Scientific Research Publishing

Journal of Computer and Communications, 2017, 5, 24-41
http://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

A Dynamic Approach to MIB Polling for Software Defined Monitoring

Israfil Biswas[1], Mamun Abu-Tair[1], Philip Morrow[1], Sally McClean[1], Bryan Scotney[1], Gerard Parr[2]

[1]School of Computing and Information Engineering, Ulster University, Northern Ireland, UK
[2]School of Computing Sciences, University of East Anglia, Norwich, UK
Email: mi.biswas@ulster.ac.uk, m.abu-tair@ulster.ac.uk, pj.morrow@ulster.ac.uk, si.mcclean@ulster.ac.uk, bw.scotney@ulster.ac.uk, g.parr@uea.ac.uk

How to cite this paper: Biswas, I., Abu-Tair, M., Morrow, P., McClean, S., Scotney, B. and Parr, G. (2017) A Dynamic Approach to MIB Polling for Software Defined Monitoring. *Journal of Computer and Communications*, **5**, 24-41.
https://doi.org/10.4236/jcc.2017.55003

Received: January 10, 2017
Accepted: March 20, 2017
Published: March 23, 2017

Abstract

Technology trends such as Software-Defined Networking (SDN) are transforming networking services in terms of flexibility and faster deployment times. SDN separates the control plane from the data plane with its centralised architecture compared with the distributed approach used in other management systems. However, management systems are still required to adapt the new emerging SDN-like technologies to address various security and complex management issues. Simple Network Management Protocol (SNMP) is the most widespread management protocol implemented in a traditional Network Management System (NMS) but has some limitations with the development of SDN-like services. Hence, many studies have been undertaken to merge the SDN-like services with traditional network management systems. Results show that merging SDN with traditional NMS systems not only increases the average Management Information Base (MIB) polling time but also creates additional overheads on the network. Therefore, this paper proposes a dynamic scheme for MIB polling using an additional MIB controller agent within the SDN controller. Our results show that using the proposed scheme, the average polling time can be significantly reduced (*i.e.*, faster polling of the MIB information) and also requires very low overhead because of the small sized OpenFlow messages used during polling.

Keywords

Software-Defined Networking (SDN), Management Information Base (MIB), OpenFlow, Simple Network Management Protocol (SNMP)

1. Introduction

With the popularity of cloud computing features e.g., network virtualisation [1]

[2], live migration [3] [4] etc., various network services are deployed on the Internet for dynamic resource provisioning. However, these advances generate a considerable amount of Internet traffic volume and require advance network management for security and high efficiency. The conventional network devices are designed and configured for basic Internet access services, and therefore, are static and inflexible in their physical hardware implementation. As a result, existing networking devices requiring frequent updates as new network services are continuously deployed.

Provisioning of network systems is very important for network management including network operations [5]. Large data centres (DCs) or enterprises are also often under threat from new security issues in NMS that have arisen due to the fast growth of the networks; analysis using traffic monitoring is a key for network utilisation. SNMP [6] with its popularity in traditional NMS is mostly used for exchanging management information between network devices. An efficient management system using SNMP can monitor the network effectively and usually provides network utilisation information per trunk or link. A MIB stores this information while agents run on the network devices, and is widely supported by all network devices.

Traditional management systems show inadequacies when deployed in DCs and enterprises with new SDN-like services [7] [8] [9] although they have gained many achievements. For example, SDN with a traditional management system will create inefficiencies in data forwarding within complex management systems. Therefore, new management mechanisms are required to satisfy both users and the network operators for a robust network management [10].

Network virtualisation techniques allow service providers to slice infrastructure resources, enabling a flexible deployment of new network technologies. SDN breaks the old hardware barrier by introducing reconfigurable and extensible modules in network devices by separating the control plane from the data plane. SDN increases network flexibility and service agility with resource provisioning. Hence, continuous monitoring of SDN traffic is also required for utilisation of the network resources. SDN manages data flows and switching using the OpenFlow protocol [11] whereas, SNMP has been widely used in TCP/IP-based networks for the monitoring of network elements and hosts. However, the monitored devices are represented as managed objects and defined as a MIB. Network traffic statistics via SNMP correspond to periodic polling of MIB objects (for example, *if Table* objects in *MIB II*). Hence, periodic MIB polling is required for continuous monitoring.

SNMP largely deals with the management plane where focus is on collecting information about the traffic and status of the elements and is typically consumed by a NMS through polling the information periodically. Hence, the management plane monitors and configures the network element. Whereas, the control plane defines how packets flow through the network element. OpenFlow, by definition, focuses on the control plane but also supports the management plane of the network.

OpenFlow-like protocols are required to implement the SDN paradigm using the new network elements to incorporate Network Function Virtualisation [12]. Real-time higher level executable policies across the management control plane between the main network elements are also required to expose underlying performance attributes across the end-to-end system. Hence, new enterprise MIB schema is required for agile cloud enterprise MIB data structure.

The work described in this paper is conducted as part of a wider US-Ireland funded project concerned with enabling efficient and secure cloud computing for high capacity applications, including dynamic optical Terabit scale networking. Software Defined Monitoring with a MIB will necessitate real-time higher level executable policies across the management control plane between the main network elements. The MIB schema and syntax together with a policy engine will be capable of allowing the SDN controller to make real-time decisions about the cost and benefits of migration and/or replication. In particular, in this paper we initially used the SNMP protocol for MIB polling through the SDN controller *i.e.*, merging the SDN controller with old NMS and found that using SNMP not only increases the average MIB polling time but also creates significant overheads on the network. Hence, this paper proposes a dynamic scheme of MIB polling using an additional controller inside the SDN controller. Our results show faster polling of the MIB information and very low overhead in the network compared to the NMS MIB polling.

The rest of the paper is organised as follows: Section II describes the related work in this area and how our work is unique; Section III provides details of the Software Defined Monitoring techniques and illustrates our proposed scheme. Section IV describes the experimental setup and configuration for this work. Section V presents the results with discussions comparing the old NMS with SDN and our proposed scheme. Finally, section VI provides some conclusions and a view for future work.

2. Related Work

Many research studies related to network management have been undertaken. However, new network architectures with NMS required SNMP-like network management protocols to manage the architecture effectively. An approach for managing SDN using traditional NMS is presented in [5], where to verify the approach, they have built and implemented a prototype in their own test bed. The approach was deployed in virtual networks and services and claimed that SDNMP works well in practice. In [13], a SNMP based model CNMM has been developed for cloud networks. The proposed model provides a solution to manage the growing traffic in the cloud and improve communication of manager and agents as in SNMP.

A management architecture and Manager-agent communication model has been modelled in [14] to coordinate the information residing on the single elements of the multi-stage router. The model presents a unified view to the external network management station concerning requests from SNMP.

Much research also has been conducted without using the SNMP for Software Defined Monitoring. *John et al.* proposed a split selected monitoring control functionality onto node-local control planes in [15]. It takes the advantage of processing capabilities on programmable nodes. Their approach is a rate monitoring function in SDN that is implemented using node-local control plane components introducing a messaging bus for simple and flexible communication between monitoring function components as well as control and management systems. They claim that their rate monitoring approach generates only a tiny fraction of the monitoring traffic from comparable SNMP and OpenFlow implementations, while providing the same information granularity.

However, the main issue here is in considering the entire infrastructure as one unified service production environment and therefore, the challenge is to provide up-to-date, accurate, and detailed monitoring information to orchestration and control layers in a scalable way.

In optical networks, Non-SDN Reconfigurable Optical Add-Drop Multiplexer (ROADM)s are not always able to update hardware or software in the ROADMs to adapt legacy SDN architecture. In [16], a software defined monitoring architecture has been deployed using SNMP protocol for Optical Non-SDN ROADMs. They have proposed an architecture using a proxy that translates OpenFlow messages sent by Open Network Operating System (ONOS) into SNMP messages to configure the ROADMs. The solution is for flexible monitor and manages an optical network via SDN architecture. They claim that their solution is also able to recover and reroute wavelengths when a link is down. The adapted solution to legacy networks does not require any upgrade on the optical network elements. The proposed SDN architecture is adapted to include legacy non-SDNROADMS.

Although they claim their proposal does not require any software modification of the SDN controller or ROADM SNMP agent, the issue in such architectures is that it uses a proxy that translates the of messages sent by the controller into SNMP commands to apply the desired configurations on the ROADM and vice-versa. This can increase delay in a large data centre or inter-data centre networks and reduce the monitoring performance.

In [17], an efficient scheme for performance management is developed to collect traffic statistics data via the SDN controller plane. The scheme proposes a periodic collection and transfer of MIB objects for bulk traffic statistics collection. The scheme is developed in the controller plane and provides a northbound interface for upper network management applications. Instead of using SNMP and MIBs, the scheme is implemented by periodically gathering statistics information of flow tables from SDN-enabled switches via the OpenFlow protocol. However, the issues here are the various OpenFlow packet sizes that create overheads in the network. The architecture also considers possible performance degradation in the SDN controller for additional controllers and distributed task queues to achieve high availability and scalability.

However, our work is motivated for such architectures and considered very small packets for SDN monitoring. Therefore, our scheme not only reduces the

overall network overhead but also achieves high speed data polling. In summary, this paper is unique in the following aspects:

- This work uses small packet sizes *i.e.*, only 64-byte OpenFlow packets for SDN monitoring and hence can perform high speed polling.
- Small sized packets will also reduce the overall network overhead for SDN monitoring techniques and therefore can improve the QoS of the data centre.
- The architecture achieves high availability by ensuring reduced latency between the SDN controller and the developed additional MIB controller with scalable efficient task queues.

The next Section describes old network management with MIB using SNMP protocol and proposes a dynamic approach of MIB polling in a software defined network for centralised network monitoring.

3. Software Defined Monitoring

This paper aims to develop a dynamic approach for MIB polling in SDN for monitoring. Our proposed approach includes an additional MIB controller agent in the controller plane of SDN. The MIB controller agent is designed considering a loosely coupled architecture for MIB polling to support high availability and scalability as defined in OpenFlow 1.2 or later.

3.1. Management Information Base (MIB)

SNMP agents (e.g., Net-SNMP) are allowed to collect the management information database from the device locally and make it available to the SNMP manager. Hence, the agent maintains an information database describing the managed device parameters.

NMS uses this database for specific information and this commonly shared database between the Agent and the Manager is called a MIB. A MIB is basically a collection of information for managing network elements. The MIB contains a standard set of statistical and control values defined for hardware nodes on a network. Private MIBs extends these standard values with values specific to a particular agent.

The MIBs contains of managed objects identified by the name Object Identifier (Object ID or OID). Each Identifier is exclusive and represents specific features of a managed device. However, the return value of each identifier could be different e.g. Text, Number, Counter, etc. Like a folder structure on PCs, OIDs are very structured, and follow a hierarchical tree pattern as shown in **Figure 1**. However, unlike folders all SNMP objects are numbered. Therefore, the top level is the root and after the root is ISO with the number "1". ORG is the next level with the number "3" as it is the 3rd object under ISO. OIDs are always written in a numerical form, instead of a text form.

For example, three object levels are written as 1.3.0 not *iso*|*org*|*standard*. As shown in the figure, a typical object ID will be a dotted list of integers. Hence, the OID in RFC1213 for *sysDescr* is .1.3.6.1.2.1.1.1 and using the OID the system can get the hardware and software information used on the host.

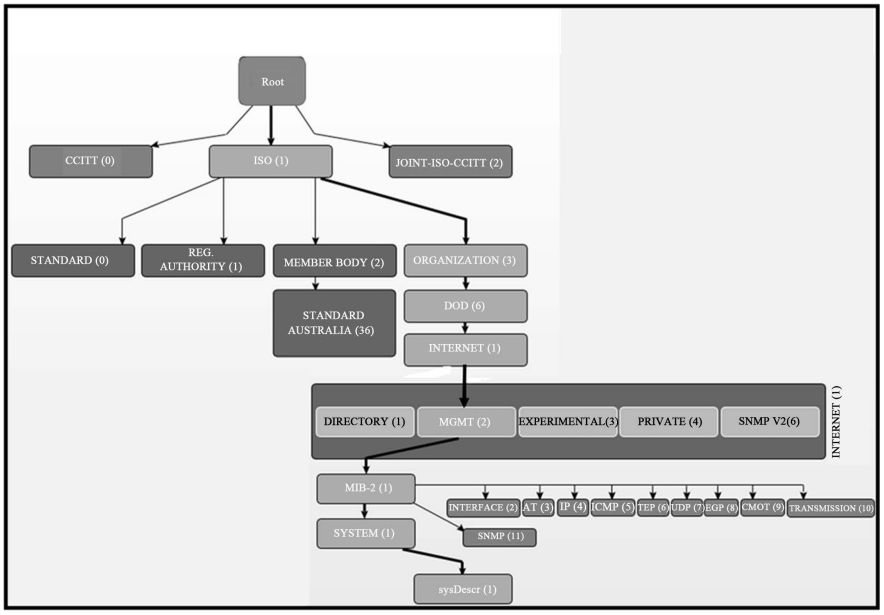

Figure 1. The MIB registered tree.

3.2. NMS with SNMP

In NMS, SNMP polls MIB information and gets a response from its MIB agents (e.g., switches, routers). **Figure 2** shows a network management system that polls information by sending a request through the SNMP Manager and gets a response from a SNMP agent. An agent can send a spontaneous TRAP to the NMS if required. SNMP TRAPs are initiated by the agents and the agent sends the TRAP to the SNMP Manager on the occurrence of an event.

NMS using SNMP fetches MIB information directly from network devices for traffic monitoring. The collection of managed object values is performed periodically and then the information can be automatically transferred to a database. Under the NMS control via SNMP protocol, polling is still a popular mechanism to gather information from the managed networks. Most NMSs collect data from network elements directly via SNMP. However, in recent developments of data centre networks, OpenFlow based SDN requires monitoring of network devices and there has not yet been sufficient research done on SDN monitoring.

3.3. NMS with SDN

This work first aims to develop a MIB polling mechanism for SDN monitoring through the NMS using SNMP. As shown in **Figure 3**, we have introduced a MIB manager at the NMS to bring a change in management paradigm from a distributed NMS to a centralised SDN control. The MIB manager fetches MIB information from the SDN controller. The manager provided in our NMS is to get MIB information through the management plane service over the SNMP protocol. The MIB data are delivered in the SDN when requested. Therefore, NMS can easily access MIB data for monitoring using SDN controller as supported in OpenFlow.

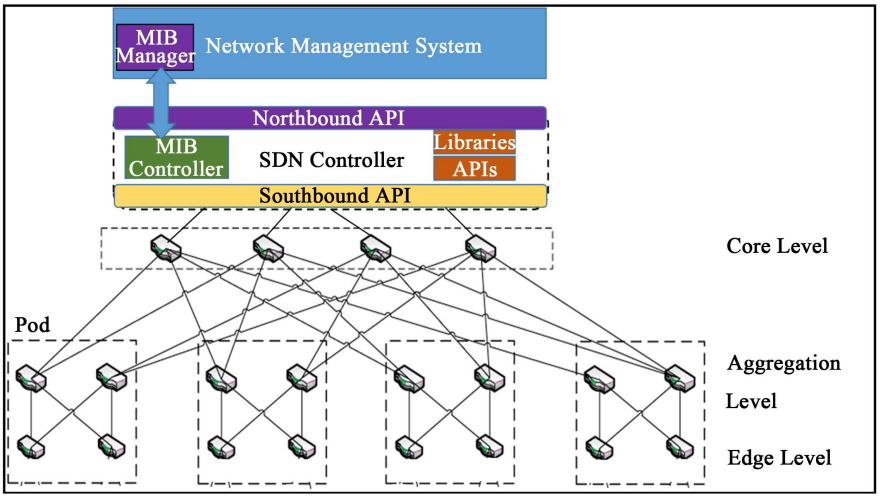

Figure 2. MIB polling scheme with NMS initiated in K-ary fat tree topology.

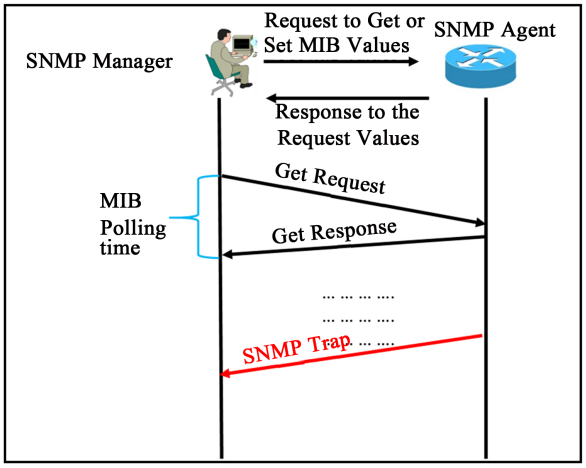

Figure 3. Illustration of MIB polling.

3.4. The SDN MIB Controller Agent

SNMP was envisioned for exposing data to external applications for remote monitoring. A distinctive feature of SNMP includes the capability of sending trap messages so that the agent device can push information about their status or condition to the management plane. However, SNMP has many shortcomings, including being limited in the number of data types it can handle. The vendors can extend the SNMP OID in their own numbering scheme but the extension does not solve the whole problem with the advances of the emerging technologies like SDN.

Hence, in this paper we have introduced a MIB controller agent in the SDN controller using the RYU SDN Framework development [18] as shown in **Figure 4**. The MIB controller agent can set and query MIB configuration parameters in the switch with the *SET_MIB_CONFIG* and *GET_MIB_REQUEST* messages. The switch responds to a MIB value request with an *GET_MIB_REPLY* message. Moreover, like the OpenFlow switch reply messages, it does not reply to a request to set the configuration as shown in **Figure 5**.

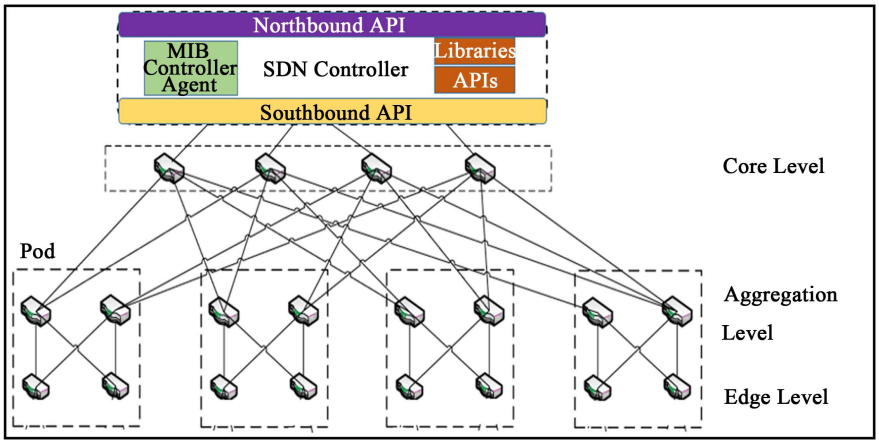

Figure 4. MIB polling scheme with proposed approach in K-ary fat tree topology.

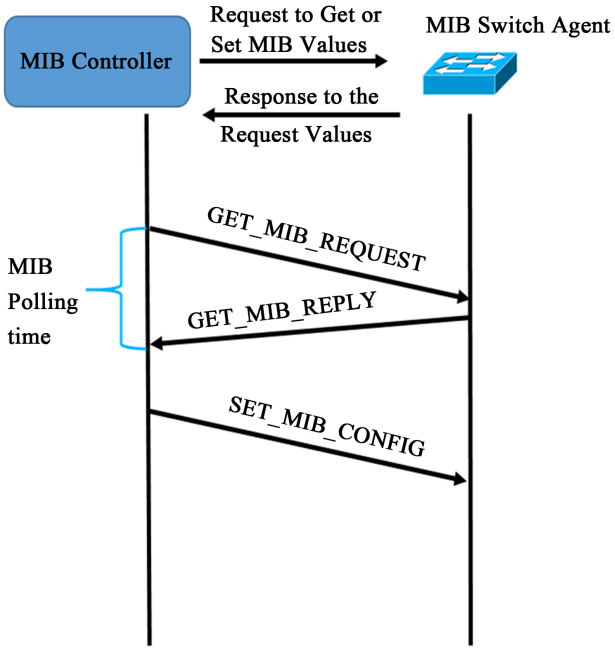

Figure 5. Illustration of MIB Polling in SDN environment.

The MIB controller agent in the SDN controller is implemented as a controller agent that sends MIB requests to a TCP port by using Netcat [19] to generate Traffic in a Mininet topology. In this work, for simplicity we have stored the exact MIB information in the Switch agent memory cache as we have used for the SNMP MIB information. **Figure 6** shows the state diagram used for MIB polling:

- In Step 1: The *GET_MIB_REQUEST* is sent by the controller, which is a small TCP Packet using Netcat. We have used 64-byte frames to generate high packet rates and force high packet processing in the OpenFlow switch from the MIB controller.
- In Step 2: With the help of Wireshark, we are able to trace corresponding Data-path IDs (DPID) of the OpenFlow switch and we have maintained a TCP Port to DPID table for this experiment to dynamically forward the MIB request to the memory cache.

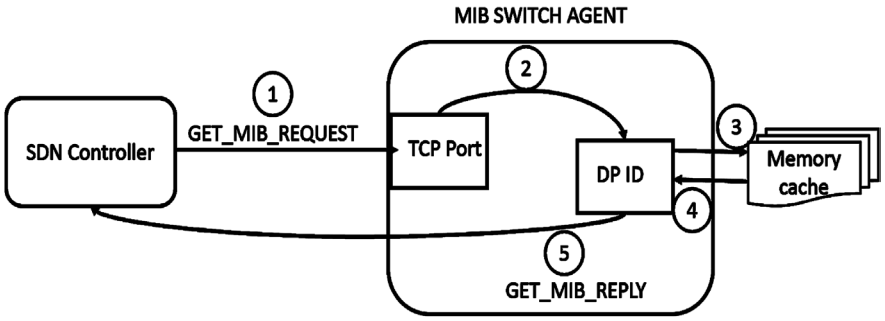

Figure 6. State diagram of MIB polling in SDN environment.

- In Step 3: The DPID finally requests the MIB information from the Memory cache.
- In Step 4: The switch returns the MIB info as OpenFlow small 64-byte packets to the DPID.
- In Step 5: The info is return as the *GET_MIB_REPLY* to the SDN controller directly.

For better performance, the MIB information is written in an in-memory cache maintaining a single list. The MIB data then can be dynamically configured via the northbound interface of the controller for monitoring. We have used the *miss_send_len* field in the OpenFlow that defines the number of bytes of each packet sent to the controller to reduce the packet size to generate high packet rates and force high packet processing in the OpenFlow switch from the MIB controller [20]. The *miss_send_len* is set to 64-bytes for small packets, whereas the default is flexible in OpenFlow version 1.3. The ofctl_v1_3 sends 0-byte length data in a *packet_in* message if *max_len* is not specified, which is 65,535.

In NMS, SNMP allows Protocol Data Units (PDUs) sized up to the Maximum Transmission Unit (MTU) of the network *i.e.*, Ethern*et a*llows up to 1500-byte frame payloads [21]. Therefore, in each MIB polling, our proposed approach can reduce noticeable network overhead. Moreover, in each polling interval, we can reduce overhead of (16 × 2872 = 45,952 byte) or 45.9 kB from 16 active MIB switch agents at one polling compared to the NMS MIB polling approach (for a general calculation, here we are not considering the retransmitted packets).

4. Experiments and Results

4.1. Setup and Configuration

We have used Mininet version 2.2.1 and OpenFlow version 13 running on an Intel(R) Core (TM) i7 3.40 GHz CPU with 16 GB of memory for the experiments. All the experiments are done over 1000 runs with 0.95 or, 95% confidence interval [22]. All the polling times in this paper are measured using Wireshark traces [23]. Table 1 shows the configuration details for the fat tree topology.

We started some initial capacity variation experiments using SNMP and the SDN controller in a fat tree topology to check the Mininet topology. SDN commenced with SNMP protocol shows that the average polling time is lower with respect to the higher link capacities between the Top of Rack and the Aggregate

Table 1. Configuration of K-ary fat tree topology: Scenario 1.

Parameters	Value
Servers/Hosts	16
Top of Rack switches	8
Aggregate switches	8
Core switches	4
Bandwidth	
Host to Top of Rack (EDGE Level) switches	1 Gbps
Aggregate to Top of Rack (EDGE Level) switches	1 Gbps
Aggregate to Core switches	1 Gbps
Polling Interval	60 sec

level switches. We found the gigabit links takes only a few milliseconds for MIB polling on average whereas, the average time for MIB polling can be up to 50 times higher using 100 Mbps links compared to the gigabit links as expected. We have performed a number of experiments described in various scenarios; the next sub-sections present the experimental results:

- The first scenario considers a comparison between the developed MIB manager in the NMS application with the proposed additional MIB controller agent at the SDN without background traffic.
- The second scenario continues the comparison considering various amounts of background traffic.

4.2. Test Scenario 1

The first scenario is chosen to measure the polling speed considering a data centre with no background traffic. We have compared the Average Polling time for the developed MIB Manager in the NMS with the proposed MIB controller agent in the SDN by varying the MIB switch agents. Using NMS, the MIB Manager gets the bandwidth of the interface to the MIB switch agent. The *If Speed* variable is used in this case that replies with the speed of the interface as reported in the SNMP *if Speed* object. Our proposed approach requests similar MIB information that has been stored in the MIB switch memory cache, considering the fat tree topology using Mininet.

Figure 7 shows that the Average Polling time initiated by the MIB controller can be up to nine times lower compared to the polling initiated by NMS. The reason is, when the NMS required any polling, it uses the MIB manager at the application level and send the request via the SDN controller. The SDN controller checks its port information and forwards the request to the associated MIB agent. Hence, this requires a number of stages to send the request to the MIB switch agent and certainly add delays. In contrast, our approach directly sends MIB request to the switch and the switch fetches the MIB info from the Memory cache and returns back directly to the SDN controller.

The figure also shows that with the number of increased active MIB switch agents, the average polling time difference between the two approaches increases.

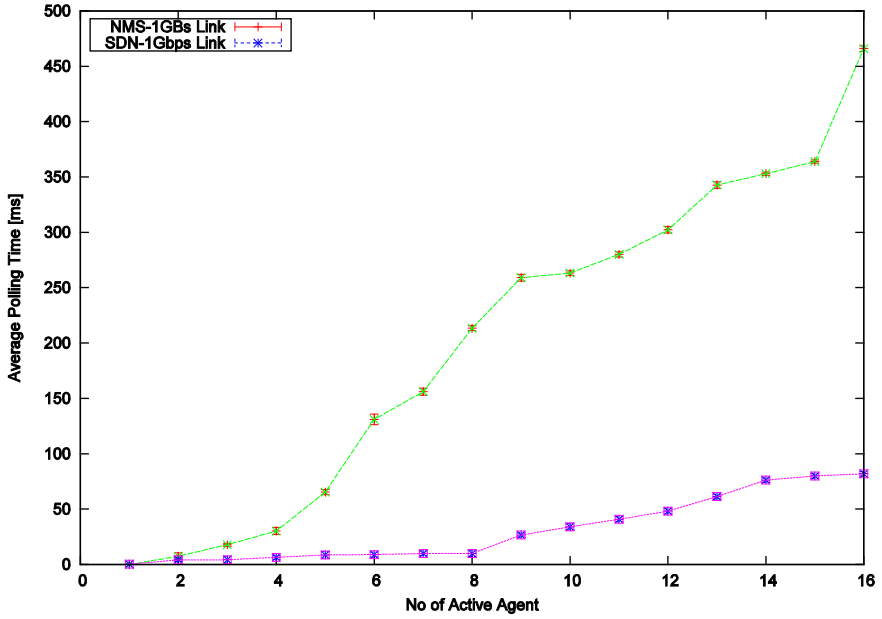

Figure 7. Average polling time [ms] with No backgound traffic.

For example, while 4 MIB switch agents are active, the average polling time initiated by NMS is 26 ms, whereas our approach shows only 7 ms. However, with 16 Active Switch Agents the polling time initiated by NMS is 460 ms, whereas the proposed approach can take up to 96 ms.

4.3. Test Scenario 2

In the second scenario, we have considered various amount of background traffic while MIB polling to observe the overall network impact. **Table 2** shows the configuration details used in this scenario in the fat tree topology. With various amounts of background traffic, many polling request packets are sent but didn't get a response within the keep alive time and therefore are retransmitted by the NMS. Our observation is the number of retransmissions significantly increases with the increase in background traffic during the MIB polling initiated by the NMS. We have used *iperf* [24] with UDP packets in Mininet to create background traffic flows.

With 20% background traffic, **Figure 8** shows that high retransmission happens due to NMS application delays during MIB polling, *i.e.*, packets are lost and no reply before the keep alive times. For example, with 4 active Switch agent, similar average polling times are observed by using both NMS and proposed approach, which is less than 1sec. However, the average polling time can be very high *i.e.*, up to several minutes, whereas our MIB controller agent does not require any MIB Manager from the application plane and anticipates that latency can be shorten and polling time is minimized as shown in the figure With 16 Active Switch Agents, the figure shows that the average polling time can be up to 36 sec, whereas the proposed approach shows that the average polling time can be few seconds.

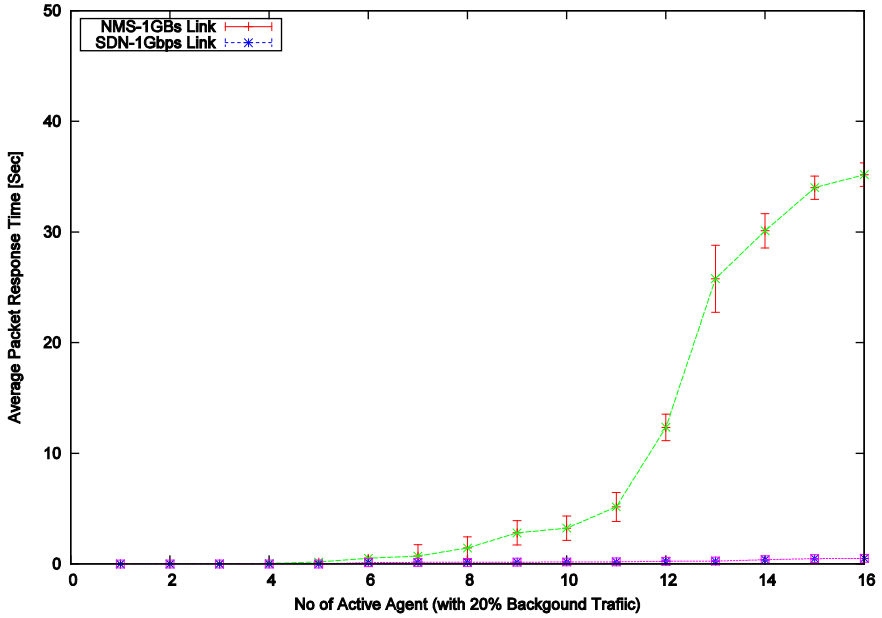

Figure 8. Average polling time [Sec] with background traffic (20%).

Table 2. Configuration of K-ary fat tree topology: Scenario 2.

Parameters	Value
Servers/Hosts	16
Top of Rack switches	8
Aggregate switches	8
Core switches	4
Bandwidth	
Host to Top of Rack (EDGE Level) switches	1 Gbps
Aggregate to Top of Rack (EDGE Level) switches	1 Gbps
Aggregate to Core switches	1 Gbps
Background Traffic	UDP
Background Traffic with respect to Network bandwidth	20%, 50% and 80%
Polling Interval	60 sec

The impact of the retransmissions can be observed in **Figure 9**, the overall packet drop was less than 1% when the number of Active MIB Switch is 4 using both approaches and it has increased up to 11% when the number of switches has increased to 16 using the NMS MIB polling approach. However, using the proposed approach the average packet drops observed is 2% for 16 MIB switch agents.

We have also obtained full sets of results considering 50% and 80% background traffic. **Figure 10** shows that considering 50% background traffic on the link, more requested MIB packets are lost or, the MIB info reply has not arrived within the keep alive time compare to the 20% background traffic. For example, the figure shows that the average response time is less than a second while the

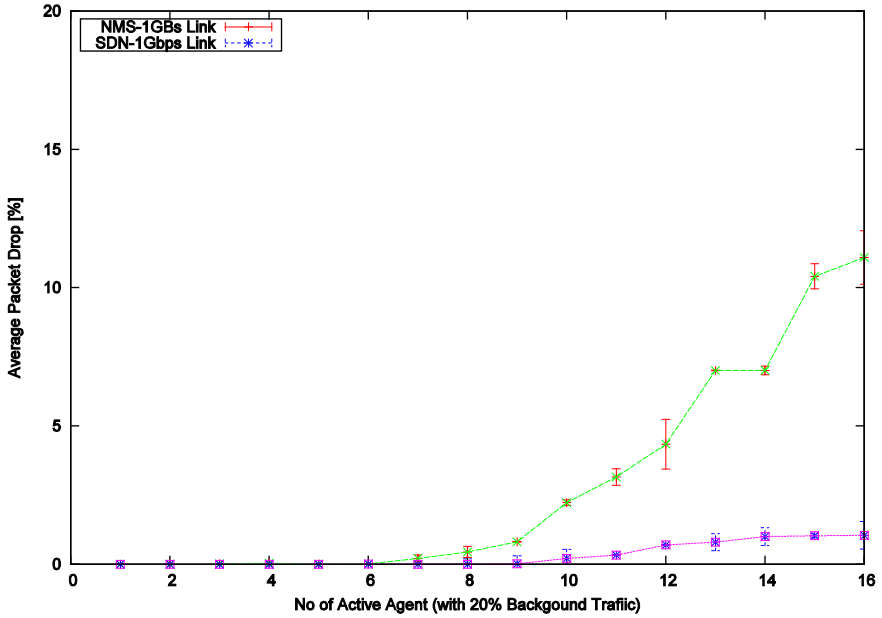

Figure 9. Average packet drops with background traffic (20%).

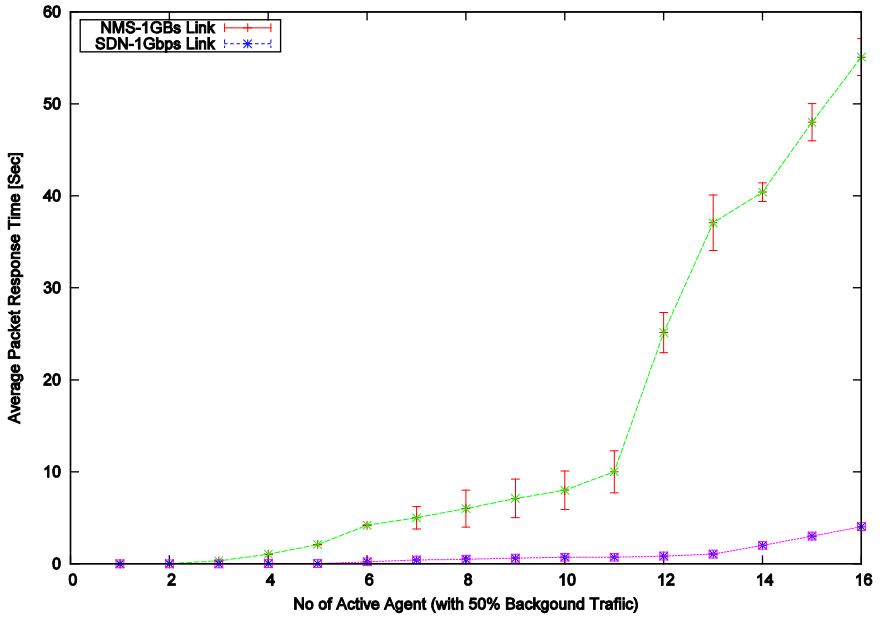

Figure 10. Average polling Time [Sec] with background traffic (50%).

number of active switch agents is 3 using both approaches and it can increase up to 56 sec using NMS MIB polling. However, using the proposed approach it increases only up to 5 sec.

The packet drops graph considering 50% background traffic also shows that the average packet drops also increases compared to 20% background traffic as shown in Figure 11. It can be up to 22% for 16 active switches using NMS MIB polling, whereas using our approach the packet drops increased to 4%.

Considering 80% background traffic, the average polling time can be very high *i.e.*, up to several minutes using NMS MIB polling, whereas our MIB controller

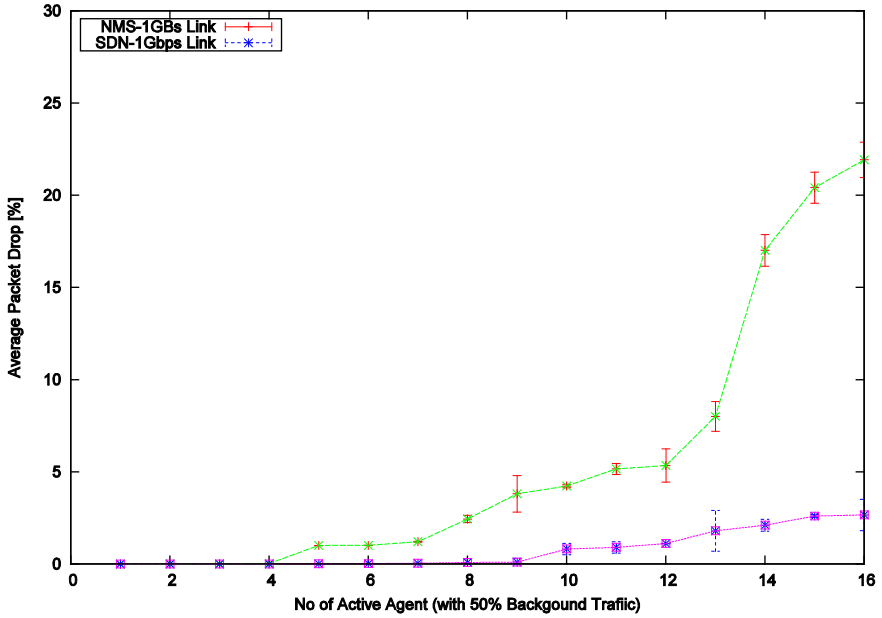

Figure 11. Average packet drops with background traffic (50%).

agent does not required any MIB manager from the application plane and it is anticipated that latency can be shorten and polling time is minimized as shown in **Figure 12**. For example, considering MIB polling using NMS, many retransmissions occur while 16 active switch agents are replying to the MIB requests and the average polling time observed is up to 118 sec. However, our approach shows that the average polling time is less than 6 sec.

The effect of the increased retransmissions can be observed in **Figure 13**, where the overall packet drops can be up to 40% using the NMS MIB polling approach when the number of active MIB switch agents is 16. However, using the MIB controller as proposed in this paper, the maximum overall packet drops can be around 6%.

The proposed approach proposes an additional MIB controller in the SDN that provides centralized control and does not require querying devices individually. The MIB controller in the SDN controller is implemented as a controller agent which sends MIB requests by using OpenFlow messages with small packet size. Hence, by reducing the overhead our results show that using a K-ary Fat tree topology in various test scenarios the proposed approach outperforms a comparative traditional SNMP based polling.

An alternative to the K-ary Fat topology has been developed known as leaf-spine where a series of leaf switches form the access layer known as "pine switches". The administrators claim that spine switches are one hop away and minimise the latency and the likelihood of bottlenecks between access-layer switches. The proposed approach sends small packets for MIB requests using OpenFlow messages and using leaf-spine architecture should not deteriorate the polling performance as the approach is not affected by latency and not affected by bottlenecks between access-layer switches.

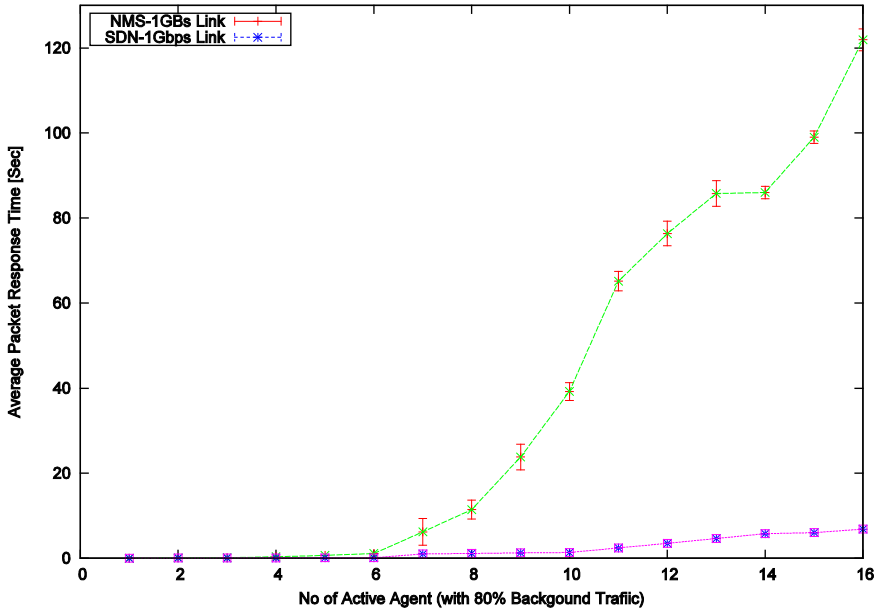

Figure 12. Average polling time [Sec] with background traffic (80%).

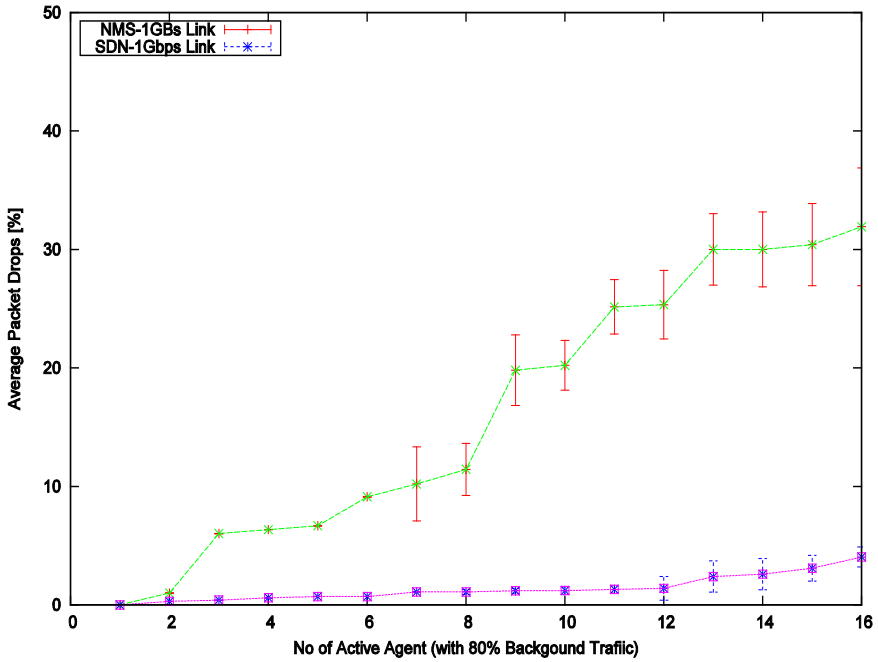

Figure 13. Average packet drops with background traffic (80%).

5. Conclusions and Future Work

Network monitoring is essential for network management where MIB polling from network devices is well recognised. Traffic monitoring using MIBs helps network operators understand network traffic volume and bandwidth utilisation, and is also important for network planning and design. In this paper, we have proposed a dynamic approach to effectively collect MIB information for SDN, and implemented the proposed architecture with an SDN controller to confirm its feasibility. Furthermore, we addressed issues in the MIB polling initiated by the NMS

via SDN and proposed effective solutions.

However, sending small packets could result in lower throughput and therefore, a network administrator's choice is a trade-off between the throughput and the polling response time in the case of high speed polling for network monitoring without interfering with the network data traffic. Future work will further investigate and develop high speed polling mechanisms considering high throughput in data centre environments by prioritizing the polling mechanisms within the management plane by developing new OpenFlow data compression techniques and scheduling algorithms. However, we expect the proposed scheme to be useful for many network management applications that require faster polling and continuous networking monitoring with very low overhead in a real data centre environment.

In SDN, a flow could be related to Inter-DC or Intra-DC. Accordingly, it is possible to attain more detailed MIB traffic in SDN, for example, network traffic consumed by an optical network or application. The low level optical attributes can be augmented with a formal illustration of the current network configuration and traffic load which will be closely coupled to the scheduling algorithms that will suggest reconfigurations to the SDN controller to be pushed down to the network elements. This formal representation of the network can monitor data from the network to be maintained on a per-link basis: average queuing delay, data loss, modulation scheme, encoding scheme, throughput, utilisation, jitter and other metrics that will become available from fast optical switching. Future work will propose an SDN architecture that will redesign including ROADMs. A proxy will be designed to translate the OpenFlow messages sent by the controller into SNMP commands to apply the desired configurations on the ROADM initially, without software modification of the controller or agent. This work will further provide such architecture by leveraging Packet Transport Routers and industry-leading optical systems into packet optical convergence architecture [25]. In this innovative converged architecture, the data plane, NMS, and control plane will be tightly coupled together into a single consistent system. This will give service providers a complete view of the network with reduced complexity in provisioning, maintenance, and troubleshooting events. This will enable a revolutionary and innovative solution for today that will be scalable and agile into the future.

Acknowledgements

This research is supported by the "Agile Cloud Service Delivery Using Integrated Photonics Networking" project funded under the US-Ireland Programme NSF (US), SFI (Ireland) and DEL (N. Ireland).

References

[1] Chowdhury, N. and Boutaba, R. (2009) Network Virtualisation: State of the Art and Research Challenges. *Communications Magazine*, **47**, 20-26.

[2] Biswas, M.I., Parr, G., McClean, S., Morrow, P. and Scotney, B. (2014) SLA-Based Scheduling of Applications for Geographically Secluded Clouds. 1*st Workshop on*

Smart Cloud Networks & Systems, Paris, 3-5 December 2014, 57-64.

[3] Biswas, M.I., Parr, G., McClean, S., Morrow, P. and Scotney, B. (2016) A Practical Evaluation in Open Stack Live Migration of VMs Using 10 Gb/s Interfaces. *The 2nd International Workshop on Education in the Cloud*, Oxford, 29 March-2 April 2016, 346-351.

[4] Biswas, M.I., Parr, G., McClean, S., Morrow, P. and Scotney, B. (2016) An Analysis of Live Migration in Open Stack Using High Speed Optical Network. *IEEE Technically Sponsored SAI Computing Conference*, London, 13-15 July 2016, 1267-1272. https://doi.org/10.1109/sai.2016.7556142

[5] Zhang, Y., Gong, X., Hu, Y., Wang, W. and Que, X. (2015) SDNMP: Enabling SDN Management Using Traditional NMS. *IEEE International Conference on Communication Workshop*, London, 8-12 June 2015, 357-362.

[6] Case, J., Fedor, M., Schoffstall, M. and Davin, J. (1990) Simple Network Management Protocol. STD 15, RFC 1157, SNMP Research, Performance Systems International, MIT Laboratory for Computer Science, Cambridge.

[7] Feamster, N., Rexford, J. and Zegura, E. (2013) The Road to SDN: An Intellectual History of Programmable Networks. *ACM Queue*, **11**, 20. https://doi.org/10.1145/2559899.2560327

[8] Kreutz, D., Ramos, F., Verissimo, P., Rothenberg, C., Azodolmolky, S. and Uhlig, S. (2014) Software-Defined Networking: A Comprehensive Survey. *Proceedings of the IEEE*, **103**, 14-76.

[9] Haleplidis, E., Pentikousis, K., Denazis, S., HadiSalim, J., Meyer, D. and Koufopavlou, O. (2015) Software-Defined Networking (SDN): Layers and Architecture Terminology, RFC 7426. http://www.rfc-editor.org/info/rfc7426

[10] Shevenell, M. and Diep, T. (2015) Managing the Software Defined World, WHITE PAPER|FEBRUARY.

[11] ONF, Open Flow Switch Specification Version 1.5.0. https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-switch-v1.5.0.noipr.pdf

[12] Network Functions Virtualisation (NFV); Infrastructure; Hypervisor Domain, ETSI GS NFV-INF 004 V1.1.1 (2015-01). http://www.etsi.org/deliver/etsi_gs/NFV-INF/001_099/004/01.01.01_60/gs_nfv-inf004v010101p.pdf

[13] Madan, M. and Mathur, M. (2014) Cloud Network Management Model a Novel Approach to Manage Cloud Traffic. *International Journal on Cloud Computing: Services and Architecture*, **4**, 9-20.

[14] Bianco, A., Birke, R., Debele, F.G. and Giraudo, L. (2011) SNMP Management in a Distributed Software Router Architecture. 2011 *IEEE International Conference Communications*, Kyoto, 5-9 June 2011, 1-5. https://doi.org/10.1109/icc.2011.5963221

[15] John, W., Meirosu, C., Pechenot, B., Sköldström, P., Kreuger, P. and Steinert, R. (2015) Scalable Software Defined Monitoring for Service Provider DevOps. 4*th European Workshop on Software Defined Networks*, Bilbao, 30 September-2 October 2015, 61-66.

[16] Alawe, I., Cousin, B., Thorey, O. and Legouable, R. (2016) Integration of Legacy Non-SDN Optical ROADMs in a Software Defined Network. *IEEE International Conference on Cloud Engineering Workshop*, Berlin, 4-8 April 2016, 60-64. https://doi.org/10.1109/IC2EW.2016.11

[17] Wang, T., Chen, Y., Huang, S., Hsu, C., Liao, B. and Young, H. (2015) An Efficient

Sche-me of Bulk Traffic Statistics Collection for Software-Defined Networks. 17*th Asia-Pacific Network Operations and Management Symposium*, Busan, 19-21 August 2015, 360-363.

[18] RYU SDN Framework. https://osrg.github.io/ryu/

[19] Netcat: The TCP/IP Swiss Army. http://nc110.sourceforge.net/

[20] Otto Carlos, M.B.D. and Pujolle, G. (2013) Virtual Networks: Pluralistic Approach for the Next Generation of Internet. Wiley, Hoboken.

[21] Presuhn, R., Case, J., McCloghrie, K., Rose, M. and Waldbusser, S. (2002) Protocol Operations for SNMP, RFC 3416.

[22] Huang, D.Y., Yocum, K. and Snoeren, A.C. (2013) High-Fidelity Switch Models for Software-Defined Network Emulation. *Proceedings of the* 2*nd ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking*, Hong Kong, 16 August 2013, 43-48. https://doi.org/10.1145/2491185.2491188

[23] Wireshark User's Guide. https://www.wireshark.org/download/docs/user-guide-a4.pdf

[24] iPerf—The Network Bandwidth Measurement Tool. https://iperf.fr/

[25] Juniper ADVA Packet Optical Convergence, White Paper. www.juniper.net