Q&A for the paper ”Heterogeneous Networks for Audio and Video: Using IEEE 802.1 Audio Video Bridging” by Teener et al., Proc. IEEE, 2013.

General:

Is there a naming structure for the standards?

- The first part of the name indicates the Working Group that developed the standard. Upper-case letters indicate a certain document. Lower-case letters are used to indicate an amendment to an existing standard. Finally, the year indicates the year it was published. For example, IEEE 802.1Q-2018 is probably the most famous standard as it specifies how a bridge works. Before it was published, the most recent version was 802.1Q-2014. One of the TSN standards is 802.1Qbv-2015, which is an amendment to 802.1Q-2014. It was later rolled into 802.1Q-2018. Another example is the time synchronization standard 802.1AS-2020. The actual letters (upper-case and lower-case) are given when a standardization project is approved (a so-called PAR – Project Authorization Request) to develop a standard.

The article is relatively old from 2013. What is the status of the TG and the technologies today? Are any of the presented future works existing today?

- While the article is old, it represents technology that is still widely in use and will be continued to be used in the future. The TSN TG has completed many standards since the article was published in 2013. Many of the technologies we covered in the course was developed by the TG (e.g., time-aware shaping, redundancy, ingress filtering, and asynchronous traffic shaping, to name a few).

The paper also mentioned energy efficient Ethernet and I was wondering, what is the relation of the networking strategy with that? isn't the energy management a hardware manufacturing challenge ?

- Not sure. To my knowledge, energy-efficient Ethernet has not been discussed in the context of TSN.

It is mentioned that the interoperability test for devices which follows ABV standards is carried out by AVnu Alliance, but how efficiently? and they are depending on a single third party trusting blindly!!

- AVnu has specified interoperability conformance tests. This has worked out well. AVnu only develops the specifications. The actual conformance and interoperability tests are offered by several companies. Spirent and Ixia are two companies that offer test solutions.

How do we make sure that cut-through switching does not ”pollute” the network with partial packets (i.e. when a stream is preempted)?

- Cut-through switching, while commonly supported in network bridges, is not standardized in 802.1 (but there have been discussions to specify cut-through in 802.1

standards). The effects of cut-through in combination with TSN standards such as preemption has not been widely studied.

Since packet loss is not the most important issue in transmitting streams, why don't we use a wireless network? I know you can not give guarantees about reachability, but I was wondering if there is any work on that.

- Many application still require packet loss to be bounded and not too frequent. Some applications (e.g., professional audio/video in big stadiums) require large physical distances between endpoints and bridges; this may make wired networks favorable.

Is there any information about the implementation of these methods in a specific car? I know that might not be the case because of security issues.

- This annual conference is a good resource (see presentations from past events): https://standards.ieee.org/events/automotive/

The paper very briefly notes packet preemption, but the mechanism is not discussed exactly. Do we need to change the MAC layer in order to support the packet preemption?

- Yes, the MAC layer changes in order to support preemption. This was standardized in 2016 (802.3br and 802.1Qbu). See also the lecture notes.

The paper was published many years ago (i.e., 2013). Is there any new major enhancement on the gPTP mechanism to clock synchronization?

- Yes, there is a new revision of the standard, 802.1AS-2020. For example, it now supports multiple clock domains, which can be used to implement redundancy to handle GM and link failures in gPTP.

PTP:

In the gPTP protocol and best master clock selection, what happens if a GM-capable device is evil or bugged and continues to transmit its own announcements despite there being a "better" one?

- It depends on the priority value that the "evil" device sends. If the priority is lower than the "better" device, all bridges and endpoints will converge towards the correct GM. If the "evil" device sends a higher priority, then bridges will stop forwarding Announce frames from the "better" device, and this may lead to the situation that the "evil" device becomes the GM.
- Security was not really built in to gPTP. One can rely on existing solutions for link layer security, secure boot, etc. to address security issues.

What is the role of a boundary clock and a transparent clock in gPTP?

- PTP has boundary clocks. gPTP does not. A boundary clock is a slave on one port and master on another. Transparent clocks merely forward sync event frames and provide corrections such as residence times.

Can a malicious node exploit gPTP by inducing others to grant itself the GM role and then cause synchronisation errors between other nodes?

- Yes, this could be possible. There is some literature on security attacks on PTP. I will include this important topic in the next edition of the course.

What's the difference between Fig. 5. and Fig. 7.? Why do we need this "averaging- like" process to calculate the path-delay?

- Figure 5 explains how sync and follow-up frames are propagated. These are the frames that are used by devices to adjust their local time.
- In order for bridges to correctly adjust the accumulated delay in the follow-up frame from Figure 5, the delay on each link needs to be calculated. This is done through the averaging-like process in Figure 7. The reason why averaging is a good method is because the link rate is symmetric (same in both directions).

Shaping:

Is it possible to route traffic between Audio Video Bridging endpoints located in separate VLANs using Audio Video Bridging?

- Yes. Stream reservations will need to be made between the endpoints and the device that performs the routing between two VLANs.

When talking about the future of SRP, the paper mentioned the implementation of multiple talkers per stream and I was wondering how could that be implemented? What are the use cases that may pushed the development of the protocol in that direction?

- One possible use case is for redundancy. Imagine a sensor that is critical to the operation of a system, and that a redundant sensor is needed to meet reliability requirements. In this case, a sensor stream could have two talkers. To my knowledge, SRP has not been extended to support such a use case.

How efficient the traffic shaping in reducing the latency while considering the prioritization of packets?

- Traffic shaping actually increases latency with the benefit that lower-priority streams get a certain guaranteed bandwidth. Shaping and prioritization are two tools that can be used to meet the overall temporal requirements of the network.

802.1Qcc introduced the CUC and the CNC as the control plan for TSN-enabled Ethernet networks and the paper treated the coordinated shared networks in general so I was asking could the CNC be used in this context or we should have a separate controller for every technology? and if that is the case, how would these controllers collaborate?

- Qcc is limited to full-duplex, bridged LANs. Coordinated shared networks (CSNs), as defined in the paper, do not fall into this category. Some other control plane, other than what is defined in Qcc, needs to be used to handle configuration of the CSN. This is, to my knowledge, still an open problem, in particular to figure out how these controllers should collaborate.

Regarding Section III B. Supposing two listeners have different paths with different delays to one talker advertising his stream (ie L1: xμ s and L2:3xμs. The text says the talker starts to transmit once it receives the confirmation that a stream has been reserved. Is it possible for the talker to receive a stream reservation from L1 and start transmitting before the registration from L2 propagates back, causing L2 to loose the first few frames of the transmission? How is it dealt with?

- Yes, this can happen and depends on the network topology. AVB/TSN does not deal with this issue. It is expected that this is not a major issue for audio/video applications.

Defining jitter as the difference between best and worst-case response time, the jitter for packets is way more in Traffic Shaping than other scheduling policies (e.g., FIFO). Using FIFO, you can claim a guaranteed response time given a system state. Why don't we use FIFO?

- Egress ports have one or more FIFO queues. The shaper is attached to a FIFO queue. So, even though we use shaping, the packets are still sent in FIFO order.

What's the relationship between credit-based shaper and time-aware shaper in Fig. 10.? In Fig. 10., there is only one "Scheduled Traffic Gate". Does it mean that one "Schedule Traffic Queue" corresponds to one "Scheduled Traffic Gate"?

- Yes, the figure only intends to show the time-aware shaper.

In the Talker/Listener scenario, what happens if the talker sends data with more bitrate than it was supposed to send? Is there any mechanism to reactively adapt to the new situation by the network, or the connection should forcefully be dropped?

- If the talker, due to some error, sends more than it is supposed to, it can lead to errors that may propagate through the network and cause other packets to be dropped. Ingress filtering/policing can be used to mitigate this situation and enforce the reserved bit rates. See our lecture notes.

Security:

In general, are TSN standards developed considering resilience against malicious nodes in the network?

- Not always. There is a Security Task Group within 802.1. The TSN group has mostly relied on the Security task group, which develops MACsec and various authentication solutions.

From a security aspect I'm just curious to know while read about the data formatting concept of AVTP, is there any specific cryptographic algorithms or security standards will be used to ensure that the data preserves privacy?

- MACsec (802.1AE) supports integrity and confidentiality through the use of symmetric-key cryptography.

Would it be possible for a malicious node to flood spoofed stream re- quests in SRP so that the target nodes (the spoofed ones) availability is compromised?

- Yes. Mitigations for these kind of attacks would be the use of MACsec and ingress filtering/policing.