations, it is calculated that the outcome of the study can be combined and extrapolated. The scope of this research work therefore involves the establishment, from a security perspective, of a framework for monitoring computer networks.

Variation of Packet Size

Packet sizes are predefined to be within a fixed range that is dependent on the structure of the packet. They are fragmented at the gateways and reassembled at the destination, depending on the Maximum Transmission Unit (MTU). However, it is known that attackers use large numbers of fragmented packets to cause DoS assaults, port scanning, reconnaissance, etc. The scope for this project included a comparative analysis of average packet sizes.

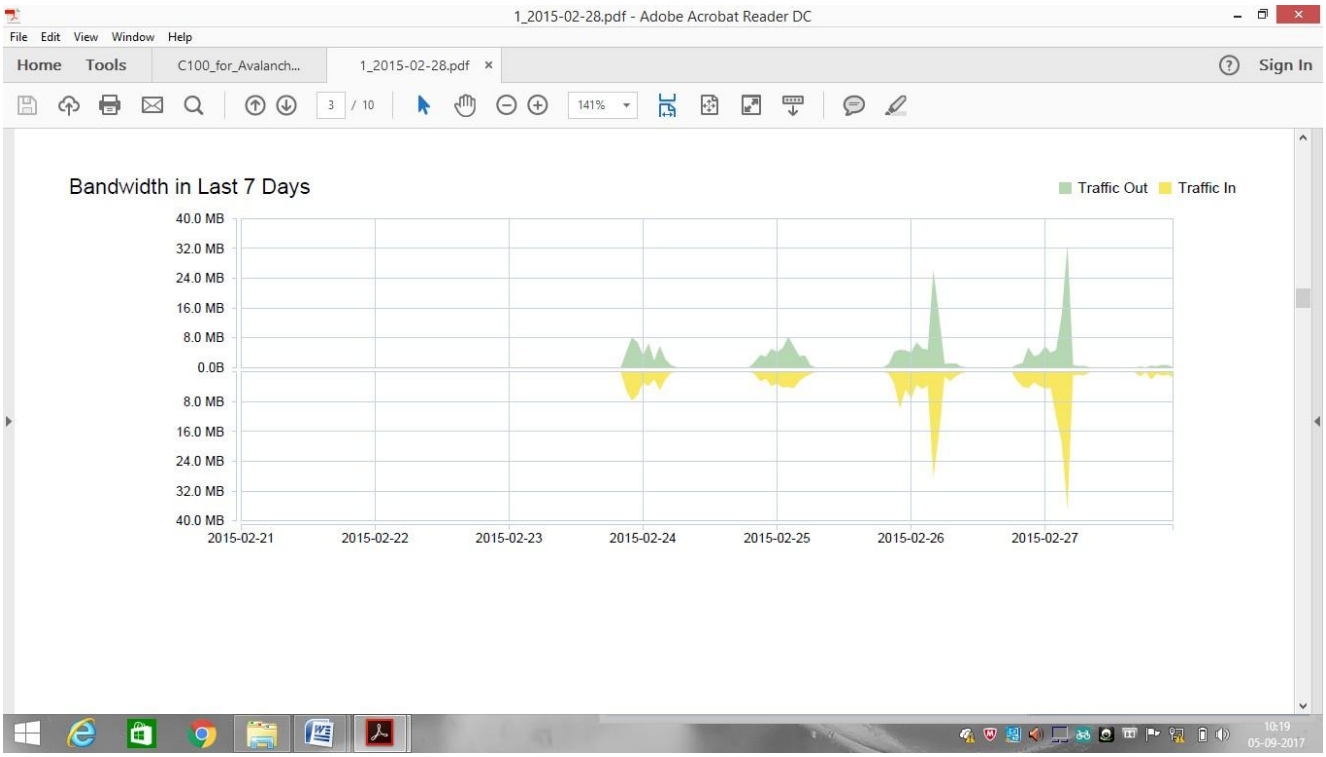

Figure-2 Bandwidth Report using FortiAnalyzer

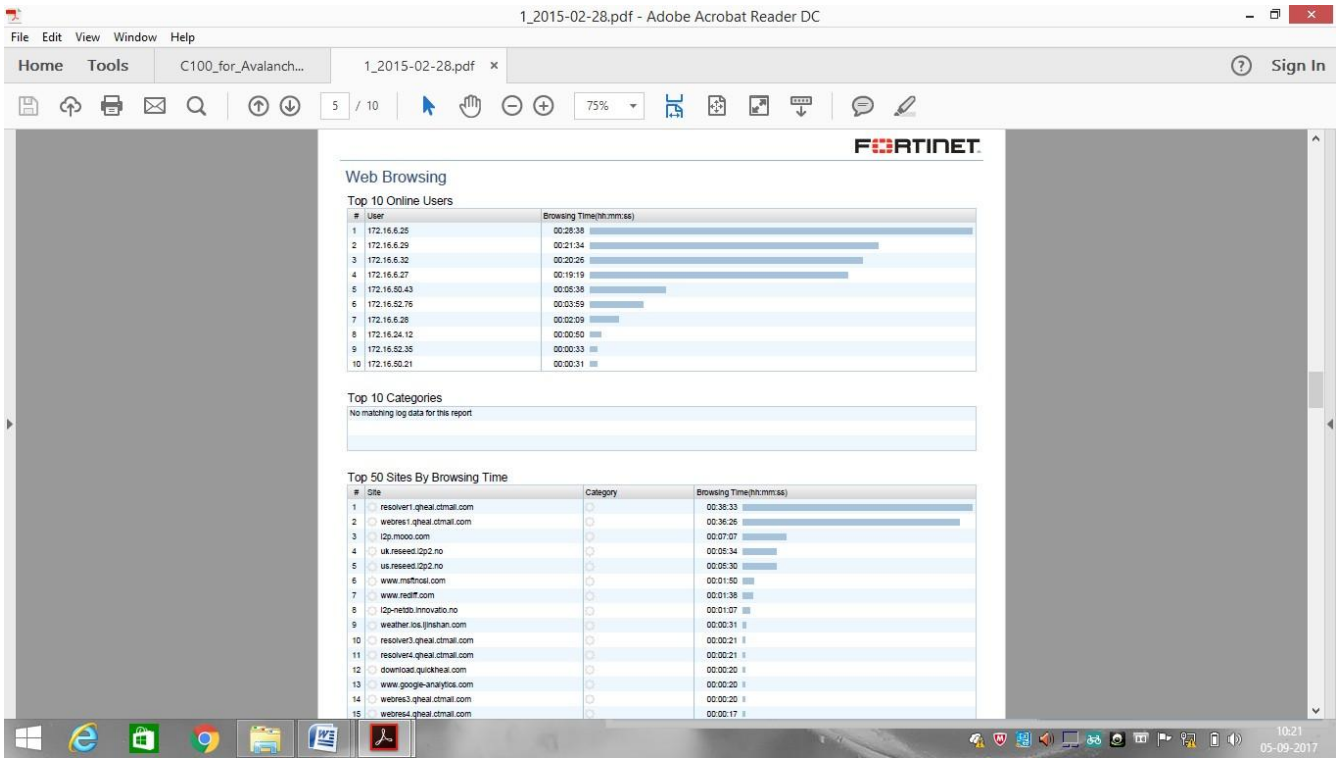

Figure-3 Web Usage Report using FortiAnalyzer

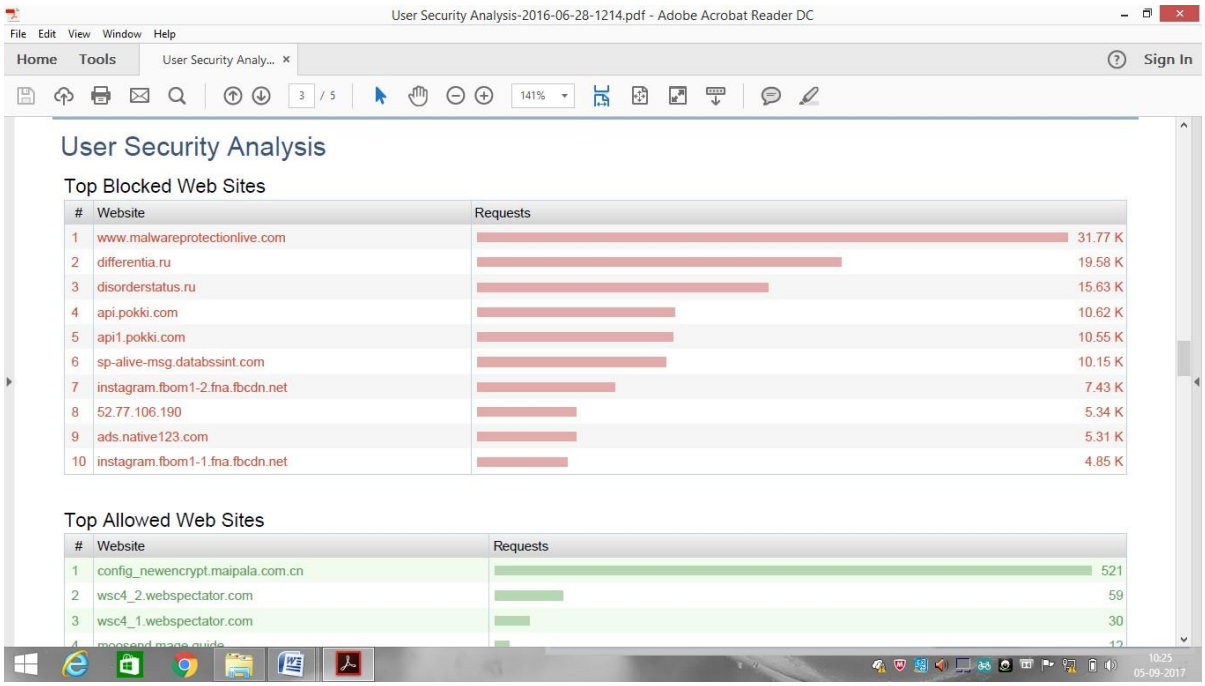

Figure-4 User Security Analysis using FortiAnalyzer

Identifying Potential Cyber Threats

For 40 samples, preliminary traffic capture from the network gateway was performed for 15 to 30 minutes to understand the protocol population within the results. Typical flow patterns and differences in the percentages of the different protocols were observed during the interruption of the internet link during the analysis of the results. In addition, for a span of 65 days, traffic analysis of the entire network at the campus server was conducted. However, any significant shifts in data flow patterns that suspect any abnormal activities have not been found in view of local anti-malware, firewall settings and data capture limitations. The FortiAnalyzer Threat Analysis, which showed no malware, botnets, intrusion, etc., was confirmed.

4. Conclusions

Simulation of Network Result

Network simulation methods such as NS2, NS3 and GNS3 have been used to model network topologies. Using ns3, we simulated by specifying the amount of packet flow between the end points, packet size, transmission medium, time interval, etc. However, the real networks will consist of different protocols, different packet size, different flow time intervals, traffic congestions, etc. Therefore, taking into account the current limitations of simulation software, simulation of complex networks on ns3 and replication of the monitoring parameters as found on real networks was not feasible. Using GNS3, we can simulate network topologies and establish routing, switching and firewall system configurations. The produced packets were captured using Wireshark and analysed.

Some essential protocols of TCP, UDP, ARP and ICMP have been selected for the analysis of irregular data flow during scanning, IP spoofing, enumeration, ARP poisoning, TCP incomplete handshake and ICMP flood, based on the preliminary traffic study of the networks using packet sniffers at the gateway and based on the theoretical study of common cyber attacks that cause deviations in the data flow pattern, TCP, UDP, ARP and ICMP statistical values/percentages, flow rate, average packet size, suspicious/abnormal conversations are chosen to analyse the variations via the wavelet analysis method during the above cyber threats. In terms of spectral elements, wavelet analysis defines an input signal. The existence of anomalies is calculated by examining each spectral window. Wavelets provide a simultaneous definition of time and frequency. The time at which such frequency elements are present is determined by them.

References

1. Jerome Kunegis, "Handbook of Network Analysis", 12 July 2016
2. Jie Lu, "Handling Uncertainties in Big Data by Fuzzy Systems", IEEE International Conferences on Fuzzy System, Aug 2019
3. Dimitris Gritzalis, "History of Information: The case of Privacy and Security in Social Media", Athens, 2014
4. Mafaisu Chewae, Sameer Hayikader, Muhamad Hairulnizam Hasan, Jamaludin Ibrahim, "How much Privacy we still have on Social Network?", International Journal of Scientific and Research Publications, Volume 5, Issue 1, Jan 2018
5. Hsinchun Chen, "Intelligence and Security Informatics for Homeland Security: Information, Communication, and Transportation", 1524-9050/04 IEEE Transaction on Intelligent Transportation Systems, Vol 5, No 4, Dec 2014
6. P.M. Santiago del Rio, "Internet Traffic Classification for High Performance and Off-The-Shelf Systems", 2019
7. Changwei Liu, Anoop Singhal, Duminda Wijesekera, "A Model towards using Evidence from Security Events for Network Attack Analysis"
8. Herkko Hietanen, "Networked Digital Video Recorders and Social Networks", IEEE 2009

9. Felix Erlacher, "Network Monitoring for Todays Internet" Mohan V Pawar and Anuradha J, "Network Security and Types of Attacks in Network", International Conference on Intelligent Computing, Communication and Convergence (ICCC-2015), www.sciencedirect.com, 48 (2015) 503-506
10. Pavel Celeda, "Network Security Monitoring and Behavior Analysis", CESNET led Working Group, GN3-NA3-T4-CBPD133, Sep 2011
11. Gustavo J A M Carneiro, "Network Simulator 3", Labmeeting 2010-04-20
12. J. Svoboda, "Network Traffic Analysis with Deep Packet Inspection Method", 2014
13. H. Kapri, "Network Traffic Data Analysis", Dec 2011
14. "ns-3 Tutorial Release ns-3.26", Oct 04, 2016
15. Hansen et al, "Numbers, Facts and Trends Shaping the World", Pew Research Center, www.pewresearch.org
16. Joseph Gehring, "Packet Analysis using Wireshark", CNT 4104, Florida Gulf Coast University, Dec 13, 2011
17. Shafi'i M Abdulhamid, Sulaiman Ahmad, Victor O Waziri and Fatima N Jibril, "Privacy and National Security Issues in Social Networks: The Challenges", International Journal of the Computer, The Internet and Management Vol 19 No 3 (Sep-Dec, 2011) pp 14-20

