INTERNET 2021

The Thirteenth International Conference on Evolving Internet

ISBN: 978-1-61208-880-8

July 18 – 22, 2021

Nice, France

INTERNET 2021 Editors

Eugen Borcoci, University Politehnica of Bucharest, Romania
Parimala Thulasiraman, University of Manitoba - Winnipeg, Canada

INTERNET 2021

Forward

The Thirteenth International Conference on Evolving Internet (INTERNET 2021) continued a series of events dealing with challenges raised by the evolving Internet making use of the progress in different advanced mechanisms and theoretical foundations. The gap analysis aimed at mechanisms and features concerning the Internet itself, as well as special applications for software defined radio networks, wireless networks, sensor networks, or Internet data streaming and mining.

Originally designed in the spirit of interchange between scientists, Internet reached a status where large-scale technical limitations impose rethinking its fundamentals. This refers to design aspects (flexibility, scalability, etc.), technical aspects (networking, routing, traffic, address limitation, etc), as well as economics (new business models, cost sharing, ownership, etc.). Evolving Internet poses architectural, design, and deployment challenges in terms of performance prediction, monitoring and control, admission control, extendibility, stability, resilience, delay-tolerance, and interworking with the existing infrastructures or with specialized networks.

We take here the opportunity to warmly thank all the members of the INTERNET 2021 technical program committee, as well as all the reviewers. The creation of such a high quality conference program would not have been possible without their involvement. We also kindly thank all the authors who dedicated much of their time and effort to contribute to INTERNET 2021. We truly believe that, thanks to all these efforts, the final conference program consisted of top quality contributions. We also thank the members of the INTERNET 2021 organizing committee for their help in handling the logistics of this event.

INTERNET 2021 Chairs

INTERNET 2021 Steering Committee
Renwei (Richard) Li, Future Networks, Futurewei, USA
Eugen Borcoci, University "Politehnica" of Bucharest (UPB), Romania
Terje Jensen, Telenor, Norway
Przemyslaw (Przemek) Pochec, University of New Brunswick, Canada
Parimala Thulasiraman, University of Manitoba – Winnipeg, Canada
Dirceu Cavendish, Kyushu Institute of Technology, Japan

INTERNET 2021 Industry/Research Advisory Committee
Michael Bahr, Siemens AG Corporate Technology, Munich, Germany
Hanmin Jung, KISTI, Korea
Yung Ryn (Elisha) Choe, Sandia National Laboratories, Livermore, USA
Dirceu Cavendish, Kyushu Institute of Technology, Japan
Steffen Fries, Siemens AG, Germany
Terje Jensen, Telenor, Norway

INTERNET 2021 Publicity Chair
Mar Parra, Universitat Politecnica de Valencia, Spain
Alvaro Liebana, Universitat Politecnica de Valencia, Spain

INTERNET 2021
Committee

INTERNET 2021 Steering Committee
Renwei (Richard) Li, Future Networks, Futurewei, USA
Eugen Borcoci, University "Politehnica" of Bucharest (UPB), Romania
Terje Jensen, Telenor, Norway
Przemyslaw (Przemek) Pochec, University of New Brunswick, Canada
Parimala Thulasiraman, University of Manitoba – Winnipeg, Canada
Dirceu Cavendish, Kyushu Institute of Technology, Japan

INTERNET 2021 Industry/Research Advisory Committee
Michael Bahr, Siemens AG Corporate Technology, Munich, Germany
Hanmin Jung, KISTI, Korea
Yung Ryn (Elisha) Choe, Sandia National Laboratories, Livermore, USA
Dirceu Cavendish, Kyushu Institute of Technology, Japan
Steffen Fries, Siemens AG, Germany
Terje Jensen, Telenor, Norway

INTERNET 2021 Publicity Chair
Mar Parra, Universitat Politecnica de Valencia, Spain
Alvaro Liebana, Universitat Politecnica de Valencia, Spain

INTERNET 2021 Technical Program Committee
Majed Alowaidi, Majmaah University, Saudi Arabia
Mário Antunes, Polytechnic of Leiria & INESC-TEC, Portugal
Andrés Arcia-Moret, Xilinx, Cambridge, UK
Damian Arellanes Molina, UniversityofManchester, UK
Marcin Bajer, ABB Corporate Research Center Krakow, Poland
Michail J. Beliatis, Research Centre for Digital Business Development | Aarhus University, Denmark
Driss Benhaddou, University of Houston, USA
Nik Bessis, Edge Hill University, UK
Maumita Bhattacharya, Charles Sturt University, Australia
Filippo Bianchini, Studio Legale Bianchini, Perugia, Italy
Eugen Borcoci, University "Politehnica" of Bucharest (UPB), Romania
Fernando Boronat Seguí, Universidad Politécnica De Valencia-Campus De Gandia, Spain
Christos Bouras, University of Patras, Greece
Matthew Butler, Bournemouth University, UK
Alina Buzachis, University of Messina, Italy
Lianjie Cao, Hewlett Packard Labs, USA
Dirceu Cavendish, Kyushu Institute of Technology, Japan
Franco Cicirelli, ICAR-CNR, Italy
Hao Che, University of Texas at Arlington, USA
Albert M. K. Cheng, University of Houston, USA
Hongmei Chi, Florida A&M University, USA
Andrzej Chydzinski, Silesian University of Technology, Poland

Victor Cionca, Munster Technical University, Ireland
Monireh Dabaghchian, Morgan State University, USA
Noel De Palma, University Grenoble Alpes, France
Angel P. del Pobil, Jaume I University, Spain
Flavia Delicato, Fluminense Federal University, Brazil
Jun Duan, IBM T. J. Watson Research Center, USA
Said El Kafhali, Hassan 1st University, Settat, Morocco
Khalid Elbaamrani, Cadi Ayyad University, Marrakech, Morocco
Carlos Enrique Palau Salvador, Universidad Politécnica de Valencia, Spain
Zongming Fei, University of Kentucky, USA
Steffen Fries, Siemens AG, Germany
Song Fu, University of North Texas, USA
Marco Furini, University of Modena and Reggio Emilia, Italy
Dimitrios Georgakopoulos, Swinburne University of Technology, Australia
Victor Govindaswamy, Concordia University Chicago, USA
Shuyang Gu, Texas A & M University-Central Texas, USA
Wladyslaw Homenda, Warsaw University of Technology, Poland
Fu-Hau Hsu, National Central University, Taiwan
Pengfei Hu, VMWare Inc, USA
Takeshi Ikenaga, Kyushu Institute of Technology, Japan
Oliver L. Iliev, FON University, Republic of Macedonia
Khondkar R. Islam, George Mason University, USA
Terje Jensen, Telenor, Norway
Sokratis K. Katsikas, Norwegian University of Science and Technology, Norway
Brian Kelley, University of Texas at San Antonio / 5G Program Management Office - JBSA 5G NextGen, USA
Ahmed Khaled, Northeastern Illinois University, USA
Aminollah Khormali, University of Central Florida, USA
Rasool Kiani, University of Isfahan, Iran
Lucianna Kiffer, Northeastern University, USA
Kishori Mohan Konwar, MIT / Broad Institute of MIT and Harvard, USA
Hovannes Kulhandjian, California State University, Fresno, USA
Ayush Kumar, Singapore University of Technology and Design, Singapore
Mikel Larrea, University of the Basque Country UPV/EHU, Spain
Kevin Lee, Deakin University, Australia
Kin K. Leung, Imperial College London, UK
Renwei (Richard) Li, Future Networks, Futurewei, USA
Xin Li, Google, USA
Zhijing Li, Facebook, USA
Jinwei Liu, Florida A&M University, USA
Qiang Liu, Nokia Bell Labs, USA
Xiaoqing "Frank" Liu, University of Arkansas, USA
Pranay Lohia, IBM Research, India
Luís Miguel Lopes de Oliveira, Institute Polytechnic of Tomar, Portugal
Olaf Maennel, Tallinn University of Technology, Estonia
Imad Mahgoub, Florida Atlantic University, USA
Zoubir Mammeri, IRIT - Paul Sabatier University, France
Philippe Merle, Inria Lille - Nord Europe, France

Copyright Information

For your reference, this is the text governing the copyright release for material published by IARIA.

The copyright release is a transfer of publication rights, which allows IARIA and its partners to drive the dissemination of the published material. This allows IARIA to give articles increased visibility via distribution, inclusion in libraries, and arrangements for submission to indexes.

I, the undersigned, declare that the article is original, and that I represent the authors of this article in the copyright release matters. If this work has been done as work-for-hire, I have obtained all necessary clearances to execute a copyright release. I hereby irrevocably transfer exclusive copyright for this material to IARIA. I give IARIA permission or reproduce the work in any media format such as, but not limited to, print, digital, or electronic. I give IARIA permission to distribute the materials without restriction to any institutions or individuals. I give IARIA permission to submit the work for inclusion in article repositories as IARIA sees fit.

I, the undersigned, declare that to the best of my knowledge, the article is does not contain libelous or otherwise unlawful contents or invading the right of privacy or infringing on a proprietary right.

Following the copyright release, any circulated version of the article must bear the copyright notice and any header and footer information that IARIA applies to the published article.

IARIA grants royalty-free permission to the authors to disseminate the work, under the above provisions, for any academic, commercial, or industrial use. IARIA grants royalty-free permission to any individuals or institutions to make the article available electronically, online, or in print.

IARIA acknowledges that rights to any algorithm, process, procedure, apparatus, or articles of manufacture remain with the authors and their employers.

I, the undersigned, understand that IARIA will not be liable, in contract, tort (including, without limitation, negligence), pre-contract or other representations (other than fraudulent misrepresentations) or otherwise in connection with the publication of my work.

Exception to the above is made for work-for-hire performed while employed by the government. In that case, copyright to the material remains with the said government. The rightful owners (authors and government entity) grant unlimited and unrestricted permission to IARIA, IARIA's contractors, and IARIA's partners to further distribute the work.

Table of Contents

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.

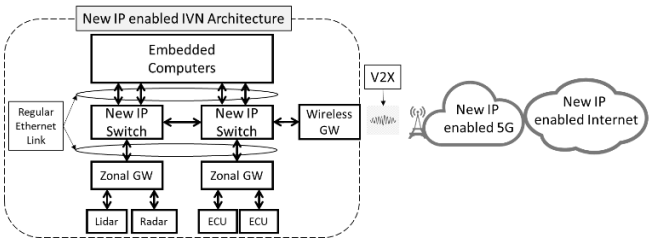


Figure 1. New IP enabled IVN architecture in future Internet

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.

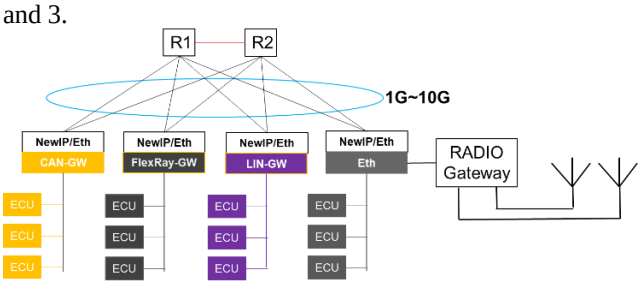


Figure 2. The Spine-Leaf IVN topology

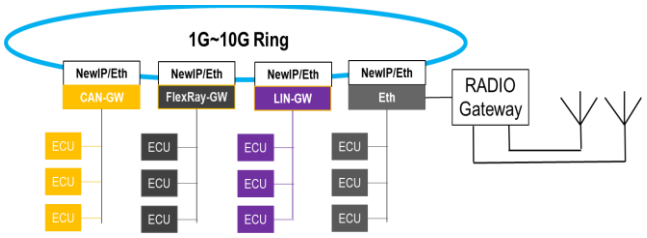


Figure 3. The Ring IVN Topology

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.

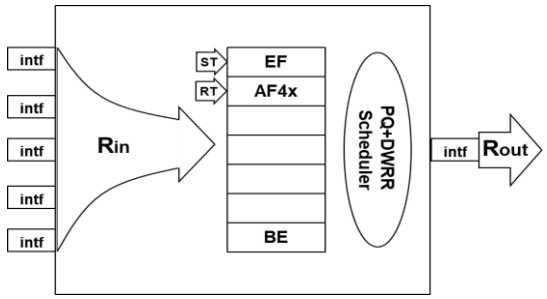


Figure 4. 1st Algorithm: Asynchrous Solution

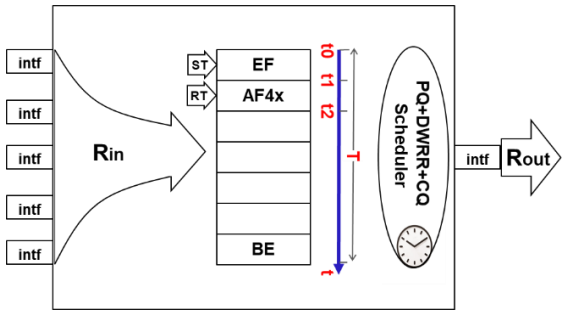


Figure 5. 2nd Algorithm: Synchrous Solution

- 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.

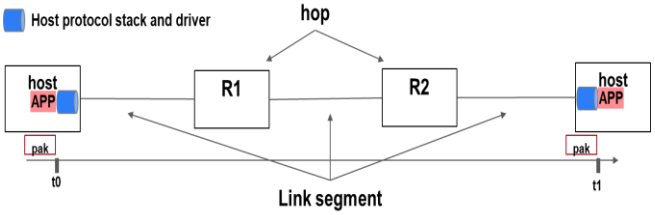


Figure 6. The End-to-End Latency for IP Applications

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).

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

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

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

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

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

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

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.

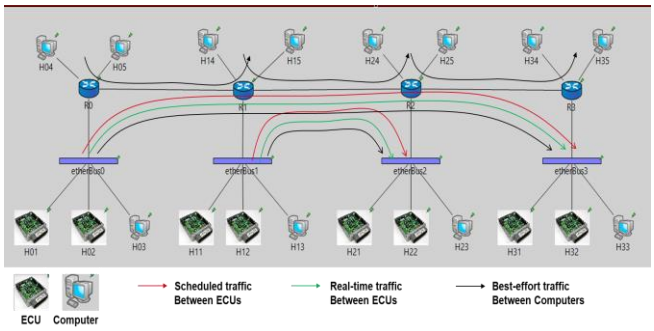


Figure 7. Network Topology and traffic

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.

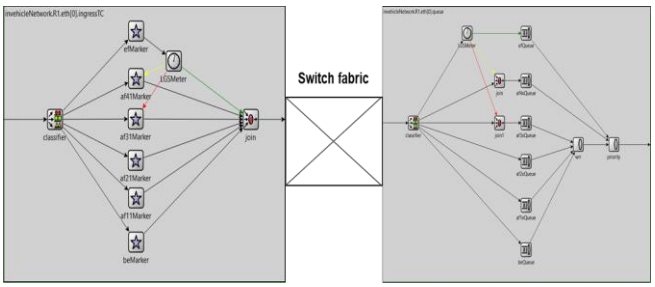


Figure 8. Router structure

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.

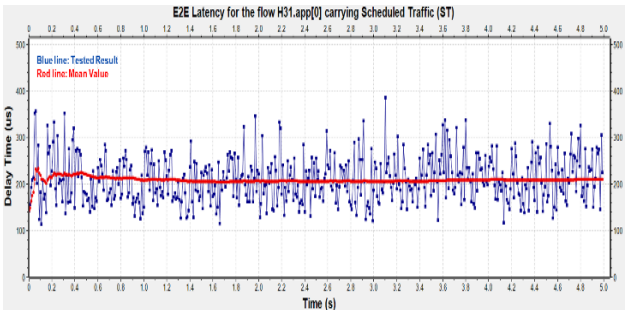


Figure 10. 1st Algo: The E2E Latency (min=108us, max=391us) for the worst performed ST flow

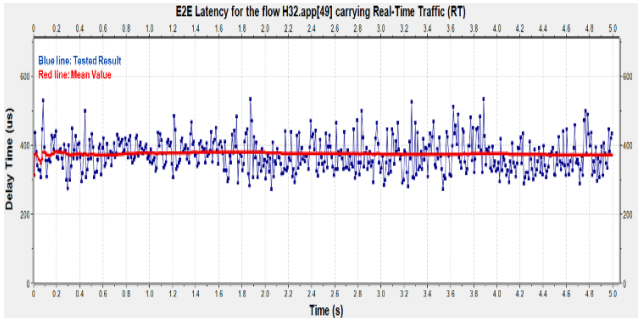


Figure 11. 1st Algo: The E2E Latency (min=278us, max=542us) for the worst performed RT flow

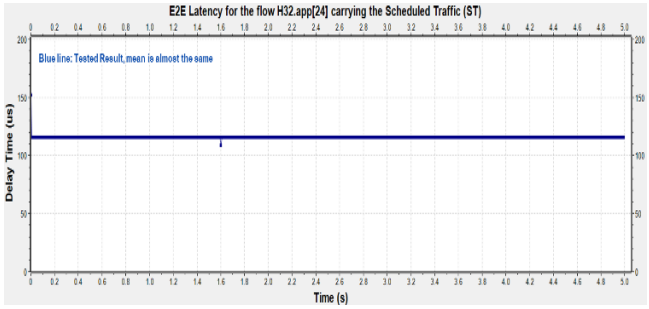


Figure 12. 2nd Algo: The E2E Latency (min=109us, max=152us) for the worst performed ST flow

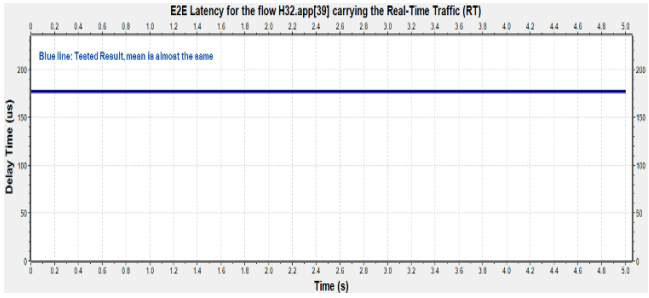


Figure 13. 2nd Algo: The E2E Latency (min=169us, max=169us) for the worst performed RT flow

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.

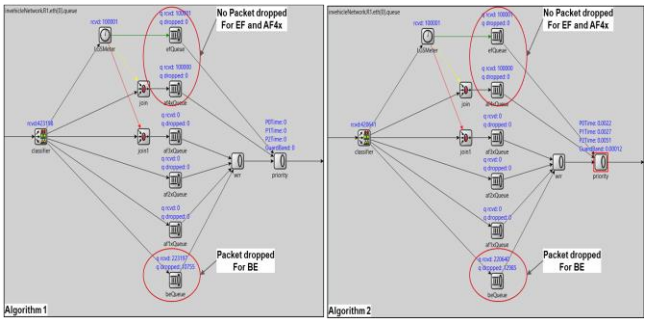


Figure 14. The statistics for all Queues for two algorithms

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"

 ISBN: 978-1-61208-880-8

Path Schedulers Performance on Cellular/Wi-Fi Multipath Video Streaming

Masayoshi Kondo*, Dirceu Cavendish**, Daiki Nobayashi**, Takeshi Ikenaga**
*Graduate School of Engineering, **Faculty of Engineering
Kyushu Institute of Technology
Fukuoka, Japan
e-mail: kondo.masayoshi146@mail.kyutech.jp {cavendish@ndrc, nova@ecs, ike@ecs}.kyutech.ac.jp

***Abstract*—Internet traffic nowadays is predominantly composed by video streaming. Moreover, most video streaming traffic is carried over Hypertext Transfer Protocol/Transmission Control Protocol (HTTP/TCP). Understanding TCP stack performance in transporting video streams has become paramount, specially in face of recent multipath transport protocol evolutions and multiple client device interfaces available. In this paper, we characterize path schedulers performance of streaming of video sessions over cellular and Wi-Fi access networks, the two most common and dominant wireless technologies in the market. We use network performance level as well as video quality level metrics to characterize multiple path schedulers and resulting network and application layers' interactions.**

Keywords*—*Video streaming; TCP congestion control; TCP socket state; Multipath TCP; Packet retransmissions; Packet loss.

I. INTRODUCTION

Internet data transmission relies heavily on transport protocols to pace data delivery to avoid network congestion and uncontrolled data losses. Transmission Control Protocol (TCP) has arguably become the most successful transport protocol of the Internet, supporting reliable data delivery for most diverse applications nowadays. In particular, streaming applications, the most dominant type of application in sheer volume, data transport quality is related with the amount of data discarded at the client due to excessive transport delay/jitter, as well as data rendering stalls due to lack of timely playout data. Transport delays and data starvation performance measurers depend heavily on how TCP handles flow and congestion control, as well as packet retransmissions.

More recently, the evolution of portable device hardware, in particular support of multiple high bandwidth interfaces, has prompted the development of multipath transport protocols, allowing, for instance, video streaming over multiple IP interfaces and diverse network paths. Multipath video streaming is advantageous because it not only increases aggregated device downloading bandwidth capacity, but also improves transport session reliability during transient radio link impairments. An important issue in multipath transport is selecting a path among various active networking paths (called sub-flows), which can be done on a packet by packet basis. A path packet scheduler is used for this purpose, and should be designed to prevent head-of-line blocking across various networking paths, potentially with diverse loss and delay characteristics. Head-of-line blocking occurs when data already delivered at the receiver is waiting for additional packets that are blocked at another sub-flow, potentially causing incomplete or late frames to be discarded at the receiver, as well as stream stalling. Interplay between path schedulers and TCP variants will untimately define streaming quality, hence we propose to analyze video performance vis-a-vis popular TCP variants and path schedulers.

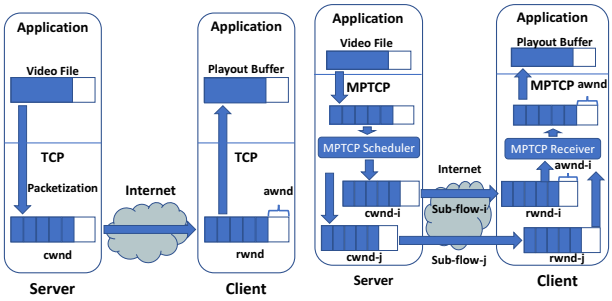
The paper is organized as follows. Related work is included in Section II. Section III describes video streaming transport over Transmission Control Protocol. Section IV describes recently proposed alternative path schedulers. Section V characterizes video streaming performance over Wi-Fi and cellular paths via network emulation, addressing performance evaluation of a default path scheduler, as well as alternative schedulers, working with popular TCP variants. Section VI summarizes our studies and addresses directions we are pursuing as follow up to this work.

II. RELATED WORK

Since the advancements of multipath transport protocols, several multipath transport studies have appeared in the literature, mostly focusing on throughput performance of data transfers over mobile networks (see [18] aggregate throughput studies and related work). Only recently, however, path scheduler research has been recognized as an important piece of multipath transport sessions performance. For instance, [13] has analyzed loss based congestion control TCP variants interactions with minimum Round Trip Time (RTT) default Multipath TCP (MPTCP) path scheduler, and showed how sender/receiver buffers dimentioning impacts throughput performance via inflation of sub-flow RTTs. Little research work, however, has focused on video performance over multiple paths. Recent multipath video streaming on ad-hoc network studies have appeared, motivated by vehicular communication in assisted driving systems. [2], for instance, introduces an interference aware multipath video streaming scheme in Vehicular Ad-hoc Networks (VANETs). Vehicle to vehicle throughput performance of video streams over multiple paths is evaluated, taking into account interference within neighbors, as well as shadowing effects onto Signal to Noise ratio, and data delay. Their goal is reliable transport of high quality video streams, minimizing video freezes and dropped frames, via link layer channel interference control, coupled with efficient routing strategies on ad-hoc vehicular networks. In contrast, we focus on video streaming over regular Internet paths,

 ISBN: 978-1-61208-880-8

where link layer channel and route optimization opportunities are limited. [1] focuses at integrating application layer with transport protocol, by introducing a path-and-content-aware path selection approach which couples MPEG Media Transport (MMT) with multipath transport. They estimate path quality conditions of each subflow, and avoid sending I-frames on paths of low transport quality. A similar approach, where different sub-flows are utilized for segregating high priority packets of Augmented Reality/Virtual Reality streams has been introduced by Silva et al. [23]. In contrast, our previous and current work do not couple applications with multipath transport, rather focusing on generic path schedulers and TCP variants to deliver high quality video streaming. Recently, Ferlin et al. [7] have introduced a path scheduler based on a path head-of-line blocking predictor. They carry out emulation experiments of their proposed scheduler against minimum RTT default scheduler, in transporting bulk data traffic, Web transactions and Constant Bit Rate (CBR) applications. Hence, they use goodput, data transport completion time and packet delays as performance evaluation metrics. Kimura et al. [12] have shown throughput performance improvements using schedulers driven by path sending rate and TCP window space, on bulk data transfers. Xue et al. [26] has introduced a path scheduler based on estimation of the amount of data each path is able to transmit. They evaluated the scheduler's throughput performance on simulated network scenarios. Also, Frommgen et al. [9], consistent with [13] work, have shown that stale RTT information causes problems with path selection of small streams, such as HTTP traffic. Similar to [13] tail burst probing, the authors propose an RTT probing to improve transport latency and throughput performance of thin streams. In contrast, the schedulers evaluated in our work do not rely on path probing mechanisms, but on sender based passive path evaluation metrics to steer video traffic appropriately. Along the same lines, Dong et al. [6] have introduced a path loss estimation scheme to select paths that may be subjected to high and bulk loss rates. Although they have presented video streaming experiments, they do not measure application level stream performance, as we do. By contrast, in our previous works, we have introduced multipath path scheduling generic principles, which can be applied in the design of various path schedulers to specifically improve video stream quality. Using these principles, we have introduced in [14] Multipath TCP path schedulers based on dynamically varying path characteristics, such as congestion window space and estimated path throughput. In addition, in [15], we have also proposed to enhance path schedulers with TCP state information, such as whether a path is in fast retransmit and fast recovery states. Finally, in [16], we have introduced a novel concept of sticky scheduling, where once a path switch is executed, the scheduler stays with the new path until the path bandwidth resources become exhausted. In this work, for the first time we propose to evaluate a multitude of path schedulers, some of our proposal, over realistic Wi-Fi/Cellular multipath scenarios, focusing on video quality at application layer. Our evaluation include widely deployed TCP variants, exposing best TCP/path scheduler combinations.



(a) TCP (b) MPTCP

Figure 1: Video Streaming over TCP/MPTCP

III. Video Streaming Over TCP

Video streaming over HTTP/TCP typically sources video content from an HTTP server, where video files can be streamed from upon HTTP requests over the Internet to video clients. At the transport layer, a TCP variant provides reliable transport of video data over IP packets between the server and client end points. Figure 1(a) illustrates these video streaming components. As mentioned, HTTP server stores encoded video files. Triggered by a HTTP video request, a TCP sender is instantiated to transmit packetized data to the client machine, connected to the application by a TCP socket. At this TCP transport layer, a congestion window is used at the sender to control the amount of data injected into the network. The size of the congestion window ($cwnd$) is adjusted dynamically, according to the level of congestion experienced through the network path, as well as the space available for data storage ($awnd$) at the TCP client receiver buffer. Congestion window space at the sender is freed only when data packets acknowledged by the receiver arrive. Lost unacknowledged packets are retransmitted by the TCP layer to ensure reliable data delivery. At the client, in addition to acknowledging arriving packets, the TCP receiver informs the TCP sender about its current available space ($awnd$), so that $cwnd \leq awnd$ condition is enforced by the sender at all times. At the client application layer, a video player extracts data from a playout buffer, which drains packets delivered by the TCP receiver from its socket buffer. The playout buffer hence serves to smooth out variable data network throughput.

A. Video Application and TCP Transport Interaction

As mentioned earlier, at the server side, the HTTP server transfers data into the TCP sender socket according to TCP $cwnd$ space availability. Hence, the injection rate of video data into the TCP socket is constrained by the congestion condition of the network path used, and thus does not follow the video variable encoding rate. On its turn, TCP throughput performance is affected by the RTT of the TCP session over a specific path, since only up to a $cwnd$ worth of data can be delivered without acknowledgements. Hence, for a given $cwnd$ size, from the moment a first packet is sent until the first acknowledgement arrives back, the TCP session throughput is capped at $cwnd/RTT$. As there are various TCP

congestion avoidance schemes regulating $cwnd$, according to the TCP variant, the size of the congestion window size is computed by a specific algorithm at the time of packet acknowledgement reception by the TCP source. Regardless of the variant, however, the size of the congestion window computed is capped by the available TCP receiver space $awnd$ communicated back from the TCP client, in order to ensure no receiver buffer overflow. At the client side, video data is retrieved from the TCP client socket by the video player into a playout buffer, from which data is delivered to the video renderer. Even though client playout buffer may underflow, if TCP receiver window empties out, the playout buffer never overflows, since the player will not pull more data into the playout buffer if space is not available during video rendering.

B. Multipath TCP

Multipath TCP is an Internet Engineering Task Force (IETF) transport layer protocol that supports data transport over multiple concurrent TCP sessions [8]. The multipath nature of the transport session is hidden from application layer by a single TCP socket exposed per application session. At the transport layer, however, MPTCP works with concurrent TCP variant sub-flows, each of which in itself unaware of the multipath nature of the application session. A path scheduler connects the application facing socket with transport sub-flows, extracting packets from the MPTCP socket exposed to the application, selecting a sub-flow, and injecting packets into a selected sub-flow TCP socket. MPTCP transport architecture is illustrated in Figure 1(b).

The most commonly used path scheduler, called default scheduler, selects the path with shortest RTT among paths with currently available congestion window space for new packets. Path schedulers may operate in two different modes: uncoupled, and coupled. In uncoupled mode, each sub-flow congestion window $cwnd$ is adjusted independent of the other sub-flow. In coupled mode, MPTCP couples the congestion control of the sub-flows, by adjusting the congestion window $cwnd_k$ of a sub-flow k according with current state and parameters of all sub-flows. Although several coupling mechanisms exist, we focus on Linked Increase Algorithm (LIA) [20], Opportunistic Linked Increase Algorithm (OLIA) [11], and Balanced Linked Adaptation algorithm (BALIA) [25]. We include also evaluation of various alternative uncoupled schedulers recently proposed.

IETF MPTCP protocol supports the advertisement of IP interfaces available between two endpoints via specific TCP option signalling. As IP option signalling may be blocked by intermediate IP boxes, such as firewalls, paths that cross service providers may require VPN protection so as to preserve IP interface advertizing between endpoints. Morever, both endpoints require MPTCP to be running for the establishment and usage of multiple transport paths. Notice that IP interfaces may be of diverse nature (e.g., Wi-Fi, cellular).

C. TCP variants

TCP protocol variants can be classified into delay and loss based congestion control schemes. Loss based TCP variants use packet loss as primary congestion indication signal, typically performing window regulation as $cwnd_k = f(cwnd_{k-1})$, hence being ack reception paced. Most f functions follow an Additive Increase Multiplicative Decrease (AIMD) window adjustment scheme, with various increase and decrease parameters. TCP NewReno [3] and Cubic [21] are examples of AIMD strategies. On the other hand, delay based TCP variants use queue delay information as the congestion indication signal, increasing/decreasing the window if the delay is small/large, respectively. Compound [22] and Capacity and Congestion Probing (CCP) [5] are examples of delay based congestion control variants. Most TCP variants follow a phase framework, with an initial slow start, congestion avoidance, fast retransmit, and fast recovery phases, regardless of the window adjustment congestion control used during congestion avoidance.

IV. MPTCP Path Schedulers

MPTCP scheduler selects a sub-flow to inject packets into the network on a packet by packet basis. As mentioned earlier, the default strategy is to select the path with shortest average packet delay, hereafter called LRF. Other path schedulers evaluated in this paper are as follows:

- **Low RTT First (LRF):** In low RTT first, the scheduler first rules out any path for which there is no space in its sub-flow congestion window ($cwnd$). Among the surviving paths, the scheduler then selects the path with small smooth RTT ($sRTT$). Smooth RTT is computed as an average RTT of recently transmitted packets on that sub-flow. Since on most TCP stacks each sub-flow already keeps track of its smooth RTT, this quantity is readily available.
- **Largest Packet Credits (LPC):** In largest packet credits scheduler, among the sub-flows with space in their congestion window $cwnd$, this scheduler selects the one with largest available space. Here available space consists of the number of packets allowed by current $cwnd$ size subtracted from the number of packets that have not been acknowledged yet.
- **Largest Estimated Throughput (LET):** In largest estimated throughput scheduler, among the sub-flows with large enough $cwnd$ to accommodate new packets, the scheduler estimates the throughput of each sub-flow, as $cwnd/sRTT$, selecting the one with largest throughput.
- **Greedy Sticky (GR-STY):** As it is the case of default scheduler (LRF), on the onset of a video streaming session, greedy sticky scheduler selects the path with smallest RTT. However, once a new path is selected, the scheduler stays on a new path for as long as there is available congestion window space, until the new path experiences congestion.
- **Throughput Sticky (TP-STY):** Similar to default scheduler (LRF), throughput sticky scheduler selects the path of lowest RTT. However, a new path is selected only if the throughput of the new path is larger than the throughput of the currently selected path.

 ISBN: 978-1-61208-880-8

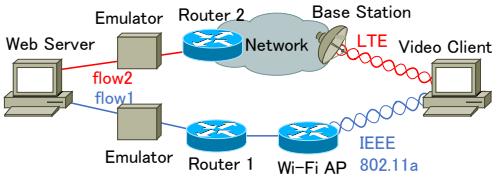


Figure 2: Video Streaming Emulation Network

TABLE I: EXPERIMENTAL NETWORK SETTINGS

Element	Value
Video size	409 MBytes
Video rate	5.24 Mb/s
Playout time	10 mins 24 secs
Video Codec	H.264 MPEG-4 AVC
MPTCP variants	Cubic, Compound, LIA, OLIA, BALIA
MPTCP schedulers	LRF, LET, LPC, GR-STY, TP-STY, TR-STY

TABLE II: EXPERIMENTAL NETWORK SCENARIOS

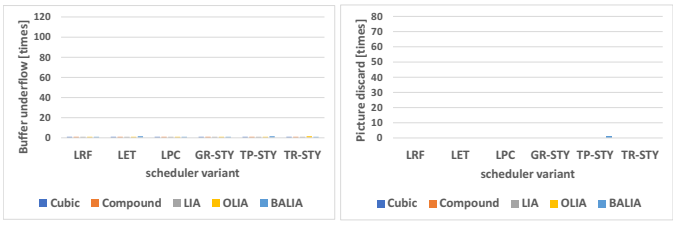
Scenario	Emulator	Path properties (RTT)
A- Baseline (LTE/Wi-Fi) no loss	LTE) Delay 0 ms Wi-Fi) Delay 20 ms	RTT 80 ms RTT 40 ms
B- TwoPath (LTE/Wi-Fi) no loss	LTE) Delay 0 ms Wi-Fi) Delay 30 ms	RTT 80 ms RTT 60 ms
C- TwoPath (LTE/Wi-Fi) Wi-Fi 6% loss	LTE) Delay 0 ms Wi-Fi) Delay 30 ms, Loss 6%	RTT 80 ms RTT 60 ms
D- TwoPath (LTE/Wi-Fi) no loss	LTE) Delay 0 ms Wi-Fi) Delay 40 ms	RTT 80 ms RTT 80 ms
E- TwoPath (LTE/Wi-Fi) Wi-Fi 6% loss	LTE) Delay 0 ms Wi-Fi) Delay 40 ms, Loss 6%	RTT 80 ms RTT 80 ms

- **Throughput RTT Sticky (TR-STY):** As with default scheduler (LRF), the path of lowest RTT is first chosen. However, in addition to requiring a larger throughput of a new candidate path as per TP-STY, in throughput RTT sticky scheduler, path switch requires also that a new path has smaller RTT than the current one.

LPC focuses on scenarios in which addresses a large RTT path has plenty of bandwidth, as compared to a shorter RTT path. LRF default scheduler may avoid this path due to its large RTT, regardless of having plenty of bandwidth for the video stream to flow unimpeded. LET addresses another scenario, in which a short path has plenty of bandwidth. Although the default scheduler may select this path due to its short RTT, if the short RTT has a smaller cwnd, LET will divert traffic away from this path prior to path congestion, whereas default scheduler will continue to inject traffic through it. Finally, the last three sticky schedulers attempt to reduce the number of path switches during transport session, in an attempt to reduce head of line blocking probability during the streaming session.

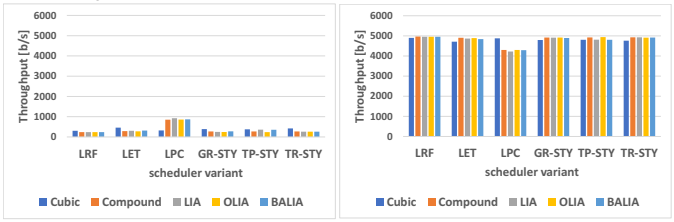
V. Path Schedulers over Wi-Fi & Cellular Paths

Figure 2 describes the network testbed used for emulating network paths with Wi-Fi and Cellular (LTE) wireless access links. An HTTP Apache video server is connected to two L3 switches, one of which directly connected to an 802.11a router, and the other connected to an LTE base station via a cellular network card via emulator boxes. In this paper, the emulator boxes are used to vary each path RTT, as well as inject controlled packet losses. The simple topology and isolated traffic allow us to better understand the impact of differential



(a) Buffer Underflow (b) Picture Discard

Figure 3: A- Baseline Scenario - Video Performance



(a) Throughput Cellular (b) Throughput Wi-Fi

Figure 4: A- Baseline Scenario - Throughput Performance

delays, packet loss, TCP variants, and path schedulers on streaming performance.

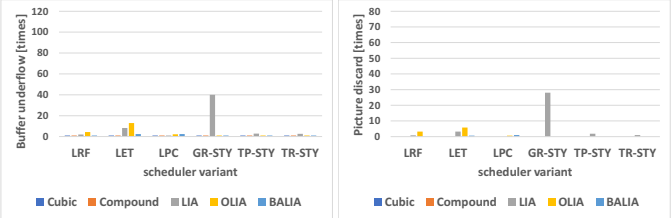
Network settings and scenarios under study are described in Tables I and II, respectively. Video settings are typical of a video stream, with video playout rate of 5.24 Mb/s, and size short enough to run multiple streaming trials within a short amount of time. Emulator boxes are tuned to generate various multiple path network conditions, and have been selected as per Table II to represent commonplace LTE/WiFi streaming situations at home. TCP variants used are: Cubic, Compound, LIA, OLIA and BALIA. Performance measures are:

- **Picture discards:** number of frames discarded by the video decoder.
- **Buffer underflow:** number of buffer underflow events at video client buffer.
- **Sub-flow throughput:** the value of TCP throughput on each sub-flow.

We organize our video streaming experimental results in network scenarios summarized in Table II): A- A Wi-Fi-Cellular (LTE) baseline scenario, where Wi-Fi path of good quality (RTT/loss) is predominantly used; B- A Wi-Fi-Cellular scenario, where a slightly larger Wi-Fi path delay causes cellular path to be used; C- A Wi-Fi-Cellular scenario, where a Wi-Fi link with medium delay suffers a 6 % packet loss degradation, representing user situation at which device is at the end of Wi-Fi range; D- A Wi-Fi-Cellular scenario, with a Wi-Fi path delay large enough to have cellular path predominantly being used; E- A Wi-Fi-Cellular scenario, where a Wi-Fi link with large delay also suffers a 6 % packet loss degradation.

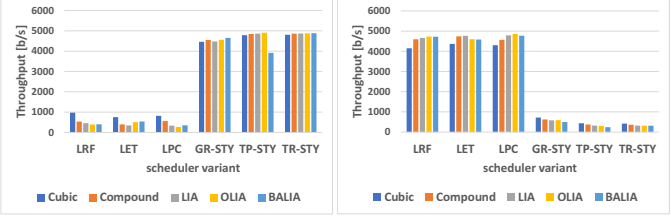
A. Baseline Scenario

Figures 3(a) and (b) report on video streaming buffer underflow and picture discard performance. Video performance is excellent for all TCP variants and path schedulers. Figures 4(a) and (b) report of Cellular and Wi-Fi throughput. We can see that Wi-Fi path is most used for all TCP variants and path schedulers.



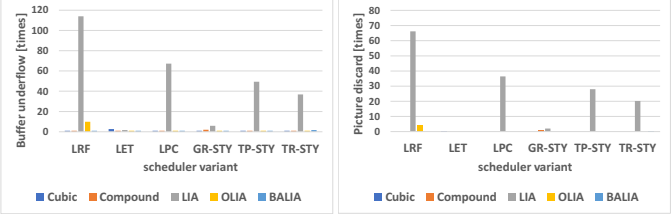
(a) Buffer Underflow (b) Picture Discard

Figure 5: B- Medium Delay Wi-Fi - Video Performance



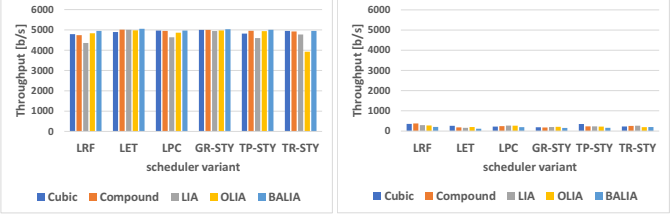
(a) Throughput Cellular (b) Throughput Wi-Fi

Figure 6: B- Medium Delay Wi-Fi - Throughput Performance



(a) Buffer Underflow (b) Picture Discard

Figure 7: C- Medium Delay&loss Wi-Fi - Video Performance



(a) Throughput Cellular (b) Throughput Wi-Fi

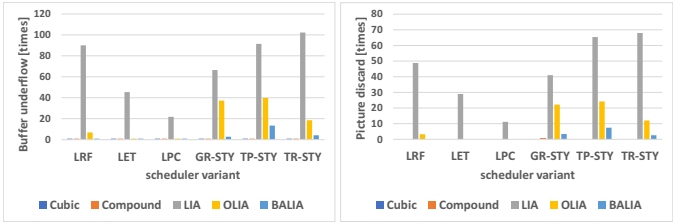
Figure 8: C- Medium Delay&loss Wi-Fi - Throughput Performance

B. Two path Medium Delay Wi-Fi Scenario

Figures 5(a) and (b) report on video streaming performance of Wi-Fi - Cellular network scenario with a medium Wi-Fi path delay. Even though most TCP variants and path schedulers perform well, LIA TCP variant under GR-STY scheduler results in video degradation, albeit not serious. Throughput performance in Figures 6 shows an that path schedulers drive the usage of one path versus the other, independent of the TCP variant. In particular, LRF (default), LET, LPC utilize Wi-Fi path mostly, whereas all sticky schedulers (GR-STY, TP-STY, TR-STY) use mostly the cellular path. This shows how sensitive path selection is to delay differentials.

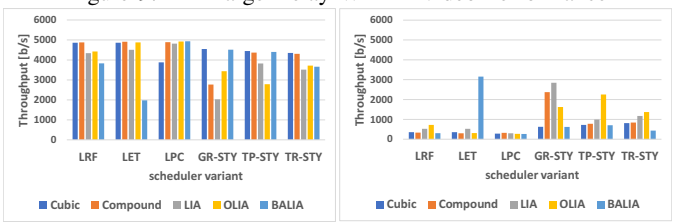
C. Two path Medium Delay&Loss Wi-Fi Scenario

Figures 7(a) and (b) report on video streaming performance of Wi-Fi - Cellular network scenario with a medium Wi-Fi path delay and 6 % packet loss. We notice a wide variety of performances vis a vis path scheduler/TCP variant combinations, which is expected because of loss impact on TCP



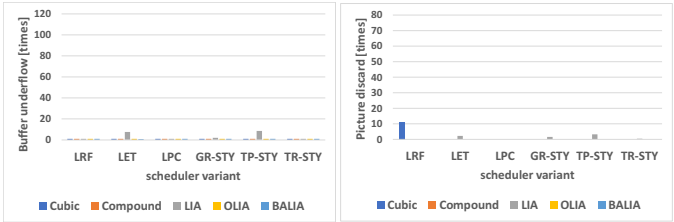
(a) Buffer Underflow (b) Picture Discard

Figure 9: D- Large Delay Wi-Fi - Video Performance



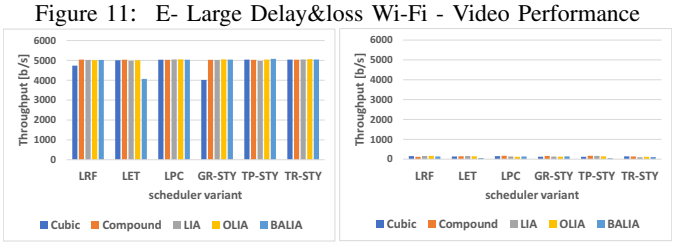
(a) Throughput Cellular (b) Throughput Wi-Fi

Figure 10: D- Large Delay Wi-Fi - Throughput Performance



(a) Buffer Underflow (b) Picture Discard

Figure 11: E- Large Delay&loss Wi-Fi - Video Performance



(a) Throughput Cellular (b) Throughput Wi-Fi

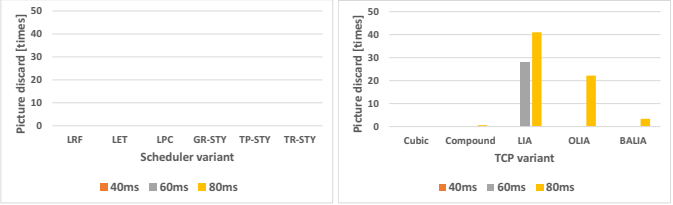
Figure 12: E- Large Delay&loss Wi-Fi - Throughput Performance

variants' performance and delay differential impact on path schedulers. We can identify, however, some trends. Firstly, GR-STY path scheduler delivers high video quality across all TCP variants. Noticeable also is Cubic consistent performance across all path schedulers. Finally, if taken together as a class, coupled TCP variants seem to incur video degradation across all schedulers.

Throughput performance in Figures 8 shows that a Wi-Fi packet delivery degradation pushes path utilization to mostly cellular path, regardless of the TCP variant. Good path schedulers design are expected to select high quality paths in both delay and loss path attributes.

D. Two path Large Delay Wi-Fi Scenario

Figures 9(a) and (b) report on video streaming performance of Wi-Fi - Cellular network scenario with a large Wi-Fi path delay. Even though most TCP variants and path schedulers perform well, LIA and OLIA TCP variants under all sticky



(a) TCP Cubic - Picture Discard (b) GR-STY - Picture Discard

Figure 13: TCP & Scheduler-Picture Discard Video Performance

schedulers results in video degradation. Throughput performance in Figures 10 shows that cellular link is mostly used, although some video traffic still goes through Wi-Fi path. We can see that sticky schedulers are responsible for streaming over the Wi-Fi path, despite its large RTT delay.

E. Two path Large Delay&Loss Wi-Fi Scenario

Figures 11(a) and (b) report on video streaming performance of Wi-Fi - Cellular network scenario with a large Wi-Fi path delay and 6 % packet loss. We again notice a wide variety of performances vis a vis path scheduler/TCP variant combinations. Firstly, all scheduler deliver similar video performance across all TCP variants. We believe this is because once the scheduler selects the cellular path, it continues to re-selecting it unless the path degrades, which does not occur in this scenario. Also, default scheduler operating with Cubic variant presents video degradation on picture discards. Throughput performance in Figures 12 shows that Cellular path is used predominantly during video streaming, due to Wi-Fi large delay and packet loss.

Finally, Figures 13(a) and (b) report on TCP Cubic variant and GR-STY scheduler impact on picture discard performance across multiple no loss Wi-Fi delay scenarios, respectively. TCP Cubic consistently deliver high performance, whereas GR-STY delivers high performance across all TCP variants except coupled LIA, OLIA and BALIA. A Cubic and GR-STY combo is our recommended variant/scheduler choice.

VI. Conclusion and Future work

We have provided an extensive analysis of path schedulers and TCP variants impact on video streaming performance over multiple paths. We have shown that some combinations of path schedulers with TCP variants negatively impact video streaming performance under certain network scenarios. In particular, we have shown video performance degradation for popular LIA and OLIA TCP variants, for which their congestion adjustment coupling slows down their recovery from packet losses. We are currently investigating if similar performance issues appear in 5G cellular links.

Acknowledgments

Work supported in part by JSPS KAKENHI Grant #20K11792, and National Institute of Information and Communication Technology (NICT).

References

[1] S. Afzal et al., “A Novel Scheduling Strategy for MMT-based Multipath Video Streaming,” In Proc. of IEEE Global Communications Conference - GLOBECOM, pp. 206-212, 2018.

[2] A. Aliyu et al., “Interference-Aware Multipath Video Streaming in Vehicular Environments,” In IEEE Access Special Section on Towards Service-Centric Internet of Things (IoT): From Modeling to Practice, Volume 6, pp. 47610-47626, 2018.

[3] M. Allman, V. Paxson, and W. Stevens, “TCP Congestion Control,” IETF RFC 2581, April 1999.

[4] Arzani et al., “Deconstructing MPTCP Performance,” In Proceedings of IEEE 22nd ICNP, pp. 269-274, 2014.

[5] D. Cavendish, K. Kumazoe, M. Tsuru, Y. Oie, and M. Gerla, “Capacity and Congestion Probing: TCP Congestion Avoidance via Path Capacity and Storage Estimation,” IEEE Second International Conference on Evolving Internet, pp. 42-48, September 2010.

[6] E. Dong et al., “LAMPS: A Loss Aware Scheduler for Multipath TCP over Highly Lossy Networks,” *Proc. of the 42th IEEE Conference on Local Computer Networks*, pp. 1-9, October 2017.

[7] S. Ferlin et al., “BLEST: Blocking Estimation-based MPTCP Scheduler for Heterogeneous Networks,” In Proc. of IFIP Networking Conference, pp. 431-439, 2016.

[8] A. Ford et al., “Architectural Guidelines for Multipath TCP Development,” IETF RFC 6182, 2011.

[9] A. Frommgen, J. Heuschkel and B. Koldehofe, “Multipath TCP Scheduling for Thin Streams: Active Probing and One-way Delay-awareness,” IEEE Int. Conference on Communications (ICC), pp.1-7, May 2018.

[10] J. Hwang and J. Yoo, “Packet Scheduling for Multipath TCP,” IEEE 7th Int. Conference on Ubiquitous and Future Networks, pp.177-179, July 2015.

[11] R. Khalili, N. Gast, and J-Y Le Boudec, “MPTCP Is Not Pareto-Optimal: Performance Issues and a Possible Solution,” IEEE/ACM Trans. on Networking, Vol. 21, No. 5, pp. 1651-1665, Aug. 2013.

[12] Kimura et al., “Alternative Scheduling Decisions for Multipath TCP,” IEEE Communications Letters, Vol. 21, No. 11, pp. 2412-2415, Nov. 2017.

[13] R. Lubben and J. Morgenroth, “An Old Couple: Loss-Based Congestion Control and Minimum RTT Scheduling in MPTCP,” IEEE 44th Conference on Local Computer Networks, pp.300-307, October 2019.

[14] Matsufuji et al., “Multipath TCP Packet Schedulers for Streaming Video,” IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM) , August 2017, pp. 1-6.

[15] Nagayama et al., “TCP State Driven MPTCP Packet Scheduling for Streaming Video,” IARIA 10th International Conference on Evolving Internet, pp. 9-14, June 2018.

[16] Nagayama et al., “Path Switching Schedulers for MPTCP Streaming Video,” IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM) , August 2019, pp. 1-6.

[17] R. K. P. Mok et al., “Measuring the Quality of Experience of HTTP Video Streaming,” Proc. of IEEE International Symposium on Integrated Network Management, pp. 485-492, May 2011.

[18] M. R. Palash et al., “MPWiFi: Synergizing MPTCP Based Simultaneous Multipath Access and WiFi Network Performance,” IEEE Transactions on Mobile Computing, Vol. 19, No. 1, pp. 142-158, Jan. 2020.

[19] Z. Lu, V. S. Somayazulu, and H. Moustafa, “Context Adaptive Cross-Layer TCP Optimization for Internet Video Streaming,” In Proc. of IEEE ICC 14, pp. 1723-1728, 2014.

[20] C. Raiciu, M. Handly, and D. Wischik, “Coupled Congestion Control for Multipath Transport Protocols,” IETF RFC 6356, 2011.

[21] I. Rhee, L. Xu, and S. Ha, “CUBIC for Fast Long-Distance Networks,” Internet Draft, draft-rhee-tcpm-ctcp-02, August 2008.

[22] M. Sridharan, K. Tan, D. Bansal, and D. Thaler, “Compound TCP: A New Congestion Control for High-Speed and Long Distance Networks,” Internet Draft, draft-sridharan-tcpm-ctcp-02, November 2008.

[23] F. Silva, D. Bogusevschi, and G-M. Muntean, “A MPTCP-based RTT-aware Packet Delivery Prioritization Algorithm in AR/VR Scenarios,” In Proc. of IEEE Intern. Wireless Communications & Mobile Computing Conference - IWCMCC 18, pp. 95-100, June 2018.

[24] H. Sinky et al., “Proactive Multipath TCP for Seamless Handoff in Heterogeneous Wireless Access Networks,” IEEE Transactions on Wireless Communications, Vol. 15, Iss. 7, pp. 4754-4764, 2016.

[25] A. Walid et al., “Balanced Linked Adaptation Congestion Control Algorithm for MPTCP,” IETF draft draft-walid-mptcp-congestion-control, 2014.

[26] Xue et al., “DPSAF: Forward Prediction Based Dynamic Packet Scheduling and Adjusting With Feedback for Multipath TCP in Lossy Heterogeneous Networks,” IEEE/ACM Trans. on Vehicular Technology, Vol. 67, No. 2, pp. 1521-1534, Feb. 2018.

 ISBN: 978-1-61208-880-8

Advances in Mobile Medium Ad Hoc Network Research

John DeDourek, Przemyslaw Pochec
Faculty of Computer Science
University of New Brunswick
Fredericton, Canada
e-mail: {dedourek, pochec}@unb.ca

***Abstract*—Mobile Medium Ad Hoc Network (M2ANET) is the network model that can replace the Mobile Ad Hoc Network (MANET) model. New features of the simulation environment for experimenting with Mobile Medium are presented: random motion generation with no border effect, a technique for transforming motion paths and extensions of 2D simulation to 3D. Factors impacting Mobile Medium performance are reviewed, including node density and node mobility patterns.**

Keywords-MANET; Mobile Medium; simulation; movement generators

I. INTRODUCTION

Ten years have passed since the introduction of Mobile Medium: a new model of a mobile ad hoc network [1]. Since then, in collaboration with 10 graduate students, we developed simulation tools for evaluating new models and investigated numerous scenarios and configurations demonstrating the power of the new model. The purpose of this paper is to provide a summary of our findings and give a single go-to resource for referencing the body of our research.

In Section II, we compare the new Mobile Medium model to a standard MANET. In Section III, we present selected contributions to wireless network simulation that were developed when investigating M2ANETs. In Section IV, the highlights of the developed network configurations and their performance are summarized. Finally, Section V presents the ideas about the future of Mobile Medium.

II. MANET VS M2ANET

A Mobile Ad hoc Network is created from a group of mobile wireless nodes exchanging messages with one another [2]. Mobile devices are linked together through wireless connections without infrastructure and can change locations and reconfigure network connections. During the lifetime of the network, nodes are free to move around within the network and node mobility plays an important role in determining mobile ad hoc network performance [2]. A Mobile Medium Ad Hoc Network, proposed in [1], is a particular configuration of a typical MANET where mobile nodes are divided into two categories: (i) the forwarding only nodes forming the so called Mobile Medium, and (ii) the communicating nodes, mobile or otherwise, that send data and use this Mobile Medium for communication. The advantage of this M2ANET model is that the performance of such a network is based on *how well the Mobile Medium can carry the messages between the communicating nodes and not based on whether all mobile nodes form a fully connected network (Figure 1, note that the path between two communicating nodes marked in red exists, while some of the forwarding nodes in blue remain out of range).*

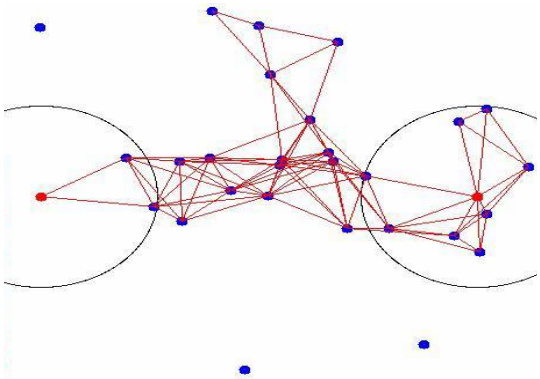


Figure 1. Sample M2ANET with two communicating nodes [1].

Multi-hop transmissions are possible when routing is used to forward packets to more distant nodes. An example of an implementation of a M2ANET is a cloud of drones equipped with routers released over an area of interest to facilitate communication in this area. A deployment of a MANET is characterized by the physical parameters of transceivers at each node, the number of nodes used, their movement pattern and the routing and transmission protocols used. They all impact the performance of the network. Given a MANET with its many complicated deployment characteristics, simulation can be applied to evaluate its performance.

III. ADVANCES IN MOBILE NETWORK SIMULATION

Mobile Medium can be viewed as a cloud of nodes buzzing in space and ready to carry a message between any nodes trying to communicate through it. Standard simulation tools used for MANET research can be used for experimenting with such a network. In our work, we addressed two particular features of the modelling environment: modelling motion and modelling in 3D.

A. Avoiding the border effect

Random mobility model is commonly used as a reference scenario in mobile network investigations. The model available in a popular open source simulator ns2 is the Random Way Point (RWP) model [3]. In RWP, nodes are

 ISBN: 978-1-61208-880-8

moved in a piecewise linear fashion, with each linear segment pointing to a randomly selected destination and the node moving at a constant, but randomly selected speed. RWP models suffer from what is called the border effect, which is a non uniformity in node density along the edges of the region where the mobile nodes are confined to stay. To create models of Mobile Medium with uniform density of nodes, we modified the RWP movement generator and created a new movement generator for the ns2 simulator that does not suffer form the border effect [4].

B. Transforming movement paths

A typical RWP movement generator directs the node to move along a straight path. Aiming at a new modelling environment with movements along curves, we created a new tool, which uses the RWP generated paths as input and then generates new movements with each straight line replaced by a fractal curve [5].

C. Modelling mobile networks in 3D

A typical mobile network simulation environment, like ns2, models mobile nodes moving on a 2D plane. We modified the open source ns2 simulator [3] to allow for modelling Mobile Medium with nodes moving in 3D [6]. This work included developing an RWP movement generator for the 3D environment.

IV. FOCUS ON DENSITY AND NODE MOVEMENT IN M2ANETS

Mobile Medium is a structure (medium) through which data is transmitted. The quality of communication depends on the properties of individual nodes (range, data rate, protocol) and the placement of the nodes in the network. The topology of the network and the movement of the nodes was the main focus of our research on Mobile Medium.

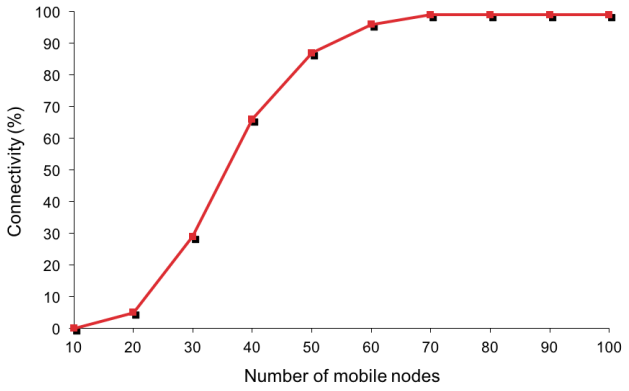


Figure 2. A typical relation between node density and user connectivity in a M2ANET [1].

The early work demonstrated a strong relation between the node density and the quality of the channel (measured as user connectivity, Figure 2) [1]. Using the RWP movement as the base scenario, we researched the Mobile Medium behavior with the node movement constrained. Either the allowed paths were constrained, like in a simulated city grid where the nodes travel in the predetermined corridors only [7], or the individual node movement was controlled by an algorithm. Two controlled movement scenarios were used: nodes moving in formations with the leader node moving at random and a number of follower nodes tracing behind at a distance [8], and all nodes still moving along random paths but exercising autonomous control ever their speed [9]. In the latter scenario the nodes would slow down when placed in a location with lots of network traffic.

V. CONCLUSION AND FUTURE WORK

Mobile Medium proved itself as an interesting way to model ad hoc networks. In the course of investigating Mobile Medium, a number of generic simulation tools were created. These include novel traffic generators, a novel tool for transforming movement directions used in simulation and a 3D version of a popular open source simulator. The experiments showed Mobile Medium works best when there are enough nodes in the medium (high density) to form reliable paths for communication and when nodes are able to stay in the areas where most traffic occurs.

The model may form the basis of future infrastructureless autonomous and adaptable ad hoc networks.

REFERENCES

[1] J. DeDourek and P. Pochec, "M2ANET: a Mobile Medium Ad hoc Network", Wireless Sensor Networks: Theory and Practice, WSN 2011, Paris, France, Feb. 2011, pp. 1-4.

[2] S. K. Sarkar, T. G. Basavaraju, and C. Puttamadappa, Ad hoc Mobile Wireless Networks, Principles, Protocols, and Applications, Auerbach Publications Taylor & Francis Group, 2007.

[3] H. Ekram and T. Issariyakul, Introduction to Network Simulator ns2, Springer, 2009

[4] R. Alghamdi, J. DeDourek, and P. Pochec, "Avoiding Border Effect in Mobile Network Simulation", The Twelfth International Conference on Networks ICN 2013, Seville, Spain, Jan 27 - Feb 1, 2013, pp. 184-189.

[5] H. Alseef, J. DeDourek, and P. Pochec, "A Method for Transforming Movement Paths in Wireless Mobile Network Simulation", the International Journal on Advances in Networks and Services, 2016, Vol. 9, No. 1 & 2, pp. 11-19.

[6] N. Mahmood, J. DeDourek, and P. Pochec, "M2ANET simulation in 3D in ns2", The Sixth International Conference on Advances in System Simulation SIMUL 2014, Nice, France, Oct. 12-16, pp. 24-28.

[7] M. Alzaylaee, J. DeDourek, and P. Pochec, "Linear Node Movement Patterns in MANETS", The Ninth International Conference on Wireless and Mobile Communications ICWMC 2013, Nice, France, July 21-26, 2013, pp. 162-166.

[8] A. Alshehri, J. DeDourek, and P. Pochec, "The Advantage of Moving Nodes in Formations in MANETs and M2ANETs", The Ninth International Conference on Wireless and Mobile Communications ICWMC 2013, Nice, France, July 21-26, 2013, pp. 228-232.

[9] H. Almutairi, J. DeDourek and P. Pochec, "Dynamic Node Movement Control in a Mobile Medium Ad hoc Network", The Seventh International Conference on Emerging Networks and Systems Intelligence, EMERGING 2015, July 19 - 24, 2015, Nice, France, pp. 50-54.

 ISBN: 978-1-61208-880-8

Integrating Traffic Network Clustering with Multi-objective Route Planning: a Heuristic Approach

Ying Ying Liu

Department of Computer Science
University of Manitoba
Winnipeg, Canada
Email: umliu369@myumanitoba.ca

Parimala Thulasiraman

Department of Computer Science
University of Manitoba
Winnipeg, Canada
Email: thulasir@cs.umanitoba.ca

***Abstract*—We model the autonomous path planning problem as a three-objective minimization problem with the constraint of collision free. We optimize the three objectives of distance, time, and traffic congestion, measured by the inverse of road network congestion index, with Non-dominated Sorting Genetic Algorithm II (NSGA-II) using real time traffic information on the road. In order to reduce the domino effect of congestion, we propose a novel technique to improve our optimization algorithm with road point clustering using Speed Performance Index (SPI) based similarity measurement. Our experiment shows that NSGA-II with clustering produces more congestion smart solutions than NSGA-II without clustering.**

Keywords–Internet of Things. Autonomous Path Planning. Collision Free. Multi-Objective Optimization. NSGA-II. Traffic Clustering. Affinity Propagation.

I. INTRODUCTION

Long Term Path planning for an autonomous vehicle is a complex task. Autonomous planning algorithms should be efficient and, most importantly, avoid traffic collisions. The efficiency of the algorithm is usually measured by the travel time and/or travel distance [1] under dynamic real time traffic conditions on the road network. With the importance of reducing greenhouse emission, being traffic aware and choosing less congested paths have become important objectives as well [2]. The traffic on the road adds some constrains in route planning. *Depending on the real time traffic condition, the shortest path may not be the fastest route, or the "greenest" route (least congestion), or the safest route (collision-free).* While this paper does not consider the steps for an autonomous vehicle after the initial long term path planning, such as short term maneuvers and decision making, we argue that it is important to generate more than one path at the path planning stage to provide the decision making process with alternative paths for different preferences of the sometimes conflicting objectives. Therefore, we model our autonomous path planning task as a multi-objective optimization problem [3]. The multi-objective optimization problem is to solve the minimization or maximization of N conflicting objective functions $f_i(x)$ for $i \in [1, N]$, simultaneously, subject to equality constraint function $g_j(x) = 0$ for $j \in [1, M]$ and inequality constraint function $h_k(x) \leq 0$ for $l \in [1, K]$, where the decision vectors $x = (x_1, x_2, ...x_n)^T$ belongs to the nonempty feasible region $S \subset R^n$ [4] [5]. Solution x_1 dominates x_2 if two conditions are satisfied: 1) $\forall i \in [1, N]$: $f_i(x_1) \leq f_i(x_2)$, and 2) $\exists j \in [1, N]$: $f_i(x_1) < f_i(x_2)$. Solution x_1 is also called the *non-dominated* solution. The goal of the multi-objective optimization problem can also be modeled as finding the *Pareto front* that has the set of all non-dominated solutions. Multi-objective optimization problems are often NP-hard [5]. Therefore, exact or deterministic algorithms are infeasible.

A road network can be modeled as a planar graph, where the nodes represent road points, and edges represent road segments. This graph may be considered as static or dynamic (time-dependent), and as deterministic or stochastic with respect to different aspects of the network. We consider our road network as dynamic and stochastic taking into consideration the effect of real-time traffic that changes over time. Evolutionary algorithms, based on natural and biological systems, have been adapted to solve dynamic optimization problems. Genetic algorithms is one such common evolutionary algorithm. Evolutionary meta-heuristics have applications in difficult real-world optimization problems that possess non-linearity, discreteness, large data sizes, uncertainties in computation of objectives and constraints, and so on [5] [6] .

We model the autonomous path planning problem as a three-objective minimization problem: that is, minimization of distance, time, and traffic congestion, with collision avoidance as the constraint. We consider one of the most applicable evolutionary algorithms, Non-dominated Sorting Genetic Algorithm II (NSGA-II) [7] in this paper. We further improve our optimization algorithm using real time traffic information on the road. The road network exhibits both spatial and temporal locality. Spatial because a congested road affects other roads within its neighbourhood and temporal because the traffic spreads over a period of time. This creates a domino effect on the road network. We propose an innovative technique to solve the route planning problem on this traffic network. We propose to cluster road points based on traffic conditions and integrate the clusters with the multi-objective optimization algorithm to reduce the domino effect of congestion. The paper is organized as follows. Section II discusses the related work in multi-objective path planning using NSGA-II and traffic clustering. Section III provides the formal problem statement, objectives and assumptions. Section IV explains the workings of our algorithm. Section V shows our experiment result and analysis, including visualization of the pareto front and alternative routes. Finally, Section VI concludes the paper with a summary and thoughts for future work.

II. RELATED WORK

Chitra and Subbaraj [8] use NSGA to minimize cost and delay of the dynamic shortest path routing problem in

 ISBN: 978-1-61208-880-8

computer networks. The authors show that the pareto approach generates more diverse pareto optimal solutions than the single objective weighting factor method based on Genetic Algorithm (GA). NSGA-II is an improvement of the NSGA algorithm in terms of diversity preservation and speed. In [9], timeliness reliability and travel expense are considered as the two objectives in path planning on a stochastic time-dependent transportation network. A route between an origin-destination pair is encoded as a variable-length chromosome in the NSGA-II to find the pareto-optimal routes. A road network, consisting of main streets in Beijing is considered as the case study. The selection of the route from the resulting pareto-front is said to be dependent to the travelers' decision based on their risk-sensitivity and cost-sensitivity.

Rauniyar et al. [10] formulate the pollution-routing problem with two objectives, minimization of fuel consumption (CO2 emissions), and minimization of total distance to be traversed by multiple vehicles. The authors incorporate a new paradigm of evolutionary algorithm, called multi-factorial optimization, into NSGA-II and show better performance and faster convergence than the traditional NSGA-II framework. In [11], we study 4-objective dynamic path planning using NSGA-II based on real road network and real traffic data from Aarhus, Denmark. Our 4 objectives include Total vehicular Emission Cost (TEC), travel time, number of turns, and distance. Our experiments produced a diverse set of solutions for this problem and provided the user the flexibility of selecting a path based on their preferences of the four objectives. However, this framework does not consider the collision avoidance constraint. It also does not include clustering the traffic network first before searching for the routes in the network.

We further notice that in the literature of multi-objective path planning on dynamic and stochastic road networks, the focus has been on the total cost of individual road segments that are part of the paths. Few works have extended the consideration of node-node relationship that exists naturally on a dynamic road network, that is, the temporal and spatial domino effects of traffic congestion. One approach of understanding this node-node relationship is through traffic clustering. Wang et al. [12] developed a distributed traffic clustering system based on affinity propagation algorithm [13] using Internet of Things (IoT) technologies and sensors around road points, that dynamically collects and analyzes the traffic flow data using concepts from network theory, in particular maximum flow and shortest path algorithms.

In this paper, we will first improve the traffic clustering in [12] with Speed Performance Index (SPI) [14] based similarity instead of flow based similarity. Then, we will integrate the traffic clustering into the multi-objective path planning to improve the overall solution quality of the path planning algorithm. To our best knowledge, there are few works in improving the accuracy of multi-objective dynamic path planning with clustering. In the literature, clustering has been employed to reduce the complexity of multi-objective problems. In [15], clustering of objectives is used to reduce the dimension of the optimization problem. In [16], density based clustering is used to classify regions into clusters to improve the efficiency and reliability of coverage path planning method for autonomous heterogeneous Unmanned Aerial Vehicles (UAVs). The contributions of this paper are as follows:

1) We improve the multi-objective dynamic path planning algorithm in [11] with a new objective for traffic congestion minimization and collision free constraint.
2) We improve the traffic clustering in [12] with SPI [14] based similarity instead of flow based similarity.
3) We propose an innovative technique to integrate the clusters with the multi-objective optimization algorithm to improve route planning.

III. OBJECTIVES

A road network is modeled as a directed graph $G = (V, E)$, where V is the set of nodes, and E is the set of edges. A link from node $v_i \in V$ to node $v_j \in V$ is shown by $e_{ij} \in E$. A loop-free path is represented as a linked list of nodes, with the source node S as the head and the destination node T as the tail of the linked list, with no node appearing more than once. The constrained multi-objective path planning problem is a minimization problem that finds a set of solutions with the minimum travel time, minimum distance and minimum traffic congestion, with the constraint of avoiding collisions based on real-time sensor data.

A. Objective 1: Distance

The distance of a path is calculated using (1)

$$f_1(Distance) = \sum_e l_e, \forall e \tag{1}$$

where l_e is the length of edge e on a path. l_e is calculated based on the static road network once a path is determined.

B. Objective 2: Time

The total time on a path is given by (2)

$$f_2(Time) = \sum_e t_e \forall e \tag{2}$$

where e is an edge on a path, and t_e is the total time the vehicle travels on the edge. t_e is recorded by the simulator based on real-time vehicle dynamics.

C. Objective 3: Inverse of Road Congestion Index

Road Segment Congestion Index is a measure introduced by He et al. [14]. In [14], the *SPI* R_v is expressed in (3), where v represents average vehicle speed in km/h, and V_{max} represents speed limit on the road segment in km/h. To normalize SPI, speeding is not considered in this equation, and R_v is in the range of $[0, 100]$.

$$R_v = \begin{cases} \frac{min(v, V_{max})}{V_{max}} \times 100 & \text{if vehicle count} > 0 \\ 100 & \text{otherwise} \end{cases} \tag{3}$$

The traffic state level is considered

- heavy congestion if $R_v \in [0, 25]$
- mild congestion if $R_v \in (25, 50]$
- smooth if $R_v \in (50, 75]$
- very smooth if $R_v \in (75, 100]$

The Road Segment Congestion Index, R_i, is calculated in (4) and (5), where $\overline{R_v}$ represents the average of SPI, R_{NC} denotes the proportion of non-congestion state, i.e., when the SPI is in the range of $(50, 100]$, t_{NC} denotes the duration of non-congestion state in minutes, and T_t denotes the length of the observation period in minutes. The value of R_i is in the range

of $[0, 1]$. The smaller the value of R_i, the more congested a road segment is.

$$R_i = \frac{\overline{R_v}}{100} \times R_{NC} \tag{4}$$

$$R_{NC} = \frac{t_{NC}}{T_t} \tag{5}$$

The road network congestion index, R is then expressed in (6), where L_i is the length of road segment in km. Similarity, $R \in [0, 1]$, and the smaller the value of R, the more congested a road network is. For our minimization problem, we want to find the minimal values of R^{-1} for the least congested paths using (7). Theoretically, it is possible for R to be 0, meaning that every road segment on a path is congested. However, this scenario rarely happens in reality. As shown in Figure 1, at the rush hour of 7:30 a.m., only a few disconnected road segments were color coded as red, representing high congestion status. Even if a path has R as 0 and therefore infinite value for R^{-1}, this path will be deemed a bad solution and abandoned by the optimization algorithm.

$$R = \frac{\sum\limits_{i} R_i L_i}{\sum\limits_{i} L_i} \tag{6}$$

$$f_3(R^{-1}) = \frac{\sum\limits_{e} L_e}{\sum\limits_{e} R_e L_e} \forall e \tag{7}$$

D. Constraints

The minimization optimization of the three objectives is subject to the following constraints:

$$e \in G, \forall e \in P \tag{8}$$

$$count(v) = 1, \forall v \in P \tag{9}$$

$$g_(e) = \sum_{e} CollisionCount_e = 0, \forall e \in P \tag{10}$$

where the first constraint (8) ensures that a path P is valid, that is, all its edges belong to the road network G, the second constraint (9) ensures that a path P is loop free by making sure any node in P appears exactly once, and the third constraint (10) ensures that the collision count on the entire path is zero.

IV. Solution Methodology

A. Affinity Propagation Clustering

Clustering is a preprocessing step for the multi-objective path finding. Our clustering algorithm is based on the distributed, message-passing Affinity Propagation clustering proposed by [12]. We further improve the clustering algorithm with SPI based similarity instead of flow based similarity.

First, we generate a node based SPI using algorithm 1.

Then we calculate pairwise similarity based on SPI at nodes using algorithm 2. The similarity is based on the assumption that if the target node j is congested, then the similarity between source node i and j is related to the most congested node on the shortest path from i to j. In addition, the closer i and j are spatially, the more likely they are similar.

Once the similarity is defined, the Affinity Propagation clustering algorithm works as follows. First, a node i considers itself as a cluster k, then it calculates two local variables responsibility $r(i, k)$ using (11), and availability $a(i, k)$ using (12) based on a, r values from other nodes of its communication range, as well as pair-wise similarity s it calculates based on the traffic information received from the other nodes. To compute responsibility $r(i, k)$, the algorithm finds another data point $k^{'}$ that has the highest (maximum) availability and similarity, and computes the difference in the similarity. In addition, responsibility $r(i, k)$ represents how well k is the center of i, so it does not only consider how similar i and k are, but also considers which one of i and k is more suitable be the center. Self responsibility $r(k, k)$ could be negative or positive. If it is negative, it implies that the node is more likely to be a member of some cluster rather than the center of a cluster. Finally, node i belongs to the center k that gives maximum $a(i, k) + r(i, k)$. The message passing Affinity Propagation clustering algorithm has no central control, does not require the number of clusters to be given, and runs dynamically unless terminated deliberately.

Algorithm 1 Node Speed Performance Index

Require: road graph G, node i, time step t, SPI Matrix S
Ensure: SPI_i
1: ine = G.in_edges(i)
2: oute = G.out_edges(i)
3: ineSPI, outeSPI = 0
4: **for** i, j, d in ine **do**
5: $ineSPI = ineSPI + S[i, j][t]$
6: **end for**
7: **for** i, j, d in oute **do**
8: $outeSPI = outSPI + S[i, j][t]$
9: **end for**
10: SPI_i = average($\frac{ineSPI}{len(ine)}$,$\frac{outeSPI}{len(oute)}$)

Algorithm 2 Pairwise SPI Similarity

Require: road graph G, origin i, target j, time step t, SPI Matrix S
Ensure: $Sim(i, j)$
1: Calculate SPI_j
2: p = G.ShortestPath(i, j)
3: $minSPI$ is the smallest SPI on p {Distance in km}
4: $dist = len(p)$
5: $Sim(i, j) = \frac{minSPI}{SPI_j * max(dist,1)}$

$$r(i, k) = s(i, k) - \max_{k' \neq k}(a(i, k') + s(i, k')) \tag{11}$$

$$a(i, k) = \begin{cases} \min(0, r(k, k)) - \sum\limits_{i' \neq i,k} \max(0, r(i', k)) & \text{if } i \neq k \\ \sum\limits_{i' \neq i,k} \max(0, r(i', k)) & \text{if } i = k \end{cases} \tag{12}$$

B. Multi-objective Path Finding

Once we have cluster ids of each node at time step t, the NSGA-II multi-objective path finding process in (4) [11] is executed.

Algorithm 3 Message Passing Affinity Propagation Traffic Clustering at Node i

Require: road graph G, time step t
Ensure: cluster id k
1: Initialize availability $a_i = [0]$
2: **while** not terminated **do**
3: Compute pair-wise similarity s
4: Collect a from adjacent nodes
5: Calculate r_i
6: Broadcast r_i
7: Receive r from adjacent nodes
8: Calculate a_i
9: Broadcast a_i
10: Compute local cluster id k at time t
11: **end while**

Algorithm 4 NSGAII for Traffic Aware Many-Objective Dynamic Route Planning

Require: road graph G, start node s, end node t, $initPopulationSize$, $generations$, $crossoverPoints$, $tournamentSize$, $mutationProb$
Ensure: $paretoFront$
{Initialization}
1: $population$ = randomLoopFreePath (s, t, $initPopulationSize$)
{Main loop}
2: **for** $generation \leftarrow 1, generations$ **do**
3: $population$ = breedPopulation($population$, $crossoverPoints$, $tournamentSize$, $mutationProb$)
4: $scores$ = scorePopulation($population$)
5: $population$ = buildParetoPopulation($population$, $scores$)
6: **end for**
{Final Pareto Front}
7: $scores$ = scorePopulation($population$)
8: $paretoFront$ = identifyPareto($population$,$scores$)

1) Collision Avoidance: The constraint of collision avoidance is added to the solution selection process of the main algorithm. Solution x_1 constrained-dominate x_2 in the following three situations [5]:

- solution x_1 is feasible and x_2 is not.
- x_1 and x_2 are both infeasible, but x_1 has a smaller constraint violation.
- x_1 and x_2 are both feasible and solution x_1 dominates solution x_2 in the usual sense.

This relaxed selection process allows infeasible but less constrained parents to be included in the breed process, and allows for better diversity in the end. At the selection of the final pareto front, all the infeasible solutions are removed from the solution set.

2) Clustering Incorporation: In order to incorporate the clustering result into the process, we make an important assumption: if start node i and j of a directed edge $e = i- > j$ are in the same traffic cluster at time t, then all the incoming edges of i are affected by e in terms of traffic, because the traffic flows in this order: the incoming edges of $i- > i- > j$. Based on this assumption, we take the average of all SPI values of the incoming edges of i and e, and assign the average value back to these edges. This process is described in the following algorithm 5.

Algorithm 5 Cluster Average SPI

Require: road graph G, begin node i, end node j, time step t, SPI matrix S, Cluster matrix C
Ensure: Cluster Average SPI matrix S'
1: **if** C[i][t] == C[j][t] **then**
2: ine = G.in_edges(i)
3: eid = G.edges.index((i,j))
4: sumSPI = S[eid][t]
5: **for** a, b, d in ine **do**
6: eid = G.edges.index((a,b))
7: sumSPI += S[eid][t]
8: **end for**
9: avgSPI = $\frac{sumSPI}{(1+len(ine))}$
10: **for** a, b, d in ine **do**
11: eid = G.edges.index((a,b))
12: S[eid][t] = avgSPI
13: **end for**
14: **end if**

V. Evaluation and Analysis of Results

A. Road Network and Traffic Data

The road network of Aarhus, Denmark [17] is represented as a graph composed of 136 nodes and 443 edges. In addition to the topology, the metadata also includes the latitude and longitude of the nodes, the street name of a node, and the speed limit and length of an edge. The traffic data includes sensor data recorded on each edge from February to June 2014, such as vehicle counts and average speed. The sensor data is collected every five minutes. Because there is no collision data available at the data set, we simulated random collision points using the roulette wheel selection, that is, if a random number is smaller than the probability calculated using a small constant p and the road segment congestion index R_e, then there is a collision on the road. In this paper, $p = 5$. Since $R_e \in [0, 1]$, the selection probability is in the range of $[5\%, 10\%]$. The more congested a road segment is, the more likely there is a collision. In the future work, we will simulate the traffic flow and collision in the road network simulator SUMO (Simulation of Urban MObility) [18].

B. Implementation and Parameters

The code of the paper is written in Python 3, with references to code snippets from [19]–[21].The experiments are run on a MacBook Pro with 2.3 GHz Intel Core i5 and 8 GB 2133 MHz LPDDR3.

For our experiments, we consider multi-objective dynamic path planning from $startNode$ 4320 (city of Hinnerup) to $endNode$ 4551 (city of Hasselager). We determine experimentally the parameters for NSGA-II as $initPopulationSize = 100$, $generations = 100$, $crossoverPoints = 5$, $tournamentSize = 2$, $mutationProb = 0.8$. For traffic data, we treat the beginning timestamp 2014-03-01T07:30:00 as $timeIdx = 0$.

C. Improvement of Traffic Clustering using SPI Based Similarity

We evaluate the cluster quality using the same metrics used by [12], including Silhouette coefficient [22] and the mean

 ISBN: 978-1-61208-880-8

TABLE I. RESULT COMPARISON OF FLOW BASED AND SPI BASED AFFINITY PROPAGATION CLUSTERING

Time Stamp	Flow Based Clustering			SPI Based Clustering		
	Number of Clusters	Silhouette coefficient	Mean Similarity	Number of Clusters	Silhouette coefficient	Mean Similarity
2014-03-01 T07:30:00	0	0	0.041	25	0.481	0.710
2014-03-01 T07:35:00	26	0.207	0.313	25	0.480	0.713
2014-03-01 T07:40:00	21	0.174	0.266	25	0.480	0.712
2014-03-01 T07:45:00	22	0.206	0.296	25	0.475	0.710

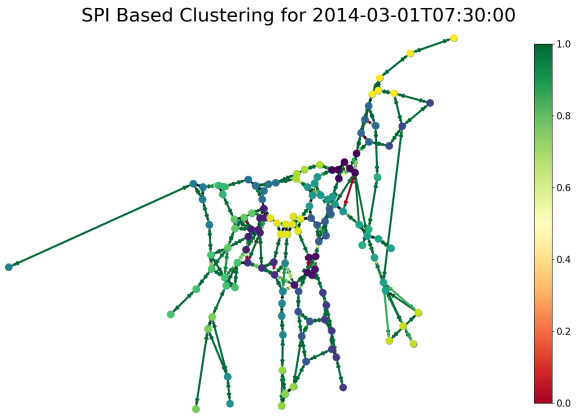


Figure 1. Traffic Clustering of the road network of Aarhus, Denmark

similarity within all clusters. Silhouette coefficient evaluates item similarities of inter and intra clusters. Mean similarity is the average of all pairs of intra-cluster similarity. For both metrics, higher values indicate higher cluster quality. As shown in table I, the use of SPI based similarity is very effective in improving the clustering of the road points. In these four time stamps, SPI based clustering creates much higher values of Silhouette coefficient and mean similarity consistently. Figure 1 is a visualization of the road map of Aarhus, Denmark at 7:30 a.m. on 2014-03-01, where the nodes are marked and color coded with their cluster ids, and the edges are color coded with road segment congestion index R_i. The color red means heavy congestion with $R_i = 0$, and green means very smooth with $R_i = 1$. The visualization shows that adjacently connected road points usually belong to the same cluster, and these road segments have similar traffic conditions. This is because the SPI based similarity considers both congestion conditions and spatial adjacency between two road points.

D. Improvement of Multi-objective Path Planning with Clustering

For the multi-objective path planning, we compare our NSGA-II with clustering with the same algorithm without incorporation of clustering. Table II shows the comparison of A* [23] shortest path, NSGA-II and NSGA-II with clustering in terms of the three objectives, one constraint, and an additional metric called total vehicular emission cost (TEC) [24]. This metric is used in our previous paper [11] as one objective of monetized value for vehicular emission. For the convenience of comparison, we take average of each object for all the pareto

TABLE II. RESULT COMPARISON OF A*, NSGA-II, AND NSGA-II WITH CLUSTERING

Path Finding Algorithm	Number of Solutions	Objectives			Constraint	Other Metric
		Average Distance (KM)	*Average Time (Minutes)*	*Average R Inverse*	*Average Collision*	*Average TEC*
A*	1	22.825	33.031	1.201	1	0.069
NSGA-II	100	29.769	57.828	1.132	0	0.075
NSGA-II with Clustering	100	31.072	45.457	1.089	0	0.068

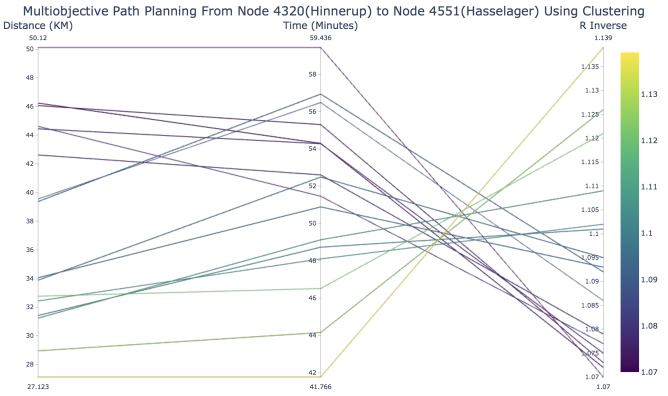


Figure 2. MOO with Clustering Pareto Front Visualization

front solutions in three independent executions of the programs. The single objective A* path has the shortest distance, but it does not guarantee collision free. It also has higher than average R^{-1} compared to the multi-objective approaches. In comparison, the multi-objective approaches produce a diverse variety of solutions for the decision making process to choose from. Between the two multi-objective approaches, we observe that although the clustering based approach generates longer paths in average, the travel time and congestion are both more optimized than the other approach. The lower average value of TEC also indicates that these solutions are more traffic smart. Figure 2 is the parallel coordinate visualizations of pareto front.

Finally, Figure 3 shows three alternative paths found by the clustering based approach: the path with minimum distance (blue nodes), the one with minimum time (yellow nodes), the one with least congestion (green nodes). For comparison, A* shortest path is also highlighted (red nodes). This visualization has a limitation that a node belonging to multiple paths only carries the color of one path following the coloring sequence mentioned in the previous sentences. For example, if a node is on both the MOO path of least congestion and the A* path, it is colored as red. Despite of this limitation, this figure shows different possibilities of path planning depending on the preference of the decision making system.

VI. Conclusion and Future Work

In this paper, we model the autonomous path planning problem as a three-objective minimization problem with the constraint of collision free. We show that our NSGA-II based framework finds a diverse set of alternative solutions for the decision making system to choose from based on the

 ISBN: 978-1-61208-880-8

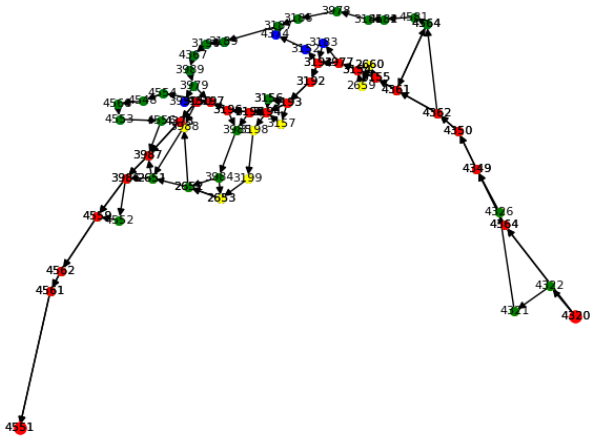


Figure 3. MOO with Clustering Path Examples Visualization

preference of the three objectives: distance, time, and traffic congestion, instead of one single solution from the A* shortest path algorithm. We propose a novel approach to integrate SPI based road point clustering into the multi-objective optimization considering the domino effect of congestion. Our experiment shows that NSGA-II with clustering produces more congestion smart solutions than NSGA-II without clustering.

As a future work, we would like to extend our work in three directions:

1) Explore other multi-objective evolutionary algorithms, such as multi-objective Ant Colony Optimization (ACO) [25] and MultiObjective Evolutionary Algorithm based on Decomposition (MOEA/D) [26].
2) Explore traffic prediction techniques such as the emerging Graph Neural Networks [27].
3) Simulate the traffic flow and collision in the road network simulator SUMO (Simulation of Urban MObility).

REFERENCES

[1] S. Aggarwal and N. Kumar, "Path planning techniques for unmanned aerial vehicles: A review, solutions, and challenges," Computer Communications, vol. 149, 2020, pp. 270–299.

[2] V. Roberge and M. Tarbouchi, "Fast path planning for unmanned aerial vehicle using embedded gpu system," in 2017 14th International Multi-Conference on Systems, Signals & Devices (SSD). IEEE, 2017, pp. 145–150.

[3] H. W. Kuhn and A. W. Tucker, "Nonlinear programming," in Traces and emergence of nonlinear programming. Springer, 2014, pp. 247–258.

[4] M. Abido, "A novel multiobjective evolutionary algorithm for environmental/economic power dispatch," Electric power systems research, vol. 65, no. 1, 2003, pp. 71–81.

[5] J. Branke, J. Branke, K. Deb, K. Miettinen, and R. Slowiński, Multiobjective optimization: Interactive and evolutionary approaches. Springer Science & Business Media, 2008, vol. 5252.

[6] J. Del Ser, E. Osaba, J. J. Sanchez-Medina, and I. Fister, "Bioinspired computational intelligence and transportation systems: a long road ahead," IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 2, 2019, pp. 466–495.

[7] K. Deb, A. Pratap, S. Agarwal, and T. Meyarivan, "A fast and elitist multiobjective genetic algorithm: NSGA-II," IEEE transactions on evolutionary computation, vol. 6, no. 2, 2002, pp. 182–197.

[8] C. Chitra and P. Subbaraj, "A nondominated sorting genetic algorithm for shortest path routing problem," International journal of computer engineering, vol. 5, no. 1, 2010, pp. 55–63.

[9] Y. Li and L. Guo, "Multi-objective optimal path finding in stochastic time-dependent transportation networks considering timeliness reliability and travel expense," in 2016 Prognostics and System Health Management Conference (PHM-Chengdu). IEEE, 2016, pp. 1–6.

[10] A. Rauniyar, R. Nath, and P. K. Muhuri, "Multi-factorial evolutionary algorithm based novel solution approach for multi-objective pollution-routing problem," Computers & Industrial Engineering, vol. 130, 2019, pp. 757–771.

[11] Y. Y. Liu, F. Enayatollahi, and P. Thulasiraman, "Traffic aware many-objective dynamic route planning," in 2019 IEEE Symposium Series on Computational Intelligence (SSCI). IEEE, 2019, pp. 1241–1248.

[12] Z. Wang, P. Thulasiraman, and R. Thulasiram, "A dynamic traffic awareness system for urban driving," in 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2019, pp. 945–952.

[13] B. J. Frey and D. Dueck, "Clustering by passing messages between data points," science, vol. 315, no. 5814, 2007, pp. 972–976.

[14] F. He, X. Yan, Y. Liu, and L. Ma, "A traffic congestion assessment method for urban road networks based on speed performance index," Procedia engineering, vol. 137, 2016, pp. 425–433.

[15] X. Guo, Y. Wang, and X. Wang, "Using objective clustering for solving many-objective optimization problems," Mathematical Problems in Engineering, vol. 2013, 2013.

[16] J. Chen, C. Du, Y. Zhang, P. Han, and W. Wei, "A clustering-based coverage path planning method for autonomous heterogeneous uavs," IEEE Transactions on Intelligent Transportation Systems, 2021, pp. 1–11.

[17] "Road traffic data of Aarhus, Denmark," http://iot.ee.surrey.ac.uk:8080/datasets.html, accessed: 2021-04-20.

[18] P. A. Lopez, M. Behrisch, L. Bieker-Walz, J. Erdmann, Y.-P. Flötteröd, R. Hilbrich, L. Lücken, J. Rummel, P. Wagner, and E. WieBner, "Microscopic traffic simulation using SUMO," in 2018 21st International Conference on Intelligent Transportation Systems (ITSC). IEEE, 2018, pp. 2575–2582.

[19] "Python for healthcare modelling and data science," https://pythonhealthcare.org/2019/01/17/117-genetic-algorithms-2-a-multiple-objective-genetic-algorithm-nsga-ii/, accessed: 2021-04-20.

[20] "Platypus - multiobjective optimization in python," https://platypus.readthedocs.io/en/latest/, accessed: 2021-04-20.

[21] "scikit-learn - machine learning in python," https://scikit-learn.org/stable/, accessed: 2021-04-20.

[22] P. J. Rousseeuw, "Silhouettes: a graphical aid to the interpretation and validation of cluster analysis," Journal of computational and applied mathematics, vol. 20, 1987, pp. 53–65.

[23] P. E. Hart, N. J. Nilsson, and B. Raphael, "A formal basis for the heuristic determination of minimum cost paths," IEEE transactions on Systems Science and Cybernetics, vol. 4, no. 2, 1968, pp. 100–107.

[24] Y. Wang and W. Y. Szeto, "Multiobjective environmentally sustainable road network design using pareto optimization," Computer-Aided Civil and Infrastructure Engineering, vol. 32, no. 11, 2017, pp. 964–987.

[25] L. Ke, Q. Zhang, and R. Battiti, "Moea/d-aco: A multiobjective evolutionary algorithm using decomposition and antcolony," IEEE transactions on cybernetics, vol. 43, no. 6, 2013, pp. 1845–1859.

[26] Q. Zhang and H. Li, "Moea/d: A multiobjective evolutionary algorithm based on decomposition," IEEE Transactions on evolutionary computation, vol. 11, no. 6, 2007, pp. 712–731.

[27] Z. Cui, K. Henrickson, R. Ke, and Y. Wang, "Traffic graph convolutional recurrent neural network: A deep learning framework for network-scale traffic learning and forecasting," IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 11, 2019, pp. 4883–4894.

Web Vulnerability in 2021: Large Scale Inspection, Findings, Analysis and Remedies

Borka Jerman Blažič
International Postgraduate School Jožef Stefan
IJS; Laboratory for Open systems and networks
Ljubljana, Slovenia
e-mail: borka@e5.ijs.si

Primož Cigoj
Institute Jožef Stefan
Laboratory for Open systems and Networks
Ljubljana, Slovenia
e-mail: primoz@e5.ijs.si

Abstract: **The main focus of the cyber-security community has been to make operating systems and communication networks more secure and harder for attackers to penetrate. The most frequently used web application and user web pages are developed today with the Web Content Management System (WCMS), as it allows user-friendly access, easy development and operation. Any malware that can penetrate the WCMS can significantly affect the system itself and the service the web pages offer. This paper presents the approach for identifying the vulnerabilities of the majority of Internet sites with WCMS applications and the remedies to be applied with the use of an automated, fast and dynamic vulnerability detection tool. The state of the web sites vulnerability in Europe and the impact factors that influence the vulnerability to be present are presented and discussed.**

Keywords- cybersecurity; scanners and crawlers; WCMS vulnerability; security state of European web space.

I. INTRODUCTION

We do business, pay through the Internet, store documents and share our personal information, card numbers and identification data online very frequently. There is no doubt that this data is private and should be stored as safely as possible. The vision of the future Internet involves building a new generation of applications made by merging services and data from different providers and organizations [1]. Web services provide the basic interface between the provider and the consumer, supported by complex software components like the operating system, the server application and many additional systems like databases, shops and selling systems, appliances for different services, etc. Web services are subject to several unique security concerns, due to their pervasiveness, seamless interoperability and operations that can be remotely invoked by the user, and they need to be carefully considered in view of the envisioned architecture of the future Internet. The major web-security concern is related to the differences between the web applications that do not have embedded security protection and the security solutions present in traditional messaging techniques applied within other Internet services. For instance, the SOAP protocol used in web-service communications does not address the security itself and can be bypassed by a firewall [2].

This article provides a brief overview of the tools used for inspecting the web vulnerability at large and the newly developed tool called VulNet that scan the Internet web space at large for identifying vulnerability within websites built with WCMS (Web Content Management System) application. The tool is an advancement in the field when compared with other known proprietary or open-access tools. Its major improved properties are fast scanning at large, ethical search of vulnerability, acceptable scoring mechanism enabling comparison of the security between the web spaces in different regions of the world. The paper is divided into five sections. After the introduction, the second section introduces the reader to the area and describes the problem being addressed. The third section presents the tool components and its functionality. The next section provides an overview of the results and informs about the factors that impact the appearance of higher presence of vulnerability among particular web spaces. The paper ends with a conclusion and points to the limitation of the tool and the presented study results.

II. OVERVIEW OF THE AREA

A. WCMS

The continuous evolution of networks based on Internet technology has made its services very attractive and many different new applications appeared with the use of WCMS. A modern Content-Management System (CMS) like Word-Press simplifies website creation as it allows the functionality of the site to be extended with additional applications known as plug-ins that are available for downloading from known databases. Currently, the estimated number of plug-ins is close to 54,000 and the total number of downloads is close to 900 million. Public web applications are usually accessible from anywhere in the world, but many corporate web applications that are set on networks with restricted access are also accessible. Web applications handle very sensitive information, ranging from banking to health directories, as well as personal images and photographs that are of interest to criminals and attackers. According to a survey carried out by W3Tech, about 52.9% of Internet websites use some kind of web-content management system [3]. The most popular open-source Web-Content Management Systems (WCMSs) are

 ISBN: 978-1-61208-880-8

WordPress, Drupal and Joomla [4]. A technology survey by BuiltWith Pty Ltd in 2017 concluded that about 46% of the top one million websites use WordPress [5]. The reason is that WCMSs allow users, even without an in-depth knowledge of web technology, to deploy and offer system content to users. Due to the popularity of these systems, they have become an interesting target for malicious attackers, and, therefore, the importance of the security features and the overall vulnerability of these applications have become very important, especially in cases where the web-content owners do not possess the necessary knowledge and understanding of the possible threats to the system. Writing computer programs is a complex task and modern software development usually involves combining many libraries and frequently not all the bugs have been removed in the developed software. Design errors become a risk, especially when the security of the program has not been taken into consideration from the beginning of the design process. The architecture and the design of a computer system are expected to be coherent and to follow the security principles, but this is not the case in the current web space [5]. Knowing the system's vulnerability represents the most vital and precious information for malicious parties. The removal of the vulnerability increases the resilience of the underlying system. That is why the operation and management of the web system should be actively monitoring and removing the vulnerable parts of the system to prevent possible attacks. The vulnerability testing of websites can be performed using two approaches. One is called white-box testing, in which the testing software has access to the source code of the application and this source code is then analyzed to track down defections and vulnerabilities in the code. These operations are expected to be integrated into the web-development process with the help of add-on tools within the development environments, but they are usually not used, especially when the system is upgraded with new plug-ins to enhance the service and user satisfaction. The other approach is called black-box testing, where the tool has no direct access to the source code, but instead it tries to find vulnerabilities and bugs with special input test cases that are generated by the tool and then sent to the application. Responses are then analyzed for unexpected system behaviors that indicate the errors or vulnerabilities of the system. A black-box security scanner typically uses a mixture of passive (typically, during the crawl) and active (typically, post-crawl) vulnerability- testing techniques like code execution [6].

B. Crawlers and scanners

Identifying the vulnerabilities across the whole web space of the Internet is not an easy task, though this information is extremely valuable, helpful and required by the website owners. The available vulnerability-testing tools are either restricted to internal use by the owners of corporate or organization networks, as they use software mimicking real attacks, or they just scan the basic web server's vulnerability, without providing sufficient information about the whole WCMS system and the associated plug-ins. A common approach for inspecting the web vulnerability is scanning the Internet sites and associated domains with the use of a web crawler in combination with a search engine, such as Google. Web crawlers, however, have multiple problems. Some crawlers access the same URLs [7] more than 1000 times, as there is no intelligence in-built into the crawler that help in avoiding repeating accesses to a web site. Any web-vulnerability inspection of the web application, besides the crawler, needs additional software, as the information sought beyond the port data is located in the plug-ins and in the web pages applications. The detection of infinite loops and the actual depth of crawling in the web space are difficult as the websites are not static and the web pages change over time due to user intervention. A more difficult problem is related to the large number of pages and the amount of data included. As a consequence, the crawling process can take a long time and the results are frequently not a snapshot of the system, as multiple pages might have changed during the scan. However, in recent years some improvement to Internet-wide scanning was achieved with tools such as ZMap and MasScan [8]. ZMap was developed by the University of Michigan and is now the main tool of the Internet-search service known as Censys [9]. Shodan is a similar service that uses behavior or grab techniques to identify the vulnerabilities of sensors and similar devices. Shodan collects data mostly on web servers, but it is supplied with applications to access FTP servers and other known Internet ports such a Telnet (virtual terminal), SNMP (mail), IMAP (encrypted mail) and the Real Time Streaming Protocol. The latter are used to access web cameras and their video stream. However, Shodan does not conduct a deep review of the sites. Despite the popularity of these tools, they are not real crawlers, but rather ports scanners looking for the HTTP type of servers that are usually extended with additional applications. The collected port information using these tools does not include information about the vulnerability of the applications and the plug-ins as they operate only with an IP address and do not crawl links within the website's content. The systems are proprietary, but the service is publicly available. A similar publicly available tool is called Nmap [8], which requires multiple machines and weeks to complete any horizontal scan of the public address space, making it rather slow [5]. Running regular web vulnerability scanners against numerous websites is time consuming and, if exploit techniques are used, the scan is considered as illegal if browsing permission is not granted by the owners. Another way of detecting the vulnerability without breaking the law [6] is to detect the application and then identify its issuing version or its fingerprint and then look in a database with the identified vulnerabilities of that particular version. The most well-known vulnerability database with vulnerable plug-ins is the National Vulnerability Database (NVD) that is hosted by the National Institute of Standards and Technology [10] and is used by most of the known scanners. The capacity of scanning web

 ISBN: 978-1-61208-880-8

sites differs among the scanners. The first group of known scanners usually scans data sets between 20,000 and 200,000 websites [11]–[13], but forgetting the rest of the web, and they are focusing on specific vulnerability, such as XSS, SSL, SQL injection, phishing, Heartbleed and search-redirection attacks, instead of covering all of them at once. In addition, their methods are also time-consuming: they need more than 9 days to measure a dataset of 200,000 websites. They focus on determining whether a given input propagates, rather than efficiently finding the propagating inputs, for arbitrary vulnerabilities [12] [14]. The second group performs the scanning of the Internet IPv4 protocol for a specifically defined subject area, such as hosted services, SSL/TLS, vulnerabilities or specific software or protocol vulnerabilities by using mass scan tools such as ZMAp, Nmap and Massscan [15]–[17]. This technique is good for the fast TCP/IP stack-fingerprinting technique to identify the OS's type, port range scan, and basic web, but not for a detailed overview of the online content vulnerabilities. In this case the CMS's core and plug-in vulnerabilities are not inspected.

TABLE I. TOOLS COMPARISON

Characteristics / Tools		Shodan	Censys	WPScan	[5]	[11]	[12]	[13]	VulNET
General Characteristics	OpenSource	No	No	Yes	No	No	No	No	Yes (A)
	URL or IP	IP	IP	URL	IP	URL	URL	URL	Both
	Results are Freely Accessible on the Internet	Yes (P)	Yes	No	No	No	No	No	Yes
	Internet-connected Devices	Yes	Yes	No	Yes	No	No	No	Yes (E)
	Automatic Scanning	Yes	Yes	No	Yes	Yes	No	No	Yes
	Ethical	Yes	Yes	Yes (P)	Yes	No	Yes	Yes	Yes
	Web UI and Command Line (CL)	Both	Both	CL	CL	No	No	No	Both
	Real-time Visualization while Scanning	No	No	No	No	No	No	No	Yes
	Free API	Yes (P)	No	No	No	No	No	No	Yes
	More than 1 million scanned IPs or Websites	Yes	Yes	No	Yes	No	No	No	Yes
WP Specific	CMS Scan	No	No	Yes	Yes	Yes	Yes	Yes	Yes
	CVE Exposer	Yes	No	Yes	Yes	No	No	No	Yes
	Plugins Scan	No	No	Yes	No	No	No	Yes (L)	Yes
	Scoring	No	No	No	No	No	No	No	Yes

P = Partly, E = Extension, A = Attended, L = Limited.

IV. VULNET AND ITS FUNCTIONALITY

The general methodology for web scanning and data collecting consists of six steps: a) collecting the IP addresses of the web targets, b) accessing and c) getting responses, d) sending queries for application patterns, e) collecting vulnerability information and f) saving and validating the results. The last three steps in current web scanners differ very much due to their capability to catch relevant objects, the range of the collected data, the speed of the provision of answers and the vulnerability analysis provided. The VulNet tool provides effective search for vulnerable servers on a large scale by scanning multiple web pages on the same host with different IP addresses.

The VulNet tool is built from four modules presented on Figure 1. The first module is the local Signature database, which stores all the known WordPress plug-ins and different core versions of the WCMS. The second module is the Common Vulnerabilities and Exposures (CVE) database, built up from different public resources available online (CVE databases, Exploit databases, etc.). In the production of these two blocks a specific methodology for scoring the vulnerability was used that indexes each known plug-in or version of the WCMS. The value of a particular index depends on the assessment of the potential threat if the vulnerability is exploited. The CVE database contains 300 identified vulnerabilities of the WordPress core versions and more than 1300 WordPress plug-ins exploits. The index value is assigned based on the developed scoring mechanism that enables easier verification of the potential damage and the vulnerability assessment. The index values for seven known vulnerabilities run from 3 to 9, but the group of all the vulnerability types is scored to 10.

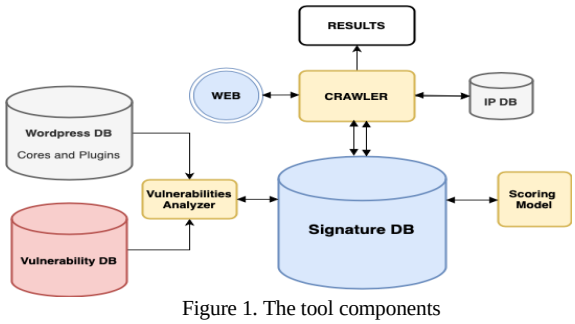


Figure 1. The tool components

The search mechanism is fast as the likelihood of false or repeated access to web site is reduced feedback information received from the crawler and the matching with the data of the temporary set data base that is set up to prevent repeating access to already visited web server. Enabled parallel computation of the code as well reduce the time for scanning. Specific scoring mechanism of insecurity based on the found vulnerability enables a rapid and reliable analysis and assessment. Since there is no list of WordPress sites on the Internet, the first step in the search process is to scan the entire web space and to find

 ISBN: 978-1-61208-880-8

the sites with a WCMS. According to Verisign's data (verysign.com) the web space is enormous, as there are more than 350 million web domains registered on the Internet. Unfortunately, not all DNS (Domain Name Server) zones are accessible (due to private networks) and for that reason a list of root domains is created in the initiation operational phase of the tool. To speed up the process, all the services that allow the use of shortened URLs, and large sites like Facebook, YouTube, and Instagram are removed from the search list as they are not operating any significant device. After identifying the presence of a WCMS the query part of the tool looks for the presence of the file under the name ''robots.txt'', used to verify whether the site allows browsing, meaning that the reviewing of the web applications is legal. The next step is sending queries to the site and collecting information about the content.

Figure 2. The vulnerability of one affected domain.

The tool looks for the web meta tag generator (<meta name ''generator'' content ''WordPress 5.1.1''>), which usually contains information about the version of the plat- form. If the data is missing, then the tool looks for CSS and JS files, (/wp-includes/js/wp-emoji-release.min.js?ver 5.2); this information is provided at the end of the file. The tool then parses the plug-ins (wp-content/plugins/wp-hide-post/public/js/wp-hide-post-public.js?ver2.0.10) to obtain the version applied. If the version of the plug-ins is not avail- able in the CVE database, then the plug-ins are stored in a separate folder for further analysis and a search of exploits. The server vulnerability of the affected domain (e.g., the country top-level domain) is presented in a way that does not show the ownership of the web site type (e.g. Apache/2.2.15 CentOS), and the IP address are also stored and used later to identify the server's location and the country of origin. The scoring assessment for the vulnerability of the website's page is based on two sets of parameters: the first set is used for the risk assessment of the website's core C(s), and the second set is used for a risk assessment of the attached plug-ins P(s). The version of the website's core is first verified and then the tool looks for the potential vulnerability of the core in the signature database. In the case of several identified vulnerabilities in a web page, the score with the highest value is selected for the website core's risk parameter. The same approach is applied to the plug-ins: the first match is found for each of the plug-ins and then the vulnerability with the highest risk parameter is selected for the plug-in's risk value.

The calculated vulnerability-risk score for the web WCMS is calculated as an aggregated score from the score obtained of the web-server core and the highest found vulnerability found among the plug-ins. The scan speed and the answers that provide the data are very important characteristics of any scanning tool. VulNet is capable of scanning 90,000 web pages in 15 minutes. The answering speed is variable, as the response of the WCMS pages depends on how fast the web server is at delivering the responses. Some servers need up to 15 seconds to respond and that timing influences the speed of the data collection. The program's logic is written in the Python programming language.

IV. THE STUDY RESULTS

A. General findings

In the first scan with Vulnet 115 million randomly scanned web addresses from around the world (over 194 countries) were accessed. The tool established 126,086,633 links, but some of the visited web servers were found to not be active as the waiting time response of 15 seconds was exited. Among these sites there were 16,274,980 valid WordPress installations and 14,887,047 plug-in installations. In the identified web set, more than 5,018,262 were found to be vulnerable, representing 31% of all the WordPress installations on the Internet, where 2,475,337 had a higher score than 5. A total of 4,356,067 vulnerabilities were detected among the detected plug-ins and 2,795,855 had a score higher than 5. The analysis of the results revealed that there are very vulnerable core versions of WordPress, recent versions of WordPress accounting for over 1 million vulnerable pages tool of found vulnerability in an affected domain. The repeated scan that was implemented six months later showed that the number of identified top-10 vulnerable plug-ins as well the top-10 outdated vulnerable plug-ins were not changed very much, neither in frequency nor in plug-in type. However, some other changes were noticed in the general scan. The status of 12,865,441 websites from the first run and 10,330,577 among them retained the same vulnerability status. There was found lower number of unknown core version and higher version of secure web sites. This transitions from hidden core versions with the implementation of new WP core versions release in 2020 contributed the percentage of the overall security to be higher.

B. *Study results from the inspected European web spaces*

The exploratory study with the Vulnet tool started in the middle of September 2019. The scanning of the

European web space provided a set of 23,131,336 websites, among which 3,738,654 with WordPress applications (16%) The websites belong to the following European countries: Germany (DE), Netherlands (NL), France (FR), Great Britain (GB), Italy (IT), Denmark (DK), Poland (PL), Spain (ES), Sweden (SE), Switzerland (CH), Czech Republic (CZ), Ireland (IE), Finland (FI), Austria (AT), Romania (RO), Belgium (BE), Hungary (HU), Bulgaria (BG), Norway (NO), Slovakia (SK), Estonia (EE), Slovenia (SI), Portugal (PT), Croatia (HR), Lithuania (LV), Luxembourg (LU), Greece (GR), Iceland (IS), Latvia (LT), and Cyprus (CY). The selection of these countries was based on the availability of data regarding the digital development provided from credible sources like the International Telecommunication Union (ITU) (ITU, 2019) and Eurostat (Eurostat, 2019). The number of WordPress sites that were vulnerable in the European sample of 3,738,654 WordPress websites was 1,339,325 and the number of websites without vulnerabilities was 1,187,085. The rest of the websites did not provide vulnerability information as the versions of the core and plug ins were hidden. A website was considered to be secure if no vulnerability was detected in the core and in the attached plug-ins. The percentage of insecure WordPress sites in a particular EU country ranged between 30 and 47 %, with the average of the whole set being 38%.

The macro-analysis of the collected data provided a good insight into how plug-ins and the web core state influence the overall state of a website's vulnerability. The correlation between the plug-ins vulnerability and the overall web site vulnerability was high (r = 0.91). So it concluded that the number of insecure websites primarily depends on the number of insecure plug-ins (at least one) in the web sites. All found insecure-core websites were critically unsafe, as their score was, for the majority, above 5 from maximum score of 10. Plug-ins overall insecurity is the greatest risk for a website to become insecure, similar conclusion was presented in the study presented by Vases & Moore [18] but on much less entries in their sample. The comparison of the level of digital development with the level of web insecurity among was intended to discover whether different parameters that measure the digital economy and social advancement provide an impact on the appearance of higher insecurity. Two indexes were considered Cost of the fixed access to Internet normalized with GNI data (Gross National Income) and the level of Digital skills among country population. Eurostat recognize three levels of DS: low, middle and high. Figure 3 shows the relationship between the percentage of secure and insecure websites in a particular country with indication of the DS levels. DS index higher than 75 is colored in green, orange is used for a DS index between 75 and 50, and the lowest DS country index being below 50 is colored blue.

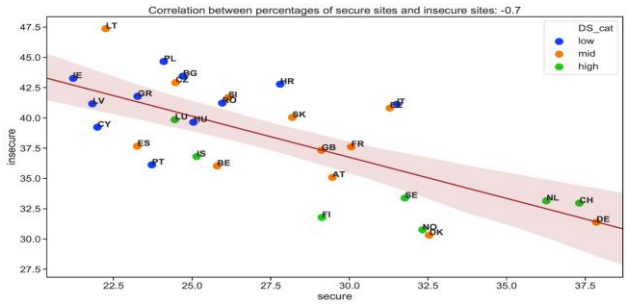


Figure 3. Percentage of secure and insecure sites in a country with different level of Digital skills.

The following countries: Finland, Sweden, Norway, the Netherlands, Denmark, Switzerland, Germany with high digital skills, have high percentage of secure websites and a low percentage of insecure websites are grouped in the bottom-right corner in Fig 3. They have high DS index as well. In the group of countries with low digital skills and a high percentage of insecure websites, the following countries are found: Lithuania, Poland, Bulgaria, Greece, Latvia, Portugal, Ireland, Czech, Romania, Slovenia, Croatia, Hungary and Cyprus. In the group of countries with a middle level of digital skills and a moderate percentage of insecure websites are Belgium, Austria, Slovakia, Great Britain, France, Austria, Iceland, Estonia, and Italy. The findings suggest that high DS contributes to the higher security of the country web space.

The correlation of the fixed-cost access to the Internet normalized with the country's GNI, as shown in Fig. 4, provides another insight into the influential factors affecting the presence of insecurity with the Cost of access to fixed Internet normalized with GNI (the Gross Income of a Country). At a lower fixed-access cost rate, the percentage of insecure websites is also the lowest, and the countries that belong to this group have the highest level or middle DS level, similar to the group in Fig 3. In this group, the following countries can be found: Denmark, Germany, Switzerland, Norway, Finland, Sweden, the Netherlands and Austria. The other group of countries with a much higher cost of fixed access have higher percentage of insecure websites. They are as follows: Hungary, Bulgaria, Italy, Croatia, Slovenia, Poland, Latvia, Romania, Czech Republic, Estonia, Italy, Iceland, Luxembourg and Belgium. They form the middle group. These findings are also in line with the linear dependency between the level of DS and the percentage of insecurity sites (r = -0.68) and imply that a low fixed-access price for the internet is a positive factor for higher security. Both factors have indirect influence on the awareness about the security provision in the web sites.

 ISBN: 978-1-61208-880-8

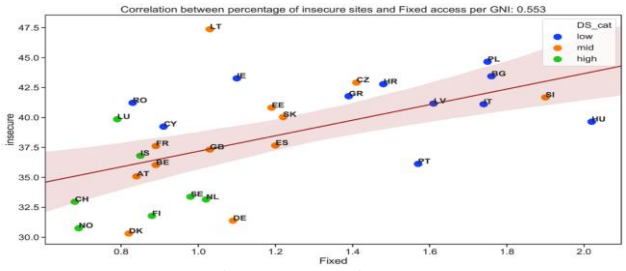


Figure 4. Impact of the Fixed cost for Internet access per GNI

The Vulnet tool was further reshaped as publicly available notification service for better management of the web site vulnerability. Developed platform is offered as a public service available to any individual web owner or web administrator for regular monitoring of the websites and discovering the vulnerabilities. By entering the website's URL and the owner's e-mail address on the platform portal, the platform sends information about this URL's inspection regarding the potential presence of vulnerability. The vulnerabilities of the website are revealed only to the owner on the platform screen or by notification with an e-mail.

V. CONCLUSION AND LIMITATIONS OF THE STUDY

The current known services and tools for measuring the WCMS vulnerabilities lack to provide real insight in the security of the websites operating with WordPress applications [18] as they usually provide only raw data, the address of the accessed server and the associated ports. The effectiveness of these known security tools is low as they do not provide information about the security holes within the web applications supported by the installed plug-ins. The presented tool and the study results show that known vulnerabilities and potential exploits can be found among the great part of the web space on the Internet. The advantage is in the applied scanning approach that allows a fast and reliable overview of almost all accessible web space and enables safe patch fingerprinting to be applied for improving the web security. Evidence that this is happening was notified in 2020 when the security of WordPress site installations rose sharply after the release of the new version of WordPress applications by the WordPress organization, that happen for a first time from 2007 year on. However, the approach and the tool have some limitations. The study was carried on websites with WCMS WordPress applications only. Although they represent the largest part of open-source WCMS installations in the whole web space, other systems like Joomla were not inspected. An additional limitation comes from the collected data sample for the further stud, with sites having in their URL the Top Level Domain of a particular EU country and accessible zone files. The presence of other websites in the country with TLD different from the TLD of that country were not collected as affiliation to the country population was not known. Despite that, the size of the obtained samples contained enough data for the carried exploratory analysis to be credible. The applied and improved scoring system for insecurity follows the approaches in other studies with added vulnerabilities of the plug-ins. Due to the ethical requirements of the applied web scanning, the search for vulnerabilities was limited only to websites with an accessible web core and a displayed core version, which can be considered as another limitation of the study. In case of hidden core version, data were not obtained.

ACKNOWLEDGEMENT

The support of the ARRS under contract P2-0037 is appreciated.

REFRENCES

[1] S. Karumanchi and A. C. Squicciarini, ‘‘A large scale study of Web service vulnerabilities,’’ J. Internet Service Inf. Secure, vol. 5, no. 1, pp. 53–69, 2015.

[2] The Hague Security Delta. (Oct. 2018). The Hague Security Delta. Accessed: May 2018. [Online]. Available: https://www.thehague securitydelta.com/news/newsitem/976

[3]W3Techs. Accessed: May 2019. [Online]. Available: https://w3techs.com

[4] M. Hassan, K. Sarker, S. Biswas, and H. Sharif, ‘‘Detection of wordpress content injection vulnerability,’’ 2017, arXiv:1711.02447. [Online]. Avail- able: https://arxiv.org/abs/1711.02447

[5] P. Laitinen, ‘‘Vulnerabilities in the wild: Detecting vulnerable Web applica- tions at scale,’’ M.S. thesis, Univ. Jyväskylä, Dept. Comput. Sci. Inf. Syst., Jyväskylä, Finland, 2018.

[6] H. Trunde and E. Weippl, ‘‘WordPress security: An analysis based on publicly available exploits,’’ in Proc. 17th Int. Conf. Inf. Integr. Web-Based Appl. Services, vol. 81, 2015, pp. 1–7

[7] Uniform Resource Location—Identification of the Web Site by Its Inter- net Address (IP). Accessed: May 2019. [Online]. Available: https://www. w3.org

[8] A. Tundis, W. Mazurczyk, and M. MÜhlhäuser, ‘‘A review of network vulnerabilities scanning tools: Types, capabilities and functioning,’’ in Proc. 13th Int. Conf. Availability, Rel. Secur., vol. 65, 2018, pp. 1–10

[9] Z. Durumeric, E. Wustrow, and A. J. Halderma, ‘‘ZMap: Fast Internet-wide scanning and its security applications,’’ presented at the 22nd USENIX Secur. Symp. (USENIX Secur.), 2013.

[10] NIST. National Vulnerability Database. Accessed: May 2019. [Online] Available: https://nvd.nist.gov

[11] T. V. Goethem, P. Chen, N. Nikiforakis, L. Desmet, and W. Joosen, ‘‘Large- scale security analysis of the Web: Challenges and findings,’’ in Proc. Int. Conf. Trust Trustworthy Comput. New York, NY, USA: Springer-Verlag, 2014, pp. 110–126.

[12] B. Stock, G. Pellegrino, F. Li, M. Backes, and C. Rossow, ‘‘Didn't you hear me?—Towards more successful Web vulnerability notifications,’’ in Proc. Netw. Distrib. Syst. Secur. (NDSS) Symp., 2018.

[13] M. Vasek, J. Wadleigh, and T. Moore, ‘‘Hacking is not random: A case- control study of Webserver-compromise risk,’’ IEEE Trans. Dependable Secure Comput., vol. 13, no. 2, pp. 206–219, Mar./Apr. 2015.

[14] N. Schagen, K. Koning, H. Bos, and C. Giuffrida, ‘‘Towards automated vulnerability scanning of network servers,’’ in Proc. 11th Eur. Workshop Syst. Secur., vol. 5, 2018, pp. 1–6

[15] A. Nappa, Z. M. Rafique, J. Caballero, and G. Gu, ‘‘CyberProbe: Towards Internet-scale active detection of malicious servers,’’ in Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS), 2014, pp. 1–15.

[16] H. Kim, T. Kim, and D. Jang, ‘‘An intelligent improvement of Internet- wide scan engine for fast discovery of vulnerable IoT devices,’’ Symmetry, vol. 10, no. 5, pp. 151–166, 2018.

 ISBN: 978-1-61208-880-8

[17] F. Li, Z. Durumeric, J. Czyz, M. Karami, D. McCoy, S. Savage, and V. Paxson, ‘‘You’ve got vulnerability: Exploring effective vulnerability notifications,’’ in Proc. 25th USENIX Secur. Symp. (USENIX Secur., 2016, pp. 1033–1050.

[18] M. Vasek and T. Moore, Identifying risk factors for webserver compromise, 18th International conference on financial cryptography and data security, Springer, LNCS, (V) 8437, 2014, pp.326-345