3GPP CT1 5G Standardization

Christian Herrero-Veron, Principal Research Engineer, Huawei Technologies Sweden AB, 3GPP CT1 Rapporteur of the 5GS Phase 1 Work

3GPP TSG CT WG1 (CT1)[1] is the 3GPP core-network and terminal working group responsible for specifying terminal (user equipment) interfaces, terminal capabilities and core-network aspects. Specifically, the user equipment (UE) and core-network layer 3 or non-access stratum (NAS) protocols used for mobility management, session management, and also session initiation protocol (SIP) call control and session description protocols for IP multimedia subsystem (IMS). 3GPP CT1 also defines cellular vehicle-to-everything (V2X) connectivity and Cellular Internet-of-Things (CIoT) and multi-mode terminals aspects. 3GPP CT1 further specifies network selection, interoperability between 3GPP networks (e.g., universal terrestrial radio access network (UTRAN), evolved UTRAN (E-UTRAN), new generation radio access network (NG-RAN) and also to external networks (wireless local area network (WLAN), non-IMS SIP, public-switched telephone network (PSTN), public warning systems, support for different services such as emergency, mission critical, control-plane location, multimedia priority and proximity-based services.

5GS Phase 1 Work

In March 2017, 3GPP CT1 started work on 5G to study and later specify in the 3GPP release 15 the core-network and terminal protocol aspects of the 5G system (5GS) work based on the requirements, architecture, security and the new radio access (5G new radio (NR)) developed by other 3GPP working groups. The main aspects of the work were network selection, security management, mobility including legacy architecture (evolved packet core (EPC)), control-plane protocols, network slicing, quality-of-service (QoS) and policy control and charging aspects. The 5GS includes connectivity via both 3GPP accesses and untrusted non-3GPP access (WLAN).

Milestones

The work had a target timeline of providing the 5GS study by December 2017 and the specification work by June 2018. In December 2017, 3GPP CT1 successfully provided the study phase (TR 24.890[2]; technical report of CT WG1 aspects of 5G system phase 1). The work and analysis developed during the study phase was used as the basis for the specification work that was delivered in June 2018.

5GS Standardization Work

Compared to previous 3GPP systems, the 5GS is defined as service based. The architecture elements are defined as network functions (NFs) that offer their services via interfaces of a common framework to any consumers that are permitted to make use of these provided services. The 5G core network is designed based on separation of the control plane and user plane. The services are defined for the control plane in the 3GPP release 15. The system is defined with a separate access and mobility function (AMF) and session management function (SMF), to provide flexible and modular access control, mobility and session management.

3GPP CT1 has created several new technical specifications (TS) for the 5GS (TSs 24.501[3], 24.502[4], 24.526[5]) and updated many existing ones. The group worked on a large number of functions or features. As per legacy systems, for data connectivity services there is support of various packet data session types including IPv4, IPv6, IPv4v6, Ethernet and unstructured. The system provides traditional session and service continuity mode (SSC mode 1), where the IP anchor remains unchanged to provide IP address preservation and service continuity. The system also introduces new models such as SSC mode 3 (make-before-break) that achieves fast mobility and minimizes user experience impact.

Support of a flow-based QoS framework is added, including new reflective QoS which provides symmetric QoS differentiation over downlink and uplink is supported with minimal control-plane signalling QoS.

3GPP CT1 has integrated untrusted non-3GPP access networks so that NAS signalling is now possible via non-3GPP access using common procedures also defined for 3GPP access. Simultaneous registration over 3GPP and non-3GPP access is supported. New authentication methods for non-3GPP access networks are added. All this opens up new business opportunities.

3GPP CT1 has also defined interworking with E-UTRAN connected to the EPC (with or without a signalling reference point between the EPC and the 5G core network) which will play an important role in the early deployment of 5G which relies on 4G to be the anchor or underlying system.

Short message service (SMS) in the 5GS is supported by SMS over NAS (including over E-UTRA, NR and non-3GPP access) and using new service-based interfaces.

A distinct feature of the 5GS is network slicing, which includes support of logically isolated network slices across all the public land mobile network (PLMN). The operator can decide based on business scenario how many network slices to deploy and also what features are shared across multiple slices. Slices are standardized and enable inter-PLMN operation with reduced coordination effort between operators. Further, there are operator-defined slices enabling more differentiation among network slices with the same slice. UEs may use multiple network slices simultaneously, including network slice selection policies in the UE linking applications to network slices. Network slicing interworking with legacy evolved packet system (EPS) is supported.

The UE to core-network protocol for IMS has been enhanced by 3GPP CT1 so that IMS services (including support of existing IMS emergency services over 3GPP and non-3GPP access) are supported by adding support for voice and for network handover based radio access fallback and EPS fallback when IMS services are not supported natively in 5GS.

3GPP CT1 has developed support for customized mobility management such as mobile initiated connection only (MICO), and support for RAN enhancements like RRC inactive state.

Unified access control is provided by 3GPP CT1 together with support in RAN, which allows for categorizing each access attempt into one access category. The network can restrict UE access on a per-access category basis.

Additionally, 3GPP CT1 is providing steering of roaming of UEs in a visited network which allows the home network operator to provide and update a list of preferred PLMN/access technology combinations to the UE when roaming in a VPLMN.

There is also support for location-based services, which is optional and restricted to regulatory (emergency) services in the 3GPP release 15.

The 5GS supports the multi-operator core network (MOCN) style of network sharing architecture, in which the RAN is shared by multiple core networks.

The public warning system has been enhanced by 3GPP CT1 so that it is supported in the 5GS by either using new service-based interfaces between the cell broadcast centre function (CBCF) and the AMF or using an interworking function between the cell broadcast centre (CBC) and the AMF (for interconnection with legacy warning deployments).

Mission critical services are supported by having a subscription in place for both 5G QoS profile and the necessary policies. Some standardized QoS characteristics are defined for these services.

Multimedia priority services are also supported by adding specific exemptions for mobility management and session management.

3GPP CT1 provides congestion and overload control in the 5GS by NAS-level mobility management congestion control, DNN (data network name) based congestion control and S-NSSAI (single network slice selection assistance information) based congestion control.

Moving Forward

In just sixteen months the 5G work in 3GPP CT1 progressed from the study period of 2017 to the delivery of a complete set of Stage 3 level specifications and important Stage 2 specifications in June 2018. 3GPP CT1 has now specified the 5GS Phase 1, but the group continues consolidating the first version of the specifications and starting planning the 5GS Phase 2 work within the 3GPP release 16 with targeted completion by December 2019.

References

1 http://www.3gpp.org/specfications-groups/ct-plenary/36-ct1-mm-cc-sm-lu
2 http://portal.3gpp.org/desktopmodules/Specifications/SpecfificationsDetails.aspx?specificationId=3172
3 http://portal.3gpp.org/desktopmodules/Specifications/SpecfificationsDetails.aspx?specificationId=3370
4 http://portal.3gpp.org/desktopmodules/Specifications/SpecfificationsDetails.aspx?specificationId=3371
5 http://portal.3gpp.org/desktopmodules/Specifications/SpecfificationsDetails.aspx?specificationId=3472

Status of the 3GPP Study on 5G Message Service for MIoT

Jianping Zheng, China Mobile, Rapporteur of the 3GPP FS_5GMSG

The 3GPP Release 16 study item FS_5GMSG was created in August 2017 to develop use cases and potential requirements of 5G message service for Massive IoT (MIoT) communications, including thing-to-thing communications and person-to-thing communications.

Massive Internet of Things (MIoT) is one of the key market segments of 5G. The typical IoT device communication is sending and receiving small data that can be delivered just in a message. Although an IoT application may implement its own message enabler or data communication enabler, it will introduce problems such as interoperability, signalling overhead, etc. For the benefit of the IoT ecosystem, it is expected that mobile network operators (MNOs) provide message service for MIoT.

Today MNOs provide SMS service for IoT applications. However SMS has limitations in terms of service capabilities (e.g. 140 bytes payload) and performance (e.g. long latency); in addition, the overhead of the control plane resource is high. There have been enhancements and optimizations on 3GPP network capabilities to facilitate IoT applications, including device triggering, small data transfer, Non IP Data Delivery (NIDD), and group messaging etc. Nevertheless, MIoT will bring various new demands on message communication, e.g. lightweight message communication for provision and monitoring, ultra low delay and high reliability message communication for remote control, and extremely high resource efficiency for large-scale connections. To address this new and huge market segment, 3GPP is going to innovate MNOs' message service and improve 3GPP network capabilities.

As the prologue of standardization work of the 5G message service in 3GPP, the study item FS_5GMSG has developed a number of use cases of message communication for MIoT, including efficient lightweight message communication, low delay message communication, group message communication, multicast and broadcast message communication for both thing-to-thing and person-to-thing communications, which are documented in 3GPP Technical Report 22.824. Based on the use cases, the potential service level requirements of 5G message service, and the associated potential new requirements on the 5G system, are identified.

In August 2018, 3GPP finished the study work and created a followed-up Release 16 work item 5GMSG. This work item, as Stage 1 work in 3GPP, is to specify the service level requirements of 5G message service, and is expected to be completed by the end of 2018. The corresponding Stage2/3 work will be continued after that.

3GPP SA1 Standardization: 5G Requirements for Communication for Automation in Vertical Domains

Joachim W. Walewski, Siemens AG, Rapporteur for 3GPP's FS_CAV and 3GPP's Work Item cyberCAV; Michael Bahr, Siemens AG, Rapporteur for 3GPP's Work Item cyberCAV

The 3rd Generation Partnership Project (3GPP) is currently standardizing the fifth generation of mobile networks (5G). The first 5G release, i.e. Release 15, focused on enhanced massive broadband networks, while one of the focus areas of the ongoing Release 16 is the support of demanding vertical applications, e.g. the coordination of robots and the control of electric power distribution.

In this context, 3GPP working group SA1, which is responsible for the standardization of service requirements, launched a study on communication for automation in vertical domains (FS_CAV) in May 2017. This wide-ranging study covered verticals such as factories of the future, electric power distribution and generation, wind power plants, and smart agriculture, among others. Pertinent use cases and background information can be found in the related technical report TR 22.804. Version 16.0.0 of this report was approved in June 2018. Two other studies also touched on automation in vertical domains: FS_5GLAN (Feasibility Study on LAN Support in 5G), which produced TR 22.821; and FS_BMNS (Feasibility Study on Business Role Models for Network Slicing), which produced TR 22.830.

All three studies are concluded, and three related work items were launched in the meanwhile: cyberCAV, QoS_MON, and BRMNS.

cyberCAV, service requirements for cyber-physical control applications in vertical domains, addresses the formulation of normative requirements for the support of cyber-physical control applications. Cyber-physical systems include engineered, interacting networks of physical and computational components; control applications are applications that control physical processes. An example for a cyber-physical control application is the motion control of a mobile robot. This work item leverages TR 22.804 and TR 22.821.

QoS_MON–QoS Monitoring addresses requirements for QoS monitoring of the 5G network by the user, in this context the vertical as a 3rd party. Verticals may deploy 5G networks as so called non-public networks that are under discussion in cyberCAV.

BRMNS–Business Role Models for Network Slicing addresses enhanced network slice requirements based on the business role models identified in TR 22.830.

All three work items formulated new normative requirements for the existing specification TS 22.261 (service requirements for the 5G system). cyberCAV also results in a new specification, i.e. TS 22.104 (service requirements for cyber-physical control applications in vertical domains), which contains normative requirements that are specific to

cyber-physical control applications. The work items are slated to be finished in November 2018. The requirements will then be used by other 3GPP working groups for the definition of 5G architecture extensions, 5G features and functionalities in order to support vertical and cyber-physical control applications.

Release 16 will conclude at the end of 2019, and the first products are expected in early 2021.

Support of User Identities in 3GPP

Kurt Bischinger, Deutsche Telekom, Rapporteur of TR 22.904 and Work Item UIA

Identifying a user or a certain user role in a 3GPP network will enable an operator to provide customization and enhanced user experience for services inside and outside the network. Also, operator services can be offered to devices that are not part of the 3GPP network.

Up to now 3GPP networks have been subscription centered, which was sufficient as long as a typical user only had one device, mainly running operator provided services, like telephony and SMS. Nowadays, using multiple connected devices, for example mobile phones, tablets or laptop computers, and with sharing devices or access gateways among users, it becomes more important to additionally support the identification of the actual user.

So after six months of work in its services group SA1, 3GPP TSG SA (Technical Specification Group Service and System Aspects) approved the TR (technical report) 22.904, study on user centric identifiers and authentication [1], in June 2018. The study is a collection of use cases and requirements related to user identity management, whereby a user in this context could be a person using a UE (user equipment) with a certain subscription, or an application running on a UE, or a non-3GPP device that connects to the 3GPP network and services via a gateway UE or non-3GPP access.

The TR describes a framework for user identities, which could be provided by an entity within the operator network or an external party. The actual identity provisioning service with creation, managing and authentication of identities is out of scope. The focus lies on the interaction of such a service with the 3GPP system:

- How to take a user identity into account for adapting network and operator-deployed service settings (policies, IP multimedia subsystem, service chain) and for network slice selection.
- Support of providing the user identity to external services via the 3GPP network.
- Extending 3GPP services to non-3GPP devices that are identified by user identifiers, for example to enable network and service access by these devices and to make them addressable and reachable from the network.
- Additionally, if the operator acts as identity provider, how to improve the level of security or confidence in the identity by taking into account information from the network.

The results of the study will be transferred into normative specifications. A related work item on User Identities and Authentication (UIA) was approved in June 2018. Besides some final consolidation work for the TR, SA1 has already agreed on the requirements during their August meeting. Subject to the approval in the upcoming SA plenary in September, an updated Release 16 version of two technical specifications [2], [3] and the TR [1] will be published.

After that, Stages 2 and 3 can be developed, with the main part to be done in 3GPP's security group SA3. Release 16 Stage 3 is expected to be closed by the end of 2019.

References

[1] 3GPP TR 22.904: "Study on user centric identifiers and authentication", http://www.3gpp.org/DynaReport/22904.htm
[2] 3GPP TS 22.101: "Service aspects; Service principles", http://www.3gpp.org/DynaReport/22101.htm
[3] 3GPP TS 22.115: "Service aspects; Charging and billing", http://www.3gpp.org/DynaReport/22115.htm

Introduction to Study on Maritime Communication Services over 3GPP

Hyounhee Koo, SyncTechno Inc., 3GPP SA1 FS_MARCOM Rapporteur

3GPP SA1 started the study item FS_MARCOM (Feasibility Study on Maritime Communication Services over 3GPP System) in 2016, with the original objective of maritime safety and traffic management for use cases introduced by the International Maritime Organization (IMO) Maritime Service Portfolio. It extended to the commercial maritime use cases in February 2017.

3GPP Technical Report (TR) 22.819 is the outcome of the feasibility study detailing the use cases and potential requirements for the support of maritime communication services over 3GPP systems. This is to enable 3GPP systems as a good candidates for innovative tools and to help address the information gap between users on land and users at sea as well as the maritime safety and vessel traffic management that IMO intends to achieve, especially in the 5G era.

Potential requirements are consolidated and specified to enable existing 3GPP enabling technologies to be applicable for the support of maritime communication services over 3GPP systems. Examples of existing features include:

- Mobile services such as Mobile Internet access, real time audio and video streaming for transmission and reception, TV broadcast and multicast services, short message service (SMS), multimedia messaging service (MMS), voice call and video call, etc.
- Machine type communications such as additional MTC enhancements for LTE (eMTC) and Narrowband Internet of Things (NB-IoT)[LZ(1)[H2].
- Public warning services for Public Warning System (PWS) [LZ(3)[H4] and enhancements of PWS (ePWS[LZ(5)[H6]).
- Mission critical services on-network and off-network.
- General 5G services as specified in 3GPP SMARTER (New Services and Markets Technology Enablers) [LZ(7][H8] work.
- Enabling technologies developed in 3GPP 5GSAT [LZ (9] [H10] (Integration of Satellite Acess in 5G) and 5GLAN (LAN support in 5G) [LZ(11][H12].
- Indoor positioning services developed in 5G_HYPOS [LZ(13][H14] (5G positioning services).

Also considered were potential requirements that are common for the general maritime usage applicable for commercial maritime usage as well as authority-related usage for the purpose of maritime safety and traffic management over 3GPP system. Potential requirements also included are those dedicated to authority-related usage on maritime safety and traffic management.

Based on the conclusions and recommendations in the TR 22.819, 3GPP SA1 is continuing to standardize and specify the Release 16 stage 1 requirements specific to maritime usage over 3GPP systems for commercial as well as safety purposes from June 2018 to December 2018.

3GPP 5G Phase-2 Network Slicing Standardization for Release 16

Tricci So, ZTE TX Inc., Rapporteur for 3GPP SA2 Study Items "Enhancement of Network Slicing (eNS)" and "Access Traffic Steering, Switching and Splitting (ATSSS)"

The 3GPP TSG SA WG2 (SA2) Architecture Working Group is working on 5G Phase-2 delivery for 3GPP Release 16, and one of the main features in 3GPP Release 15, network slicing, has a few open issues that need to be addressed. When 3GPP 5G Phase-2 development started in January 2018, a new study item "Enhancement of Network Slicing" (eNS) was approved to analyze the possible solutions for the three outstanding issues that have not been completed in 3GPP Release 15. The three key open issues are:

1) Determining the practical non-roaming and roaming deployment scenarios and system impacts when the 3GPP 5G System is not able to support all possible combinations of network slices, identified by Network Slice Selection Assistance Information (NSSAI), for the UE which is the aspect of mutually exclusive access to network slices.

2) Studying possible enhancements for the interworking between the 4G Core (EPC) and network slicing in the 5G Core (5GC) while the UE is in connected and idle modes.

3) Studying how to provide network slice access authentication and authorization specific for the authorization method that uses user identities and credentials instead of the 3GPP subscription permanent identifier (SUPI) and that takes place after the required primary authentication and authorization between the UE and the 5G System.

The technical report that captures the results for the study of eNS is documented in TR 23.740, and the target conclusion date for the study is December 2018. It will then be followed by the normative phase starting in January 2019 to specify the standard solutions based on the conclusions from the technical report. The goal is to complete the normative work for eNS by June 2019.

For the key issue 1), the main deployment considerations that restrict which network slices can serve the UE simultaneously are due to the internal regulation (of the subscriber, of the employer, of the operator, etc.) or network capability. The target solution must not impact the Release 15 UE and must support the various combinations of Release 15 and Release 16 end-to-end configuration, including the roaming scenarios.

For the key issue 2), the main consideration is to define common procedures to support mobility from EPC to 5GC on one or more packet data network (PDN) connections that are connective active in EPC. Note that EPC does not support network slicing, whereas 5GC does, so the key issue is how to retrieve the correct NSSAI of the PDN connection and how to select a correct target interworking Access and Mobility Management Function (AMF)/Visited Session Management Function (V-SMF) based on the NSSAI. The final solution must be compatible with the Release 15 EPC and 5GC interworking solution that has been specified for the idle and connected mode scenario.

For the key issue 3), the main objective is to determine how the UE and the network can know that additional authorization and authentication is required for a network slice. Furthermore, the solution must also address the additional authorization and authentication are triggered and performed.

As of August 2018, the basic definitions and some working assumptions corresponding to the three key issues above have been defined, and each of the three key issues has multiple proposals submitted for considerations. Given that there are only two meetings left until the end of 2018 to conclude the study, the way forward is to start converging similar solution proposals and to start the evaluation of the solutions in the October 2018 SA2 meeting, which is then followed by finalizing the respective solutions that address the three key issues during the November 2018 SA2 meeting so that they can be approved and endorsed by the SA plenary meeting in December 2018.

ETSI NGP ISG: Network Protocols for Next Generation

Kiran Makhijani, Principal Engineer, Huawei Technologies, USA; Dr Richard Li, ETSI NGP, Vice Chair, Huawei Technologies, USA

Next Generation of Protocols (NGP) Industry Specification Group (ISG) was formed with a goal to identify and address limitations in the current network protocol suite vis-à-vis the 5G world enabled with new services and applications. NGP addresses issues that hinder the efficient operation of Internet Protocols over largely heterogeneous access technologies in order to provide end to end user Quality of Experience (QoE). NGP studies different topics in networking technologies, architectures, and protocols for the next generation of communication systems as 'work items' which are then published as independent guidelines in the form of General Recommendation (GR) or General Specification (GS).

The work is split into two baskets: generalized network architecture study, proposing reference models and performance indicators to validate any protocol or approach; and specific solutions and technologies such as those for better and deterministic throughput, bounded-latency have taken prominence in the light of networked Augmented and Virtual Reality (AR/VR), connected vehicles and machine type communications.

In the first year of NGP 2015-2016 the following work began:

- GS NGP 001 on scenario definitions (completed): our foundational work driven by innovations necessary to deploy 5G networks. It recognizes in total 11 key issues; the most critical ones identified were the device or end user addressability, mobility, security, context awareness, virtualization and performance of end to end network operations.
- GS NGP 002 (completed) and GR NGP 006 (due mid 2018) are management centric and provide an architecture for self-organizing control of networks and use of machine learning in Intelligence-Defined Networking (IDN).
- GS NGP 003 (completed) an evaluation of different types of candidate packet forwarding architectures suitable for next generation networks and motivations for such 'packet routing technologies'.
- GR NGP 004, Identity Oriented Networks (ION), proposes 'Identity' as a fundamental component toward the evolution of addressing by using a framework of identities and their awareness in networks to solve problems relating to mobility, address extensibility and scalability. Since its publication, it has been discussed at IETF IDEAS (https://datatracker.ietf.org/wg/ideas), a distributed inter-operable network identity system, and in the Distributed Mobility Management (DMM) work group for the purpose of user plane optimization in 5G.

The second year, 2016-2017, saw the following:

- GS-NGP-005 (completed) is a summary of requirements that emerged from scenarios studied in GS NGP 001.

- GSP NGP 007 (completed), presents an abstract reference model on the basis of which different network architectures should be evaluated because protocol models vary in each of the networks, such as service provider core networks (CN), LTE mobile networks (MN), virtual private networks (VPN), and mobile edge compute (MEC) networks. GS NGP 007 helps to unfold complexities and inefficiencies, and expose meaningful commonalities across such systems.

In the current period, 2017-2018, the following work has begun and is yet to be finished:

- GR NGP 008 deterministic mobile networks for Ultra Reliable Low-Latency Communications (URLLC) in cellular networks identifies gaps and proposes integrated radio access and fixed networks framework.
- GR-NGP-009 elaborates on principles for a Generic Network Protocol Architecture based on fundamentals covered in GR NGP 005.
- GR-NGP-010 on new transport technology, since multimedia continues to be the biggest and most heavily used service in the Internet. This GR provides recommendations for evolved media requiring guaranteed throughput through new types of transport technologies.
- GR NGP-011 recommends a managed object-based network slicing architecture with a comprehensive description of its interfaces and functional components.
- GR NGP 012 proposes a new packet format for deterministic multimedia broadcast services.

The NGP helps with preliminary work needed for the adoption of new technologies with a holistic look at the protocol stack. It continues to recommend improvements in several sectors. More is yet to come; we aim to liaise with other Standard Developing Organizations (SDOs) and refine our work on packet formats, protocol stacks, and routing technologies toward the new Internetwork paradigm.

ETSI NGP will host the first "New Internet Forum" on 12 October 2018 at The Hague, co-located with the SDN NFV World Congress, and invites everyone to participate.

ESTSI NGP home contains more information: https://portal.etsi.org/tb.aspx?tbid=844&SubTB=844.

P802.1Qcx CFM YANG Data Model Status

Marc Holness, Ciena, Editor IEEE 802.1Qcp, P802.1Xck, and P802.1Qcx

The P802.1Qcx project specifies a unified modeling language (UML) based information model and a YANG data model that supports the configuration and status reporting for connectivity fault management (CFM), as defined in IEEE 802.1QTM-2018.

- A data model is an abstract model that explicitly and precisely defines the structure, relationships, syntax, and semantics of the data.
- YANG is a newly defined network configuration data modeling language that can model configuration data, state data, operations, and notifications for network management protocols.

Utilization of a standardized YANG model can be used in conjunction with a network configuration protocol (e.g., NETCONF) to enable network automation within service providers, cloud providers, and enterprise networks. This allows the management of network element time and cost to be significantly reduced, since manual steps can be removed. Additionally, standard-based YANG data models allow applications to subscribe to specific configuration and operational data items to be automatically streamed in real-time to the subscriber.

The P802.1Qcx project builds on top of the YANG data models developed by IEEE 802.1Qcp (Bridges and Bridged Networks YANG Data Model). The development of the CFM YANG model will support the connectivity fault management protocol suite defined by 802.1QTM-2018 and will also provide the foundation and framework for which the ITU-T Study Group 15 Recommendation G.8052.1 (Transport OAM Management Information/Data Models for Ethernet Transport Network Element) can build on. The G.8052.1 Recommendation will specify the management information models and data models for the transport Ethernet network element (NE) to support specific interface protocols and G.8013/Y.1731 specified OAM.

In addition, it is anticipated that the P802.1Qcx defined CFM YANG model will be used by other SDOs (e.g., Broadband Forum, MEF). Consequently, the CFM YANG data model is being structured and defined such that it can be used by IEEE 802.1Q compliant bridging devices as well as non-bridging devices, which are often defined and used by other SDOs.

This project has entered the Task Group balloting phase of the standards development process. At the time of this writing, draft version 0.3 of the P802.1Qcx specification has been created and is available for review. The CFM YANG modules are defined and have reached a state of stability. The structure of the CFM YANG modules allows a diverse user community to apply the CFM data model.

- **ieee802-dot1q-cfm-type.yang**. Type definitions for the overall CFM YANG modules.
- **ieee802-dot1q-cfm.yang.** Generic CFM YANG model structure. This module can be utilized by users who may not be IEEE 802.1Q Bridge compliant.
- **ieee802-dot1q-cfm-bridge.yang.** Augmentations and extensions to the generic CFM YANG model that is specific to IEEE 802.1Q bridges.
- **ieee802-dot1q-cfm-mip.yang.** Explicit MIP YANG model structure that is optional.

The CFM YANG modules can also be found in GitHub, and are found at https://github.com/YangModels/yang/tree/master/standard/ieee/802.1/draft.

It is anticipated that this project should reach formal completion by the middle of 2019. This would require traversal through Working Group balloting, and Sponsor balloting process.

IETF Multipath TCP Standards Activities and Outputs

Yoshifumi Nishida, GE Global Research, IETF Multipath TCP Working Group Co-chair; Philip Eardley, BT, IETF Multipath TCP Working Group Co-chair

The Multipath TCP (Transmission Control Protocol) Working group [1] at the IETF (Internet Engineering Task Force) has standardized a new extension of TCP that allows a TCP connection to be spread over multiple paths, bringing benefits of better resilience, throughput and load balancing. Multipath TCP is a key technology to help exploit the existence of multiple access technologies, which is increasingly the norm.

Today, most traffic on the Internet is carried by TCP. A TCP connection has (exactly) one IP address at each endpoint, so traffic flows over a single path. However, it is now typical for end devices, such as smartphones, to be equipped with multiple network interfaces, typically Wi-Fi and cellular. Multipath TCP (MPTCP) is an extension to TCP that enables traffic from a TCP connection

to be spread across more than one path, and hence exploit the existence of multiple access technologies.

The IETF MPTCP working group published the protocol, RFC6824 [2], in 2013. An updated spec is currently (2018) under review, and incorporates lessons learned from the various implementations, deployments and experiments, in order to achieve improved reliability and security. The updated spec is also planned to be on the IETF Standards track, while the current version is experimental. Publication is expected in early 2019.

The MPTCP specification defines how a TCP connection can spread traffic across multiple subflows, as identified by different IP addresses (or ports), and how the subflows can be created and terminated on demand during the session.

The specification meets two key design criteria:

- Application compatibility: Applications use the same socket interface (API) and get the same service model. Therefore, existing TCP applications can utilize Multipath TCP without being changed, as soon as the underlying OS supports the feature.
- Network compatibility: Multipath TCP needs to be compatible with the network as it exists today. Since all MPTCP traffic is TCP segments, network devices can handle it without upgrading their software. However, the main design challenge was to enable MPTCP's signalling messages to work through the many types of middleboxes, such as NATs, firewalls and performance enhancing proxies. MPTCP has been measured to work successfully across the large majority of Internet paths, but the protocol falls back to ordinary TCP where there is an incompatibility on the path.

The WG has published seven RFCs so far, which include the core specification (RFC6824), congestion control (RFC6356), API considerations (RFC6897), threat analysis (RFC6181), and operational experiences (RFC8041) [2-8]. The congestion control scheme balances traffic across the paths, so as to best exploit the available capacity, while also ensuring that an MPTCP connection is not too greedy for other normal TCP connections that share the same network. Alternatively, MPTCP can set up multiple subflows, but only use one at a time, with the other subflows on 'hot standby' in order to improve resilience or provide a form of mobility management.

Multipath TCP has been extensively implemented and deployed. An open source Linux version is available, and commercial vendors such as Apple, F5 and Citrix support Multipath TCP in their products. The standard has been in all Apple smartphones since 2013 and is used by Siri, and recently (since iOS11) the MPTCP API has been open to third-party developers.

While the baseline MPTCP runs between two end devices, it is also advantageous to exploit multiple paths where one (or both) end points run regular TCP. This requires one (or two) proxies: a device to convert between TCP and MPTCP. There are already some commercial deployments of this, for example, where a residential or business gateway has multiple technologies, such as 3G /4G wireless in addition to DSL. The IETF is currently developing an MPTCP proxy standard in the TCPM working group [9].

References

[1] https://datatracker.ietf.org/wg/mptcp/
[2] A. Ford *et al.*, "TCP Extensions for Multipath Operation with Multiple Addresses," RFC 6824, Jan. 2013.
[3] M. Bagnulo, "Threat Analysis for TCP Extensions for Multipath Operation with Multiple Addresses," RFC 6181, Mar. 2011.
[4] C. Raiciu, M. Handley, and D. Wischik, "Coupled Congestion Control for Multipath Transport Protocols," RFC 6356, Oct. 2011.
[5] A. Ford *et al.*, "Architectural Guidelines for Multipath TCP Development," RFC 6182, Mar. 2011.
[6] M. Scharf and A. Ford, "Multipath TCP (MPTCP) Application Interface Considerations," RFC 6897, Mar. 2013.
[7] M. Bagnulo, "Analysis of Residual Threats and Possible Fixes for Multipath TCP (MPTCP)," RFC 7430, July 2015.
[8] O. Bonaventure, C. Paasch, and G. Detal, "Use Cases and Operational Experience with Multipath TCP," RFC8041, 2017
[9] https://datatracker.ietf.org/wg/tcpm/

Standardization Activity of Quantum Key Distribution in ISO/IEC

Jiajun Ma, QuantumCTek Co. Ltd.; Hongsong Shi, China Information Technology Security Evaluation Center; Kai Chen, University of Science and Technology of China; and Gaëtan Pradel, INCERT GIE, Luxembourg

Quantum key distribution (QKD) provides a solution to establish information theoretic security keys between communication parties. The keys can then be supplied to cryptographic algorithms to achieve the so called long-term secure or quantum-safe communication. QKD is expected to become an important building block of the global information communication infrastructures, especially in scenarios with high-level security requirements. Therefore, the formulation of QKD-related international standards is expected to play a crucial role in promoting the industrialization of QKD technology.

Although in recent decades there has been significant development of QKD from experimental demonstration to the emerging worldwide commercialization, rigorous security testing and evaluation of QKD remains an underdeveloped area. Note that some standard development organizations, e.g., ETSI and IEEE P1363, have been developing QKD testing or security requirement related specifications. However, less work has been done under the framework of ISO/IEC 15408, also known as the Common Criteria, for solving the security certification problems of QKD. This is not commensurate with the potentially extensive applications of QKD technology, where security evaluation certificates of the Common Criteria are generally required in the procurement of IT products.

With this in mind, the subcommittee of IT security techniques, ISO/IEC JTC1/SC27, launched the study item "Security requirements, test and evaluation methods for quantum key distribution" at the Working Group meeting in November 2017 in Berlin. Experts from China and Luxembourg National Bodies were nominated as rapporteurs of the project. The study item intends to systematically investigate the potential threats to QKD devices and the security requirements that a QKD system should meet to defend them. More importantly, corresponding security testing and evaluation methodology are planned to be studied within the Common Criteria framework. A Call for Contributions was then circulated globally to the stakeholders of QKD.

The project is currently in the study period stage. The rapporteur group, during the first study period, produced a technical report covering many aspects of QKD, including the relevant research and projects undertaken in this area, the technology maturity and market analysis, and a brief description of the security testing and evaluation methodology for QKD. After the ISO/IEC JTC1/SC27 Working Group meeting in April 2018 in Wuhan, China, the study item was evolved into its second study period, where the Call for Contributions was updated with an emphasis on the topics:

- The security risks confronted by the transmitter module, receiver module, and post-processing procedure of a QKD system.

- The security requirements, test and evaluation methods for optical modules of a QKD system in the information theoretic sense that the adversary is of unbounded computing power.

The second study period is expected to be complemented in the next working group meeting in October 2018, where a new work item proposal will be launched to push the project to the working draft stage.

The establishment of this security evaluation standard is expected to allow different manufacturers and users to better understand the QKD technology. The standard would also help make security requirements merged into the design, manufacture and use of QKD products, thereby reducing the technical thresholds and security risks of this technology.

ITU-T SG17 Question 5: Countering Spam by Technical Means

Yanbin Zhang, ITU-T SG17 Q5 Rapporteur, and Xiaotian Yao, China Academy of Information and Communications Technology

Spam is information that is unsolicited, unwanted, and even harmful for recipients. It has been a widespread problem that can cause a loss of revenue for Internet service providers, telecommunication operators, mobile telecommunication operators and business users all over the world.

Countering spam requires multifaceted, comprehensive approaches. Study Group 17 (SG17), as the lead Study Group on security and in supporting the activities of WTSA (The World Telecommunication Standardization Assembly) Resolutions 52 (countering and combating spam), is well-positioned to study the wide range of potential technical measures to counter spam, as it relates to the stability and robustness of the telecommunication network.

Question 5 in SG17 is dedicated to countering spam by technical means. In addition, the technical structure for existing and potential Recommendations on countering spam by technical means has been established to facilitate Recommendation production. Furthermore, new Recommendations shall be developed to counter new emerging forms of spam.

Question: Study items addressed by Question 5 include, but are not limited to:

- How to understand and identify spam?
- What are new forms of spam in existing and future networks?
- What are serious effects of spam?
- What are technical factors that contribute to difficulties of identifying the sources of spam?
- What are the effective and efficient solutions for countering spam?
- What are the best practices for countering spam?

Work Program: Question 5 has work items that are currently in progress as follows:

- **X.gcims**, guidelines for countering instant messaging spam (to be completed in September 2020).
- **X.sup-ctss**, supplement to ITU-T X.1231 technical framework for countering telephone service spam (to be completed in September 2018).
- **X.tfcas**, technical framework for countering advertising spam in user generated information (to be completed in September 2019).
- **X.tfcma**, technical framework for countering mobile in-application advertising spam (to be completed in September 2018).
- **X.tsfpp**, technical security framework for the protection of users' personal information while countering mobile messaging spam (to be completes in September 2020).
- **X.tecwes**, technologies in countering website spoofing for telecommunication organizations (to be completed in 09/2019).

Question 5 will expand its work program in the future to continue developing, as a matter of urgency, Technical Recommendations with a view to exchanging best practices and disseminating information through joint workshops, training sessions, etc.

Question 8 of ITU-T Study Group 17: Cloud Computing Security

Liang Wei, China Academy of Information and Communications Technology, ITU-T Q8/17 Rapporteur

The wide application of cloud computing enables flexible and dynamic resource provisioning, as well as simpler and highly automated administration of IT infrastructure. However, the open systems and shared resources of cloud computing raise many concerns about security, which is perhaps the most important barrier to the adoption of cloud computing. Question 8 of ITU-T Study Group 17, Cloud Computing Security, was established in 2010 to take charge of all the Study Group 17 activities on cloud computing security, aiming at advancing cloud computing security by developing recommendations to identify security requirements and threats, define security architecture to organize security functions, and identify specific technologies and mechanisms to achieve trustworthy relationships within the cloud computing ecosystem. Q8/17 also collaborates with related Questions such as 2/17, 3/17, 4/17, 7/17, 10/17 and 11/17 for joint activities in the development of cloud computing.

Q8/17 has established a layered cloud computing security recommendation structure, which consists of overview, security design, security implementation, and best practices and guidelines. Within this recommendation structure, Q8/17 has identified security threats and challenges, and defined security capabilities that could mitigate these threats and address security challenges (X.1601) at the overview layer. The security design layer focuses on security requirements, security capabilities, the trust model, the security architecture, security functions, and security controls (X.1602 and X.1603, X.SRIaaS, X.SRCaaS, X.SRNaaS under development and scheduled for completion in September 2019). The security implementation layer aims at developing recommendations of security solutions, security mechanisms, incident management, disaster recovery, security assessment and audit. Best practices and guidelines include lifecycle data protection requirements for cloud service customers (CSCs) and operation security guidelines for CSPs (X. 1631, X.1641, X.1642), and security protection measures of big data platform (X.GSBDaaS under development and scheduled completion in September 2019).

With the continuous development of cloud computing technology, Q8/17 intends to improve its cloud security recommendation structure up to date and expedite the development of draft recommendations, particularly for IaaS, CaaS, NaaS and BDaaS security requirements. Moreover, as cloud computing and big data have long been conjoined in industry, the core processes of big data such as data storage, retrieval, analysis, management and visualization become inseparable with cloud computing, and security issues of cloud computing and big data have always been discussed together. Q8/17 will incorporate big data security into its study category, thus forming a sufficient complement to the existing cloud computing standardization system, and meanwhile providing a practical environment to advance big data security.

Biology-to-Machine (B2M) Protocol: Connecting Life to the Internet

John Caras, Rapporteur ITU-T SG 17 Question 9, Editor of X.b2m, Biology to Machine Protocol

In 2018, ITU-T SG17/WP4/Q9 began development on an open-architecture, Biology-to-Machine (B2M) protocol, enabling bidirectional communication between biological-entities (wetware) and IoT enabled computers. B2M expands the Internet of Things (IoT) to include not just electrical but biological based computation systems. B2M enables autonomous systems to recognize life and enable life-protecting measures, e.g. autonomous vehicles and life supporting robotics. B2M also provides a common data format for mobile health devices independent of manufacture, e.g. wearables including but not limited to electrocardiogram (ECG/EKG) and continuous glucose monitors. ITU-T SG17 is open to liaison with other standards organizations with similar interests.

In much the same way Vinton Cerf and Dr. Robert Kahn changed the world with the Transmission Control Protocol (TCP/IP) forming the basis of open-architecture networking between two computers, B2M is designed to connect to biological systems, which includes people, livestock, and plants to computers and the network. B2M's purpose is to extend the Internet of Things to include biological endpoints with a universal language and make B2M a native protocol to IoT devices globally.

At the heart of the B2M protocol is a "Telebiometric Interaction Model" which organizes all collected or derived data by the sciences: physics, chemistry, biology, culturology, and psychology. A simple analogy equates the body as a territory and the scientific fields are the borders of the body. Nothing can go in or out of a biological system except through one or more of the scientific fields. Adding a measurement system including values and units, one can determine how the biological system was influenced by its environment. (See Fig. 1, upper left.)

From this model, a data packet is structured containing essential information about the biological entity, hardware, and the type of interaction. The data is extracted, managed, and protected, enhancing the value of the application by creating sets of raw-data, derived-data, and graphical data supported by deep learning algorithms. The B2M protocol enables an IoT network to bi-directionally communicate with a biological entity. The B2M Protocol communicates descriptors directly into

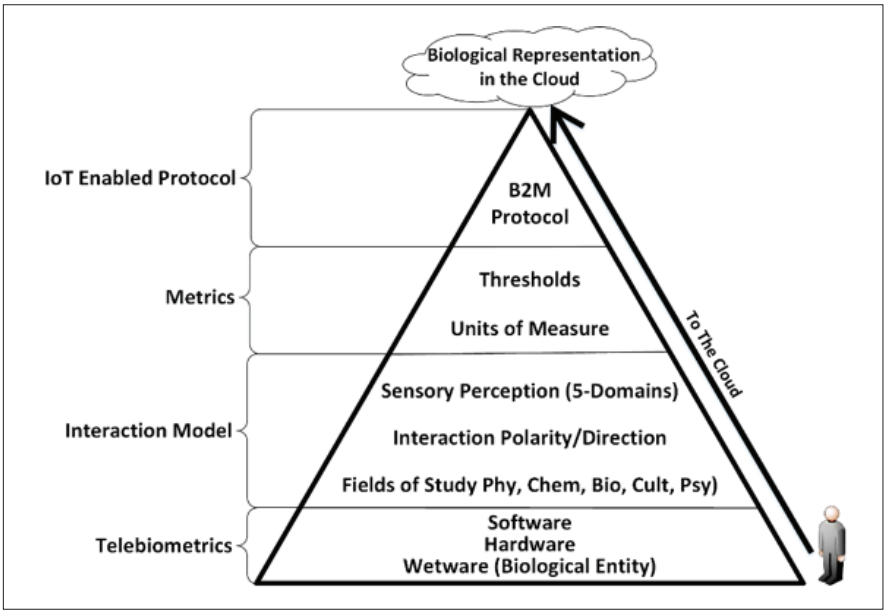

Figure 1. Components of the Biology-to-Machine Protocol..

Machine-to-Machine (M2M) protocols, thereby extending the Internet of Things (IoT) to include biological entities. The value of the B2M protocol is that it is application-independent and market-independent and supports unlimited devices, thereby increasing the biological representation in the cloud universally accessible and useful.

Q9 ITU-T SG17/WP4/Q9 intends to finalize the standard by 2020 with a diverse group of industry and government editors from Alibaba, Korean Internet Security Agency (KISA), Telebiometrics, Denmark, and Senegal

ITU-T SG 17 Question 10: Identity Management Architecture and Mechanisms

Abbie Barbir, Aetna USA, Q10/17 Rapporteur; Hiroshi Takechi, NEC Japan, Q10/17 Associate Rapporteur; Junjie Xia, China Unicom, China, Q10/17 Associate Rapporteur; and Keundug Park, Seoul University of Foreign Studies, Korea, Q10/17 Associate Rapporteur

ITU-T SG 17 is the lead study group on security within ITU-T, and Q10/17 is the lead question on identity management architecture and mechanisms. Q10/17 is dedicated to vision setting and the coordination and organization of the entire range of IdM activities within ITU-T.

There are many work items that are currently in progress in Q10/17. The work items can be broken into the main focus areas. The first area includes efforts to update ITU-T Recommendation X.1254 "Entity authentication assurance framework" to reflect the updated version of NIST SP 800-63-3 "Digital Identity Guidelines." This work aims to incorporate recent changes in identity validation and authentication. The objective here is to advance X.1254 to reflect a risk-based approach to identity vetting and authentication. This work keeps liaison and informed to ISO/IEC JCT1 SC27/WG5 on revision work of ISO/IEC 29115. It is expected that these work items will be finished within the current study period 2017-2020.

Another area of focus of Q10/17 is an initiative to update X.1252 "Baseline identity management terms and definitions" to include current industry advances in decentralized identity. Q10/17 is working on developing a decentralized identity model including terms and definitions that is suitable and compatible with current efforts on using distributed ledgers for self-sovereign identity. Q10/17 is also working with Q14/17 (DLT specific question) to develop security risk and assessment (X.dltsec) for distributed ledger decentralized identity management systems. It is expected that these work items will be finished within the current study period 2017-2020.

Another area of focus is the promotion of standards to eliminate the use of passwords for online interactions. In this regard, Q10/17 is working with the FIDO Alliance to further standardize their specifications into ITU-T recommendations in a way that is similar

to what Q10/17 has done with OASIS SAML (X.1141) OASIS XACML (X.1144) and OASIS Trust Elevation (X.1276) specifications. In particular, the FIDO Alliance "Client to Authenticator Protocol (CTAP)" and the FIDO Alliance Universal Authentication Framework (UAF) specifications are being adopted in Q10/17 as ITU-T recommendations. Target delivery of this work is September 2018. Q10/17 is expected to finish the above work within the current SG17 study period.

There are also many other joint work items in the question with other questions on PKI and biometric based client server authentications. In addition, Q10/17 fulfils its role with the operation of the Joint Coordination Activity on IdM (JCA-IdM) to ensure proper coordination in the IdM arena to avoid duplication within the ITU and other standard organizations.

Going forward, Q10/17 would appreciate contributions on risk based authentication, decentralized identifiers authentication, and digital wallet interoperability. Q10/17 would appreciate your participation and looks forward to staying engaged in developing internationally recognized interoperable standards.

ITU-T SG17 Question 13: Security Aspects for Intelligent Transport Systems

Dr. Sang-Woo Lee, Electronics and Telecommunications Research Institute, Rapporteur of Q13 in SG17

Significant development has taken place over the past few years in the area of vehicular communications for Intelligent Transport Systems (ITS). Connected vehicles are considered the key enabling technology in ITS. However, connected vehicles without security functions can make ITS applications vulnerable to various security threats. Therefore, security functions should be guaranteed in order to utilize vehicular communications since the vulnerability of the vehicle is directly related to the life of drivers and pedestrians. This results in many standard organizations developing international standards to cope with the security requirements of ITS. ITU-T Study Group 17 (SG17) started standardization on ITS security in 2014 and established a new Question 13 in 2017. Q13/17 completed one recommendation, X.1373, in 2017. X.1373, Software Update Capability for ITS Communications Devices, defines the secure software update procedure for electric devices inside a vehicle such as electronic control units (ECUs), electric toll collections (ETCs) and car navigation systems. Since electric devices inside a vehicle are becoming more sophisticated, software modules need to be appropriately updated for the purpose of bug fixing, performance improvements, and security enhancements. Q13/17 is now considering the update of X.1373 in order to reflect practical information from the ITS industry. Q13/17 currently has the following seven work items in progress.

X.itssec-2, Security guidelines for V2X communication systems. V2X is a generic term for communication modes of V2V (Vehicle-to-Vehicle), V2I (Vehicle-to-Infrastructure), V2ND (Vehicle-to-Nomadic Devices) and V2P (Vehicle-to-Pedestrian) in this draft Recommendation. This item identifies threats in the V2X communications environment and specifies security requirements and use cases (expected completion: 2019-Q4).

X.itssec-3, Security requirements for vehicle accessible external devices. This item provides analysis on security threats in vulnerable points like OBD-II [LZ(1] (On-Board Diagnostics) [SWL2] port or wireless connectivity and security requirements for vehicle accessible external devices. This draft Recommendation can be practically utilized by car manufacturers, suppliers, third-party external device manufacturers and ITS-related industries (expected completion: 2019-Q4).

X.itssec-4, Methodologies for intrusion detection system on in-vehicle systems. This draft Recommendation includes classification and analysis of attack types on internal networks and systems in vehicles. This item also provides an architecture framework with lightweight plugins that include specialized detection models with respect to characteristics of vehicle system environments (expected completion: 2020-Q4).

X.itssec-5, Security guidelines for vehicular edge computing. This draft Recommendation provides security guidelines for vehicular edge computing (VEC). VEC is a model that supports the core cloud's capacity for decentralizing the concentration of computing resources in data centers. VEC also provides more localized storage and application services to road users, thereby making it possible to achieve lower latency delays, faster responses, providing mobility support, location awareness, high availability and Quality of Service for real-time applications like streaming since data processing is conducted closer to the vehicle (expected completion: 2020-Q4).

X.srcd, Security requirements for categorized data in V2X communication. This item categorizes the data used in V2X communications into several types and defines the security level for each categorized data type. Based on these categorized data in each security level, this draft Recommendation provides security requirements for categorized data in V2X communications (expected completion: 2020-Q4).

X.mdcv, Security-related misbehavior detection mechanism based on big data analysis for connected vehicles. This item addresses misbehaviour detection mechanism models and how to use big data analysis in ITS environments (expected completion: 2020-Q4).

X.stcv, Security threats in connected vehicles. This item can be referred and utilized from other Recommendations developed in Q13/17 as a baseline (expected completion: 2019-Q2).

Q13/17 will continuously develop Recommendations that address security aspect of ITS. Q13/17 will further focus on ITS security standardization activities to address emerging technology such as autonomous driving.