Review of Computer Engineering Research
2020 Vol. 7, No. 2, pp. 54-61.
ISSN(e): 2410-9142
ISSN(p): 2412-4281
DOI: 10.18488/journal.76.2020.72.54.61

QUALITY ASSESSMENT AND MONITORING OF NETWORKS USING PASSIVE TECHNIQUE

Abiola Olawale Ilori[1+]
Omoniyi Ajoke Gbadamosi[2]
Oluwafemi Clement Adeusi[3]

[1]*Department of Physical Sciences, Olusegun Agagu University of Science and Technology, Okitipupa, Nigeria.*
[1]*Email: iloriabiola99@gmail.com Tel: +2348036381583*
[2,3]*Department of Mathematical Sciences, Olusegun Agagu University of Science and Technology, Okitipupa, Nigeria.*
[2]*Email: gbadamosiajoke2015@gmail.com Tel: +2349068438014*
[3]*Email: adeusic@gmail.com Tel: +2348039546721*

(+ Corresponding author)

Article History
Received: 13 July 2020
Revised: 17 August 2020
Accepted: 3 September 2020
Published: 24 September 2020

Keywords
Assessment
Computer
Monitor tools
Network
Passive measurement
Performance.

ABSTRACT

Continuous evaluation and monitoring of the network are essential for assessing the network's performance level, and at the same time, it helps to identify and locate problems within the network. This study focuses on the general state of passive network measuring techniques, principally due to its reputation in terms of assessing and monitoring with a high level of accuracy. Olusegun Agagu University of Science and Technology Okitipupa Nigeria network was used as a real-life case study of how the network is being passively monitored and evaluated. For the study, Capsa network analyzer and a double network card splitter were used as the passive tool. Packet size, one-way delay, and packet fragmentation were metrics assessed on the University's network. Although the capturing device was synchronized with the network, captures are quite short, with some negative values, so the clocks are not simultaneous in the process. However, passive tools were reported to assess and monitor the network's performance efficiently and effectively.

Contribution/Originality: This study is one of the very few studies which have investigated passive measuring techniques as a tool in the assessment and monitoring of networks. The study reported values with a high level of accuracy. Hence, passive tools are effective in the assessment and monitoring of the network's performance.

1. INTRODUCTION

The network had become the bedrock of many organizations and institutions' success since they all now rely on internet facilities to administer their efficiency and effectiveness [1-3]. The network is getting increasingly complex though it is the core necessity for internet facilities. Managing the network of a giant or ordinary public or private enterprise is mostly a dynamic challenge for service providers [4, 5].

All network protocols are now multilayered within modern internet facilities. Also, many of today's internet applications need fast and precise network facilities for optimal performance. The speed of connections is continuously growing and increasing day-by-day; hence there is a need for networking to work effectively with adequate security to protect organizations' confidentiality and integrity. In the same light, it must provide cost-effectiveness in its architecture with network availability.

This implies that there must be no leakage across the network, between specific private or public network services [6]. Therefore, packet breakage should not occur within the network, and the network's speed must be

efficiently constant at all instances [7, 8]. The network operators track the network's quality, and most of the time, their main problems are ensuring that intruders do not have a hole to penetrate or exploit it. The passive technique of network quality assessment and monitoring tools are very suitable for these purposes in tackling the challenges of data theft or leakage in a network, thereby providing an active and efficient service [9, 10].

Accurate assessment, monitoring, and diagnosis of network traffic and its devices were not too successful due to the frequently usually employed in active monitoring technique [8]. Most preliminary work on assessing the Internet structure was based on dynamic assessment tools that use tomographic testing or test packets, which do not capture all traffic network loss packets [11, 12]. Therefore, the passive assessment technique has been deployed for its perceived quality and effectiveness since user traffic is observed without inserting additional test traffic (probe packets) into the Network [13, 14].

Passive network assessment tools are used to check for problems from a single network computer, identify all issues affecting the whole network, and diagnose and repair some of the network's issues based on the information available about the situation [15, 16]. This is also useful for network performance assessments and for creating metrics for network output assessments [17]. There are passive tools for assessing and tracking network characteristics, which are both hardware and software tool-based. Passive tools for network assessment and monitoring are often incorporated into some networking devices such as routers and switches. Most of the built-in passive monitoring tools cannot operate effectively and efficiently, like stand-alone tools. Passive assessment and monitoring of the network is required and should be carried out more frequently for the following essential reasons. Firstly, it provides the vast resources necessary for assessing the network output from a different perspective to recognize any strategic issues which may emerge, such as delays, levels of unreliability, quality of service needed, etc. Secondly, passive assessing tools are used to provide background network output assessments useful for network operators and those charged with delivering network services.

Passive assessment techniques have proved capable of reliably calculating a network's output in its capacity to collect data on the operating network without altering the network's activities [18]. This technique gathers enough traffic that can be used to measure and monitor the routine and performance of an extensive area network as well as the local area network [18, 19]. Assessing and forecasting network efficiency is crucial to a grid application performance, and many other distributed computing uses. The importance of this domain was reflected in the vast number and range of assessment tools developed.

Over the years, Olusegun Agagu University of Science and Technology Okitipupa (OAUSTECH) have found it challenging to provide an efficient and comprehensive network service to its public (staff and students). There has been a lot of misunderstanding between the University's management and the student over providing an adequate internet facility year-on-year and out. Following the above scenarios, this study would be critical in such a way that it will provide valuable information and data on the assessment and monitors the University network using passive tools as the best technique in delivering quality network services. This study focuses on the general state of passive assessment tools regarding network monitoring, assessment, diagnosis, and network performance testing. It gathers data from different points within the University Network and deducing weak points in the network.

2. METHODOLOGY

2.1. The Core Sampling Network

In this study, a passive tool was used to assess and monitor the internet network setup of Olusegun Agagu University of Science and Technology Okitipupa. The University's server was connected to a central network, as shown in Figure 1, with the sampling points for this study in Table 1. This work was carried out based on the primary data from the assessments and monitoring of OAUSTECH's network in September 2017.

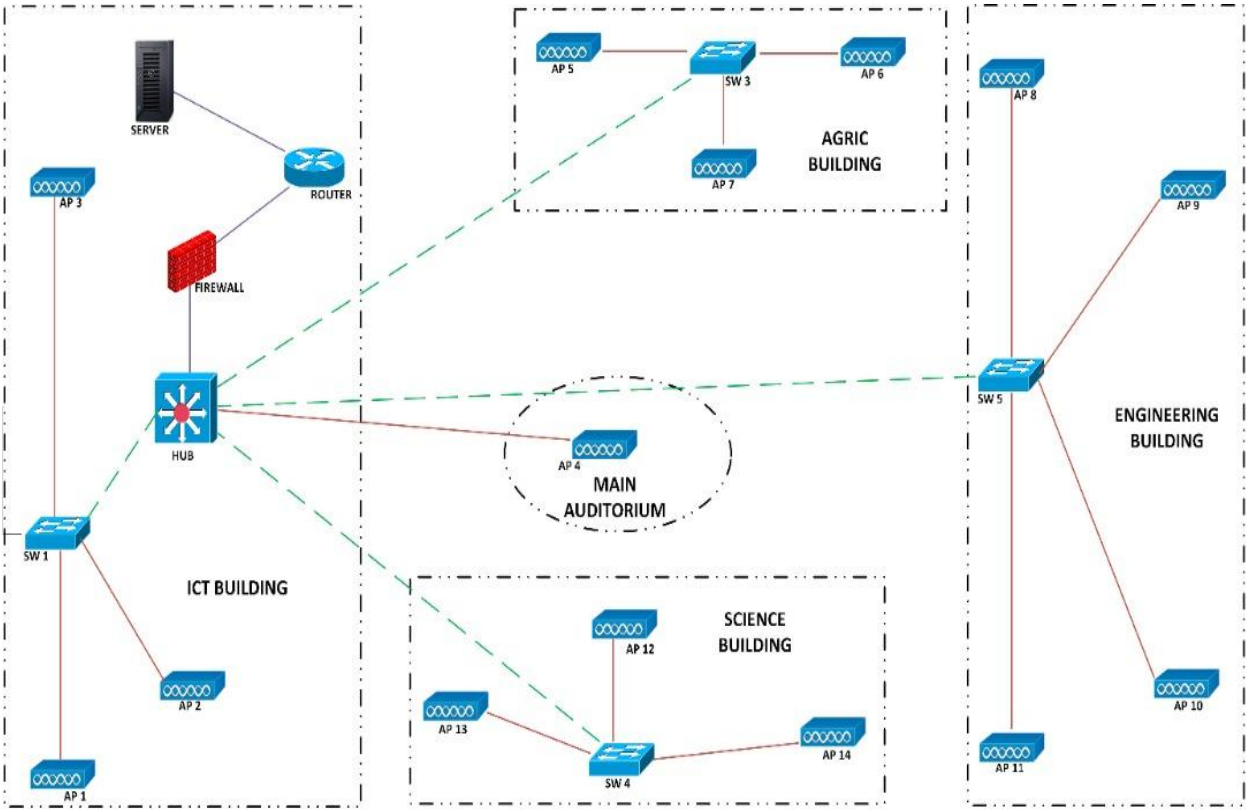

Figure-1. The Sampling network.

Table-1. GPS Locations of the sampling points within the study area.

Sampling Points	Latitude	Longitude	Locations
Access point 01	4.76487822	6.45921756	First-floor ICT
Access point 02	4.76509997	6.45919424	Second-floor ICT
Access point 03	4.76517979	6.45922351	Second-floor ICT
Access point 04	4.76415983	6.45878624	Main auditorium
Access point 05	4.76523866	6.45971597	Second floor Agric
Access point 06	4.76535548	6.45974129	Ground floor Agric
Access point 07	4.76523866	6.45971596	First floor Agric
Access point 08	4.7652666	6.45983436	Engineering A (first floor)
Access point 09	4.7654851	6.45988431	Engineering (second floor)
Access point 10	4.76605894	6.45956735	Engineering (ground floor)
Access point 11	4.76563885	6.45980534	Engineering B (first floor)
Access point 12	4.76540282	6.4594528	Science (ground floor)
Access point 13	4.76555687	6.45952108	Science A(second floor)
Access point 14	4.76517979	6.45922351	Science B (second floor)

The methodology adopted in this study is the quantization of packets at different captured points of the University network, as shown in Figure 1. It entails details as traffic enters and exits the core network and evaluates the one-way delay (OWD) of in / out traffic within the network. The links at the edge router of the core network of the University have speeds of one gigabit, which was initially checked, and work efficiently.

2.2. System Requirements for the Capturing Computer

The computer used as the passive capturing tool in the study has the following configurations: 500G SATA HDD, 8.00GB RAM, a single processor of speed at 2.40GHz, and a Core (TM) i3 Intel (R) processor and installed 64-bit Linux OS Kernel 2.6.8. Other items include 10/100 Mbps Ethernet NIC, Fiber-optical splitters, and 4x1Gbps Copper Ethernet. Open source Utility software, Capsa Network Analyzer, was installed on the passive capturing tool used for the network analysis. Capsa Network Analyzer is an easy-to-use Ethernet packet sniffer for

network monitoring and troubleshooting purposes [20-22]. The tool handles real-time packet capture, 24/7 network assessments, accurate network forensics, advanced protocol analysis, accurate packet decoding, and automated expert diagnostics [23]. The capture tool makes it easy to isolate and solve technical problems, identify network bottleneck, bandwidth usage, and detect network vulnerabilities by providing visibility into the core network operations.

2.3. Experimental Procedures

The splitters used were bidirectional splitters to allow data capture as the device is in use. Two separate network cards were used to efficiently monitor the entry of traffic and to leave the network's core network at each access point. The capture device was connected to the University server serving as the passive instrument of assessment. The number of packets (in and out of the network) was assessed and analyzed using the capturing computer (tool). In contrast, the network's one-way delay was estimated by tracking the same individual packet at specific capturing points. There are various assessments within the network for both in- and out traffic. There is one clock in use while capturing the traffic, as shown in Figure 2, this allows reliable time to be obtained between the in and out packets of one device in use.

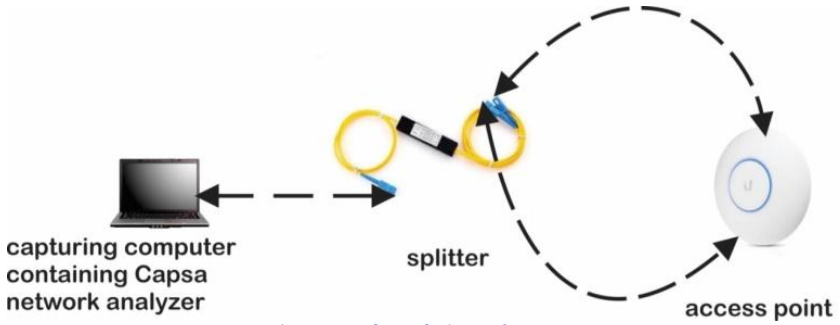

Figure-2. The technique of capture.

Delay information from the University's network is not available in the absence of traffic. Packet fragmentation in the University's (OAUSTECH) core network will also be studied by capturing known end-to-end file transfer protocol with large files from the network to an end-user. The maximum network's packet capacity shall be used for this study.

3. RESULTS AND DISCUSSION

3.1. Assessment of in/Out Packets

Tables 2 and 3 showed the values for the number of packets flowing in and out of the University network.

Table-2. Incoming packets as traffics enter the network

Capturing Points	IN	OUT
S_1	1451	0
S_2	1451	0
S_3	1451	0
S_4	1451	0
S_5	1451	0
S_6	0	0
S_7	1451	0
S_8	1451	0
S_9	1451	1451
S_{10}	0	2645
S_{11}	1451	0
S_{12}	1451	0
S_{13}	0	2645
S_{14}	1451	0

Table-3. Outgoing packets as traffics leaves the network.

Access Points (Capturing Points)	IN	OUT
S_1	0	28425
S_2	0	28425
S_3	0	0
S_4	0	0
S_5	0	0
S_6	0	32614
S_7	0	41029
S_8	0	41029
S_9	0	41029
S_{10}	0	0
S_{11}	0	33405
S_{12}	0	33405
S_{13}	0	0
S_{14}	0	32614

It was observed that all the evaluated packets have gone along the same route, except for capturing points 6, 10, and 13. This can be due to faulty configuration design in switches or time wandering and clock error during measurements. The routes have been observed as not optimal, thus consuming too much capacity during connections when traffic goes only to turn in an interface and recovers immediately in the same direction. The observed packets appear to overwhelm the devices' processing power when they interrupt, causing a possible bottleneck.

3.2. Assessment of One-Way Delay (OWD) in the Network

The one-way delay in the network was measured at different sampling locations within the network by following individual packets. These were done by separating the core network's measurements for IN and OUT traffic.

Table-4. OWD measured in milliseconds (ms) when traffic direction is IN to the network.

Points	S_2	S_3	S_5	S_7	S_8	S_9	S_{12}	S_{14}
S_1	0.115	-0.078	0.093	0.102	-	-	-	-
S_4	-	-	-	0.205	-	-	-	-0.098
S_9	-	-	-	-	-	-	0.072	-
S_{11}	-	-	-	-	0.830	0.153	-	-
S_{12}	-	-	-	0.103	-	-	0.083	-

Table-5. OWD measured in milliseconds (ms) when traffic direction is OUT of the network.

Points	S_1	S_2	S_6	S_8	S_9	S_{11}	S_{12}	S_{14}
S_{14}	0.213	-	-	0.194	-	-	-	0.072
S_9	-	-	-0.318	-	-	-0.245	-	-
S_7	-	0.097	-	-	0.430	-	0.416	-

As shown in Tables 4 and 5, respectively, the delays are minimal and sometimes negligible, so it does not cause significant delays in the encryption and decryption of packets. Although the capturing device was synchronized with the network, captures are quite short, with some values being negative, so the clocks are not simultaneous in process.

3.3. Fragmentation of Packets

The fragmentation of packets in the network was observed in this study by capturing an established end-to-end file transfer protocol over the core network with large device files to an end-user with a maximum packet size of 1500 bytes. The packet lengths distribution was captured, as shown in Table 6 and Figure 3, respectively, where

the delivery is from the core network's traffic towards the users. The results showed that there is no or little fragmentation of the packets during the transfer of data. Across all captured points, the packet length ranged from 286 to 1350 bytes.

Table-6. Distribution of packet lengths for the access points.

Points	S_1	S_2	S_6	S_7	S_8	S_9	S_{11}	S_{12}	S_{14}
Packet Lengths (bytes)	835	1050	450	750	349	658	1350	286	1240

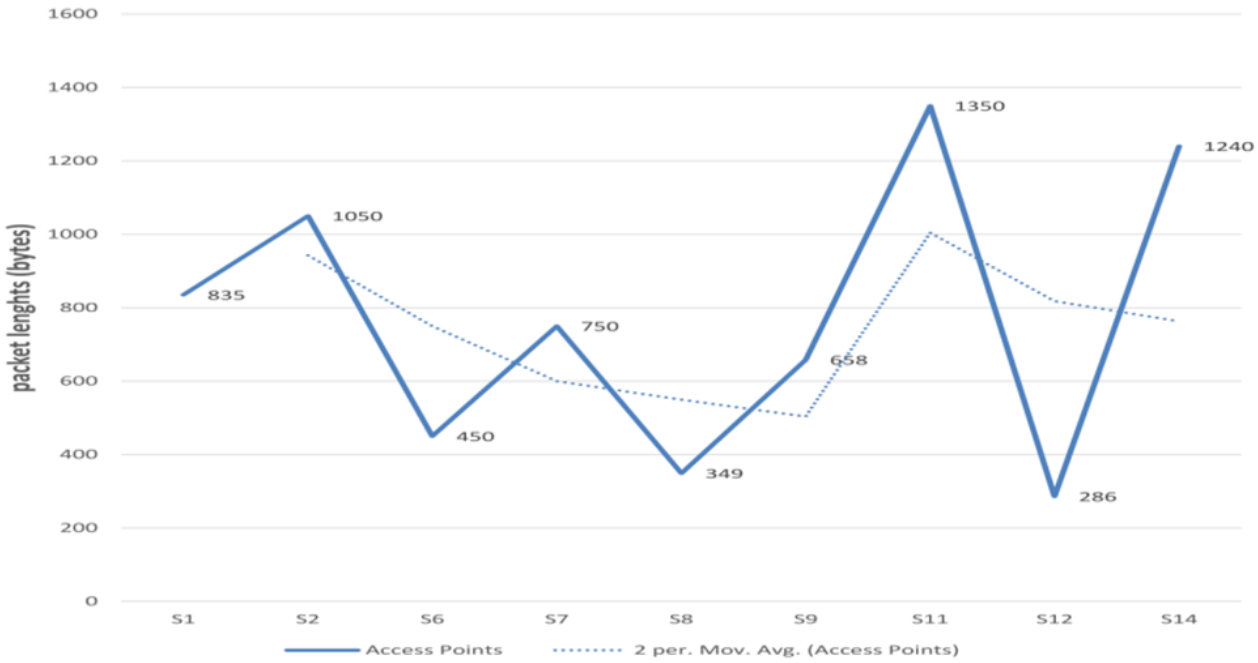

Figure-3. Packets distributions for traffic out of the network.

4. SUMMARY

This study aimed to assess and monitor the performances of a network using passive tools. Based on data collected and analyzed from the OAUSTECH's network, it was deduced that passive tool in analysis and troubleshooting is a very productive and effective way to assess and evaluate the network's performance. The passive testing technique was not based on a single method but different methods, depending on the case structure (network) in consideration. The sensitivity and non-intrusive nature of passive monitoring techniques have helped a great deal of accurate measurement and one way of delay monitoring. Also, in the study, data fragmentation, including traffic metric, comes in and out of various University network's access points, thus predicting server behaviour patterns and bandwidth use within the University community.

5. CONCLUSION

Data were collected from the core network at the study location using a passive network tool as the monitoring method. When analyzed, the results showed that testing and troubleshooting with passive network tools provides a reliable and efficient result and recommendation that can be used to improve network organization in others to satisfy its users. In particular, the sensitivity analysis conducted showed what is happening in the field of packet size, one-way delay (OWD), and packet fragmentation within the University's network.

Funding: This study received no specific financial support.
Competing Interests: The authors declare that they have no competing interests.
Acknowledgement: All authors contributed equally to the conception and design of the study.

REFERENCES

[1] P. Owezarski, *IP network monitoring and measurements: Techniques and experiences (Tutorial). In: Boavida F., Monteiro E., Orvalho J. (eds) protocols and systems for interactive distributed multimedia. IDMS 2002. Lecture notes in computer science* vol. 2515. Berlin, Heidelberg: Springer, 2002.

[2] A. J. Karim, "The significance of management information systems for enhancing strategic and tactical planning," *Journal of Information Systems and Technology Management*, vol. 8, pp. 459-470, 2011.Available at: https://doi.org/10.4301/s1807-17752011000200011.

[3] O. Icha and E. Agwu, "Effectiveness of social media networks as a strategic tool for organizational marketing management," *J Internet Bank Commer*, vol. 21, pp. 1-19, 2015.

[4] A. Scharnhorst, "Complex networks and the web: Insights from nonlinear physics," *Journal of Computer-Mediated Communication*, vol. 8, p. JCMC845, 2003.Available at: https://doi.org/10.1111/j.1083-6101.2003.tb00222.x.

[5] C. Rotsos, D. King, A. Farshad, J. Bird, L. Fawcett, N. Georgalas, M. Gunkel, K. Shiomoto, A. Wang, and A. Mauthe, "Network service orchestration standardization: A technology survey," *Computer Standards & Interfaces*, vol. 54, pp. 203-215, 2017.Available at: https://doi.org/10.1016/j.csi.2016.12.006.

[6] H. Takabi, J. B. Joshi, and G.-J. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Security & Privacy*, vol. 8, pp. 24-31, 2010.Available at: https://doi.org/10.1109/msp.2010.186.

[7] R. Boutaba, M. A. Salahuddin, N. Limam, S. Ayoubi, N. Shahriar, F. Estrada-Solano, and O. M. Caicedo, "A comprehensive survey on machine learning for networking: evolution, applications and research opportunities," *Journal of Internet Services and Applications*, vol. 9, pp. 1-99, 2018.Available at: https://doi.org/10.1186/s13174-018-0087-2.

[8] D. Zhou, Z. Yan, Y. Fu, and Z. Yao, "A survey on network data collection," *Journal of Network and Computer Applications*, vol. 116, pp. 9-23, 2018.

[9] A. W. Moore, J. Hall, C. Kreibich, E. Harris, and I. Pratt, "The architecture of a network monitor," In Passive & Active Measurement Workshop (PAM 2003), LaJolla, CA2003.

[10] H. Tabrizchi and R. Kuchaki, "A survey on security challenges in cloud computing: Issues, threats, and solutions," *The Journal of Supercomputing*, pp. 1-40, 2020.

[11] B. Xi, G. Michailidis, and V. N. Nair, "Estimating network loss rates using active tomography," *Journal of the American Statistical Association*, vol. 101, pp. 1430-1448, 2006.Available at: https://doi.org/10.1198/016214506000000366.

[12] T. Garrett, L. E. Setenareski, L. M. Peres, L. C. Bona, and E. P. Duarte, "Monitoring network neutrality: A survey on traffic differentiation detection," *IEEE Communications Surveys & Tutorials*, vol. 20, pp. 2486-2517, 2018.Available at: https://doi.org/10.1109/comst.2018.2812641.

[13] C. e. a. Fraleigh, *Design and deployment of a passive monitoring infrastructure. In: Palazzo S. (eds) evolutionary trends of the internet. IWDC 2001. Lecture notes in computer science* vol. 2170. Berlin, Heidelberg: Springer, 2001.

[14] J. Hall, "Multi-layer network monitoring and analysis. Retrieved from: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-571.pdf," 2003.

[15] J. Gonzalez and M. Papa, "Passive scanning in modbus networks. In: Goetz E., Shenoi S. (eds) critical infrastructure protection. ICCIP 2007," *International Federation for Information Processing*, vol. 253, pp. 175 – 187, 2008.Available at: https://doi.org/10.1007/978-0-387-75462-8_13.

[16] G. Gürkan, B. Şerif, and A. Fatih, "Modeling and cimulation of computer networks and systems," *Methodologies and Applications*, vol. 1, pp. 861-898, 2015.

[17] P. Arlos, M. Fiedler, and A. A. Nilsson, "A distributed passive measurement infrastructure. In: Dovrolis C. (eds) passive and active network measurement," *Lecture Notes in Computer Science*, vol. 3431, pp. 215-227, 2005.

[18] S. Gorlatch, P. Fragopoulou, and T. Priol, *On the integration of passive and active network monitoring in grid systems. In: Gorlatch S., Danelutto M. (eds) Integrated Research in GRID Computing.* Boston, MA: Springer, 2007.

[19] V. Mohan, Y. J. Reddy, and K. Kalpana, "Active and passive network measurements: A survey," *International Journal of Computer Science and Information Technologies*, vol. 2, pp. 1372-1385, 2011.

[20] B. Yu, "Based on the network sniffer implement network monitoring," in *2010 International Conference on Computer Application and System Modeling*, *7*, *V7-1 - V7-3*, 2010.

[21] P. Asrodia and H. Patel, "Network traffic analysis using packet sniffer," *International Journal of Engineering Research and Applications*, vol. 2, pp. 854-856, 2012.

[22] S. Amit, "Sniffers – the threat to ntwork scenarios and associated dimensions," *International Refereed Journal of Reviews and Research*, vol. 4, pp. 1-13, 2016.

[23] M. Natarajan, R. A. Sumanth, and A. M. Loretta, "Tools and techniques for network forensics," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 1, pp. 14 – 25, 2009.