Appendix D:
Details on Device Selection, Deployment Procedures and Guidelines

Contents

1.0 Introduction

In this Appendix recommendations on IoT Device Selection and Deployment Procedures and Guidelines are presented based on the experience with IoT Smart City devices platform deployed in Montreal downtown, QdS location in summer 2017.

2.0 Supported Protocol/Security requirements

IP-enabled devices (IPv4 and IPv6 support) are recommended for the ease of integration. When IP-enabled devices are not available, RS232/485/422 to Ethernet adapters can be used for integration to the IP network.

Devices with SSH, HTTPS, SNMPv3/v2c capabilities are recommended for security protection (NOTE: availability of SNMPv3 capable devices is low and normally significantly more expensive then SNMPv1 or v2c).

3.0 Management Monitoring and Control features requirements

Overall multivendor IoT network and sensor devices status monitoring and alerts could be performed by commercially available tools such as NetCrunch by Adrem Software, or a custom application could be developed, similar to the application that have been developed in BCR lab at McGill University, and discussed in more detail in Appendix F. Protocols such SSH, HTTPS, SNMP, and ONVIF for cameras, could be used for monitoring.

Controlling and managing/updating firmware of IoT devices is recommended through vendor specific supplied application as this could be the most stable and quickly deployable solution. We have not found a single open source or commercial application which could control multivendor devices. The main reason for this is there is no single standard set of commands that can be applied to all different purpose devices. A custom application could be developed and the most common protocol used for this purpose could be SSH for any most of the devices, or ONVIF for camera devices. However, central application development would have to be tailored to each specific vendor and device type set of commands and would require a major development effort.

In device selection and procurement process it should be required that a given device or sensor support SSH protocol, SNMP and ONVIF for camera. Ideally SNMP v3 should be supported for maximum security, however, many of presently available devices do not support this latest version and are not upgradable.

4.0 Transmission mode requirements

The following are the recommended transmission modes based on the device type.

Specialized Stereo Image Cameras (~ 77 Mbps):

These could be special application cameras or high bandwidth sensors and the amount of data rate generated by these devices could be large. In those cases it is recommended to store data on a local (to the sensor) storage device, and once the data collection is finished, transport/offload the data to the private data center using high speed 1Gbps wired Ethernet connection. Ideally offload should occur at the gateway connection to the private IoT network, alternatively it could be transported over a public network, assuming data is first encrypted (or using Secure FTP), and the connection over public network to the data center is fast.

Video Cameras (~ 16 Mbps):

Ideally camera should be connected to the Gateway by a fixed (100Mbps/or 1Gbps) Ethernet wire connection, if not feasible, a dedicated Wi-Fi bridge (up to 200 m clear Line-of-Sight, CLOS) with TDMA protocol should be used (5.8GHz ISM unlicensed or 3.65GHz licensed band).

Note, Wi-Fi based bridge connection may not provide lossless continuous video transmission, some video frames will be lost due to random interference from other Wi-Fi systems. For a typical video recording and analysis application the occasional video frame loss may not be important, as we observed during the pilot project, however, for specific critical applications it is recommended to use dedicated wired Ethernet connection from the camera to the gateway.

Medium data rate devices such as radar, RFID readers, etc (~ 45 kbps):

For ease of connectivity and reliability could also use/or share Wi-Fi radio bridges.

If Wi-Fi bridges are not available, Zigbee 900MHz for longer range (up to 340m), and Zigbee 2.4GHz for shorter up to 50 m range could be used. Note: 2.4GHz Zigbee may have limited <20kbps average throughput in urban scenario.

Other low data rate mobile devices such as sensors on vehicles (~ 0.123 kbps):

Use cellular LTE based Gateways, as discussed in main report, with per device data bandwidth monitoring tools such as Bell-Jasper. NOTE: Potential LoRa transmission mode could be investigated in the next step.

Other very low data rate fixed or mobile low power devices such as infrequent update rate temperature, light, proximity sensors:

Use LoRa radio enabled devices, typical range could be typically up 2km in urban environment. Theoretical data rate: 0.3 to 50 kbps.

Note, that for all so far deployed devices we recommend star based network topology to the gateway as this will ensure minimum data delay, and maximum link throughput. Adding more than one relays/hops in the wireless network could significantly increase data delay and overall throughput capacity.

5.0 Environmental Resistance requirements

Dust and water protection: IP66, IP67 certified (at least IP66).

Industrial Temperature range: -40 ˚C to +85 ˚C.

Cameras should have anti-fog and self-cleaning, image stability features.

NOTE: some of the devices could have applications only during the non-freezing temperatures season, such as prototype/experimental and could be relaxed

6.0 Urban design requirements

Most of the commercial IoT devices and sensors designed for outdoor use, already have packaging suitable for urban deployment with neutral colors.

When selecting an IoT device it might be desired to make sure with the supplier that a given device could be painted over to match the installation location background. The security/traffic video cameras that used in the pilot project had this option available.

Other IoT sensors and necessary accessories (power supply or network interfaces) might need custom, paintable, packaging. Deployment subcontractor might need to review with Ville de Montreal desired urban design requirements.

7.0 Data Formats requirements

Specific Data format for each sensor will depend on the application. For video the transport data format should be standard H.264, for other sensors data will need to be formatted at the network edge, before it is stored to the database, in an agreed-on and unified data format JSON files, as discussed in more detailed in Appendix E.

8.0 Power supply mode requirements

Many of the modern Ethernet interface based devices (such as cameras, wireless access points and bridges) have the option to be powered by Ethernet cable using a PoE standard (Power over Ethernet). This technology helps to reduce the number of wires to the remotely installed device, make installation of the device easier, and could allow to move the power supply unit further away from the device (might be important for esthetic Urban design), or in certain cases, even move it all the way to indoor location (which would relax environmental requirements of the power supply unit and its cost).

PoE support should be one of the preferred desired options on the selected IoT device.

Unfortunately, the selection of PoE module cannot be general for all IoT devices, since there are couple of existing standards, which are not necessarily interoperable. For example, many of the devices (like wireless bridges used in the pilot project) use Passive PoE, other devices could use 802.3af (also called 802.3at Type 1) “PoE”, or 802.3at Type 2 “PoE+”, or vendor proprietary High PoE (based on 802.bt standard in development). Final PoE module or midspan type selection would depend on the specific set of devices and deployment scenario.

Other non PoE IoT devices should support a standard 24V DC Power Supply. This requirement will ensure simplified deployment and maintenance of the IoT Smart City devices network.

9.0 Additional General Installation guidelines and recommendations

In general, installation of IoT devices in locations with multi-use (such as poles in QdS which are often used by events organizers) should be typically avoided, as that increases the chance of disconnecting, altering or breaking a given device by other users. The ideal would be a dedicated location, where the chance of accidental alteration is very low. Availability of 110 V AC power at the installation location for most of the IoT sensors would be very important.

Video Cameras specific:

For people and objects counting, cameras should be installed high directly above the observed area, avoid shallow angles

Cameras with zoom should be installed on solid Structures (building wall) as poles in general will swing in the wind and will make the image unstable (could be an issue for self-run analytics applications), image stability features might not be sufficient

Each Camera could have a maximum throughput of 20Mbps, thus a single P2MP Wi-Fi bridge Gateway connecting Camera stations in a star network topology should not have more than 4 stations for 802.11n with 100Mbps interface limit, if greater concentration is needed 802.11ac with 1Gbps ETH interface, and 360Mbps limitation, radios should be used which could support up to 13 stations.

NOTE: some cameras could support higher throughput, for example 50 Mbps, however, the recording application would have to be verified it can support such a speed configuration. We have observed some incompatibility in that maximum bitrate aspect between Axis Q6128-E camera and Milestone xProtect VMS.

High gain (16 or 19dBi) directional antennas for the radio end-stations should be used to avoid interference

Wireless bridges specific:

Use wireless bridges to extend connection reach from the fiber drops, for areas with distances more than 200 m, but less than 400 m, from a fiber drop, a Wi-Fi Relay could be used (but no more than 1 relay per link is recommended). Practical implementation of Relay in urban QdS Montreal downtown scenario should be tested in the next step.

Wireless Wi-Fi bridge between connected devices should have clear line of sight (NOTE: tree branches in a way are acceptable, but buildings blocking the signal will be a problem)

A single Wi-Fi bridge connection could be shared between collocated cameras and other sensors using Ethernet switch installed in the support unit

Mobile camera, for example installed on the car, will need to store images/videos to an on board storage unit, and offload data at the end of a day ideally through 1Gbps wired Ethernet connection or through dedicated 802.11ac Wi-Fi Access Point to the database center (as LTE will be too expensive for high volume data)

Each device should support reliable remote firmware update, multi-devices firmware update tools should be provided by vendor.

Physical maintenance of devices (cleaning domes of the cameras), reconnecting downed or failed devices could be significant, there should be a dedicated team to maintain deployed IoT devices.

10.0 IoT Smart City VdM platform summary and comments

Bandwidth by sensor type

Specialized Stereo Image Camera: ~ **77 Mbps** (based on 2fps, 1024x768, 16bit color tests)

Security Video Camera: ~ **16 Mbps** typical maximum for HD and UHD resolution with compression

Traffic Radar: ~ **45 kbps**

Temperature (x2)/Ultra Sound Level (x1) /GPS (x1) sensor: ~ **0.123 kbps** (based on 40 MB/month tests)

Cost-benefit

IoT devices with available high security features could be very expensive (up to 6 times) compared to unsecured or medium security devices. In the table below we have listed an example of a typical interface device need for connecting non-IP devices (for example Temperature sensor or Traffic radar) to the IP network.

Cost-benefit of 2 port RS232-to-Ethernet adapter/gateway

Device Model	Manufacturer	Security Features	Approx. Cost (CDN)
IOLAN SDS1 W	Perle	SNMP v3	$616
SGX5150202US	Lantronix	SNMP v3	$577
ED2100002-01	Lantronix	SNMP v2	$292
USR-N520	USR-IoT	No security (HTTP only)	$102

Outdoor security cameras typically already have high security features included, however camera cost could be optimized by application, if there is only a fixed view needed, there is no need to overpay (up 2x more) for an optical zoom and PTZ features. There seems to be also big price difference (up 2.2x more) between vendors for similar equipment, the following table highlights the price differences. One justification for higher price of Axis cameras could be better product support in terms of management control applications.

Cost-benefit of Security Video Cameras

Device Model	Manufacturer	Features	Approx. Cost (CDN)
DS-2CD4585F-IZH	Hikvision	Fixed pos., no opt. zoom, UHD res.	$1,100
DS-2DF6236-AEL	Hikvision	PTZ, with optical zoom, HD resolution	$2,000
WV-SW598A	Panasonic	PTZ, with optical zoom, HD resolution	$4,400
Q6128-E	Axis	PTZ, with optical zoom, UHD resolution	$3,650

Flexibility and ease of deployment

Security/Traffic Cameras are fairly flexible and easy to deploy as there exist a lot of standard installation options (pole, or wall mount), some Camera manufactures also supply outdoor rated power supply units for these cameras, however, others do not.

Note that not all the cameras use the same standard supply power interface and protocol, and thus in case of multi-vendor camera and other IoT devices deployment this could lead to non-uniform power supply installation requirement.

These differences result from the fact outdoor industrial temperature range cameras need a lot more power than a typical PoE standard can supply. For example, Axis -40 C rated outdoor camera will need “Axis High PoE midspan 60W”, however this midspan may not be compatible with other cameras and/or other IoT devices or wireless bridges.

Currently there are a couple of Power over Ethernet PoE standards for low and medium power devices, and there are other standards in development for higher power devices. The following table list these PoE versions.

PoE standards summary

	Power available at Powered Device PD	Maximum power delivered by PSE	Voltage range (at PSE)	NOTE
802.3af (802.3at Type 1) "PoE"	12.95 W	15.40 W	44.0–57.0 V	IEEE Standard
802.3at Type 2 "PoE+"	25.50 W	30.0 W	44.0–57.0 V	IEEE Standard
802.3bt Type 3 "4PPoE"	51 W	60 W	44.0–57.0 V	In dev.
802.3bt Type 4	71 W	100 W	44.0–57.0 V	In dev.

Ref. https://en.wikipedia.org/wiki/Power_over_Ethernet

All of the reviewed cameras, and most of the other IoT devices tested, also have option to accept 24V DC power supply, with varying current/power load (depending on the device) requirement. Thus for uniformity of deployment, a standard 2.5A (60W) rated 24V DC power supply unit could be used for most, if not all, of IoT devices deployments. Note that this alternative, might add a requirement of separate pair of power supply wires to the camera.

Other IoT sensor devices should also be fairly easy to deploy, although depending on the particular sensor or device some customized packaging or installation fixture might be necessary. For example, installation of Microphone sensors at the camera location, or data interface adapter for Traffic Radar sensor, or RFID readers will need some customized design and installation. In general, a 3rd party design and installation team might be needed to help Ville de Montreal with complete end-to-end IoT devices deployment.

Total cost of ownership

Based on experience with this pilot deployment project, it is clear that besides initial investment in the IoT devices equipment and installation, a dedicated team of technicians and IT specialists (at VdM or subcontracted) would be needed to keep the deployed IoT devices operational/maintained (normal equipment failures, accidental failures, physical misconfigurations/alterations), properly monitored, controlled and kept updated in terms of evolving network security, which would add to the cost ownership. Total cost of ownership would need to be evaluated on a specific deployment case scenario.

Sensor life cycle

For security of the whole IoT network purposes, IoT sensors and network devices should be never be deployed with factory default configuration, all factory default login credentials should be removed, for normal operation only the needed login account and needed communication protocols/ports should be enabled on the devices, broken or our-dated IoT devices should be disposed of with care, to make sure there is no information left on the device which could compromise network security. If possible reset device to factory defaults before disposing.

The life time of the IoT device depends on the device itself, some of the security cameras (for example AXIS) have 3 year warranty, other items, such as wireless bridges, have a typical 1 year warranty. Some

manufactures could offer extended warranty at extra cost, and could be negotiated during the procurement.