Modeling and Simulating the Performance-Impact of Network Security Mechanisms on Network Traffic

Nils Lohmiller
Eberhard Karls Universität Tübingen
nils.lohmiller@student.uni-tuebingen.de

I. Motivation and Problem definition

Digitization is making its way into all areas of life. Accordingly, also in industry, the structure of such industrial networks is based on zones and conduits. Before the emergence of the digital networked industry, real-time capability was only necessary within zones. Only switches were considered in the development of Time-Sensitive Networking (TSN) up to now. Also because TSN has not existed for very long.

The fourth industrial revolution (Industry 4.0) brings new requirements for communication between devices. Industry 4.0 now makes it necessary to transport time sensitive data through several zones as well. TSN provides deterministic messaging on standard Ethernet. Standard Ethernet has been used in industry to provide new connectivity options and cost savings. It is not known how firewalls or similar security devices, at the edge of a zone, behave in this context. In the Industry 4.0 environment, reliable and real-time communication is essential to ensure that automated processes run safely and efficiently. TSN provides an open and manufacturer-independent basis for these challenges. Standard Ethernet cannot meet the requirements in terms of real-time capability of the control devices. Therefore, TSN is used for these purposes [4].

It is important to be able to make accurate statements about the delay and jitter within TSN networks. Without this, real-time control of industrial equipment using TSN is not possible. It is not known exactly which combination of network devices has which influence on the different measurands regarding delay and jitter. These are network devices whose functionality is not purely mapped in hardware. However, current TSN task group require just that. Not even the effect of the hardware load on the respective network devices has been investigated in detail so far. In particular, it is not possible to estimate the manufacturer-dependent differences between similar network components. The most important variables that have an influence on the measurement variables mentioned are also for software implemented not yet known.

In order to set up test scenarios, basic test scenarios are created using various network devices from Hirschmann. Based on this, characteristic curves can be derived for the individual devices and parameters investigated. With the help of the Eagle 40, on which a normal Linux distribution is installed. At the same time, potential behavior patterns for Linux-based software firewalls can be derived. This must be verified with the help of other devices (potentially also from other manufacturers).

II. Design

In the context of this work, different network devices and network security mechanisms are to be examined for their different factors of influence on measurable variables within the network. In particular, delay, jitter, packet loss and throughput will be considered. First of all, already existing results in this field will be searched and presented as related work in chapter IV. Not only to get to know the measurement methodologies used there, but also to be able to determine and estimate already investigated measurement quantities. Based on this, a matrix with the most important variable parameters can be set up. With the help of this matrix it can be estimated which combinations are to be investigated.

Since every device from every manufacturer performs differently, it is not possible to draw conclusions from one device to all others, but certain parallels can be found. The aim is to create manufacturer-independent characteristic curves that can be used to predict the individual parameter relationships.

There are no standardized test scenarios for our use case, so we first have to define exactly how the tests are structured and what results are expected. For each test case, the four mentioned parameters are used to measure, score, or create a characteristic curve for the test case. A characteristic curve graphically describes the dependency relationship of several parameters to each other. This makes it possible to estimate future behavior under different conditions without knowing the system in detail. The test cases must show at which position within the device the measuring points are set. The following approach can serve as an idea for this.

An RSPE from Hirschmann is used to set the time stamps. The packets are sent from the load generator to the RSPE. The RSPE sends the packets to the device under test. At the egress of the RSPE the first timestamp is set. The device under test sends the packets back to the RSPE at whose ingress the second timestamp is set. The difference represents the processing time. From this the delay can be derived that adds the respective device to the network. Before such results are meaningful, the data must first be processed. In order to evaluate the generated data, it must be ensured that the data

does not contain any possible errors. This can be done by a plausibility check. Scaling is not a problem within a device, but can vary depending on the device type. Accordingly, we must adjust the scaling if necessary.

Another problem will be how deep the reasons for possible anomalies in the characteristics are. Can these be fixed by a simple hardware exchange or are they part of the operating system. In this work, the characteristic curves are used to show how network devices behave in the different parameters. The goal is also to examine, for example, a firewall software to find out where possible performance fluctuations come from, which can not be explained with superficial points.

III. Evaluation

Ideally, the characteristic curve for one network device type can be applied to all, including those from other manufacturers. However, this will most likely not happen, so the curves should approximate the behavior. The behavior in real applications can then be derived from these curves.

A firewall is to be examined more closely as an example in order to find possible problems or performance issues. On the basis of this, the procedure will be shown how a characteristic curve can be explained, so that a possible load behavior is changed or at least made plausible.

Perhaps a formula can be developed, which makes a prediction of the behavior of a network. This formula is dependent on the parameters mentioned and should provide concrete values for delay, jitter, packet loss and throughput depending on the consideration. To find out if this formula is correct, certain measuring points are entered into the formula. This involves checking how well the formula can be applied to different parameters. Different parameters are chosen and both calculated in the formula and measured in reality. The result from the formula and the real measurement should be compared. The closer the prediction of the formula is to reality, the more likely it is that the formula is correct.

The test cases should be applicable independent of the manufacturer. So that the results allow a comparison between different manufacturers. The tests contain test sequences for each of the four output parameters in which the input parameters such as CPU load, packet rate or packet size are varied. This gives a matrix of results. A characteristic curve can be created from this matrix with the aid of interpolation. If a similar or even identical curve is created from sufficient test data for different devices, then a characteristic curve can be approximated for a specific device type. New test data are compared with this curve and their deviation from it is determined. Accordingly, the significance of the curve can be determined.

In terms of CPU load, all tested firewalls are expected to perform worse with increasing CPU load. Regardless of how the CPU load comes about. The performance of the firewalls will not decrease linearly. Depending on the firewall test, a sudden increase in delay and jitter is expected.

In later measurements, several devices are to be located within the network so that a realistic picture of a real application is obtained. This can also be used to determine which device has the decisive influence on the network. If it turns out that delay, jitter, packet loss and throughput behave linearly when only one input parameter is changed, one could predict the entire network behavior based on this parameter. In the simplest case, the devices would behave linearly in every situation, but this cannot be assumed based on the preliminary work.

IV. Related Work

M. Pudelko et al. published a ”Performance Analysis of VPN Gateways” [1]. In their research they show the dependencies on CPU Load, packet rate and number of flows of different VPN Gateways. Pudelko et al. show that the internal setup of some VPN Gateways is responsible for spin locks, which lead to performance losses. This is important to this work because it shows the importance of examining a network security feature to determine such performance degradation.

Another related work was published by Wüsteney et al. ”Impact of Packet Filtering on Time-Sensitive Networking Traffic” [2]. Based on the trend in industrial networks delay and jitter became an increasing problem in such networks, especially with time sensitivity. Among other things, it shows how the delay of a firewall behaves with increasing link load.

In ”Can Encrypted DNS Be Fast?” discribed Hounsel et al. how they compared different DNS types [3]. They describe in detail how their test setup looks like and which assumptions are made. A spezialized Whitebox with custom software and hardware enables the measurement of setup times and compare them with each other to find an ideal solution. Their methodology for test setup description can be applied to this work.

With their work to ”WiFi, LTE, or Both?” S. Deng et al. described the way how to measure the differences between Wifi, LTE or a mix of both [5]. The geographic conditions are also taken into account. The different results are used to create a distribution function. This in turn is used for the evaluation. From this it is derived that the tests also take place in different network environments and the results depending on this can be represented with the help of a distribution function.

”Performance Analysis over Software Router vs. Hardware Router: A Practical Approach” measured the delay between Client-Server and displayed it with a time diagram. The only relevant parameter from this related work is the delay. Nevertheless, a different conclusion was drawn. Despite lower throughput of the software router compared to the hardware router, the software router is rated as more predictable [6].

V. Result

With the help of the results of this work, it should be possible to predict how different network security devices affect the network. So that delay, jitter, packet loss and throughput across zones and conduits is also predictable. The work should make it possible to predict the behavior of specific

devices within a network. It may also be possible to identify performance optimizations.

REFERENCES

[1] M. Pudelko, P. Emmerich, S. Gallenmüller, G. Carle, *Performance Analysis of VPN Gateways*, Technical University of Munich, Department of Informatics, Chair of Network Architectures and Services, 2020.

[2] L. Wüsteney, M. Menth, R. Hummen, T. Heer, *Impact of Packet Filtering on Time-Sensitive Networking Traffic*, University of Applied Sciences Esslingen, Germany, 2021.

[3] A. Hounsel, P. Schmitt, K. Borgolte, N. Feamster, *Can Encrypted DNS Be Fast?*, Princeton University, Princeton, TU Delft, 2628 BX Delft, The Netherlands, University of Chicago, Chicago, 2020.

[4] S. Luber, *Was ist Time Sensitive Networking (TSN)*, Bigdata Insider, 04.05.2018. https://www.bigdata-insider.de/was-ist-time-sensitive-networking-tsn-a-708987/

[5] S. Deng, R. Netravali, A. Sivaraman, H. Balakrishnan, *WiFi, LTE, or Both? Measuring Multi-Homed Wireless Internet Performance*, MIT Computer Science and Artificial Intelligence Lab Cambridge, Massachusetts, USA.

[6] E. Guillen, A. María Sossa, E. Paola Estupiñán, *Performance Analysis over Software Router vs. Hardware Router: A Practical Approach*, World Congress on Engineering and Computer Science 2012, San Francisco, USA.