DIPL.ING.(FH)KLAUS ROCK

HTTP-QuSS

HTTP - QUANTUM SPEED AND SECURITY

February 14, 2022

FOR DUMMIES

ROCK TECHNOLOGIES
Bonhoefferstr. 37 | 73432 Aalen | Germany | +49-7367-9222-958

Table of Contents

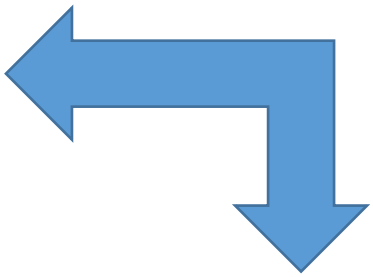
DIPL.-ING. (FH) KLAUS ROCK
BONHOEFFERSTRASSE 37

73432 AALEN – GERMANY

PHONE: 0049-7367-9222958
MAIL: K.ROCK@ROCK-TECHNOLOGIES.COM

1.0 How Data are transported on the Internet

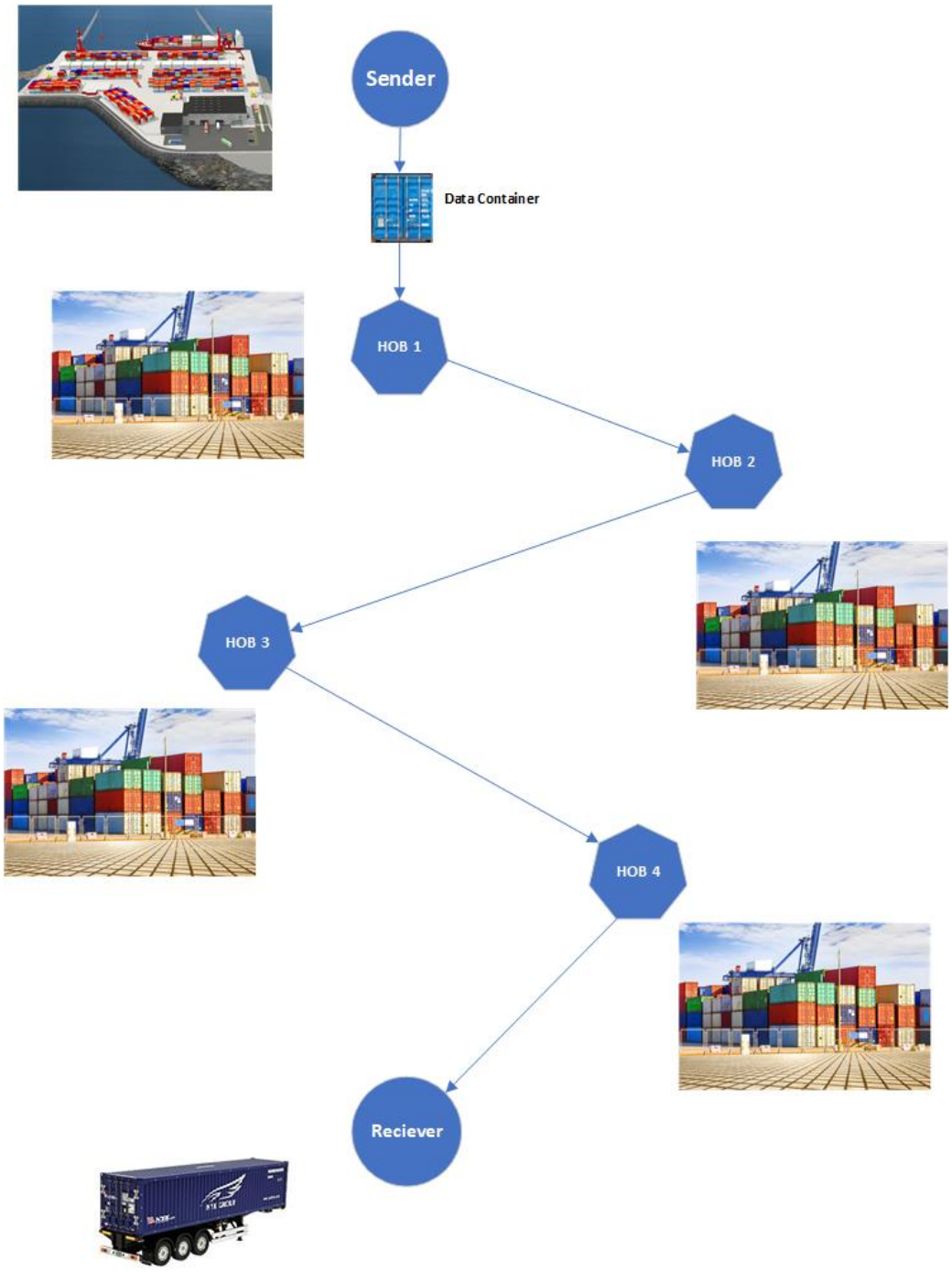
The transport of Data on the Internet is like Containers in the real World and they are called IP Data Packages which drive from a Source to a Destination Address.



On the travel to the destination they must bypass Railway Stations called Hops in the IT Network Language.

In these Railway Stations the Data Containers are moved from one Train to another one and this work is done in the Internet by Data Package Switches which we can compare like a powerful Computer System but specialised only on this kind of Work called Routing.

This Data Package Switch Network does not care about an orderly delivery or arrival and the Sender must take own precautions that all Data arrive complete and in a good shape.



There are two major Types of IP Data Containers.

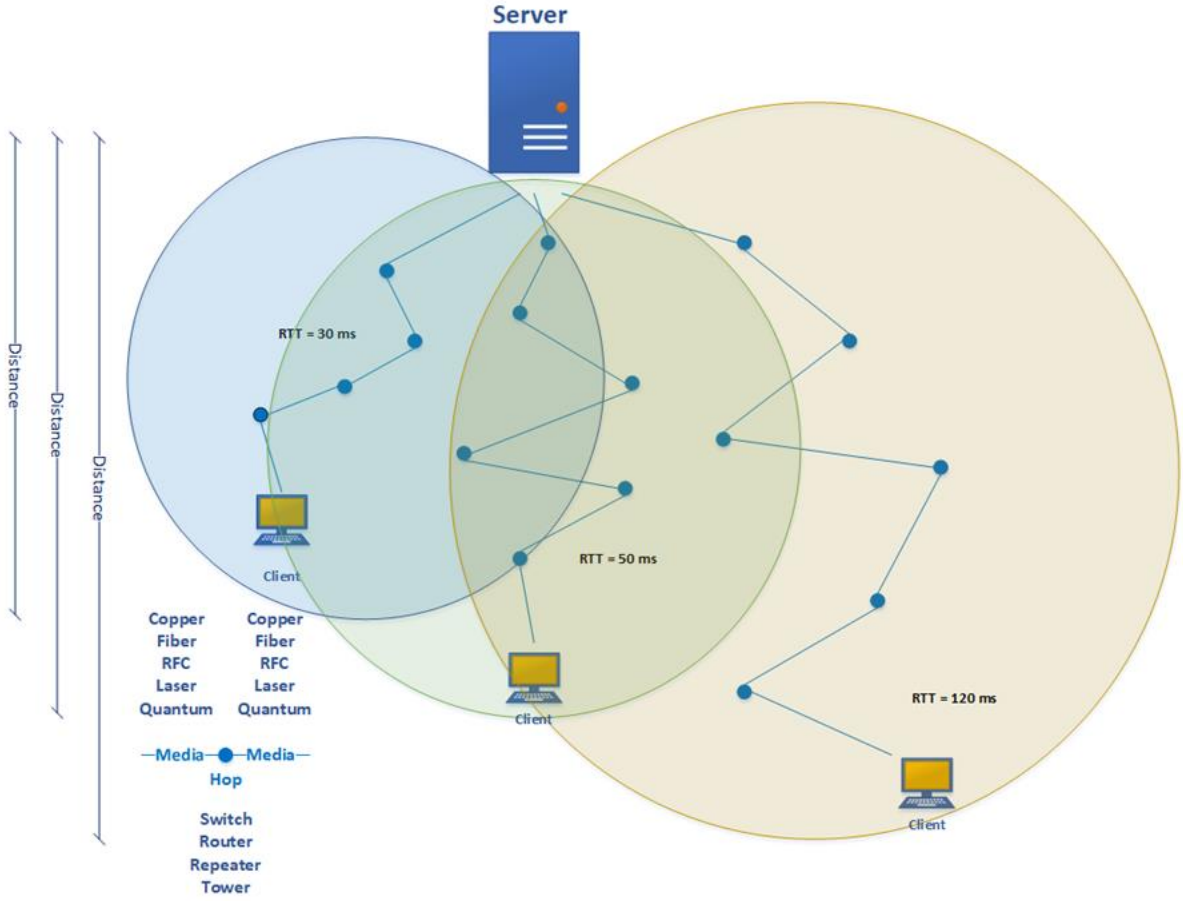
- **TCP** with secure Data Delivery
- **UDP** without secure Data Delivery

The Secure Data Delivery is provided by an intensive complicated Flow Control Handshakes Protocol which is Part of TCP.

2.0 What is Latency

- Latency is the Time an IP Data Packages needs from Sender die Receiver and back again.
- Latency Time depends on the Number of Hops, Quality of Transport Media and finally the Distance and is measured in Milliseconds (***ms***) and called Round Trip Time (***RTT***)

$$\text{Latency} = f\,\Sigma\text{Hops} + \text{Media} + \text{Distance}$$



Example:

The distance between Berlin and Tokyo is 8941.2 km. Assuming a transmission at the speed of light (in a vacuum approx. 300,000 km/s), the result is a minimum possible package transfer time of approximately:

$$2 \cdot \frac{8941{,}2\,\text{km}}{300000\,\text{km/s}} \approx 0{,}0596\,\text{s} = 59{,}6\,\text{ms}$$

A more realistic value for the speed would be about 150,000 km/s, considering the reduced speed of light in matter (glass fiber) as well as delays at transfer stations, routers, and switches. Assuming this more realistic speed and the direct line path, a minimum **RTT** of about 120 **ms** is obtained.

3.0 The Internet TCP Protocol

Called **T**ransmission **C**ontrol **P**rotocol.

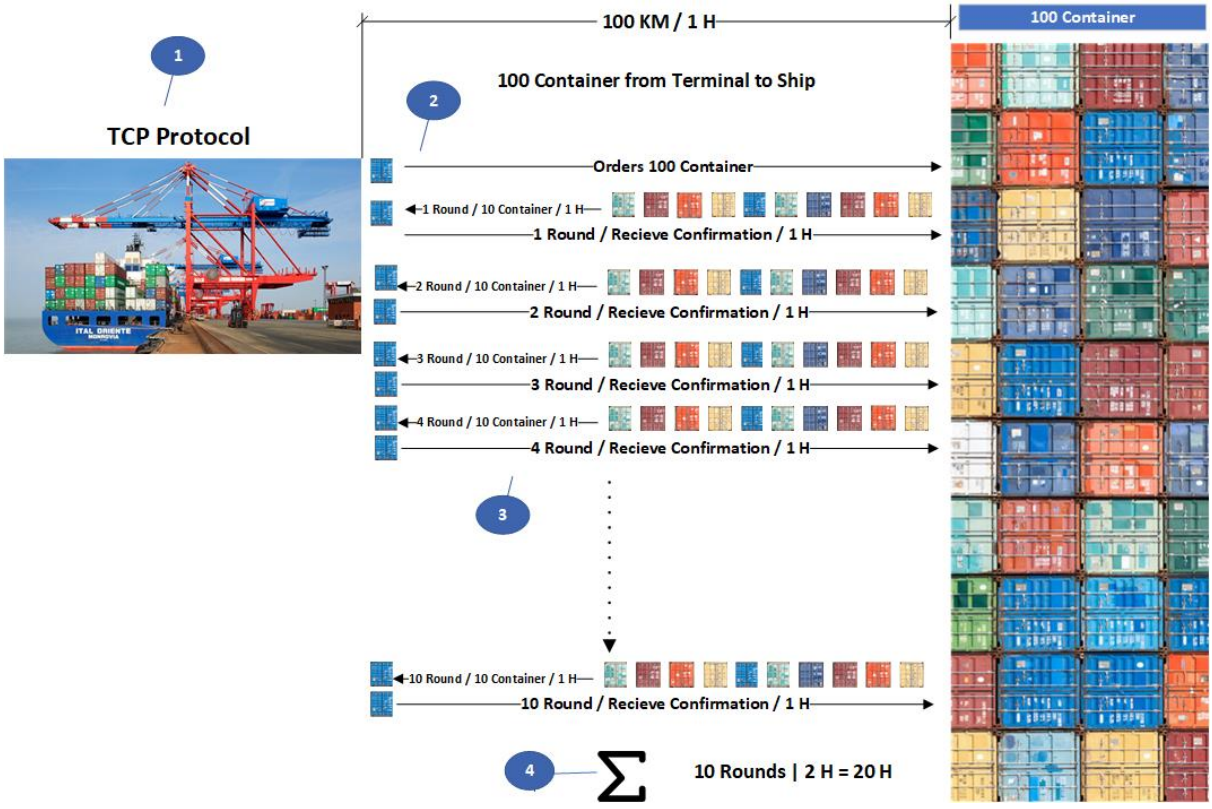
As mentioned before within this Container Network (Data Package Switch Network) there is no Container Damage or Loss Detection, so we must recognize by ourselves using a Communication Protocol.

About 90 % of all Internet Applications use this **TCP** Protocol which is now nearly over 50 Years old and come from a time where the Streets where very bad and unsecure.

Container Loss and Damage was quite common, and the Sender needed a Mechanism to recognize and correct this.

This leads into a very pessimistic and careful Container Transmission Behaviour as explained in the Container Example below.

It is very simplified but there are much more complicated Mechanism which makes this Protocol very secure especially in an overbooked Internet with many Advantages for Network Providers.



The Data Container Receiving Acknowledgement is the most Bandwidth killing Handshake within the TCP Protocol because of:

Very simplified !!!

1. The Container Ship requests 100 Container from the Terminal

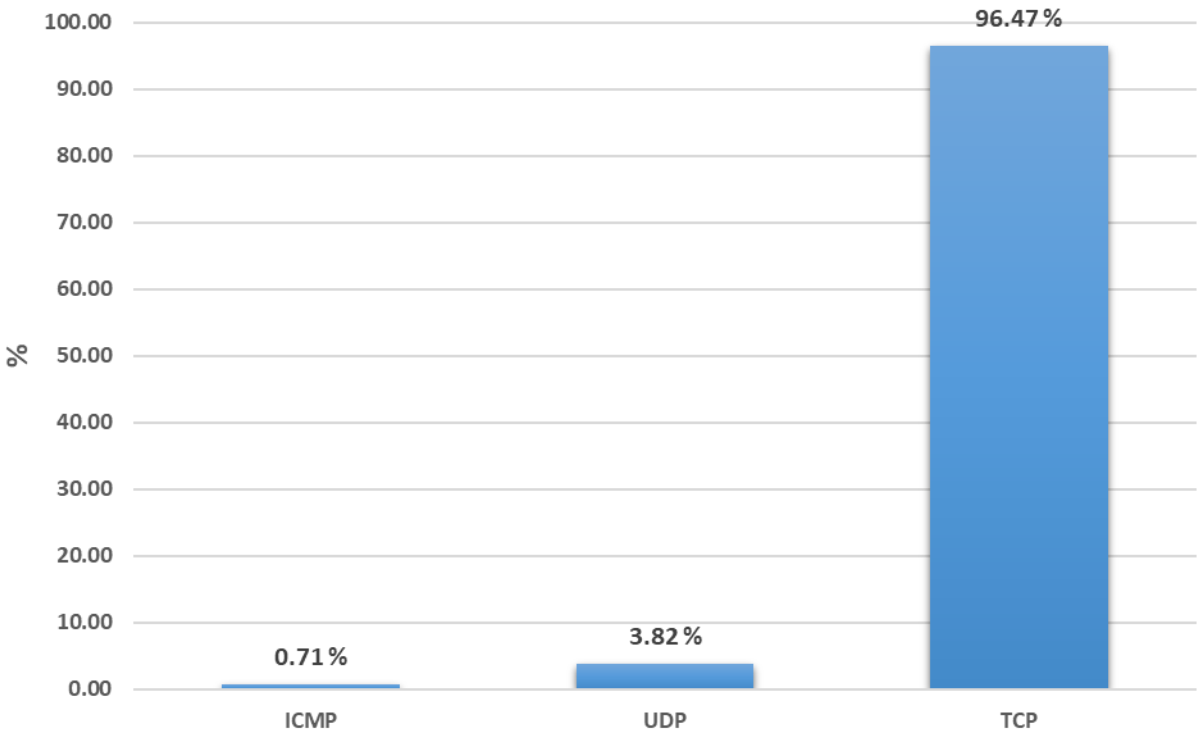
2. But Terminal sends in a first Round only 10 because he wants to see whether they arrive.

3. When Terminal receives a Receipt Confirmation he sends another 10 Containers.

4. In our example we need for one Round Trip 2 H and a total of 20 H for the complete 100 Container Transmission.

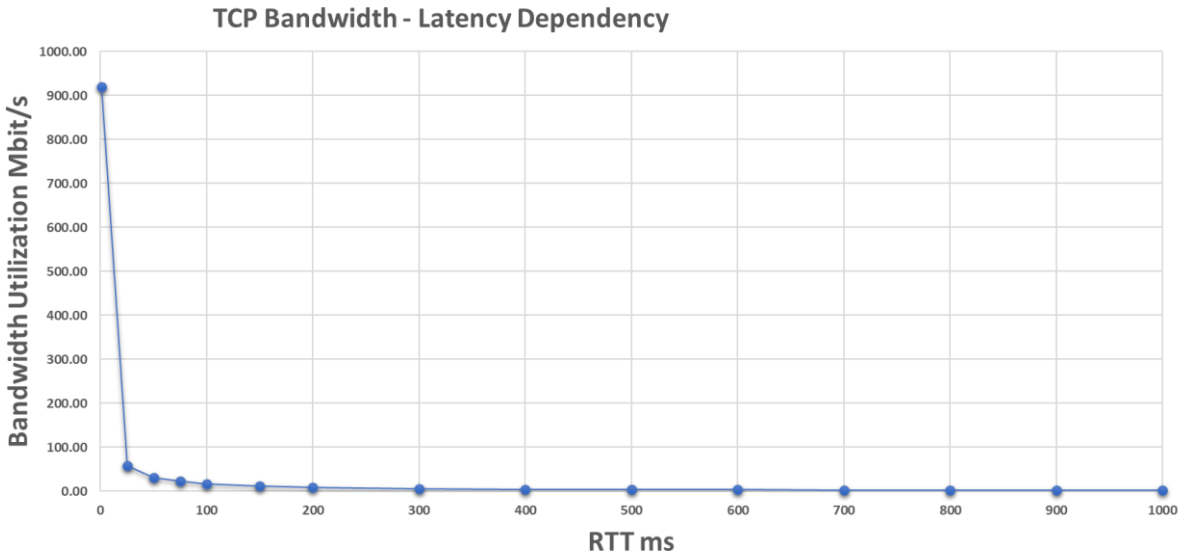
The Conclusion is that this **TCP** Protocol does not fully utilize modern Network Communication Infrastructures and Technologies and still mutes like in old times.

Used Protocols in normal Internet Traffic



4.0 The Latency Impact on TCP Speed

These **TCP** Protocol Round Trips which are needed for a secure Data Package Flow Control and the Latency Time (**RTT**) have a huge impact on the **TCP** Data Transmission Speed.



- So as longer the **RTT** and as Higher the available Bandwidth as more dramatically is the Bandwidth Loss.
- Great efforts are therefore made to reduce this Latency Time by reducing the distance between the transmitter and the receiver.
- This can be achieved by placing WEB Contents using WEB Caching Servers (Content Delivery Networks) as near as possible to the Customer or in the Satellite Industry by using thousands of Micro Satellites in a 1 000 km Low Orbit instead geostationary ones in a 36 000 km Orbit.

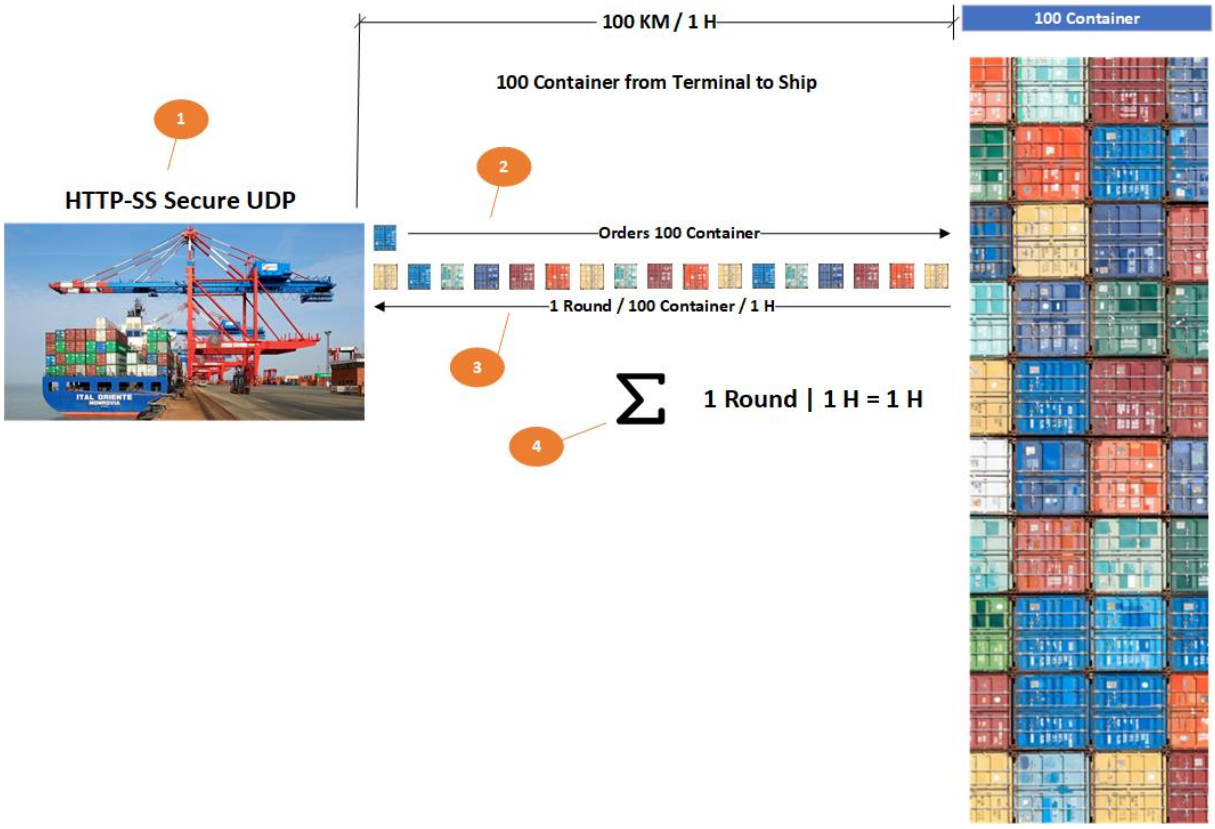
5.0 How HTTP-QuSS solves this TCP Latency Problem

5.1 New AI-Supported secure UDP Data Push

Modern Communication Networks therefor have meanwhile a very high Quality of Service by using Fibre Optic Cables and it is time to think optimistic within the Data Communication Industry.

Let's have a look onto our Container Example when we send 100 Containers between a Terminal and a Ship.

We do it now very simple and robust and think very optimistic.



Optimistic because we always think the Container will arrive without any Loss and Damage.

1. – 2. After receiving an Order of 100 Containers we send at once all 100 onto the Street and think positive that all will arrive in a good shape.

3. – 4. We need no Arrival Confirmation and so we need only half of a Roundtrip which is only 1 H instead of 20 H when we would think pessimistic.

Of course, we must take precautions of Container (Data Package) Losses and Damages but in modern Communication Networks we see only 1 Loss on 1 000 sent Data Packages which is 0,1 %.

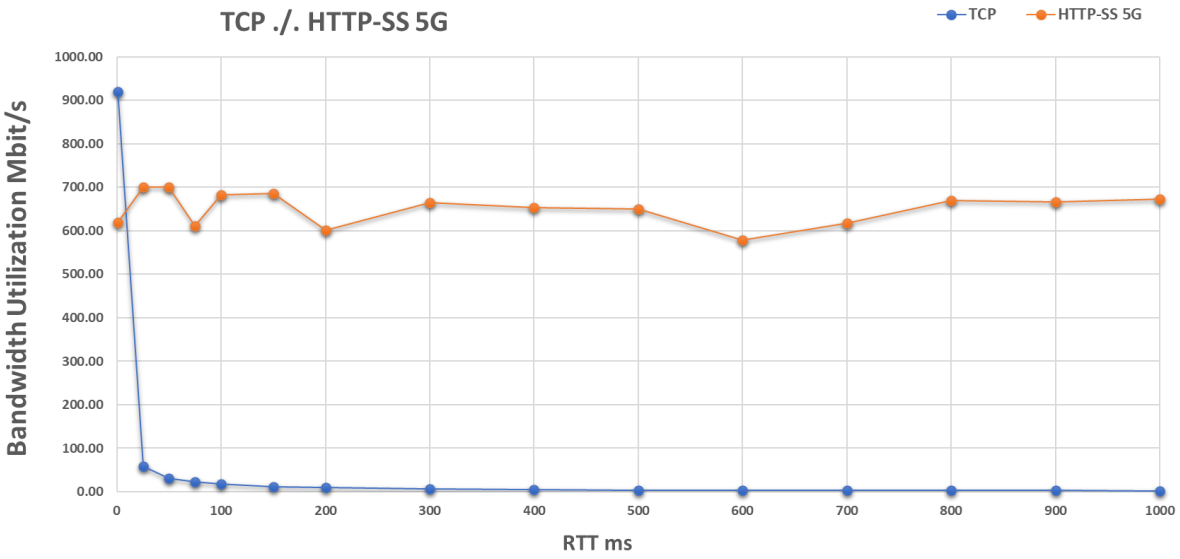
So, this 0,1 % does not rectify this still very pessimistic Data Transmission Behaviour in modern Communication Networks.

HTTP-QuSS uses therefore a secure very optimistic UDP Data Communication Protocol with Package Loss Recognition and Retransmission, Bandwidth Shaping and Slicing to fully utilize modern high-Speed Internet Connections without any Bandwidth Latency Losses and even fulfils 5G Requirements.

Also, worth to know:

- **UDP** is a Standard Internet Protocol but with a HTTP-QuSS Algorithm to avoid Bandwidth Losses produced by long Round Trips.
- Works on all Distances and Round-Trip Times with removal of the bandwidth latency dependency
- With integrated Artificial Intelligence (**AI**) Support for Real-Time Bandwidth Shaping and Slicing for a maximum of Bandwidth Utilization.

So, Latency Problem solved !!



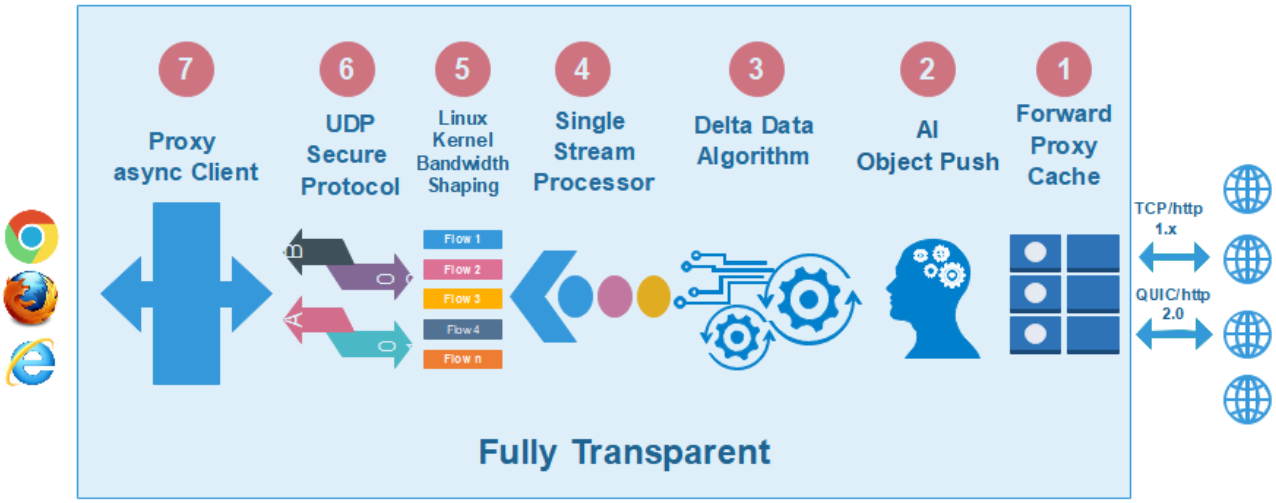
5.2 New AI-Supported Process Chain for WEB Application

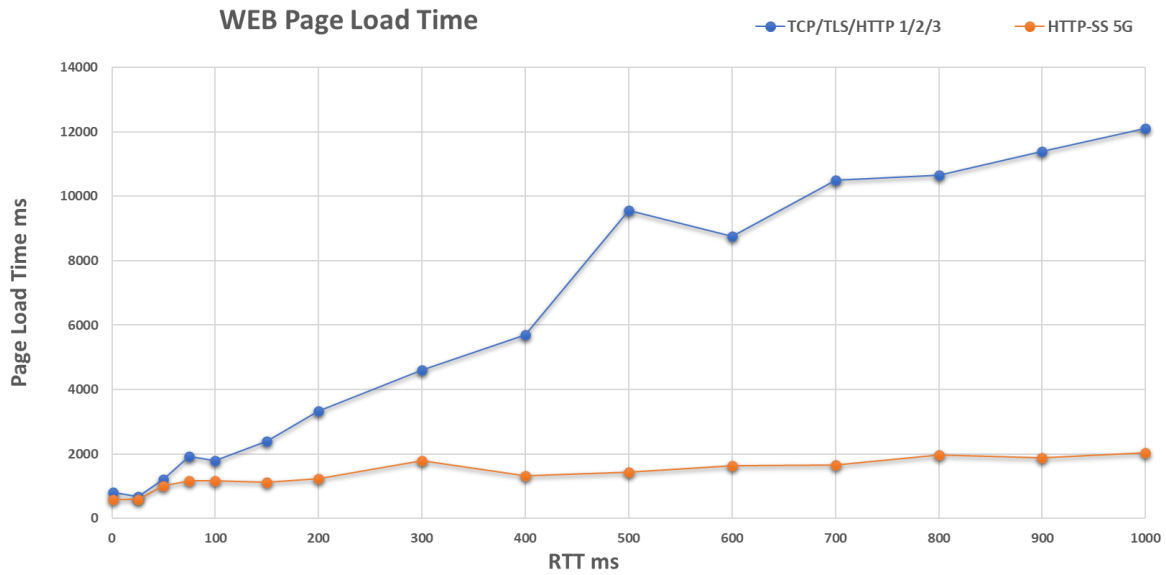
The most important Software we use when we work on the Internet is a WEB Browser no matter opening a WEB Site, downloading a File, or watching Streaming Contents like Videos, Live TV, or MP3 Music.

The most two important Criteria how user feel the Speed of the Internet is:

1. How fast a WEB Site is loaded
2. How fast a big File is downloaded
3. Jerk fee Video display and Music listening

The new world-wide patented and AI-Supported Server Process Chains for all these Kinds of WEB Application significantly improves this important User Experience no matter of long Latency Times or Low Bandwidth.



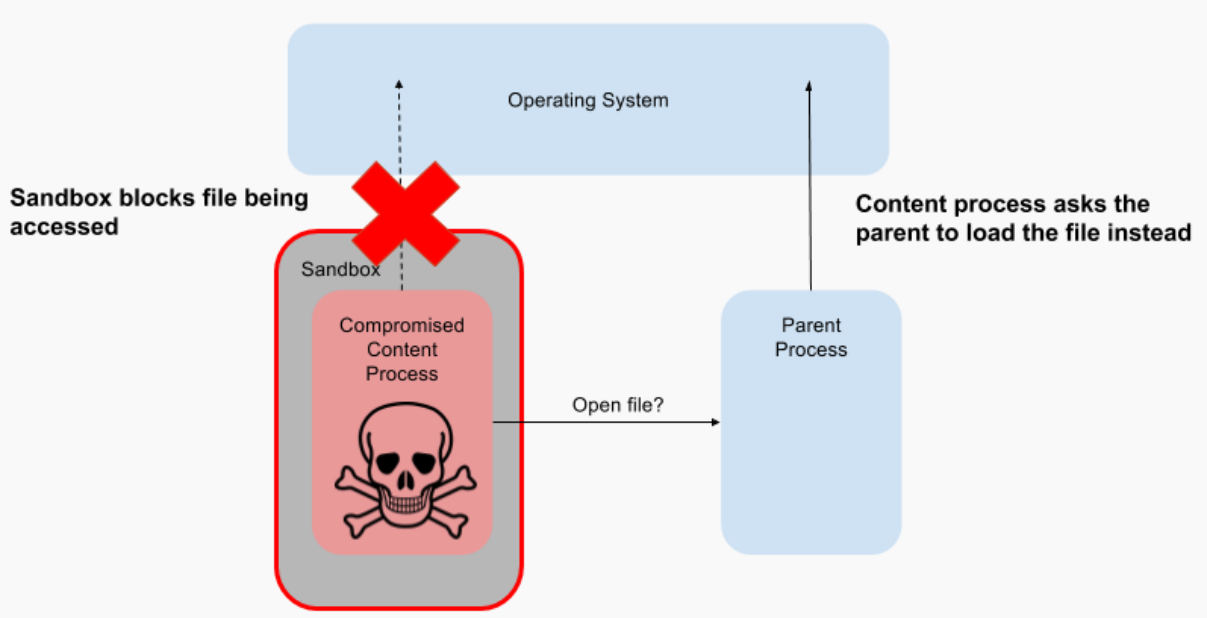


6.0 Integrated Active Real-Time Cyber Security

Computer security, cybersecurity or information technology security (IT security) is the protection of computer systems from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

The field is becoming more and more important due to increased reliance on computer systems, the Internet and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including smartphones, televisions, and the various devices that constitute the "Internet of things". Due to its complexity, both in terms of politics and technology, cybersecurity is also one of the major challenges in the contemporary world.

This new Process Chain for WEB Application includes also an AI supported real-time Sandboxing Cyber Security Module which detects malicious activities caused by all kinds of security vulnerabilities before sending the Data Stream to the WEB Browser.



Advantages

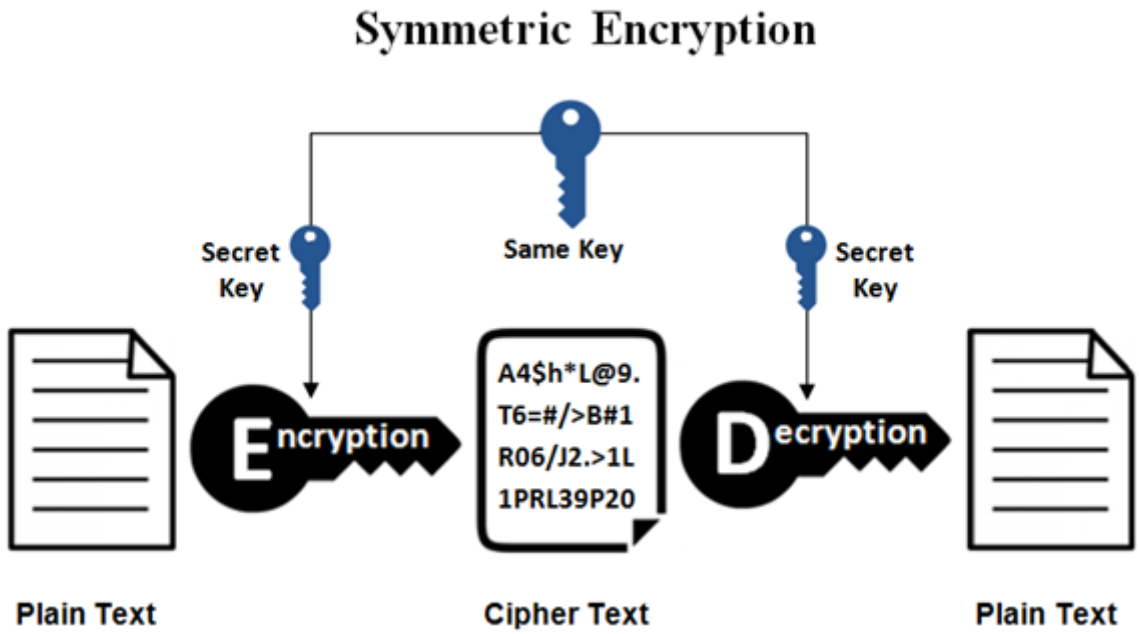
- No need of Antivirus or malicious Software Protection which is difficult to handle by normal End Users
- Real-Time Protection and Defence
- Cookie Protection with digital Spy Defence

7.0 Integrated Quantum-Secure Encryption

Security has grown to be a colossal factor, especially with modern Communication Networks like HTTP-QuSS. Leaving Loopholes that could be leveraged to devastating Effects. The new HTTP-QuSS Process Chain includes a Method for a **Zero Handshake** Encryption that will be used to tighten Communication Security in Symmetric Encryption.

Zero Handshake in this Connection means that there is no Exchange of the important Secret Key over the Network and therefore it is **Quantum Secure**.

Quantum Secure means that it is even very difficult for a **Quantum Computer** with a huge processing power to decrypt the Data Stream between the HTTP-QuSS Server and the Client.



8.0 Climate-Friendly Network Integration

By Using NVIDIA Supercomputer Hardware of the newest Generation for the HTTP-QuSS AI supported Process Chains it is now possible to substitute complete Data Centers by a few Server Modules to save huge amount of electrical Energy.

NVIDIA relies on TSMC (Semiconductor Producer in Taiwan) to produce the Ampere Chips, the Result of the Collaboration is the A100, currently the most complex 7-nanometer Chip in the world. It consists of 54 Billion Transistors, Nvidia's Predecessor Chip Volta from the End of 2017 had just 21 Billion Transistors.

But why should a Company even operate a Data Center full of Graphics Cards?

Because Graphics Cards are ideal for performing complex Calculations for Physics Simulations or for Training Artificial Intelligence Algorithms at a frenzied Pace.