GlobalLogic®

The Role of Telecommunications in Smart Cities

Rohit Kumar Sethi
Senior Solution Architect, GlobalLogic Inc.

A smart city uses digital technologies or information and communication technologies (ICT) to enhance the quality and performance of urban services, reduce costs and resource consumption, and engage more actively with its citizens. By effectively leveraging telecommunications technologies, smart cities can connect various “things” (e.g., sensors, devices, analytics tools, etc.) to each other, either directly or via the Internet.

This white paper will explain the mechanics behind smart cities and how they leverage telecom technologies to connect all these various things.

www.globallogic.com

Table of Contents

Introduction

A “smart city” is one that marries both traditional infrastructures (e.g., buildings and transportation) and modern communication infrastructures (e.g., information & communication technologies) to fuel sustainable economic growth and a high quality of life.

The below figure identifies the typical focus areas of a smart city. It should be noted that many players in the telecom space are now directing their efforts towards developing new services for these focus areas.

The foundation of any smart city is a modern smart infrastructure that is composed of devices that are connected through telecom networks back to data repositories, where all the data gathered from these devices is stored. This data is leveraged by various systems and platforms to make decisions and initiate activities, and to address the needs of users via services and applications.

In this white paper, we will outline the challenges of adapting a city to smart technology and the various telecom options available for integrating sensors, gathering data, and processing it effectively.

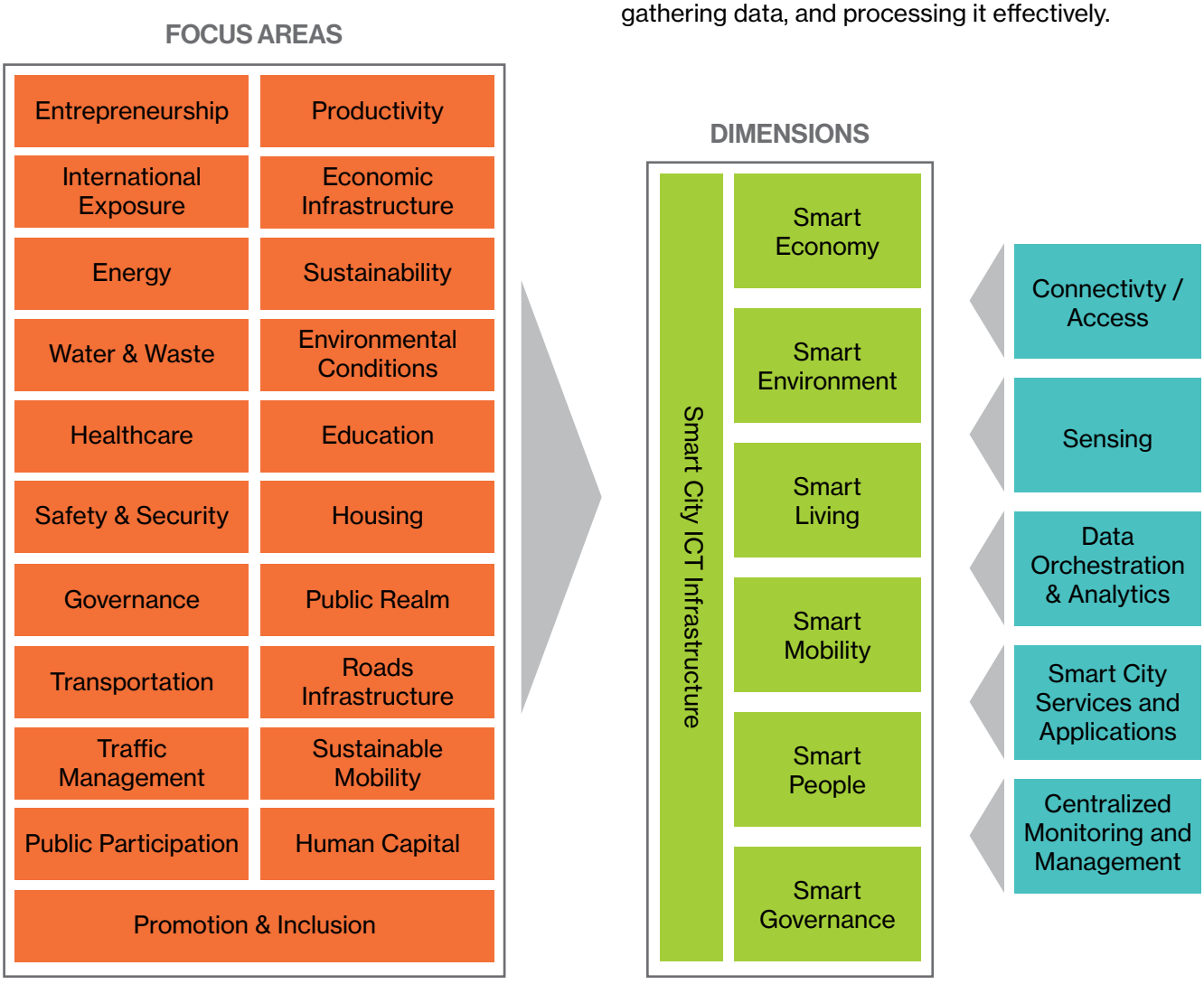

Figure 1. Smart City focus areas

The Challenges of Creating a Smart City Infrastructure

Although the benefits of a smart city infrastructure are great, so are the challenges. For example, since IoT solutions are complex, end-to-end systems, there tends to be excessive vendor specialization and segmentation. The sheer amount of different standards and proprietary initiatives between technology vendors can make it difficult to integrate all these varying devices into a single architecture, which (as seen in the below figure) can be quite complex.

Similarly, once a city does have a network in place, it must find a way to effectively aggregate, secure, analyze, and share the huge amounts of data that the sensors gather.

These challenges are very important to consider, but since this white paper is focused on the telecom requirements of smart city networks, we'll take a deeper look at the protocol and connectivity issues facing large-scale IoT ecosystems.

First of all, sensors must consume low battery power in order to be efficient devices in a smart city infrastructure. They must also be relatively low-cost in order to create a large network across a city or district level. This combination of low power requirements and cost restraints can unfortunately results in sensors and sensor node devices that have very limited processing, memory, and bandwidth capabilities -- thereby requiring specific protocols to function successfully.

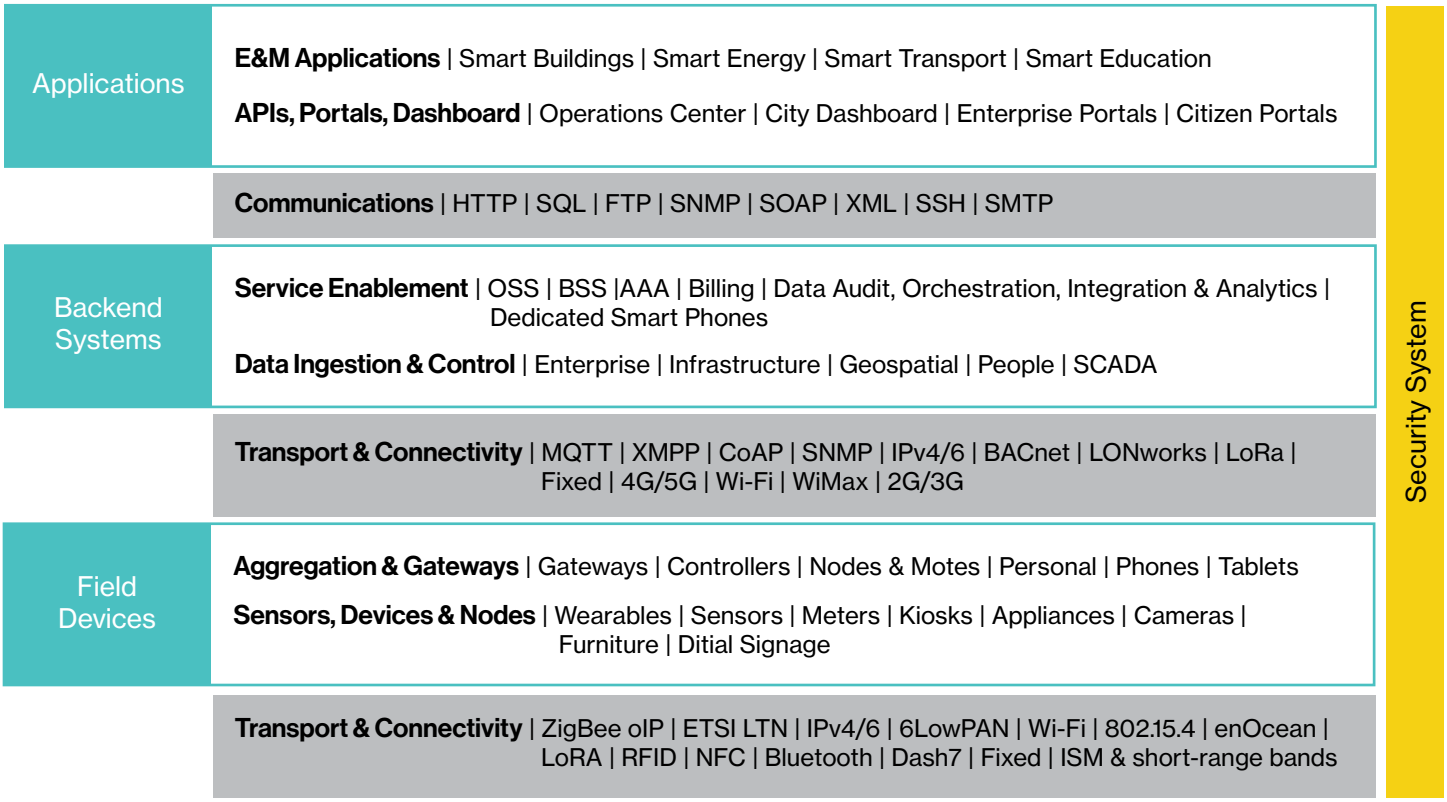

Figure 2. Typical architecture required to implement IoT smart services

Cities must also take into consideration how their devices will transmit data since a typical IoT ecosystem involves multiple sensors that are tailored for a specific purpose, from detecting cracks in a building to measuring the distance between cars on a highway.

Each one of these sensors may utilize a different radio connectivity solution to transmit its gathered data to backend systems, whether wired or wireless. For example, because there is limited availability of IPv4 addresses due to its addressing structure, sensor networks require IPv6 addresses to route data across the Internet.

Let's now take a look at the various wireless connectivity and protocol options currently available for implementing an IoT city infrastructure.

Wireless Connectivity Options for IoT Ecosystems

As I mentioned in the previous section, the range of available, unlicensed frequencies for wireless connectivity in IoT networks is fairly limited. Excluding NFC, there are four bands that are widely available (although not in every country) and utilised by wireless protocols: 433MHz, 868 MHz, 900MHz and 2.4GHz. The latter is shared by protocols such as IEEE 802.11 Wi-Fi and Bluetooth.

Among these four bands, there are several protocols (including many proprietary ones). Below is an overview of the most well-known protocols, as well as a table that summarizes the total range of available options for wirelessly transmitting data in a smart city IoT ecosystem.

Radio Type	Protocol	Frequency	Throughput	Range
3G, GPRS, 4G	UMTS, GPRS, LTE	850/900/1800/1900/2 IHz MHz Other	>Mbps	- Km - Typical carrier
Bluetooth Low Energy	Bluetooth /Bluetooth Smart	2.4GHz	1Mbps	100m
DASH7	RF – ISO/IEC 18000-7	433MHz	200Kbps	2Km
EnOcean	RF – ISO/IEC 14543-3-10	868MHz,900MHz	125kbps	300m
ETSI LTN	802.15.4	868Mhz	50Kbps	40Km
LoRa	RF	433, 868 and 900 MHz	0.3 Kbps to 50 kbps	22km
Wavenis	*RF*	*868MHz,900MHz, IHz*	*19.2Kbps*	*1Km*
Wi-Fi	802.11	2.4GHz	>Mbps	50m500m
ZigBee and ZigBee Pro	802.15.4	2.4GHz,868MHz,900	250Kbps	7 to 12Km
Z-Wave	RF	868MHz,900MHz	100Kbps	30m

Figure 3. Smart city wireless transmission options

LoRA
IBM and Semtech have created an alliance to promote the usage of the LoRAWAN wireless protocol. According to the LoRA alliance, LoRaWAN is a Low Power Wide Area Network (LPWAN) specification intended for wireless battery operated things in regional, national, or global networks. LoRaWAN targets key requirements for IoT systems, such as secure bi-directional communication, mobility, and localization services. Communication between end-devices and gateways is spread out on different frequency channels and data rates, which range from 0.3 kbps to 50 kbps. LoRA is very promising when low throughput is to be sent over very long distances, so it is likely to become a key protocol for sensors in the coming years, especially with the type of players backing the technology (i.e. IBM, Cisco, etc.).

Wavenis
Promoted by the Wave2M Community, Wavenis can be used for applications such as metering, home monitoring, and active RFID applications. Its typical rate is 19.2kbps. However, the Wave2M community recently announced its dissolution, stating that "Wave2M (is) a technology that no longer has a unique point of differentiation compared to others used in the market."

Zigbee
ZigBee is an IEEE 802.15.4-based specification that runs over 868MHz, 900MHz, and 2.4GHz, and it has a defined rate of 250 kbit/s (i.e., best suited for intermittent data transmissions from a sensor or input device). The technology defined by the ZigBee specification is intended to be simpler and less expensive than other WPANs. ZigBee's low power consumption limits transmission distances to 10–100 meters line-of-sight, depending on power output and environmental characteristics. It is typically used in low data rate applications that require long battery life and secure networking (ZigBee networks are secured by 128 bit symmetric encryption keys.)

Z- Wave
Supported by over 250 manufacturers in the Z-Wave Alliance, Z-Wave is used primarily for home automation systems because (1) it is easily embedded into consumer electronics devices and (2) it minimizes power consumption (i.e., best suited for battery-operated devices). Z-Wave runs on 868MHz and 900MHz over a 30m range and is designed to provide reliable, low-latency transmission of small data packets at data rates of up to 100kbit/s (unlike Wi-Fi and other IEEE 802.11-based WLAN systems).

LTE
Long Term Evolution (LTE) is a wireless data communications technology that is based on GSM/UMTS standards. Although the LTE registered trademark is owned by the European Telecommunications Standards Institute (ETSI), other nations and companies do play an active role in the project. The goal of LTE was to increase the capacity and speed of wireless data networks using new digital signal processing (DSP) techniques and modulations that were developed around the turn of the millennium. It also aimed to redesign and simplify the network architecture to an IP-based system with significantly reduced transfer latency compared to the 3G architecture. The LTE wireless interface is incompatible with 2G and 3G networks, so it must be operated on a separate radio spectrum.

Wi-Fi
Wi-Fi is a local area wireless computer networking technology that allows electronic devices to network, mainly using the 2.4 gigahertz (12 cm) UHF and 5 gigahertz (6 cm) SHF ISM radio bands. The Wi-Fi Alliance defines Wi-Fi as any "wireless local area network" (WLAN) product based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards. However, the term "Wi-Fi" is used in general English as a synonym for "WLAN" since most modern WLANs are based on these standards.

Many consumer electronic devices can use Wi-Fi, as they can easily connect to a network resource such as the Internet via a wireless network access point. Such an access point (or hotspot) typically has a range of about 20 meters indoors and a greater range outdoors. Hotspot coverage can be as small as a single room with walls that block radio waves, or as large as many square kilometres (achieved by using multiple overlapping access points).

Communications Protocol Options for Backend Systems

Whether wired or wirelessly connected, communications protocols are required to run over the physical and link layers. Communications protocols enable field devices, controllers, and gateways to be remotely configured and managed.

They also ensure that the information gathered from these devices reach their intended destinations, whether that is a data repository, application, display, or control center. For each IoT ecosystem, communications protocols can be grouped into four categories:

1. Gateway/controller to end device
2. Backend systems to gateway level
3. Internal to backend systems
4. Applications to backend systems

Backend internal communications are comprised of an especially large number of protocols because they are heavily dependent on interfacing/integration systems and platforms. In this next section, we'll focus on communications protocol options for (1) the backend system to gateway level pathways and (2) the application to backend system pathway. Below are examples of protocol options for these two pathways:

LonWorks and BACnet
These platforms are typically used for monitoring and controlling of lighting, energy, HVAC and building/home automation systems. It may be integrated with IP.

CoAP
Constrained Application Protocol (CoAP) is an application-level protocol that is designed for low-bandwidth sensors and devices. It can be used in conjunction with 6LoWPAN, which is highly compatible with HTTP.

ModBus
This serial communication protocol is generally used by SCADA systems for monitoring and controlling devices that may run over TCP/IP.

MQTT
Message Queue Telemetry Transport (MQTT) is a messaging protocol that can be used between a broker and field devices. It can also be utilized with TCP/IP or over non-IP networks such as non IP Zigbee.

RESTful HTTP
This is a simpler alternative to Simple Object Access Protocol (SOAP) and WSDL-based Web services. It uses HTTP commands.

XMPP
XMPP is a communications protocol that runs over TCP. Efficient XML compression (EXI) techniques (as defined by XMPP.org for XEP-322, XEP-323 and XEP-324 specifications) aim to enhance this protocol for IoT usage. XMPP was formerly known as Jabber.

Leveraging IoT Platforms

Taking into account the complexity of implementing the different architectural layers of an IoT ecosystem, as well as the necessity of selecting the right protocols and components, the task of creating a smart city can seem daunting. Thankfully, the market offers a variety of IoT platforms such as n.io, Thingworx, and Sensorflare to help make this transition easier. These IoT platforms typically implement the below functionality:

- Rapidly develop and implement applications through open APIs
- Display IoT information (e.g., readings, list of sensors, locations)
- Integrate IoT-related technical implementations for the required enterprise support systems (e.g., OSS, BSS)
- Remotely configure, control, and manage any type of device (e.g., controllers, devices, appliances)
- Gather, process, broker, share, transform, and analyze data from field devices
- Implement IoT-specific wireless solutions
- Specialized functionality for specific industries / markets (e.g., energy, automotive, etc.)

Of course, no single platform can provide all the functionality required for a network that spans an entire city and all of its properties, sensors, and specialized requirements. This is why it's crucial to partner with an IoT consultation partner who can select the best platforms available, tailor them to a city's specific needs, and implement and manage the system.

Conclusion

While protocol standardization and limited wireless connectivity options remain roadblocks in implementing IoT across a large ecosystem, sizeable industry efforts are being made to resolve them. Leveraging an IoT platform can aid cities in managing their extensive network of connected devices and sensors, as well as the huge amount of data that will be gathered through them.

It is equally crucial for city managers to partner with an IoT integration partner who can help recommend the right technologies, implement the different platforms and/or components necessary for a city's specific needs, and further manage and/or consult on ongoing initiatives. In addition to streamlining the IoT implementation process, contracting with one or more technology vendors frees up city managers to focus on long-term strategies for their smart cities rather than day-to-day management tasks.

References

- https://en.wikipedia.org/wiki/Internet_of_Things
- http://www.nxn.ae/wp-content/uploads/2015/08/Smart-City-and-the-Internet-Of-Things1.pdf
- https://en.wikipedia.org/wiki/LTE_(telecommunication)
- https://en.wikipedia.org/wiki/Smart_city

About the Author

Rohit Kumar Sethi is a Senior Solution Architect at GlobalLogic's Noida facility. With over 14 years in the IT and Telecom industries, Rohit's focus areas include testing VoIP telephony-based products and solutions that use protocols defined by IETF, ETSI, ITU-T, and 3GPP international standardization bodies. He is currently exploring new areas of testing in the field of Telecom OSS and BSS.

About GlobalLogic Inc.
GlobalLogic is a full-lifecycle product development services leader that combines deep domain expertise and cross-industry experience to connect makers with markets worldwide.Using insight gained from working on innovative products and disruptive technologies, we collaborate with customers to show them how strategic research and development can become a tool for managing their future. We build partnerships with market-defining business and technology leaders who want to make amazing products, discover new revenue opportunities, and accelerate time to market.

For more information, visit www.globallogic.com