REDUCING THE MONITORING REGISTER FOR THE DETECTION OF ANOMALIES IN SOFTWARE DEFINED NETWORKS

Luz Angela Aristizábal Q.[1] and Nicolás Toro G.[2]

[1]Department of Computation, Faculty of Management,
National University, Manizales, Colombia
[2]Department of Electrical and Electronic Engineering,
National University, Manizales, Colombia

ABSTRACT

Reducing the number of processed data, when the information flow is high, is essential in processes that require short response times, such as the detection of anomalies in data networks. This work applied the wavelet transform in the reduction of the size of the monitoring register of a software defined network. Its main contribution lies in obtaining a record that, although reduced, retains detailed information required by the detectors of anomalies.

KEYWORDS

Network Monitoring, anomalies Detectors, Software Defined Networking (SDN), Wavelet transform

1. INTRODUCTION

Monitoring the activity of a data network involves the verification of operating limits such as changes in bandwidth that ensure quality of service (QoS), congestion levels of servers and interconnection devices, safety conditions, etc. This verification is a constant activity that requires the analysis of large volumes of information and short response times, and it is an activity that must compensate the overhead in the measurement and its accuracy [1].

Traffic measurement approaches are active and passive. The passive methods take measurements from traffic passing through network devices without introducing overhead, whereas active methods add traffic to the network by sending packets that are used to obtain network parameters, for example, latency of a link or of some device. [2].

With the emergence of software-defined networks in 2008, a new prospect for the implementation of network monitors was visualized. In its operation model, each switch connected to a controller also includes the generation of statistics associated with the flows of data circulating through its ports. [3] [4] This makes the implementation of passive monitoring simpler, although with the difficulty involved in the analysis of large volumes of information [5]. Subsampling techniques have been used in passive monitoring in order to reduce the amount of data in analysis processes [6][8]. However, for an abnormalities detector to achieve a high accuracy, it is necessary to

Natarajan Meghanathan et al. (Eds) : CSITA, DMAP, ISPR, NMCO - 2017
pp. 01– 07, 2017. © CS & IT-CSCP 2017 DOI : 10.5121/csit.2017.71401

consider as many statistics as the network can provide, which can be achieved by considering all the statistical information that the switches of the software defined network can send to controller.

Our interest was considering the wavelet transform as a method that could reduce the statistics data number generated in the network, retaining the level of detail that a detector needs for the evaluation of anomalous behaviours.

The results were evaluated by considering the percentage of data reduction and contrasting the reliability of the anomalies detector with original and reduced data.

This article begins by illustrating the structure of software defined networks and the statistics obtained by network switches. It continues with the explanation of the transform wavelet and concludes with the experimental results.

2. SOFTWARE DEFINED NETWORK

2.1. Structure

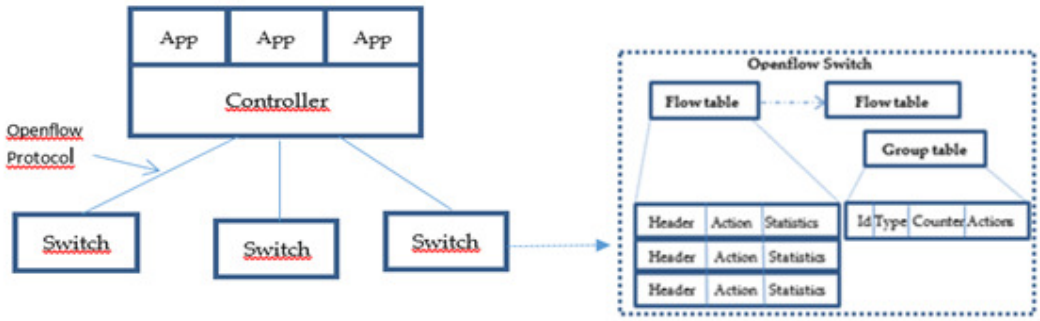

Figure 1. Software Defined Network

A Software-defined network (SDN) consists of at least two parts: controllers and interconnection devices, such as switches and routers, fig 1. The switches basically forward data according to the forwarding policies considered by the controller. A controller is a centralized software that tells the switch what to do with incoming data flows: It determines which port will forward the data and if it is necessary to duplicate or drop the data. This decision is made with each data flow that arrives to switch. The communication between switches and controllers is established by using the protocol "openflow" [4]. An Openflow switch has a flow table, each entry consists of header fields, which identify the incoming flow, an action on the flow and statistics information (right table in fig 1).

When a packet enters the switch, its fields are compared with the table header. If they match, the corresponding actions are realized.

Unlike traditional networks, the software-defined network allows: [3][9]

1. The controller to update the switch's flow table with rules on execution time
2. The controller to request the traffic statistics from switches.
3. The data path of flows to change at runtime

These characteristics make the data network more flexible, facilitating the implementation of strategies that make it safer and more dynamic.

2.2. Statistics Information.

Openflow switches send statistical information to the controller when required: Per interface, flow, queue and table.

We choose the interface statistics to illustrate the effectivity of the wavelet transform. The information that the openflow switch sends to the controller includes received packets, transmitted packets, received bytes, transmitted bytes, receive drops, transmitted drops, received errors, and transmitted errors.

The exchange of information between the openflow switch and controller is made with two messages: *Statistics Request* is used by the controller to request statistical information to the switch and *Statistics Reply* is sent by the switch to the controller in response to a request.

The algorithms implemented to obtain the statistics begin with a temporizer with an interval of 20 s. The controller sends a request message to all the connected switches each time the temporizer changes. After the controller receives the answer from the switches, it chooses the ports associated with the servers and it sends that information to the anomalies detector.

3. REDUCTION OF REGISTER

Based on the hypothesis that the performance register of a node on a data network under normal conditions presents little variation (low frequencies), and that a relatively abrupt or atypical change in the behavior of the node would result in the appearance of high frequencies, we chose to implement the wavelet transform that provides information about spatiality and frequency and that is proportional to the changes of the wavelet in the transform (The factor k in equation 1). Depending of this factor the wavelet ($\psi(t)$) shrinks or dilates [7]. When the analyzed register has low frequencies, a dilated wavelet will allow to obtained coefficients of high value, indicating the presence of low frequencies; when the register has high frequencies, a contracted wavelet would allow to obtain coefficients of high value, indicating the presence of high frequencies. The more similar the wavelet to the form of the network activity register, the wavelet coefficients will be higher in a given time [1]

$$W(d,k) = \int_{-\alpha}^{\alpha} x(t) \frac{1}{\sqrt{|k|}} \psi\left(\frac{t-d}{k}\right) dt \qquad (1)$$

Equation 1. Wavelet transform.

At the discrete level the transform is implemented using a bank of filters, the low pass filters perform the process similar to that performed in the continuous transformation when having a high scaling factor (low frequency extraction) and filters high pass have the same effect of calculating the transform with a small scale factor (high frequency extraction). Dado que nos interesa reducir el número de valores que conforman el registro se utilizó el método “wavelet packed”, ilustrado en la fig. 2.

The implementation consists in the application of a bank of filters one step low (LP) and another step high (HP), whose coefficients are determined by the base wavelet. In this case, the Register (i) is filtered by performing the convolution operation obtaining register (i + 1) with a larger

number of samples with respect to the signal of the upper level of the transformation tree, which makes it necessary to apply a subsampling reduces the number of samples in half, for each time the filters are applied. ***Thus in the third level of the tree we would have a signal of 256 samples, when the original signal initiated the process with 1024 samples***. The decision to continue applying the discrete transform is determined by the energy level of the filtered signal. If we take the fig. 3 the tree expands by the LP branch, which implies that the energy of the LP register (i + 1) signal is greater than the HP (i + 1).

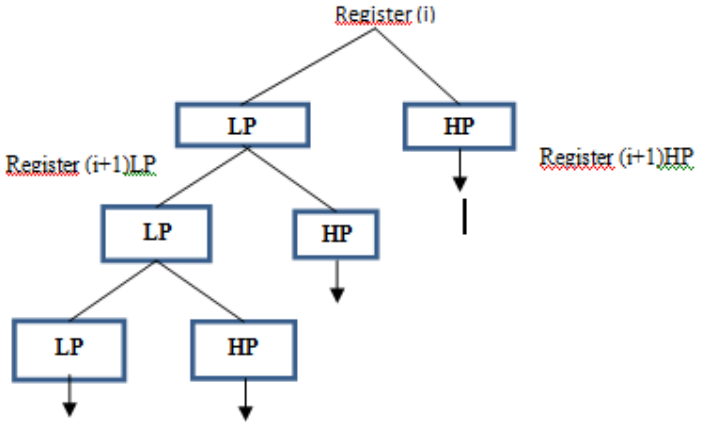

Figure 2. Descompositon tree. Discrete wavelet transform.

4. EXPERIMENTAL RESULTS

Since the basic objective of this work was to determine the reliability of the application of the wavelet transform in order to reduce the size of the statistical records obtained by the controller in a software-defined network, we considered the statistics of the associated interfaces with servers in a mininet simulation environment to reduce the sequence of transmitted bytes. (see fig 3).

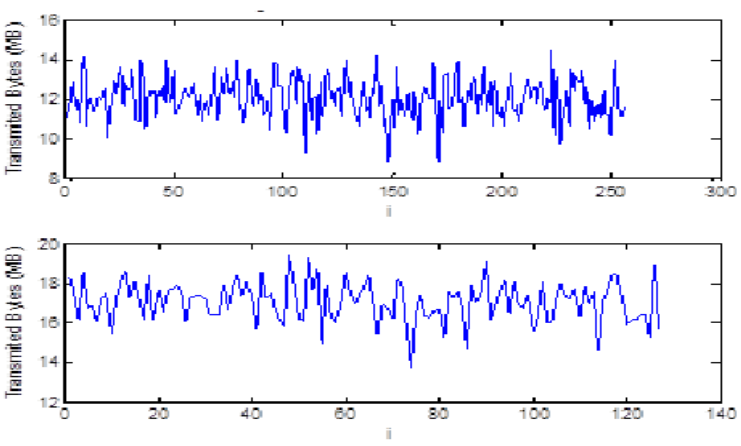

Figure 3. Reduction of register with wavelet transform

The upper graph represents the original register and shows 256 values of transmitted bytes. The lower graph represents the reduced register with 128 values, showing a good approximation to the waveform and a reduction of 50% of the original register.

We carried out the synthesis process to determine the effectiveness of the application of the wavelet transform for this type of data. We applied the inverse wavelet transform to the output of the filter banks. Fig. 4 shows the similarity between the two registers.

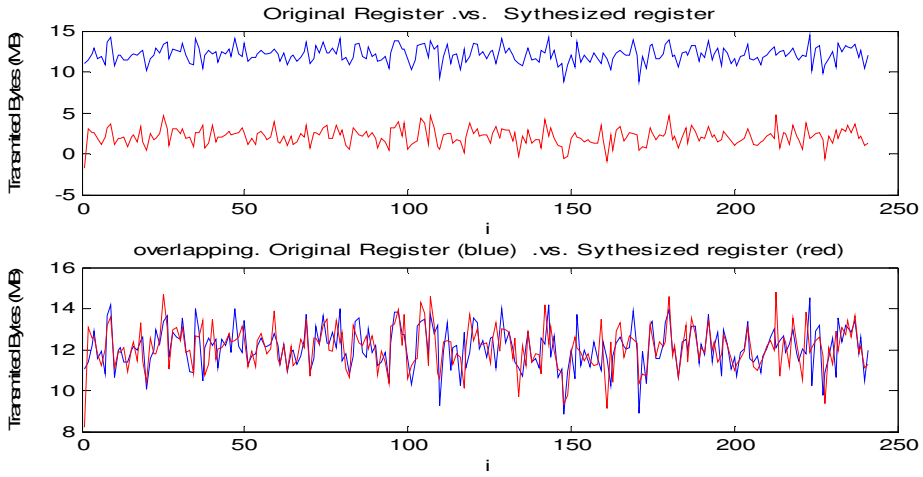

Figure 4. Comparison between the original register (blue) and the wavelet synthesized register (red).

We applied a Gaussian anomalies detector to the original and synthesized register to determine the effectiveness of the wavelet transform in the conservation of atypical data. See fig. 5. The atypical values are marked with red circles.

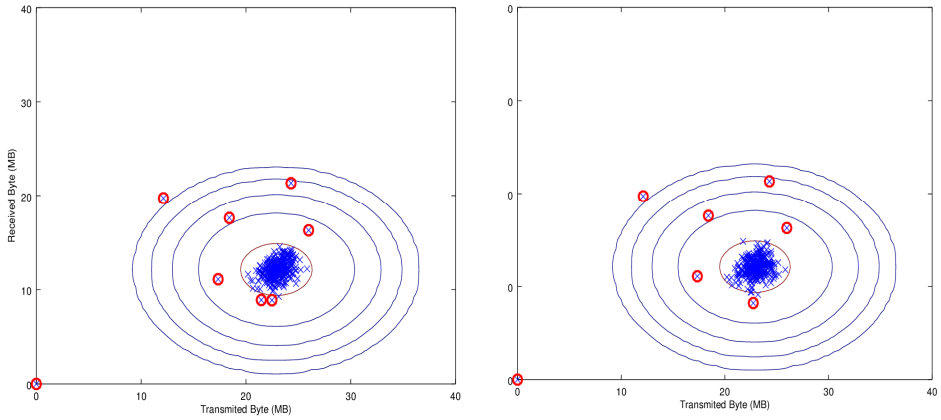

Figure 5. Result of anomaly detector. Left, Original data. Right synthetized register.

We concluded by observing how atypical behavior was conserved in fig. 6.

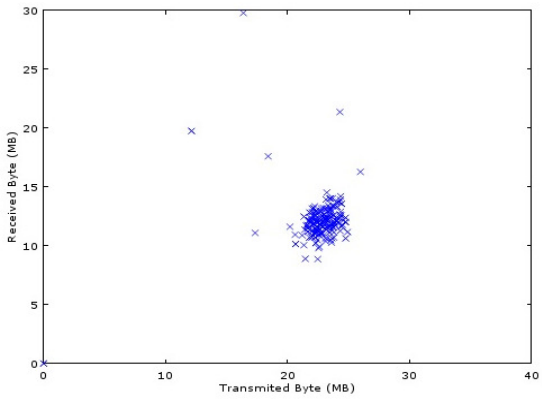

Figure 6. Relation of atypical points in the reduced register.

With this last result, we were able to verify that the detection of anomalies can be done with a shorter register than the original. This will generate less costs for computing processes and the storage of data.

5. CONCLUSIONS

The algorithm of reduction has a compression factor of at least a 50%. It *retains the atypical behaviour* of statistics data generated by the Openflow switch, which reduces the execution time of an anomaly detector.

The results of this work leave a door open for the analysis of the effectiveness of other wavelet bases in the reduction of the length of the statistical parameters in Software Defined Networks. Since this work only used the "daubechies" wavelet, evaluating other base wavelets could lead to a better reduction rate.

REFERENCES

[1] Ibidunmoye, Olumuyiwa, Hernandez R Francisco, Elmroth Erick .(2015) “Performance Anomaly Detection and Bottleneck Identification”. ACM Computing Surveys, Vol. 48, No. 1, Article 4.

[2] M, Jammal, T. Singh, A. Shami, R.l Asal, Y. Li, (2014) "Software defined networking: State of the art and research challenges", Computer Networks.

[3] Dabbagh, B.Hamdaoui, M. Guizani, and A. Rayes,(2015) "Software-Defined Networking Security: Pros and Cons", IEEE Communications Magazine.

[4] N, S. Bailey, Deepak Bansal, Linda Dunbar, Dave Hood, Zoltán Lajos Kis, (2012) "SDN Architecture Overview”. Open Network Foundation. (https://www.opennetworking.org/images/stories/downloads/sdnresources/technical-reports/SDN-architecture-overview-1.0.pdf)

[5] K. Giotis, C. Argyropoulos, G. Androulidakis, D. Kalogeras, V. Maglaris, (2014) "Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments”, Computer pag. 122–136

[6] L. Jose, M. Yu, and J. Rexford, (2011) “Online measurement of large traffic aggregates on commodity switches”, in Proc. of the USENIX workshop.

[7] Stéphane. Mallat, (2008) “A wavelet tour of signal processing”. Academic Press, USA.

[8] L. Kalinichemko, I. Shanin, I. Taraban,(2014) "Methods for Anormaly Detection: a Survey", Advanced Methodos and Technologies, digital collections. Pag. 20-25.

[9] M. Dabagh, B. Handaoul, M. Guizani, A. Rayes, (2015) "Software-Defined Networking Security: Pro and Cons", IEEE Communications Magazine. pags. 73-79.

[10] L. Seunghyeon, K. Jinwoo, S. Seungwon, P. Porras, (2017). "Athena: A framework for scalable Anormaly Detection in Software Defined Networks",47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. Pags 249-260.

AUTHORS

Luz A. Aristizábal Q. is a professor in the Department of Computing in the Faculty of Management at the National University of Colombia. She received her MEng in Physical Instrumentation from the Technological University of Pereira in 2009, her degree in Data Networks Specialization from Valle University in 1991, and her degree in Engineering Systems from Autónoma University in 1989. Her research focuses on aspects of computer and data networks, including the network simulators, signal processing and network paradigms.

Nicolás Toro G. is a professor in the Department of Electrics, Electronics and Computing. He received his PhD in Engineering-Automation and SB in Electrical Engineering from the National University of Colombia in 2013 and 1983 respectively, and his MEng degrees in Automated production systems from the Technological University of Pereira in 1992. His research focuses on many aspects of industrial automation, including the design, measurement, and analysis of networks.