International Journal of Electrical and Computer Engineering (IJECE)
Vol. 6, No. 1, February 2016, pp. 235~241
ISSN: 2088-8708, DOI: 10.11591/ijece.v6i1.9013

QoS Design Consideration for Enterprise and Provider's Network at Ingress and Egress Router for VoIP Protocols

Manjur Kolhar*, Mosleh M Abualhaj, Faiza Rizwan***
* Dept. Computer Science and Information, Prince Sattam Bin Abdulaziz University, Wadi Ad Dwaser, Kingdom of Saudi Arabia
** Dept. of Network and Information Security, Faculty of Information Technology
Al-Ahliyya Amman University, Amman, Jordan

Article Info

Article history:

Received Sep 13, 2015
Revised Nov 15, 2015
Accepted Dec 3, 2015

Keyword:

MPLS
QoS
VoIP
VPN

ABSTRACT

Compliance with the Service Level Agreement (SLA) metric is a major challenge in a Multiprotocol Label Switching Virtual Private Network (MPLS VPN) because mandatory models must be maintained on both sides of the MPLS VPN in order to achieve end-to-end service levels. The end-to-end service of an MPLS VPN can be degraded owing to various issues such as distributed denial of service (DDoS), and Random Early Detection (RED) that prevents congestion and differentiates between legitimate and illegitimate user traffic. In this study, we propose a centralized solution that uses a SLA Violation Detector (SLAVD) and intrusion detection to prevent SLA violation.

Corresponding Author:

Mosleh M Abualhaj,
Dept. of Network and Information Security, Faculty of Information Technology
Al-Ahliyya Amman University,
Amman, Jordan
Email: m.abualhaj@ammanu.edu.jo

1. INTRODUCTION

Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) technology has enabled the service provider network and enterprise network to agree on common terms for the provision of end-to-end service levels. This agreement is the key factor in the increasing preference for MPLS VPN technology. MPLS VPN elements such as customer edge (CE) router and provider edge (PE) router play a pivotal role in managing the service level agreements (SLAs) between the enterprise and provider networks. Figure 1 shows the MPLS VPN architecture to achieve end-to-end QoS. End-to-end QoS is achieved by applying various policies to the PE and CE [1, 2]. In this study, we investigate the policies that can achieve the best QoS. Numerous issues prevent the provider from achieving the agreed service levels. These issues can be classified as technical issues and threats. The standard technical issues are TCP starvation [3], Random Early Detection (RED) [4] to avoid congestion, and the mixing of TCP and UDP protocols. These technical issues cause underperformance in the provider network. Further, threats affect the ability of the provider network to achieve agreements. Numerous threats hamper the performance of the provider network and enterprise network. Among these threats, Distributed Denial of Service (DDoS) is considered to be extremely dangerous because it floods the CE and PE networks [5]. In such situations, the compliance with agreements on a VoIP network becomes extremely critical and challenging. Hence, this study proposes architecture to provide seamless connectivity between the endpoints via the service provider network.

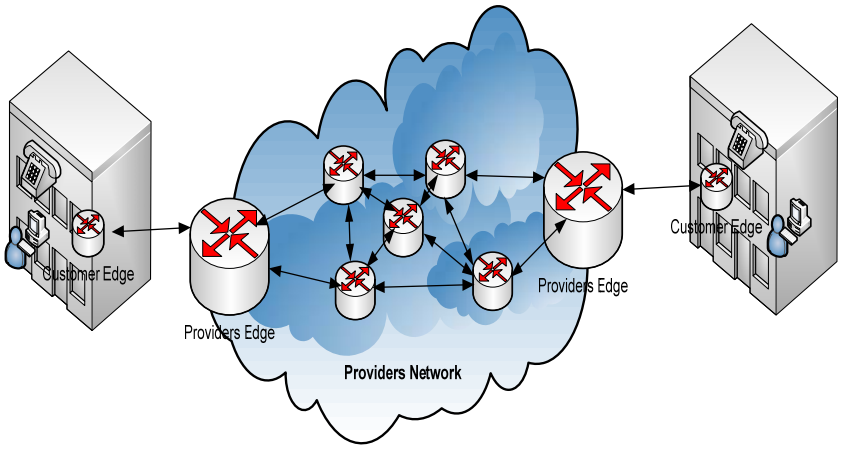

Figure 1. MPLS VPN Architecture

The standard SLA agreement specifies the maximum one-way latency from the mouth to ear, maximum jitter, and maximum packet loss as 150 ms, 30 ms, and 1%, respectively [6]. In order to meet this challenge of providing service to the endpoints, we should agree on common terms such as mapping models between the enterprise and provider networks. The most important task is to assign priority class of service to the carriers of real-time data. Hence, the VoIP network should have the highest priority for signaling and video traffic. In addition, signaling plays an important role in a VoIP network although it does not use a real-time protocol as its carrier. However, in order to achieve the SLA for the signaling, the PE must provide the best service even for non-real time traffic; further, the traffic (bandwidth requirement) for signaling is negligible when compared with the RTP data for audio and video. Differentiated service (DiffServ), another element of an MPLS VPN, involves the marking and remarking of traffic (classification and management of traffic) to provide QoS. In the case of DiffServ, both the sides of an MPLS VPN are responsible. The enterprise network must adopt the methods and policies applied by the provider network. For example, if expedited forwarding (EF) is used to shape the traffic of video, audio, and signaling, it should be a common feature between CE and PE routers. Traffic mixing of TCP and UDP should not be used because it will starve TCP. Therefore, signaling and real-time data must use a single protocol. Thus, we can conclude that, to achieve QoS for an MPLS VPN with VoIP protocol, the following points are important.

- Service Level Agreement.
- Signaling should be marked as real time.
- Not mixing of UDP and TCP.
- Marking and remarking of Traffic.

2. LITERATURE SURVEY

In [7], the authors propose delay margin-based traffic for the MPLS network, and suggest three algorithms to achieve end-to-end QoS in MPLS networks. In [8], the authors propose that MPLS and DiffServ are the only elements that provide QoS for multimedia traffic by using network resources effectively. Further, they utilize label switched paths to measure the network state in order to adapt network configurations to changing traffic conditions. In [9], the authors prove that merging IP and WDM will not automatically handle traffic that is adaptive in nature. Further, they show that their proposed network efficiently adapts to the changes in traffic patterns that disrupt its operation. They apply QoS end-to-end functions in their proposed network. In [10], the authors use pre-congestion and notification to provide feedback about load conditions on the path to the boundary nodes. Further, they utilize this information to propose lightweight admission control and flow termination, and do not use the knowledge of per-flow state on interior nodes; hence, they avoid using DiffServ to achieve the QoS for the proposed network. In [11], the authors propose provisioning techniques for a mesh network, and use link vector techniques to explore the sharing potential among backup paths and achieve bandwidth-assignment flexibility. In [12], the manuscript describes layer 2 tunneling techniques such as MPLS-based tunnels to establish an end-to-end VPN service by merging the services offered by various network domains along the path between end users. In [13], the authors use delay-based congestion detection and admission control for voice quality in enterprise networks. In [14], the SLA is used to provide QoS by utilizing the elements of SLA such as connection holding time to

improve the routing efficiency. In [15], the authors describe the routing mechanism of Ethernet-specific load balancers, which is active for dynamic traffic demands. This mechanism significantly reduces overprovisioning, and requires only the bandwidth profiles associated with SLAs at the PE and CE. In [16], the authors describe a method to reduce network cost with improved bandwidth efficiency, and offer practical options for internetworking during the migration. In [17], the authors propose Virtual Network-based DiffServ/MPLS III transport network architecture for scalable IP service deployment and efficient network resource management. In [18], the authors propose a QoS management and control system that combines two services, such as service admission control and the rate feedback control, and uses the combination to maintain the preset QoS parameters in the backbone network of the provider. In [19], the authors describe a new Rate Control Scheme, RCS, for real-time applications in networks with high bit error rates. RCS uses dummy packets to probe the availability of network resources.

In summary, every study focuses on one of the above mentioned aspects to achieve QoS on an MPLS VPN. However, previous studies have not used these aspects to create an architecture for real-time traffic. Our MPLS VPN architecture uses all these aspects in the CE and PE networks to obtain end-to-end QoS.

3. PROPOSED ARCHITECTURE

Figure 2 shows the proposed architecture for achieving QoS for MPLS VPN at CE and PE routers. We performed an initial study on VoIP protocols, and determined that the Session Initiation Protocol (SIP) is the most suitable protocol for our proposed architecture. SIP can be used to create, modify, and disconnect an SIP session between two or more remote parties [20]. Further, SIP has been used in various comparison tests with the Inter Asterisk protocol and ITU-based protocol, H.323 [21-22]. SIP performed better than these other protocols under various network impairments that were induced by using the NetEm tool. SIP is only a signaling protocol, and the real-time data transmission of audio and video traffic is performed by RTP over UDP [23-24]. SIP media negotiation can be performed with the Session Description Protocol.

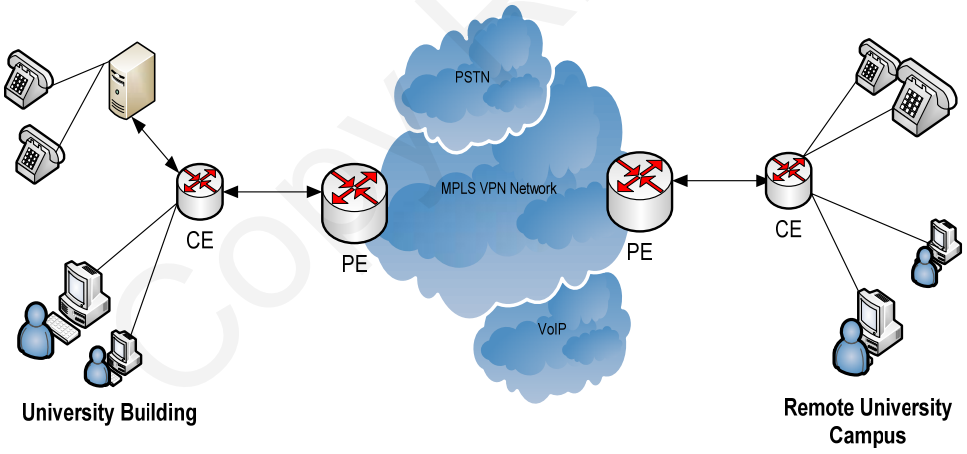

Figure 2. Proposed Architecture

The proposed architecture must avoid DDoS attacks by using the Intrusion Detection system (IDS), and real-time media transmission should comply with the SLA agreement and routers that have capabilities to mark and remark traffic. Our SIP server is equipped to provide an authentication-based service. SIP clients are software-based and hardware-based IP phones, and Public Service Telephone Network (PSTN) phones. The SLA can be compromised by DDoS attacks, and marking and remarking of traffic; however, one-way delay should not be considered owing to the synchronization problem and asymmetric links [25]. An SLA violation cannot be verified and rectified at core routers because they serve the provider network according to the DS field of DiffServ. Hence, it is mandatory for PEs and CEs to be equipped for the detection and correction of SLA violations. Our proposed architecture uses an SLA system to detect attacks that cause an MPLS VPN to violate the SLA agreement. Figure 3 shows the architecture for SLA violation detector.

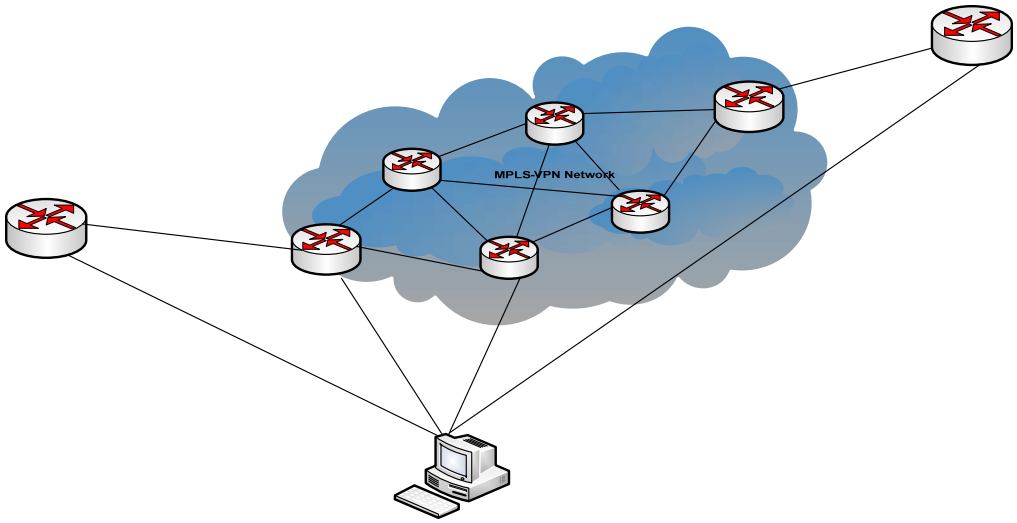

Figure 3. SLA Violation Detector

Our proposed SLA Violation Detector (SLAVD) will monitor traffic across the MPLS VPN edge routers of the provider network and enterprise network. The SLA violations that are detected in the SLAVD system are:

- Higher than the SLA bit rate.
- Illegitimate and Legitimate users.
- DDoS attack.

3.1. SLAVD

SLAVD assumes that real-time traffic will use the assigned IP and ports for VoIP. The bandwidth is calculated to ensure that each user obtains the agreed bandwidth. SLAVD is responsible for measuring the traffic and taking necessary actions if a user exceeds the bandwidth. If the Ingress router receives a VoIP packet, the router copies the header in order to calculate the delay. If the delay between the PE and CE is determined to be large, it is reported to the SLAVD for further action. When the SLAVD receives the investigation report of the delay between the ingress and egress routers, it reloads the IPtables for that particular route. In addition, SLAVD detects overflooding users. However, it is extremely difficult to identify the victim or intruder. SLAVD comes to the rescue of the user who may be a victim or intruder. This case is considered to be a special one, and this report is provided to the IDS for further investigation.

The ingress router may receive less bandwidth of data owing to a global attack or RED as part of congestion control [26]. The ingress router buffers the packet to the greatest extent possible, and drops the packet if the threshold is reached. These dropped packets may affect the QoS of the PE and CE. When the SLAVD learns about the RED and global attack, it reduces the traffic width between the PE and CE. When this abnormality ceases to exist, the SLAVD resets the traffic between the PE and CE.

3.2. SLA Parameter Measurements

The basic SLA parameters are delay, loss, and throughput. We classify the traffic measurement as intrusive and non-intrusive. An intrusive traffic method requires the alteration of the traffic flow between the PE and CE routers, whereas a non-intrusive method would require injection of dummy packets between the PE and CE. These methods introduce additional delay in the system [27, 28], and hence, we do not consider these methods of delay calculation. We use the equation 1 for calculating the delay between the PE and CE.

$$\text{Total Delay} = (Tp_{CE} - Tp_{PE}) \quad (1)$$

According to Equation 1, Tp CE is the time taken by the packet at the CE router, and Tp PE is the time taken by the packet at the PE router. If the total delay is found to be more than the SLA bit rate, the SLAVD will perform an appropriate action according to the report. Packet loss is the number of packets sent to the ingress router by the egress router. It can be calculated from equation 2:

Packet Loss = Packet Sent – Packet Received (2)

Similarly, average packet loss is computed from equation 3:

Average packet loss = (Avg pket Sent – Avg Pket Recd)/ Avg Pket Sent (3)

3.3. SLA Parameter Measurements

The RED and Weighted RED (WRED) queue management policy cause the egress router to drop packets. A DDoS attack in the network at this time is considered to be the worst-case scenario. The performance is already degraded owing to the queue policy, and it degrades further because of the DDoS attack. However, our SLAVD is equipped with the open-source Snort IDS to protect the CE from the DDoS attacker. If an enterprise network node is misbehaving or is a victim of a DDoS attack, its bandwidth is measured; if the bandwidth consumed exceeds the value in the SLA agreement, it is considered to be a victim or intruder. Figure 4 shows the expanded version of the proposed system. It consists of the Snort IDS, and traffic is diverted from the ingress router to the SLAVD system. The SLAVD system is used to avoid threats and to maintain the QoS metrics mentioned in the SLA agreement between the CE and PE networks. Our proposed network has been implemented at our university. In order to measure and induce loss, packet delay, and throughput we used the Network Emulator, NetEm.

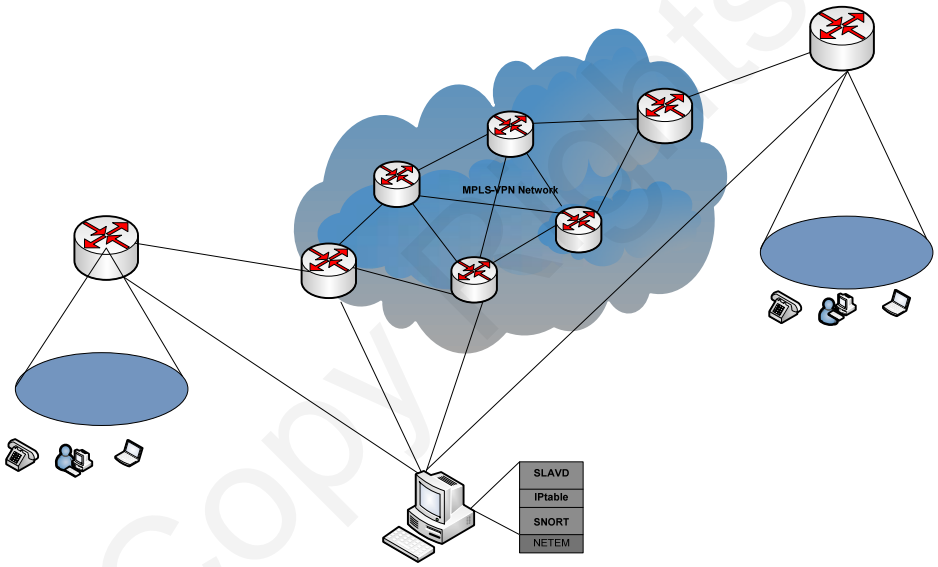

Figure 4. Expanded version proposed network architecture

4. CONCLUSION

The architecture proposed in this manuscript consists of network elements such as SLVD, NetEm, and IPtables. We have strived to create a simple architecture so that it can be implemented easily, and the QoS metric can be measured without additional efforts or network elements. The delay caused by the redirection of traffic from the ingress router to the SLAVD instead of directly to the egress router is minimal. If the ingress router is equipped with the IPtables configuration, then, the IPtables configuration at the SLAVD can be removed. We measured the loss, delay, and throughput between the PE and CE; these values are found to be adequate to ensure non-violation of SLA metrics. When packet reordering and simultaneous flooding of packets occur in a network, they will cause loss, delay, and change in throughput; however, these values satisfy the QoS metrics.

In the future work, we will further classify traffic according the threats such as virus, botnets and DDoS. More-ever we try to port anti-threats module at SLAVD so that it can take instant action.

REFERENCES

[1] CISCO, "*Enterprise QoS Solution Reference Network Design Guide*", San Jose: CISCO, 2005, pp. 5-1.

[2] Haeryong Lee; Jeongyeon Hwang; Byungryong Kang; Kyoungpyo Jun, "*End-to-end QoS architecture for VPNs: MPLS VPN deployment in a backbone network*," Parallel Processing, 2000. Proceedings. 2000 International Workshops on , vol., no., pp. 479, 483, 2000
[3] Widmer, J.; Denda, R.; Mauve, M., "A survey on TCP-friendly congestion control", *Network, IEEE*, vol.15, no.3, pp. 28, 37, May 2001
[4] Baklizi, Mahmoud, Hussein Abdel-Jaber, Ahmad Adel Abu-Shareha, Mosleh M. Abualhaj, and Sureswaran Ramadass, "Fuzzy logic controller of gentle random early detection based on average queue length and delay rate", *International Journal of Fuzzy Systems*, Vol. 16, No. 1, pp. 9, 19 March 2014.
[5] Zargar, S.T.; Joshi, J.; Tipper, D., "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks". *Communications Surveys & Tutorials, IEEE*, no. 99, pp. 1, 24, March 2013
[6] Janssen, Jan, Danny De Vleeschauwer, and Guido H. Petit. "*Delay and distortion bounds for packetized voice calls of traditional PSTN quality*", Proceedings of the 1st IP Telephony workshop (IPTEL 2000). 2000.
[7] Ashour, Mohamed; Tho Le-Ngoc, "Delay-margin based traffic engineering for MPLS-DiffServ networks", *Communications and Networks, Journal of*, vol.10, no.3, pp.351,361, Sept. 2008
[8] Anjali, T.; Scoglio, C.; de Oliveira, J.C., "New MPLS network management techniques based on adaptive learning", *Neural Networks, IEEE Transactions on*, vol.16, no.5, pp.1242,1255, Sept. 2005
[9] Androulidakis, S.; Doukoglou, T.; Patikis, G.; Kagklis, D., "Service Differentiation and Traffic Engineering in IP over WDM Networks", *Communications Magazine, IEEE*, vol. 46, no. 5, pp. 52, 59, May 2008
[10] Menth, M.; Briscoe, B.; Tsou, T., "Precongestion notification: new QoS support for differentiated services IP networks", *Communications Magazine, IEEE*, vol. 50, no. 3, pp. 94, 103, March 2012
[11] Lei Song; Jing Zhang; Mukherjee, B., "Dynamic provisioning with availability guarantee for differentiated services in survivable mesh networks", *Selected Areas in Communications, IEEE Journal on*, vol. 25, no. 3, pp. 35, 43, April 2007
[12] Saad, T.; Alawieh, B.; Mouftah, H.T.; Gulder, S., "Tunneling techniques for end-to-end VPNs: generic deployment in an optical testbed environment", *Communications Magazine, IEEE*, vol. 44, no. 5, pp. 124, 132, May 2006
[13] Burst, Ken; Joiner, L.; Grimes, Gary, "Delay Based Congestion Detection and Admission Control for Voice quality in enterprise or carrier controlled IP Networks", *Network and Service Management, IEEE Transactions on*, vol. 2, no. 1, pp. 1, 8, Nov. 2005
[14] Tornatore, M.; Baruffaldi, A.; Hongyue Zhu; Mukherjee, B.; Pattavina, A., "Holding-Time-Aware Dynamic Traffic Grooming", *Selected Areas in Communications, IEEE Journal on*, vol. 26, no. 3, pp. 28, 35, April 2008
[15] Van Haalen, R.; Malhotra, R.; de-Heer, A., "Optimized routing for providing ethernet LAN services", *Communications Magazine, IEEE*, vol. 43, no. 11, pp. 158, 164, Nov. 2005
[16] Hache, L.; Li Li, "Unified control infrastructure for carrier network evolution", *Communications Magazine, IEEE*, vol. 38, no. 11, pp. 74, 77, Nov 2000
[17] Yu Cheng; Farha, R.; Tizghadam, A.; Myung-Sup Kim; Hashemi, M.; Leon-Garcia, A.; Hong, J.W.-K., "Virtual network approach to scalable IP service deployment and efficient resource management", *Communications Magazine, IEEE*, vol. 43, no. 10, pp. 76, 84, Oct. 2005
[18] Dongli Zhang; Ionescu, D., "Measurement and Control of Packet Loss Probability for MPLS VPN Services", *Instrumentation and Measurement, IEEE Transactions on*, vol. 55, no. 5, pp. 1587,1598, Oct. 2006
[19] Akyildiz, I.F.; Akan, O.B.; Morabito, G., "A rate control scheme for adaptive real-time applications in IP networks with lossy links and long round trip times", *Networking, IEEE/ACM Transactions on*, vol. 13, no. 3, pp. 554,567, June 2005
[20] Session Initiation Protocol RFC 3261.
[21] Abu-Alhaj, Mosleh M., S.K. Manjur, R. Sureswaran, Tat-Chee Wan, Imad J. Mohamad, and Ahmed M. Manasrah. "ITTP: A New Transport Protocol for VoIP Applications", *International Journal of Innovative Computing, Information and Control (IJICIC)*, vol. 8., no. 3, pp 1–10-12026., March 2013.
[22] AbuAlhaj, Mosleh, et al. "*Multiplexing SIP applications voice packets between SWVG gateways*", Proceedings of International Conference on Computer Engineering and Applications (ICCEA 2009). 2009.
[23] Abu-Alhaj, Mosleh M., et al. "Delta-Multiplexing: A Novel Technique to Improve VoIP Bandwidth Utilization between VoIP Gateways", *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on. IEEE*, 2010.
[24] Abu-Alhaj, Mosleh, et al. "MuxComp-A New Architecture to Improve VoIP Bandwidth Utilization", *Future Networks, 2009 International Conference on. IEEE*, 2009.
[25] Ahsan Habib, Sonia Fahmy, Srinivas R. Avasarala, Venkatesh Prabhakar, Bharat Bhargava, On detecting service violations and bandwidth theft in QoS network domains, *Computer Communications*, Volume 26, Issue 8, 20 May 2003, Pages 861-871
[26] Floyd, Sally; Jacobson, V., "Random early detection gateways for congestion avoidance", *Networking, IEEE/ACM Transactions on*, vol. 1, no. 4, pp. 397, 413, Aug 1993.
[27] Wei-Zhou Lu, Wei-Xuan Gu, Shun-Zheng Yu, One-way queuing delay measurement and its application on detecting DDoS attack, *Journal of Network and Computer Applications*, Volume 32, Issue 2, March 2009, Pages 367-376,
[28] Hong-hua Zhao; Ming Chen, "Network Topology Inference Based on Delay Variation", *Advanced Computer Control, 2009. ICACC '09. International Conference on*, vol., no., pp. 772, 776, 22-24 Jan. 2009

BIOGRAPHIES OF AUTHORS

Dr. Manjur Kolhar (m.kolhar@psau.edu.sa) received his Bachelor of Science from KUD, INDIA in 1999 and Master in Computer Applications system from KUD, India in 2001, received PhD degree from National Advanced IPv6 Centre (NAV6) in Universiti Sains Malaysia (USM). In 2010. He has published more than 25 research papers in International Journals and Conferences of high repute. His research interest includes advanced Computer networks and security and cloud computing resource management.

Dr. Mosleh M. Abu-Alhaj is a senior lecturer in Al-Ahliyya Amman University. He received his first degree in Computer Science from Philadelphia University, Jordan, in July 2004, master degree in Computer Information System from the Arab Academy for Banking and Financial Sciences, Jordan in July 2007, and doctorate degree in Multimedia Networks Protocols from Universiti Sains Malaysia in 2011. His research area of interest includes VoIP, Multimedia Networking, and Congestion Control. Apart from research, Dr. Mosleh M. Abu-Alhaj also does consultancy services in the above research areas and directs the Cisco academy team at Al-Ahliyya Amman University.

Faiza Rizwan completed Bachelor of Science in Computer Application from Patna Women's College, India in 2002. Completed Master of Computer Application from L.N. Mishra Institute of Economic Development and Social Change, Patna, India in 2005. Working as Lecturer in Computer Science & Information department in College of Arts and Science, Women in Prince Sattam Bin Abdulaziz University, Wadi Addawasir, since February 12 to till Date. I have interested in database, software development and user interface.