Research Inventy: International Journal Of Engineering And Science
Vol.3, Issue 5(July 2013), PP 24-29
Issn(e): 2278-4721, Issn(p):2319-6483, Www.Researchinventy.Com

Principle Elements and Framework of Internet of Things

[1]Bhagyashri Katole, [2]Manikanta Sivapala, [3]Suresh V.
[1] (Senior Technical Officer, NISG, C-DAC, Pune, India)
2(Project Engineer, NISG, C-DAC, Pune, India)
3(Joint Director, NISG, C-DAC, Pune, India)

ABSTRACT *- The Internet of Things (IoT) is defined as a dynamic environment where uniquely identifiable things with self configuring capabilities based on standardized and interoperable communication protocols are integrated into the information network. This paper introduces key enablers of Internet of Things and elaborates on principle elements of Internet of Things like Machine To Machine (M2M) paradigm, device mobility and device discovery, communication protocols suitable for IoT environment. It also addresses challenges in Internet of Things. This paper also discusses about our prototype of IoT based navigation solution and gives overview of proposed architecture of IoT framework.*

KEYWORDS *- CoAP (Constrained application protocol), IoT, M2M (Machine to Machine), MQTT (Message Queue Telemetry Transport), Zero-entropy*

I. INTRODUCTION

The Internet of Things (IoT) represents the future of computing and communications. It is world of information and communication technologies (ICTs) from anytime, anyplace connectivity for anyone; we will now have connectivity for anything. It semantically means a network of interconnected objects that are uniquely addressable and connected using standard communication protocols. It will consist of connections that will multiply and create entirely new dynamic network of networks. In this, objects or things are made as smart so that they will become knowledgeable and their properties such as transformation, interactions will allow them to actively interact in environment. For example, RFID tags, sensors and actuators, NFC devices can be made seamlessly communicated and characterized by properties like modularity, reliability, scalability and robustness.[1]In Internet of Things, objects or things are made uniquely addressable by using unique way of identification. These things are heterogeneous in some capabilities. The IoT will provide them a common environment where these heterogeneous things will be able to communicate with each other using standardized communication platform. Obviously, these things will need to consume their own energy very carefully so that they not only to able to communicate for indefinitely long but also form extensive network even when infrastructure is weak or not available.

The explosion of ubiquitous devices is providing growth in Internet of Things. The Internet of Things built using four emerging components. The first one is the explosion of the amount of data collected and exchanged. Business forecasts indicate that in the year 2015 more than 220 Exabyte of data will be stored and hence for this exponential traffic growth, there is a need to re-think current networking and storage architectures used in current network. This data flood is responsible to make Internet of Things as reality. The second one is the energy required to operate the devices will dramatically decreased and hence acquisition of new devices is necessary to replace old ones. Therefore, the trend can be identified covering all devices that will satisfy the search for a zero level of entropy where the device or system will have to harvest its own energy. The third one is amazingly fast happening miniaturization of devices. The fourth is towards autonomic resources so that system will show properties like self management, self configurable and self healable. These emerging components make ‘Things’ in Internet of Things more responsive and intelligent. The development of new and more energy efficient compact storage and energy generation devices using upcoming energy harvesting mechanisms, context awareness intelligence, optimized communication network, integration of solution into packaged product, interoperability among devices and standards are key enablers for the growth of Internet of Things. In this paper, section II talks about M2M paradigm, section III describes about device mobility and device discovery, section IV compares communication protocols suitable for IoT environment, section V discusses about IoT challenges, section VI discusses about our prototype of IoT based navigation solution, section VII gives overview about our proposed architecture of IoT framework and conclusion is given in section VIII.

II. M2M PARADIGM

Machine to Machine (M2M) is paradigm in which end to end communication is executed without human intervention connecting various things to IT core network. Here, things involve commercial terminals that act automatically or on remote request. End to end communication involves network that acts as access and core network backhaul enabling connectivity taking care of AAA, security, session management and mobility management. IT core network involves data aggregation and processing involving data caching and also its interpretation. [2] The M2M refers to technological system that includes both wireless and wired systems to communicate with other devices of the same ability.

The 'Things' in the IoT, or the 'machines' in M2M, are entities whose identity, state is capable to connect to IT infrastructure using internet. M2M also uses a thing or device to capture an event, which is controlled by core network and passed to an application that translates the captured event into meaningful information. It works with standardized technologies such as TCP/IP, IEEE 802.11 wireless LANs, cellular communications technologies, and wired networks such as Ethernet. M2M nodes can operate autonomously, push information to multiple systems and other nodes, and make some decisions on their own. M2M system is eventually used to become smarter having target that we can make sense out of raw data. It involves two mechanisms i.e. Sense and Act. Sense mechanism is used to get raw data from various things involved in infrastructure and draws useful information through perception and interference. After getting knowledgeable information, the system will perform operations through Act mechanism. For some of procedure of M2M, RESTful style of data exchange can also be preferred. [2] Various segments and areas like automation, tracing and tracking, healthcare, remote maintenance and control, metering, consumer electronics, security and payment are trying to involve M2M technology to work smarter. Today, M2M is primarily being used to collect vast amounts of machine data and the 'Internet of Things' goes one step further by integrating data from various devices, allowing humans to intelligently interact with devices, devices with devices and devices back to humans to provide the ultimate social media collaboration of man and machine.

III. DEVICE MOBILITY AND DEVICE DISCOVERY

Mobility of devices is considered as one of important components of Internet of Things where devices get connected to each other. Mobility involves two processes. The first process in roaming that involves moving from one network to another and other process is handover that will involve changing point of attachment when data flows. Handover also includes delay due to handoff that takes place at several layers like layer 2 (handoff between AP), layer 3 (IP address acquisition, configuration), authentication, authorization, binding update, media redirection and rapid handoff will contribute to overall delay and packet loss. Thus, it is essential to reduce the handoff delay during handover that is introduced at different layers to provide better efficiency to end users. Mobility can also be categorized as micro mobility that involves mobility within the network and macro mobility that involves mobility among network domains where IP address changes. [3] There are various causes of mobility that includes physical movements, radio channels, network performance, sleep schedules and node failure. End users can bring their own devices in IoT environment as a part of Bring Your Own Device (BYOD) revolution and hence device mobility is one of the important aspects that need to be considered in Internet of Things.

The number of IoT devices is extremely large as they cater various applications and services under IoT and hence discovery of devices that involves the naming and addressing schemes is crucial and difficult. The IoT system should be flexible in supporting more than one naming schemes. It should support identification of devices/things of IoT by their names, temporary ID, pseudo-name, location or combination thereof. It shall be possible to re-use these names and IDs for certain classes of devices or in an environment where resources are constrained. The naming system should be flexible and should allow plug and play kind of environment. Addressing in IoT should also support discovery of devices and capabilities. This should be included in the naming and localization mechanism. Factors dealing with device exchange, failure, location change due to mobility, or service migration should also be considered in the addressing mechanism. Emphasis should be given for the use of unique IDs to the devices; such that ID based security can be deployed in future. In short, the naming and addressing scheme under IoT should have key features like consistency that involves similar naming format of devices, scalability, uniqueness, interoperability having plug and play support and also backward compatibility. The IoT system shall allow flexible addressing schemes, including IPv4 and IPv6 addressing, RFIDs, URN (Uniform Resource Naming System), URL [4]. For efficient search and discovery, metadata and semantic tagging of information will be very important.

IV. COMMUNICATION PROTOCOLS

The communication protocols will be designed for the Internet of Things platform where all objects or things are combined to analyze location, intent and even emotions over a network. The integration of machine-to-machine (M2M) and wireless sensor network (WSN) solutions need established communication services involving advanced communication protocols that connect smart devices in environment. An IoT application frequently involves a device or a smart object transmitting information regarding its state, context, or sensory measurements to other clients or devices.

The IETF Constrained RESTful Environments (CoRE) working group aims to make the REST paradigm that will available for constrained devices and networks. The main product of the CoRE WG is the constrained application Protocol (CoAP). CoAP uses an asynchronous approach to support pushing information from servers to clients: observation. In a GET request, a client can indicate its interest in further updates from a resource by specifying the “Observe” option. If the server accepts this option, the client becomes an observer of this resource and receives and asynchronous notification message each time it changes. [5] This functionality avoids the frequent server polling or keep-alive sessions that clients need to do in the case of an HTTP-based connection. CoAP has been built over the UDP since the minimally required reliability is achieved through the transaction layer of the protocol. The CoAP request has the following format:

GET coap://[<iot_device_ipv6_address>]: [<port-number>]/[<resource-URI>]

There is another protocol Message Queue Telemetry Transport (MQTT) that is developed by researchers at IBM. It is designed as a lightweight publish/subscribe messaging transport connectivity protocol. It has also been integrated with the IBM websphere application server. The MQTT protocol specification describes the protocol to be ideally suited for resource-constrained environments where the network runs on embedded devices with limited processor or memory resources and is expensive, has low bandwidth, or is unreliable. While MQTT is based on the TCP/IP stack, MQTT-S is an extension for non-TCP/IP stacks, keeping low-end sensor devices in mind. [6]

There are various communication protocols like MQTT, CoAP, XMPP, SOAP, and UPnP that can be used in Internet of Things environment having their specific characteristics that can be used to specific scenarios mentioned in following Table 1.

Table 1: Comparison of communication protocols for IoT environment.

PROTOCOLS	MQTT	CoAP	XMPP	SOAP	UPnP
XML Based	No	No	Communications protocol for message-oriented middleware based on XML	Relies on XML information set for its message format	No
TCP/UDP	TCP	UDP	TCP	Both TCP and UDP	UDP
IPv4/IPv6	IPv4,IPv6	IPv4,IPv6	IPv4,IPv6	IPv4	IPv4,IPv6
M2M support	OASIS Standard	ETSI Standard	---	---	---
USAGE	From Pervasive devices to a server/small message broker.	Simple electronic devices, Resource constrained devices	Video, File transfer, gaming, IoT apps such as smart grid & social networking services	Implementation of web services In computer networks	Permits networked devices to seamlessly discover each other presence on network

In real world application the need may arise where device that uses MQTT may need to communicate with remote device that only understand CoAP. A solution would be to simply enable the client and the server to handle both the MQTT and CoAP protocols. But for environment where the processing and memory availability is highly constrained, implementing multiple protocols on these low-powered devices would not be an ideal situation. There is need for IoT gateway or middleware that can provide protocol-level interoperability by translating the data or the meaning of the message from one protocol to another so that interoperability at device level can be avoided.

V. CHALLENGES IN IOT

In the IoT technology, hundreds of billions of devices will interact with one another without human intervention, on a Machine-to-Machine (M2M) basis. They will generate an enormous amount of data at an unprecedented scale and resolution, giving humans with information and control of events and objects even in remote physical environments. It involves intercommunication and autonomous M2M data transfer. There are following challenges in Internet of Things that need to be addressed. [7]

a. Zero-Entropy systems: This involves energy harvesting, energy conservation, energy usage. Energy will be a major technological challenge, and research must be conducted in order to develop IoT systems that are able to harvest energy from the environment and not waste any under operation.

b. Scalability: IoT will be composed of trillions of devices. It is not feasible that all devices will be connected in a mesh, but rather organized in hierarchical sub domains, the number of interconnected object will outnumber by several orders of magnitude in the current internet.

c. Security and privacy: As there are large numbers of devices are present in the IoT infrastructure, the issue of having sufficient security on devices with limited capabilities has to be addressed and solved convincingly. The technological architectures preserving the respect of privacy have to be developed and used as a basis for any future development.

d. Interoperability: Interoperability among devices and services in IoT infrastructure need to be considered as important aspect. Interoperability includes consistent standardized platform, standardized testing methodologies and well suited testing tools. The standardized platform is needed to obtain consistency. The standardized testing methodologies based on test specifications will specify how to validate devices and services. The testing tools with accurate test suites will ensure interoperability of devices and services. In IoT, semantic interoperability becomes imperative for the providers and requestors to communicate meaningfully with each other despite the heterogeneous nature of the underlying information structures.

e. Standardization and integration: In IoT, multitude of heterogeneous devices communicates and rearranges their network configuration in an autonomous way. Hence, standards regarding spectrum allocation, radiation power levels and communication protocols are primary importance. Standards are required for bi-directional communication and information exchange among things, their environ-ment, and entities that have an interest in monitoring, controlling, or assisting the things. So, there is need of common standardization and integration solution in IoT environment.

VI. OVERVIEW OF PROTOTYPE OF IOT BASED NAVIGATION SOLUTION

The IoT based navigation solution enable individuals to navigate through familiar and unfamiliar environment without assistance of guide by giving speech based instructions. This system is a based on client-server architecture, where the client is android based smart phone device. The server is capable of providing navigation directions to multiple clients simultaneously. This system is designed as Proof of Concept (PoC) phase of NISG in C-DAC, Pune, India. The IoT infrastructure involved following things.

- 3 Linksys WRT54g Wi-Fi access points
- Samsung galaxy S2 mobile (Android OS 2.3.1 based mobile)

The system uses received signal strength indicator (RSSI) based fingerprinting technique in Wi-Fi for IoT deployment where RSSI is adopted for analysis. To allow signal strength data integrated into the optimized location based on derived data, effectively received signal strength for each access point was captured. One can use various site survey tools for this purpose also. The calculation of location of user takes place in two phases: training phase and tracking phase. The training phase was performed to provide intelligence of location to server by considering radiomap as collection of points at different location where signal strength is measured. The user with hand held device is connected to server during tracking phase when online data is compared to offline site survey data and then current position and navigation instructions are given to user. [8]

In this, the probability of finding correct match of location was significantly improved by using advanced positioning and routing algorithms and then navigation instructions are given using combination of advanced navigation algorithms. The experiments performed during this prototype provided foundation for proposing Internet of Things framework that can eventually be used for indoor and outdoor navigation and also provide context awareness and intelligence where standardized communication, interoperability and robustness are considered.

VII. OVERVIEW OF PROPOSED IOT FRAMEWORK

The proposed Internet of Things framework will take care of standardization, interoperability aspects with the help of which various domain specific applications can be built. The proposed Internet of Things framework shown below in Fig. 1 will have the following components:

a. Application Service Layer – This is an independent layer that interoperates with the IoT framework to provide domain specific and application oriented services.

b. IoT Framework comprises the following layers :
Utility Layer – This layer comprises of utilities that can be used by various applications in application service layer. The possible utilities for applications like navigation, tracking, location services.
IoT Service Layer – This layer provides various services for interoperability among entities in targeted IoT environment. This includes various services like device communication service, device management service, mediator service, security service, location service, data service and external interface service etc.

c. IoT environment represents the network of the physical entities or things in the Internet of Things.

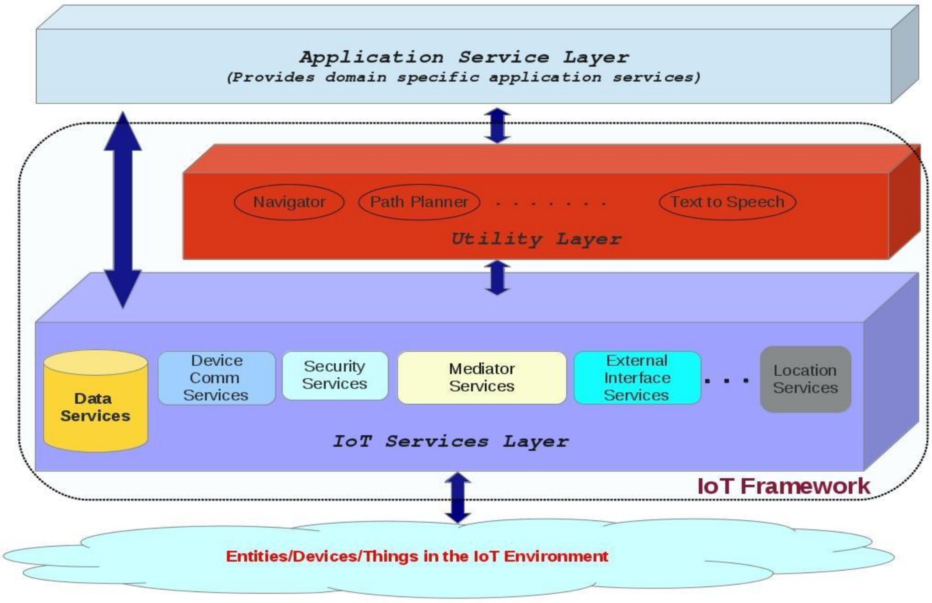

Figure 1 – Proposed IoT framework

The proposed architecture will involve standardized protocol stack that deals with communication among various devices in IoT infrastructure involving sensors, actuators, Wi-Fi based devices, RFID, NFC devices and so on. This IoT platform will also be used for implementation of other domain specific applications e.g. citizen centric applications like public transport assistance, smart house, asset management and tracking and national security applications etc.

VIII. CONCLUSION

When we look at today’s state of the technologies, we get a clear indication of how the IoT will be implemented on a universal level in the coming years. Our proposed IoT framework includes in its components the capability to fulfill identified requirements in IoT. Here, we also get an indication of the important aspects that need to be further studied and developed for making large-scale deployment of IoT a reality. While the current technologies make the concept of IoT feasible, a large number of challenges like standardization, plug and play based integration that need to be deal with radio frequency electromagnetic compatibility and interference, cross optimized and energy aware communication protocol stack and also interoperability lie ahead for making the large-scale real-world deployment of IoT applications. In the next few years, addressing these challenges will be a powerful driving force for networking and communication research and will also act as key enablers for Internet of Things.

REFERENCES

[1] ITU Internet Reports 2005: The Internet of Things – Executive Summary, 2-5

[2] Dr. Sebastian Wahle, Machine Type Communication and M2M Platform Evolution: Horizontal Service Capabilities or Vertical Silo Mindset?, 3rd IoT Forum, Bled, Slowenia ,2012

[3] XiuJia Jin, A Survey on Network Architectures for Mobility, http://www.cse.wustl.edu/~jain/cse574-06/ftp/mobility_arch/#TOP

[4] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswa, Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions, Cornell University Library Open access http://arxiv.org/pdf/1207.0203.pdf

[5] Carsten Bormann Angelo P. Castellani, Zach Shelby, CoAP: An Application Protocol for Billions of Tiny Internet Nodes, Proc. IEEE Internet computing, 2012, Volume:16 Issue:2

[6] Urs Hunkeler & Hong Linh Truong, Andy Stanford-Clark, MQTT-S – A Publish/Subscribe Protocol For Wireless Sensor Networks, Proc. Communication Systems Software and Middleware and Workshops, 2008. COMSWARE,2008.

[7] Van Kranenburg and Bassi, IoT challenges, SpringerOpen Journal Communications in Mobile Computing, 2012.

[8] E.Mok, G.Retscher, Location determination using WiFi fingerprinting versus WiFi trilateration, Journal of Location Based Services, Volume 1 Issue 2, June 2007