New IP: A Data Packet Framework to Evolve the Internet

Richard Li, Kiran Makhijani, Lijun Dong
Futurewei Technologies Inc.
2330 Central Expressway
Santa Clara, CA, U.S.A
{Richard.li, kiranm, lijun.dong}@futurewei.com

Invited Paper

***Abstract*— The IP is a primary data plane protocol on the Internet, which has several deficiencies when addressing the needs of modern digital society involving machine-to-machine communication and a remarkably enhanced user experience. New IP is an advanced network protocol specification to modernize the network layer without changing the fundamental Internet architecture. New IP envisions a new header format with 3 functional characteristics, i.e., shipping spec, contract spec, and payload spec. Using these fundamental blocks, New IP proposes a new data plane forwarding paradigm with far more advanced capabilities, such as ManyNets addressing, high precision services and qualitative communications.**

Keywords*— *Big Packet Protocol, BPP, High-Precision Communication, Contract, SLO, New IP, Internet, next-generation IP, contract-based, QoS, best effort, in-time guarantee, on-time guarantee, Qualitative Communication, ManyNets, flexible addressing

I. INTRODUCTION

The Internet Protocol (IP) is a fundamental building block of current data plane technologies in networks. Additional transport and routing protocols are developed with the assumption of having IP as the only network-level packet format. While the IP is well suited for traditional terminals and web-based applications, recent initiatives such as FG-NET-2030 [1], emerging industry verticals, and applications in 5G and Beyond 5G (B5G) have identified limitations with the current IP. Hence, a change is necessary for the data plane network technologies, since the applications attached to the terminals in many of the industry verticals (such as robotics-based automation, cloud-assisted driving) demand far greater data plane capabilities than what IP can offer. Several improvements in data plane are necessary [9] to support an entire set of functions related to data delivery, such as guarantees of arrival times and bandwidth, assurances of security and reliability.

Today's packet-switched networks have a minimal set of on-the-wire functions to support a diverse set of services. Efforts in programmability and service assurance are primarily fragmented and fail to facilitate the adoption of next-generation (5G, B5G) applications with stringent bounded latency and high throughput requirements. Secondly, we observe the foundational network infrastructure will be limited in handling the emergence of edge compute networks [2] and space internet [3], both requiring dynamic topology models. An argument can also be made for the various Internet of Things (IoT) device addressing schemes [4][5] that they do not fit in the current IP headers. Finally, the packet loss penalties in high data rate transmission lead to poor user experience. When the network is busy, alternate congestion responses become necessary to maintain a predictable throughput. While approaches like qualitative packets [6][7][8] can be utilized, the payloads need to have a relevant context to support selective transmission of smaller portions of the packet payload. A simple look at the IP packet format suggests that it is a mostly fixed structure; bringing changes to addresses, services, and payloads with flexibility is mostly impossible.

In this paper, we formalize a new data packet format called New Internet Protocol (New IP) to overcome the fixed structure of the packets. New IP captures three types of characteristics, each solving a specific class of problem in the networks stated above as follows: a) the **New IP Shipping Spec** is means of providing flexible and contextual addressing in heterogeneous networks and inter-networking systems; b) the **New IP Contract Spec** supports service-, and application- awareness. Contract allows for robust service delivery models and is a necessary step towards providing guarantees of Service Level Objectives (SLO) like latency, capacity, and reliability; c) The **New IP Payload Spec** specifies exciting capabilities through which entropy and quality of information is carried in the payload which are used to improve throughput and achieve robustness of data transmission.

The paper is structured as follows: Section II elaborates on the need for a new data packet format grounded in the fundamental limitations with the IP data plane technologies as well as a way forward to overcome those through postal services analogy. Section III introduces the New IP packet format and the details on addressing, contract, and payload specifications. We analyze this structure and its use in Section IV. The related and future work is covered in Section V and Section VI, respectively. Finally, Section VII summarizes our study.

II. MOTIVATION

The network layer or the IP is a universal network connectivity protocol for both large-scale and small-scale networks. Be it a private or public network, the TCP/IP stack has primarily been the communication protocol, including being the primary device addressing scheme used by a variety of end terminals. For networks to play a significant role in the next few years to support applications that are going to be either *time-engineered* or *Very Large Volumetric* (VLV) data transmissions.

978-1-7281-4846-5/20/$31.00 ©2020 IEEE

The FG NET-2030 in-network service capabilities [9] describes them as High-Precision Communications (HPC) and Holographic Type Communications (HTC), respectively. There is also a need to integrate better with upcoming connectivity paradigms based on public cloud internets, localization [10] [11], and space internets [3].

The question we try to answer in this paper is how we support time-engineered and high-throughput service requirements in the networks. It first requires a demonstration of limitations that are causes of concern and are discussed below.

A. Data plane Limitations

Since its start, the Internet datagram forwarding technology and its original packet format have evolved very little. Based on an end-to-end principle of control by application, a packet format besides the payload itself has an address (IPv4 or IPv6) for forwarding and some type of priority class mapped to a service. The policies necessary to forward the packets with Quality of Service (QoS) support are provided through the control plane. This type of simple packet format cannot capture the requirements of value-added services that started to emerge in the last two decades of Internet growth.

Forwarding path pipelines and router data plane designs are tightly coupled with the well-known fixed IP header format. We can generalize the data plane designs into three primary functions, viz. statistical multiplexing, best-effort paradigm, and an IP address-based reachability. In the following sections, we describe the fundamental shortcomings and gaps with these functions and means to overcome them.

Statistical to Computational Multiplexing: In packet-switched networks, statistical multiplexing helps to resolve schedule-conflicts among packets that arrive simultaneously from different input ports and are transmitted to the same output port in a network node. When enough buffers per port are available, packets eventually reach the destination, which works reasonably well for traditional applications. Statistical mechanisms schedule packets such that the entire flow, over a certain period, has a consistent rate with smooth variation as compared to a single packet in a flow. However, statistical approaches could schedule a latency-sensitive packet behind an ordinary packet on the same output port. For example, two packets A and B arrive at time t_n and $(t_n + 2)\, ms$ respectively, but B needs to depart at time t_m $(t_m > t_n)$ will likely get scheduled at a later time $(t_m + x)$ than A. Alternately, if latency-sensitive packet B arrives at the tail of an already built-up queue at an output port, it cannot depart before time t_m.

Our first premise to building New IP format is an ability to carry latency and bandwidth attributes to precisely support computational multiplexing approaches on the switches or routers. A computational multiplexing scheduler should be able to compute for a latency-sensitive packet B, the precise location in the buffers of an output port based on its time constraints. Computational scheduling takes into consideration of per-packet timing data at a finer granularity as compared to flow-level granularity. With computational multiplexing, simultaneously arriving packets on the same output ports are scheduled based on their respective latency budgets. Conflicts and delays are still possible, which could be resolved using sophisticated algorithms or at network level operations. This capability is possible when datagrams can create room to carry their latency budget because control plane methods are not designed to handle per packet requirements.

Best-Effort to High-Precision Services: Best-effort delivery model offers no guarantee of service delivery. When the communication endpoints are of machine-type, each piece of information must be delivered precisely; referred to as HPC services, their objectives such as latency, reliability, throughput, etc. may be defined at the granularity of a packet, a group of packets, or a flow. The best-effort network infrastructure could delay, buffer, or drop packet indiscriminately without considering those objectives. It makes no assumptions about the network capabilities, leading to our second premise for New IP proposal, that the means to bring new network capabilities are necessary for HPC services since they need a predictable performance. In order to support advanced services, networks should be able to distinguish different services in transit and give them suitable treatment.

OneNet to ManyNets: With the onset of multi-access edges, and satellite networks, most compute and storage will reside closer to the end-user, yet a part of the logic will be distributed in the cloud. These factors significantly offset the nature of what we have come to understand as the public Internet. Observations about shrinking transits [10] and maximal data residing in public clouds [11], have led us to believe that the public Internet of today will be just one of the ‘Internets’ as new public access Internets begin to emerge. We call this phenomenon as ‘ManyNets' and the current public Internet as 'OneNet’. Thus, ManyNets will be a group of Internets (network of networks) with their regulations, structure, and business objectives. OneNet will be one such Internet in this collection.

As this happens, we anticipate an emergence of different network structures and corresponding address schemes. For example, OneNet supports one type of address format end to end, be it IPv4 or IPv6. Additional tunnels or address translations are often necessary to cross network boundaries. At this time, IoT specific internets such as LoRA [4], and SigFox [5] have different addressing formats. With 5G and satellite internet, knowledge of location information, service- and mobility- awareness will be necessary to attach an end-user to the most reasonable service provider. This leads to our third premise for building the New IP that the extension of addressing formats different from the traditional IP is needed.

Packet Loss Probability to Linear Throughput: In dealing with VLV, a specific guarantee of throughput is necessary. Several factors, such as available bandwidth, round-trip time (RTT) variation, packet loss rate, can affect the throughput of a flow that is continuously contending with other flows in the network.

Linear throughput is computed based on available capacity and not on loss rate estimation. Modern networks could aim to achieve loss-independent throughput as in [12], which uses available bandwidth to compute throughput. Even better would be probe-free mechanisms to maintain loss-independent throughput, such as complete packet dropping avoidance, maintaining RTT, or providing in-band network feedback. This is our next rationale for creating New IP : to utilize in-network signaling and context-based qualitative payload [6][7][8] formats.

We believe, to overcome these limitations, a data plane approach is needed because providing objectives on a per-packet basis is not a control plane function, whereas the new datagram can carry what it needs the network to do. New IP is kept simple by refining the constructs already known to the IP community and emphasize backward compatibility to be a built-in feature.

B. *Courier Services Analogy*

The data transmission concept draws resemblance to the delivery logistics in postal or courier services, which is very well understood. By relating the user data or payload – to be the same as that of the contents of the letter, the payload is encapsulated into a packet – equivalent to an envelope; it carries the address information of the sender and receiver – *source, destination IP*. The letter is then delivered without any knowledge of the route or time taken by postal services. This is how the best-effort Internet service works today. Over the years, courier services added new ways in which packages and letters are delivered. They offer services such as deliver overnight (urgent and fast), by land or air (specific time-constrained path or transport), trackable (location and predicted delivery time), P.O. box (anonymity), delivery method (held off at office, delivery time reschedule), return receipt (proof of delivery), signature (acknowledgment by receivers) and so on. The merits of these services are to let customers do customization, monitoring, and control of the packages which they send.

While modern courier services have evolved, the IP data delivery model has remained unchanged. When it comes to using the network, an end-user desires a similar set of capabilities, as mentioned above, to have full control over his/her data in transit. To this end, there are no means to request either fast or exact delivery time, to receive proof of delivery with exact time (TCP acks are not time-aware), anonymity is hardly preserved because IP address identifies an end-user, and tracking root-cause of network faults is tedious when failures happen.

The current IP packet format is elementary and cannot evolve in terms of extensibility and flexibility of addresses, capturing end-user requests for a specific delivery requirement, and providing network-related context about the payload.

C. *Embedding Services in Data plane*

By relating to courier services, we observe that providing any type of service – be it old or new puts much responsibility on network operations. There is always an expectation from networks to insert new services seamlessly. However, the lack of flexibility in data plane often leads to an overlay-based approach or the middle-box insertion that needs to be maintained along with several provisioning touchpoints in the underlay networks, hence not only increasing the overall complexity but also limiting the scale. In order to provide these functionalities in the existing IP networks,

In order to provide these functionalities in the existing IP networks, addition to IPv4 options or IPv6 extension headers is necessary, both of which are very difficult to implement using the current standards.

III. New IP

New IP is a data plane technology that defines a new network datagram format, its specification, and corresponding capabilities in the network nodes. The New IP datagram format is shown in Fig. 1. Our New IP proposal includes 3 components, namely, a) addressing evolution, b) the contract inclusion, and c) the payload extension. In the figure, we also indicate the relationship of these new functions with the components in the New IP packet.

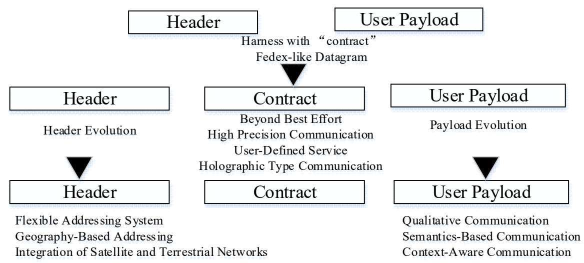

Fig. 1. New Internet Protocol (New IP) evolution

A. *Basic Structure and Function*

The essence of this paper is bringing forth an outline of the New IP datagram framework. We do not focus on a particular data structure or implementation-specific details. However, we use particular examples for the clarification of concepts that are not immediately obvious.

At the top-level, New IP Header is introduced that simply consists of 3 offsets as follows:

The *New IP Shipping* evolution is motivated by the fact that a fixed type of addressing does not fit all the reachability scenarios. New IP Shipping allows for different types and formats of addresses based on the functionality and network connecting those devices. The New IP shipping takes into consideration of the backward compatibility with the existing address schemes (e.g., IPv4 and IPv6).

The *New IP Contract* inclusion is all about the insertion of HPC and the life cycle of any type of service in the networks. It provides a piece of machinery to enable a variety of services, their operational and administrative control at the finest packet-level granularity. Contracts create avenues for the next level of programmability, customization, and non-monolithic data plane pipelines and also aim to be congenial to network operator's requirements to perform telemetry, elastically grow services on-demand and create new business models around HPC.

The *New IP Payload* associates network semantics to the user data while maintaining its (payload's) integrity. New IP payload does not dictate that the packet received by a remote end-user is unusable if it does not match bit-by-bit with the transmitted payload from the sender. Instead, it provides options to the receiver to consume partial information in payload. This partial-packet reception helps to mitigate re-transmission overheads and delays when faced with slow or congested conditions.

The New IP Packet can evolve and be deployed independently in parallel and/or sequentially. Let's say addressing enhancements are one of the most essential requirements in a particular network implementing New IP. Then the operator can only deploy and manage addressing features. Similarly, if the need for Beyond Best-Effort (BBE) service-aware infrastructure is more critical, then the contract specification will be the one that network operators will deploy. Later, as needs for payload enhancements become necessary, then Payload Specification will get incorporated in the networks. This structure is reflected in Fig. 2 and will become more apparent after we have explained the need and benefits of each specification in the New IP packet.

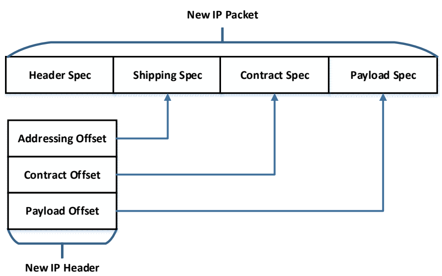

Fig. 2. New IP header

B. *New IP Header*

The New IP packet is a sequence of four specifications. Header spec is the start of the packet, merely describing the offsets to specifications for shipping, contract, and payload sections, respectively. The New IP header is shown in Fig. 2. Only the required fields are described along with their purposes.

1) `Shipping Pointer` (Addressing Offset) specifies the offset and length of the Shipping Spec.
2) `Contract Pointer` (Contract Offset) specifies where the Contract Spec starts.
3) `Payload Pointer` (Payload Offset) specifies the offset and length of the Payload Spec.

The details of each specification are as follows.

C. *Shipping Specification*

Shipping Specification (SH-Spec for short) is a mandatory section of the New IP packet. It incorporates the following key features: (a) flexible address format scheme, (b) backward compatible, and (c) hybrid addressing. The SH-Spec can support existing addressing schemes at the minimum and provide both flexible and hybrid address formats. Basically, described in Fig. 3, the addressing offset points to the SH-Spec structure for supporting new or hybrid addressing schemes.

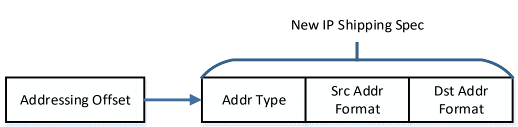

Fig. 3. Shipping Spec (SH)

1) *SH-Spec Description*

The Shipping spec allows a flexible addressing scheme in which different types of address namespaces can be embedded. For example, the New IP can carry with SigFox, LoRA, legacy addresses, and even new semantic formats like service identifiers, location identifiers, variable-length identifiers. With flexible addressing, the size of the address identifier is not fixed, i.e., for low power, low memory devices, smaller lengths can be chosen.

Shipping spec seamlessly enables backward compatibility with legacy IP/MPLS or other well-known packet type support only by use of address type field. It is not necessary to install translation when transiting from IP/MPLS to New IP networks. This direct method to carry legacy packets, makes forward migration path simpler and does not require to change end-user applications that work just as well with the legacy IP/MPLS stacks.

Additionally, Shipping Spec supports a hybrid model in which asymmetric addresses are permitted. It means that the source and destination addresses can be of different formats (for example, the source is IPv4 and the destination is MPLS). With this capability, traffic from one provider addressing scheme are forwarded to another provider's network without any need for an end-to-end tunnel to homogenize the address space.

2) *SH-Spec Structure*

The New IP SH-Spec structure includes at least the following fields. Fig. 4 (a) shows the overall New IP shipping spec which comprises of the following:

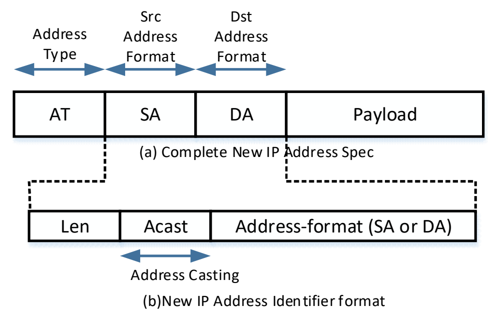

Fig. 4. Addr-cast and Addr-type fields of SH-Spec

- `AddrType (AT)`: is similar to an indication of address family or mnemonics for different address format types. It is a placeholder for a combination of address types for destination and source addresses. Future requirements may add new code types, such as geo-location-address formats are currently expected to have location awareness for reachability in broadband satellite networks (Fig. 4 (a)).
- `Addr-cast (Acast)` identifies the nature of communications one-to-one, many-to-one, anycast, broadcast, multicast, coordinated-casting, and so forth, as in Fig. 4 (b). The address casting is determined at the address format, i.e., separately for source and destination addresses, which is useful in facilitating forwarding functions. While most communication forms are well-known, the coordinated cast is the identification of coflows in another time-engineered service called coordinated service [19]; means of synchronizing subject information, for example, synchronizing a virtual orchestra when all the artists are remote at separate locations and with a different set of network conditions.

- Source/Destination address format provides at minimum the length (Len) and optionally, any other information specific to address format. SA and DA contain the source address and destination address. Source and destination formats can belong to different address spaces and have identifiers of that space (Fig. 4 (b)). Len is the size of the address format. Address formats can be flat or nested, variable length, geometry-based (longitude, latitude), or service-specific.

D. Contract specification

A contract describes a formal service specification of a service, which includes clauses to describe the type of network service capability, actions, and accounting information. A contract can be understood as a service-specific arrangement between two or more parties. Those parties include an application and network, or inter-network ISPs, application, and end-user.

1) Contract Description

The contract specification harnesses an essential functionality in the New IP, dealing with everything related to the services in the networks. The body of the contract makes it possible to express different capabilities that were mentioned in the postal services analogy and translate them into a declarative format that network nodes can parse and process. Through contracts, service assurance requirements at a packet level are provided. Contracts carry specific attributes associated with time-engineered services, high-throughput media services, and mission-critical ultra-reliable services.

The term contract is motivated in 2 parts, a) as a kind of service manifesto, to describe what its objectives are and not necessarily how they are met, and b) a symbolic agreement between two or more parties with any combination of networks, applications, and end-users. Contracts expect service assurances, can also provide instructions for monitoring. In comparison to traditional QoS, contracts operate at much lower-level – per packet, and instruct in high-level abstract commands.

2) Contract Structure

The structure of the contract is defined in Fig. 5 in a Chomsky style. The non-terminals are Contract, Contract-Clause, and Contract-ECA. The terminals are Event, Condition, and Actions. A $Contract$ is a non-terminal symbol and can have one or more $contract\ clauses$ representing different objectives. Each contract clause is then a statement described using $Contract\ ECA$: $Event$, $Condition$, and an $Action$ (ECA) of the clause. Contract-ECA could optionally include the Metadata associated with the parties involved in the Contract. An atomic contract ECA is the one where Event and Conditions can be empty.

A contract can be composed of one or more clauses. For example, in order to support Ultra-Reliable Low Latency (uRLLC) in 5G, two contracts $C1$ and $C2$ can be used. $C1$ contract clause indicates the $BoundedLatency$ action, and clause $C2$ has action $NoPktLoss$ i.e., the low latency and reliability are to be met. Those actions will be explained in Section 3).

```
<Contract> := <Contract clause>
        | <Contract clause> AND <Contract>

<Contract clause> := <Contract ECA>
        | <Contract ECA> OR <Contract clause>

<Contract ECA> := <Event, Condition, Action>
        | <Metadata>
        | <Event, Condition, Action> <Metadata>
        | <Action>
        | <Action><Metadata>
```

Fig. 5. New IP contract

3) Contract clause – Action

A sample of actions that we find relevant to meet the HPC type of services is discussed below and shown in Fig. 6.

```
<Action> := <BoundedLatency>
        | <OnTimeDelivery> | <Coordinate>
        | <NoPktLoss> | <PktMonitor>
        | <ReportInsuringParty>
        | […]
```

Fig. 6. New IP actions

An action set shall be a well-known set as per the specification, i.e., known and processed by all New IP nodes. The general idea is that applications will insert operator-defined or application-defined new actions or both. Furthermore, Actions may be categorized into operations, monitoring, telemetry, or signaling, but we do not think explicit classification in syntax is necessary. New IP Contracts assume that the implementation of actions could vary across different hardware platforms; they may use different methods or algorithms. However, the result of those must lead to packet delivery guarantees between the sender and the receiver. Several actions are described below:

- Action $BoundedLatency(t)$ instructs the router to deliver a packet any time before the t (with prescribed unit of time). It may use corresponding metadata to describe an end-to-end network latency or available latency since transmission starts from the sender. An algorithm called latency-based forwarding (LBF) [18] implements this action. Instead of a class of services, contract clauses embed exact parameters and objectives in the packet.

- Action $OnTimeDelivery(t, t')$ with metadata t and t' as a total end-to-end time and elapsed time respectively delivers packet at a specific time in order to accommodate very low values of time-jitter.

- Action $Coordinate$ enables multi-user applications to adjust packet delivery timings in the network. The action needs to identify co-flows, which is actually done from address casting part of the Shipping Spec along with timing dependency parameters as specified in metadata [19].

- Action $NoPacketLoss$ instructs networks to make possible by every means to deliver the packet.

- Action $PreferredPath$ may be a set of node addresses or other forms of path identifiers embedded in the packet to provide path guarantees.

- Action $PktTrace$ tracks the packet flow behavior across the network and may be used to understand the end-to-end service assurance and performance degradations in particular. Such actions add noise and, therefore, are subjected to specific events or conditions of interest. For example, in order to understand hop-by-hop latency, $PktTrace$ action may capture a path in the network along with the time spent in each node.

- Action $PktMonitor$ helps gain visibility into the current state of the system. This action captures events in a network relating to queue thresholds, packet drops, etc. Such actions identify situations such as congestion before they occur by monitoring the thresholds. For example, in order to identify real-time congestion, if a queue is built up to 70%, then this action sets the corresponding metric value in the metadata.

- Action $ReportInsuringParty$ is an operator driven action to be executed when a service objective violation occurs; the node in error is then required to report such violations to the insuring party. Operators use this for the assessment of damages due to service level objectives violations, which may help build trust between different network systems.

4) Contract Clause - Event and Condition

For the efficiency of the packet processing pipeline, a contract clause can specify when an Action is executed. Some of the events identified in Fig. 7. are self-explanatory. Conditions are arithmetic or logical operators to perform conditional checks. For example, Fig. 7. shows Less Than or Equal (LE) and Greater Than or Equal (GE), that may be used to check against thresholds or data rates. Several other logical operators such as OR, XOR, AND may also be used to derive the results from events and actions. Events are local occurrences or state of a network node that can impact the behavior of a packet or flow in transit. Events such as queue levels, path change, drops determine congestions or faults while others may be operands such as PktCount, NextHop that meet a specific value.

```
<Event> := [<Queue Levels> | <Path Outage>
        | <Pkt Late> | <Pkt Drop>
        | <NextHop> | <Pkt Count>
        | ⋯ | <none>]

<Condition> := [<equals> | <LE> | <GE>
              | ⋯ | <none>]
```

Fig. 7. Contract Clause - Event and Conditions

5) Contract Clause - Metadata

Metadata is a set of parameters that are associated with the actions or applications. The structure and positioning of metadata are an implementation decision.

E. Payload Specification

The New IP payload evolution allows a payload to carry additional context without exposing the private information of the transmitted data. This New IP payload can be a traditional payload (when type is set to 0), a sequence of bits/bytes, or when the type is set to 1, it may be a *qualitative payload* that carries *quality, entropy* or *semantics* of the payload. Such payloads are subjected to qualitative communication service [6] processing when corresponding events happen. The context determines how significant a particular piece of information within the payload is. As an example, a media frame can be arranged in such a manner that the initial part of the payload is the most significant frame, the middle and last part enhance the resolution of this frame.

A conceptual new IP packet wash operation is shown in Fig. 8., by using contract clause 'Wash' action. The action $Wash$ will be applied when an event corresponding to congestion notification takes place (such as high, medium or low queue occupancy) on that node. Then chunk starting from offset Ch2 till the end with low priority P2 will be dropped so that that remaining payload can be forwarded.

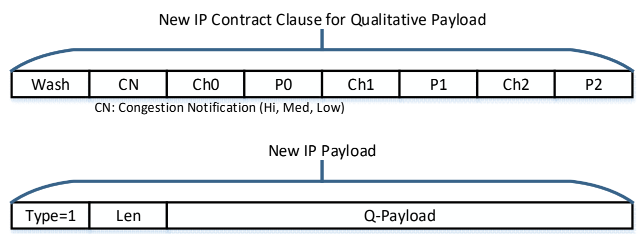

Fig. 8. Contract Clause - Wash for New IP Payload

Using this clause during high congestion just by sending the first part of the payload can make timely communication to take place without loss of important information. The context could identify these parts as chunks. Such capabilities enhance network throughput and utilization. One implementation of qualitative communications is discussed in [6]. Furthermore, New IP Contract can be utilized to carry the context of a qualitative packet. In the contract clause for the qualitative packets, the following Actions may be defined:

- `Wash`: a generic operation to arbitrarily or selectively remove the bits/bytes inside the packet payload. For example, remove every 8th bit, remove every fifth byte, etc.

- `Repair` and `Recover`: can fix the error bits/bytes in or salvage lost portions from the residual the packet payload based on context present along with the action.

- `Enrich`: The packet payload may be inserted by the New IP node with locally cached chunks that match to the packet when the network condition becomes better to pass through the larger packet.

Proposals realizing qualitative communications by applying random linear network coding are proposed in [7] [8]. In those proposals, the payload could be divided into multiple equal-sized chunks and applied with random linear network coding, such that the significance of each chunk does not differ. When qualitative processing is needed to the packet, the network node could initialize a random drop or drop from the tail as many as needed until the packet can be retained in the forwarding buffer.

IV. New IP Advantages and Analysis

Section II, described the ossified nature of the current IP is primarily due to the strict structure of IP datagram. In contrast, New IP unlocks opportunities to innovate across several dimensions as follows:

A. ManyNets Addressing

The Internet is IP-based and connects devices and networks in a homogenous way. ManyNets is a combination of all kinds of network types, devices types, and infrastructure types. The new address format not only accommodates new addressing structures mainly involving IoT type devices [4], [5], but also the need for geographic address structures for the networks involving satellites. In space- networks, Low-Earth Orbit (LEO) satellites become part of the forwarding path between the endpoints, and the location of the routers themselves is changing, unlike the case of terrestrial networks with stationary routers. Using IP addresses is not sufficient from an end point's (or an adjacent network node's) perspective since it has to attach to the nearest satellite.

B. Time-Engineered Services

New applications in both 5G and Network 2030, such as factory automation, remote operations, autonomous vehicles, or self-managing systems, are highly dependent on the precision of arrival and departure times of data over the networks because those applications are machine-based. New IP provides common a framework through which each application can individually describe its' precise requirements. This has not been possible so far with packet-based networks. By using high-precision (or time-engineered) services, every packet arrives at the destination within or at its specified time. New IP enables contract clauses on per-packet basis to provide the capability of on-time, in-time guarantee or lossless type of packet delivery.

The most important dimension in 5G services is defined to be uRLLC. When 5G new radio stack evolved, it was only possible to support uRLLC between a 5G device and the base stations. With New IP, 5G mobile backhauls can support reliability and low latency over fixed packet networks as well. In the previous section, we showed how contract specifications could convey attributes related to low-latency and reliability.

C. Service Accountability

The new IP contract framework does not just provide high precision guarantees, but clauses can be inserted for the accountability of both new and traditional services. Service accountability refers to the determination of the cause of actions and the node when service guarantees are not met, or other policy violations occur.

The network is a heterogeneous and non-deterministic system; ever so often, congestion, outages, or different attack vectors impact the service level guarantees. It is essential to monitor and notify such violations to network operators to take corresponding actions. A new IP contract mechanism allows capturing violations in per-packet, per-flow basis, which is especially useful in M2M latency-sensitive communications systems because a sending sensor does not necessarily expect or wait for the acknowledgment at the transport layer. Then the network has to deliver the commands reliably, and in case of any violations, it should also be able to determine paths or nodes that caused violations.

D. Standalone Packets

The Shipping Spec specifies that when the addressing type is reserved, and the packet itself is considered as a standalone packet of that type. For example, If the "Addr Type" are reserved values of IP version 4, IP version 6, or MPLS, then these are self-contained IPv4, IPv6 or MPLS packet, respectively. A standalone packet means New IP is carrying legacy packet format.

E. Security and Privacy

The discussion on security is twofold. First, do contract spec, shipping spec, and payload spec give more information about the services or flows that make them easier to security attacks? We agree that new authentication mechanisms need to be devised to accept a contract and qualitative payload processing.

However, we observe two advantages of New IP packet format. First, that whenever there is an unexpected change in the packet flow behavior, such as contract or payload getting modified, these anomalies can be recorded on a per-flow basis. Secondly, by not having a fixed structure in new IP addressing spec, an end-user application could encrypt or anonymize the internal identifiers and not expose them to external networks. Admittedly, these are initial ideas and the topic of security needs an in-depth study and is left as a topic for research in the New IP framework.

V. Related Work

On-going research in data plane enhancements is fragmented in their effort, such as those for programmability P4 [13], DPDK [14], etc. are being developed, but they focus on customizing pipelines around current data packet formats. These can serve as an excellent toolset for developing a user interface to New IP specific packet processing pipelines going forward. New IP is an extension of principles of the Internet and IP. The initiatives in future architectures like MobilityFirst [15], NDN [16] only capable of capturing similar capabilities through Shipping and Contract specifications, but also supports uRLLC and HPC as first-order services within the same framework.

In a more relevant work, before New IP specification, Big Packet Protocol (BPP) [17] was developed to provide many of the contract clause functionality. However, the BPP block design is based on the relatively lower level of instructions. In comparison, New IP can be seen to vary in two ways:1) it is a higher-level purpose-built action that is more declarative in syntax, 2) New IP has further flexible addressing enhancements that were not considered in BPP. In another work, relating to qualitative communications [6] describes fundamentals of

`Trim` and `Wash` actions, whereas [7][8] applies random linear network coding to support additional `Enrich, Repair, and Recover` [22] actions.

VI. Future Work

Indeed, future packet processing pipelines will need to support New IP capabilities, perform flexible address lookups, contract processing, and sufficient capabilities to collect micro-level telemetry data about the packets. Support for HPC (or computational multiplexing) can come from utilizing existing methods through cross-layering techniques [20] or by implementing new algorithms [18]. Of course, with new packet format forwarding functions are impacted as routers need to understand New IP format. In the New IP routing system, asymmetric addresses are permitted. For example, while looking up for a destination address with an MPLS label, it is possible to get next hop as an IPv6 address, if the adjoining network uses IPv6. Asymmetric address lookups require building hybrid Forwarding Information Base (FIB). Such hybrid FIB data structures eliminate Network Address Translation (NAT) and overlay schemes.

A study to handle flexible addresses and corresponding new reachability algorithms, such as those relying on geo-location, is required. We have yet to resolve challenges relating to the trust and integrity of contracts. As the first steps, we expect to provision what contracts are applicable through controller or orchestration.

New IP supports user-defined routing, and it does not suggest the stacking of segment identifiers in the *Shipping Spec* (even though it is possible). Instead, it relies on Preferred path routing (PPR) [21]. Actually, PPR can either be one type of address or can be implemented in a contract. Further study of the control plane and routing functionality is left as future work.

VII. Conclusions

We argued that New IP has potential benefits towards the evolution of IP based data plane approach: first and foremost, being fully backward compatible, it is less susceptible to adoption impetus that clean slate technologies have to deal with. Drawing the postal services analogy, per-packet processing, awareness about the assurance of services is the way forward.

Several exciting research opportunities open up with New IP, such as the design of new packet processing pipelines with capabilities to process contracts in parallel, hybrid and trustworthy routing protocols with the inclusion of hybrid address structures. More research is needed to capture the privacy and trust aspects of contracts and addressing specifications. We did not discuss them here because they are independent topics by themselves requiring in-depth discussion.

References

[1] FG-NET-2030, “Network 2030 - A Blueprint of Technology, Applications and Market Drivers Towards the Year 2030 and Beyond,” May 2019.

[2] S. Maheshwari, D. Raychaudhuri, I. Seskar, and F. Bronzino, “Scalability and performance evaluation of edge cloud systems for latency constrained applications,” in 2018 IEEE/ACM Symposium on Edge Computing (SEC), pp. 286–299, Feb 2018.

[3] M. Handley, “Delay is not an option: Low latency routing in space,” In ACM HopNet, 2018.

[4] N. Sornin, M. Luis, T. Eirich, T. Kramp, O.Hersent, “LoRaWAN™ Specification,” Oct 2016.

[5] librenard - Sigfox Protocol Library, Oct 2016.

[6] R. Li, K. Makhijani, H. Yousefi, C. Westphal, L. Dong, T. Wauters, and F. De Turck, “A Framework For Qualitative Communications Using Big Packet Protocol,” in Sigcomm workshop NEAT, 2019.

[7] L. Dong, R. Li, “In-Packet Network Coding for Effective Packet Wash and Packet Enrichment,” 2019 IEEE Globecom Workshop on Future Internet Architecture, Technologies and Services for 2030 and Beyond.

[8] L. Dong, K. Makhijani, R. Li, “Qualitative Communication Via Network Coding and New IP,” IEEE HPSR 2020.

[9] FG-NET-2030, “New Services and Capabilities for Network 2030: Description, Technical Gap and Performance Target Analysis,” 2019.

[10] G. Huston, “The Death of Transit? - The ISP Column,” Oct. 2017.

[11] M. Ammar, “Ex Uno Pluria: The Service-Infrastructure Cycle, Ossification, and the Fragmentation of the Internet,” SIGCOMM Comput. Commun. Rev., vol. 48, p. 56–63, Apr. 2018.

[12] J. Hwang and C. Yoo, “Formula-based tcp throughput prediction with available bandwidth,” IEEE Communications Letters, vol. 14, pp. 363–365, April 2010.

[13] The P4 Language Consortium, “P4 Language Specification, version 1.2.0.” ”https://p4.org/p4-spec/docs/P4-16-v1.2.0.html”, Oct. 2019.

[14] DPDK, “Intel data plane development kit (intel dpdk),” 2019.

[15] D. Raychaudhuri, K. Nagaraja, and A. Venkataramani, “MobilityFirst: A Robust And Trustworthy Mobility-Centric Architecture For The Future Internet,” SIGMOBILE, vol. 16, no. 3, pp. 2–13.

[16] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, “Networking named content,” Proc. of CoNEXT, 2009.

[17] R. Li, A. Clemm, U. Chunduri, L. Dong, and K. Makhijani, “A New Framework And Protocol For Future Networking Applications,” ACM Sigcomm Workshop on Networking for Emerging Applications and Technologies (NEAT 2018), pp. 637–648, May 2018.

[18] A. Clemm, T. Eckert, “High-Precision Latency Forwarding over Packet-Programmable Networks,” IEEE/IFIP Network Operations and Management Symposium, 2020.

[19] K. Makhijani, H. Yousefi, K. K. Ramakrishnan and R. Li, "Extended Abstract: Coordinated Communications for Next-Generation Networks," 2019 IEEE 27th International Conference on Network Protocols (ICNP), 2019.

[20] K. Makhijani, R. Li, and H. El Boukary, “Using Big Packet Protocol Framework to Support Low Latency based Large Scale Networks,”, The Fifteenth International Conference on Networking and Services (ICNS), June 2019.

[21] U. Chunduri et al., “Preferred path routing – A next-generation routing framework beyond segment routing,” Globalcom 2018.

[22] C. Fragouli, J.Y. L. Boudec, J. Widmer, “Network coding: an instant primer,” ACM SIGCOMM Computer Communication Review, vol. 36 no. 1, pp. 63-68, January 2006.