A Study of In-Vehicle-Network by New IP

Lin Han, Lijun Dong, Richard Li
Futurewei Technologies, Inc.
Santa Clara, California, U.S.A
email: {lin.han, lijun.dong, richard.li}@futurewei.com

***Abstract*— More and more applications in the latest vehicle have higher Quality of Service (QoS) and more deterministic networking requirement for communication. This paper will analyze the challenge of latency requirements for In-vehicle-network (IVN). The paper proposes an architecture to support that requirement based on New IP technology. The new architecture can provide the End-to-End (E2E) Latency Guaranteed Service (LGS) for IP flow level. It can be used for IVN and V2X communication for future Internet. The paper focuses on the design of new IVN control plane and data plane especially queuing and scheduling. The theoretical latency analysis, estimation and experimental verification are provided.**

Keywords- IVN, V2X, TCP; IP; QoS; Deterministic Networking; In-band signaling; Guaranteed service for bandwidth and latency; Class Based Queueing and Scheduling; Cyclic Queueing, End-to-End; Traffic Shaping

I. INTRODUCTION

Recently, a trend in vehicle industry is that electrical or hybrid motors are replacing the combustion engine and power transmission. The major components of Electrical Vehicle (EV) are battery and electrical motors. They are simpler, more modular, and easier to be manufactured with standard and thus reduce the manufacturing threshold. This results in tougher competitions in other areas, such as Tele-driving, Self-driving, Infotainment System, etc. All those advanced futures are computing driven and require advanced networking technologies. There are two areas of networking for vehicle:

1. In-Vehicle-Network (IVN): this is the network inside vehicle to connect different electronic devices, such as Sensors, Actuators, Electrical controller unit (ECU), GPS, Camera, Radar, LiDAR, Embedded computer, etc.
2. Vehicle-to-Everything (V2X): This is a technology that allows moving vehicle to communicate with other moving vehicles, the traffic control system along roads, and communicate anything in Internet, such as Cloud, home, environment, people, etc.

There are different types of applications within a car using IVN or V2X. Based on the requirements for network, traffic can be categorized as three types:

1. The time sensitive: For this type of communication, the latency requirement is stringent, but the data amount is limited. This includes the communication for control data, such as the control for powertrain system, braking system, security system, etc. The data rate is up to Mbps per flow.
2. The bandwidth sensitive: For this type of communication, the latency requirement is not stringent, but the data amount is higher. It includes GPS display, Radar, LiDAR data feeding. The data rate could be up to tens of Mbps per flow.
3. Best-Effort: This is the traditional IP traffic that is not belonging to 1 and 2. Network will deliver the traffic to destination without any guarantee.

The paper proposes to use New IP technology to realize IP based IVN. Section II introduces the New IP. Section III reviews the current technologies. Section IV, V and VI will discuss the architecture for introduction, control plane, and data plane respectively. Section VII addresses the latency analysis and estimation. Section VIII describes the network modeling and experiments. Section IX is about the conclusions.

II. NEW IP INTRODUCTION

New IP is a broad technology set dedicated to solving requirements from future Internet, it is still in research stage. It was first proposed in ITU [1], and some research papers were published [2][3][4].

Compared with the existing IPv4 and IPv6, New IP has many forward-looking visions and will support some new features, such as Free Choice Addressing, Deterministic E2E IP service, it can provide the guaranteed service to satisfy the pre-negotiated Service Level Agreement (SLA). New IP can be used for IVN and V2X since both have very strict QoS requirements especially in latency, jitter, and packet loss that the current IP technology cannot meet.

The paper [4] proposed key technologies to realize a E2E guaranteed service for Internet, details are as following:

1. In-band signaling. This is a control mechanism to provide a scalable control protocol for flow level guaranteed service. Through in-band signaling, the QoS path setup, SLA negotiation, Resource Reservation, QoS forwarding state report and control are accomplished without running extra control protocol like RSVP [5] for IP, or Stream Reservation Protocol (SRP) [6] for TSN.
2. Class based queuing and scheduling. It uses the concept of Class as defined in Differentiated Service (DiffServ) [7] to identify different types of traffic. Different class of traffic is queued into different queue for differentiated service. Priority Queuing (PQ) combined with Deficit Weighted Round Robin (DWRR) or any other Weighted Faired Queuing (WFQ) are used. Compared with other algorithms, this is the simplest to be implemented in high-speed hardware, and can achieve very satisfactory QoS in bandwidth, latency, jitter, and packet loss ratio. It also solves the scalability issue in Integrated Service (IntServ) [8] where the per-flow queueing was used.

 ISBN: 978-1-61208-880-8

3. New TCP/UDP transport stack. The current TCP/UDP transport protocol stack was designed based on the best-effort service from IP, new or enhanced protocols are expected to obtain the benefits if the network can provide guaranteed service while keep the backward compatibility.

Above technologies set will have different way to use for IVN and V2X. For V2X, all technologies could be used, but for IVN, control methods (such as SDN controller) other than In-band signaling can also be used.

It must be noted that the current V2X technologies in 3GPP or academy research are majorly in wireless or spectrum. They are insufficient to solve E2E latency issue in Internet since there are many fixed line networks involved for E2E communication. Only after combining New IP with V2X wireless technologies, we can provide the complete solutions for deterministic service. Figure 1 illustrates New IP enabled IVN architecture in future Internet where both 5G and Internet also need New IP enabled, with such architecture, the true E2E deterministic service can be realized.

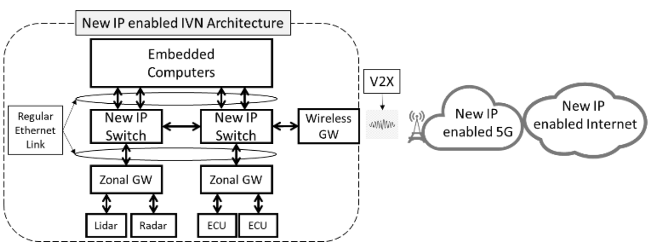

Figure 1. New IP enabled IVN architecture in future Internet

Due to the space limit, the paper will only focus on the queuing and scheduling technology used in IVN to demonstrate and prove that the New IP can provide the satisfactory deterministic service for new IVN. The use of New IP in 5G and other areas will be discussed in the future.

III. REVIEW OF CURRENT TECHNOLOGIES

The section will brief the networking protocols used in current IVN and analyze the latency requirement for IVN.

A. *Network technologies in current IVN*

The traditional IVN uses the legacy protocols, such as Local Interconnect Network (LIN) [9], Controller Area Network (CAN) [10], FlexRay [11]. These are specifically L2 technologies, they use the special designed physical media, signaling to manage strictly and timely for data to satisfy the requirements for communications inside car.

When more and more IP based applications come to IVN, the disadvantage of above legacy protocols is obvious. Its cost is normally higher than the TCP/IP plus Ethernet based network, IP based application must re-write the interface with new underlayer network if it is not Ethernet. AutoSAR [12] has proposed all IP based interface for IVN, and IP based IVN was proposed in [13][14].

However, without special technology, traditional TCP/IP and Ethernet cannot satisfy the requirement of IVN in terms of QoS. That is why IEEE TSN [15] was proposed for IVN [16].

B. *Requirement for IVN*

The most important requirement in terms of QoS for IVN is the communication latency, jitter, and packet loss ratio.

The latency is crucial to the safety of vehicle and will determine if a new technology can be used in IVN. So far, there is no industry standard or requirement for the latency for IVN. Below are some existing publications about the topic:

- From the perspective of fastest human reaction time, the IVN latency must not be slower than that. It is said the fastest human reaction time is 250ms [17]. Some papers gave lower values but not shorter than 100ms if human brain is needed to process the input signal.
- The paper [16] mentioned the latency for control data must be less than 10ms. The paper [13] and [18] said the latency for control data must be less than 2.5ms.

Based on all available analysis, it is safe to assume that the qualified IVN must support the E2E latency not bigger than 2.5ms.

There is no requirement for the jitter from current research. Theatrically, jitter can be removed by buffering technology when the maximum latency is within the target.

The zero-packet-loss is expected for control data. In a packet network (Ethernet or IP), the packet loss is normally caused by two factors: (1) the congestion in network (2) physical failure, such as link, node, hardware. The 1st factor has much more probability and higher packet loss ratio than the 2nd factor. Thus, it must be eliminated for control data in New IP based IVN. The 2nd factor can be mitigated and eliminated by sending the same data to two or multiple disjoined paths to reach the same destination, and/or, sending the same data more than one time as long as the time period is chosen below the upper bound of the latency.

IV. THE ARCHITECTURE - INTRODUCTION

The new architecture of IVN is based on New IP technologies and consists of Control plane and Data Plane. This section will discuss some basics for architecture.

A. *Topologies*

The topologies of new IVN can be any type, but to reduce the complexity and to provide a redundant protection, the paper proposes to use two topologies, one is the Spine-Leaf topology, and another is Ring topology, as shown in Figure 2 and 3.

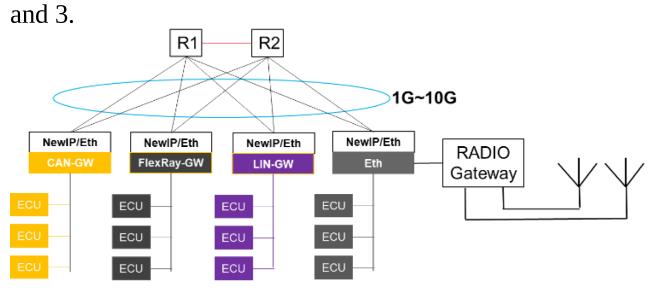

Figure 2. The Spine-Leaf IVN topology

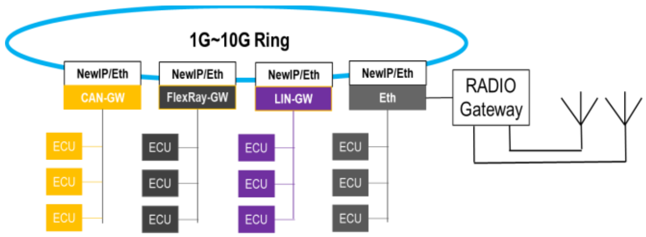

Figure 3. The Ring IVN Topology

In the topologies shown in Figure 2 and 3, there are always two disjointed physical paths between any network devices. Also, the Ethernet Bus is supported. The advantages of such design are:

- The protection of physical link. Any failure of any link does not completely stop the communication.
- The higher reliability for zero packet loss. Multiple paths can be used to transport critical packet to compensate possible packet loss due to temporary failure or fault in physical transmission media.
- Ethernet Bus can make the plug-and-play possible for most of sensors, ECU, computers, etc.

B. Network Device and Link

The network device can be either IP Router or Ethernet Switch, IP router is more powerful to provide more features in networking, such as more flexibility in routing and network state changes, higher link utilization, secured communication, etc.

When Ethernet Switch is selected, DPI (Deep Packet Inspection) should be configured to check the IP level information (address, port, protocol, DSCP values) for admission control for IP flows.

The Physical Link and protocol can be any type of Layer 2 link, Normal Ethernet or IEEE802.1 with the speed higher than 100 Mbps is minimum, and 1G ~10G is better to achieve a shorter latency. There is no need to select any special IEEE802.1Q serials, such as TSN. This is one of the advantages of the new architecture compared with TSN.

C. New Service

The new service provided by New IP based IVN is "E2E and flow level guaranteed service for bandwidth, latency, jitter and packet loss". Following is detail about the new service:

- The E2E is defined as "From Application(s) of one end-user device to other Application(s) of another end-user device. For IVN, the end-user device is any device connected to IVN that supports TCP/IP protocols, and application is running on top of TCP/IP, such as TCP/IP capable ECU, Embedded computer, Infotainment system, Mobile device, etc.
- The Flow can be any granularity, for example, it can be an IP flow defined by 5 tuples (source/destination address, source/destination port number, protocol), or a group of flows defined by less tuples, such as source/destination address.
- The Guaranteed service means that the service provided by system will go through some crucial steps like Service Level Agreement (SLA) negotiation or provisioning, admission control and user traffic conformity enforcement, etc. After all procedures are accomplished, the promised service will meet the negotiated bandwidth, latency, jitter, and packet loss defined in SLA.
- Different application may need different guaranteed service. For example, critical sensor and control data may need the guaranteed service for both bandwidth and latency. The new service is like the service for Scheduled traffic and Real-time traffic defined in FlexRay [11]. For these types of traffic, the strictest service is needed to achieve the minimum latency, jitter, and packet loss ratio. almost all other type of data does not need any guaranteed service, the best-effort service is good enough. For any application, weather it needs the new service is case by case and up to the application's requirement from the networking.

V. ARCHTECTURE- CONTROL PLANE

This section discusses the aspects of control plane for new IVN architecture including the Control Plane Candidates, and Control Plane Functions.

A. Control Plane Candidates

The control plane could have the following candidates:

- Central controller: such as SDN controller or network management controller. For IVN, it is normally a controller's responsibility to provision some basic function for IVN, such as address assignment, routing protocol configuration (for dynamic routing) and static routing table installation (for fast and simple system boot up). Central controller can also be used for the static provisioning for the guaranteed service, such as scheduled and real-time traffic configuration on ECUs,
- In-band signaling protocol [4] is an alternative control method distributed to all network nodes. It can be used for connections between IVN and cloud for critical data in V2X scenario, it can also be used in IVN for dynamic service state report, network state OAM and network problem diagnosis. In-band signaling is not mandatory for communication within IVN.

B. Control Plane Functions

In addition to the static provisioning from a central controller described in A, another key function for the control plane to achieve the guaranteed service support is the Admission Control. All flows requesting new service, except the Best Effort, must obtain the approve for the admission from central controller or from in-band signaling process. This includes three steps:

- An application requesting new service specifies the expectation of service type (BGS, LGS), the traffic pattern (rate specification) and expected End-to-End latency.
- System (Central controller or the network device) will process the request and try to reserve the resource for the flow, and notify the application about the CIR (Committed Information Rate), PIR (Peak Information Rate), bounded end-to-end latency and jitter values, packet loss ratio, etc.

 ISBN: 978-1-61208-880-8

- The application agreed the offered service will send traffic according to the system notification, i.e., send traffic no more than CIR, and monitor the notification from network to adjust the traffic pattern accordingly.

VI. ARCHITECTURE - DATA PLANE

This section discusses the aspects of data plane for new IVN architecture including the Protocol Selection, Queuing and Scheduling Algorithm, Traffic shaping, Latency estimation.

A. *Protocol Selection*

As new IVN is IP based, IPv4 is proposed to be the basic protocol for New IP, a protocol extension is needed if in-band signaling is used [19]. All data process, such as forwarding, traffic classification, traffic shaping, queuing, and scheduling, are for IPv4 data. It is noted that New IP's "Free address choice" feature can provide address shorter than IPv4 that can benefit the latency, but it is not discussed here.

B. *Traffic Classification*

This paper will propose to classify all IVN traffic as Four types. Both Scheduled Traffic (ST) and Real-Time Traffic (RT) are treated as Latency Guaranteed Service (LGS) as described in [4], and other type of traffic that only needs the bandwidth guarantee is treated as Bandwidth Guaranteed Service (BGS):

1. Scheduled traffic (ST). This type of traffic has fixed data size, exact time of when the data is starting and what is the interval of the data. Normally, all sensor data report and control data belong to this type. Typically, IVN can configure the polling mechanism for all sensors to make use of this type of traffic. The service associated with this type of traffic will get LGS. This type of traffic is classified as EF class in DSCP value defined in DiffServ.
2. Real-Time Traffic (RT). This type of traffic has fixed data size, but the time of the data starting, and the data rate is unknow. Normally, all urgent sensor data report and control data belong to this type. IVN can configure the critical sensors to send data to controller in the situation of emergency and the polling mechanism did not catch the latest data changes. The service associated with this type of traffic is also LGS. But the latency and jitter might be a little bigger than for the ST depending on the algorithm and burst of RT. This type of traffic is classified as AF41 class in DSCP value.
3. Bandwidth Guaranteed Traffic. This type of traffic has special requirement from the network bandwidth, but not the latency, jitter, and packer loss ratio. Normally, the IVN software update from cloud, diagnosis data uploading to cloud, on-line gaming and streaming for infotainment system, etc., belong to this type. It can be classified as any AFxy class (other than EF and AF41) in DSCP value.
4. Best-Effort Traffic. This is a default class of traffic, all applications that do not require any special treatment from network perspective can be classified as this type of traffic, Best Effort Class is used.

C. *Queuing and Scheduling Algorithm*

The paper proposes two types of algorithms illustrated in the Figure 4 and 5. One is for asynchronous environment that there is no clock sync for network. Another is synchronous environment that clock is synced with certain accuracy for network including all devices. Below are details, also, the experiment section is based on the two algorithms discussed here.

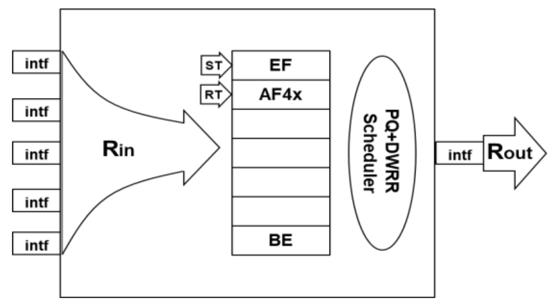

Figure 4. 1st Algorithm: Asynchrous Solution

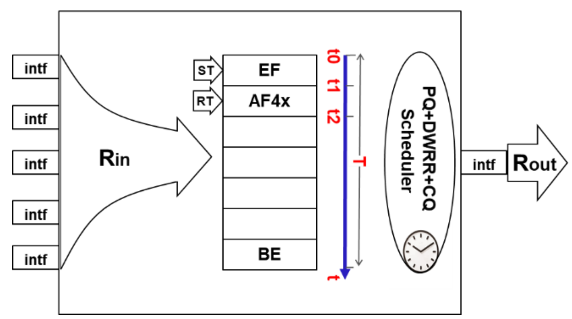

Figure 5. 2nd Algorithm: Synchrous Solution

- For asynchronous environment, Priority Queuing (PQ) combined with Deficit Weighted Round Robin (DWRR) or any type of Weighted Faired Queuing (WFQ) are used. It is called the 1st Algorithm in the document thereafter. Normally, the time sensitive flows, i.e., scheduled traffic (EF class) and real-time traffic (AF41 class) are put into the 1st and 2nd priority of the queue, and other classes of traffic, BGS and Best Effort class of traffic, are put into the lower priority queues. For admission control and scheduler configuration, the total CIR for LGS class, and the WEIGHT values of BGS class can be calculated from the sum of CIR of all flows in the same class. This algorithm has already deeply analyzed in [4].
- For synchronous environment, above asynchronous PQ+DWRR algorithm is combined with Cyclic Queuing (CQ). It is called the 2nd Algorithm in the document thereafter. Each class of traffic has a dedicated time window to be served by the scheduler. The service time is associated with the sum of CIR of all flows in the same service. The Scheduler will calculate and adjust the serving time window for each class when a flow's state is

changed, such as new flow is added, or old flow is removed.

D. Traffic Shaping

Traffic shaping is used to absorb the overflow and burst of the traffic in the class and its objectives are: (1) the packet in the class is never built up, thus reducing the latency (2) traffic in lower priority class is never starved by higher priority traffic. Existing Single Rate Three Color Marker [20] or Two Rate Three Color Marker [21] could be used for traffic shaping. Other type shaping like leaky bucket shaping can also be used. Traffic shaping deployment is very flexible. It can be configured in both ingress and egress interface. It can be per flow based, or per class based.

Flow-level traffic shaping in ingress interface can also be used as the policy enforcement module, it will check the user's traffic to see if it is allowed to pass or trigger some policy, such as discard or put into lower priority to process.

VII. Latency Analysis and Estimation

To provide the Latency Guaranteed Service (LGS) for ST and RT, the network must be able to estimate the latency for a network path and offer to user in the provisioning stage. This is the requirement for SLA negotiation. This section will analyze all factors that can result in network latency and discuss some basic formulas.

A. The Latency Analysis for IP Network

In this paper, the latency estimation is for E2E from the perspective of user's application. The latency must include all delay occurred in network and hosts. This is illustrated in the Figure 6. The formula for the latency is as in (1) and (2). The superscript "LGS" denotes LGS packet.

$$D_{e2e}^{LGS} = PD + \sum_{i=1}^{n}(OD_i^{LGS} + QD_i^{LGS}) + \sum_{s=1}^{m} SD_s^{LGS} = t1 - t0 \quad (1)$$

$$SD_S^{LGS} = L^{LGS} * 8/R_{out} \quad (2)$$

- $t0$: the time the 1st bit of a pack is leaving the application process on the source host.
- $t1$: the time the 1st bit of the pack is received by the application process on the destination host.
- PD: Propagation delay, this delay is limited by the speed of light in a physical media. For example, it is approximately 200k KM/s in optical fiber.
- ODi : The other delays (pack process, deque, de-capsulation, lookup, switch, L2-rewrite, encapsulation, etc.) at the *i-th* hop and source host. This delay is related to the Forwarding Chip and hardware, it is normally and relatively steady for a specified router or switch and can be easily measured. This delay is insignificant compared with QD and SD described below.
- QDi: The queuing delay at the *i-th* hop and source host.
- SDs: The serialization delay at the *s-th* link segment, it can be calculated by the formula (2). L^{LGS} is the packet length (byte) for the LGS flow. R_{out} is the link speed.

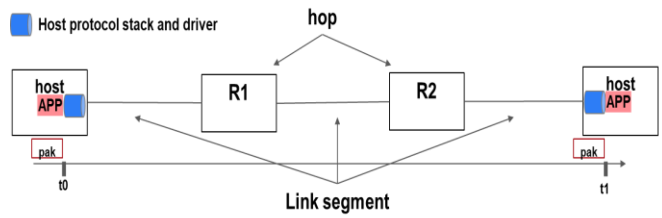

Figure 6. The End-to-End Latency for IP Applications

B. Estimation for the Queuing Latency (QD)

The formulas for the queueing latency estimation (for the same packet size) have been derived in [4] for the 1st Algorithm. In this paper, different packet size for two class is used, thus formulas are different as in [4]. The maximum number of packet and queuing time for a queue (EF or AF4x) under the worst scenario for a hop are shown in equations from (3) to (8).

$$N_{max}^{EF} = \lceil R_{in}^{EF}/R_{out} * (L_{max}^{LOW}/L_{max}^{EF} + 1) + 1 \rceil \quad (3)$$

$$D_{max}^{EF} = N_{max}^{EF} * L^{EF} * 8/R_{out} \quad (4)$$

$$N_{max}^{AF4x} = \lceil R_{in}^{EF}/R_{out} * (L_{max}^{LOW}/L_{max}^{EF} + 1) + 1 \rceil + \lceil (R_{in}^{AF4x}/R_{out} * (L_{max}^{LOW}/L_{max}^{AF4x} + 1) + 1) * (R_{in}^{AF4x}/R_{out}) \rceil \quad (5)$$

$$D_{max}^{AF4x} = N_{max}^{AF4x} * L^{AF4x} * 8/R_{out} \quad (6)$$

$$R_{in}^{EF} = r_{EF} \sum_{i=1}^{m} cir_i^{EF} \quad (7)$$

$$R_{in}^{AF4x} = r_{AF4x} \sum_{i=1}^{n} cir_i^{AF4x} \quad (8)$$

For the 2nd Algorithm, the packet in any queue is served on a pre-allocated time window, and this will guarantee that flows will not be interfered by any packets in other queues. So, it is easy to estimate that the maximum number of packets in a queue is as in (9), (10). The associated queuing time is the same as in (4) and (6). However, for the worst scenario when a packet is out of the allocated window for some reason, the maximum latency will be as the (11).

$$N_{max}^{EF} = \lceil R_{in}^{EF}/R_{out} + 1 \rceil \quad (9)$$

$$N_{max}^{AF4x} = \lceil R_{in}^{AF4x}/R_{out} + 1 \rceil \quad (10)$$

$$D_{max}^{EF} = D_{max}^{AF4x} = T \quad (11)$$

The symbols and parameters in the formulas above are described as below,

- The symbol "⌈ ⌉" is the rounding up operator.
- N_{max}^{EF}: the maximum queue depth for *EF* queue.
- N_{max}^{AF4x}: the maximum queue depth for *AF4x* queue.
- D_{max}^{EF}: the maximum queueing time for *EF* queue.
- D_{max}^{AF4x}: the maximum queueing time for *AF4x* queue.
- R_{in}^{EF}: the ingress rate for *EF* queue.

- R_{in}^{AF4x}: the ingress rate for *AF4x* queue.
- cir_i^{EF}: the Committed Information Rate (*cir*) for the *i-th* flow for *EF* queue.
- cir_i^{AF4x}: the Committed Information Rate (*cir*) for the *i-th* flow for *AF4x* queue.
- r_{EF}: the burst coefficient for the traffic of *EF* queue.
- r_{AF4x}: the burst coefficient for the traffic of *AF4x* queue.
- T: the cycle time for the scheduler when CQ is used.

VIII. NETWORK MODELING AND EXPERIMENTS

To verify and analyze the New IP based IVN architecture can meet the requirements of IVN, OMNeT++ [22] is used to simulate the network, the detailed bandwidth, E2E latency, pack loss, etc., can be retrieved from tests.

A. Network Topology

The network is illustrated in the Figure 7. It is a ring topology but with the cut of another ring link to focus on the latency simulation under the worst scenario (longer latency). All links speed is 100 Mbps. The network consists of ECU, computers, and routers. ECU is to simulate the sensors with control connected on Ethernet Bus. it has a full TCP/IP stack and responsible for the ST and RT generation and process. The ST and RT are simulated by UDP packets. Computers are simulating the generation and process of Best-Effort traffic (TCP and UDP) that is used to interfere ST and RT between ECUs.

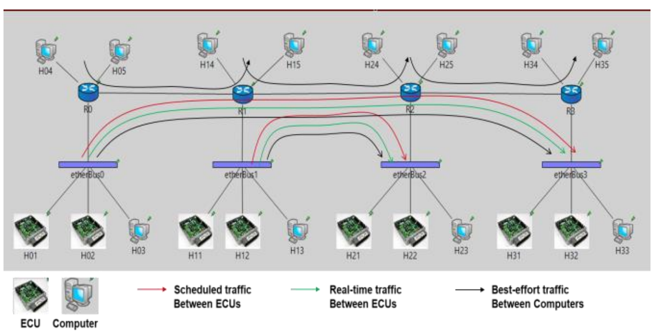

Figure 7. Network Topology and traffic

The purpose of simulation is to illustrate the new architecture can provide the E2E guaranteed service for ST and RT when the network is severely congested and interfered by the Best-Effort traffic. The E2E guaranteed service includes three criteria: (1) bounded latency (2) bounded jitter (3) congestion free and lossless. Moreover, the tested latency and jitter for ST and RT should be close to the estimated latency described in the section VII.

B. Network Devices

Each router consists of Ingress Modules, Switch Fabric and Egress Modules that are illustrated in the Figure 8. The Ingress Modules simulate the traffic classification and ingress traffic shaping functions; The Egress Modules simulate the egress traffic shaping, queuing, and scheduling functions. The Switch Fabric Modules simulate the IP lookup, switching and L2 re-writing functions. Two types of schedulers are used. Only class level traffic shaping is used for ST for ingess and egress.

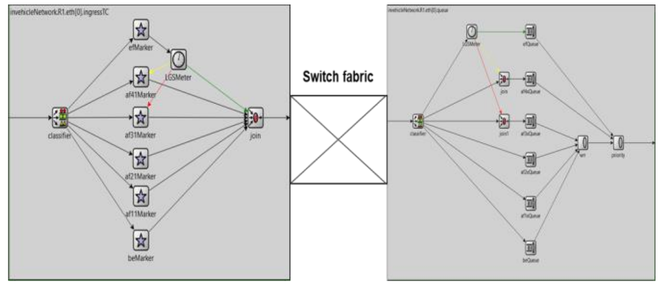

Figure 8. Router structure

C. Traffic Configuration

To simulate the worst scenario, very heavy traffic for the IVN simulation is configured as below:

- There is total 100 ST flows and 100 RT flows using UDP, each flow has the packet size 254 bytes (200 bytes data, 54 bytes of UDP and Ethernet header), the send interval is 10ms. So, each flow has a rate of 203.2 Kbps. Both rate for ST flows and RT flows are 20.32Mbps, it means the remained bandwidth for BGS, and BE is about 60Mbps.
- 50 ST flows and 50 RT flows are from ECU H01 and H02 to H31 and H32, these flows' results are checked and compared with the estimation. 50 ST flows and 50 RT flows are from ECU H11 and H12 to H21, H22.
- There is total 250 interference flows configured between other computers. The interference flows will cause all links between routers congested, R1 link Eth[0] is the most severely congested router and link. All flows packet size are 200 bytes or 1500 bytes. Both TCP and UDP are configured for interference flows.

D. Cyclic Queueing and Scheduler Configuration

For the 2nd algorithm, the detail of the cyclic queuing is configured as in Figure 9.

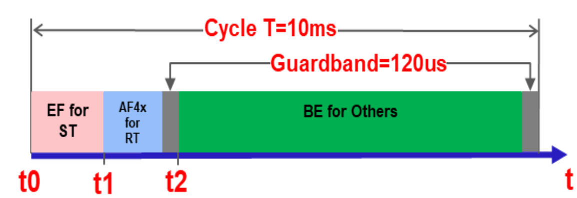

Figure 9. The Cyclic Queueing Configuration

o The cycle T for all router and hosts are 10ms.
o A guard band of 1500 bytes or 120 us are configured for both AF41 and BE classes. This is to protect the higher priority packets (EF and AF4x) are not interfered by lower priority packet.

o The time window size for EF and AF41 are 22% and 32% of the cycle T respectively.

E. Experiment Results and Analysis

The Table 1 shows the detailed calculation for the E2E latency estimation. First, estimate the maximum number of packets in each egress link of all routers on the path, then calculate the maximum queuing delay. The minimum E2E latency means there is no queueing latency in each hop, so it is determined by the sum of all link segment's serialization latency on the path. Each 100M link will have 20.3 us serialization latency for 254 bytes ST or RT traffic. The burst coefficient for each case is also shown in the Table. Higher coefficients for router R0 and R1 are selected since there are aggregation of the traffic for the routers. For other routers, the coefficient is selected as 1, or no burst effect.

TABLE 1. THE E2E DELAY ESTIMATION OF ST AND RT FLOWS

Algorithm	Class and traffic	Estimated max number of packet in Egress Q					Estimated Total Queuing Latency (us)	Calculated Total Serialization Delay (each hop has 20 us)	Estimated Total E2E Delay (us)
		Host	R0	R1	R2	R3			
PQ+DWRR	EF for ST	0	3 (r_{EF}=2)	6 (r_{EF}=4)	3 (r_{EF}=1)	3 (r_{EF}=1)	305	100	405
	AF4x for RT	0	4 (r_{AF4x}=2)	6 (r_{AF4x}=4)	4 (r_{AF4x}=1)	4 (r_{AF4x}=1)	365	100	465
PQ+DWRR +CQ	EF for ST	0	2 (r_{EF}=1)	2 (r_{EF}=1)	2 (r_{EF}=1)	2 (r_{EF}=1)	162	100	262
	AF4x for RT	0	2 (r_{AF4x}=1)	2 (r_{AF4x}=1)	2 (r_{AF4x}=1)	2 (r_{AF4x}=1)	162	100	262

Table 2 shows the Min/Max E2E Delay for the worst performed flow, and estimation values also compared. The worst performed flow is defined as that the flow's Max E2E delay is the biggest in all flows in the same class.

Jitter is not shown in the table, but it can be easily calculated by the variation of mean and Min/Max value, the mean value can be simply calculated by the average of Min/Max values.

TABLE 2. THE COMPARISON OF EXPERIMENT RESULT AND ESTIMATION

Algorithm	Min/Max E2E Delay (us) for the worst performed flow carrying ST between H01/H02 to H31/H32		Min/Max E2E Delay (us) for the worst performed flow carrying RT between H01/H02 to H31/H32	
	Experiment	Estimation	Experiment	Estimation
PQ+DWRR	108/391	100/405	278/542	100/465
PQ+DWRR+CQ	109/152	100/262	169/169	100/262

Figure 10-13 illustrate the E2E delay changes with time for the worst performed flows shown in the Table 2.

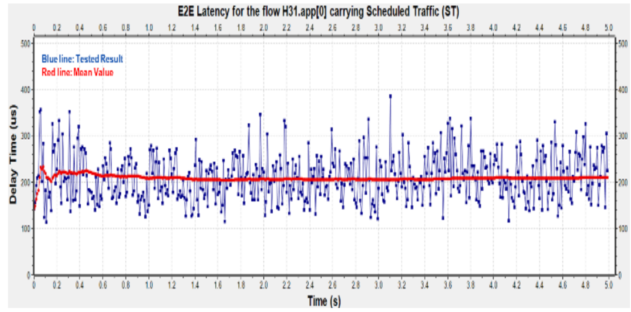

Figure 10. 1st Algo: The E2E Latency (min=108us, max=391us) for the worst performed ST flow

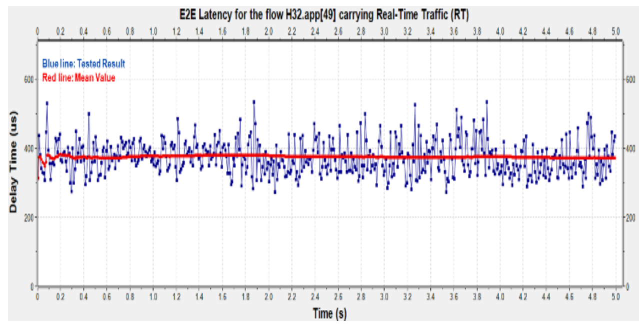

Figure 11. 1st Algo: The E2E Latency (min=278us, max=542us) for the worst performed RT flow

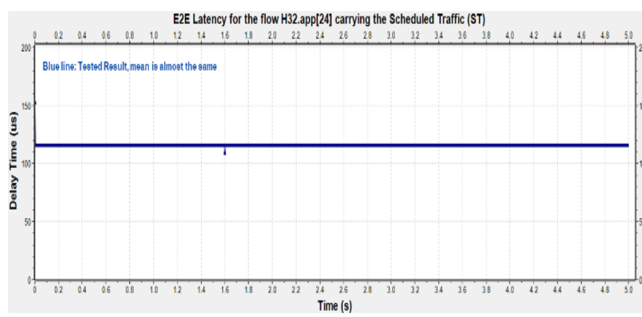

Figure 12. 2nd Algo: The E2E Latency (min=109us, max=152us) for the worst performed ST flow

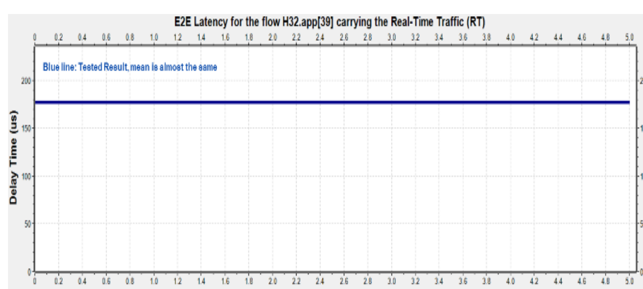

Figure 13. 2nd Algo: The E2E Latency (min=169us, max=169us) for the worst performed RT flow

To demonstrate the lossless and congestion-free for ST and RT flows, Figure 14 shows the statistics of all queues in R1 for two algorithms. No packet dropped in EF and AF4x queues while there are packets dropped in BE queue. This is as expected, congestion should only happen for BE traffic, ST and RT flows are not impacted and are lossless and congestion-free. R1 is the most severely congested, other Router's queues also have similar pattern. No packet drops for EF and AF4x.

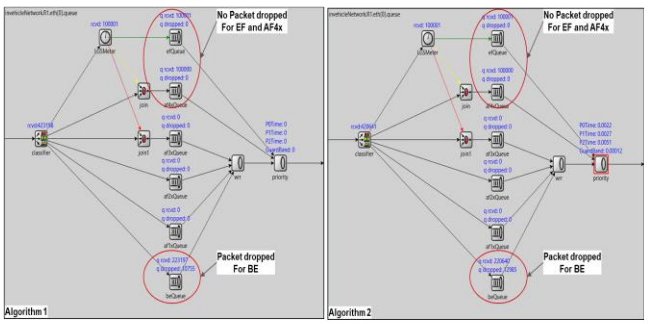

Figure 14. The statistics for all Queues for two algorithms

Here is a summary from the test results:

- The queuing latency of higher priority queues by PQ is very short and is not impacted by the congestion of lower priority class of traffic. E2E Maximum latency estimation in the section VII can cover almost all traffic's real maximum latency.
- Lossless and congestion free can be achieved for ST and RT flows if the admission control is done for the flows.
- The E2E latency shown in the experiment does not include "Other Delay" and "Propagation Delay" described in section VII. "Propagation Delay" is very trivial in IVN, but "Other Delay" should be considered and added up if they are significant compared with the final queueing latency. For most of forwarding chip, "Other Delay" is very small and below hundred microseconds, but for x86 based virtual router, it might not be true depending on the forwarding software design.
- The latency per hop is inversely proportional to the link speed. For example, the experiment using 100M link with 4 hops network can achieve hundreds microsecond for E2E latency. It is expected that the corresponding latency for the same network is about tens of microsecond and couple microseconds for 1G and 10G link, respectively. Higher link rate will not only reduce latency, but also provide more bandwidth for non-time-sensitive applications. So, the paper proposes to use at least 1G link for the IVN in the future.

IX. Conclusions

Classed based queueing and scheduling plus traffic shaping can provide per-hop guaranteed LGS and BGS. Combined with Central Controller or In-band Signaling, the E2E guaranteed service for IP network can be achieved by enforcing the per-hop guaranteed service on all network devices on the IP forwarding path. The solution is backward compatible as the existing IP traffic can coexist with the new classes of traffic.

If the accurate clock can be provided, the synchronous solution by using CQ could improve the latency and jitter significantly. But it must be noted that costs of synchronous solution are not trivial, following tasks are mandatory:

- The crucial requirement of using CQ is the clock sync in the IVN, this is a different topic, and the paper does not address it. Basically, a central controller or distributed protocol, such as IEEE1588 can be used to sync all device clock with a certain accuracy.
- Cycle value selection. The cycle value and the clock accuracy requirement depend on each other, both will determine the granularity of the served packet size, the link utilization, the maximum latency, and the cost of the scheduler design.
- Time window allocation for different flows with different constraints in bandwidth and latency. The optimized solution needs complicated math and cause an overhead for the solution.

As a summary, the New IP based IVN can satisfy very well the requirements for the communications of different applications. It opens the door for future IVN and V2X.

Further research is still needed in the following areas:

- TCP congestion control: The congestion control for different service is expected to be different. New algorithms are critical for application to effectively utilize the new guaranteed service provided by network.
- New TCP and UDP stack for IVN: More efficient and faster protocol stack are needed to improve the control of new service and reduce the latency happened on host protocol and interface.
- Algorithm for network resource planning and allocation for synchronous solution, such as optimized cycle number, fast and efficient time slot allocation, scheduler management, etc.

References

[1] S. Jiang, S. Yan, L. Geng, C. Cao, and H. Xu, "New IP, Shaping Future Network: Propose to initiate the discussion of strategy transformation for ITU-T", TSAG C-83

[2] R. Li, A. Clemm, U. Chunduri, L. Dong, and K. Makhijani, "A New Framework and Protocol for Future Networking Applications," ACM Sigcomm NEAT workshop, 2018, pp 21–26.

[3] L. Han, Y. Qu, L. Dong and R. Li, "Flow-level QoS assurance via IPv6 in-band signalling," 2018 27th Wireless and Optical Communication Conference (WOCC), 2018, pp. 1-5, doi: 10.1109/WOCC.2018.8372726..

[4] L. Han, Y. Qu, L. Dong and R. Li, "A Framework for Bandwidth and Latency Guaranteed Service in New IP Network," IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2020, pp. 85-90, doi: 10.1109/INFOCOMWKSHPS50562.2020.9162747.

[5] R. Braden, L. Zhang., S. Berson, S. Herzog, and S. Jamin, "RFC 2205: Resource ReSerVation Protocol (RSVP)-Version 1 Functional Specification", IETF, Sept. 1997.

[6] "Stream Reservation Protocol (SRP)", IEEE 802.1Qat

[7] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, “RFC 2475: An Architecture for Differentiated Services,” IETF, Dec. 1998.

[8] R. Braden, D. Clark, and S. Shenker, “RFC 1663: Integrated Services in the Internet Architecutre: an Overview,” IETF, Jun. 1994.

[9] LIN, "ISO/AWI 17987-8"

[10] CAN: “Road vehicles - Controller area network (CAN) - Part 1: Data link layer and physical signalling”, ISO 11898-1:2003

[11] FlexRay: ISO 17458-1 to 17458-5

[12] AUTOSAR: AUTomotive Open System ARchitecture

[13] H. Lim, L. Völker, and D. Herrscher, “Challenges in a future IP/Ethernet-based in-car network for real-time applications”, 48th ACM/EDAC/IEEE Design Automation Conference (DAC), 2011

[14] R. Steffen, R. Bogenberger, J. Hillebrand, W. Hintermaier, A. Winckler, and M. Rahmani, “Design and Realization of an IP-based In-car Network Architecture”, Proceedings of “1st International ICST Symposium on Vehicular Computing Systems”, 2008

[15] "IEEE 802.1 Time-Sensitive Networking Task Group".

[16] "P802.1DG – TSN Profile for Automotive In-Vehicle Ethernet Communications". 1.ieee802.org.

[17] Evan Ackerman, “Upgrade to Superhuman Reflexes Without Feeling Like a Robot”

[18] S. Tuohy, M. Glavin, C. Hughes, E. Jones, M. Trivedi and L. Kilmartin, "Intra-Vehicle Networks: A Review," in IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 2, pp. 534-545, April 2015, doi: 10.1109/TITS.2014.2320605.

[19] “Supporting internet protocol version 4 (IPv4) extension headers”, United Stats Patent, 10,742,775.

[20] J. Heinanen and R. Guerin, “RFC 2697: A Single Rate Three Color Marker”, IETF, Sept. 1999.

[21] O. Aboul-Magd and S. Rabie, “RFC 4115: A Differentiated Service Two-Rate, Three-Color Marker with Efficient Handling of in-profile Traffic”, IETF, Jul. 2005.

[22] "OMNeT++ Discrete Event Simulator"