A survey on Internet of Things - DOI 10.5752/P.2316-9451.2013v1n2p78

Article *in* Abakós · May 2013

DOI: 10.5752/P.2316-9451.2013v1n2p78

2 authors, including:

Dario Vieira
EFREI, France
54 PUBLICATIONS **255** CITATIONS

SEE PROFILE

PUC Minas
A B A K Ó S
Instituto de Ciências Exatas e Informática

A survey on Internet of Things*

Um estudo sobre Internet das Coisas

Shashank Agrawal[1,2]
Dario Vieira[1]

Abstract

This paper presents Internet of Things in a wider context. Main enabling factor of this concept is the integration of various technologies. In this paper, we describe the key technologies involved in the implementation of Internet of Things and the major application domain where the Internet of Things will play a vital role. Later we will discuss about the open issues which are to be addressed before the worldwide acceptance of these technologies. There are lots of open issues to address. Here we address the most relevant among them in detail.

Keywords: Internet. Internet of Things.

*Invited communication.

[1]EFREI – Ecole d'ingénieur Informatique & technologies du numérique, FRANCE
[2]VIT University, INDIA

Resumo

Este artigo apresenta a Internet das Coisas em um contexto mais amplo. O principal fator de crescimento desse conceito é a integração de várias tecnologias. Neste artigo são descritos as tecnologias-chave envolvidas na implementação da Internet das Coisas e o principal domínio de aplicação onde a Internet das Coisas vai desempenhar um papel vital. Em seguida são discutidas as questões em aberto que devem ser tratadas antes da aceitação mundial dessas tecnologias. Existem ainda muitas questões para serem resolvidas sobre esse tema. Aqui serão abordadas uma amostra daquelas mais relevantes em detalhes.

Palavras-chave: Internet. Internet das Coisas.

1 INTRODUCTION

The term Internet of Things (IoT) has been around for quite a few years. In this scenario, it is gaining ground with the evolution of advanced wireless technology. The basic idea of this concept is the presence of a variety of objects – such as RFID, NFC, sensors, actuators, mobile phones, etc. which, through unique addressing schemes, are able to interact with each other (GIUSTO; A.LERA; L.ATZORI, 2010).

When IoT idea came into existence, Radio-frequency Identification (RFID) seemed to be necessary for Internet of Things (WIKIPEDIA, 2013), but in scenario there are lots of new technologies available in the market. Technologies like RFID, Near Field Communication (NFC), Machine-to-Machine Communication (M2M) and Vehicular-to-Vehicular communication (V2V) are there in the markets which are used to implement the modern concept of IoT as explained in Section 2.

Upon widespread adoption of different technologies of IoT, the life of the potential user can become very comfortable and safe as explained in Section 3. From the sense of personal use, the most obvious effect of IoT is visible in domestic sphere. To name a few, assisted living, smart homes, smart cars, etc. are potential areas where IoT helps in increasing the living standard of an individual. From business user point of view, the effect of this smart technology is noticeable in manufacturing and service industry like more production, superior quality and better services.

The worldwide adaption of these technologies does not appear so handy; lots of issues are there to be solved before the worldwide acceptance of IoT as described in Section 4. The main problem IoT is facing in scenario is of security, as there are enough potential hackers who are always eager to attack. Other problem includes the standardization problem, addressing problem, scalability problem, etc. New research is needed to resolve these issues.

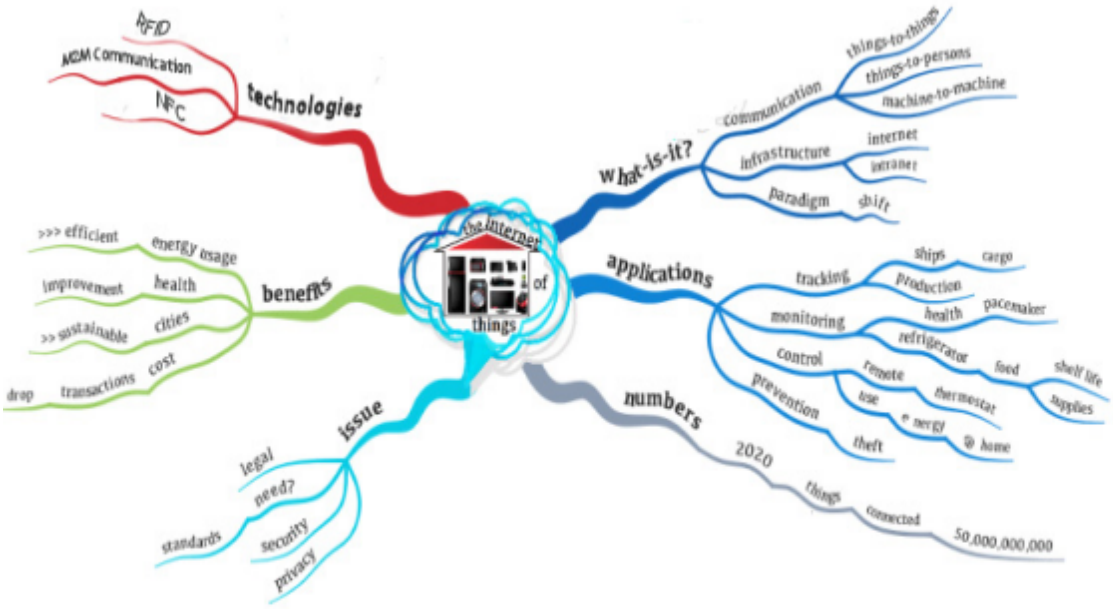
The main objective of this paper is to provide the reader the possibility of understanding what is IoT, what are the technologies involving in IoT, the application of IoT and the open issues which are to be addressed in the near future as shown in Figure 1.

2 TECHNOLOGIES INVOLVED

There are several technologies that can be used to implement the concept of Internet of Things. In this paper, we discussed the following technologies:

- Radio Frequency Identification (RFID)
- Near Field Communication (NFC)
- Machine-to-Machine Communication (M2M)
- Vehicle-to-Vehicle Communication (V2V)

Figure 1 – Internet of Things.



Fonte:http://www.biggerplate.com/mindmaps/1K7h9YNQ/the-internet-of-things-50-billion-things-connected

2.1 Radio frequency identification (RFID)

RFID system is composed of one or more reader(s) and several RFID tags. Tags are characterized by a specific address and are applied to objects. Tags uses radio-frequency electromagnetic fields to transfer data attached to an object. The tags contained electronically stored information which can be read by the RFID reader when the object came in the proximity of the reader (WIKIPEDIA, 2013). RFID allows to monitor objects in real-time, without the need of being in line-of-sight.

From the physical point of view RFID tag or label is a tiny microchip combined with an antenna in a compact package. The tag's antenna picks up signals from an RFID reader and then returns the signal, usually with some additional information. Hitachi has developed a tag with dimensions 0.4*0.4*0.15 mm (ATZORI; IERA; MORABITO, 2010).

The RFID tags comes in three configurations, the first one is Passive Reader Active Tag (PRAT) in which the reader is passive and receives the signal from the battery operated active tags. The transmission range of the RFID tag and the reader is from 1-2000 feet depending upon the architecture. The second one is Active Reader Passive Tag (ARPT), which is most commonly used. This tag does not have onboard power supplies, so it harvests the energy required to send data from the query signal sent by the RFID reader. The last one is an Active Reader Active Tag (ARAT). In this both the reader and the tags are active, but tags are only awoken by the reader when it comes in the proximity of the reader. Transmission may appear

in various frequency bands spanning low frequencies (LF) at 124-135 KHz up to ultra-high frequencies (UHF) at 860-960 MHz (WIKIPEDIA, 2013).

An Electronic Product Code (EPC) is one common set of data stored in a tag. EPC's are coded on RFID tags because of which objects can be tracked and identified uniquely. The tag contains a 96-bit string of data. The first eight bits are a header which identifies the version of the protocol. The next 28 bits identify the organization that manages the data for this tag, the organization number is assigned by the EPCGlobal consortium (EPCGLOBAL, 2013). The next 24 bits are an object class, identifying the kind of product; the last 36 bits are a unique serial number for a particular tag. These last two fields are set by the organization that distributed the tag (WIKIPEDIA, 2013). Rather like a URL, the entire electronic product code number can be used as a key into a global database to exclusively identify a particular product (BURLINGTON, 2009).

The RFID tags are used in many applications like Monitoring the life cycle of a product, manage the inventory in the warehouse, tracking of goods, tracking of animals, airport baggage tracking logistics (HARRISON, 2009), mobile payment, etc. We can combine the RFID technology with the other technologies like sensing technology to open a new horizon for new applications.

2.2 Near field communication (NFC)

NFC is quite similar to RFID, or it can be looked as an integration of RFID reader into a mobile phone, which makes NFC customer-oriented as mobile phone is the most popular personal device worldwide (VILMOS; MEDAGLIA; MORONI, 2011). NFC can also be seen as a type of radio communication between NFC enabled mobile devices by touching them together or bring close in the proximity of the other phone.

From the technical point of view, NFC operates within the unlicensed Radio Frequency band of 13.56 MHz (MEDAGLIA, 2011); the typical operating range of NFC device is 20 cm. The operating range is directly depended on the size of the antenna in the device.

NFC is a short range, low power wireless link evolved from RFID that can transfer small amounts of data between two devices held in proximity. Unlike Bluetooth, no paring is required before the actual transfer of data (TECHRADAR, 2013). NFC enabled communication between the smart objects is safe as this cannot be done from a remote location, so one with his/her NFC enabled device should be present there for the application like payment.

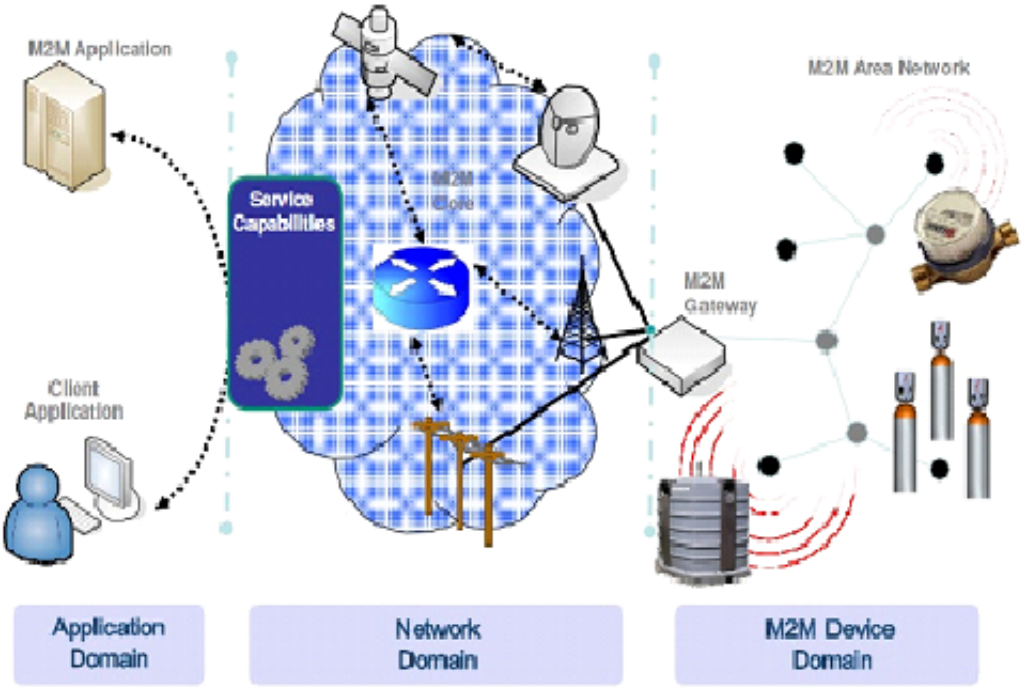
The NFC technology will significantly contribute to the future development of IoT. It will provide the necessary tool to be wirelessly connected to any smart objects. Mobile NFC also has the potential to transform the mobile headsets into different types of smart objects like when we need to pay the bills and then our mobile can be used as our credit card.

2.3 Machine-to-machine communication (M2M)

Machine-to-Machine (M2M) refers to the communications between computers, embedded processors, smart sensors, actuators and mobile devices (DYE, 2008). The use of M2M communication is increasing in the scenario at a fast pace. For instance, researchers predicted that, by 2014, there will be 1.5 billion wirelessly connected devices excluding mobile phones. There are four components of M2M which are sensing, heterogeneous access, information processing, application and services (CHEN; WAN; LI, 2012).

From the technical point of view, M2M is a five-part structure (ETSI, 2013) shown in Figure 2. The structure is defined as follows:

Figure 2 – M2M architecture.



Fonte: http://4gwirelessjobs.com/articles/article-detail.php?3-Key-enablers-for-WiMAX-LTE-Delivery&Arid=MTUy&Auid=MTIy

- M2M Device: A device capable of replying to request for data contained within that device.
- M2M Area Network (Device Domain): Provide connectivity between M2M Devices and M2M Gateways.
- M2M Gateway: Use M2M capabilities to ensure M2M Devices inter-working and interconnection to the communication network.
- M2M Communication Networks (Network Domain): Communications between the M2M Gateway(s) and M2M application.

- M2M Applications: Contains the middleware layer where data goes through various application services and is used by the specific business-processing engines.

M2M has several applications in various fields like healthcare, smart robots, cyber-transportation systems (CTS), manufacturing systems, smart home technologies, and smart grids (LAWTON, 2004). Example of M2M area network typically includes personal area network technologies, such as Ultra-wideband and Bluetooth or local networks.

2.4 Vehicle-to-vehicle (V2V) communication

V2V Communication is a new concept in which lots of research has to be done. In this, vehicles act as a node in a network and communicate with each other with the use of sensors connected in an ad-hoc network. The infrastructure of V2V network is a bit complicated as there is no fixed topology to be followed as vehicles are moving from one place to another all the time. Applications for vehicular networks can be divided into four broad categories, namely safety and collision avoidance, traffic infrastructure management, vehicle telematics, and entertainment services and Internet connectivity (BOOYSEN; ZEADALLY; ROOYEN, 2011).

Vehicles communicate with each other within a range of 1000 m. Two types of communication are possible; first one is vehicle-to-vehicle and the other one is the vehicle with the road-side infrastructure. Vehicular communication system is developed as a part of Intelligent Transport System (ITS). From a network architecture point of view, focus is initially placed on routing protocols; Physical layer (PHY), Medium Access Control (MAC) layer, and broadcasting(BOOYSEN; ZEADALLY; ROOYEN, 2011).

3 APPLICATION

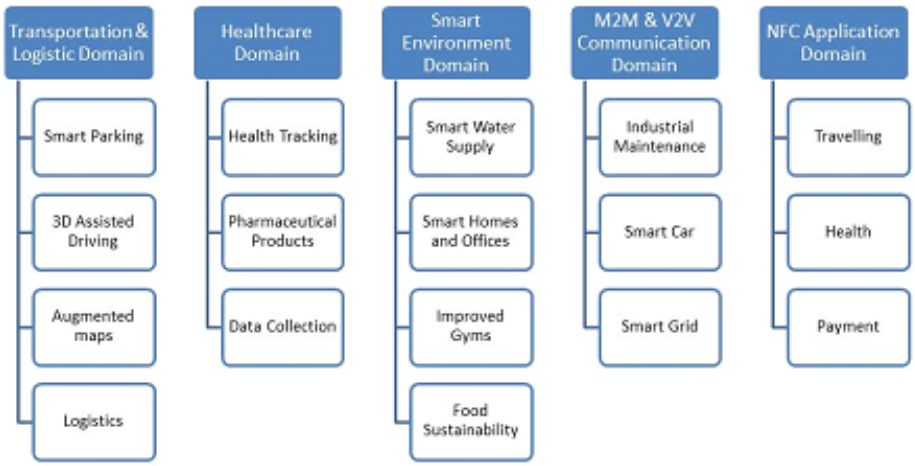
Ample of application is there where Internet of Things is playing a vital role. In the near future, there will be even more applications using Internet of Things. As the world is going through a technological revolution, more and more objects will use the technology of RFID, NFC, M2M communication and V2V communication for automation as shown in Figure 3.

3.1 Transportation and logistic domain

3.1.1 Smart parking

The new Smart Parking sensor's to be buried in parking spaces to detect the arrival and departure of vehicles. The Smart parking provides extensive parking management solutions which helps motorists save time and fuel (LIBELIUM, 2013). A significant contribution to

Figure 3 – Applications of IoT



congestion arises from motorists searching for accessible parking spaces. Providing accurate information about parking spaces helps traffic flow better, and this will also allow the deployment of application to book parking spaces directly from the vehicle. This will help to reduce CO2 emissions and to minimize traffic jams.

3.1.2 3D Assisted driving

Vehicles like cars, buses and trains along with the roads and rails equipped with sensors may provide valuable information to the driver to provide better navigation and safety. With the use of assisted driving, we will be able to find the right track with prior information about traffic jams and incidents. In an Enterprise context, information about the vehicle transporting goods together with information about the type and status of the goods can integrate to provide valuable information about the delivery time, delivery delays and faults.

3.1.3 Augmented maps

Tourist augmented maps with tags allow NFC-equipped phones to browse the information about the places and quickly connect it to the web services providing information about hotels, restaurants, monuments, theater and the local attractions. This can be done by hovering your mobile phone over the tag within its reading range so that the additional information about the marker can be displayed on the screen.

3.1.4 Logistics

Implementing the Internet of Things in Retail chain monitoring has many advantages: RFID and NFC can be used to monitor almost every link of supply chain, ranging from commodity details, raw material purchasing, production, transportation, storage, sale of product and after sales services. With the help of IoT, we will track the inventory in the warehouse so that stock can be refilled at the appropriate time for continuous sale and this will reduce the waiting time of customer which result in customer satisfaction, which further results in increased sales.

3.2 Healthcare domain

3.2.1 Health tracking

We can track health of a person with the help of combination of RFID and NFC technology together. With the use of sensors and the technology stated above we can track the person's body temperature, heart beat rate, blood pressure, etc. In case of emergency, the individual and their personal doctor will be notified with all the data collected by the sensors.

3.2.2 Pharmaceutical products

Safety of pharmaceutical product is of utmost importance to prevent the health of patients. Attaching smart labels to drugs, tracking them through the supply chain and monitoring their status with sensors has benefits like items require specific storing conditions so they can be monitored whether their requirements are fulfilled or not. We can also track the expiry of drugs with the use of sensors; this will prevent the transferring of expired drugs to the patient.

3.2.3 Data collection

Automatic data collection and transfer of that data to the doctor will help in reducing in the processing time, reducing the data collection errors, automated care and routine auditing. This will also forward all the previous health record related to the patient which helps in accuracy of the medication given by the doctor.

3.3 Smart environments domain

3.3.1 Smart water supply

Smart cities must monitor water supply to ensure that there is adequate access for resident and business need. Wireless Sensor Networks provide the technology for cities to monitor their water piping systems more accurately and discover their greatest water loss risks. Cities that are addressing water leakage problem with sensor technology are producing high savings from their investment. Tokyo, for example, has calculated they save $170 million each year by detecting water leakage problems early (LIBELIUM, 2013). The system can report pipe flow measurement data regularly, as well as send automatic alerts if water use is outside of an estimated normal range. This allows a smart city to determine the location of leaking pipes and prioritize repairs based on the amount of water loss that could be prevented.

3.3.2 Smart homes and offices

We are surrounded by various electronic gadgets around us such as microwave ovens, refrigerators, heaters, air conditioners, fan and lights. Actuators and sensors can be installed in these devices in order to utilize the energy sufficiently and also to add more comfort in life. These sensors can measure the outside temperature and even can determine the occupants inside the rooms and thereby control the amount of heating, cooling and flow of light etc. Doing all these can help us to minimize the cost and increase energy saving.

3.3.3 Improved gyms

The gymnasium experience can be enhanced by involving new technologies like a separate exercise profile which can be installed on machines and each person can be identified from his identification id alone and thereby, concerned profile will get activated.

3.3.4 Food sustainability

Food that we eat has to go through various stages before they arrive in the refrigerators. They are bound in a strict food cycle: production, harvesting, transportation and distribution. With the use of appropriate sensors, we can prevent the food from climatic damages by keeping a good eye on temperature, humidity, light, healt etc. Sensors can measure these variations precisely and notify the concerned person. Monitoring helps in prevention of possible plant

diseases or manages watering requirements based on soil humidity.

3.4 M2M and V2V communication domain

3.4.1 Industrial maintenance

The sensors fit in the machinery are used to monitor the temperature and vibration in industrial motors, and also warn when irregular operation is detected. Industrial maintenance is the term for the task of keeping the equipment running at peak efficiency in a factory. It includes scheduled cleaning, parts replacement and lubrication and repairs. The field of industrial maintenance does not involve just the repair of already existing malfunctions (LIBELIUM, 2013), but preventive maintenance typically is also a vital part of the field. Companies waste billions due to inefficient maintenance management. This will help Companies to save money and time.

3.4.2 Smart cars

Machine to machine (M2M) communications, and especially Smart Cars, could help to improve accident prevention. A pilot to operate remote control car in order to minimize car accident and reduce human error was developed by McGill University (SANTORELLI; MORAWSKI; LE-NGOC, 2011). These driverless cars will provide functioning more than just safety such as they can save valuable time, reduce stress of driving etc. Some studies carried out by the Institute of Electrical and Electronics Engineers (IEEE) reveal that, by 2040, driverless cars will account for up to 75 per cent of cars on the road worldwide (LIBELIUM, 2013).

3.4.3 Smart grid

Smart Grid is defined as an electrical grid which is designed to improve the efficiency of power transmission, and quality of service to the end user. In Smart Grid, all the devices in the network are connected with the sensors which regularly send the data related to power consumption to the central server. Central server determines the pattern of consumption and the amount of power consumption. This allows companies to increase their production to meet the transient power requirement (BOOYSEN et al., 2012).

3.5 NFC application domain

3.5.1 Travelling

NFC can enhance the travelling experience to a greater extent: it can help us to minimize the check in time during the stay in hotels. When the room is booked in a hotel, a secure digital key is sent to the traveler. One can use that digital ticket, with the NFC enabled locks, and directly enter into the room without wasting any time in check-in lounges.

3.5.2 Health

NFC can be useful in monitoring personal health. It can gather information about health and send the collective data to health monitoring center. These centers can, therefore, analyze health and provide the valuable report and information to the individual.

3.5.3 Payment

With the help of NFC technology, a user can leave his credit cards at home and can make a copy of credit cards on the mobile device. In case he needs to make any payment, he can electronically make the payment by using the clone of credit cards on the mobile phone, and NFC activated devices.

4 OPEN ISSUES

In scenario, the effect of IoT can be seen in all technical areas. It helps in smart communication between objects but several issues are there to be addressed before the worldwide implementation of IoT. In this section, we identify some important issues related to addressing, routing protocol, security and privacy, standardization issue and congestion and overload issue.

4.1 Addressing and networking issue

Each and every device connected in the network has a unique address by which it can be identified. As the IoT is gaining grounds in scenario, the demand for these unique address increases at a very fast rate. There are very limited number of address available in IPv4 addressing and will soon reach zero as it identifies each node through a 4-byte address. To handle

the ever increasing demand of unique address, one require IPv6 addressing scheme to fulfill the requirement. IPv6 addresses are expressed by means of 128 bits and, therefore, it is possible to define 1038 addresses, which should be enough to identify any object.

Another important issue is regarding networking i.e. which protocol is to be used to send the data from source to destination. In traditional internet, the protocol utilized at the transport layer for reliable communications is the Transmission Control Protocol (TCP) (CERF; DALAL; SUNSHINE, 1974). It is clear that TCP is insufficient for the IoT because we need to set-up a connection first in case of TCP, but most of communication in IoT is a very short communication. So, considerable time will be wasted in the connection setup. One more issue with TCP is congestion control, TCP is responsible for end-to-end congestion control, but in case of IoT the amount of data transfer is very small, so TCP congestion control is useless. As a consequence, TCP cannot be used efficiently for the end-to-end transmission control in the IoT. Till now, no solutions have been proposed and, therefore, research is required in this area.

4.2 Routing protocol issue in V2V communication

Routing is a very important aspect in the field of V2V communication as it is a type of distributed processing with a great number of nodes and a constrained and highly variable network topology. There are two basic ways by which one can route the data from source to destination. The first one is source routing: in this all the information like how to get from source to destination is collected on the source and then stored in the packets to be send, and the job of the intermediate node is to read this information and route the packet according to it towards the destination. Second one is hop-to-hop routing: in this routing technique, node has information only about the next node; the work of intermediate node is a bit complex as they know the destination address only, not the whole route to get towards the destination (KUMAR; KUMAR; KADIAN, 2011). This hop-to-hop is more efficient as in this we can choose the best next hop according to the topology.

The architecture of routing in V2V communication is the same as the architecture of routing in other connectionless networks. Routing is the backbone of the network. There are lots of protocols present there like Geographical Source Routing (JERBI et al., 2009) which is hop-to-hop routing. This routing is based on the topology information given by global positioning system; frequently changes in topology causes route oscillation and path instability. In On-Demand Routing protocol (DAS; PERKINS; ROYER, 2000) node attempts to discover a route to the destination when it has a packet to send. In this protocol, flooding method is used to discover the route which creates the congestion in the network as it sends the packet to all the nodes for route discovery.

There are various other routing technique like Greedy Perimeter Stateless Routing (GPSR) (KARP; KUNG, 2000), Dynamic MANET on Demand (DYMO) (CHAKERES; PERKINS, 2006), etc., but each one has its shortcoming. The key challenge is to design a protocol which will im-

prove reliability of protocols and reduce delivery delay time and number of packet transmission. To make VANET a reality, lots of research is needed as each one of the existing protocol has some drawbacks as explained above. The driver behavior should also be concerned in designing the routing protocols.

4.3 Privacy and security issue

The IoT is extremely vulnerable to attacks as its components spend most of the time unattended, so it became very easy to attack them. Apart from this, one more thing is that, most of the communication is wireless which makes snooping very easy. This is probably one of the biggest concerns for consumers when it comes to IoT. For instance, in NFC enabled devices, the device not only works as a credit card but also the key to your house, it will also contain the personal information of the owner. If a smartphone is stolen, the thief move's the phone over a card reader at a store to make a purchase (NFC, 2013). To avoid this, smartphone owners must protect their phone with strict password protection, so hacker is not able to come out with the correct password.

More specifically, the major problems related to security concern authentication and data integrity. Authentication is required before making a connection between the two devices to prevent data theft. The infrastructure is required for the authentication as we generally have to exchange some public and private keys through the node. Solutions like cryptography and key management have been proposed in the recent past (e.g., (KAVITHA; SRIDHARAN, 2010), (ESCHENAUER; GLIGOR, 2002a)), but none of them will prevent from the man-in-the-middle attack and proxy attack problem.

Data integrity prevents any modification in the data by middle man; it ensures that the data received at the receiver node is in the unaltered form as send by the sender. Solutions have been proposed like Keyed-Hash Message Authentication Code (HMAC) scheme (ESCHENAUER; GLIGOR, 2002b), to protect the data against the attack but still new research is required in the field of security and privacy.

4.4 Standardization issue

Standards are required to allow global interoperability. As the term Internet of Things is gaining popularity, the more and more number of devices is activated daily. To ensure the proper functionality of these devices, there should be certain standards we have to follow to provide proper service to the client. As the platform on which these IoT devices works is not the same in all cases, so it became more necessary to define certain standards to make those devices compatible with the others. EPCglobal (Electronic Product Code) (EPCGLOBAL, 2013), as well as ISO (International Organization for Standardization), offers a family of standards,

and they are gaining popularity in the wireless sensor area.

4.5 Congestion and overload issue

Congestion is occurred due to simultaneous messages from several devices that can lead to peak load situation and may have a tremendous impact on the network (3GPP, 2010). This affects the performance of the network, and may lead to failure of the network if the network is overloaded. This situation is mainly seen in M2M and V2V communication, and it can be solved with the help of emerging technologies like LTE-advanced or existing technologies like LTE high bandwidth networks (TALEB; KUNZ, 2012). The congestion situation also occurred because of malfunction of server or application; so to avoid this one has to design an application in such a way that can handle maximum load with minimum failure.

Overload issue can be solved with the help of time controlled features, i.e., allow connection to the network only at a certain time periods, defined by the network operator. Only in this time period, the devices are allowed to connect, devices are not able to connect to the network in the forbidden time period. The other solution is by rejecting the connection request by specific network nodes, particularly from those that are causing congestion and shall have no impact on the traffic (TALEB; KUNZ, 2012). This will help in managing the overall load of the network by rejecting the nodes which are creating the congestion.

5 CONCLUSION

The internet has drastically changed the way we lived, as in scenario all the interaction is done over the internet. The IoT has the potential to add a new dimension to this process by enabling communication between smart objects. IoT should be considered as a part of future internet as everything is going to be connected in a network so that objects can interact with each other, but still there are lots of issues which are to be solved to make this a reality. Lot of research is required in this field, once implemented successfully, the quality of life is improved because of the reduction of the effort made by humans on unimportant things.

In this paper, we presented the technologies and its specification that can be used to make Internet of Things a reality. After that, we state some good examples where Internet of Things is of great use, and at last we discuss some open issues which are still to be solved before the wide acceptance of this technology.

REFERENCES

3GPP. **Service Requirements for Machine-Type Communications**. 2010.

ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. The internet of things: a survey. **Computer Networks**, v. 54, n. 15, p. 2787 – 2805, 2010. ISSN 1389-1286. DOI.10.1016/J.COMNET.2010.05.010.

BOOYSEN, M.J.; ZEADALLY, S.; ROOYEN, G.-J Van. Survey of media access control protocols for vehicular ad hoc networks. **IET Communications**, v. 5, n. 11, p. 1619 – 1631, jul. 2011. DOI: 10.1049/IET-COM.2011.0085.

BOOYSEN, M. J. et al. Machine-to-machine communications in vehicular networks. **KSII Transactions on internet and information systems**, v. 6, n. 2, p. 529–546, 2012. DOI.10.3837/TISS.2012.02.005.

BURLINGTON, John R. Vacca. **Computer and information security handbook**. Burlington, Massachusetts, USA: Morgan Kaufmann, 2009. 208 p.

CERF, V.; DALAL; SUNSHINE, C. Specification of internet transmission control program. **IETF RFC 675**, Dec. 1974.

CHAKERES, I; PERKINS, C. **Dynamic MANET On-Demand (DYMO) Routing**. Mobile Ad hoc Networks Working Group, 2006.

CHEN, Min; WAN, Jiafu; LI, Fang. Machine-to-machine communications: Architecture, standards and applications. **KSII Transactions on Internet & Information Systems**, v. 6, n. 2, p. 480 – 497, 2012.

DAS, S.R.; PERKINS, C.E.; ROYER, E.M. Performance comparison of two on-demand routing protocols for ad hoc networks. In: ANNUAL JOINT CONFERENCE OF THE IEEE COMPUTER AND COMMUNICATIONS SOCIETIES, 19, 2000. **Proceedings of the INFOCOM, IEEE**. Washington, DC, USA, 2000. v. 1, p. 3–12. ISSN 0743-166X. DOI.10.1109/INFCOM.2000.832168.

DYE, S. **Machine-to-Machine Communications**. 2008. Retrieved March 28, 2008, from <http://www.mobilein.com/M2M.htm>.

EPCGLOBAL. **The language of business**. 2013. Retrieved May 30, 2013, from <http://www.gs1.org/epcglobal>.

ESCHENAUER, Laurent; GLIGOR, Virgil D. A key-management scheme for distributed sensor networks. In: ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, 9, 2002, Washington, DC, USA. **Proceedings of SIGGRAPH 87**. New York, NY, USA, 2002.

ESCHENAUER, Laurent; GLIGOR, Virgil D. HMAC: Keyed-hashing for message authentication. In: ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, 9, 2002, Washington, DC, USA. **Proceedings...** New York, NY, USA: Indeks Verlag, 2002. p. 41–47. DOI.10.1145/586110.586117.

ETSI. **European Telecommunications Standards Institute**. 2013. Retrieved May 14, 2013, from <http://www.etsi.org>.

GIUSTO, D.; A.LERA; L.ATZORI, G. Morabito. **Análise de sistemas e gerência de operações**. Berlin Heidelberg: Stringer, 2010. 129 p. ISBN 978-3-642-11710-7.

HARRISON, Peter. EU **considers overhauling rules for lost air luggage**. Reuters, 2009. Retrieved May 30, 2013, from <http://www.reuters.com/article/2009/07/28/eu-aviation-baggage-idUSLS63631320090728>.

JERBI, M. et al. Towards efficient geographic routing in urban vehicular networks. **Vehicular Technology, IEEE Transactions on**, v. 58, n. 9, p. 5048–5059, 2009. ISSN 0018-9545. DOI.10.1109/TVT.2009.2024341.

KARP, Brad; KUNG, H. T. GPSR: greedy perimeter stateless routing for wireless networks. In: ANNUAL INTERNATIONAL CONFERENCE ON MOBILE COMPUTING AND NETWORKING, 6, 2000, Boston, Massachusetts, USA. **Proceedings of the MobiCom '00**. New York, NY, USA: ACM, 2000. p. 243–254. ISBN 1-58113-197-6.

KAVITHA, T.; SRIDHARAN, D. Security vulnerabilities in wireless sensor networks: A survey. **Journal of Information Assurance and Security**, v. 5, p. 031–044, 2010.

KUMAR, Yugal; KUMAR, Pradeep; KADIAN, Akash. A survey on routing mechanism and techniques in vehicle to vehicle communication (VANET). **International Journal of Computer Science & Engineering Survey (IJCSES)**, AIRCC, v. 2, feb. 2011.

LAWTON, G. Machine-to-machine technology gears up for growth. **Computer**, v. 37, n. 9, p. 12 – 15, sep 2004.

LIBELIUM. **Libelium Comunicaciones Distribuidas**. 2013. Retrieved May 14, 2013 from <http://www.libelium.com/>.

MEDAGLIA, Carlo Maria et al. **Services, Use Cases and Future Challenges for Near Field Communication**. In: THE STOLPAN PROJECT, DEPLOYING RFID - CHALLENGES, SOLUTIONS, AND OPEN ISSUES, DR. CRISTINA TURCU (ED.). 2011. Retrieved May 30, 2013, from <http://www.intechopen.com/books/deploying-rfid-challenges-solutions-and-open-issues/services-use-cases-and-future-challenges-for-near-field-communication-the-stolpan-project>.

NFC. **Near Field Communication, Security Concerns with NFC Technology**. 2013. Retrieved May 14, 2013, from <http://www.nearfieldcommunication.org/nfc-security.html>.

SANTORELLI, Julian; MORAWSKI, Robert; LE-NGOC, Tho. Remote control sensor car for vehicle to vehicle communication testing. **Department of Electrical & Computer Engineering, Broadband Communications Research Lab, McGill University**, 2011. Retrieved May 14, 2013, <from http://www.mcgill.ca/files/engineering/SURE2011_ECE_SantorelliJulian.pdf>.

TALEB, T.; KUNZ, A. Machine type communications in 3gpp networks: potential, challenges, and solutions. **Communications Magazine, IEEE**, v. 50, n. 3, p. 178–184, 2012. ISSN 0163-6804. DOI.10.1109/MCOM.2012.6163599.

TECHRADAR. **Technology tested**. 2013. Retrieved May 30, 2013, from <http://www.techradar.com>.

VILMOS, A.; MEDAGLIA, C. M; MORONI, A. **NFC Technology and its application Scenarios in a future of IOT**. STOLPAN Project, 2011.

WIKIPEDIA. **The free encyclopedia**. 2013. Retrieved May 13, 2013, from <http://www.wikipedia.com>.