

Challenges in Internet of Things Networking

R.Sathya Prakash¹ and K.Arun Kumar²

¹CVR college of Engineering/ CSE Department, Hyderabad
Email: prakashscits@gmail.com

²CVR College of Engineering/ ECE Department, Hyderabad
Email : arun.katkoori@gmail.com

Abstract—Internet of Things(IoT) is the future trend for networks. It facilitates the physical devices like sensors, actuators, etc., buildings and many more modules to collect and barter data. In this paper, we analyse the problem of networking of IoT with respect to IoT architecture, structure of networking, and sensor network mode. Finally we explore the challenges involved in inter-networking of IoT.

Index Terms—IoT, Architecture, sensors, address/ data-centric inter networking, WSN.

I.INTRODUCTION

IoT became a hot topic in research recently, due to it is related to internet, WSN, and cellular communication networks. For providing intelligent services, IoT connects many physical components with unique ID addresses.


IoT is peculiarized by large scale different network objects. By 2025, there will be approximately 30 billion devices are connected using IoT. IoT comprises strong components like smart phone, computers, micro computer, smart watches and weak components like sensors, actuators, RFID, LED's, LCD's..etc.

sensor is an object which will catch out the changes or events in its context and then provide related output. Sensors change the physical state into electrical signals and convey them to the upper layer, and controllers perform peculiar functional behavior to the object by understanding the intelligence information from the upper layer.

Figure 2: Layered model of IoT

ii. Information Exchange layer

This layer communicates with component sensing



	RFID	Sensor	Smartphone	Computer
Quantity (by 2020)	Over 20 billions		~6 billion	~1 billion
Size	~mm to ~cm	~cm	~cm to ~dm	~dm to ~m
Computing	No	Limited	strong	strong
Communication	passive	local	global	global
Sensing	No	Yes, usually with single sensing function	Yes, with rich sensing function	no
Power	Harvested	Battery	Battery and recharged	Power supply
Storage	~KB	~KB to ~MB	~GB	~TB

Figure 1: Comparison of different components in IoT

In Figure 1, we compare strong and weak components with respect to size, power, storage, computing, and communication. The problem is how to interconnect the above mentioned components and transfer the data to the gateway. First, we frame the IoT architecture using layers, then by data-centric structure for inter-networking and finally by crowd sensing modes for sensor networking for solving the above problem.

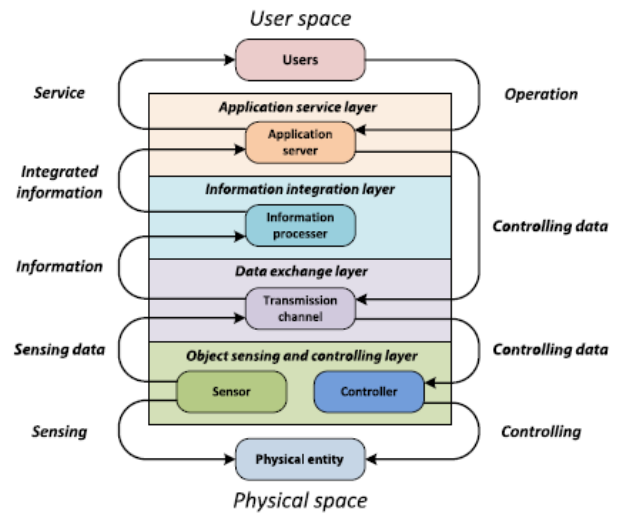
II. IOT ARCHITECTURE

We suggested an IoT Architecture which consists of four layers:

- i. Component sensing and controlling layer,
- ii. Information Exchange layer,
- iii. Data Integration Layer,
- iv. Application service Layer.

i. Component Sensing and Controlling Layer

The world-shattering feature of IoT is its relation with topological space. [3] IoT gathers up the information and controls the activity of objects in physical space. A



and controlling layer by using organized data. The parameters of data include identification number (ID), type, behavior of processing and storing, and life span. Organized data are transmitted through wired or wireless channel.[4] The common wired channels are OFC, coaxial cable, twisted pair and common wireless channels are WiFi, Zigbee, bluetooth.,satellite etc..

iii. Data Integration Layer

In this layer, the gathered information from sensors is integrated in to meaningful information. This information is converted into analogous data like audio, video and discrete data like scalar data. The main entity of this layer is data processor with parameters of computing and storage resources. The main properties of data processor are fusing the data, mining the data, security for

the data etc... Data integration layer protects the details of below layers for the developers.

iv. Application service layer

Application service layer provides services directly to the devices in user space. This layer provides variety of services by using integrated information from data integration layer.[6] Thus, this layer interacts with Data Integration Layer by using integrated information, and communicates with users by using services. The main entity is the application server. The parameters of this server are identified and locate the server. The functions of server include service release, service authorization and service management.

The summary of above four layers in shown in table 1 in terms of parameters, entities, and operations. From the table I observe that, the IoT networking problem is present in lower two layers i.e. component sensing and controlling layer and information exchange layer.[5] In component sensing and controlling layer, sensors need to form a network for sending and gathering the data efficiently. In information exchange layer, adding more sensor networks for huge internetworking will rectify the problem.

Therefore the two problems are internetworking and sensor-networking from first and second layers, respectively.

TABEL 1
Entities, Parameters, properties of layers

Layers	Entities	Main Parameters	Main Properties
Application Layer service	Application servers	Server ID, location	Service release, authorization, management
Data Integration layer	Data processor	Computing resources	Data mining, information query, data fusion, privacy protection
Information exchange layer	Transmission channel	Bandwidth, protocol	Data routing, transmission control
Component sensing and Controlling layer	Sensors	Name, Type	Signal conversion, data transmission
	controller	Name, control modes	Data receiving, command execution

III. INTER-NETWORKING STRUCTURE

The fundamental aspect of IoT is, to connect the sensor networks to Internet, where inter-networking structure should be extensible and scalable. This can be

address-centric or data-centric. [6] This networking model (Internet) being address centric, focuses on connections between end devices. Protocol like TCP and IP are designed by following peer to peer principle. IP is designed to locate devices to enable peer to peer connection between two devices. While in IoT, applications are interested in obtaining required information rather than connecting to a particular device.[2] Compared to address centric networking where to access information and services require mapping from what the users interest about to the network where, information centric networking.

A. Address Centric Networking

IP protocol is a global addressability mechanism and achieved big success in the Internet. By this, it seems that IP is a choice for addressing of IoT. We know that IP is suitable for some of IoT devices but is not a good choice for weak devices (mobiles) and applications on IoT. First, IP has huge overhead with regard to energy constraints of weak devices on IoT such as sensors & RFID's which we already discussed, and may not be able to run on these devices. Second IP is designed for stationary devices which does not handle mobility. While on IoT, many devices have spatial mobility and hence require a new addressing protocol with better mobility support.

To overcome the above problems, 1) Using IPv6 compatible protocol, we connect weak devices to Internet, 2) New locator or Identification Number (ID) for mobile devices to achieve mobility.

1) IPv6 compatible protocol: IEEE 802.15.4 is currently used for sensor networks. [2] In following two steps we combine IEEE 802.15.4 to IPv6- first, IPv6 addresses are allocated to mobile devices using address allocation method.[7] Second, by adding header bits to original data, which allows IPv6 packets to be sent to and receive from IEEE 802.15.4 and by using energy aware routing algorithm less power will be consumed by IoT devices.

2) ID separation Technique: In this technique two network elements are added to current Internet architecture and those are-P (proxy) and HR (Hybrid router) as shown in fig.3. A proxy will register Sensor's ID; When Sensor enters the coverage area of it and also will report to HR. Because of this, the sensor will become observable and accessed by other units of IoT. HR (Hybrid router) is responsible to perform ID-to-IP when a packet without a destination arrives near HR and then forward the packet to the current network location.

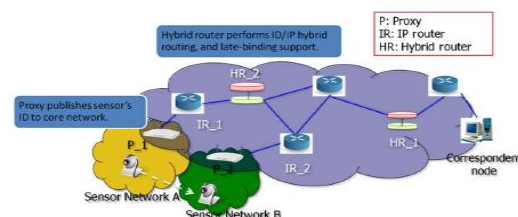
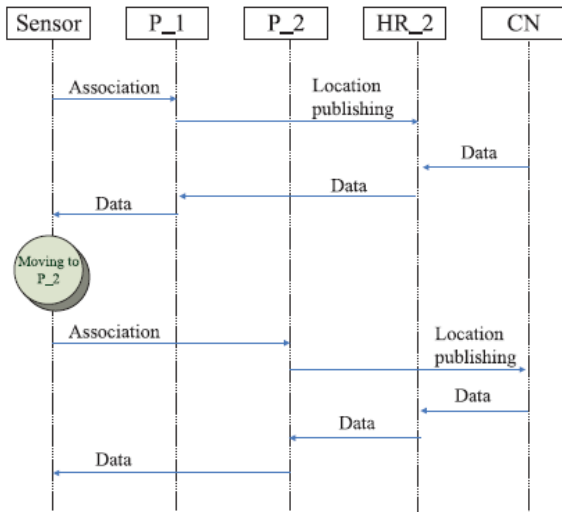


Figure 3: ID separation technique

In fig.3. Assume one sensor is in sensor network 'A', the proxy in that sensor network 'A' will report its ID to the nearest router (HR 2). In this mechanism, the network location of sensor is assumed to be IP address of proxy1 (P1). Then data is accessed from Correspondent node (CN). If the sensor moves from Sensor network 'A' to sensor network 'B' the proxy in that network will report its ID to the nearest router that is HR2 again. Here HR2 will resolve the sensor's ID to the new address location i.e P2. Then data is accessed from CN as shown in fig.4.

Figure 4: ID resolving when sensor moving from sensor



network A to sensor network B
 B. Data-Centric Inter networking

In this NDN (Named data networking) is used. The communication between data consumer and data producer is done using exchange of interest(request) and data(Acknowledge).[9] A data consumer sends interest packet(IR) which consists of name of desired piece of data to the network. Then routers forward this packet to the data producer. This is indicated by bold line in fig.5.

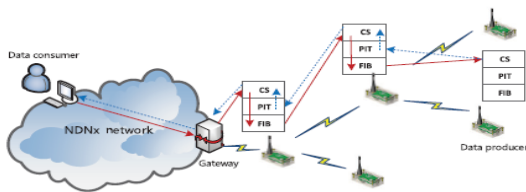


Figure 5: Data-centric networking between NDN and sensor network

Whenever the data producer receives the IR, data packet (DR) will send to the requesting data consumer. This is indicated by dotted line in fig.5.

- The network packet consists of 4 fields. (i) Range (ii) packet type (iii) periodic (iv) Data type
- (i) Range field defines the geographical location (longitude and latitude) of the user who requests the data.
 - (ii) Packet type field defines whether the packet is interest or data.
 - (iii) Periodic field consists of two times- start & end, defines the period of wanted data from starting to end.

- (iv) Data type field defines temperature, intensity, vibrations, etc- type of data.

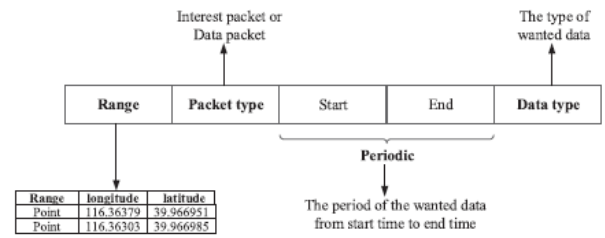


Figure 6: Packet format

Next how the routing is discovered from node is explained in fig.7. In this figure, tree topology is used; slave node calculates its range and sent to master node. The master receives all ranges & calculates its original range by finding the biggest area from all slave nodes.

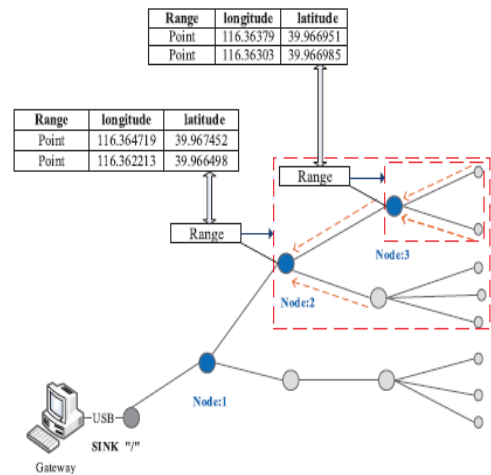


Figure 7: Calculating range of each node by routing discovery

IV. SENSOR NETWORKING

Sensor networking is most widely used in recent years. It consists of two modes: Dedicated deploying mode and crowd-sensing mode. [5] In dedicated deploying mode, we expand a given particular area with the help of using more number of sensor nodes as shown in figure 8. These sensors gather data and sent to a sink node. However, this network has to be carefully designed because most of IoT applications gather sensing data continuously (long-term).

The problems with this network are high energy consumption, heavy load, complex architecture, low reliability and data redundancy is high. The solutions for reducing data redundancy are- Data recovery and Data fusion.

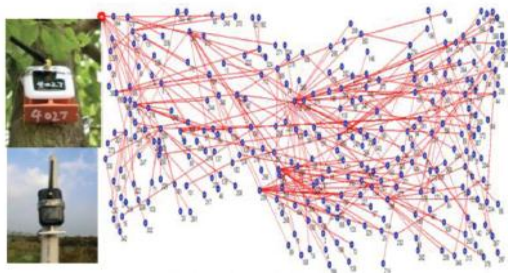


Figure 8: Dedicated deploying sensing mode

In data recovery method, we use the sensing information of small nodes and recover all other nodes by using that information. Finally recovering is done at sink node, as shown in figure 9. However this is an approximation method.

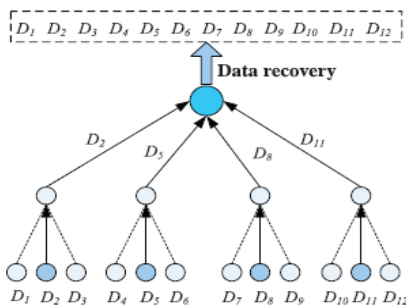


Figure 9: Recovering the data

In data fusion method, we join the readings of small nodes to intermediate nodes and finally we again join the intermediate node's information to a sink node.

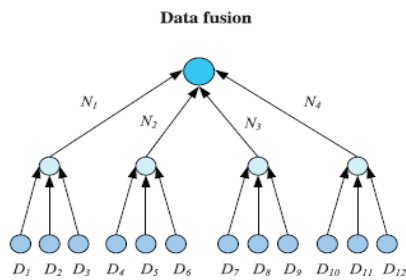


Figure 10: Fusion the data

In crowd-sensing mode, sensors are placed at either mobile phones or vehicles as shown in figure 11. This become more popular in recent times.[8] Coverage area and transmission of data are improved because of human mobility.



Figure 11: Crowd-sensing node

In dedicated- deploying mode, the coverage ratio is nothing but ratio between total area and sensor's coverage area. It is used to calculate the sensing quality of a network. But in crowd-sensing mode, sensing quality is variable due to human mobility. So, to calculate the sensing quality in this mode, we define three factors- Civil resolution, Inter-cover time, and exploitative coverage ratio (ECR).

Through sensed images, parameters like humidity, temperature, intensity, noise, etc are recorded in urban (civil) scenario. Resolution gives the image details. If resolution is high, more image details are provided and vice versa. Civil resolution is used to calculate the sensing images quality and the resolution of digital images.[1] The linear relation between resolution(r) and sensing node number(s) is given by

$$\sqrt{r} = a\sqrt{s} + b; \text{ where 'a' and 'b' are constants} \tag{1}$$

This relation is used to find how many number of mobiles or vehicles required participating in civil sensing system. To find mobile or vehicle distribution model, a truncated pareto distribution is used. Combing the linear and truncated pareto distribution, the civil resolution is

$$\Pr\{r > \gamma\} = \Pr\{s \neq 0\} \times \frac{L^\lambda (4^{-\lambda}(\sqrt{\gamma} - 0.6)^{-2\lambda} - H^{-\lambda})}{1 - L^\lambda H^{-\lambda}}$$

given by

$$\tag{2}$$

Where L, H, λ are factors of truncated pareto distribution.

Next, Inter-cover time is used to find which sub-area is covered. Whole civil sensing area is divided into number of cells, and Inter-cover time is a time gap between two consecutive cells coverage to find which cell is covered. Another factor, exploitative coverage ratio [11] is defined as, in a given time interval 'τ', how much area is covered by cell. The for ECR is

$$f(\tau) = \frac{\sum_{i=1}^m F_i(\tau; n)}{m}$$

$$\tag{3}$$

Where $F_i(\tau; n)$ - Cell's ICT distribution, m- number of cells.

V. CHALLENGES

1. Inter-networking:

Through Internet, the strong modules utilize IP technology but the weak modules (RFID, sensor network) utilize IP and non-IP technologies (using ID and named data). To build active and extensible internetworking models among various network elements, we proposed two methods of non-IP, ID separation structure and data-centric method. In ID separation structure, first we combine IP and non-IP the a unique ID is assigned to each device or a piece of data. Weak devices will become the majority beyond the strong devices, if more number of weak devices are connected with Internet.

However, eliminating the IP is not possible in the Internet. So, converging IP and non-IP is the challenge in IoT architecture.

2. Sensor-Networking:

In dedicated-deploying mode, we discussed two methods (data collection and data fusion) to join networking with in-network processing based on averaging, summation, etc. functions. If functions are complex, those methods are not suitable. So, we need to construct a suitable structure which handles both simple and complex functions.

In crowd sensing mode, sensing quality is the major issue. This was figure out by human mobility consideration, but we need to consider other factors like social psychology of human, availability of sensor, and reliability. And also, if the number of mobiles or vehicles is few, this mode cannot give the good sensing quality. So, we need to integrate both dedicated-deploying and crowd sensing modes, to achieve a good sensing quality.

VI. CONCLUSION

We concluded our research on framework of inter-networking model- we proposed a four-layer model to connect various modules in IoT and exchange information effectively. Then we discuss address-centric/data-centric methods for inter-networking and dedicated-deployed/crowd sensing modes for sensor networking. In the future, we will focus on two challenges- converging IP and non-IP and integration of dedicated-deployed mode and crowd sensing modes.

REFERENCES

- [1.] L. Liu, W.-Y. Wei, D. Zhao, and H.-D. Ma, "Urban resolution: Newmetric formeasuring the quality of urban sensing," IEEE Trans. Mobile Comput., Feb. 2015, to be published.
- [2.] Wang, Y. Cui, S. K. Das, W. Li, and J. Wu, "Mobility in IPv6: Whether and how to hierarchize the network?" IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 10, pp. 1722–1729, Oct. 2011.
- [3.] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," in Proc. 5th Int. Conf. Emerg. Netw. Exp. Technol., 2009, pp. 1–12.
- [4.] H.-D. Ma, "Internet of Things: Objectives and scientific challenges," J. Comput. Sci. Technol., vol. 26, no. 6, pp. 919–924, 2011.
- [5.] IPSO Alliance. [Online]. Available: <http://www.ipso-alliance.org>
- [6.] G. Hu, K. Xu, J. Wu, Y. Cui, and F. Shi, "A general framework of source address validation and traceback for IPv4/IPv6 transition scenarios," IEEE Netw., vol. 27, no. 6, pp. 66–73, Nov./Dec. 2013.
- [7.] L. Zhang et al., "Named data networking," ACM SIGCOMM Comput. Commun. Rev. (CCR), vol. 44, no. 3, pp. 66–73, Jul. 2014.
- [8.] H.-D. Ma, D. Zhao, and P.-Y. Yuan, "Opportunities in mobile crowd sensing," IEEE Commun. Mag., vol. 52, no. 8, pp. 29–35, Aug. 2014.
- [9.] H.-T. Zhang, H.-D. Ma, X.-Y. Li, and S.-J. Tang, "In-network estimation with delay constraints in wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 2, pp. 368–380, Feb. 2013.
- [10.] "Gartner says the Internet of Things installed base will grow to 26 billion units by 2020," [Online]. Available: <http://www.gartner.com/newsroom/id/2636073>

- [11.] D. Zhao, H.-D. Ma, S.-J. Tang, and X.-Y. Li, "COUPON: A cooperative framework for building sensing maps in mobile opportunistic networks," IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 2, pp. 392–402, Feb. 2015
- [12.] D. Zhao, H.-D. Ma, L. Liu, and X.-Y. Li, "Opportunistic coverage for urban vehicular sensing," Comput. Commun., vol. 60, pp. 71–85, Apr. 2015.