Declaration

I hereby declare that this research project report is an original piece of work carried out by me, under the guidance and supervision of Dr. Mohammad Arifuzzaman. This report is the requirement for the successive completion of BSc in Electronics and Communication Engineering under the department of Electronics and Communication Engineering.

I state that the report along with its literature that has been demonstrated in this report papers, is our own work with the masterly guidance and fruitful assistance of our supervisor for the finalization of our report successfully.

Rifat Mahmud

ID: 2013-2-55-019

Signature of Supervisor:

_____

Dr. Mohammad Arifuzzaman
Assistant Professor
Department of Electronics and Communications Engineering,
East West University
Dhaka, Bangladesh.

Approval

This Research Project report on "Name based Networking Architecture for IoT Devices" has been submitted to the following board of examiners as a partial fulfillment of the requirements for the BSc in Electronics and Communication Engineering under the department of Electronics and Communication Engineering on August 2017 by the following student has been accepted as satisfactory.

Rifat Mahmud

ID: 2013-2-55-019

Signature of supervisor:

_____

Dr. Mohammad Arifuzzaman

Assistant Professor

Department of Electronics and Communications Engineering,

East West University, Dhaka, Bangladesh

Approved By:

_____

(Dr. M. Mofazzal Hossain)

Professor & chairperson

Electronics and Communication Engineering

East West University, Dhaka, Bangladesh

Acknowledgement

I would like to express our gratitude and appreciation to all those who gave me the possibility to complete this research work. A special thanks to my supervisor Dr. Mohammad Arifuzzaman, whose help, suggestions and encouragements helped me to take my thesis especially on IoT, I have been craving to work on it for so long. He supported me by showing different methods of information collection while doing this work. He always helped me when required and he gave required direction towards completion of this work.

I also want to thank all faculty members and staffs of the Department of Electronics and Communication Engineering of East West University for their full cooperation and support during the period of the report completion, from the beginning till the end.

Abstract

Unlike the interaction methods between human and electronic devices, the devices will be the main users in the Internet of Things (IoT) ecosystem. Therefore, device-to-device (D2D) communication is expected to be an intrinsic part of the IoT arena. As expected, Device-to-Device (D2D) communication can enhance the network capacity and spectrum efficiency while sharing different genres of resources. The ability to gather relevant information in real time is the only key to leveraging the value of the IoT as such information will be transformed into intelligence, which will facilitate the creation of an intelligent environment. To make this environment more user-friendly and sustainable, the naming based scheme is proposed and probable outcomes are discussed. Ultimately, the quality of IoT promotes sharing of the infinite power with the users to communicate in-between and lead to a sustainable solution of D2D infrastructures. Considering the importance of the unique hierarchy of name based solution for D2D communication, we propose a study for standardization of work in the field of name based networking architecture for IoT devices.

Name based Networking Architecture for IoT Devices

A Research Project Submitted
By

Rifat Mahmud
ID: 2013-2-55-019

Under the Supervision of

Dr. Mohammad Arifuzzaman
Assistant Professor
Department of Electronics &Communication Engineering

East West University, Dhaka

Department of
Electronics and Communications Engineering
East West University
Semester: Spring-Summer, July, 2017

Declaration

I hereby declare that this research project report is an original piece of work carried out by me, under the guidance and supervision ofDr. Mohammad Arifuzzaman. This report is the requirement for the successive completion of BSc in Electronics and Communication Engineering under the department of Electronics and Communication Engineering.

I state that the report along with its literature that has been demonstrated in this report papers, is our own work with the masterly guidance and fruitful assistance of our supervisor for the finalization of our report successfully.

Rifat Mahmud

ID: 2013-2-55-019

Signature of Supervisor:

_____

Dr. Mohammad Arifuzzaman
Assistant Professor
Department of Electronics and Communications Engineering,
East West University
Dhaka, Bangladesh.

Approval

This Research Project report on "Name based Networking Architecture for IoT Devices" has been submitted to the following board of examiners as a partial fulfillment of the requirements for the BSc in Electronics andCommunication Engineering under the department of Electronics and Communication Engineering on August 2017 by the following student has been accepted as satisfactory.

Rifat Mahmud

ID: 2013-2-55-019

Signature of supervisor:

_____

Dr. Mohammad Arifuzzaman

Assistant Professor

Department of Electronics and Communications Engineering,

East West University, Dhaka, Bangladesh

Approved By:

_____

(Dr. M. Mofazzal Hossain)

Professor & chairperson

Electronics and Communication Engineering

East West University, Dhaka, Bangladesh

Acknowledgement

I would like to express our gratitude and appreciation to all those who gave me the possibility to complete this research work. A special thanks to my supervisor Dr. Mohammad Arifuzzaman,whose help, suggestions and encouragements helped me to take my thesis especially on IoT, I have been craving to work on it for so long. He supported me by showing different methods of information collection while doing this work. He always helped me when required and he gave required direction towards completion of this work.

I also want to thank all faculty members and staffs of the Department of Electronics and Communication Engineering of East West University for their full cooperation and support during the period of the report completion, from the beginning till the end.

Index

Table of Content — Page no.

Chapter 1: Introduction to IoT

IoT covers many areas ranging from enabling technologies and components to several mechanisms to effectively integrate these low level components. Software is then a discriminant factor for IoT systems. IoT operating systems are designed to run on small scale components in the most efficient way possible, while at the same time providing basic functionalities to simplify and support the global IoT system in its objectives and purposes. Middleware, programmability – in terms of application programming interfaces (APIs) – and data management seem to be key factors for building a successful system in the IoT realm. Management capabilities are needed in order to properly handle systems that can potentially grow up to millions of different components. In this context, self-managementand self-optimization of each individual component and/or subsystem maybe strong requirements. In other words, autonomics behaviors could become the norm in large and complex IoT systems. Data security and privacy will play an important role in IoT deployments. Because IoT systems will produce and deal with personally identifiable information, data security and privacy will be critical from the very beginning. Services and applications will be built on top of this powerful and secure platform to satisfy business needs. So many applications are envisioned as well as generic and reusable services. This outcome will require new, viable business models for IoT and its related ecosystems of stakeholders. Finally, IoT can have an impact on people and the society they live in, and so it must be conceived and conducted within the constraints and regulations of each country.

IoT is a brand new concern but the actual idea of interconnected devices had been around longer, at least since the 70s. Back then, the idea was often called “embedded internet” or “pervasive computing”. But the actual term “Internet of Things” was coined by Kevin Ashton in 1999 during his work at Procter & Gamble. Ashton who was working in supply chain optimization, wanted to attract senior management’s attention to a new exciting technology called RFID.

With the advent of the Internet, people have become increasingly interconnected at an unprecedented scale[1]. Therefore, not only humans are being interconnected, but devices also are being interconnected. This paradigm shift has led to the concept of the Internet of Things (IoT). However, due to the rapid promotion of IoT technology, there arises some confusions about its types and verities. In broad strokes, there are four main components of an IoT system:

The Thing itself (the device)

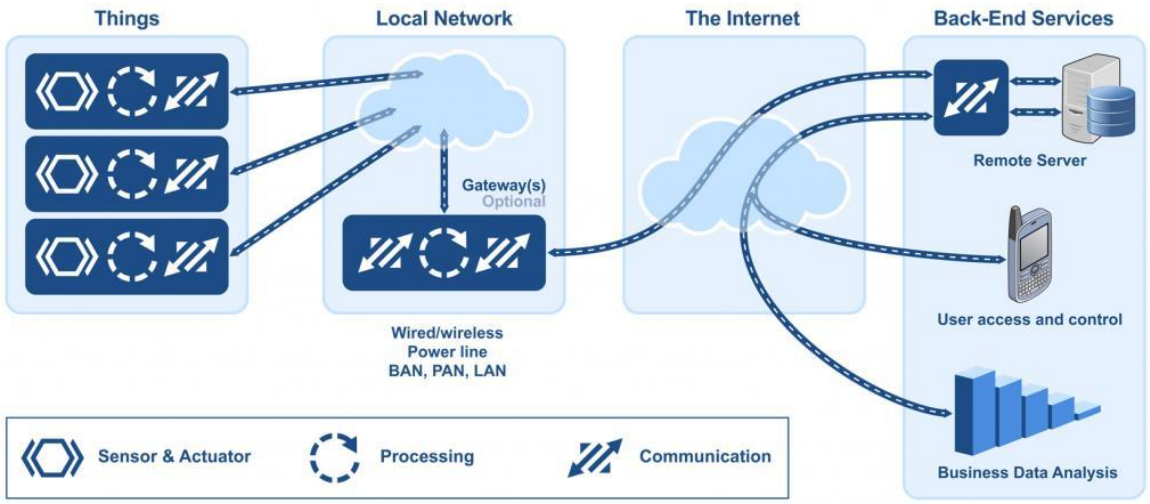


Fig 1.1: The IoT from an embedded systems point of view [1]

IoT systems are not complicated, but designing and building them can be a complex task. And even though new hardware and software is being developed for IoT systems, we already have all the tools we need today to start making the IoT a reality.

We can also separate the Internet of Things in two broad categories:

Industrial IoT, where the local network is based on any one of many different technologies. The IoT device will typically be connected to an IP network to the global Internet.

Commercial IoT, where local communication is typically either Bluetooth or Ethernet (wired or wireless). The IoT device will typically communicate only with local devices.So to better understand how to build IoT devices, you first need to figure out how they will communicate with the rest of the world.

D2D communication technologies (e.g., Bluetooth, Zigebee, and WiFi) are popular networks that will exist in the IoT. Lately, cellular D2D communication has also become an area of interest. Therefore, it is essential to look into how intelligent D2D communication can be achieved in the IoT.

The IoT is a radical evolution of the current Internet, which has been transformed from providing human interconnectionintoanetworkofinterconnecteddevices.Thesedevices interact with the physical world using Internet protocols and standards in order to collect data from the environment. The IoT will enable the transformation of sensed or gathered data into intelligent information, thus embedding intelligence into our environment. In addition, the IoT will involve billions of devices that have the ability to report their location, identity, and history over wireless connections.

The realization of the IoT is gradually coming into fruition as a result of several major trends. Advancements in the field of digital electronics have immensely contributed to the

development of miniature devices that can sense, compute, and wirelessly communicate within short distances. These devices exist as part of our everyday lives in areas such as health care, smart grid, home appliances, retail, etc. In addition, the decreasing costs of these devices have also led to a drastic increase in their deployments in recent years. According to, in 2003, when there were about 6.3 billion people in the world, only 500 million devices were connected totheInternet.Thus,atthattime,therewaslessthanonedevice per person. As a result, the IoT did not yet exist in 2003 since the number of connected devices was relatively low. Subsequent to 2003, after the unveiling of the first set of smartphones and tablet personal computers by manufacturers, there was a gradual increase in the number of connected devices. By 2010, the number of devices connected to the Internet rose to 12.5 billion while the world's population increased to 6.8 billion, making the number of connected devices per person more than one for the first time in history. From a recent forecast outlined in,thenumberofconnected devices will double compared with the number of humans on earth by 20l3 and will grow to an estimated 25 billion connected devices by 2015, when the world's population is expected to be about 7.2 billion. Moreover, it has been predicted that almost 50 billion devices will be connected by 2020. The number of devices will rise to over four times as high as the global population. This increase will be accelerated in part by the enhanced capabilities of devices used every day to orchestrate and manage human activities.

1.1 History of IoT

Radio frequency identification, or RFID, may be a crucial technology for IoT. The roots of RFID technology can be traced back to World War II. The Germans, Japanese, Americans and British all used radar—discovered in 1935 by Scottish physicist Sir Robert Alexander WatsonIWatt—to warn of approaching enemy planes while they were still miles away. But there was no way to identify which planes belonged to the enemy and which were a country's own pilots returning from a mission.

The Germans discovered that if pilots rolled their planes as they returned to base, it would change the radio signal reflected back to radar systems. This crude method alerted the radar crew on the ground that these were German planes and not allied aircraft. Essentially, this was the first passive RFID system.

Under Watson Watt, who headed a secret project, the British developed the first active "identify friend or foe" (IFF) system. When a British plane received British radar signals, it would broadcast a signal back that identified the aircraft as friendly. RFID works on this same basic concept. A signal is sent to a transponder, which wakes up and either reflects back a signal (passive system) or broadcasts a signal (active system).

Advances in radar and radio frequency (RF) communications systems continued through the 1950s and 1960s. Scientists and academics in the United States (U.S.), Europe and Japan explored how RF energy could be used to identify objects remotely. Companies began commercializing antitheft systems that used radio waves to determine whether an item had been paid for or not. Electronic article surveillance tags, for instance, which are still used in packaging today, have a 1Ibit tag. The bit is either on or off. If someone pays for the item, the bit is turned off, and a person

can leave the store. But if the person doesn't pay and tries to walk out of the store, automated readers at the door detect the tag and sound an alarm.

Mario W. Cardullo claims to have received the first U.S. patent for an active RFID tag with rewritable memory on January 23, 1973. That same year, Charles Walton, a California entrepreneur, received a patent for a passive transponder used to unlock a door without a key. In the latter application, a card with an embedded transponder communicated a signal to a reader near the door. When the reader detected a valid identity number stored within the RFID tag, the reader unlocked the door. Walton licensed the technology to Schlage, a lock maker, and other companies.

The US government was also working on RFID systems. In the 1970s, Los Alamos National Laboratory was asked by the U.S. Department of Energy (U.S. DOE) to develop a system for tracking nuclear materials. A group of scientists devised the concept of putting a transponder in a truck and readers at the gates of secure facilities. The gate antenna would wake up the transponder in the truck, which would respond with an ID and, potentially, other data, such as the driver's ID. This system was commercialized in the midI1980s when the Los Alamos scientists who worked on the project left to form a company to develop automated toll payment systems. These systems have become widely used on roads, bridges and tunnels around the world.

At the request of the U.S. Department of Agriculture, Los Alamos also developed a passive RFID tag to track cows and doses of hormones and medicines they'd received. It was difficult to ensure that each cow got the right dosage and wasn't given two doses accidentally. Los Alamos came up with a passive RFID system that used UHF radio waves. The device drew energy from the reader and simply reflected back a modulated signal to the reader using a technique known as backscatter.

Later, companies developed a low frequency (125 kHz) system, featuring smaller transponders. A transponder encapsulated in glass could be injected under a cow's skin. This system is still used in cows around the world today. Low frequency transponders were also put in cards and used to control access to buildings.

Over time, companies commercialized 125 kHz systems and then moved up the radio spectrum to a high frequency band (13.56 MHz), which was unregulated and unused in most parts of the world. High frequency RF offered greater range and faster data transfer rates. Companies, particularly those in Europe, began using it to track reusable containers and other assets. Today, 13.56 MHz RFID systems are used for access control, payment systems (e.g., Mobile Speed pass) and contactless smart cards. They are also used in antitheft devices in cars. A reader in the steering column reads the passive RFID tag in the plastic housing around the key. If it doesn't get the ID number it is programmed to look for, the car won't start.

In the early 1990s, IBM engineers developed and patented an ultrahigh frequency (UHF) RFID system. UHF offered longer read range (up to 20 feet under good conditions) and faster data transfer. IBM did some early pilots with WalIMart, but never commercialized this technology. When it ran into financial trouble in the midI1990s, IBM sold its patents to Intermec, a bar code systems provider. Intermec RFID systems have been installed in numerous different applications, from warehouse tracking to farming. But the technology was expensive at the time due to the low volume of sales and the lack of open, international standards.

UHF RFID got a boost in 1999, when the Uniform Code Council, EAN International, Procter & Gamble and Gillette put up funding to establish the AutoIID Center at the Massachusetts Institute of Technology (MIT). Two professors there, David Brock and Sanjay Sarma, had been researching the possibility of putting lowIcost RFID tags on all products to track them through the supply chain. Their idea was to put only a serial number on the tag to keep the price down, as a simple microchip that stored very little information would be less expensive to produce than a more complex chip with more memory. Data associated with the serial number on the tag would be stored in a database that would be accessible over the Internet.

Sarma and Brock essentially changed the way people thought about RFID in the supply chain. Previously, tags were a mobile database that carried information about the product or container they were on with them as they traveled. Sarma and Brock turned RFID into a networking technology by linking objects to the Internet through the tag (Roberti, “History of RFID,” 2005). For businesses, this was an important change, because now a manufacturer could automatically let a business partner know when a shipment was leaving the dock at a manufacturing facility or warehouse, and a retailer could automatically let the manufacturer know when the goods arrived.

Between 1999 and 2003, the AutoIID Center gained the support of more than 100 large endI user companies, plus the U.S. Department of Defense and many key RFID vendors. It opened research labs in Australia, the United Kingdom, Switzerland, Japan and China. It developed two air interface protocols (Class 1 and Class 0), the Electronic Product Code (EPC) numbering scheme (Sarma et al., “RFID Systems,” 2003), and a network architecture for looking up data associated on an RFID tag on the Internet (Brock, “Electronic Product Code,” 2001). The technology was licensed to the Uniform Code Council in 2003, and the Uniform Code Council created EPCglobal, as a joint venture with EAN International, to commercialize EPC technology. The AutoIID Center closed its doors in October 2003, and its research responsibilities were passed on to AutoIID Labs.

The AutoIID Center used the term "Internet of Things" beginning in about 2000 and heavily promoted the concepts and ideas of a connected world with the EPC system as the basis of how things are connected to the Internet. Though Kevin Ashton (then the executive director of the AutoIID Center) claims to have coined the term "Internet of Things," according to Prof. Daniel Engels, the term was used in a 1997 publication by the International Telecommunication Union (ITU) (Thiesse et al., “Overview of EPC,” 2006).

1.3 IoT Elements

The generic IoT scenario can be identified with that of a generic user that needs to interact with a (possibly remote) physical entity. In this short description we have already introduced the two key actors of the IoT, the “user” and “physical entity” (CASAGRAS [1], “Final Report,” 2009).

I. User

A person or some kind of active digital entity (e.g., a service, an application or a software agent) that has a goal. The attainment of the goal is achieved via interaction with the physical environment. This interaction is mediated by the IoT.

II. Physical entity

A "physical entity" may be defined as a discrete, identifiable part of the physical environment which is of interest to the user for the attainment of his/her goal. Physical entities can be almost any object or environment, from humans or animals to cars, from store or logistic chain items to computers, from electronic appliances to closed or open environments. Physical entities are represented in the digital world via a virtual entity. There are many kinds of digital representations of physical entities: 3D models, database entries, objects (or instances of a class in an object oriented programming language), even a social network account could be viewed as such a representation. In the IoT context, virtual entities have two fundamental properties:

" They are digital entities that are associated with a single physical entity that they represent. While ideally there is only one physical entity for each virtual entity, it is possible that the same physical entity can be associated with several virtual entities, e.g., a different representation per application domain or per IT system. Each virtual entity must have one and only one ID that identifies the represented object. Digital entities can be either active elements (e.g., software code) or passive elements (e.g., a database entry). " Ideally, digital entities are synchronized representations of a given set of aspects or properties of the physical entity. This means that relevant digital parameters representing the characteristics of the physical entity can be updated upon any change of the physical entity. Conversely, changes that affect the virtual entity could manifest themselves in the physical entity.

Augmented entity is defined as the composition of a physical entity and its associated virtual entity. Any changes in the properties of an augmented entity have to be represented in both the physical and digital world. This is what actually enables everyday objects to become part of digital processes.

III. Device

A "device" is used to achieve the association between virtual and physical entity. This is done by embedding, attaching or simply placing the device in close proximity to the physical entity. Devices provide the technological interface for interacting with or gaining information about the physical entity. By so doing the device actually enhances the physical entity and allows the latter to be part of the digital world. A device thus mediates the interactions between physical entities (that have no projections in the digital world) and virtual entities (which have no projections in the physical world), generating a paired couple that can be seen as an extension of either one. Devices are thus technical artifacts for bridging the real world of physical entities with the digital world of the Internet. This is done by providing monitoring, sensing, actuation, computation, storage and processing capabilities in the device.

From a functional point of view, devices can belong to any of the following types.

One of the characteristics of IoT is ubiquity, which can be realized through unique identification of the “things” that are connected to the Internet. This unique identification is done by attaching tags on the “things.” Tags are used by specialized sensors typically known as readers. Their sole purpose is to facilitate an identification process. RFID is a perfect solution for providing this unique identification of “things.”

The transponder or tag of an RFID is used to carry data, which is located on the object to be identified. This normally consists of a coupling element (such as a coil or microwave antenna) and an electronic microchip, less than one third millimeter in size. Tags can be passive, semipassive or active, based on their power source and the way they are used, and can be readonly, read/write or read/write/rewrite, depending on how their data is encoded. Tags do not need a built in power source, as they obtain the energy they require to function from the electromagnetic field emitted by readers. " An interrogator or reader reads the transmitted data (e.g., on a device that is handheld or embedded in a wall). Compared with tags, readers are larger, more expensive and powerIhungry. In the most common type of system, the reader transmits a low power radio signal to power the tag (which, like the reader, has its own antenna). The tag then selectively reflects energy and thus transmits some data back to the reader, communicating its identity, location and any other relevant information. Most tags are passive, and activated only when they are within the coverage area of the interrogator. While outside this area, they remain dormant. Information on the tag can be received and read by readers and then forwarded to a computer database. Frequencies currently used for data transmission by RFID typically include 125 kHz (low frequency), 13.56 MHz (high frequency) or 800I960 MHz (ultrahigh frequency). RFID standards relate both to frequency protocols (for data communication) and data format (for data storage on the tag). "Sensors provide information about the physical entity they monitor. Information in this context ranges from the identity of the physical entity to measures of the physical state of the physical entity. Like other devices, sensors can be attached or otherwise embedded in the physical structure of the physical entity or be placed in the environment and indirectly monitor entities. An example of the latter is a camera that recognizes people’s faces. Information from sensors can be stored for later retrieval. " Actuators can modify the physical state of a physical entity. Actuators can move (translate, rotate, etc.) simple physical entities or activate/deactivate functionalities of more complex ones.

IV. Sensor Operating Systems

Most operating systems (OS) that may be used for IoT were designed for wireless sensor networks (WSN) like TinyOS and Contiki. But, practically, it seems that most of the OSs that were designed for use in WSN fail to meet one or more of the requirements of IoT. The developers of RIOT claim that they’ve bridged this gap of OS requirements between WSN and IoT.

Chapter 2:An evolution from Intranet of Things to Internet of Things

A new approach to the design of internet structures has recently been proposed, in which internet has been expanded with new dimensions. Earlier, we have connected devices within

an unplanned infrastructure. A device connected with another with an inter network, referred as Intranet of things but now we have surpassed the web of things which are interconnected to each other, rather we are concentrating on devices which can be connected remotely to another end within a coherent network which is known as Internet of Things.The recipe of determining the difference between Intranet of Things to Internet of Things is the boundary. Intranet of Things gave us the ease of personal use of the device to device communications but by Internet of Things, we can ascribe its functionality by wider usage in industrial purpose. By Internet of Things, we consider basic things like the right infrastructure with a central middleware, its various bus and network systems and controlling via smartphone, tablet or web browser. This is a great tool to enhance the credibility of communication, systematically which is much more integrated and heterogeneous in nature. From now on IoT will refer Internet of Things throughout the whole paper.

2.1 IoT & its future challenges

In order to attain a matured technology for wide deployment and market integration of IoT, we have to concentrate on its design complexity and consequences. This part is covering all technologies needed to make IoT systems function smoothly as a standalone solution or part of existing systems and that's not an easy mission, there are many technological challenges, including Security, Connectivity, Compatibility & Longevity, Standards and Intelligent Analysis & Actions. First of all, the communication strategy needs to be taken under serious close thought. The initial solution that is presumed- a lift from IPv4 to IPv6 is not a permanent solution at all. Connecting so many devices will be one of the biggest challenges of the future of IoT, and it will defy the very structure of current communication models and the underlying technologies. At present we rely on the centralized, server/client paradigm to authenticate, authorize and connect different nodes in a network.

This model is sufficient for current IoT ecosystems, where tens, hundreds or even thousands of devices are involved. But when networks grow to join billions and hundreds of billions of devices, centralized systems will turn into a bottleneck. Such systems will require huge investments and spending in maintaining cloud servers that can handle such large amounts of information exchange, and entire systems can go down if the server becomes unavailable.

The future of IoT will very much have to depend on decentralizing IoT networks. Part of it can become possible by moving some of the tasks to the edge, such as using fog computing models where smart devices such as IoT hubs take charge of mission-critical operations and cloud servers take on data gathering and analytical responsibilities.

Other solutions involve the use of peer-to-peer communications, where devices identify and authenticate each other directly and exchange information without the involvement of a broker. Networks will be created in meshes with no single point of failure. This model will have its own set of challenges, especially from a security perspective, but these challenges can be met with some of the emerging IoT technologies such as Block chain.

Moreover, technology standards which include network protocols, communication protocols, and data-aggregation standards, are the sum of all activities of handling, processing and

storing the data collected from the sensors. This aggregation increases the value of data by increasing, the scale, scope, and frequency of data available for analysis.

2.2 Challenges facing the adoptions of standards within IoT

Standard for handling unstructured data: Structured data are stored in relational databases and queried through SQL for example. Unstructured data are stored in different types of NoSQL databases without a standard querying approach.

Technical skills to leverage newer aggregation tools: Companies that are keen on leveraging big-data tools often face a shortage of talent to plan, execute, and maintain systems.

No doubt that IoT creates unique challenges to privacy, many that go beyond the data privacy issues that currently exist. Much of this stems from integrating devices into our environments without us consciously using them. Hence it is becoming more prevalent in consumer devices, such as tracking devices for phones and cars as well as smart televisions. In terms of the latter, voice recognition or vision features are being integrated that can continuously listen to conversations or watch for activity and selectively transmit that data to a cloud service for processing, which sometimes includes a third party. The collection of this information exposes legal and regulatory challenges facing data protection and privacy law.

In addition, many IoT scenarios involve device deployments and data collection activities with multinational or global scope that cross social and cultural boundaries. What will that mean for the development of a broadly applicable privacy protection model for the IoT?

In order to realize the opportunities of the IoT, strategies will need to be developed to respect individual privacy choices across a broad spectrum of expectations, while still fostering innovation in new technologies and services.

2.1.1 Communications strategy

There are several opinions that support IPv6 is a key enabler for the future IoT. As the number of devices increase by the time, hence device to device (D2D) communication potentially increases; IPv4 cannot afford to maintain the spontaneous flow of devices. Moreover, IPv6 is a fully internet compliant. In other words, it is possible to use a global network to develop one’s own network of smart things or to interconnect one’s own smart things with the rest of the World.

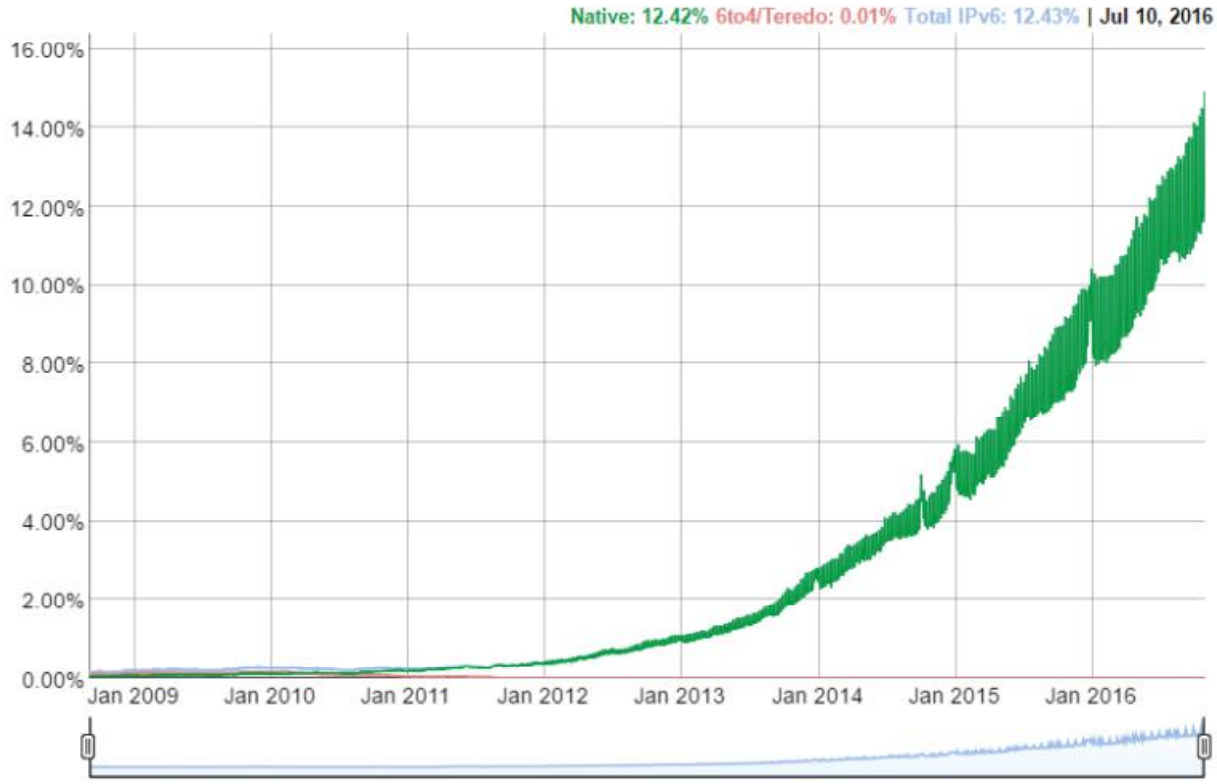


Fig 1.2: User engagement of IPv6[2]

2.1.2 Heterogeneity

IoT is approaching towards the unique challenge of making an object oriented world. At the beginning, IoT was concentrating on various digital things such as RFID (Radio Frequency IDentification), sensor or smart phones which are interconnected and can communicate with each other. So that, we got the concepts of smart objects and smart technologies from IoT at the beginning. From the recent adaptation of enabling device technology such as RFID tags and readers, Wireless Sensor Networks (WSN), Near Field Communication (NFC) devices,Bluetooth Low Energy and actuator nodes, IoT has moved out from its immaturity and become the next revolutionary combined Internet. Though WSN with IPv6 connectivity such as 6LoWPAN is considered as the main infrastructure of IoT, WSN basically consists of homomorphic devices sharing the same network types and protocols.In upcoming future, there will be trillion of devices with IPv6 connectivity which would participate to serve people through D2D or M2M interaction arranged by IoT and it will have major impacts on infrastructure, industry standards, security and business models throughout the entire IT ecosystem. The IoT will embrace, leverage, extend and enhance cloud, big data, personal devices and social networks to provide more pulverized sensor and devices closer to the edge. So, to make a smart world with the maximum range of technologies, the development of IoT architecture is much more necessary for the heterogeneity.

2.1.3 Security

IoT security has become one of the major concerns right now.It creates unique challenges to privacy, many that go beyond the data privacy issues that currently exist. Much of this stems from integrating devices into our environments without us consciously using them.

This is becoming more prevalent in consumer devices, such as tracking devices for phones and cars as well as smart televisions. In terms of the latter, voice recognition or vision features are being integrated that can continuously listen to conversations or watch for activity and selectively transmit that data to a cloud service for processing, which sometimes includes a third party. The collection of this information exposes legal and regulatory challenges facing data protection and privacy law.

In addition, many IoT scenarios involve device deployments and data collection activities with multinational or global scope that cross social and cultural boundaries. What will that mean for the development of a broadly applicable privacy protection model for the IoT?

In order to realize the opportunities of the IoT, strategies will need to be developed to respect individual privacy choices across a broad spectrum of expectations, while still fostering innovation in new technologies and services

IoT is not excessively extended and deployed because of the hardles in configuring (IPSec) for the end users and the lack of scalable certificate management for DTLS[2]. On the other hand, the ESP scheme needs to be optimized in terms of proper cryptographic ensembles. Moreover, IPSec packets can force the packet to be fragmented; thus an extra packet must be sent to the link layer which will consume more energy. In addition, this overhead problem is worse with the Encapsulation Security Protocol (ESP) mode of IPSec, since the internal headers of IPv6 and UDP[3] are encrypted and consequently cannot be compressed.

2.2 Why IPv6?

The things are connected to the internet are increasing rapidly and there will be approximately 20 billion connected ‘things’ by 2020. The internet of things and IPv6 are strongly aligned, to the extent that claims are made they are mutually reliant. An internet of things needs massively expanded protocol addresses space that only IPv6 can provide. IPv6 is very important when every connected home appliance and street will need an IP address.

IPv6 offers a highly scalable scheme. After noticing the rising numbers of connecting things, it’s easy to understand why IPv6 is important for IoT devices. IPv6 provides 2^128 unique addresses which represents 3.4*10^38 addresses. In other words, more than 2 billion of billions addresses per square millimeter of the earth surface. It’s quit sufficient to addresses the needs of any present and future communicating device.

With billions of new smart products being created everyday, security is an important thought. IPv6 offers better security solutions than its predecessor, largely due to IPSec. It can run end-to-end encryption. The encryption and integrity-checking used in current virtual private network (VPNs) are standard component in IPv6. IPv6 also support more-secure name resolution. The Secure Neighbor Discovery (SEND) protocol is capable of enabling cryptographic confirmation that a host is who it claims to be at the time of the connection.

IPv6 is fully internet compliant. In other words it's possible to use a global network to develop one's own network of smart things or to interconnect one's own smart things with the rest of the world.

3 ID separators: The unique need for increasing networks

As devices and related networks are increasing in an exponential manner, it is important to withstand the analogy of separate IDs.In current Internet, 'static' host is the basic assumption, whereas 'mobile' host is treated as a special case, as shown in MIP. It is quite reasonable approach in the fixed host dominant environment, but it should be completely opposite in the mobile dominant one. Locator ID separation has been considered as a qualitatively better approach for mobility support while improving network security and scalable routing. As IP address is used in network layer protocol as the locator to find the host and forward the data packets towards the destination, it has different set of values for host IDs and locators.

HIPuses public keys (and their hash values) as host IDs and IP addresses as locators. A new layer, called the identity layer, inserted between the transport and network layers of the host protocol stack performs the host ID-to-locator mapping functions. This value extends the Domain Name System (DNS) records to store host IDs where a host acquires its peer host's ID and locator by sending a domain name lookup request to a DNS server. While communicating with the peer host, both the source and destination hosts' IDs appear in the identity header and locators in the network header of data packets.

Although HIP is a good step in developing a locator ID separation-based mobility scheme, it is still in its infancy and lacks several functions. It has no support for smooth handover. Its session initiation process is computationally heavy, making it inappropriate for small, resource-limited devices. It uses locators in some signaling messages, thus necessitating the re-establishment of session contexts in the event of switching locators. This requirement is counterproductive to fast handover.

Another ID/locator split-based mobility protocol is LINA. Sublayer concept is introduced in this method in network layer. IDs of 128-bit length are formed by concatenating location-independent prefixes (of 64 bits) and node IDs (of 64 bits), while locators are formed by concatenating location-dependent network prefixes and node IDs. It is divided into two sublayers: the identification sublayer and the delivery sublayer. The former carries out the ID-to-locator mapping function and the latter forwards packets using destination locators present in the packet header. It uses mapping agents to resolve IDs into corresponding locators. It is a host-based mobility approach, i.e., there is no support for network-based mobility and smooth handover.

LISP uses prefix summing endpoint IDs (EIDs), which are also used as locators in the edge network. Here, routing locators (RLOC) are used as locators in the transit network. To provide host-mobility, there is a proposal for having the host possess a lightweight version of the ITR/ETR functions. However, it may not be effective for reducing the BGP routing table

size, if a distinct RLOC is assigned to each host. Hence, LISP lacks smooth handover functions.

3.1 HIMALIS network

The Heterogeneity Inclusion and Mobility Adaptation through Locator ID Separation (HIMALIS) architecture natively supports mobility by allowing the host to change its address (or locator) used in the network layer while keeping the session identifier used in the application and transport layers unchanged.

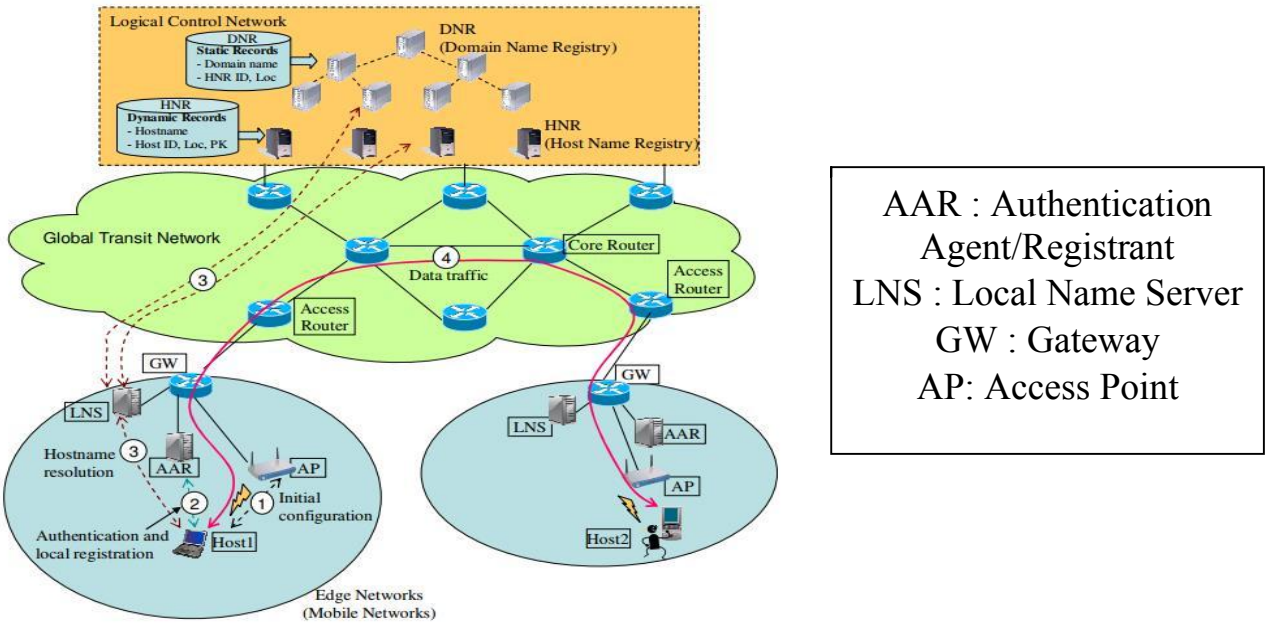


Fig 3.1: HIMALIS network components

It also facilitates faster updates of ID/locator mappings in name resolution servers or registries. However, it still lacks functions for supporting seamless host mobility when a host moves across edge networks and network mobility when a whole edge network moves. To address these issues, this paper presents an optimized host mobility management scheme and a network mobility management scheme. These schemes employ traffic redirection from the old gateway (or old access router) to the new gateway (or new access router) to reduce packet loss during handovers. Meanwhile, the intrinsic security functions of the HIMALIS architecture are leveraged to protect the newly introduced mobility schemes from various attacks such as impersonation and man-in-the-middle attacks.

Heterogeneity inclusion and mobility adaptation through a locator ID separator (HIMALIS) architecture of the new generation network is being developed as a part of AKARI project.

The HIMALIS architecture provides mobility function for handover optimization & supporting heterogeneous network layer protocols. Here, between network and transport layers, we will insert a new layer called 'identity layer'. This layer executes mobility functions in network layer mainly. Here, the mappings among between hostnames, IDs and locators are stored in two different registries. First one is called, Domain name Registry (DNR) and the second one is called Host Name Registry (HNR).

The current version of HIMALIS architecture does not support seamless host mobility because some packets may get lost during a handover. More importantly, it cannot support network mobility by maintaining session continuity when the whole edge network moves. Most importantly, ID based scheme in this network portion is not user friendly at all and very hard to remember for primary level users.

So, here we propose name based architecture in HIMALIS adding up new components for better user experience and more mobility support.

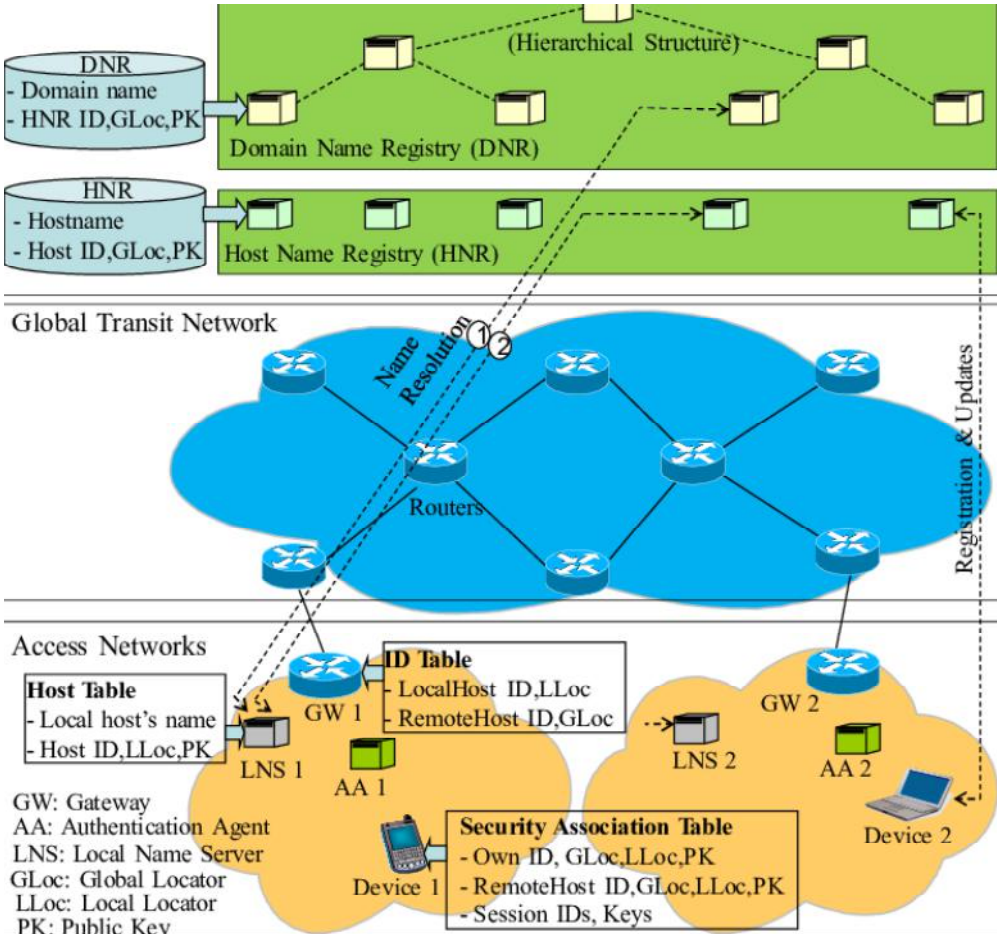


Fig 3.2: Idea of HIMALIS Network

Here, we have introduced a name based server NRS that will convert the device address to a human readable format. From the Edge Network to Global Transit Network, when the bits are transmitted as the stack of numbers, the NRS will convert it into a human readable format (reading hierarchy is given below) and send it to the host's Edge Network for host name lookup. It will translate the location and device address and update ID/Locator mapping in IDRs.

4. A Generic Name Resolution Framework

Mostly, all entities involved in communication are named and not statically bound to their physical locations. To access entities using their names, the Name Resolution Service (NRS) is introduced which will follow <Device Name, Model Number, Device code>

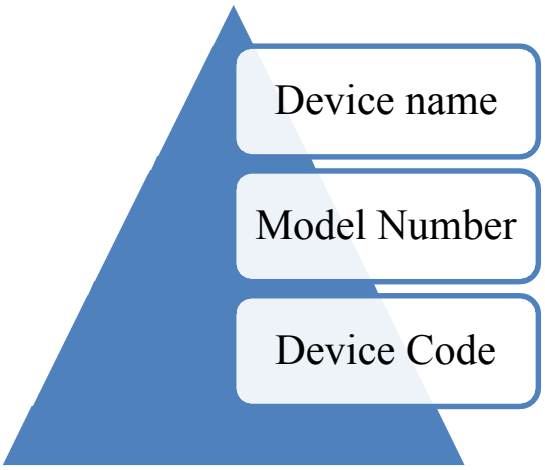
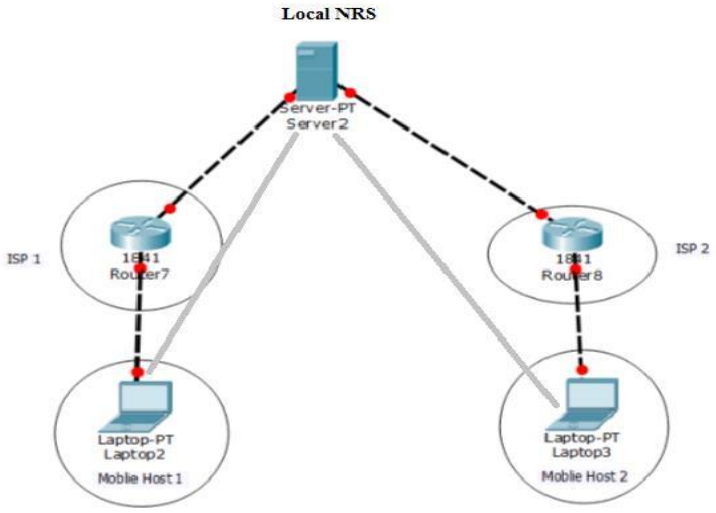


Fig 4.1: High level view of the hierarchy of name based content

Now we will go through some case studies to define exactly how this model will work.A host name is an alias that is assigned to an IP node to identify it as a TCP/IP host. The host name can be up to 255 characters long and can contain alphabetic and numeric characters, hyphens, and periods.

4.1 Case Studies

4.1.1Case study 1



Here, after "calling" the mobile host, it sends the device address to the NRS. The NRS will map the address into name scheme and send it to the ISP it belongs to. The ISP will send it to the receiver.

4.1.2 Case study 2

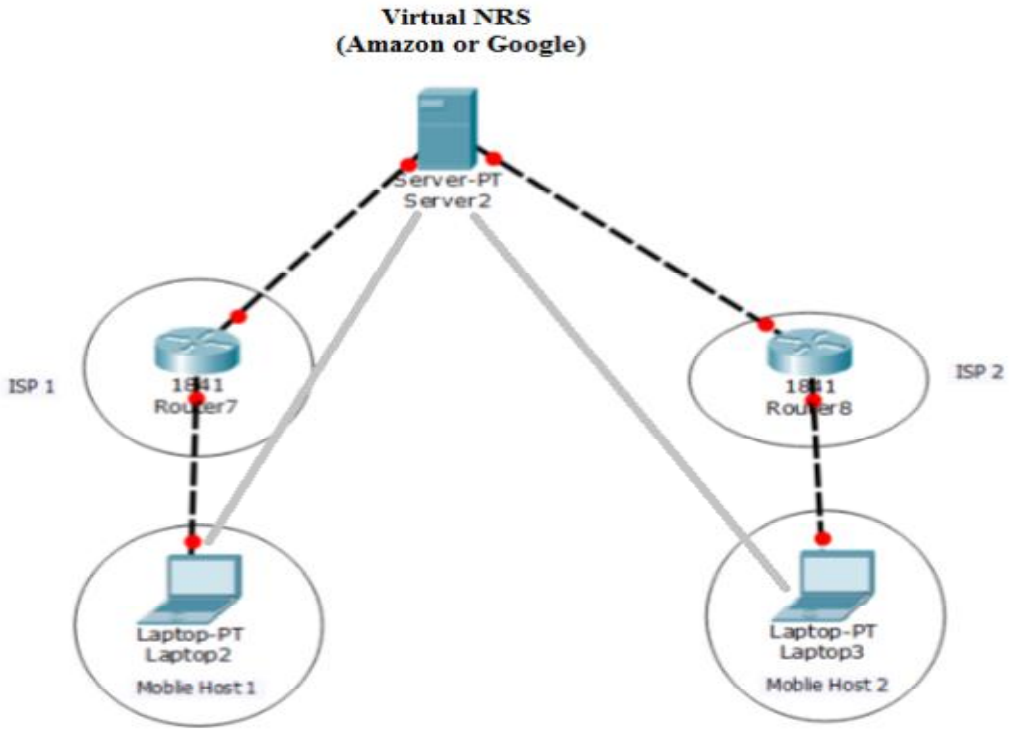


Fig 4.1: High Level view of D2D communication via NRS

The naming policy may not be adopted by all the manufacturing companies in a while. So for the time being, we propose another server to convey the conversion and transmission scheme for the time being. It should work as a digital process. We may regard google server or amazon web service as an example.

5 Simulations and Results

We simulate our proposed NRS architecture for ICN with nnnSIM (Lopez, 2015). Like NDN's simulator, ndnSIM (Afanasyev, Moiseenko, & Zhang, 2012), our simulator is a ns-3 (ns-3 Developers, 2015) module that implements our network architecture. The soundness of our proposed architecture is analyzed for the scenario where user sends the data packet to NRS and it comes back to foremost endpoints.

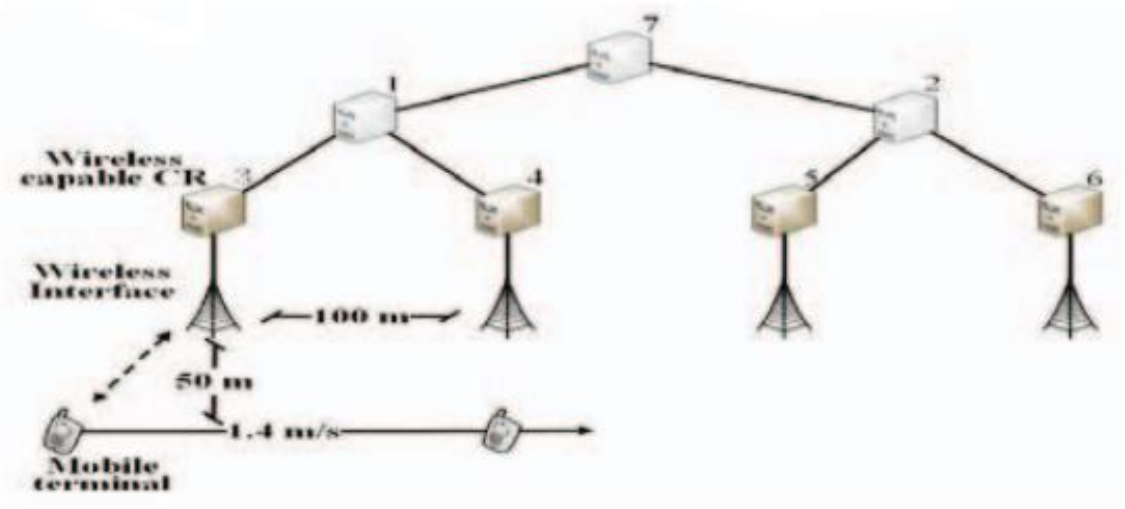


Fig 5.1: Simulation topology

Table 5.1: Simulation parameters

Simulation time	400m/ mobile node speed (10s)
Mobile node speed	1.4, 2.8, 5.6, 7, 8.4, 11.2 m/s
BW/ link capacity	100 Mbps
Link delay (wired)	1 ms
Link delay (wireless)	Constant speed propagation Three log distance propagation Nakagami propagation
Device tracing signal generation rate	120 kbit/s
Interest packet generation rate	148/s
Interest retransmit timer	50 ms
Forwarding strategy	Smart flooding

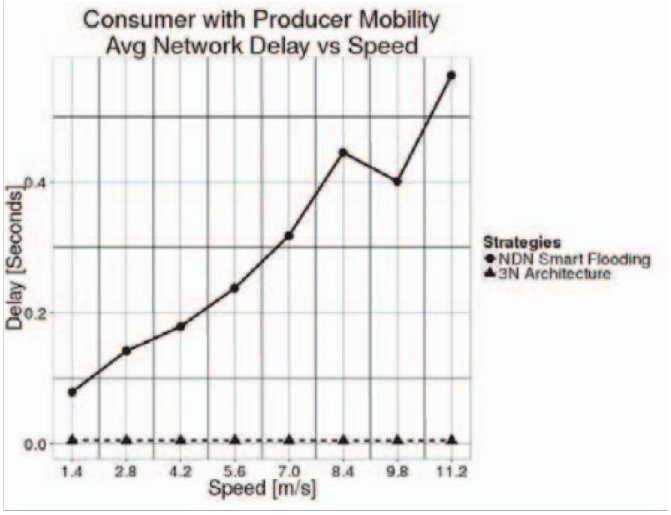


Fig 5.1: Mobility calculation- Delay vs Speed

6 Conclusions

The evolution in communications is a must for modern technology adaptation. For this, D2D communication has become an integral part of the IoT environment to design, deploy, and maintain a sustainable IoT ecosystem. Researchers in the academia and industry are currently addressing many issues. Some of the IoT research issues include energy efficiency, routing, security, context-awareness protocols, etc. In this paper, we focus on issues that impact intelligentD2DcommunicationintheIoTenvironment.

6.1 Related Works

Unlike naming the IoT devices, the way of acknowledging any final product is changing. The proposed hierarchy implements functionality above the current Internet architecture, ensuring sustainable growth in D2D communications. Here are some works related to the field of communications.

The Data-Oriented Network Architecture replaces DNS names with flat, self-certifying names and a name-based anycast primitive above the IP layer. Names in DONA are a cryptographic digest of the publisher's key and a potentially user-friendly label – however, that label is not securely bound to the content, allowing substitution attacks. Unlike CCN, data cannot be generated dynamically in response to queries – content in DONA must first be published, or registered, with a tree of trusted resolution handlers (RHs) to enable retrieval. Each resolution handler must maintain a large forwarding table providing next hop information for every piece of content in the network. Once the content is located, packets shareexchangedwiththeoriginalrequesterusingstandardIProuting.
Ifthelocationofapieceofcontentchanges,newrequestsforit will fail until the new registration propagates throughthe network. CCN, in contrast, can forward requests to all the places a piece of content is likely to be.

Anumberof systemsmakeuseofdistributedhashtables(DHTs) to route queries for opaque content names. ROFL (Routing on Flat Labels) evaluates the possibility of routing directly on

semanticfree flat labels [7]. A circular namespace is created to ensure correct routing (as in Chord), but additional pointers are added to shorten routes. In a similar approach, i3 separates the acts ofsending and receiving by using a combination of packet identifiers and a DHT. Receivers insert a trigger with the data identifier and their address into the DHT. The trigger is routed to the appropriate sender, who fulfills the request by responding with the packet containing the same id and the requested data. SEATTLE utilizesflataddressingwithaone-hopDHTtoprovideadirectoryservice with reactive address resolution and service discovery. Unlike CCN, all of these systems require content be explicitly published to inform the DHT of its location before it can be retrieved. Also unlikeCCN,thisretrievalislargelyfreeoflocality–queriesmight retrieve a cached copy of data along their routed path, but are not guaranteed to retrieve the closest available copy.

Instead of routing end-to-end based on an identifying name, the PSIRP projectproposes using rendezvous as a networkprimitive. Eachpieceofdatahasbothapublicandprivatelabel used for verifying the publisher and making routing decisions. Consumers receive content by mapping the desired, user-friendly name to an opaque public label via an unsecure directory service. The label is then used to subscribe to the piece of data, triggering thesystemtolocateanddeliverthecorrespondingcontent. Though motivated by the same problems as CCN, PSIRP suffers from its use of unstructured identifiers and lack of strong cryptographic binding between user-meaningful names (or currently, even their opaque labels) to content.

The 4WARD NetInf project has similar goals to CCN but focuses on higher level issues of information modeling and abstraction. It currently uses DONA-style names for Data and Information Objects and provides a publish/subscribe style API. The NetInf Dictionary infrastructure uses a DHT for name resolution and location lookup. TRIAD [8], like CCN, attempts to name content with userfriendly, structured, effectively location-independent names.

TRIAD uses URLs as its names using an integrated directory to map from the DNS component of the URL to the closest available replica of that data. It then forwards the request to that next hop, continuing until a copy of the data is found. Its location is returned totheclient,whoretrievesitusingstandardHTTP/TCP.TRIADrelies on trusted directories to authenticate content lookups (but not content itself), and suggests limiting the network to mutually trusting content routers for additional security. Research into content-aware routing protocols also attempts to improve delivery performance and reduce traffic overhead. For example, Anandet. al studied the benefits of large-scale packet caching to reduce redundant content transmission. In this work, routers recognize previously forwarded content and strip the content from packets on the fly, replacing the content portion with a representativefingerprint.
Downstreamroutersreconstructthecontentfromtheirowncontentcachebeforedeliveringtotherequester.

6.2 Future Works

As a scope of future work, we will do more extensive simulation to evaluate the performance of other applications like VoIP, HD Video Delivery etc. The implementation of this architecture under more practical network distribution settings will also be required. Among the tests that should be made is the leveraging of the ICN layer's underlying handoff

information, the use of a heterogeneous network and multiple and more complicated MN mobility with background traffic.

References

[1] Image url: https://www.micrium.com/iot/devices/#foobox-1/0/internet-of-things.png

[2] https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption&tab=ipv6-adoption

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[2] J. Buckley, "From RFID to the Internet of Things pervasive networked systems," Conference Centre Albert Borschette (CCAB), Brussels, Belgium, Mar. 2006.[Online]. Available: ftp://ftp.cordis.europa.eu/pub/ ist/docs/ka4/au_conf670306_buckley_en.pdf

[3] D. Evans, "The Internet of things: How the next evolution of the Internet is changing everything," Cisco IBSG, San Francisco, CA, USA, Apr. 2011. [Online]. Available: http://www.cisco.com/web/about/ac79/ docs/innov/IoT_IBSG_0411FINAL.pdf

[4] The Zettabyte Era-Trends and Analysis. Cisco, May 2013. [Online]. Available:http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ ns537/ns705/ns827/VNI_Hyperconnectivity_WP.html

[5] D. Lake, A. Rayes, and M. Morrow, "The Internet of Things," Internet Protocol J., vol. 15, no. 3, pp. 10–19, Sep. 2012. [Online]. Available: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_15-3/ 153_Internet.html

[6] ARM targets Internet of Things with New Low-Power Chip. Institute of Nanotechnology.[Online]. Available: http:// www. Instituteofnanotechnology.co.uk/arm-targets-Internet-of-things-withnew-low-power-chip

[7] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012–2017. Cisco, Feb. 2013. [Online]. Available: http://www. cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/ white_paper_c11-520862.html

[8] O. Bello and S. Zeadally, "Communication issues in the Internet of Things," in Next Generation Wireless Technologies: 4G and Beyond. London, U.K.: Springer-Verlag, 2013, pp. 189–219.

[9] J. Apcar, "Routing in the Internet of Things/M2M Networks," presented at the Ciscolive365, Melbourne, VIC, Australia, 2013, BRKSPG-1661. [Online]. Available: https://www.ciscolive365.com

[10] S. Yu and Y. Peng, “Research of routing protocol in RFID-based Internet of Things,” Int. J. Comput. Inf. Technol., vol. 1, no. 2, pp. 94–96, Nov. 2012.

Chapter 1: Introduction to IoT

IoT covers many areas ranging from enabling technologies and components to several mechanisms to effectively integrate these low level components. Software is then a discriminant factor for IoT systems. IoT operating systems are designed to run on small scale components in the most efficient way possible, while at the same time providing basic functionalities to simplify and support the global IoT system in its objectives and purposes. Middleware, programmability – in terms of application programming interfaces (APIs) – and data management seem to be key factors for building a successful system in the IoT realm. Management capabilities are needed in order to properly handle systems that can potentially grow up to millions of different components. In this context, self-management and self-optimization of each individual component and/or subsystem maybe strong requirements. In other words, autonomics behaviors could become the norm in large and complex IoT systems. Data security and privacy will play an important role in IoT deployments. Because IoT systems will produce and deal with personally identifiable information, data security and privacy will be critical from the very beginning. Services and applications will be built on top of this powerful and secure platform to satisfy business needs. So many applications are envisioned as well as generic and reusable services. This outcome will require new, viable business models for IoT and its related ecosystems of stakeholders. Finally, IoT can have an impact on people and the society they live in, and so it must be conceived and conducted within the constraints and regulations of each country.

IoT is a brand new concern but the actual idea of interconnected devices had been around longer, at least since the 70s. Back then, the idea was often called “embedded internet” or “pervasive computing”. But the actual term “Internet of Things” was coined by Kevin Ashton in 1999 during his work at Procter & Gamble. Ashton who was working in supply chain optimization, wanted to attract senior management’s attention to a new exciting technology called RFID.

With the advent of the Internet, people have become increasingly interconnected at an unprecedented scale [1]. Therefore, not only humans are being interconnected, but devices also are being interconnected. This paradigm shift has led to the concept of the Internet of Things (IoT). However, due to the rapid promotion of IoT technology, there arises some confusions about its types and verities. In broad strokes, there are four main components of an IoT system:

The Thing itself (the device)

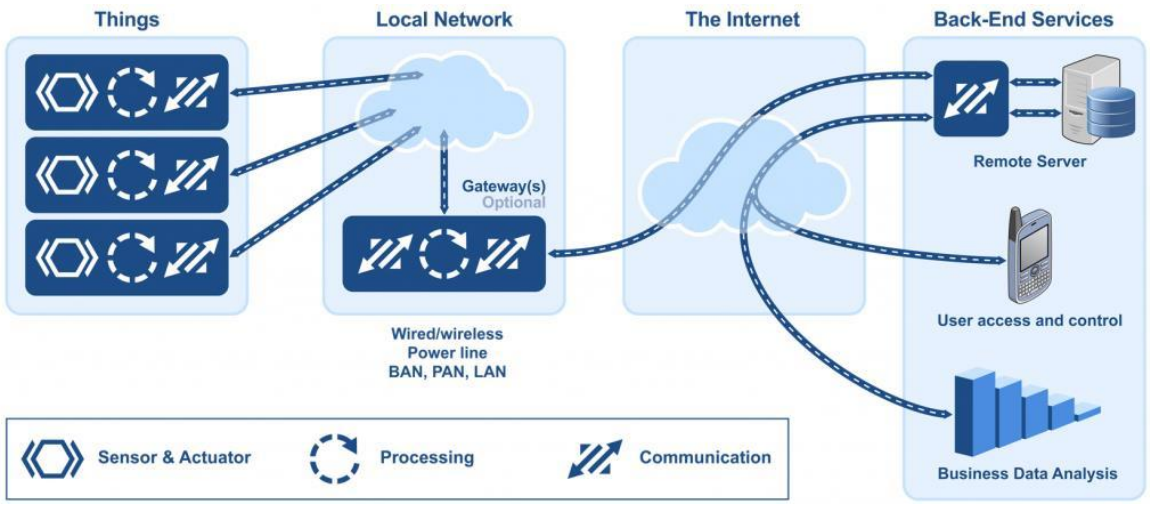


Fig 1.1: The IoT from an embedded systems point of view [1]

IoT systems are not complicated, but designing and building them can be a complex task. And even though new hardware and software is being developed for IoT systems, we already have all the tools we need today to start making the IoT a reality.

We can also separate the Internet of Things in two broad categories:

Industrial IoT, where the local network is based on any one of many different technologies. The IoT device will typically be connected to an IP network to the global Internet.

Commercial IoT, where local communication is typically either Bluetooth or Ethernet (wired or wireless). The IoT device will typically communicate only with local devices. So to better understand how to build IoT devices, you first need to figure out how they will communicate with the rest of the world.

D2D communication technologies (e.g., Bluetooth, Zigebee, and WiFi) are popular networks that will exist in the IoT. Lately, cellular D2D communication has also become an area of interest. Therefore, it is essential to look into how intelligent D2D communication can be achieved in the IoT.

The IoT is a radical evolution of the current Internet, which has been transformed from providing human interconnection into a network of interconnected devices. These devices interact with the physical world using Internet protocols and standards in order to collect data from the environment. The IoT will enable the transformation of sensed or gathered data into intelligent

information, thus embedding intelligence into our environment. In addition, the IoT will involve billions of devices that have the ability to report their location, identity, and history over wireless connections.

The realization of the IoT is gradually coming into fruition as a result of several major trends. Advancements in the field of digital electronics have immensely contributed to the development of miniature devices that can sense, compute, and wirelessly communicate within short distances. These devices exist as part of our everyday lives in areas such as health care, smart grid, home appliances, retail, etc. In addition, the decreasing costs of these devices have also led to a drastic increase in their deployments in recent years. According to, in 2003, when there were about 6.3 billion people in the world, only 500 million devices were connected to the Internet. Thus, at that time, there was less than one device per person. As a result, the IoT did not yet exist in 2003 since the number of connected devices was relatively low. Subsequent to 2003, after the unveiling of the first set of smartphones and tablet personal computers by manufacturers, there was a gradual increase in the number of connected devices. By 2010, the number of devices connected to the Internet rose to 12.5 billion while the world's population increased to 6.8 billion, making the number of connected devices per person more than one for the first time in history. From a recent forecast outlined in, the number of connected devices will double compared with the number of humans on earth by 20l3 and will grow to an estimated 25 billion connected devices by 2015, when the world's population is expected to be about 7.2 billion. Moreover, it has been predicted that almost 50 billion devices will be connected by 2020. The number of devices will rise to over four times as high as the global population. This increase will be accelerated in part by the enhanced capabilities of devices used every day to orchestrate and manage human activities.

1.1 History of IoT

Radio frequency identification, or RFID, may be a crucial technology for IoT. The roots of RFID technology can be traced back to World War II. The Germans, Japanese, Americans and British all used radar—discovered in 1935 by Scottish physicist Sir Robert Alexander WatsonIWatt—to warn of approaching enemy planes while they were still miles away. But there was no way to identify which planes belonged to the enemy and which were a country's own pilots returning from a mission.

The Germans discovered that if pilots rolled their planes as they returned to base, it would change the radio signal reflected back to radar systems. This crude method

alerted the radar crew on the ground that these were German planes and not allied aircraft. Essentially, this was the first passive RFID system.

Under Watson Watt, who headed a secret project, the British developed the first active "identify friend or foe" (IFF) system. When a British plane received British radar signals, it would broadcast a signal back that identified the aircraft as friendly. RFID works on this same basic concept. A signal is sent to a transponder, which wakes up and either reflects back a signal (passive system) or broadcasts a signal (active system).

Advances in radar and radio frequency (RF) communications systems continued through the 1950s and 1960s. Scientists and academics in the United States (U.S.), Europe and Japan explored how RF energy could be used to identify objects remotely. Companies began commercializing antitheft systems that used radio waves to determine whether an item had been paid for or not. Electronic article surveillance tags, for instance, which are still used in packaging today, have a 1Ibit tag. The bit is either on or off. If someone pays for the item, the bit is turned off, and a person can leave the store. But if the person doesn't pay and tries to walk out of the store, automated readers at the door detect the tag and sound an alarm.

Mario W. Cardullo claims to have received the first U.S. patent for an active RFID tag with rewritable memory on January 23, 1973. That same year, Charles Walton, a California entrepreneur, received a patent for a passive transponder used to unlock a door without a key. In the latter application, a card with an embedded transponder communicated a signal to a reader near the door. When the reader detected a valid identity number stored within the RFID tag, the reader unlocked the door. Walton licensed the technology to Schlage, a lock maker, and other companies.

The US government was also working on RFID systems. In the 1970s, Los Alamos National Laboratory was asked by the U.S. Department of Energy (U.S. DOE) to develop a system for tracking nuclear materials. A group of scientists devised the concept of putting a transponder in a truck and readers at the gates of secure facilities. The gate antenna would wake up the transponder in the truck, which would respond with an ID and, potentially, other data, such as the driver's ID. This system was commercialized in the midI1980s when the Los Alamos scientists who worked on the project left to form a company to develop automated toll payment systems. These systems have become widely used on roads, bridges and tunnels around the world.

At the request of the U.S. Department of Agriculture, Los Alamos also developed a passive RFID tag to track cows and doses of hormones and medicines they'd received. It was difficult to ensure that each cow got the right dosage and wasn't given two doses accidentally. Los Alamos came up with a passive RFID system that used UHF

radio waves. The device drew energy from the reader and simply reflected back a modulated signal to the reader using a technique known as backscatter.

Later, companies developed a low frequency (125 kHz) system, featuring smaller transponders. A transponder encapsulated in glass could be injected under a cow's skin. This system is still used in cows around the world today. Low frequency transponders were also put in cards and used to control access to buildings.

Over time, companies commercialized 125 kHz systems and then moved up the radio spectrum to a high frequency band (13.56 MHz), which was unregulated and unused in most parts of the world. High frequency RF offered greater range and faster data transfer rates. Companies, particularly those in Europe, began using it to track reusable containers and other assets. Today, 13.56 MHz RFID systems are used for access control, payment systems (e.g., Mobile Speed pass) and contactless smart cards. They are also used in antitheft devices in cars. A reader in the steering column reads the passive RFID tag in the plastic housing around the key. If it doesn't get the ID number it is programmed to look for, the car won't start.

In the early 1990s, IBM engineers developed and patented an ultrahigh frequency (UHF) RFID system. UHF offered longer read range (up to 20 feet under good conditions) and faster data transfer. IBM did some early pilots with WalIMart, but never commercialized this technology. When it ran into financial trouble in the midI1990s, IBM sold its patents to Intermec, a bar code systems provider. Intermec RFID systems have been installed in numerous different applications, from warehouse tracking to farming. But the technology was expensive at the time due to the low volume of sales and the lack of open, international standards.

UHF RFID got a boost in 1999, when the Uniform Code Council, EAN International, Procter & Gamble and Gillette put up funding to establish the AutoIID Center at the Massachusetts Institute of Technology (MIT). Two professors there, David Brock and Sanjay Sarma, had been researching the possibility of putting lowIcost RFID tags on all products to track them through the supply chain. Their idea was to put only a serial number on the tag to keep the price down, as a simple microchip that stored very little information would be less expensive to produce than a more complex chip with more memory. Data associated with the serial number on the tag would be stored in a database that would be accessible over the Internet.

Sarma and Brock essentially changed the way people thought about RFID in the supply chain. Previously, tags were a mobile database that carried information about the product or container they were on with them as they traveled. Sarma and Brock turned RFID into a networking technology by linking objects to the Internet through the tag (Roberti, "History of RFID," 2005). For businesses, this was an important change, because now a

manufacturer could automatically let a business partner know when a shipment was leaving the dock at a manufacturing facility or warehouse, and a retailer could automatically let the manufacturer know when the goods arrived.

Between 1999 and 2003, the AutoIID Center gained the support of more than 100 large endI user companies, plus the U.S. Department of Defense and many key RFID vendors. It opened research labs in Australia, the United Kingdom, Switzerland, Japan and China. It developed two air interface protocols (Class 1 and Class 0), the Electronic Product Code (EPC) numbering scheme (Sarma et al., "RFID Systems," 2003), and a network architecture for looking up data associated on an RFID tag on the Internet (Brock, "Electronic Product Code," 2001). The technology was licensed to the Uniform Code Council in 2003, and the Uniform Code Council created EPCglobal, as a joint venture with EAN International, to commercialize EPC technology. The AutoIID Center closed its doors in October 2003, and its research responsibilities were passed on to AutoIID Labs.

The AutoIID Center used the term "Internet of Things" beginning in about 2000 and heavily promoted the concepts and ideas of a connected world with the EPC system as the basis of how things are connected to the Internet. Though Kevin Ashton (then the executive director of the AutoIID Center) claims to have coined the term "Internet of Things," according to Prof. Daniel Engels, the term was used in a 1997 publication by the International Telecommunication Union (ITU) (Thiesse et al., "Overview of EPC," 2006).

1.3 IoT Elements

The generic IoT scenario can be identified with that of a generic user that needs to interact with a (possibly remote) physical entity. In this short description we have already introduced the two key actors of the IoT, the "user" and "physical entity" (CASAGRAS [1], "Final Report," 2009).

I. User

A person or some kind of active digital entity (e.g., a service, an application or a software agent) that has a goal. The attainment of the goal is achieved via interaction with the physical environment. This interaction is mediated by the IoT.

II. Physical entity

A “physical entity” may be defined as a discrete, identifiable part of the physical environment which is of interest to the user for the attainment of his/her goal. Physical entities can be almost any object or environment, from humans or animals to cars, from store or logistic chain items to computers, from electronic appliances to closed or open environments. Physical entities are represented in the digital world via a virtual entity. There are many kinds of digital representations of physical entities: 3D models, database entries, objects (or instances of a class in an object oriented programming language), even a social network account could be viewed as such a representation. In the IoT context, virtual entities have two fundamental properties:

" They are digital entities that are associated with a single physical entity that they represent. While ideally there is only one physical entity for each virtual entity, it is possible that the same physical entity can be associated with several virtual entities, e.g., a different representation per application domain or per IT system. Each virtual entity must have one and only one ID that identifies the represented object. Digital entities can be either active elements (e.g., software code) or passive elements (e.g., a database entry). " Ideally, digital entities are synchronized representations of a given set of aspects or properties of the physical entity. This means that relevant digital parameters representing the characteristics of the physical entity can be updated upon any change of the physical entity. Conversely, changes that affect the virtual entity could manifest themselves in the physical entity.

Augmented entity is defined as the composition of a physical entity and its associated virtual entity. Any changes in the properties of an augmented entity have to be represented in both the physical and digital world. This is what actually enables everyday objects to become part of digital processes.

III. Device

A “device” is used to achieve the association between virtual and physical entity. This is done by embedding, attaching or simply placing the device in close proximity to the physical entity. Devices provide the technological interface for interacting with or gaining information about the physical entity. By so doing the device actually enhances the physical entity and allows the latter to be part of the digital world. A device thus mediates the interactions between physical entities (that have no projections in the digital world) and virtual entities (which have no projections in the physical world), generating a paired couple that can be seen as an extension of either one. Devices are thus technical artifacts for bridging the real world of physical entities with the digital world of the Internet. This is done by providing monitoring, sensing, actuation, computation, storage and processing capabilities in the device.

From a functional point of view, devices can belong to any of the following types.

One of the characteristics of IoT is ubiquity, which can be realized through unique identification of the “things” that are connected to the Internet. This unique identification is done by attaching tags on the “things.” Tags are used by specialized sensors typically known as readers. Their sole purpose is to facilitate an identification process. RFID is a perfect solution for providing this unique identification of “things.”

The transponder or tag of an RFID is used to carry data, which is located on the object to be identified. This normally consists of a coupling element (such as a coil or microwave antenna) and an electronic microchip, less than one third millimeter in size. Tags can be passive, semipassive or active, based on their power source and the way they are used, and can be readonly, read/write or read/write/rewrite, depending on how their data is encoded. Tags do not need a built in power source, as they obtain the energy they require to function from the electromagnetic field emitted by readers. " An interrogator or reader reads the transmitted data (e.g., on a device that is handheld or embedded in a wall). Compared with tags, readers are larger, more expensive and powerIhungry. In the most common type of system, the reader transmits a low power radio signal to power the tag (which, like the reader, has its own antenna). The tag then selectively reflects energy and thus transmits some data back to the reader, communicating its identity, location and any other relevant information. Most tags are passive, and activated only when they are within the coverage area of the interrogator. While outside this area, they remain dormant. Information on the tag can be received and read by readers and then forwarded to a computer database. Frequencies currently used for data transmission by RFID typically include 125 kHz (low frequency), 13.56 MHz (high frequency) or 800I960 MHz (ultrahigh frequency). RFID standards relate both to frequency protocols (for data communication) and data format (for data storage on the tag). "Sensors provide information about the physical entity they monitor. Information in this context ranges from the identity of the physical entity to measures of the physical state of the physical entity. Like other devices, sensors can be attached or otherwise embedded in the physical structure of the physical entity or be placed in the environment and indirectly monitor entities. An example of the latter is a camera that recognizes people’s faces. Information from sensors can be stored for later retrieval. " Actuators can modify the physical state of a physical entity. Actuators can move (translate, rotate, etc.) simple physical entities or activate/deactivate functionalities of more complex ones.

IV. Sensor Operating Systems

Most operating systems (OS) that may be used for IoT were designed for wireless sensor networks (WSN) like TinyOS and Contiki. But, practically, it seems that most of the OSs that were designed for use in WSN fail to meet one or more of the

requirements of IoT. The developers of RIOT claim that they've bridged this gap of OS requirements between WSN and IoT.

Chapter 2: An evolution from Intranet of Things to Internet of Things

A new approach to the design of internet structures has recently been proposed, in which internet has been expanded with new dimensions. Earlier, we have connected devices within an unplanned infrastructure. A device connected with another with an inter network, referred as Intranet of things but now we have surpassed the web of things which are interconnected to each other, rather we are concentrating on devices which can be connected remotely to another end within a coherent network which is known as Internet of Things. The recipe of determining the difference between Intranet of Things to Internet of Things is the boundary. Intranet of Things gave us the ease of personal use of the device to device communications but by Internet of Things, we can ascribe its functionality by wider usage in industrial purpose. By Internet of Things, we consider basic things like the right infrastructure with a central middleware, its various bus and network systems and controlling via smartphone, tablet or web browser. This is a great tool to enhance the credibility of communication, systematically which is much more integrated and heterogeneous in nature. From now on IoT will refer Internet of Things throughout the whole paper.

2.1 IoT & its future challenges

In order to attain a matured technology for wide deployment and market integration of IoT, we have to concentrate on its design complexity and consequences. This part is covering all technologies needed to make IoT systems function smoothly as a standalone solution or part of existing systems and that's not an easy mission, there are many technological challenges, including Security, Connectivity, Compatibility & Longevity, Standards and Intelligent Analysis & Actions. First of all, the communication strategy needs to be taken under serious close thought. The initial solution that is presumed- a lift from IPv4 to IPv6 is not a permanent solution at all. Connecting so many devices will be one of the biggest challenges of the future of IoT, and it will defy the very structure of current communication models and the underlying technologies. At present we rely on the centralized, server/client paradigm to authenticate, authorize and connect different nodes in a network.

This model is sufficient for current IoT ecosystems, where tens, hundreds or even thousands of devices are involved. But when networks grow to join billions and hundreds of billions of devices, centralized systems will turn into a bottleneck. Such systems will require huge investments and spending in maintaining cloud servers that can handle such large amounts of information exchange, and entire systems can go down if the server becomes unavailable.

The future of IoT will very much have to depend on decentralizing IoT networks. Part of it can become possible by moving some of the tasks to the edge, such as using fog computing models where smart devices such as IoT hubs take charge of mission-critical operations and cloud servers take on data gathering and analytical responsibilities.

Other solutions involve the use of peer-to-peer communications, where devices identify and authenticate each other directly and exchange information without the involvement of a broker. Networks will be created in meshes with no single point of failure. This model will have its own set of challenges, especially from a security perspective, but these challenges can be met with some of the emerging IoT technologies such as Block chain.

Moreover, technology standards which include network protocols, communication protocols, and data-aggregation standards, are the sum of all activities of handling, processing and storing the data collected from the sensors. This aggregation increases the value of data by increasing, the scale, scope, and frequency of data available for analysis.

2.2 Challenges facing the adoptions of standards within IoT

Standard for handling unstructured data: Structured data are stored in relational databases and queried through SQL for example. Unstructured data are stored in different types of NoSQL databases without a standard querying approach.

Technical skills to leverage newer aggregation tools: Companies that are keen on leveraging big-data tools often face a shortage of talent to plan, execute, and maintain systems.

No doubt that IoT creates unique challenges to privacy, many that go beyond the data privacy issues that currently exist. Much of this stems from integrating devices into our environments without us consciously using them. Hence it is becoming more prevalent in consumer devices, such as tracking devices for phones and cars as well as smart televisions. In terms of the latter, voice recognition or vision features are being integrated that can continuously listen to conversations or watch for activity and selectively transmit that data to a cloud service for processing, which sometimes includes a third party. The collection of this information exposes legal and regulatory challenges facing data protection and privacy law.

In addition, many IoT scenarios involve device deployments and data collection activities with multinational or global scope that cross social and cultural boundaries. What will that mean for the development of a broadly applicable privacy protection model for the IoT?

In order to realize the opportunities of the IoT, strategies will need to be developed to respect individual privacy choices across a broad spectrum of expectations, while still fostering innovation in new technologies and services.

2.1.1 Communications strategy

There are several opinions that support IPv6 is a key enabler for the future IoT. As the number of devices increase by the time, hence device to device (D2D) communication potentially increases; IPv4 cannot afford to maintain the spontaneous flow of devices. Moreover, IPv6 is a fully internet compliant. In other words, it is possible to use a global network to develop one's own network of smart things or to interconnect one's own smart things with the rest of the World.

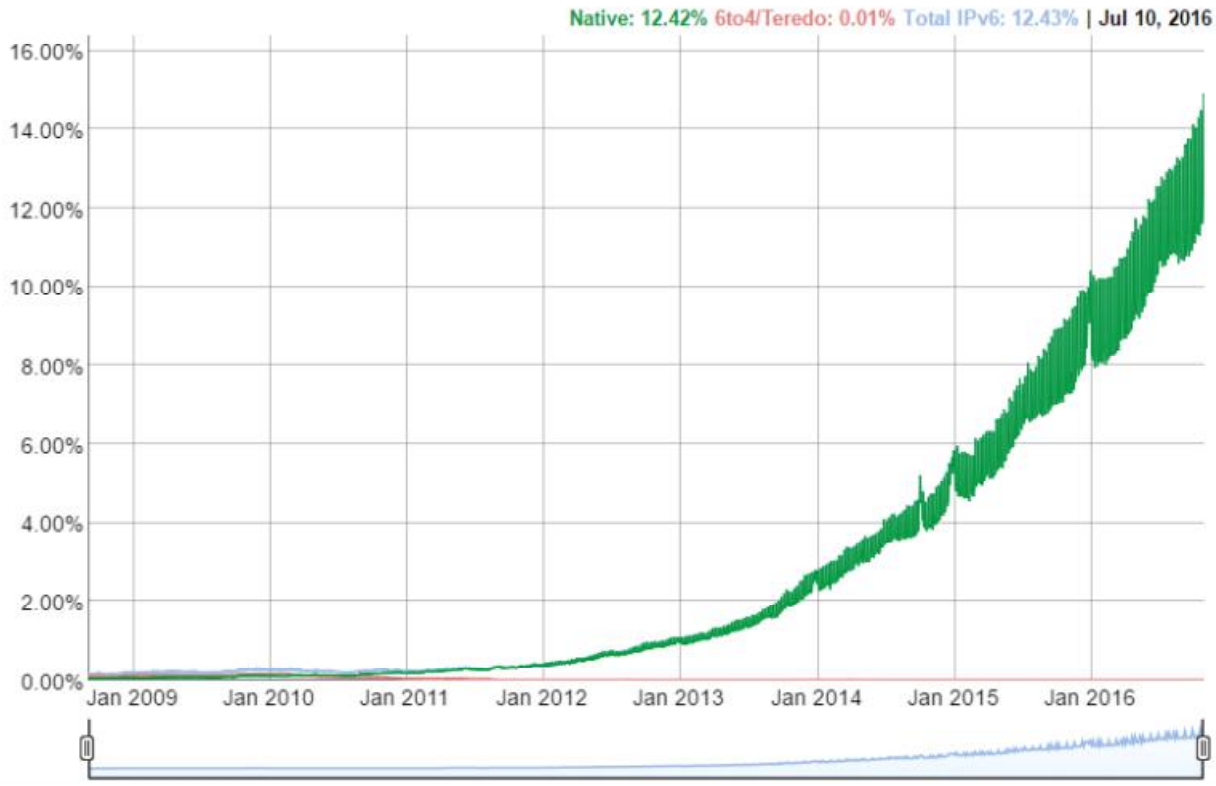


Fig 1.2: User engagement of IPv6 [2]

2.1.2 Heterogeneity

IoT is approaching towards the unique challenge of making an object oriented world. At the beginning, IoT was concentrating on various digital things such as RFID (Radio Frequency IDentification), sensor or smart phones which are interconnected and can communicate with each other. So that, we got the concepts of smart objects and smart technologies from IoT at the beginning. From the recent adaptation of enabling device technology such as RFID tags and readers, Wireless Sensor Networks (WSN), Near Field Communication (NFC) devices, Bluetooth Low Energy and actuator nodes, IoT has moved out from its immaturity and become the next revolutionary combined Internet. Though WSN with IPv6 connectivity such as 6LoWPAN is considered as the main infrastructure of IoT, WSN basically consists of homomorphic devices sharing the same network types and protocols. In upcoming future, there will be trillion of devices with IPv6 connectivity which would participate to serve people through D2D or M2M interaction arranged by IoT and it will have major impacts on infrastructure, industry standards, security and business models throughout the entire IT ecosystem. The IoT will embrace, leverage, extend and enhance cloud, big data, personal devices and social networks to provide more pulverized sensor and devices closer to the edge. So, to make a smart world with the maximum range of technologies, the development of IoT architecture is much more necessary for the heterogeneity.

2.1.3 Security

IoT security has become one of the major concerns right now. It creates unique challenges to privacy, many that go beyond the data privacy issues that currently exist. Much of this stems from integrating devices into our environments without us consciously using them.

This is becoming more prevalent in consumer devices, such as tracking devices for phones and cars as well as smart televisions. In terms of the latter, voice recognition or vision features are being integrated that can continuously listen to conversations or watch for activity and selectively transmit that data to a cloud service for processing, which sometimes includes a third party. The collection of this information exposes legal and regulatory challenges facing data protection and privacy law.

In addition, many IoT scenarios involve device deployments and data collection activities with multinational or global scope that cross social and cultural boundaries. What will that mean for the development of a broadly applicable privacy protection model for the IoT?

In order to realize the opportunities of the IoT, strategies will need to be developed to respect individual privacy choices across a broad spectrum of expectations, while still fostering innovation in new technologies and services

IoT is not excessively extended and deployed because of the hardles in configuring (IPSec) for the end users and the lack of scalable certificate management for DTLS[2]. On the other hand, the ESP scheme needs to be optimized in terms of proper cryptographic ensembles. Moreover, IPSec packets can force the packet to be fragmented; thus an extra packet must be sent to the link layer which will consume more energy. In addition, this overhead problem is worse with the Encapsulation Security Protocol (ESP) mode of IPSec, since the internal headers of IPv6 and UDP[3] are encrypted and consequently cannot be compressed.

2.2 Why IPv6?

The things are connected to the internet are increasing rapidly and there will be approximately 20 billion connected 'things' by 2020. The internet of things and IPv6 are strongly aligned, to the extent that claims are made they are mutually reliant. An internet of things needs massively expanded protocol addresses space that only IPv6 can provide. IPv6 is very important when every connected home appliance and street will need an IP address.

IPv6 offers a highly scalable scheme. After noticing the rising numbers of connecting things, it's easy to understand why IPv6 is important for IoT devices. IPv6 provides 2^128 unique addresses which represents 3.4*10^38 addresses. In other words, more than 2 billion of billions addresses per square millimeter of the earth surface. It's quit sufficient to addresses the needs of any present and future communicating device.

With billions of new smart products being created everyday, security is an important thought. IPv6 offers better security solutions than its predecessor, largely due to IPSec. It can run end-to-end encryption. The encryption and integrity-checking used in current virtual private network (VPNs) are standard component in IPv6. IPv6 also support more-secure name resolution. The Secure Neighbor Discovery (SEND) protocol is capable of enabling cryptographic confirmation that a host is who it claims to be at the time of the connection.

IPv6 is fully internet compliant. In other words it's possible to use a global network to develop one's own network of smart things or to interconnect one's own smart things with the rest of the world.

3 ID separators: The unique need for increasing networks

As devices and related networks are increasing in an exponential manner, it is important to withstand the analogy of separate IDs. In current Internet, 'static' host is the basic assumption, whereas 'mobile' host is treated as a special case, as shown in MIP. It is quite reasonable approach in the fixed host dominant environment, but it should be completely opposite in the mobile dominant one. Locator ID separation has been considered as a qualitatively better approach for mobility support while improving network security and scalable routing. As IP address is used in network layer protocol as the locator to find the host and forward the data packets towards the destination, it has different set of values for host IDs and locators.

HIP uses public keys (and their hash values) as host IDs and IP addresses as locators. A new layer, called the identity layer, inserted between the transport and network layers of the host protocol stack performs the host ID-to-locator mapping functions. This value extends the Domain Name System (DNS) records to store host IDs where a host acquires its peer host's ID and locator by sending a domain name lookup request to a DNS server. While communicating with the peer host, both the source and destination hosts' IDs appear in the identity header and locators in the network header of data packets.

Although HIP is a good step in developing a locator ID separation-based mobility scheme, it is still in its infancy and lacks several functions. It has no support for smooth handover. Its session initiation process is computationally heavy, making it inappropriate for small, resource-limited devices. It uses locators in some signaling messages, thus necessitating the re-establishment of session contexts in the event of switching locators. This requirement is counterproductive to fast handover.

Another ID/locator split-based mobility protocol is LINA. Sublayer concept is introduced in this method in network layer. IDs of 128-bit length are formed by concatenating location-independent prefixes (of 64 bits) and node IDs (of 64 bits), while locators are formed by concatenating location-dependent network prefixes and node IDs. It is divided into two sublayers: the identification sublayer and the delivery sublayer. The former carries out the ID-to-locator mapping function and the latter forwards packets using destination locators present in the packet header. It uses mapping agents to resolve IDs into corresponding locators. It is a host-based mobility approach, i.e., there is no support for network-based mobility and smooth handover.

LISP uses prefix summing endpoint IDs (EIDs), which are also used as locators in the edge network. Here, routing locators (RLOC) are used as locators in the transit network. To provide host-mobility, there is a proposal for having the host possess a lightweight version of the ITR/ETR functions. However, it may not be effective for reducing the BGP routing table size, if a distinct RLOC is assigned to each host. Hence, LISP lacks smooth handover functions.

3.1 HIMALIS network

The Heterogeneity Inclusion and Mobility Adaptation through Locator ID Separation (HIMALIS) architecture natively supports mobility by allowing the host to change its address (or locator) used in the network layer while keeping the session identifier used in the application and transport layers unchanged.

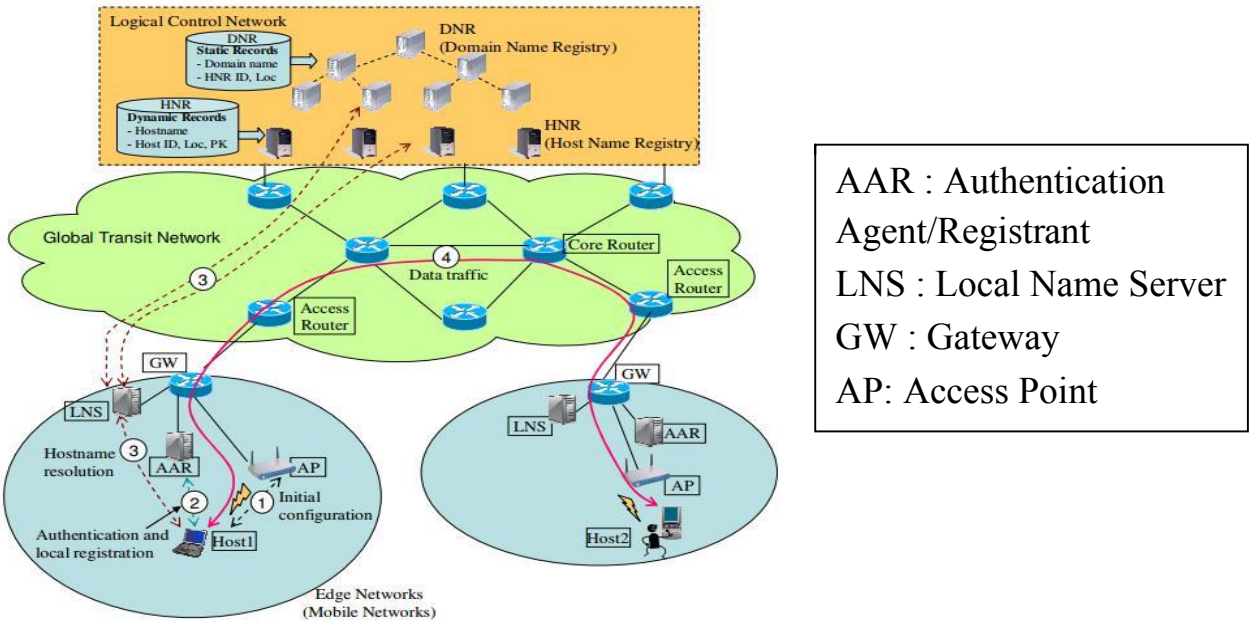


Fig 3.1: HIMALIS network components

It also facilitates faster updates of ID/locator mappings in name resolution servers or registries. However, it still lacks functions for supporting seamless host mobility when a host moves across edge networks and network mobility when a whole edge network moves. To address these issues, this paper presents an optimized host mobility management scheme and a network

mobility management scheme. These schemes employ traffic redirection from the old gateway (or old access router) to the new gateway (or new access router) to reduce packet loss during handovers. Meanwhile, the intrinsic security functions of the HIMALIS architecture are leveraged to protect the newly introduced mobility schemes from various attacks such as impersonation and man-in-the-middle attacks.

Heterogeneity inclusion and mobility adaptation through a locator ID separator (HIMALIS) architecture of the new generation network is being developed as a part of AKARI project. The HIMALIS architecture provides mobility function for handover optimization & supporting heterogeneous network layer protocols. Here, between network and transport layers, we will insert a new layer called 'identity layer'. This layer executes mobility functions in network layer mainly. Here, the mappings among between hostnames, IDs and locators are stored in two different registries. First one is called, Domain name Registry (DNR) and the second one is called Host Name Registry (HNR).

The current version of HIMALIS architecture does not support seamless host mobility because some packets may get lost during a handover. More importantly, it cannot support network mobility by maintaining session continuity when the whole edge network moves. Most importantly, ID based scheme in this network portion is not user friendly at all and very hard to remember for primary level users.

So, here we propose name based architecture in HIMALIS adding up new components for better user experience and more mobility support.

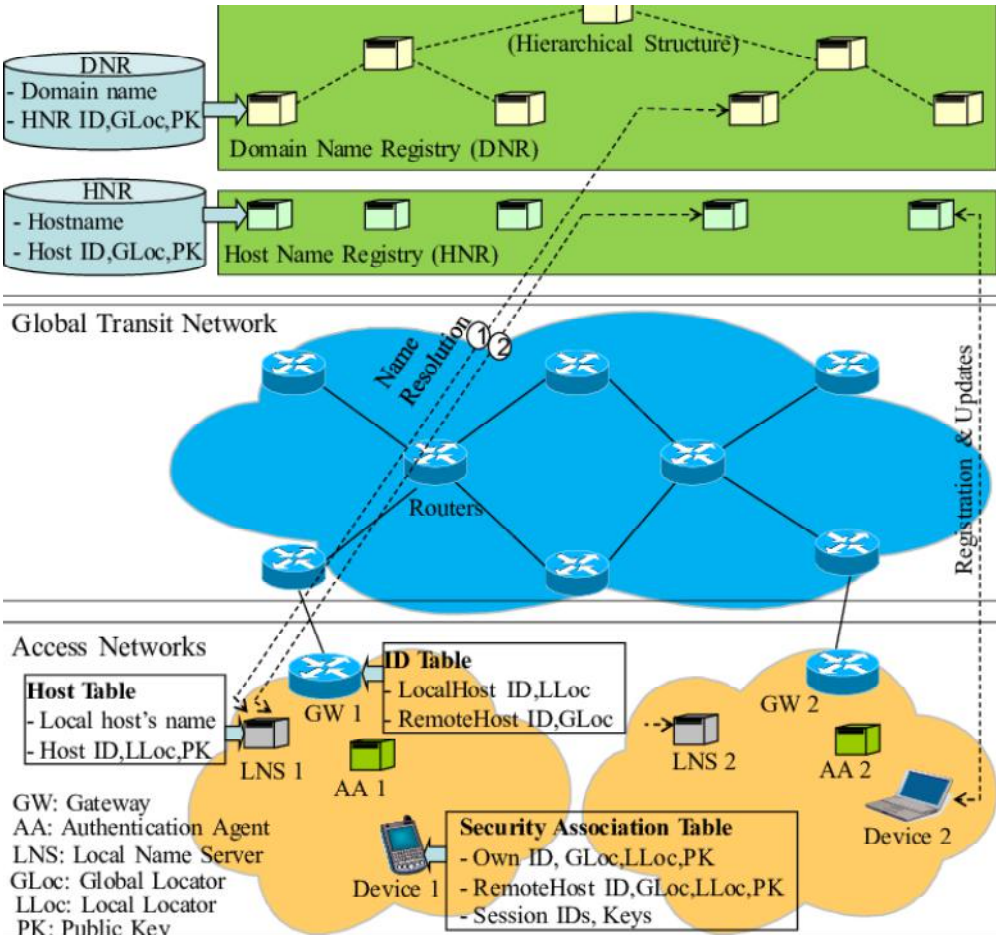


Fig 3.2: Idea of HIMALIS Network

Here, we have introduced a name based server NRS that will convert the device address to a human readable format. From the Edge Network to Global Transit Network, when the bits are transmitted as the stack of numbers, the NRS will convert it into a human readable format (reading hierarchy is given below) and send it to the host's Edge Network for host name lookup. It will translate the location and device address and update ID/Locator mapping in IDRs.

4. A Generic Name Resolution Framework

Mostly, all entities involved in communication are named and not statically bound to their physical locations. To access entities using their names, the Name Resolution Service (NRS) is introduced which will follow <Device Name, Model Number, Device code>

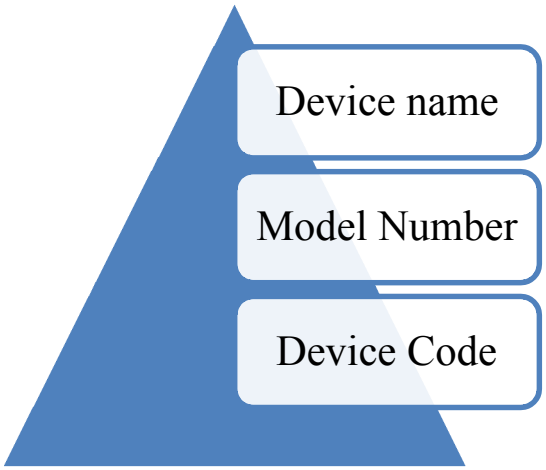
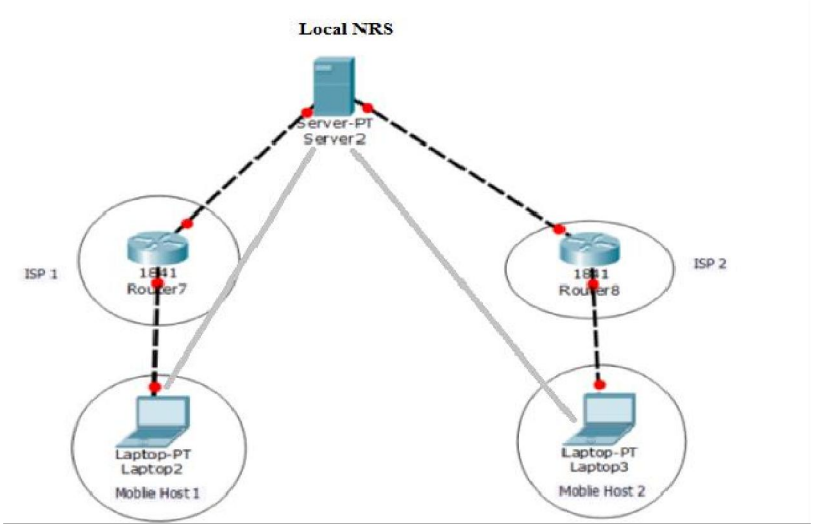


Fig 4.1: High level view of the hierarchy of name based content

Now we will go through some case studies to define exactly how this model will work. A host name is an alias that is assigned to an IP node to identify it as a TCP/IP host. The host name can be up to 255 characters long and can contain alphabetic and numeric characters, hyphens, and periods.

4.1 Case Studies

4.1.1 Case study 1



Here, after “calling” the mobile host, it sends the device address to the NRS. The NRS will map the address into name scheme and send it to the ISP it belongs to. The ISP will send it to the receiver.

4.1.2 Case study 2

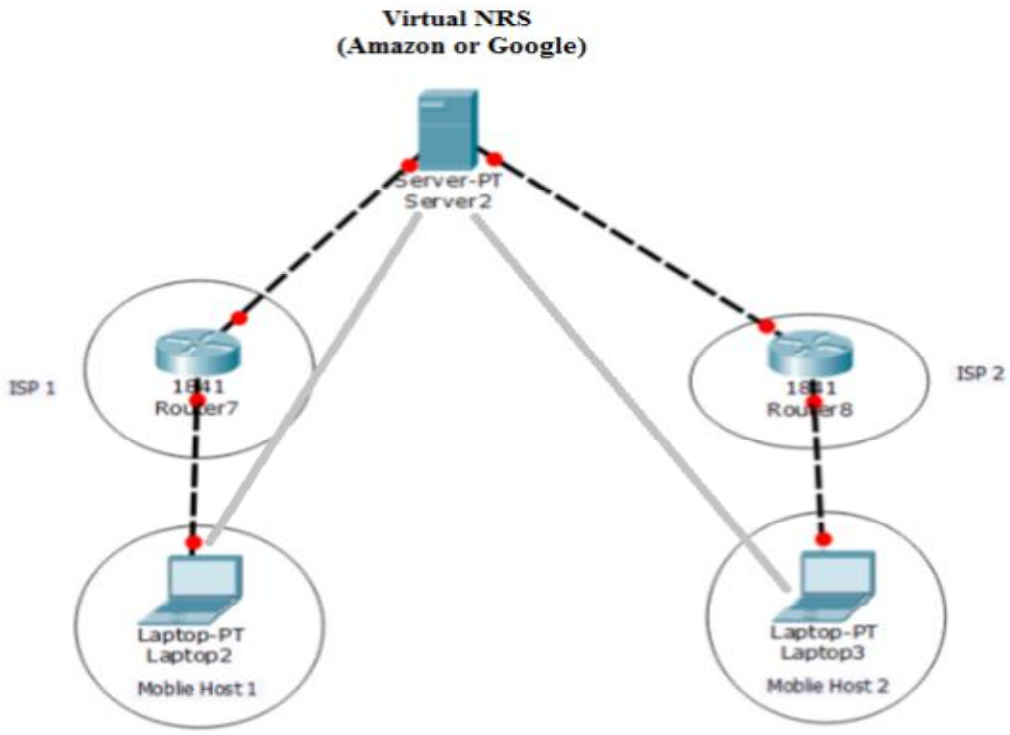


Fig 4.1: High Level view of D2D communication via NRS

The naming policy may not be adopted by all the manufacturing companies in a while. So for the time being, we propose another server to convey the conversion and transmission scheme for the time being. It should work as a digital process. We may regard google server or amazon web service as an example.

5 Simulations and Results

We simulate our proposed NRS architecture for ICN with nnnSIM (Lopez, 2015). Like NDN's simulator, ndnSIM (Afanasyev, Moiseenko, & Zhang, 2012), our simulator is a ns-3 (ns-3 Developers, 2015) module that implements our network architecture. The soundness of our proposed architecture is analyzed for the scenario where user sends the data packet to NRS and it comes back to foremost endpoints.

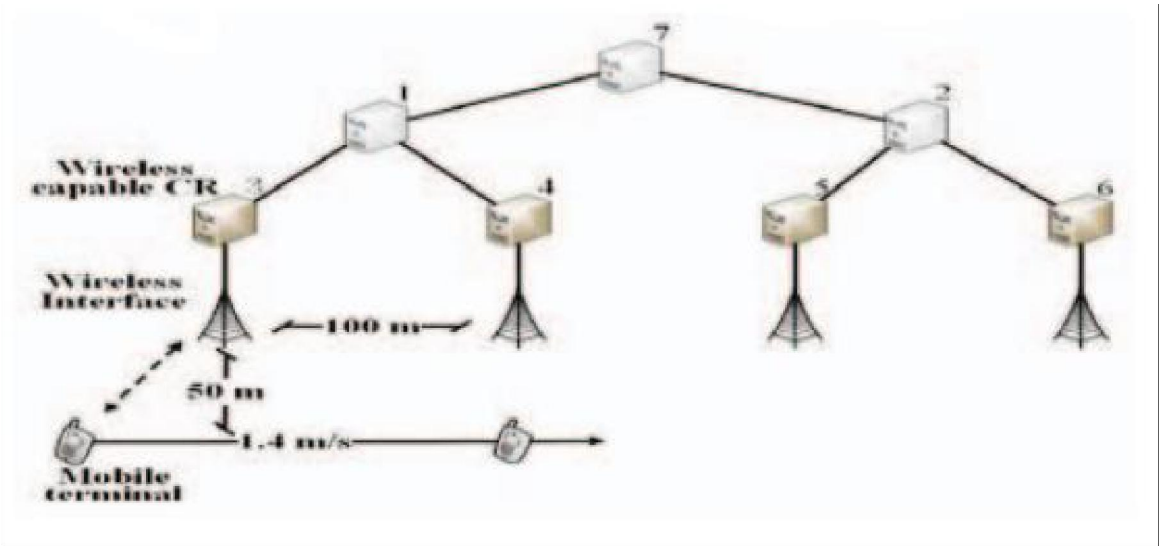


Fig 5.1: Simulation topology

Table 5.1: Simulation parameters

Simulation time	400m/ mobile node speed (10s)
Mobile node speed	1.4, 2.8, 5.6, 7, 8.4, 11.2 m/s
BW/ link capacity	100 Mbps
Link delay (wired)	1 ms
Link delay (wireless)	Constant speed propagation Three log distance propagation Nakagami propagation
Device tracing signal generation rate	120 kbit/s
Interest packet generation rate	148/s
Interest retransmit timer	50 ms
Forwarding strategy	Smart flooding

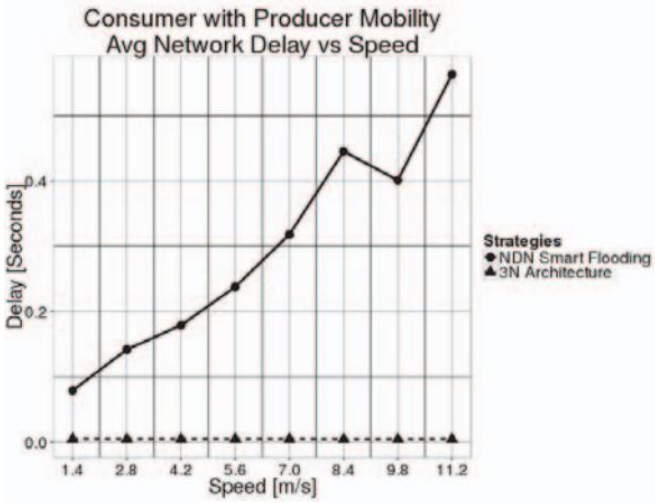


Fig 5.1: Mobility calculation- Delay vs Speed

6 Conclusions

The evolution in communications is a must for modern technology adaptation. For this, D2D communication has become an integral part of the IoT environment to design, deploy, and maintain a sustainable IoT ecosystem. Researchers in the academia and industry are currently addressing many issues. Some of the IoT research issues include energy efficiency, routing, security, context-awareness protocols, etc. In this paper, we focus on issues that impact intelligent D2D communication in the IoT environment.

6.1 Related Works

Unlike naming the IoT devices, the way of acknowledging any final product is changing. The proposed hierarchy implements functionality above the current Internet architecture, ensuring sustainable growth in D2D communications. Here are some works related to the field of communications.

The Data-Oriented Network Architecture replaces DNS names with flat, self-certifying names and a name-based anycast primitive above the IP layer. Names in DONA are a cryptographic digest of the publisher's key and a potentially user-friendly label – however, that label is not securely bound to the content, allowing substitution attacks. Unlike CCN, data cannot be generated dynamically in response to queries – content in DONA must first be published, or registered, with a tree of trusted resolution handlers (RHs) to enable retrieval. Each resolution handler must maintain a large forwarding table providing next hop information for every piece of content in the network. Once the content is located, packets share exchanged with the original

request erusing standard IP routing. If the location of apiece of content changes, new requests for it will fail until the new registration propagates through the network. CCN, in contrast, can forward requests to all the places a piece of content is likely to be.

A number of systems make use of distributed hash tables (DHTs) to route queries for opaque content names. ROFL (Routing on Flat Labels) evaluates the possibility of routing directly on semantic free flat labels [7]. A circular namespace is created to ensure correct routing (as in Chord), but additional pointers are added to shorten routes. In a similar approach, i3 separates the acts of sending and receiving by using a combination of packet identifiers and a DHT. Receivers insert a trigger with the data identifier and their address into the DHT. The trigger is routed to the appropriate sender, who fulfills the request by responding with the packet containing the same id and the requested data. SEATTLE utilizes flat addressing with a one-hop DHT to provide a directory service with reactive address resolution and service discovery. Unlike CCN, all of these systems require content be explicitly published to inform the DHT of its location before it can be retrieved. Also unlike CCN, this retrieval is largely free of locality–queries might retrieve a cached copy of data along their routed path, but are not guaranteed to retrieve the closest available copy.

Instead of routing end-to-end based on an identifying name, the PSIRP project proposes using rendezvous as a network primitive. Each piece of data has both a public and private label used for verifying the publisher and making routing decisions. Consumers receive content by mapping the desired, user-friendly name to an opaque public label via an unsecure directory service. The label is then used to subscribe to the piece of data, triggering the system to locate and deliver the corresponding content. Though motivated by the same problems as CCN, PSIRP suffers from its use of unstructured identifiers and lack of strong cryptographic binding between user-meaningful names (or currently, even their opaque labels) to content.

The 4WARD NetInf project has similar goals to CCN but focuses on higher level issues of information modeling and abstraction. It currently uses DONA-style names for Data and Information Objects and provides a publish/subscribe style API. The NetInf Dictionary infrastructure uses a DHT for name resolution and location lookup. TRIAD [8], like CCN, attempts to name content with user friendly, structured, effectively location-independent names.

TRIAD uses URLs as its names using an integrated directory to map from the DNS component of the URL to the closest available replica of that data. It then forwards the request to that next hop, continuing until a copy of the data is found. Its location is returned to the client, who retrieves it using standard HTTP/TCP. TRIAD relies on trusted directories to authenticate content lookups (but not content itself), and suggests limiting the network to mutually trusting content routers for additional security. Research into content-aware routing protocols also attempts to improve delivery performance and reduce traffic overhead. For example, Anand et. al studied the benefits of large-scale packet caching to reduce redundant content transmission. In this work, routers recognize previously forwarded content and strip the content from packets on

the fly, replacing the content portion with a representative finger print. Downstream routers reconstruct the content from their own content cache before delivering to the requester.

6.2 Future Works

As a scope of future work, we will do more extensive simulation to evaluate the performance of other applications like VoIP, HD Video Delivery etc. The implementation of this architecture under more practical network distribution settings will also be required. Among the tests that should be made is the leveraging of the ICN layer's underlying handoff information, the use of a heterogeneous network and multiple and more complicated MN mobility with background traffic.

References

[1] Image url: https://www.micrium.com/iot/devices/#foobox-1/0/internet-of-things.png

[2] https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption&tab=ipv6-adoption

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[2] J. Buckley, "From RFID to the Internet of Things pervasive networked systems," Conference Centre Albert Borschette (CCAB), Brussels, Belgium, Mar. 2006. [Online]. Available: ftp://ftp.cordis.europa.eu/pub/ ist/docs/ka4/au_conf670306_buckley_en.pdf

[3] D. Evans, "The Internet of things: How the next evolution of the Internet is changing everything," Cisco IBSG, San Francisco, CA, USA, Apr. 2011. [Online]. Available: http://www.cisco.com/web/about/ac79/ docs/innov/IoT_IBSG_0411FINAL.pdf

[4] The Zettabyte Era-Trends and Analysis. Cisco, May 2013. [Online]. Available:http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ ns537/ns705/ns827/VNI_Hyperconnectivity_WP.html

[5] D. Lake, A. Rayes, and M. Morrow, "The Internet of Things," Internet Protocol J., vol. 15, no. 3, pp. 10–19, Sep. 2012. [Online]. Available: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_15-3/ 153_Internet.html

[6] ARM targets Internet of Things with New Low-Power Chip. Institute of Nanotechnology. [Online]. Available: http:// www. Instituteofnanotechnology.co.uk/arm-targets-Internet-of-things-withnew-low-power-chip

[7] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012–2017. Cisco, Feb. 2013. [Online]. Available: http://www. cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/ white_paper_c11-520862.html

[8] O. Bello and S. Zeadally, "Communication issues in the Internet of Things," in Next Generation Wireless Technologies: 4G and Beyond. London, U.K.: Springer-Verlag, 2013, pp. 189–219.

[9] J. Apcar, "Routing in the Internet of Things/M2M Networks," presented at the Ciscolive365, Melbourne, VIC, Australia, 2013, BRKSPG-1661. [Online]. Available: https://www.ciscolive365.com

[10] S. Yu and Y. Peng, "Research of routing protocol in RFID-based Internet of Things," Int. J. Comput. Inf. Technol., vol. 1, no. 2, pp. 94–96, Nov. 2012.