# Simulation-based Evaluation of DoS Protection through Credit Based Metering in Time Sensitive Networking In-Car Networks

Philipp Meyer
philipp.meyer@haw-hamburg.de
Department of Computer Science, Hamburg University of Applied Sciences, Germany

***Abstract*—Ethernet is the most promising solution to reduce complexity and enhance the bandwidth in the next generation in-car networks. The real-time aspects in such networks are becoming possible through special Ethernet protocols. On promising candidate is the IEEE 802.1 Time Sensitive Networking protocol suite. However, the common Ethernet technology increases the vulnerability of the cars infrastructure. In this paper an algorithm is proposed which on the one hand provide protection against DoS attacks on switches by metering incoming Ethernet frames. And on the other hand adapts to the behaviour of the Credit Based Shaping algorithm which was firstly standardized in the Time Sensitive Networking predecessor Audio/Video Bridging. A simulation of this proposed Credit Based Metering algorithm evaluates the concept.**

## I. Introduction

In todays vehicles a multitude of sensors and electronic control units (ECUs) are used to enable better performance, comfort and safety. They are used to enable advanced driver assistance systems and autonomous driving. This results in complex communication architectures containing different proprietary bus technologies.

With the use of Ethernet as a backbone in future cars the architecture could be simple and efficient. Real-time Ethernet protocols enable the compliance of communication requirements and enhance the reliability of Standard Ethernet. One promising candidate is the Time Sensitive Networking (TSN) protocol which is in the process of standardization through IEEE.

The current focus in those protocols is safety. The integration of future cars in the IoT context opens its systems to global communication. This increases the vulnerability of the infrastructure and safety critical functions like brakes or the motor control unit resulting in manipulations of the driving characteristics. The Results could provide fatal consequences for vehicle and passengers.

Therefore security has to be a major goal for the development of the next generation on-board communication technologies.

This work provides a concept for the protection of queues in a TSN switch from DoS attacks. Those queues output is handled by the so called Credit Based Shaper (CBS). But there is no system that controls the input is matching the configured output. Therefore the queues in switches could be filled to prevent other messages from reaching the output destination. Here the concept introduces a Credit Based Metering (CBM) algorithm to control the queues input flow. Its a syntactic approach to prevent that attack independent streams are affected. So a safety relevant stream can not be blocked by not safety relevant streams.

This paper is organised as follows: Section II presents previous and related work. In Section III the concepts of security, in-car networks and the credit based shaping are made known. Section IV introduces the attack scenario and the Credit Based Metering protection concept. Section V provides an simulation based evaluation and analysis of the CBM concept. Finally, Section VI concludes the work and gives an outlook on future research.

## II. Related & Previous Work

In previous work the focus is analysing the safety aspects of combining synchronous and asynchronous traffic in a in-car Time Sensitive Networking architecture [1]. A simulation based analysis of the impact of TDMA traffic on Audio Video Bridging streams is discussed. In contrast this work will analyse security aspects of the asynchronous part of Time Sensitive Networking in-car networks.

Checkoway et al. [2] examine wich interfaces are attackable in an automobile. This interfaces are classified in three categories. The first one is indirect physical access. It includes ODB-II diagnose interface and the infotainment ports (CD, USB). The next category is called short distance wireless access. Examples are Bluetooth, WiFi and Remote-Keyless-Entry. Long distance wireless access is the last category. Interfaces in this part are GPS, digital Radio and mobile services. The authors use reverse-engineering and debugging to gain access to the on-board network in each category. For example through the CD player with a corrupt WMA file, though Bluetooth via stack vulnerabilities or addressable over mobile services. By introducing even more technologies for comfort and safety of cars the quantity of vulnerabilities will rise also. That is why a protocol like TSN has to be secure and robust to prevent the propagation of attacks over the in-car network architecture.

A specific attack is shown in the work of Koscher et al. [3]. They use the ODB-II diagnostic interface to attack the in-car systems. They extract all necessary data by analysing the output of individual ECUs. With this data extensive manipulations

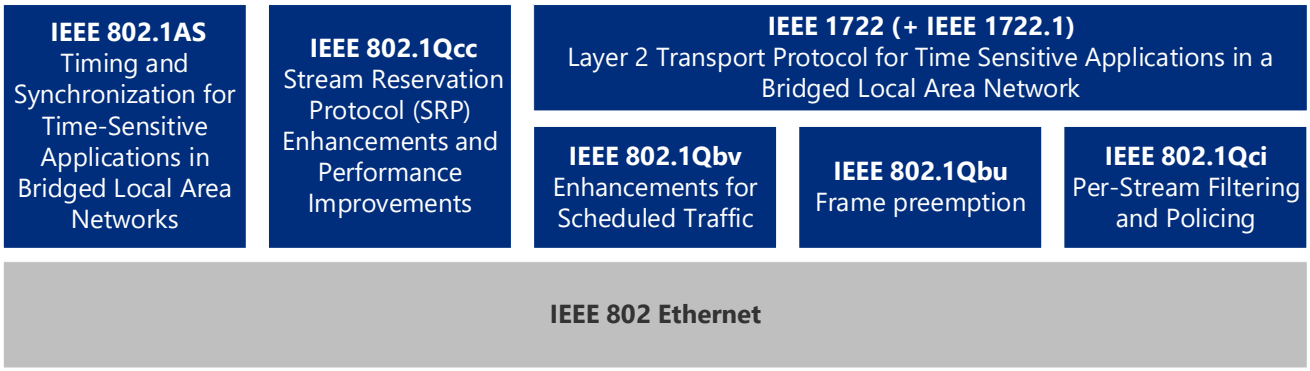


Fig. 1. Time Sensitive Networking Structure

are possible. In the next step this manipulations are executed through a PC connected with the ODB-II interface. This allows access to car components like radio, speed indicator, individual breaks and parts of the engine controls. A less specific but easier way to attack the in-car communication is a Denial of Service (DoS) attack on the busses which can prevent communication between ECUs. This is possible without the effort of analysing individual ECU output and could lead to the same disastrous outcome. In comparison this work examine the prevention of such DoS attacks in the next generation in-car communication. This should avoid corrupt ECUs from destroying the communication between others.

Henniger et al. [4] presenting a structured process to develop security requirements for in-vehicle networks. The base is a car with a heterogeneous bus system composed of CAN and FlexRay busses. The process includes four steps. First step is the identification of threats. This is enabled by attack trees. Here the root is a attack target and the leafs are sub goals that enable the superordinate target. All this targets and sub goals for the attacker are threats to the system. In the second step security requirements are identified which impede the identified threats. The last step is the prioritisation of the security requirements to determine the importance of each requirement. The risk is the indicator of the priority. It is calculated from occurrence probability, checkability and severity. The severity is a vector of different classes. So the damage to humans or financial loss can be rated individually. This process is the base for the discovery of threats to a TSN network in this work. The process is adapted to Ethernet in-car communication system.

Bouard et al. [5] present a middleware independent protection concept for IP based in-car communication. It provides concepts for encryption, authentication, policy administration and recognition of security violations. For the key administration secure hardware is required. Through modularity ECUs with different requirements can be implemented. In contrast this works focus is the transport layer. Weaknesses in this layer can undermine the security concepts in higher layers. Additionally the transition to a full IP based in-vehicle network will be stepwise. So TSN have to support protection mechanisms.

## III. Background

This Section introduces the concepts of security, in-car networks and the TSN credit based shaping algorithm.

### A. Security

The safety aspect is highly integrated in the automobile development process. This did not prevent unauthorised modification and stealing of sensitive information. Therefore security mechanisms have to be implemented in a system. A secure system is also a safe system but not reverse. A secure system provides [6]:

- Confidentiality: Secrecy of data objects. System information is only readable with an appropriate authorisation.
- Integrity: Prevention of unauthorised modification. Prevention of attacks with the target to modify the system behaviour.
- Availability: No loss in performance. Attacks can not corrupt the system performance.

The in-car networks of vehicles with advanced distributed technologies have to have this protection to prevent harm to automobile and passengers.

### B. In-Car Networks

The on-board network of a vehicle is a highly distributed system defined by its electronic control units (ECUs). Currently the communication of this control units is enabled though proprietary bus technologies (CAN, MOST, FlexRay).

The future could be lead to a stepwise transition to Switched-Ethernet networks. Because of the higher bandwidth it is possible to transmit raw data streams of cameras, laser scanners and other sensors in those in-car networks. In addition the further development and acquisition is low priced through the wide distribution of Ethernet technologies. Higher layer protocols are easily adaptable as well.

To support the domain spanning communication of in-car functions a Switched-Ethernet network provides the technology to establish a structured architecture. The future target is to deploy one flat Ethernet network that provides the simultaneous transmission of messages with different priorities.

To maintain a safety communication so called real-time Ethernet protocols are used to guarantee quality of service. They extend the standard Switched-Ethernet protocol functionality.

### C. Time Sensitive Networking

The Time Sensitive Networking [7] real-time Ethernet protocol is a collection of draft standards which are adapted to real-time control stream network requirements. Domains for this protocol suite are for example industrial control facilities or in-car networks. The figure 1 shows major parts of this collection.

The first one is the IEEE 802.1AS [8] for the time synchronisation of TSN applications.

Secondly IEEE 802.1Qcc [9] describes the dynamic route and bandwidth reservation over the network.

IEEE 802.1Qbv [10] provides forwarding and queueing descriptions for the simultaneous transmission of asynchronous and synchronous messages.

The next standard is IEEE 802.1Qbu [11]. It contains the function of frame preemption. This allows to interrupt a packet in transmission for a higher priority frame.

IEEE 802.1Qci [12] describes an ingress control through per-stream filtering and policing. This is where the later, in section IV, introduced Credit Based Metering takes place.

The Last one in this set of standards is the IEEE 1722 transport protocol specified in IEEE 1722 [13] and IEEE 1722.1 [14].

In figure 2 the path of a message through a TSN switch is shown.

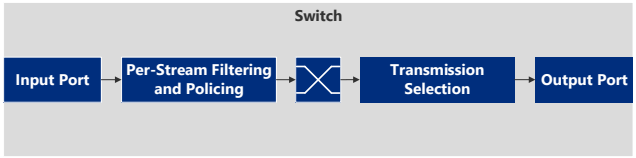


Fig. 2. Message Path in a TSN Switch

Firstly an incoming frame is forwarded to the ”Per-Stream Filtering and Policing” block defined in IEEE 802.1Qci. The function of this is described in detail in the section IV-B.

The next step is the crossbar block which decides the route of the packet.

Each route guides to a ”Transmission Selection” block and the connected output port. The selection implements the forwarding and queuing strategy of TSN IEEE 802.1Qbv.

Each TSN device output behaviour is regulated by the forwarding and queueing strategy. This is shown in detail in the Figure 3.

TSN packets could be assigned to one of eight different priorities (0 lowest - 7 highest priority). A switch has one

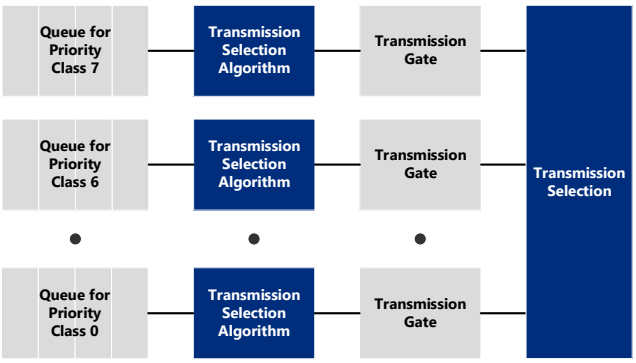


Fig. 3. IEEE 802.1Qbv Transmission Selection

queue per port and priority. Firstly a specific Transmission Selection Algorithm decides if a packet of its queue is ready to be send. One of this algorithms is later described in detail.

In the next step the gate has one of the two states ”OPEN” or ”CLOSE”. This gate states can be static or change in a predefined timed behaviour. If the gate is in the state ”CLOSE” the message has to wait. If its in the state ”OPEN” the last step decides if it can be forwarded to the port.

Transmission Selection is a simple priority based decision. If more than one frame is ready to be send it chooses the one with the highest priority.

The important part in this work is Transmission Selection Algorithm. One of this algorithms is the Credit Based Shaping (CBS) standardized in the Audio Video Bridging (AVB) protocol [15]. It is the predecessor of TSN and specifies message streams that traverse the network over dynamic reserved routes. This reservation contains the maximum interval and size of such stream frames. Therefore the task of the CBS algorithm is to maintain this reserved bandwidth.

The dynamic stream reservation is called Stream Reservation Protocol (SRP) and is defined in the standard IEEE 802.1Qat [16].

The basic functionality is that a source (Talker) broadcasts information of a stream into the network (Talker Advertise). Each switch in this network saves this information and the destination of the Talker.

A sink (Listener) that wants to receive a stream answers with an acknowledge message (Listener Ready). Each switch on the route examine if enough bandwidth is free for the stream. If so the Listener Ready is forwarded in the destination direction and the switch reserved the bandwidth on the specific route. The next switch does the same till the message reaches the Talker.

Now the Talker starts to send the stream. On each device from Talker to Listener a CBS algorithm shapes the traffic flow to comply with the reserved bandwidth on the egress port.

The Credit Based Shaper is defined in IEEE 802.1Qav [17]. It is based on a credit value manipulated by two different gradients called ”$idleslope$” and ”$sendslope$”. This gradients

are composed of the reserved bandwidth ($RB$) and the total bandwidth ($B$) of the connected egress port.

$$idleslope = RB \tag{1}$$

$$sendslope = RB - B \tag{2}$$

The CBS functionality is shown exemplary in figure 4.

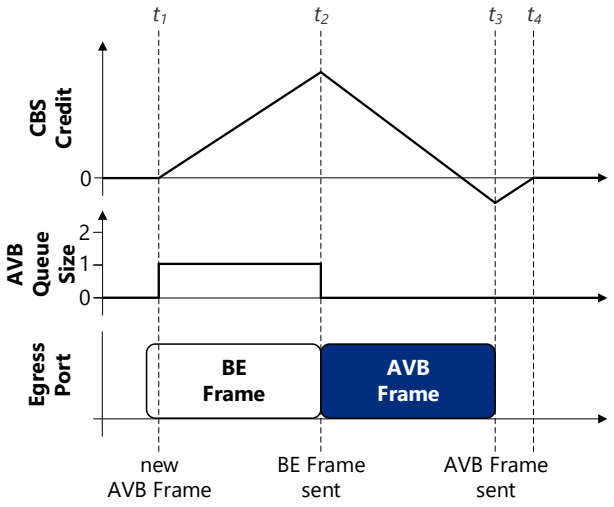


Fig. 4. IEEE 802.1Qav Credit Based Shaping example

At the beginning the credit start with 0. Whenever the credit is greater or equal to 0, an AVB frame is allowed to be transmitted. When no frame is sent and the credit is lower than 0, the credit increases according to the "$idleslope$" till 0 (see $t_3$ in figure 4). If the transmission of a frame is blocked by a higher priority frame, the port is occupied or the specific gate is in the state "CLOSE", the credit increases according to the "$idleslope$" above 0 ($t_1$ in figure 4). If an AVB frame is sent, the credit decreases according to the "$sendslope$" ($t_2$ in figure 4). If no frame is waiting in queue or in transmission the credit stays at 0 ($t_4$ in figure 4).

## IV. Protection through Credit Based Metering

This Section introduces the attack scenario and the Credit Based Metering protection concept.

### A. Attack Scenario

The attack scenario is build upon the previous presented protocols for stream reservation (SRP) and traffic shaping (CBS). The attack tree in figure 5 shows this attack scenario for an AVB switch.

The attack target is to delay or delete frames of a stream traversing the network. The trees root represents this target (see #0 in figure 5).

To enable this an attacker has to fill the queue with the class of the target stream to delay other frames or produce a overflow to provoke the switch to drop other frames (#1 in figure 5). This is possible when the input bandwidth is higher than the CBS is shaping on the output of a switch (#2 in figure 5).

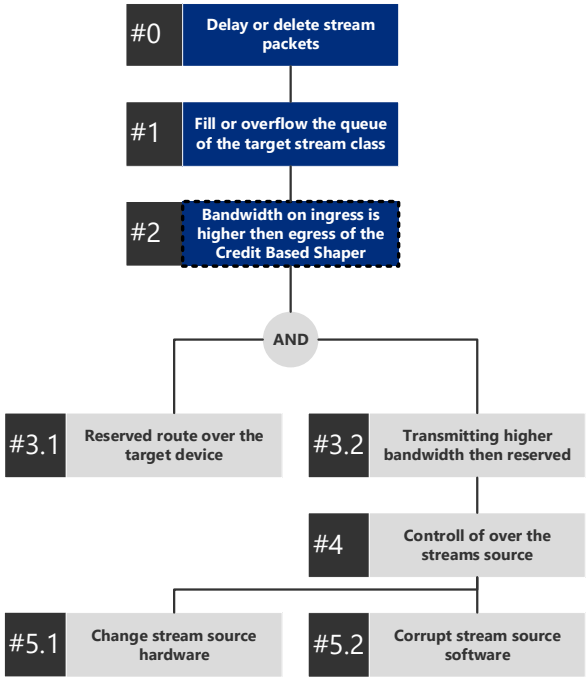


Fig. 5. DoS Attack Tree for an AVB switch

Two criteria have to be fulfilled to produce a higher input bandwidth. First a reserved route over the target switch (#3.1 in figure 5) and secondly a device that sends a higher bandwidth than reserved(#3.2 in figure 5). By taking control over an already established stream source both criteria are achieved (#4 in figure 5). In other cases a Listener for the attack stream has to be connected behind the target switch.

To gain control over a Talker the attack has to corrupt the software or exchange the device running the software (#5.1 and #5.2 in figure 5).

Now the Talker under control can send frames in any pattern. All switches on the path to the Listener will try to forward this frames and queue them in the Transmission Selection queues. If the bandwidth of this transmission pattern exceeds the reserved bandwidth frames from other sources will be delayed or, if the queue is full, destroyed.

### B. Preventing the Attack

To prevent those attacks for different traffic classes IEEE 802.1Qci is in the standardization process. Figure 6 shows the structure of this per-stream filtering and policing.

This mechanism takes place behind each input port of a TSN networking device. The result is that all queued frames are filtered.

There are three levels a message has to pass through before it can be queued.

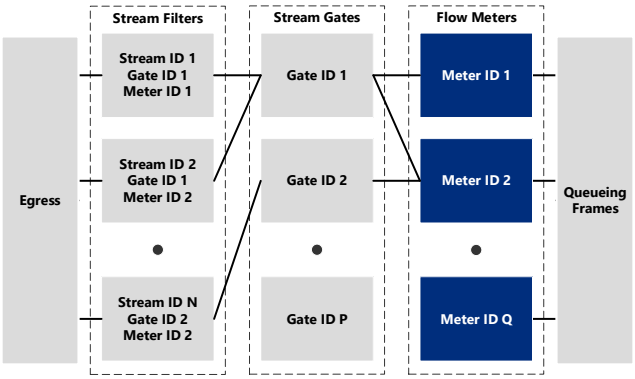


Fig. 6. IEEE 802.1Qci Per-stream filtering and policing

The first are the stream filters. They are configured to decide wich gates and meters are responsible for handling a specific message stream id set.

Secondly there are the stream gates. Those have one of the two states "OPEN" or "CLOSE". This state can change based on a predefined timed behaviour. If the responsible gate is in the state "OPEN" the message forwards to the defined meter. If the gate is in state "CLOSE" the message is dropped.

This flow meters contain individual algorithms to assert if a message is allowed to be queued. This work presents a concept for such a meter called Credit Based Meter. Like the name is hinting it is a specific ingress counterpart for the Credit Based Shaping egress behaviour.

In general the Credit Based Meter is based on a credit value like the CBS. But in this case the reception of the AVB like stream frames is allowed when the credit is greater or equal to 0. When a stream frame is received and the credit is lower than 0 this frame will be discarded.

The Slopes "$idleslope$" and "$sendslope$" from equation 1 and 2 in section III-C are also used for the CBM. The difference is that the reserved bandwidth ($RB$) is the bandwidth of the stream the CBM is metering. Additionally the CBM contains a maximum burst size parameter ($Burst_{max}$) configuring the maximum count of stream frames that are allowed in an incoming burst. This is used in combination with the stream frame sending duration ($T_{duration}$) composed of the frame size ($FS_{stream}$) , the port bandwidth ($B$) and the Ethernet inter frame gap ($T_{ifg}$) to calculate the maximum credit value ($Credit_{max}$) of the CBM shown in equations 3 and 4.

$$T_{duration} = \frac{FS_{stream}}{B} + T_{ifg} \tag{3}$$

$$Credit_{max} = |sendslope| * T_{duration} * (Burst_{max} - 1) \tag{4}$$

Because a burst of one frame is allowed when the credit is 0 $Burst_{max}$ has to be divided by 1. So the definition of $Burst_{max} = 1$ results in $Credit_{max} = 0$.

The CBM state machine is shown in figure 7. It has two major states. They are "RUNNING RECEIVING ALLOWED" (R-RA) and "RUNNING RECEIVING FORBIDDEN" (R-RF).

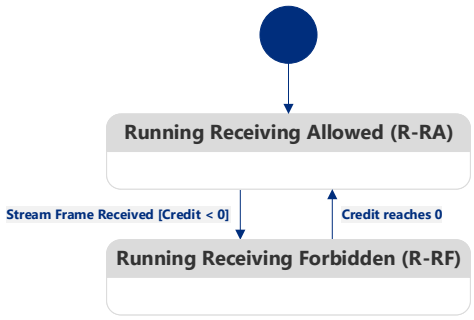


Fig. 7. Credit Based Metering state machine

When the CBM starts the state is R-RA. In this state the credit starts with 0 and increases according to $idleslope$ till the first stream frame is incoming or the credit reaches the maximum. In the second setting the credit now stays at the maximum value until a stream frame is incoming.

In the R-RA state the credit is decreased by "$sendslope$" for the receiving duration of a stream frame. When the frame is received and the credit is greater or equal to 0 the credit increase again with "$idleslope$" or allows an additional stream frame reception and decreases again by "$sendslope$". When the credit reaches the maximum credit it stays on this value until a stream frame is incoming. If the credit is lower than 0 the state will be switched to R-RF.

In R-RF each incoming stream frame will be deleted. Simultaneously the credit increases with "$idleslope$". In the moment the credit reaches 0 the state is changed back to R-RA.

In figure 8 an example of the CBM algorithm behaviour is shown.

Firstly the state is R-RA and the credit is 0 and increases according to "$idleslope$" until the first stream frame arrives (see $t_1$ in figure 8). The credit decreases by "$sendslope$" for the duration of the stream frame ($t_2$ in figure 8). Now the state is changed to R-RF and the credit increases by "$idleslope$" till it reaches 0. The state changes to R-RA and the credit increases further until the next stream frame arrives. This is delayed by an incoming best effort (BE) frame ($t_3$ in figure 8). The next stream frame arrives and the credit is decreased again ($t_4$ to $t_5$ in figure 8). The credit increases till the third stream frame receiving starts ($t_6$ in figure 8). And again the credit decreases by "$sendslope$" until the end of the frames duration.

The performance of the CBM is dependent on $Burst_{max}$. A target configuration of this parameter is as low as possible and still supports a valid worst case scenario.

On the one side this is because of the counterpart CBS. The valid maximum stream frame burst that is produced by an CBS

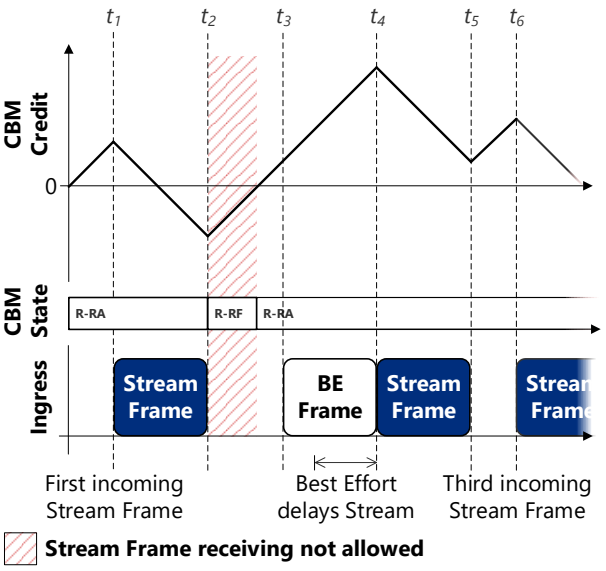


Fig. 8. Credit Based Metering example

algorithm is dependent on its specific worst case scenario.

On the other side a attack created maximum stream frame burst could not harm the network because it is designed to support worst case traffic workload.

There are different ways to determine a minimum $Burst_{max}$ value.

One example is analysing the worst case burst behaviour for each streams output port ($Burst_{out}$). To allow one closeup frame following the burst $Burst_{max}$ has to be calculated like shown in equation 5.

$$Burst_{max} = Burst_{out} + 1 \tag{5}$$

Another example to determine a $Burst_{max}$ value is by simulating different configurations to find one that fits the requirements.

## V. Simulation-based Evaluation

This section evaluates the integration of the Credit Based Metering algorithm. This is done by using the OMNeT++ [18] simulation environment with the INET [19] and CoRE4INET [20] frameworks. For this work the CoRE4INET framework is extended with an CBM implementation.

### A. Topology

The chosen topology is known from previous work [1]. The figure 9 shows this topology.

Three major configurations are simulated. The first is the base configuration without CBM filtering. Secondly a configuration with active CBM filtering is used. The last one emplaces a compromised "Node 1" into the simulation which is spamming into the network.

For all simulations this is the base configuration:

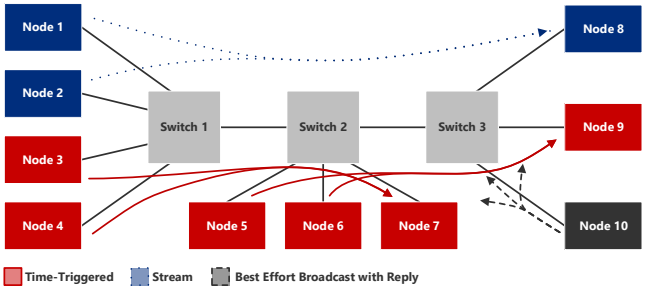


Fig. 9. Simulation Topology

- All links are configured with a bandwidth of 100 Mbit/s.
- "Node 1" and "Node 2" are the sources of the AVB "Stream 1" and "Stream 2" with "Node 8" as its destination. Both class A streams have a reserved route with a individual bandwidth of 25 Mbit/s.
- Full size time-triggered frames are generated by "Node 3", "Node 4", "Node 5" and "Node 6". The first two are received by "Node 7" and the latter by "Node 9". In all switches a gap of 123 µs is configured to allow intermediate stream frame bursts.
- For extra background traffic "Node 10" is broadcasting full size best-effort Ethernet frames. All nodes replying by sending a full size best-effort frame back to "Node 10".

The worst case output stream burst sizes ($Burst_{out}$) are known in this base configuration. They are 2 for "Node 1" and "Node 2" and 4 for "Switch 1" and "Switch 2". Therefore the $Burst_{max}$ value for CBM filtering in "Switch 1" is 3 for both input ports and 5 for the input metering in "Switch 2" and "Switch 3".

### B. Results

The figures shown in this section are a selection of results generated by the simulations. All shown simulation results are based on 10 second duration runs.

The first result set presents and compares the end-to-end latency of the AVB streams in all three major configurations. Because of the assumption that valid packets are not influenced by the CBM these latencies are expected to be nearly the same.

Figure 10 shows the end-to-end latency of the two AVB streams in the base configuration without CBM filtering. Only standard nodes and switches are participating in the network.

Two histograms are shown. They show the number of frames that arrived at the target with a specific consolidated end-to-end latency. Blue shows these results for "Stream 1" and grey for "Stream 2".

"Stream 1" has a maximum end-to-end latency of 925 µs and "Stream 2" a maximum of 899 µs.

The end-to-end latency of both streams in the configuration with CBM filtering is shown in figure 11. In this configuration each node and switch is using a CBM ingress control on each port and for each stream.

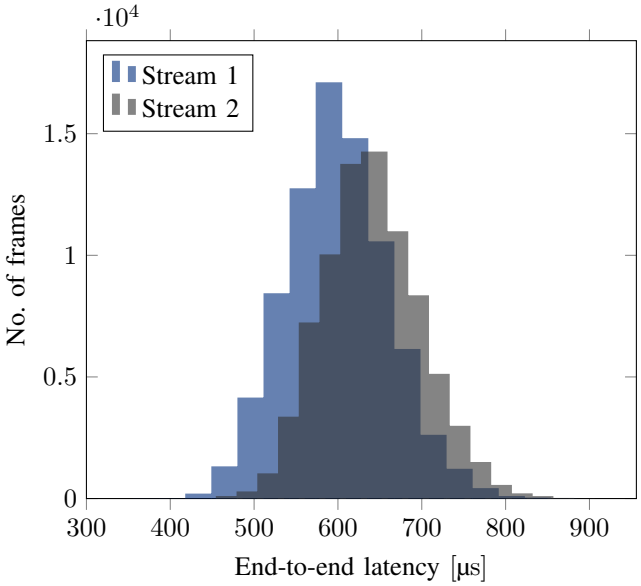


Fig. 10. End-to-end latency of AVB streams without CBM filtering

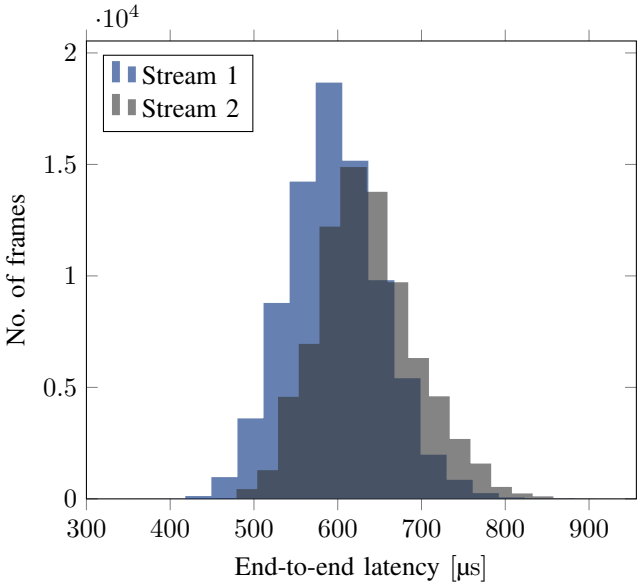


Fig. 11. End-to-end latency of AVB stream with CBM filtering

The representation is the same as in the previous figure.

In this simulation the maximum end-to-end latency for ”Stream 1” is 922 µs and 948 µs for ”Stream 2”.

In comparison with figure 10 it is shown that the use of CBM is not influencing the end-to-end latency of both valid streams. Minor variations are present because of clock inaccuracies in the different nodes.

Finally figure 12 shows the end-to-end latency of the AVB streams in a configuration where ”Node 1” is corrupted. All nodes and switches are using CBM ingress control again. The difference is that ”Node 1” is generating the ”Stream 1” packets in a non valid pattern. In this case by spamming subsequent frames.

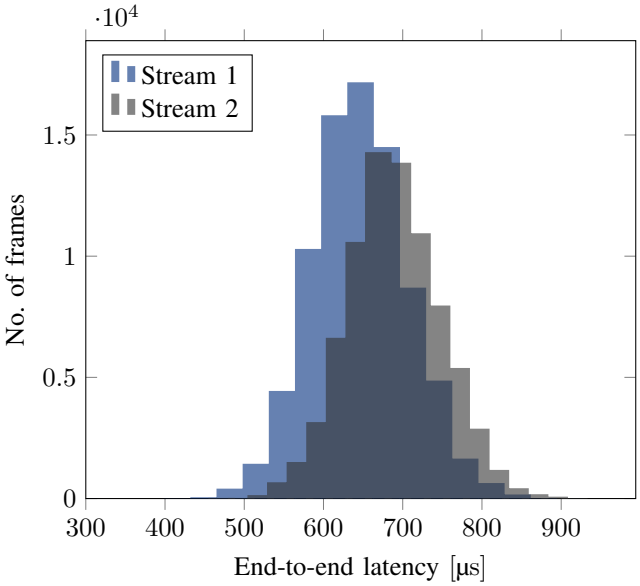


Fig. 12. End-to-end latency of AVB stream with CBM filtering and attack

Again the same representation as in both previous figures is used.

Now a maximum end-to-end latency of 944 µs is recorded for ”Stream 1”. For ”Stream 2” the maximum value is 933 µs.

The comparison shows no major differences between the other two configurations. This demonstrates that CBM is successfully enforcing valid behaviour. This is done by removing all ”Stream 1” frames of the corrupted source that would excel the reserved bandwidth. Therefore passing ”Stream 1” frames are not delayed by successive buffering effects. ”Stream 2” is also not affected by ”Node 1” spamming.

Figure 13 presents output bandwidth size and number of frames dropped in the CBM in ”Switch 1” for ”Stream 1” produced by 8 simulation runs. For each run the input bandwidth produced by ”Node 1” is incremented. The reserved bandwidth of 25 Mbit/s is fixed. It is expected that the output would not cross this reserved bandwidth value.

This reflects the wanted CBM behaviour. No frame is dropped and the output bandwidth is the same as the input bandwidth till the input size overshoot the reserved bandwidth of 25 Mbit/s. At this point the number of frames dropped increases as a function of the input bandwidth. Because each non valid frame will be dropped by the CBM.

A selected section of this CBM algorithm is shown in Figure 14. It presents the credit value, frame ingress and ouput bandwidth for a specific timeslot of the simulation. ”Node 1” produces a valid ”Stream 1” packet flow of 25 Mbit/s in this scenario.

Although the CBM output bandwidth never crosses the reserved bandwidth over time, the zoomed in behaviour allows those crossings like its counterpart CBS.

Because no frame is received between 146.625 ms and 146.75 ms the credit increases as a function of this duration.

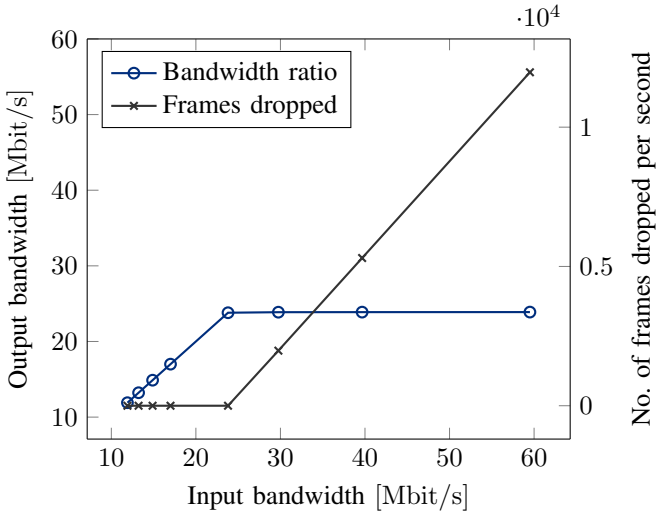


Fig. 13. Impact of CBM filtering on Stream 1 in Switch 1

This continues until it reaches its maximum which is dependent on $Burst_{max}$.

In this case the $Burst_{max}$ value is 3. This results in a $Credit_{max}$ value of ca. 4650. The corresponding equation 6 shows the calculation of this $Credit_{max}$ value.

$$Credit_{max} = |sendslope| * T_{duration} * (Burst_{max} - 1) \tag{6}$$

$$\approx 75\,\text{Mbit/s} * 31\,\mu\text{s} * (3 - 1) = 4650 \tag{7}$$

Now a continuous stream of 3 frames would be allowed. In this case just 2 subsequent packages are incoming. This results in a zoomed in bandwidth of $50\,\text{Mbit/s}$ between $146.75\,\text{ms}$ and $146.875\,\text{ms}$.

This shows that the reserved bandwidth could be overshoot massively for shorter periods. This is dependent on the configuration of $Burst_{max}$. From this follows also that $Burst_{max}$ value has no influence on the over time bandwidth restriction. Buffer sizes have to support the $Burst_{max}$ values to guarantee that they did not overflow.

This upper barrier is enforced by the CBM. For a configured network the maximum delays could be calculated and are valid even if a malfunction or attack results in a non valid behaviour of individual network participants. This protects integrity and availability of the in-car communication system.

## VI. Conclusion & Outlook

Through the interconnected multitude of sensors and ECUs in todays vehicles the demand for a new communication technology lead the development to Ethernet. This seeds new vulnerabilities into the in-car network architecture. The CBM is a solution for a TSN meter algorithm or could be implemented additionally with the AVB protocol to protect the system against DoS attacks. It protects integrity and availability of an in-car communication system by individually controlling the stream input on each port in the network. As

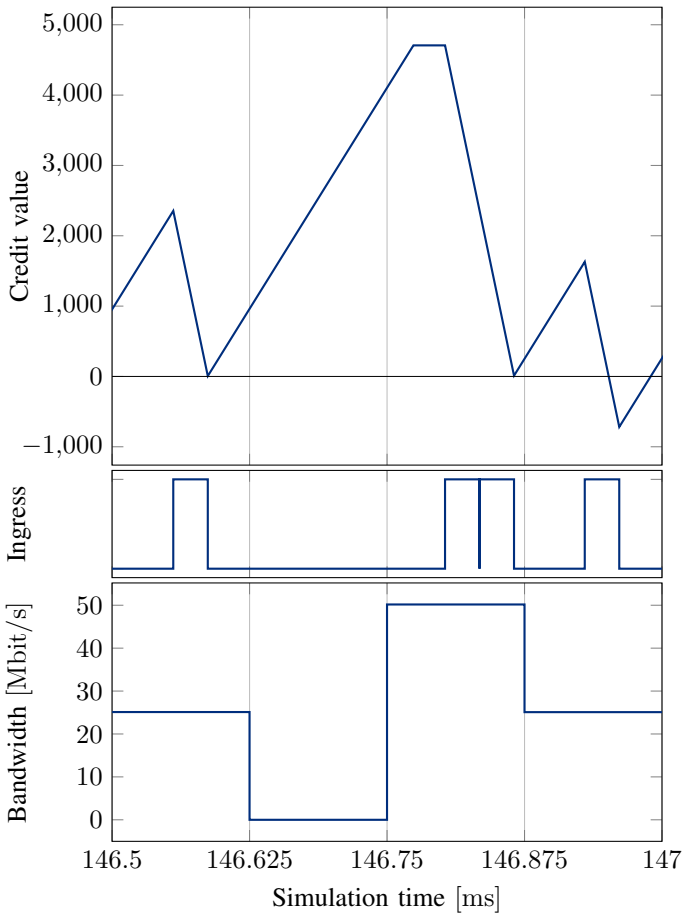


Fig. 14. Section of CBM simulation credit, frame, and bandwidth vector

shown the CBM allows all valid traffic patterns of a CBS algorithm. An attacker could use the burst behaviour to shortly overcome the reserved bandwidth restrictions. However the credit boundary limits the bandwidth over an extended period. This limit is the same as the reserved bandwidth. To gain the best performance the maximum burst parameter has to be as low as possible. But it still must allow the valid worst case scenario of a specific input port. This trade-off between performance and worst case estimation has to be considered.

In future work the compatibility with other TSN traffic shaper concepts will be evaluated. Furthermore combined operation of different ingress control mechanisms will be simulated. In addition the benefits of the ingress control metrics for anomaly detection could be analysed.

## References

[1] P. Meyer, T. Steinbach, F. Korf, and T. C. Schmidt, "Extending ieee 802.1 avb with time-triggered scheduling: A simulation study of the coexistence of synchronous and asynchronous traffic," in *2013 IEEE Vehicular Networking Conference*, Dec 2013, pp. 47–54.

[2] S. Checkoway, D. Mccoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces." *USENIX Security*, 2011. [Online]. Available: http://www.autosec.org/pubs/cars-usenixsec2011.pdf

[3] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental security analysis of a modern automobile," in *2010 IEEE Symposium on Security and Privacy*, May 2010, pp. 447–462.
[4] O. Henniger, L. Apvrille, A. Fuchs, Y. Roudier, A. Ruddle, B. Weyl, T. Paristech, C. Ltci, and S. Antipolis, "Security requirements for automotive on-board networks," pp. 641–646, 2009.
[5] A. Bouard, B. Glas, A. Jentzsch, A. Kiening, T. Kittel, F. Stadler, and B. Weyl, "Driving automotive middleware towards a secure ip-based future," in *10th conference for Embedded Security in Cars (Escar'12)*, Berlin, Germany, November 2012. [Online]. Available: https://www.sec.in.tum.de/assets/staff/alexandre/Escar_Paper_final.pdf
[6] C. Eckert, *IT-Sicherheit Konzepte - Verfahren - Protokolle*, 9th ed. Muenchen: Oldenbourg, 2014.
[7] IEEE 802.1 TSN Task Group, "IEEE 802.1 Time-Sensitive Networking Task Group." [Online]. Available: http://www.ieee802.org/1/pages/tsn.html
[8] ——, "IEEE 802.1AS-Rev - Timing and Synchronization for Time-Sensitive Applications." [Online]. Available: http://www.ieee802.org/1/pages/802.1AS-rev.html
[9] ——, "IEEE 802.1Qcc - Stream Reservation Protocol (SRP) Enhancements and Performance Improvements." [Online]. Available: http://www.ieee802.org/1/pages/802.1cc.html
[10] ——, "IEEE 802.1Qbv - Enhancements for Scheduled Traffic." [Online]. Available: http://www.ieee802.org/1/pages/802.1bv.html
[11] ——, "IEEE 802.1Qbu - Frame Preemption." [Online]. Available: http://www.ieee802.org/1/pages/802.1bu.html
[12] ——, "IEEE 802.1Qci - Per-Stream Filtering and Policing." [Online]. Available: http://www.ieee802.org/1/pages/802.1ci.html
[13] "Ieee standard for layer 2 transport protocol for time sensitive applications in a bridged local area network," *IEEE Std 1722-2011*, pp. 1–57, May 2011.
[14] "Ieee standard for device discovery, connection management, and control protocol for ieee 1722(tm) based devices," *IEEE Std 1722.1-2013*, pp. 1–366, Oct 2013.
[15] Institute of Electrical and Electronics Engineers, "IEEE 802.1BA - IEEE Standard for Local and metropolitan area networks - Audio Video Bridging (AVB) Systems," IEEE, Standard IEEE 802.1BA-2011, Sep. 2011.
[16] ——, "IEEE 802.1Qat - IEEE Standard for Local and metropolitan area networks - Virtual Bridged Local Area Networks - Amendment 14: Stream Reservation Protocol (SRP)," IEEE, Standard IEEE 802.1Qat-2010, Sep. 2010.
[17] ——, "IEEE 802.1Qav - IEEE Standard for Local and metropolitan area networks - Virtual Bridged Local Area Networks - Amendment 12: Forwarding and Queuing Enhancements for Time-Sensitive Streams," IEEE, Standard IEEE 802.1Qav-2009, Dec. 2009.
[18] OpenSim Ltd., "OMNeT++ Discrete Event Simulator." [Online]. Available: https://omnetpp.org/
[19] ——, "INET Framework." [Online]. Available: https://inet.omnetpp.org/
[20] CoRE Working Group, "CoRE Simulation Models for Real-time Networks." [Online]. Available: http://core4inet.core-rg.de/trac/