VC-D-004E-1.0.0

iNode Reference Manual

July 1st, 2015

M2M Solutions
Sensor Solutions

Valley Campus Japan, Inc.

Table of Contents

Version	Date	Revision	Name
1.0.0	2015/07/01	Initial Release	T. Kitahara

1. Summary

This document describes the role and functions of iNode.

iNode is a network node device in the internet. iNode performs gateway functions in the internet system utilizing leading edge technologies in the internet application, cloud computing, client-server computing, and mobile computing.

2. The role of iNode

iNode is one of the key components in the internet to configure the scalable network system to fulfil specific business needs.

iNode generally connects with two different networks. The internet is an upper network to iNode. iNode connects wired or wireless with the internet. The lower network to iNode is device network such as various sensors and application specific devices. iNode connection with the lower network is also wired or wireless. iNode is a gateway combining those upper-network and lower-network

iNode is under control of the cloud server located in the internet. The cloud server controls and manages various devices in the lower network via iNode gateway.

VCJ provides Platform services in the cloud server. VCJ Platform services interfaces user application developed for specific business needs.

Business application, fully utilizing VCJ Platform services, can collect the current status of the target network and control various network devices. (Fig.1.)

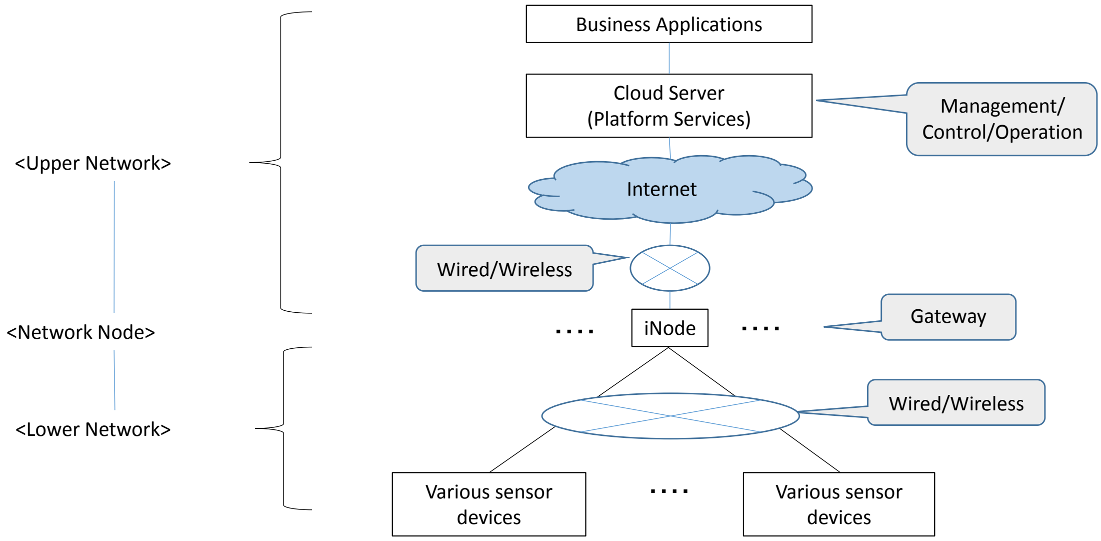


Fig. 1. iNode positioning and its role in Internet system

3. The functions of iNode

iNode receives commands from business application via VCJ Platform services. iNode interprets command and send relative command to lower network devices. iNode, as a gateway, sends device data collected from the lower-network to the business application via VCJ Platform services and sends control parameters to various devices in the lower-network. iNode converts protocol/format when necessary.

4. The network interface of iNode

4.1. The upper network interface of iNode

iNode has the following interfaces to connect with the internet, the upper-network. (Fig.2)

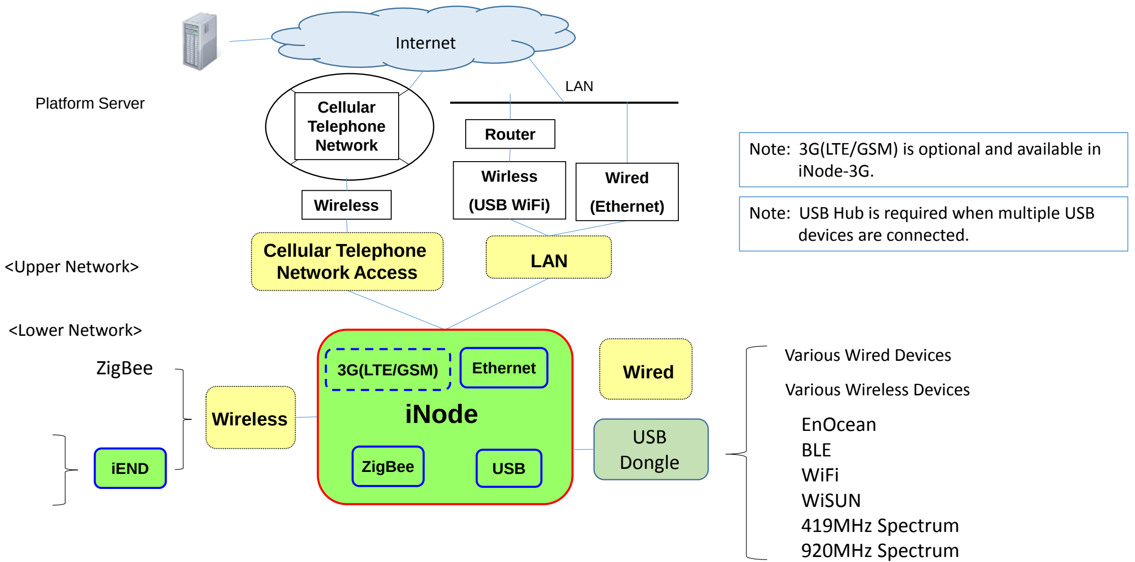
(1) Wireless interface

A. 3G modem (LTE/GSM): Internet access via cellular telephone network

B. WiFi (USB connection): Internet access via wireless router

(2) Wired interface

A. Ethernet (LAN cable connection): Internet access via LAN



Note: 3G(LTE/GSM) is optional and available in iNode-3G.

Note: USB Hub is required when multiple USB devices are connected.

Fig 2. iNode Network Interface

4.2. The lower network interface of iNode

iNode has the following interfaces to connect with various devices in the lower network.

(1) Wireless interface: B – G are connected by USB dongle

A. ZigBee (2.4GHz/920MHz)

B. EnOcean

C. BLE (Bluetooth Low Energy)

D. WiFi (Wireless Fidelity)

E. WiSUN

F. 419MHz

G. 920MHz

(2) Wired interface

A. USB: USB hub is required when multiple USB devices are connected.

5. Devices supported by iNode in the lower-network

iNode supports the following devices in the lower-network.

<Wireless interface>

ZigBee devices are connected directly with iNode.
Other devices are connected with iNode via iEND which has adapter function to iNode.
(iEND is another product of VCJ.)

(1) ZigBee

iNode complies with ZigBee standard and supports HA Profile (Home Automation Profile).

ZigBee Home Automation Profile includes various home devices for lighting control, HVAC management, energy saving, security management, etc. which enables to build a “smart home”.

The following are ZigBee compliant devices. Most of them are battery powered and easy to install anywhere without power cabling problem.

A. Power sensor (CT type, Consent type, Precision type)

B. Light sensor

C. Temperature/Humidity sensor (indoor/outdoor)

D. Motion detector

E. Window sensor

F. Window breakage sensor

G. Gas detector

H. Smoke detector

I. Alarm

J. Switch

K. Dimmer control

L. RS232C ZigBee Adapter
M. RS485 ZigBee Adapter

(2) EnOcean

EnOcean device operates without battery. An EnOcean device is connected wirelessly with iNode through USB dongle. The following devices are some EnOcean device examples.

A. Lighting switch
B. HVAC controller
C. Window sensor
D. Motion detector

(3) BLE (Bluetooth Low Energy)

BLE operates with low power and can be connected wirelessly. BLE uses 2.4MHz and transmission speed is up to 1Mbps. A single button battery may run BLE device for several years in some case. BLE is expected to use for various sensors and wearable devices.

BLE devices are connected wirelessly with iNode through USB dongle.

(4) WiFi

WiFi is well known as “Wireless LAN” technology. Transmission distance reaches up to 50-60 meters and transmission speed is Max. 54Mbps.

WiFi devices are connected wirelessly with iNode through USB dongle.

(5) WiSUN (under development)

WiSUN has been adopted as wireless transmission standard for next generation smart power meter in Japan. Meter reading of various infrastructure related meters such as power, gas, water, etc. are target application currently under development. WiSUN power consumption is not as low as ZigBee but WiSUN sends data at higher speed than ZigBee. 2.4GHz or 920MHz spectrum is used.

WiSUN devices are connected wirelessly with iNode through USB dongle.

(6) 419MHz spectrum

419MHz devices are connected wirelessly with iNode through USB dongle.

(7) 920MHz spectrum

920MHZ devices are connected wirelessly with iNode through USB dongle.

<Wired interface>

(1) USB

USB Devices can easily be connected with the internet by way of connecting with iNode. Web cameras, LCD monitors, audio speakers, etc. are available with USB interface.

USB devices can be connected with iNode by putting the USB cable to the USB jack. USB hub is required when multiple USB devices are connected.

6. iNode M2M network system API

Development process of M2M network application system using iNode is as follows.

iNode complies with ZigBee standard and supports HA Profile (Home Automation Profile).

In order to explain iNode M2M network system API, this manual assumes a typical M2M network system configuration with iNode and ZigBee sensors. When other devices than ZigBee sensors are used in the target network, API is to be modified and enhanced to accommodate related requirements. The following API is standard and basic API in M2M environment.

6.1. System configuration

The iNode M2M network system consists of the M2M cloud server in the internet and the iNode gateway system in the remote location. The iNode gateway system is configured by iNode and a number of ZigBee sensors wirelessly connected to iNode. The M2M cloud server interfaces with user application and provides M2M gateway platform services regarding system configuration management and system operation. (Fig.3.)

iNode has to be registered at M2M cloud server when iNode is deployed in the target network system. A M2M client device (PC/Smart phone) specifies system configuration by accessing the management page of M2M cloud server. A M2M client device can add, delete, and change iNode and ZigBee sensor via the administration page of VCJ M2M cloud server .

iNode is connected with M2M cloud server wired or wireless.

Communication between iNode and M2M server is done in REST-XML.

Communication between user application and M2M cloud server is done in REST-JSON.

When M2M client devices (PC/smart phone) are used in the application, communication between M2M client device and user business application is recommended to use industry standard protocol such as HTTP/JSON

iNode configures ZigBee sensor network. And receiving the commands from user application via M2M cloud server, iNode collects data from the sensors and sends them to user application via M2M cloud server. M2M server sends commands to iNode and iNode interprets them and controls sensors accordingly. M2M cloud server can monitor and control remote sensors & devices over the internet via iNode using VCJ iNode M2M API.

M2M cloud server command can update iNode firmware remotely.

A single iNode can accommodate up to 30 ZigBee sensors. There is no limit in the maximum number of iNode in a system.

ZigBee sensors are battery powered. iNode requires commercial power source (not battery powered).

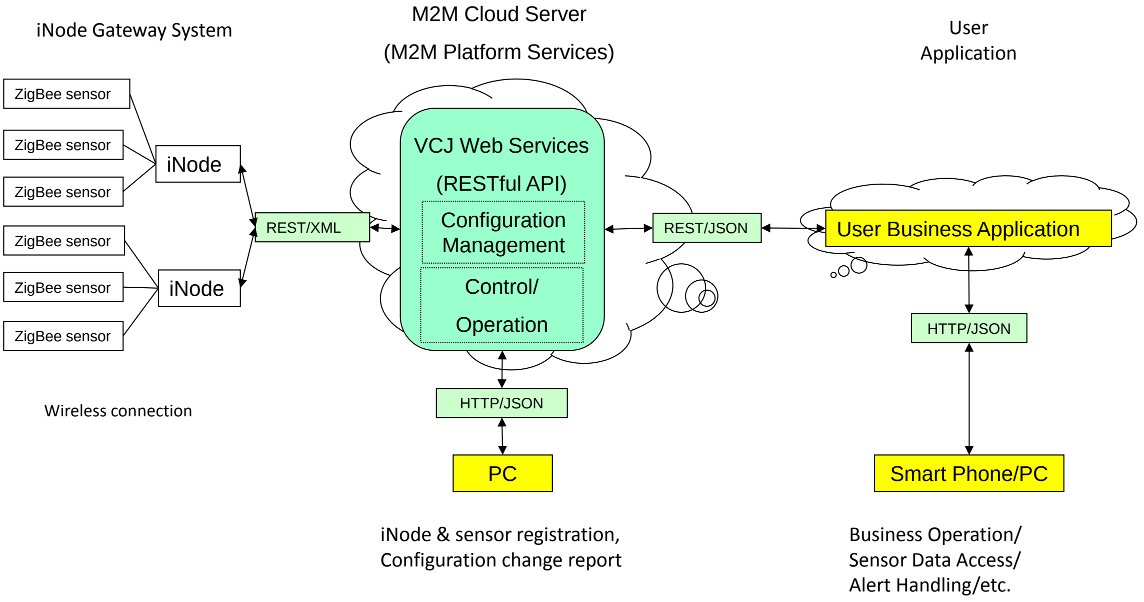


Fig 3. iNode M2M Network System Configuration Concept

6.2. iNode registration and ZigBee sensor network installation

Every iNode and ZigBee sensor has unique manufacturer-defined IEEE 64 bit address given at manufacturing site. iNode and ZigBee sensors are shipped with this unique IEEE 64 bit address information.

iNode registration to M2M cloud server is done by M2M client devices (PC/smart phone) accessing VCJ M2M Platform service management page after iNode power on.

ZigBee sensor is enrolled to iNode network when the sensor is set power-on near the iNode and a procedure of switch manipulation is completed. Once iNode acknowledges the sensor by IEEE 64 bit address, iNode automatically configure the ZigBee network and manages the sensor using the IEEE 64 bit address. Correspondence of the IEEE 64 bit address of the sensor to the operational name and the physical location of the sensor have to be carefully designed from efficient system operation perspective.

6.3. VCJ Sanctuary M2M Platform Services

(Fig 4. VCJ Sanctuary M2M Platform Services)

VCJ Sanctuary is a name of VCJ M2M Platform Services. VCJ Sanctuary M2M Platform Services consists of ZigBee device services and M2M application services.

(1) ZigBee device services
   - A. iNode (gateway) control
   - B. ZigBee sensor control
   - C. System configuration control

(2) M2M application services
   - A. Web application interface
   - B. M2M command: GET/POST/PUT/DELETE
   - C. iNode (Gateway) management
   - D. ZigBee sensor management

User business application issues M2M command ((2)-B.) to control iNode and ZigBee sensor. Interface protocol is industry standard REST-JSON. OAuth2.0 and SSL are used for security.

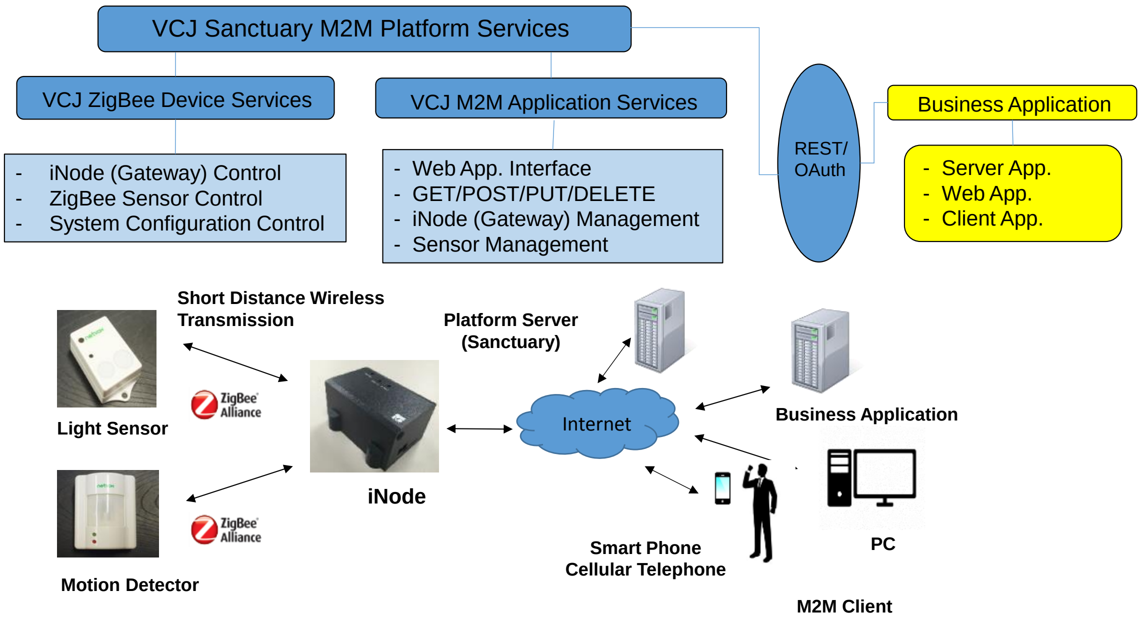

VCJ Sanctuary M2M Platform Services
VCJ ZigBee Device Services
VCJ M2M Application Services
- iNode (Gateway) Control
- ZigBee Sensor Control
- System Configuration Control
- Web App. Interface
- GET/POST/PUT/DELETE
- iNode (Gateway) Management
- Sensor Management
REST/ OAuth
Business Application
- Server App.
- Web App.
- Client App.
Short Distance Wireless Transmission
Light Sensor
ZigBee Alliance
ZigBee Alliance
Motion Detector
iNode
Platform Server (Sanctuary)
Internet
Business Application
Smart Phone Cellular Telephone
PC
M2M Client

Fig 4. VCJ Sanctuary M2M Platform Services

6.4. VCJ Sanctuary operation outline

Outline of VCJ Sanctuary M2M Platform Services operation is as follows. (Fig. 5.)

(1) Account registration

In order to use VCJ Sanctuary, user account registration is required. VCJ Sanctuary Web page has user registration page that can be accessed by M2M client (PC/smart phone)

(2) Registration and parameter setting of iNode and ZigBee sensor

M2M client (PC/smart phone) accesses VCJ Sanctuary Web page to register iNode and ZigBee sensor. Parameter setting of iNode and ZigBee sensor is done also by M2M client. Configuration change, addition and deletion of iNode/sensor are done via VCJ Sanctuary administration page.

When a user wants to use application program to manage iNode and sensors without M2M client manipulation, the user has to develop application program issuing M2M command to do the management function.

(3) Sensor data collection and system operation

Once iNode and ZigBee sensor are registered and parameter setting is done, the sensor network starts to operate accordingly. Data collection is done as scheduled or on demand, and collected data is sent to M2M cloud server via iNode. Data collection and reporting can be done as scheduled or on demand by prior parameter setting.

Alert can be detected and reported to user business application via M2M cloud server by prior proper parameter setting.

Receiving sensor data from iNode via M2M cloud server, user application can send sensor data to M2M client (PC/smart phone). When alert is reported, M2M client can send related command to remote network device via VCJ Sanctuary through iNode.

Usually sensor parameter setting/change is done by M2M client but, if necessary, user business application can do so by issuing VCJ Sanctuary command.

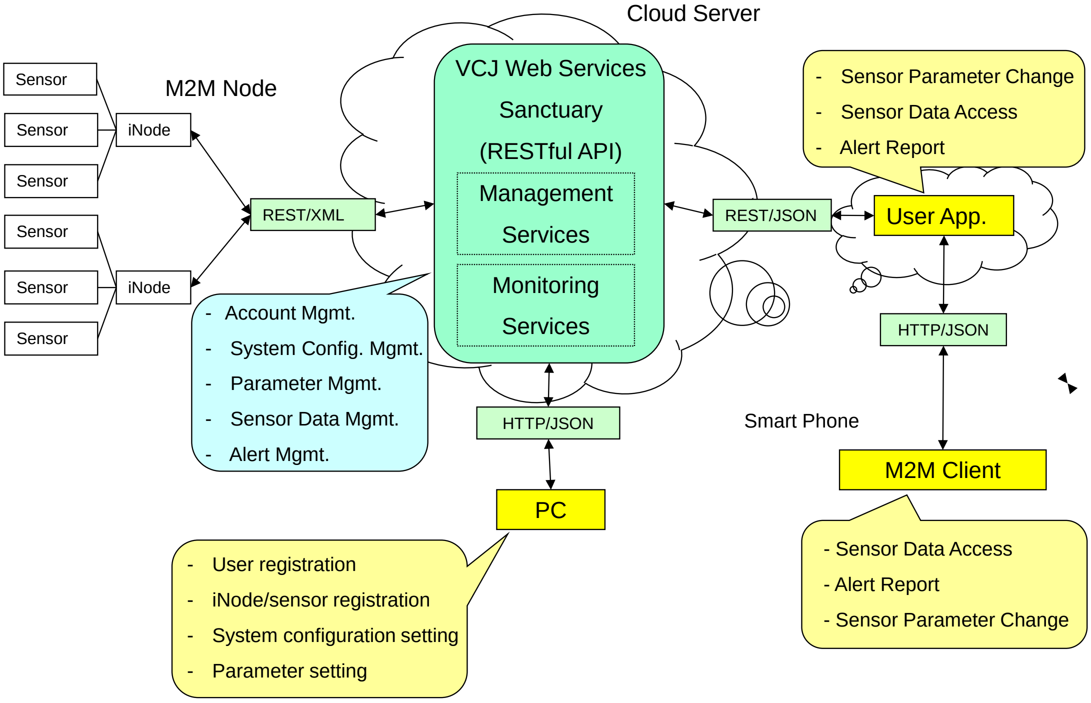


Fig 5. VCJ Sanctuary M2M Platform Service Functionality