Question 12/11 – Testing of internet of things, its applications and identification systems

(Continuation of Question 12/11)

1 Motivation

In a broad perspective, the Internet of things (IoT) can be perceived as a vision with technological and societal implications. From the perspective of technical standardization, IoT can be viewed as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies. Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst maintaining the required privacy. The concepts of u1-society, u-network, u-city and others have been formulated in support of the worldwide perspective for IoT applications, services and technologies which may be enabled by radio frequency identification (RFID), ubiquitous sensor network (USN), machine-oriented communication (MOC), machine-to-machine (M2M) communication, smart device communication (SDC), Cloud-enabled IoT services (CIS), where RFID has been taken into account by ISO/IEC JTC 1/SC 31, sensor network technologies by ISO/IEC JTC 1/WG 7, USN by ITU-T SG20, MOC by ITU-T SG13, M2M by ITU-T and ETSI, SDC by TIA, CIS by ETSI, OGC, and W3C.

NOTE 1 – "u" stands for "ubiquitous" which has been interpreted as a capability for any services at anytime and anywhere through any devices.

All these keywords have some similar use cases and imply some identical functions but consider some different technology views. The IoT may be seen as an umbrella for all these technology keywords.

Since the IoT has such broad concept and may be associated with various enabling technologies, interoperability issues shall be considered.

In general, IoT discovers various new types of connectivity which may be used in different customer-oriented applications (e.g., flying ubiquitous sensor networks (FUSN), IoT-based augmented reality (AR) and so on).

Also, taking into account the secure authentication mechanism used by IoT-based technologies and IoT identity, IoT may be considered as one of the tools to be used for combating counterfeiting.

Bearing in mind all the above, the testing of the IoT technologies/applications are becoming more important today, especially in terms of interoperability of the IoT devices and trust of the used IoT systems.

In addition to traditional IoT applications, it is advisable to consider testing in areas in which the largest implementation of IoT-devices is observed:

– Smart Sustainable Cities;
– Wearable devices;
– Industrial Internet of things (IIoT);
– Network-based driving assistance for autonomous vehicles;
– Flying networks based on Unmanned Aerial Vehicles.

As a rule, in each of these areas there are different scenarios for connecting IoT-devices to the Internet, cloud platforms and remote services. In this regard, the consideration of issues of testing procedures of IoT-devices seems to be very relevant.

2 Question

Study items to be considered include, but are not limited to:

– What types of tests are needed for IoT network elements?
– How to test the security of IoT-device taking into account their parameters (e.g., performance, memory size, communication channel etc.)?
– What test suites need to be developed for testing IoT identification/authentication procedures?
– How to test IoT technical solutions to be used for combating counterfeiting?
– What new Recommendations need to be developed in order to provide mechanisms to test the IoT applications, including the security and privacy aspects?
– What new Recommendations need to be developed in order to provide mechanisms to test the interoperability, capability, and security of IoT identification systems?
– What are the testing scenarios to be used for testing wearable devices?
– What are the testing scenarios to be used for testing Industrial IoT (IIoT) system and devices?
– What test suites need to be developed for testing methodology and/or mechanism (procedures) for testing the technologies and protocols for IoT and IIoT based on prediction analytics?
– What new Recommendations need to be developed in order to provide the interoperability, compatibility, and security of IoT devices to be used in Smart Sustainable City?
– What testing procedures need to be developed for IoT-based technologies and protocols for network-based driving assistance to be used in autonomous vehicles?

3 Tasks

Tasks include, but are not limited to:

– develop the test suites to be used for testing IoT network elements;
– develop the methodology for security testing and test specification related to security testing of IoT;
– develop test suites for testing IoT identification/authentication procedures;
– develop test suites for testing IoT technical solutions to be used for combating counterfeiting;
– develop the methodology and/or mechanism for testing the IoT applications, including the security and privacy aspects;
– develop the methodology and/or mechanism for testing the interoperability, capability, and security of IoT identification systems;
– develop the methodology and/or mechanism for testing the wearable devices;
– develop the methodology and/or mechanism for testing the Industrial Internet of Things and IIoT applications;
– develop the methodology and/or mechanism for testing the technologies and protocols for IoT and IIoT based on prediction analytics;
– develop the methodology and/or mechanism for testing the IoT-based technologies and protocols to be used in Smart Sustainable City;
– develop the methodology and/or mechanism for testing the IoT-based technologies and protocols for network-based driving assistance to be used in autonomous vehicles.

An up-to-date status of work under Q12/11 is contained in the SG11 work programme (https://www.itu.int/ITU-T/workprog/wp_search.aspx?sp=17&q=12/11).

4 Relationships

Recommendations:

– Q, Y, H, I, M and F-series

Questions:

– 15/11; 16/11

Study Groups:

– ITU-T SG2
– ITU-T SG5
– ITU-T SG13
– ITU-T SG16
– ITU-T SG17
– ITU-T SG20

Other bodies:

– ETSI especially TC cyber
– IEEE
– IETF
– ISO/IEC JTC 1 (especially ISO/IEC JTC 1 TC27, JTC1 WG 7, ISO/IEC JTC 1/SC 6, ISO/IEC JTC 1/SC 31, ISO/IEC JTC 1/WG 10)
– OGC
– TIA
– W3C

WSIS action lines:

– C5

Sustainable Development Goals:

– 9