ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 6, June 2016

Internet of Things

Anamika Sharma, Er. Sonia Saini

***Abstract*— The Internet of Things is a new concept in IT Field. Route designing is an important part in the field of Internet of Things. Internet of Things is creating an environment of convergence in the society. This technology environment yields a paradigm shift in our professional and personal life. As a connected environment, IOT adds customer value and liability. Nowadays IOT is being performed extremely well in certain fields which is of human related that are stylish and smart city, smart environment, security, smart business process, smart agriculture, home automation and wellness. IOT is build up of layered architecture named application layer, network layer and perception. Each layer has its own components, security issues and working strategy. NLEE algorithm guarantees an improved efficient usage of nodal energies. It also provides the shortest path in the network while routing setup delay is increased.**

***Index Terms*—architecture of IOT, cloud computing, data encryption, security counter measures.**

1. INTRODUCTION

Internet of Things (IOT): Interconnected devices, embedded in all kinds of objects. The IOT is the vision of machine-to-machine communication between devices embedded in things, so-called smart objects [1]. IOT could be conceptually defined as a dynamic global network infrastructure with self configuring potential based on standard and interoperable communication protocols where physical and virtual things have identities, physical properties, and virtual personalities, use intelligent interfaces, and are seamlessly combined into the information network [2]. Now the aim is to link things to each other and establish a chain of command among them, such as connecting Personal Digital Assistant(PDA) devices to home appliances in a master-slave relationship to make our life simpler including connecting home applications to start coffee machines, adjust car seats, etc. With the current situation, only a few devices can be connected with network and limited tasks are performed. To make it limitless; all the devices should interconnect with each other and perform tasks as per the requirement [3].

1.1 RELATION IN THINGS, DEVICES AND RESOURCES:

In order to monitor and communicate with one or more entities and make the connection to the Internet, technical communication devices are necessitating. The devices can be attached to or embedded in the entities themselves – thus creating smart things – or they can be installed in the framework of the things to be watched. Typical examples of devices consists RFID readers, sensors and actuators, implanted computers as well as mobile phones. The relationship between all these terms is schematically encapsulated in Fig. 1: An entity of interest is monitored by a device in the environment, or it can also have a device connected to or embedded in it. As described above both classes of devices can be seen as entities of interest when looking from a management perspective, hence the subclass relationship. The device hosts one or more resources which are accessed through services [4].

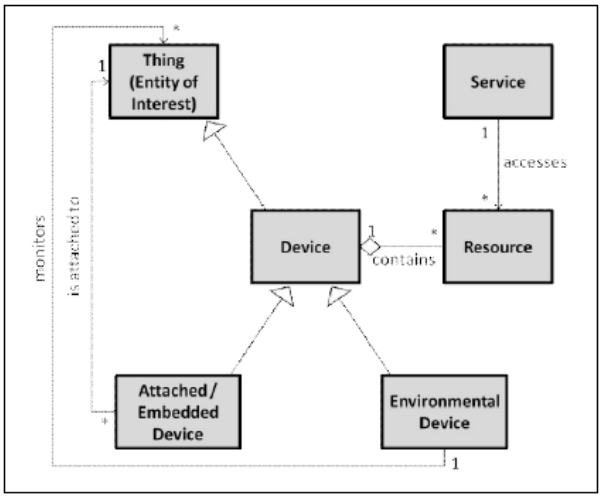

Figure 1: Relationship between things, devices, resources and services

1.3 ARCHITECTURE OF IOT:

A layered architecture of IOT is described as normally, IOT is partition into three layers: Perception layer, Network layer, and Application layer. All of these three layers have huge scale of information with different enabling technologies and features as shown in figure 2.

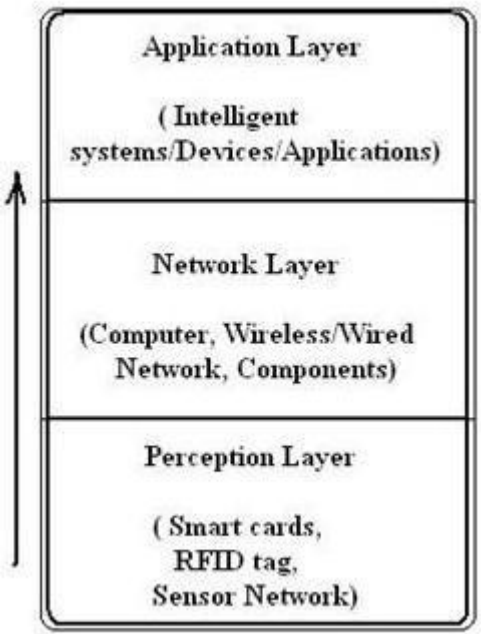

Fig 2: Architecture of IOT

1.3.1 Perception layer: The main working of IOT i.e. collection of information is done at the perception layer with the help of various devices like smart card, RFID tag, reader and sensor networks, etc. It has properties of comprehensive sensing through the RFID system to get object's information anytime and anywhere.

1.3.2 Network layer: The data collected by sensors used to be sent to the internet via network layer with the help of computers, wireless/ wired network and other elements. Hence network layer is mainly responsible for the transmission of information with the property of reliable delivery hence this layer also includes the functionality of transport layer.

1.3.3 Application layer: Examine the received information and making the control decisions to achieve its feature of intelligent computing by connection, identification and control between objects and devices [5].

1.4 Node level energy efficiency protocol for Internet of Things:

Node Level Energy Efficiency Algorithm considers residual energy of its one hop neighbor nodes and the mean value of residual energy of all nodes in the network [3]**.**

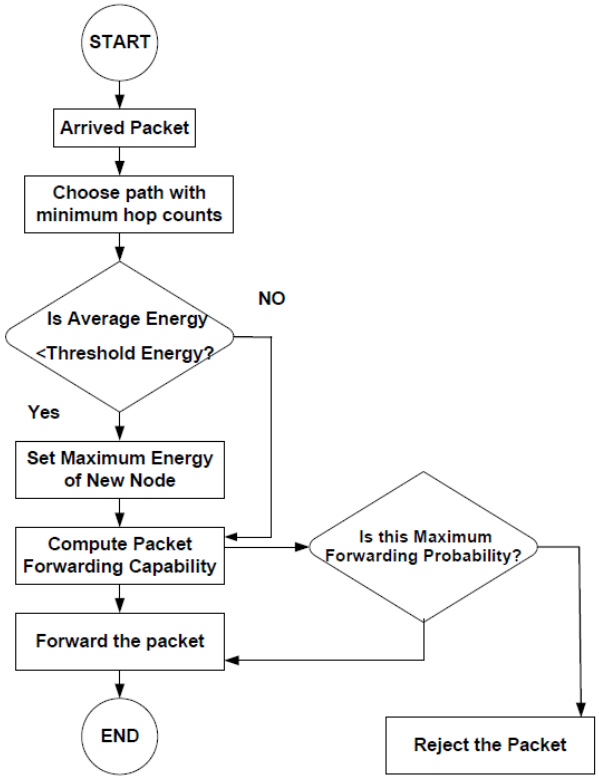

Figure 3: Working process of Node level energy efficiency algorithm [3].

1.5 SCOPE AND BENEFITS OF IOT:

IOT has given a concept of Machine to-Machine (M2M) transmission. IOT is going to have great effect on home automation and building automation system where every convenience will be taken care of by the interlinked appliances on IOT. IOT is proved to be an emerging technological innovation. In the current theme, it is now possible that an helmet of a two wheeler can interact with a car for avoiding collision. Connected toothbrush can now analyze and make one's experience pleasurable .A three dimensional senor of the electric brush can linked with Smartphone apps and deliver real time feedback to the person [6].

1.6 SECURITY COUNTERMEASURES:

Counter calculates for the safety issues of IOT are access control, data encryption and cloud computing.

1.6.1 Cloud Computing:

Cloud is a name for huge data storage capacity, high performance with affordable low cost. In the necessary working of IOT i.e. huge number of sensor nodes that collect and analyze huge amount of data, storing and processing of data where cloud computing can be used very effectively. Another use of cloud computing is providing third party security. IOT security can be enhanced using clouds security at minimum cost, as cloud provides the feature of "pay for how much you use". While using cloud computing it needs to make sure that the Scale of IOT is large for example in areas such as, earthquake monitor, smart grid, industrial applications etc.

1.6.2 Data Encryption:

Encryption technique is used to prevent the information from tampering and to maintain confidentiality as well as integrity of the information. When data is intercepted by an attacker, encryption prevents that data from being deciphered. There are two ways of Encryption: 1) Hop by Hop Encryption provides cipher text conversion on each node to make it more secure for network layer. 2) End to End Encryption in which encryption-decryption performed at sender-receiver end only. According to the business needs, one can choose different encryption methods. Using more secure key exchange and key management schemes one can prevent attacks on IOT such as eavesdropping, fabrication, record and replay etc

1.6.3 Access Control:

Access control is another mechanism which gives secure environment of IOT by limiting the access control for machines, objects or people which are illegal to access the resources. Certification and access control technology are correlated with each other. For correct access control, IOT should ensure the correct identification by certification technique. Access control can be implemented on the area such as: Encrypt password, confidential directories or files, configuration and update rights etc. Designing a secure key agreement scheme to restrict the key information to be attacked on can be helpful for it.

.

1.6.4 Certification:

Certification is a secure way of confirming the true identity of both the parties which communicate with each other. Hence by using Public Key Infrastructure (PKI), it is possible to achieve the strong authentication by two way public key certification for preventing authenticity and confidentiality of the IOT system. Notarization is another solution for security purpose. Notarization is a trusted third party i.e. a certificate authority that facilitates interactions between the users to assure the properties of data exchange [5].

LITERATURE SURVEY

Lotte Steenbrink et al. (2014) The creation and adaption of standardized benchmarks for routing in the Internet of Things may advance the comparison of candidate protocols for the IOT. Furthermore, the topology and attributes of the IOT complicate experiment and simulation setup: while the former is expensive to set up and maintain, the latter quickly fails to represent the network properties and inWuences correctly. there already are many existing approaches which may prove to be suitable for the IOT. Their direct comparison in both simulation and realistic testbed scenarios could provide further insight into their suitability for distinct IOT

scenarios and reveal optimization potential.

Marie-Aurélie Nef et al.(2012) With the emergence of the Internet of Things (IOT),it is necessary to define service models, which can classify IOT applications and determine the Quality of Service (QoS) factors necessary to satisfy the requirements of those facilities. On the other hand, as Wireless Sensor Networks (WSN) Constitute a main component of the IOT, they become a key factor regarding QoS provision. In this perspective, we focus our analysis on the possible WSNs integration approaches in the IOT while presenting QoS and which best practices to adopt. Furthermore, regarding QoS requirements, we also define service models for the IOT and reveal their feasibility through a categorization of IOT applications.

Vellanki M et al.(2016) Internet of things (IOT) contains connecting all the devices and networks which work based on our surroundings, and can mould our lives safer, healthier and faster. We are going to intended and explain energy issues that emerge while using Internet of Things. Universal detecting authorized by Wireless Sensor Network (WSN) innovations cuts crosswise over countless territories of current living. This offers the potential to quantify, derive and comprehend ecological pointers, from sensitive preservation and characteristic assets to urban conditions. The expansion of these gadgets in a communicating–activating system that makes the Internet of Things (IOT) intriguing, wherein sensors and actuators mix constantly with nature around us, and the data is shared crosswise over phases to build up a typical working picture. Infused by the late adjustment of an assortment of empowering remote promotions, for example, RFID labels and inserted sensor and actuator hubs, the IOT has progressed out of its early phases and is the following progressive innovation in changing the Internet into a entirely coordinated Future Internet. All these advancements in internet of things involves high energy consumption.

Stephan Haller (2010) The Internet of Things is a hyped term and many definitions for it exist. Worse still, it comes with a lot of concerned terminology that is not used uniformly either, hindering scientific discourse. This paper tries to bring clarity by defining the most important terms like things, devices, entities of interest, resources, addressing, identity and, more especially, the relationships between them.

Mayuri A. Bhabad et al. (2015) Internet of things (IOT) is broadly distributed network of things in which all the information is sent to the internet with the help of sensing equipment and Radio Frequency Identification (RFID) tagging system. As IOT does not need any human to machine interaction, it appears to be one of the largest waves of revolution as per the research going on, hence security is needed. But the fast development of IOT has evolved with the challenges in terms of security of things. This paper is mainly stressing on the concept of IOT, architecture and security issues with suggested countermeasure and suggested further areas of research needed.

TABLE 1

ROUTING PROTOCOLS FOR IOT		
TYPE	**APPROACH**	**NAMES OF PROTOCOLS**
TABLE DRIVEN PROTOCOL	In Table-driven node maintains consistent route information in tables from neighbour nodes time to time. This will lead to quick and easy route establishment for the source node to forward packets to the destination.	1. DSDV: Destination-Sequenced Distance Vector. 2.FSR: Fisheye State Routing
ON-DEMAND DRIVEN	In on-demand driven the source node first sends a route request packet which is received by neighbour nodes and it is forwarded to other neighbour nodes to increase the vicinity until a route could be established to the destination node. Once the route is discovered a response packet is sent through the same path used by route request packet	1. DSR: Dynamic Source Routing. 2. AODV: Ad-Hoc On-Demand Distance Vector. 3.AOMDV: Ad-hoc On-demand Multipath Distance Vector 4.EEPR:energy-efficient probabilistic routing 5.NLEE: Node Level Energy Efficiency

TABLE 2: **IOT layers and its specifications**

Layer	**Working**	**Security Issue**	**Security Parameters**	**Components**
Perception layer	Collection of information	Terminal Security issue Sensor network security issue	Authentication Confidentiality	Smart Card, RFID tag, Sensors
Network layer	Transmission Of information	Information transmission security	Integrity Availability Confidentiality	Wireless or wired network, computer, components
Application layer	Analysis Of information Control decision making	Information processing safety of IOT	Privacy	Intelligent devices

A. References

1. Lotte Steenbrink, "Routing in the Internet of Things", July 25, 2014.

2.Marie-Aurélie Nef, Leonidas Perlepes, Sophia Karagiorgou, George I. Stamoulis, Panayotis K. Kikiras, "Enabling QoS in the Internet of Things",2012.

3.Vellanki M, Kandukuri SPR and Razaque, "A Node Level Energy Efficiency Protocol for Internet of Things",Volume 3 , Issue 1,2016

4. Stephan Haller, "The Things in the Internet of Things",2010.

5. Mayuri A. Bhabad, Sudhir T. Bagade, "Internet of Things: Architecture, Security Issues and Countermeasures", Volume 125 – No.14, September 2015.

6. Jyotiranjan Hota**,** Pritish Kumar Sinha**, "**Scope and challenges of Internet of Things :An Emerging Technological Innovation", February 2015.

7. Yicong TIAN, Rui HOU, "An Improved AOMDV Routing Protocol for Internet of Things",2010.

8. John A. Stankovic, "Research Directions for the Internet of Things", 2014.

Conclusion

IOT is an forthcoming technology of transformation but still at its early stage of research and development. IOT cannot be used widely if it is not safe. Even in recent years a thorough research on IOT is going on still some issues are there like Application oriented study is needed for different industrial application in which IOT can be used in order to initiate a new technological revolution, New security challenges and application of lightweight cryptographic protocol need to be improved. IOT becomes a utility with increased sophistication in sensing, actuation, communications, control, and in generating knowledge from vast amounts of data. This will result in qualitatively different lifestyles from today. New research problems arise due to the large scale of devices, the connection of the physical and cyber worlds, the openness of the systems of systems, and pursuing problems of privacy and security. The main aim of further research in the field of IOT is to improve the energy efficiency by considering expected transmission count, residual energy of nodes, and hop count of nodal paths as routing metrics and NLEE algorithm guarantees an improved efficient usage of nodal energies. It also provides the shortest path in the network while routing setup delay is increased. NLEE algorithm performs better than AOMDV-IOT and EEPR in terms of energy efficiency.

First Author Anamika Sharma M.Tech student in electronics and communication department of Seth Jai Parkash Mukand Lal Institute of Engineering & Technology.

Second Author Er. Sonia Saini Lecturer in electronics and communication of Seth Jai Parkash Mukand Lal Institute of Engineering & Technology.