IoT Based Smart Services

Jingjing.chen, jingjing.chen (at) go.wustl.edu (A paper written under the guidance of Prof. Raj Jain)

Abstract

IoT Based technology and contracture mode are a core stone for constructing proactive and predictive network smart service. A series of related technologies and intellectual options have driven transformations within every industry. IoT Based Smart Services has two essential components, that is, collection system and management system. The collection system is a smart agent systems on the managed devices gathering the device and network information via numerous methods, for instance, Simple Network Management Protocol (SNMP) requests, Command-Line Interface (CLI) commands, Netflow aggregates. They perform one or two of the FACPS (Fault, Accounting, Configuration, Performance, and Security) management requirements. The data collection systems collect information from various sensors/entities and transfer to local and/or global service management systems for further process. In the management system, the network communication protocols are crucial. This paper explores Bluetooth Low Energy and 6LoWPAN, and the possibility to apply both of them. Based on the query of whether the IoT is end of cloud computing, the smart distributing system has been studied in Part 3 as one of significant component of data processing architecture. In the last part, other important technologies involved in the data processing and managing will also be discussed like signal processing, reconstruction technologies, Artificial intelligence (AI) and RFID technology.

Keywords

Networking, Network Management, Collection System, Management System, Smart Technologies, SNMP, CLI, Netflow, Distributed System, 6LoWPAN, BTLE

Table of Contents:

1. Introduction
2. Collecting Data for IoT Based Smart Service
   2.1 Simple Network Management Protocol
   2.2 Command Line Interface
   2.3 NetFlow Protocol
   2.4 Other Data Collection Protocol
3. Communication Support of IoT-based Smart Service
   3.1 Bluetooth Low Energy
   3.2 6LoWPAN
4. Data Processing Services of IoT-based Smart Service
   4.1 The Centralized Management Model and the Distributed Management Model
   4.2 Stream Processing System
   4.3 Alternative Approaches for Better Data Reconstruction and Decision Making
Conclusion
References
Appendix A - List of Acronyms

1. Introduction

The Internet of Things (IoT) is a recent communication paradigm that has made plenty of headlines. The basic idea is that any "thing" or object, embedded with MCU (micro-controllers) and transceivers, may be able to communicate with one another through internet or any other protocols. It has potential power to transform nearly every industry, from manufacturing segment to Smart Homes or cities industry, from eHealth to IT infrastructure, changing the way we live and work, locally and globally. As the world becomes more connected via IoT, network suppliers are asking themselves why they forgo some essential feedback information from their products when they can sell related service, as they have ability to develop enough advanced technologies to monitor the functionality of devices and analyze response information.[cisco01] A lot of network company have commissioned numerous studies on it, like Cisco, IBM and GE. As one of proponents of the trend toward the IoT, Cisco has predicted that IoT installation base will increase to 26 billion by 2020 and the connected devices will spread across the entire globe. [Gartner01]

Regardless of the underlying vertical (in manufacturing industry, home security or in health care services), Smart Service is a broad conception that integrates all services that use automated and technology-enabled connectivity and intelligence to more effectively deliver better insights and predictability through smart analysis.[Cisco02] It is comprised of rich intellectual capital, real-time tools, analytics, and automation.[Cisco03] The core of smart service is the Smart Agent and Collection System that discovers the network and captures all required FACPS (Fault, Accounting, Configuration, Performance, and Security) parameters. The collected information could be transferred via machine-to-machine interface to the smart service back end. The technologies under this process include Simple Network Management Protocol (SNMP), Command-Line Interface (CLI), and Netflow. They perform one or two of the FACPS management requirements. At the back end, which is typically deployed at the vendor or partner (like Cisco), they proceed the collected data through their intellectual database. The reports or notifications are proactively produced based on that. Therefore how to communicate these data to management center is significantly important. There are many different delivering methods to implement that task, like WiFi, Bluetooth, and IPv6 over Low power Wireless Personal Area Networks. (6LoWPAN) The common way in Smart health care industry is BluetoothAc Low Energy and 6LoWPAN. To solve the query on whether the IoT is end of cloud computing, the smart distributing management system mode and central management system mode will be discussed. The prediction that hybrid system model will be the future development trend will be present in Section four. Other important technologies involved in the data processing will also be discussed like signal processing, reconstruction technologies, artificial intelligence (AI) and RFID technology.

http://www.cse.wustl.edu/~jain/cse574-14/ftp/iot_ssvc/index.html
2. Collecting Data for IoT Based Smart Service

The first step to advanced analytics is to collect the right kind and quality of information. That requires an external collection system or smart agent on the devices to gather the information of device and network. They allow network administrators monitor the connections between them, the functionality of the network devices, and the services they offer. They mainly include the following three technologies, Simple Network Management Protocol (SNMP), Command-Line Interface (CLI), and Netflow.

2.1 Simple Network Management Protocol

An example for how input of such data for IoT-based services can be collected is the Simple Network Management Protocol (SNMP), which is developed by the Internet Engineering Task Force (IETF) in the late 1980s for essential FACPS management. It proved to be a very popular de facto standard for network management. It has been used as a network management tool for the Cisco Smart Care Service[Cisco02]

SNMP is the most basic method of gathering bandwidth and network usage data that allows for external monitoring of changing the state of some SNMP-based device port-by-port. SNMP has four versions. SNMPv3, Version 3 of SNMP, described in RFC 2271 through RFC 2275, is a full IETF standard. SNMP is comprised of two entities: SNMP-capable devices (Agent) and Network Management Stations (NMSs). The agent is a piece of software that runs on the network devices (like router, switch, or Unix server) for collecting information. They can track of various operational aspects of the device. For instance, they could, monitor the state of each of its interfaces: which ones are up, which ones are down, collect management information about its local environment, and store and retrieves management information. NMS on the other hand, is a managing server running some kind of software system that can handle management tasks for a network, like polling and receiving traps from agents in the network. It is also responsible for performing responsive actions based on the data received from an agent.[Cisco03]

Once agents notice that bad thing has happened, they will alarm the NMS by sending SNMP traps information, as Figure 1 shows. While agents still perform collection operation via SNMP get or multi-get, NMSs make response, perform real-time local analysis and take some action. They even can page customer to let them know that something has happened while at same time agent send a response to NMS. If it is applied manufacturing industry, it would bend the traditional linear value chain into a "feedback loop" through which the heartbeats of manufactured objects transferred back the center.

![Simple Network Management Protocol](http://www.cse.wustl.edu/~jain/cse574-14/ftp/iot_ssvc/index.html)

2.2 Command Line Interface

In spite of what was originally intended, in recent years it becomes apparent that SNMP was not being used to configure network equipment, but was mainly being used for network monitoring, i.e. Performance Management and Fault. Because, in SNMP, When a NMS performs polling on network devices, for instance, to find out the central processing unit utilization, it would result wasting network bandwidth and missing the actual threshold on the polling interval. The alternative way to monitor configuration aspects of network devices such as configuration file, and inventory, is to use interface, by monitoring the number of broadcast packets received. A threshold of a variable on rising and falling it, data type, and interval would been set and hold as standard to make comparison. Once if the actual value exceeds or falls below it, notice will be sent.[Wikipedia01]

Besides, Command Line Interface (CLI) allows proactively monitor. It not only provides an alarm for the problem and but also initiates predefined automatic restoral processes that is possible to minimize downtime. Though most of devices will support CLI for configuration, SNMP normally could also be used for that if SNMP is well documented and support for a device. CLI is primarily for installation and setup commands, with additional configuration functionality.

2.3 NetFlow Protocol

A useful accounting management tool is NetFlow Protocol, which is a powerful tool used to capture IP Traffic for analysis. Though SNMP has already been a powerful tool to help people manage and troubleshoot their network, NetFlow has more impressive function on tracking CP/IP flows within the network. NetFlow as a necessary part for collecting IP traffic information in IoT network system enables the management center track the information package around the whole network from local IoT system to public internet. It also ensures that computing and network resources are used fairly by all groups or individuals who access them, by knowing who is using network service and for which purpose and accounting and charging back according to the resource utilizing level. The system could make proactively preparation, and reduce the computing load of network by then only send aggregated data. It also minimizes the possibility of error incident in network, and improves the performance of smart service. [Wikipedia02]

2.4 Other Data Collection Protocol

One of other ways in network management is Syslog. It is constructed to collect information on network, by sending syslog messages to a syslog server that act as event collector, in response to specific events. It permits separation of generating messages system from storing message system and allows the
software report and analyze these messages. When data collected by SNMP is not sufficient to satisfy individual device transactions requirements (because of SNMP's scope limitation), Syslog is necessary. For example, in a large Cisco switch a Syslog monitor has capability of holding 6,000 different types of events, which is much greater than a SNMP monitor, with only 90 trap notifications potential.

On the other hand, within some network SNMP is used to alert on critical actions, like the Hot Standby Router Protocol (HSRP) state changes. It allows people to dig deeper to the reason of state change, in addition to collecting transporting and collecting information. Compared with SNMP, the device sending the syslog message does not require any communication from the devices transporting or logging the message. As defined in RFC 3164, a network device can send Syslog messages on User Datagram Protocol (UDP) port 514 to a Syslog server. However it uses UDP without guarantee that they have delivered the information. [Cisco04]

3. Communication Support of IoT-based Smart Service

As one of critical components of Management System, the communication devices transfer data gathered by the sensing devices, which is then processed by local processing devices to the destinations identified by the local processing devices. Sometimes this could be as simple as sensing a room light, turning it on based on energy use, and after analyzing the data, automatically turning it off via an electronic mechanism. In health care industry, it could be as sophisticated as communication to sensor on diabetes patients to measure and process specifically the relevant clinical data, e.g. glucose level, blood pressure, weight etc. Or in manufacturing industry, it could be a feedback loop from sales of product to post-sales, from delivering to remote problems check. These solutions are deployed enterprise-wide, so that send and support expertise can proactively manage and optimize entire installed bases of assets at multiple customer locations. Once the data is remotely processed and new commands are generated, the communication node brings back the new commands to the local embedded processing nodes to execute a task. The IoT-based smart service encompass all aspects of one's everyday life, every corner of industry, hence there is no limit to the distances for which command and control communication can be used. Every communication techniques have their target application areas, just like Bluetooth Low Energy (BTLE), IEEE 802.15.4, and ZigBee etc. BTLE has traditionally targeted health applications, IEEE 802.15.4 manufacturing industry, ZigBee the power management.

Although the battle among ZigBee, 6LoWPAN and BTLE technologies for industrial control and automation still continue, the battle in health care industry and power industry seems to be settled down. The final winner in healthcare industry is BTLE. The power companies seem to have settled on ZigBee for the Smart Energy home area network (HAN). But all of them become decaying as 6LoWPAN development platform has been released for monitoring. Securing Home Building automation, and as devices in HAN are more likely using BTLE because they would work with inexpensive interface controller on smartphones and tablets. To work with Smart Meter is not decisive factor any more especially as there is no controller readily available.

3.1 Bluetooth Low Energy

BTLE has been adopted by health care industry for portable medical and lifestyle and the general management model has been held in this IoT segment now. It is embedded on many health and wellness devices already on the market, like wireless blood glucose monitors, heart rate monitors, weight scales and stethoscopes. Although BTLE is less complex compared to classic Bluetooth, low-energy feature make it become one of the best wireless communication options to periodically collect vital health information about consumers with a wide variety of medical conditions - even allowing healthcare providers to monitor patients while at home or on the go. BTLE as its name indicates can only consume only a fraction of the power of Classic Bluetooth radios (only 1% to 50%). The classic traditional Bluetooth technology is connection oriented. When a device is connected, a link is maintained, even if there is no data flowing. Although sniff modes allow devices to sleep, it may reduce power consumption to give months of battery life, the peak transmit current is still a comparative large number typically around 25mA. In other words, the power consumed by traditional Bluetooth is not low enough for coin cells to let manufacturers design wireless devices that are extremely small and yet last comparative longer. On the other hand, the health care devices embedded traditional Bluetooth technology is much more expensive compared with BTLE. High cost may also result of scalability problem, preventing the net designer to build a moderate size networks (say, below 1,000 nodes). Quick connections and disconnections of BTLE, can also contribute to its high energy efficiency. Before quickly tearing down the link, an application can quickly form a connection and makes transfer authenticated data in few milliseconds for a short communication burst. BTLE solves the scalability problem the traditional Bluetooth suffered, by accessing each slave with a 32 bit address on every packet, allowing millions and billions of "smart dust" to be connected. The technology is optimized for one-to-one connections while allowing one-to-many connections using a star topology.

The main drawbacks of BTLE, on the other hand, are that it is an unproven technology. Merchants must install expensive BTLE infrastructure if they want to use; it is a star bus topology, that all other nodes are connected to one control node that waste more energy than mesh network; and it also does not have any energy efficient way for timed reconnect. Besides, it doesn't have any IoT type addressing method. Currently it only relies on pairing and fixed ID. [Joe13]

Despite the above disadvantage, BTLE earns an impressive success of market that can be almost contributed to two reasons. One is its competitively low energy feature. The other is its per existence of market share, ease promotion on smart health care compared with using other wireless technologies. Millions of people carry a Bluetooth enabled phone almost everywhere they go. Provider can simply persuade them to subscribe their wireless service by buying their embedded devices with BTLE and pairing their phone with new types of BTLE wireless sensors. The existing market has paved way for service provider quickly expanding their market in health care industry.

3.2 6LoWPAN

IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) is a wireless protocol standard and acts as an additional layer for making the IPv6 link layer suitable for the lower-power and lossy networks. It is developed as one of new manifold options based on Wireless Sensor Networks (WSN), especially on the low-power personal area networks technology (LoWPANs) [Hu08] It is highly compatible to various network, like IEEE 802.15.4 (and its variants like ZigBee) or BTLE, allowing IPv6 packets to be sent to and received from over them. 6LoWPAN even can run across power-line technologies like PRIME and G3. It enjoys all the advantages from IP design, without using IP, such as flexibility, extended, tested, scalability, ubiquitous, end-to-end connectivity, etc. IP is unnecessary in IoT-based service, because IoT devices normally collect and transfer small data whereas IP protocols were originally designed for exchanging large blocks of data, in other words IP is fundamentally designed toward larger payloads. Even though each device keeps no IP, each WSN node serves as an IP router. The 6LoWPAN protocol is implemented in sensor nodes and one or several LoWPAN border routers (LBSs) connected to the Internet. LoWPAN border routers works as router, they can compress and decompress packets, as Figure 2 shows.
6LoWPAN, however, is more than just IPv6 “header compression”. The 6LoWPAN OSI model also includes other components in their protocol stack to support mesh network, like 6LoWPAN-ND (Neighbor Discovery), IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL), Transmission Control Protocol (TCP), and Internet Control Message Protocol version 6 (ICMPv6). A design deficiency of 6LoWPAN fails mobility over 6LoWPAN link with host based mobility protocols, because host based protocols requirement on significant amount of signaling is hard to realize on 6LoWPAN nodes' limited energy and resource. For example, a 6LoWPAN node may run out of energy and cause errors as result. To avoid that, 6LoWPAN normally offer a more aggressive energy saving method like longer sleep period. This approach cause lose some transferring data. [Antonio14] Several studies about mobility issue of 6LoWPAN have been introduced such as Supporting mobility architecture [Antonio14], and neighbor discovery [Shelby09].

4 Data Processing Services of IoT-based Smart Service

The applications of Smart Services involve not only better tools to collect data and communicate data but also improving the tools for processing data. This is true especially when large quantities of IoT data are needed to be processed and analyzed in real time. End-users demands smart objects provide with a myriad of services to achieve their goals will increase workloads on management system. This section is mainly study on two processing data model approaches adopted nowadays.

4.1 The Centralized Management Model and the Distributed Management Model

The current trend of management model is centralization. The centralized managed system includes a set of devices, as a set of managed objects controlled by a manager in network management. The system performs the FCAPS management tasks on central management stations or servers. The central management station control all the peripheral devices directly, initiate an interaction with the managed system, and request them to send response. This system is also referred as Cloud Computing Model. [Wikipedia03] It is simplicity and cost-effective design. It also offers greater security over decentralized systems since all of the processing is controlled in a central management stations. In addition, the central system may even offer a function that allow a devices resume their connection from the point they were at before, as if nothing had happened.

This type of model does have some disadvantages. First, a large number of devices in IoT networks may send near-real-time requirements and request to interact with back-end centralized databases. That will cause network overloaded. Second, there still exists some security concern. If the central management system crash, when it performs the computing functions and controls the remote devices, the entire system will go down. Third concern is scalability problem. There is a limitation on the scale of centralization system. To monitor the function of peripheral devices/agents, central management station polls the managed entities; its number is limited by the responding node. [GEORGE13]

The traditional distributed system scheme cannot directly be applied in IoT, considering the dynamic nature of the ubiquitous computing paradigm. Therefore when we design distributed model we have to consider several factors i) dynamic characteristics of nodes, ii) user's changing requirements and iii) availability of client devices. Several technologies supports this dynamic feature, for example matching historical data with current CPU, storage usage levels to predict execution time of computing services, or reallocate the whole task process instead of only the problematic part when they detect unexpected delays in computing units.

Some extreme argument is that de-centralization of IoT may result the end of cloud computing. It assumes the existing convergent domain of Cloud and IoT technologies, and attempts to realize real “everything connection.” Actually cloud structures has boost the computational capabilities of IoT applications, permitting to several multi-sensor applications to perform complex big data processing that is subject to different QoS limits. [Nick12]

4.2 Stream Processing System

The truth is the value of the IoT only comes from the astounding mass of data. All of connected smart devices will generate high-volume data, and all of this data will end up to be processed in data-processing center. That requires every devices can communicate with each other in the same language in real time. New high speed real-time processing techniques are pushing the limits of traditional data processing system.
Stream processing is a technology that can collect, integrate, analyze, and visualize, in real time, while the data is being produced, and without disrupting the activity of existing sources, and storage activity. This technology is comprised of eight of data processing requirements such as keeping the data moving, handle delayed, missing and out-of-order data, integrating processing data, predict outcomes after processing and data safety, etc. [Michael05]

A Smart Service provides a proactive intelligence-based solution addressing the problems before occur. That require process data in a predictive manner. The Stream processing offer such a service that could predict the results of data processing by using a time-series messages and solve the issue of uncertainty since the data may change over time and arrive in bursts, especially when the two data are dependent each other. The correct processing can be produced only when message are processed in descending time order. Any disturbing disorder may cause disastrous effect. The Stream processing can continuously optimize the query execution plan according to their computational performance. [Zachary09]

4.3 Alternative Approaches for Better Data Reconstruction and Decision Making

In a large IoT networks, it may consist of different ways of data collection. Due to various sensors, devices or different collecting patterns, protocols, IoT is facing the issue of heterogeneous resources and data insufficiency for decision making. Hence, they established a higher demand for IoT technology, in other word, the request for a more "smart" IoT.

To overcome these limitations, a lot of signal processing and reconstruction technologies have been introduced into the IoT field. For example, compressed sensing, as an extensively investigated technology, has been applied to IoT recently. [Shancang13] The idea of compressed sensing is to recover the signals using some prior knowledge or assumptions about the signals. Compressed sensing is able to get more information from the signal, or recover signals with fewer samples than the Nyquist theorem requires, which is fit for IoT applications with sampling and sensing limitations.

Artificial intelligence (AI) has been introduced to IoT as well, in order to make IoT smarter. [yang12] First of all, AI provides a way to comprehensively analyze the data from different sources and make an overall optimal decision. A health-IoT platform has been built recently. [Yang14] The information of patient and medicine is gathered by bio-chip and RFID chip, processed by a intelligent MedBox, then further direction can be send to remote hospital. Secondly, to overcome heterogeneous sensing data, AI has been used as a consensus decision-making algorithm as well, to provide better services. [Shancang14]

RFID technology represent one of the key enabling technologies of Internet of Things (IoT)[Xu14]. Some healthcare RFID based examples include the potential of exploiting information stored in RFID tags, supported by an NFC platform to improve data management in a care center and keep up-to-date with elderly people's evolution, through a Web2.0 social service [Sarvapali12].

Conclusion

IoT uses data collection systems and technologies to collect information from various sensors/entities or nodes and communicate with local and/or global service management systems, making proactively decision based on that with their advanced data management system. IoT-based smart services is broad notion. There are only three part this paper has focused on. First part is on how to collect data, how to communicate the collected data through IoT based network and IP based network. And then how to process the data in two management structure model and how to predict the processing result with the stream processing technologies. IoT involves a big regime of knowledge and study. It is binding on several vertices, each of which has their specific preferred technologies and standards. We still have a long way to study of it.

References

[Cisco01] "Cisco Information Technology. IoE Based Smart Services 2014," rfp14086.html

[Gartner01] "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020" www.gartner.com/newsroom/id/2636073

[Cisco02] Cisco Smart Care Service Security* ses_security_wp.pdf

[Cisco03] "Cisco's paper on internet of thing 2013" 153_internet.html

[Cisco02] "Cisco Smart Care Service Security" ses_security_wp.pdf


[Wikipedia01] "Command Line Interface" Command_line_interface


[Cisco04] "Cisco Smart Care Firewall Configuration Guide" SCS_Firewall_Configuration_Guide_WP_v1b.pdf

[Joe13]"Bluetooth4.0:Low Energy" csv-1205-decur.pdf


[Shancang13] The idea of compressed sensing is to recover the signals using some prior knowledge or assumptions about the signals. Compressed sensing is able to get more information from the signal, or recover signals with fewer samples than the Nyquist theorem requires, which is fit for IoT applications with sampling and sensing limitations.
List of Acronyms

6LoWPAN "IPv6 over Low power Wireless Personal Area Networks"
AI "Artificial intelligence"
AP "Access Points"
BTLE "BluetoothAc Low Energy"
CLI "Command Line Interface"
CAN "Controller Area Network"
FACPS "Fault, Accounting, Configuration, Performance, and Security"
HAN "Home Area Network"
HSRP "Hot Standby Router Protocol"
IETF "Internet Engineering Task Force"
IoT "Internet of Things"
MCU "Micro-Controllers"
NMS "Network Management Stations"
RFID "Radio-frequency identification"
SNMP "Simple Network Management Protocol"
UDP "User Datagram Protocol"
WAN "Wide area network"
WBAN "Body area network"

Last Modified: April 30, 2014
This and other papers on current issues in Wireless and Mobile Networking are available online at http://www.cse.wustl.edu/~jain/cse574-14/index.html
Back to Raj Jain's Home Page