Critical Packet Loss Improvement in the AFDX Communication Protocol

Fatemeh Masoodi-pour
Dependable Distributed Embedded Systems (DDEmS) Laboratory,
Department of Computer Engineering
Ferdowsi University of Mashhad
Mashhad, Iran

Yasser Sedaghat
Dependable Distributed Embedded Systems (DDEmS) Laboratory,
Department of Computer Engineering
Ferdowsi University of Mashhad
Mashhad, Iran

Mohammad Hossein Yaghmaee
IP-PBX Type Approval Laboratory,
Department of Computer Engineering
Ferdowsi University of Mashhad
Mashhad, Iran

Abstract— Nowadays, Avionics Full Duplex Switched Ethernet (AFDX), as a safety-critical communication protocol, is employed in modern aircrafts, such as the Boeing B787 and Airbus A380. This protocol has been equipped with a variety of fault tolerance techniques. However, some of these techniques (e.g., a protecting technique from the babbling-idiot failure) may result in some consequences such as packet loss. AFDX is a real-time communication protocol and therefore, if a packet arrives after its deadline, the packet will be discarded in the receiver node. In this paper, a traffic policing algorithm and a scheduling algorithm are proposed to resolve the mentioned issues. To evaluate the proposed technique, the primary and the improved AFDX networks have been simulated with OPNET simulator. The simulation results have been seen that the number of lost packets, due to deadline miss, is decreased about 10%. Furthermore, the number of discarded packets due to the traffic policing algorithm has been improved up to 100%.

Keywords— Avionics Full Duplex Switched Ethernet (AFDX); Fault tolerance; Traffic policing algorithm; Scheduling algorithm; OPNET simulator

I. Introduction

A failure in a safety-critical system results in loss of human lives, significant property damages, or cause extensive environmental damages. Therefore, fault tolerance becomes an important requirement to prevent system failures. A typical example of these systems is avionics systems which are employed in the aviation industry, such as aircraft [1]. The avionics system is designed as a distributed system which consists of subsystems, such as navigation, monitoring, aircraft flight control systems, collision-avoidance systems, weather systems, and aircraft management systems.

Until the 1990s, the avionics distributed systems were analog with point-to-point connections [2]. With the development of digital technology, analog systems were replaced with digital systems. Therefore, the exchange of data between them was possible through a communication network [3]. Recently, AFDX is the most commonly implemented protocol on long-haul, wide-body, and large passenger airliners such as the Boeing B787 and Airbus A380 [4].

In distributed systems, the communication network is a single point of failure [5]. Any failure in the network will cause one or more packets to fail to reach their destinations which is known as a packet loss [6]. Packets are the fundamental unit of information transport in all networks. In case of packet loss, even if the connected subsystems work correctly, they cannot communicate with each other, and the system will fail. Various factors that may result in packet loss are as follows [6,7]:

- Change of the values of the routing table
- Missing the Packet deadline
- Change of the packet content
- Not enough buffer storage on a switch in the packet transmission path
- Hardware failure
- Network congestion

In the last factor, a system does not allow other systems to send their packets (due to resource constraints) by creating multiple copies or sequentially sending a packet. This type of failure is known as a Babbling-idiot failure [8].

AFDX is a safety-critical avionics network protocol which is equipped with fault tolerance techniques to guarantee correct communications among avionics systems. For example, a traffic policing unit is employed in switches to protect the network from the babbling-idiot failure [9]. To achieve this goal, the concept of a virtual link is introduced in the AFDX protocol, and a specified bandwidth is assigned to any virtual link. This bandwidth is determined by two parameters, i.e., Bandwidth Allocation Gap (BAG) and largest length of VL frames (L_{MAX}). Each received packet is policed with the bandwidth assigned to the virtual link. Packets that do not adjust to this bandwidth are discarded.

With the mentioned policy, if a system should send packets which need more bandwidth than the determined value, these packets are discarded, even if they are critical. To resolve the mentioned issue, the traffic policing algorithm presented in [8] does not pay attention to the virtual link bandwidth for sending critical packets, therefore the critical packets are not discarded. However, in the proposed traffic policing algorithm, a system can cause babbling-idiot failure by creating multiple copies or sequentially sending a packet. Therefore, the mentioned traffic policing algorithm needs to be modified such that if there is not enough virtual link bandwidth for valid critical packets, these packets are not discarded as far as possible.

Furthermore, AFDX is a real-time communication protocol. In the real-time networks, if the packet's deadline is expired, the packet will be discarded by the receiver node, which results

978-1-7281-8566-8/20/$31.00 ©2020 IEEE

in a packet loss. In these networks, a scheduler plays an important role to reduce the number of discarded packets due to deadline misses. To deliver packets before their deadline, the deadline should be considered as a main parameter in the scheduling algorithm.

In this paper, a traffic policing algorithm and a scheduling algorithm are proposed to reduce the number of discarded critical packets. In the proposed traffic policing algorithm, for each physical link, the remaining bandwidth is calculated. This bandwidth is the difference between the general bandwidth of physical link and the total bandwidth of virtual links that is carried by the physical link. However, if the remaining bandwidth does not exist for a physical link, the unused bandwidth of other virtual links which are carried by that physical link can be used.

Moreover, a scheduling algorithm is proposed to reduce the number of discarded packets due to a deadline miss. This algorithm initially sends packets with high priority and earliest deadline. In the result, the destination will discard less critical packets due to deadline miss.

The paper is structured as follows: In Section II, the main properties of AFDX protocol are described. Section III reviews common failures and the fault tolerance techniques for AFDX, as a switch-based network. The proposed traffic policing and scheduling algorithms are explained in Section IV. In Section V, the simulation results are presented and finally, Section VI concludes the paper.

II. Overview of The AFDX Protocol

Avionics Full Duplex Switched Ethernet (AFDX) is based on Ethernet protocol. The main characteristics of AFDX are full-duplex, redundancy, deterministic, and high-speed performance [15]. The AFDX protocol meets the requirement of reliability for avionics systems by having a duplicated network, and this means that each packet is sent through two networks [7]. The AFDX network consists of End Systems (ES), Virtual Links (VLs), and switches, which will be reviewed.

A. End system

It comprises two parts: the transmitting and the receiving ES. The transmitting ES is responsible for sending frames from the system to the duplicated network, and consists of the following main functions:

- A regulator is responsible for controlling the time interval between two frames.
- Virtual Link Scheduler multiplexes received frames from regulators and specify the order of sending frames.
- In Redundancy Management (RM), to specify the order of the frames, the Sequence Number (SN) field is added to the frame. After adding SN, the frame is duplicated and sent to the MAC interface.

The receiving ES is responsible for receiving frames from the duplicated network and consists of the following main functions:

- Integrity Checking (IC) detects and eliminates frames with an invalid SN.
- Redundancy Management (RM) or Redundancy Check (RC) in the receiver node evaluates two frame sequences delivered by IC. Then, this unit forwards one of two frame copies to the destination.

B. Virtual Link

Each AFDX ES is connected to the switch via a physical link. However, it is possible to define many logical communication links, called Virtual Links (VL). Packets are routed from the specified path for each virtual link. The virtual links and the traffic policing unit in the AFDX network guarantee deterministic behavior. The bandwidth for each virtual link is specified by two parameters: BAG and L_{MAX} [7]. The Bandwidth Allocation Gap (BAG) is the time interval between two consecutive frames (packets). The BAG value must be in the range 1ms to 128ms, and this value must be a power of 2 (according to the standards). The L_{MAX} is the largest frame that can be transmitted on the virtual link.

C. Switch

An AFDX switch implements filtering and policing functions to ensure that only valid incoming frames are forwarded to the right physical ports. The switch is responsible for routing frames to output ports based on a static configuration table [16].

III. Related Work

The AFDX protocol is equipped with a variety of fault tolerance techniques to protect the protocol against failures, such as hardware failure, packet failure, deadline miss and babbling-idiot failure.

Hardware failure is one of the common failures in the network. According to Fig. 1, the AFDX network consists of two identical networks, and each ES connects to these networks [7].

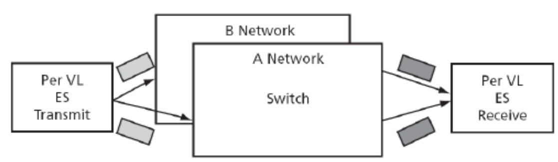

Fig. 1. The redundant networks [7]

A packet failure includes any change in the packet content or the packet size due to any noise [17]. Cyclic Redundancy Check (CRC) technique is a method for detecting a packet failure. In the AFDX protocol, two identical packets sent through its two identical networks [7]. With this strategy, the probability of a simultaneous failure in the both packets is very low.

In real-time networks, the packets are discarded if they are received later than their deadlines, therefore the scheduling of packets is important. Several different scheduling algorithms have been proposed by [10-14].

- First-In-First-Out (FIFO) scheduling policy the packets are transmitted in order their arrival time in the queue [10].
- The shortest frame earliest scheduling algorithm [11], firstly, sends the short packets to reduce their delay time.
- The Static Priority (SP) scheduling algorithm [12] classifies all data flows according to their priorities and sends the packets with highest priority, firstly.
- In the Round Robin (RR) scheduling algorithm [14] all packets are selected respectively.
- In the jitter Earliest-Due-Date (jitter-EDD) scheduling algorithm, the packets are sent before a specific period of their deadline [13].

The babbling-idiot failure means that a system creates multiple copies or sequentially sends a packet. Therefore, the other systems are not allowed to send their packets [8]. In the AFDX protocol, the traffic policing unit in each switch is applied to protect the network from this failure [9]. The traffic policing unit checks the VL bandwidth for each packet that arrives. If the bandwidth is not enough to send the packet, the switch will discard that packet [8]. However, a system may have to send critical packets that need more bandwidth than the determined value for a virtual link. Therefore, these packets should not be discarded. The traffic policing algorithm presented in [8] reduces the number of critical packets that are discarded in this unit. In this algorithm, two queues are used for critical and non-critical packets and the VL bandwidth is not checked to send the critical packets. However, a system may send multiple copies of a critical packet, and this issue may cause the babbling-idiot failure. Therefore, the mentioned traffic policing algorithm needs to be modified to consider the VL bandwidth for critical and non-critical packets and also reduces the number of critical packets which are discarded.

Based on the mentioned studies, there are many techniques for prevention of packet loss. The motivation of this paper is to propose a technique to reduce the number of discarded packets due to the babbling-idiot failure and the deadline miss. In this technique, a scheduler algorithm is proposed that sends the packets with an earliest deadline. In addition, an algorithm for the traffic policing unit in the AFDX switch is presented. In this algorithm, if there is not enough the VL bandwidth, unused bandwidth is checked and it will be employed.

IV. Proposed Technique

To prevent discarding packets in the AFDX network, it is necessary to express some assumptions as follows:

1) Each packet has a specific priority (two levels: 0 and 1) and a deadline (the sum of the arrival time and the network delay) [18, 19].

2) The goal is to reduce the packet loss ratio for critical traffics. The critical packets have the priority equal to "1" and they also have the earliest deadline compared to deadlines of the other packets.

To reduce the number of discarded packets, a two-step technique is proposed, as follows:

Step (1): The scheduling algorithm should check the priority and the deadline of each packet. If the packet is critical, it should be sent, before the other packets. Therefore, the number of discarded critical packets due to deadline miss is reduced. This scheduler has four queues that the packets are inserted into one of the four existing queues, based on their critical degree. For example, the critical packets are placed in queue 0. In Algorithm 1, a pseudo-code is presented for this scheduling algorithm.

Algorithm 1: The proposed scheduling algorithm with the priority and the deadline

Input:
Deadline_ Indicator: Based on this value, one of four queues is selected (initially, this value is set to 0),
Deadline: The deadline for an arrived packet,
Priority: The priority of an arrived packet.

```
If a packet arrives:
If Priority = 1 Then
  If Deadline_ Indicator = 0 or Deadline <= Deadline_ Indicator Then
     The packet is inserted in the subqueue0;
     Deadline_ Indicator = Deadline;
  Else if Deadline > Deadline_ Indicator Then
     The packet is inserted in the subqueue1;
If Priority = 0 Then
  If Deadline_ Indicator = 0 or Deadline <= Deadline_ Indicator Then
     The packet is inserted in the subqueue2;
     Deadline_ Indicator = Deadline;
  Else if Deadline > Deadline_ Indicator Then
     The packet is inserted in the subqueue3;
The queued packets are sent in the order sub-queue with indexes of 0, 1, 2 and 3.
End
```

Step (2): The traffic policing unit in the AFDX switch, checks the VL bandwidth for each arrived packet. If a packet does not adjust to its VL bandwidth, the traffic policing unit will discard it. Therefore, a new traffic policing algorithm should be employed to reduce the number of discard critical packets. In the proposed algorithm, if there is not enough the VL bandwidth for new packets, the remaining bandwidth should be checked. If the remaining bandwidth is enough, packets are accepted by the traffic policing unit. This bandwidth is calculated using Equation 1. In this equation, "Bandwidth" is the bandwidth of a specified physical link, and "BandwidthVL$_i$" is the bandwidth of the virtual link (i) that is defined in this physical link.

$$\text{RemainingBandwidth} = \text{Bandwidth} - \sum_{i=1}^{n} \text{BandwidthVL}_i \quad (1)$$

The remaining bandwidth for a specified physical link can be used by all virtual links that defined in this physical link. However, if the remaining bandwidth does not exist for a physical link, the unused bandwidth of other virtual links, which are defined in that physical link, can be used. In this case, each virtual link is not limited by its bandwidth. For this purpose, the switch should have a table to specify the input port of each VL.

In Algorithm 2 a pseudo-code is presented for the proposed traffic policing algorithm. This pseudo-code is written for a specific physical link.

Algorithm 2: The proposed traffic policing algorithm

Input:
Bandwidth: The bandwidth for a specific virtual link,
Bandwidth_ general: The bandwidth for a specific physical link,
Time: The start time of simulation is placed in this variable, then this variable is updated every one-time unit,
Simulation_ time: The simulation time when a packet arrives,
Packet_ size: The size of a received packet,
Total_ Bandwidth: The total bandwidth of virtual links that are defined in the specific physical link,
Remaining_ Bandwidth: the difference between Bandwidth_ general and Total_ Bandwidth,
Remaining_ Time: The remaining time until one-time unit,
Temp: This binary variable indicates that the bandwidth of a virtual link is used or not used,
Packet_ NUM: The number of packets that can be sent in the remaining time.

```
If a packet arrives:
If Simulation_ time >= Time+1  Then
    Time++;
    Bandwidth is reset;
    Remaining_ Bandwidth is reset;
    The packet is sent;
If Packet_ size <= Bandwidth  Then
    Bandwidth = Bandwidth  -  Packet_ size;
    The packet is sent;
Else if  Packet_ size <=  Remaining_ Bandwidth
        Remaining_ Bandwidth = Remaining_ Bandwidth  -  Packet_ size;
      The packet is sent;
  Else For  all virtual links that are defined in a specific physical link  do
      Remaining- Time = (Time+1) - Simulation_ time;
      Packet_ NUM =  Remaining_ Time / BAG;
     If  Bandwidth – (Packet_ NUM *L_MAX) >= Packet_ size Then
         Bandwidth  = Bandwidth – (Packet_ NUM *L_MAX);
         Temp = 1;
     End for
     If  Temp=1 Then
         Bandwidth = Bandwidth -  Packet_ size;
       The packet is sent;
     Else
         The packet is discarded;
End
```

V. Simulation Results

To evaluate the proposed technique, a primary and the improved Avionics Full-duplex switched Ethernet (AFDX) networks have been simulated with optimized network engineering tools (OPNET). OPNET simulator is one of the most popular tools to simulate the behavior and the performance of any type of networks [20, 21].

The simulated AFDX network consists of nine end systems and five switches. The simulated network setup on OPNET is shown in Fig. 2. As shown in this figure, the main and the redundant networks are marked with green and pink boxes, respectively. TABLE I shows the configuration parameters for all virtual link, such as a resource, destination(s), a path, and the BAG value [22].

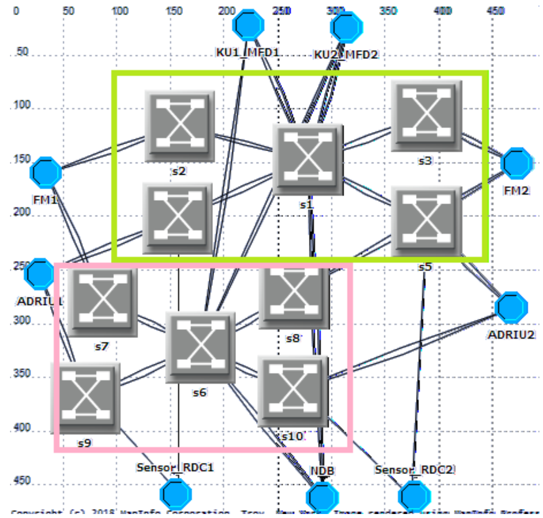

Fig. 2. The network setup on OPNET

TABLE I
The configuration parameters for virtual links [12]

Virtual Links	Source	Destinations	L_{MAX} (bits)	BAG (ms)	Paths
VL1	KU1	FM1, FM2	600	32	S1, S2, S1, S3
VL2	KU2	FM1, FM2	600	32	S1, S2, S1, S3
VL3	FM1	MFD1	5000, 1000	8	S2, S1
VL4	FM1	NDB	1000	16	S2, S1
VL5	FM2	MFD2	5000, 1000	8	S3, S1
VL6	FM2	NDB	1000	16	S3, S1
VL7	NDB	FM1	4000	64	S1, S2
VL8	NDB	FM2	4000	64	S1, S3
VL9	RDC1	ADRIU1	512	32	S4
VL10	RDC2	ADRIU2	512	32	S5
VL11	ADRIU1	FM1, FM2	800	32	S4, S1, S2, S4, S1, S3
VL12	ADRIU2	FM1, FM2	800	32	S5, S1, S3, S5, S1, S2

The primary AFDX network has a FIFO policy in the scheduler unit and a leaky bucket algorithm in the traffic policing unit. The simulation of the AFDX network by applying the proposed scheduling and the traffic policing algorithms is specified as improved AFDX.

The average flight time of an airliner is considered 1 hour and the simulations run for both AFDX networks in two modes:

Mode A: All nodes send the packets as much as their VLs bandwidth.
Mode B: There is a node that uses more VL bandwidth.

Moreover, it should be noted that in the following figures, the simulation results for the primary and the improved AFDX networks are shown with blue and red lines, respectively.

Fig. 3 and Fig. 4 show the number of critical packets that their deadlines are expired in the primary network (the blue line) and in the improved network (the red line). As shown in these figures, the number expired critical packets in the improved network is less than the primary network in the both modes (Mode A and Mode B). This improvement has been achieved because the proposed scheduling algorithm in the improved network sends critical packets, first.

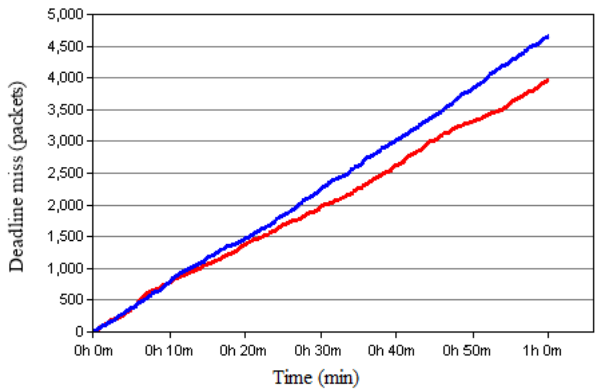

Fig. 3. Comparison of the number of discarded critical packets due to the deadline miss in Mode A

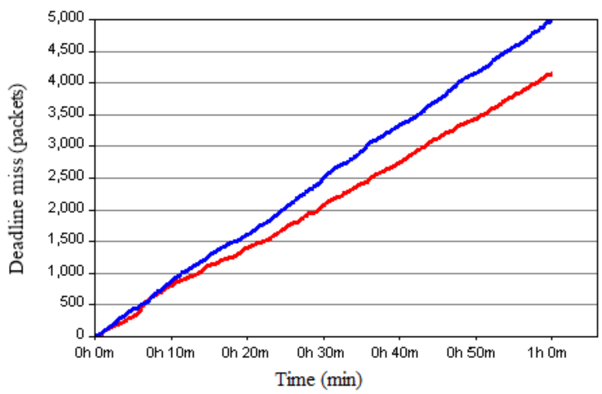

Fig. 4. Comparison of the number of discarded critical packets due to the deadline miss in Mode B

As illustrated in Fig. 5, simulation results show that the number of discarded critical packets in the traffic policing unit for both networks in the Mode A is zero. This result is due that all nodes send the packets as much as their VLs bandwidth and the traffic policing algorithm (in the primary and the improved AFDX networks) will accept these packets.

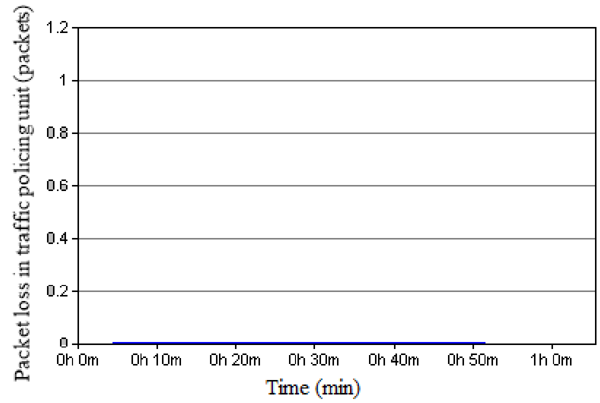

Fig. 5. Comparison of the number of discarded packets in the traffic policing unit in Mode A

However, simulation results in Mode B show that about 170 packets have been discarded in the traffic policing unit by the leaky bucket algorithm in the primary AFDX network. This number has reduced to zero in the improved AFDX network. Moreover, it should be noted that if a node sends packets more than the bandwidth of the physical link, it is possible the number of discarded packets in the proposed traffic policing algorithm may be more than zero.

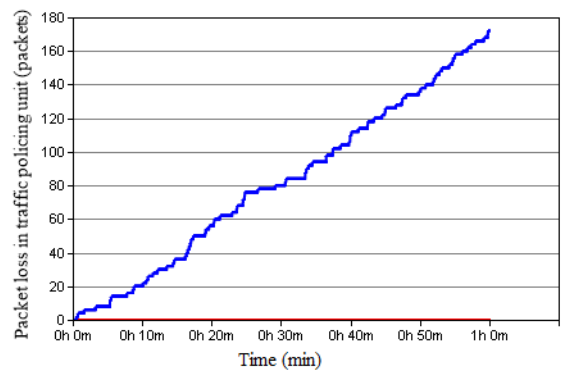

Fig. 6. Comparison of the number of discarded packets in the traffic policing unit in Mode B

TABLE II and TABLE III illustrate the percentage of packet loss reduction and the percentage of deadline miss reduction for the primary and the improved networks in the specified Mode A and Mode B, respectively.

TABLE II
Outputs simulation as a percent for Mode A

Mode A	**The number of routed packets**	**The number of discarded critical packets due to the deadline misses**		**The number of discarded critical packets in the traffic policing unit**		**Improved Deadline Miss (%)**	**Improved Packet Loss (%)**
Network / Time	-	**Primary** AFDX	**Improved AFDX**	**Primary** AFDX	**Improved AFDX**	-	-
20 min	477390	1382	1269	0	0	8.17	0
40 min	959196	2871	2490	0	0	13.27	0
60 min	1441022	4426	3740	0	0	15.49	0

TABLE III
Outputs simulation as a percent for Mode B

Mode B	The number of routed packets	The number of discarded critical due to deadline misses		The number of discarded critical packets in the traffic policing unit		Improved Deadline Miss (%)	Improved Packet Loss (%)
Network / Time	-	Primary AFDX	Improved AFDX	Primary AFDX	Improved AFDX	-	-
20 min	477328	1473	1429	50	0	2.98	100
40 min	959076	3085	2698	105	0	12.54	100
60 min	1440824	4643	3956	170	0	14.79	100

VI. Conclusions

In this paper, to reduce the number of discarded packets and to improve the primary AFDX network, a traffic policing algorithm and a scheduling algorithm were proposed. The proposed traffic policing algorithm can reduce the number of discarded packets in the switch. In this technique, if a critical packet arrives at traffic policing unit and there is not enough virtual link bandwidth for this packet, the algorithm checks the remaining or unused bandwidth of the physical link. If there is required bandwidth, the packet is accepted. Otherwise, the packet will be discarded. Moreover, a scheduling algorithm was proposed to reduce the number of discarded packets due to the deadline miss.

To evaluate the proposed improved AFDX network, a case study was carried out. The number of discarded packets in the traffic policing unit, and the number of discarded packets due to the deadline miss were analyzed for the primary and the improved AFDX networks. The results show that the proposed scheduling algorithm reduced the number of critical packets which are discarded due to the deadline miss about 10%. Furthermore, the number of critical packets which are discarded in the traffic policing unit has been improved up to 100%.

References

[1] R. Li, J. Wang, H. Liao, and N. Huang, "A new method for reliability allocation of avionics connected via an airborne network," Journal of Network and Computer Applications, vol. 48, pp. 14-21, 2015.

[2] P. Bieber, F. Boniol, M. Boyer, E. Noulard, and C. Pagetti, "New Challenges for Future Avionic Architectures," AerospaceLab, 2012.

[3] A. Shahsavar, "Defining a Modular, High Speed and Robust Avionic Architecture for UAVs," 2008.

[4] X. Li, J.-L. Scharbarg, F. Ridouard, and C. Fraboul, "Existing offset assignments are near optimal for an industrial AFDX network," ACM SIGBED Review, vol. 8, pp. 49-54, 2011.

[5] M. Ahmed and S. Dao, "Method and apparatus for increasing fault tolerance for cross-layer communication in networks," ed: Google Patents, 2011.

[6] C. Wang, J. Li, and F. Hu, "Fault tree synthesis for an avionic network," in Transportation, Mechanical, and Electrical Engineering (TMEE), 2011 International Conference on, 2011, pp. 155-159.

[7] N. E.-D. Safwat, M. El-Dakroury, and A. Zekry, "The evolution of aircraft data networks," International Journal of Computer Applications, vol. 94, 2014.

[8] H. Jung, P. Park, D. Shin, K. Lim, and J. Choi, "Fast transmission mechanism of emergency data in AFDX network systems," in Proceedings of the 2nd conference on European computing conference, 2008.

[9] M. Li, M. Lauer, G. Zhu, and Y. Savaria, "Determinism enhancement of AFDX networks via frame insertion and sub-virtual link aggregation," IEEE Transactions on Industrial Informatics, vol. 10, 2014.

[10] L. Jing, "Using Holistic Queue Scheduling to Optimize the Real-Time Performance of AFDX," Open Automation and Control Systems Journal, vol. 6, pp. 1612-1619, 2014.

[11] S. Gurjar and B. Lakshmi, "Optimal scheduling policy for jitter control in AFDX End-System," in Recent Advances and Innovations in Engineering (ICRAIE), 2014, 2014, pp. 1-4.

[12] H. Dong, Y. Lin, Y. Zhang, Z. Zhou, and Z. Zhang, "Using Static Priority Queueing to optimize the Avionics Full Duplex Switched Ethernet," in Natural Computation (ICNC), 2013 Ninth International Conference on, 2013, pp. 1610-1616.

[13] Y. Ren, F. Hu, and J. Li, "End to end jitter control on AFDX network," in Transportation, Mechanical, and Electrical Engineering (TMEE), 2011 International Conference on, 2011, pp. 515-518.

[14] C. Suthaputchakun and Z. Sun, "Impact of End System scheduling policies on AFDX performance in avionic on-board data network," in Advanced Informatics: Concepts, Theory and Applications (ICAICTA), 2015 2nd International Conference on, 2015, pp. 1-6.

[15] L. Xiaosheng, Z. Jian, and H. Tianxiang, "Research on Intelligent Substation Redundant Communication Network Based on AFDX," 2013.

[16] N. Rejeb, A. K. B. Salem, and S. B. Saoud, "AFDX simulation based on TTEthernet model under OMNeT++," in Advanced Systems and Electric Technologies (IC_ASET), 2017 International Conference on, 2017.

[17] Q. Li, O. Oyman, and X. E. Lin, "Retransmission techniques in wireless networks," ed: Google Patents, 2014.

[18] H. Bauer, J.-L. Scharbarg, and C. Fraboul, "Improving the worst-case delay analysis of an AFDX network using an optimized trajectory approach," IEEE Transactions on Industrial informatics, vol. 6, pp. 521-533, 2010.

[19] K. Zhu, Y. Zhuang, and Y. Viniotis, "Achieving end-to-end delay bounds by EDF scheduling without traffic shaping," in INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, 2001, pp. 1493-1501.

[20] J. Lee, R. Life, G. Elmasry, C. Phillips, and N. Dave, "Using opnet with satcom planning," in MILITARY COMMUNICATIONS CONFERENCE, 2010-MILCOM 2010, 2010, pp. 1541-1546.

[21] S. Mittal, "Opnet: An integrated design paradigm for simulations," Software Engineering: An International Journal, vol. 2, pp. 57-67, 2012.

[22] N. E.-D. Safwat, A. Zekry, and M. Abouelatta, "Avionics Full-duplex switched Ethernet (AFDX): Modeling and simulation," in Radio Science Conference (NRSC), 2015 32nd National, 2015, pp. 286-296.