VOL.3 NO.2September 2014 - ISSN 2233 – 1859

Operations Research Society in Bosnia and Herzegovina

Southeast Europe Journal of Soft Computing

Available online: www.scjournal.com.ba

IUS Soft Computing Research Group

Internet of Things: Current Technological Review and New Low Power Wireless Sensor Network Protocol Proposal

Indira Muhić and Migdat Hodzić

Address: International University of Sarajevo, Faculty of Engineering and Natural Sciences
Hrasnicka Cesta 15 Ilidža, 71210 Sarajevo, Bosnia and Herzegovina

Article Info

Article history:
Received Sep.2014
Received in revised form 2014

Keywords:
Interent of Things
"Intelligent Life"
Smart Devices and Sensors
Wireless Network Protocol

Abstract

This paper addresses Internet of Things (IoT) with state-of-art approach. The purpose is to give insight into concept of "smart living", a concept that meets requirements of today's modern society. Implementation of this new technology requires new hardware and software installed and run on devices ("things") connected to the Internet anytime and anywhere. In order to make possible this new technology for wide use, few technological, standards and legal issues need to be solved. In a view of this a new low power wireless sensor network protocol is proposed in the IoT spirit.

1. INTRODUCTION

The Internet of Things (IoT) refers to a broad technological vision enabling completely new concept of living called "intelligent life". Smart devices, smart phones, smart cars, smart homes, smart cities, smart transport, smart energy, smart industry, smart world are synonyms that describe new paradigm in the world of Internet. Internet of Things enables affluence of new opportunities different from the traditional one. New era in modern communication and internet will be outside of the traditional one. The IoT concept, hence, aims at making the Internet even more immersive including wide areas of possible applications.

The IoT is a system of technologies which can monitor the status of physical objects, capture meaningful data, and communicate that data over a (often wireless) network to a software application for analysis on a dedicated computer or to the cloud. Objects can be electronic devices such as a utility meter, organisms or a natural part of the environment such as an area of ground to be measured for moisture or chemical content. A smart device is associated with each object which provides the connectivity and a unique digital identity for identifying, tracking and communicating with the object. A sensor within or attached to the device is connected to the Internet by a local area connection (such as RFID, NFC or BTLE) and can also have wide area connectivity.
Typically, each data transmission from a device is small in size but the number of transmissions can be frequent. Each sensor will monitor a specific condition or set of conditions such as vibration, motion, temperature, pressure or utility quality. More applications have become feasible because the cost and size of such devices continue to decrease and their sophistication for measuring conditions keeps increasing. Technological giant Cisco predicts that 25 billion devices will be connected in the IoT by 2015, and 50 billion by 2020.

The IoT is a new technological ground that is not still standardized and therefore there is still no stable definition for it. The widely used definition is one from ITU and IERC as a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes and virtual personalities, use intelligent interfaces and are seamlessly integrated into the information network [1]. Simply stated, Internet of Things can be loosely defined as: "From anytime, anyplace connectivity for anyone, we will now have connectivity for anything" [2].

For the first time the Internet of Things concept was mentioned in 1999 by Kevin Ashton who was cofounder and executive director of the Auto-ID Center.

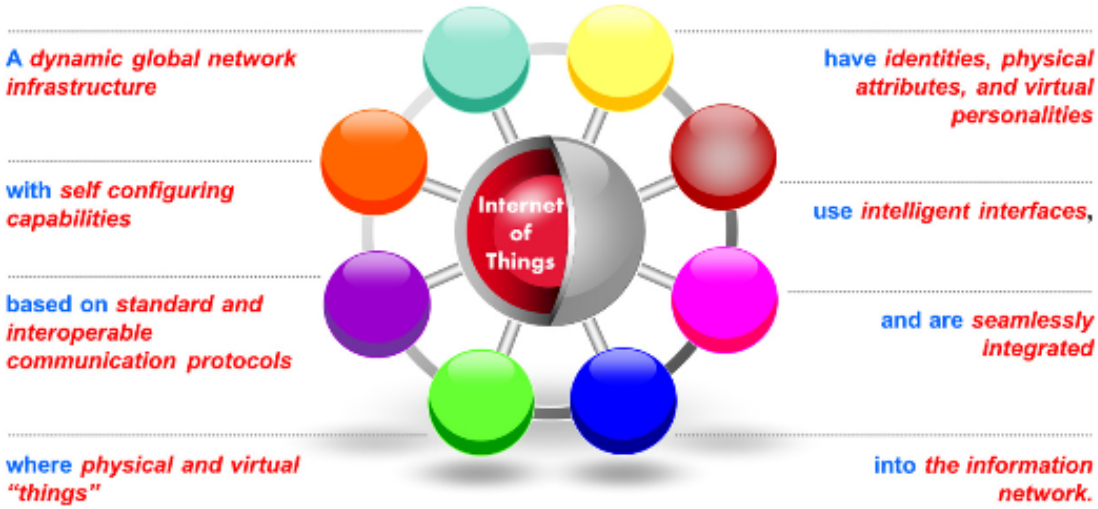

Figure 1.Definition of IoT [1]

Auto-ID Center represents collaboration between industry and private sector in order to work on new technology for tracking goods globally. The center closed door in 2003, but Auto-ID Labs continued working on the project. Now Auto-ID Labs are leading academic research network on Internet of Things. Auto-ID Labs are formed of seven research labs positioned on four continents, holding over 60 researchers and 15 professionals in leading positions.

Historical development of this idea started in 1999 as mentioned. Two years later in 2001 MIT Auto-ID Labs presented their vision of Internet of Things [3]. During the 2005 International Telecommunication Union (ITU) for the first time mentioned Internet of Things in a series of reports. In 2008 in Zurich the first conference was held on the Internet of Things. China has announced their interest in building smart cities, proposing Wuxi city representative of new idea called "Sensing China", during 2009. In June 2013 Kantara initiative was founded [4]. This group is formed in order to solve open questions and issues like discussion about ownership and identity relationships, object identifier, namespace, authentication, authorization, governance of data and privacy as specific open questions. Also in 2014,a state of the art report was published by Auto-Id Laboratory [5].

Even two years ago growth of Internet of Things was still considered with a skepticism. But several recent and key announcements(Net Labs, Google, Samsung Gear, developing and embedding of Smart Home feature into Apple's iOS), have made Internet of Things big business opportunity [1]. In addition, Cisco has conducted market research showing that Internet of Things has potential financial value of $14 trillion. All of that made Internet of Things even more attractive in today's research centers as well as industry.

2. ARCHITECTURE

In new era sensor and network technologies will develop to meet new IoT challenge. Enormous data need to be stored and transferred in real time environment. What will be the platform or platforms that support vision of Internet of Things?

Cisco market prediction is that by 2020, there will be over 50 billion permanently connected "things", with over 200 billion with intermittent connections enabled. Solutions that exist now are not capable of supporting this number of users, so research groups are still trying to design architecture that will meet these challenges.

IoT until now suggested two types of architecture, three-tier and five-tier. In three-tier architecture authors propose simplified concept consisting of three layers. First layer is context aware, where sensors embedded in different technologies are collecting information and where different communication protocols are developed. Next layer is called network tier which connects different networks in order to transfer information collected by lower layer. Next layer is application layer which originally consists of three layers. This layer supports monitoring QoS, with different management systems depending on the application. Since three-tier architecture doesn't specify enough details as far as roles of each layer, five layers architecture is also proposed. This architecture is more specific, briefly describing functionalities of each layer. The first layer is perception layer

which collects information about environment conditions like temperature, location of the sensor etc. On second transport layer all information collected on lower layer are transferred to the upper layer in order to process information. Processing layer than processes information in a way of storing and analyzing. The fourth layer is called application layer. Here various types of application are described that will be used in IoT. At the top of architecture is business layer which purpose is management of services, privacy and choice of type of applications that will be used [6].

Other authors hold the view of Service Oriented Architecture (SOA) [7]. Here a Cloud-Assisted remote sensing approach is proposed with four layer architecture consisting of Fog Layer, Stratus Layer, Alto Cumulus Layer and Cirrus Layer. Fog Layer consists of "things" that sense and collect environment data. This layer serves for unique identification through IPv6, to connect "things" and for collection of data at one central point. Stratus Layer is mid layer and consists of clouds managing migration of different clouds, ensuring functionalities for transferring data and for controlling agreed level of service with customers. Alto Cumulus Layer is intermediate layer between stratus and cirrus layer.
On this layer question related to pricing, policy and regulations are negotiated and agreed upon. At the top of architecture is Cirrus Layer with functions that serve clients. This layer can actually performs functions like customers entry point to the system allowing customers to set their own requirements regarding sensing, service models and providing online applications [8].

Globally, all mentioned architectures meet basic IoT concept, which is so far best described in architecture proposed by ITU-T and represented in figure 2.

Lower layer is device layer that contains devices, named sensors, for collecting information and gateways for sending collected information to upper layer. Network layer is responsible for choosing appropriate networks for transporting information over the Internet.

Service and application layer offers support for variety of different services. Application layer is service for different

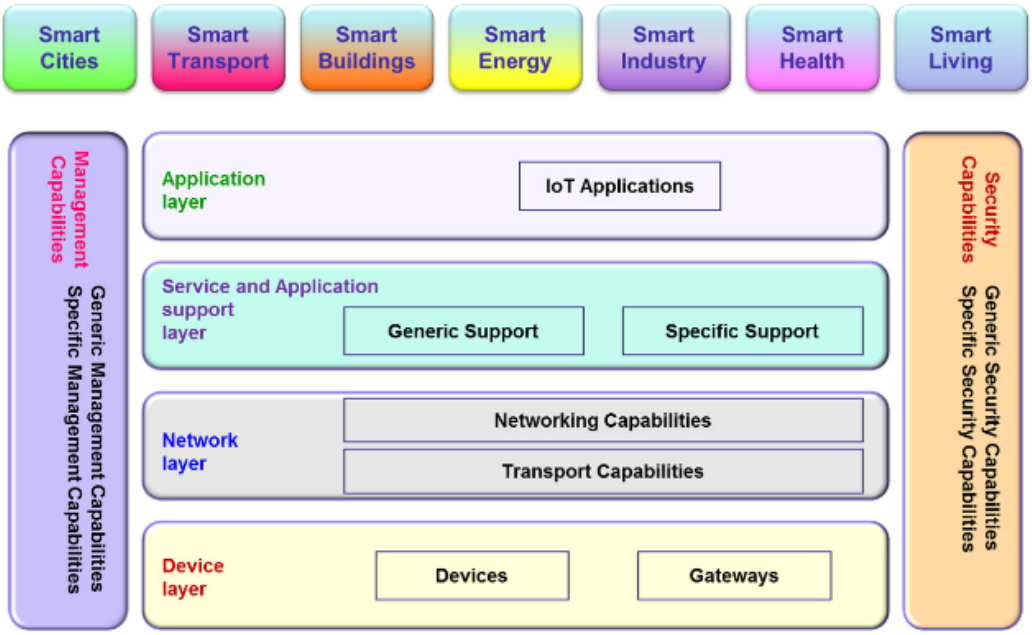

Figure 2.Internet of Things Architecture Proposed by ITU-T [1]

Applications, management of transmitted data as well as monitoring of QoS (Quality of Service).

Beside all proposed architectures, there is also an additional proposal favored by the researchers, one proposed by EPC global Network. EPC global is a part of global non-profit high tech standardization bodies. In IoT context, the objective of the EPC global is production of recommendations for "EPC global Architecture Frame Work". The EPC global is widely accepted and has support from other standardization organizations as well as industry. Results of their work are already available at [9].

3.OPEN QUESTIONS AND ISSUES

Potential offered by the Internet of Things concept, makes it possible to develop a huge number of new applications, of which only a very small number exist today. The

Internet of Things will lead to an increasing amount of data sources producing a tremendous amount of data related to a society. Here computers ("things") will replace people in a way of gathering information which would benefit in less waste of time, lower material loss and reduced overall cost. Computers need to be empowered to see, hear, and smell the real world, observe, identify and understand without limitation of data entered by humans. This simple idea, brings a number of open questions like availability of technologies for implementation, addressing security and privacy issues, and the standardization.

Technologies suitable for Internet of Things which exist today are short range Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSN), plus few more in development. In current literature RFID is presented as technology which can implement the Internet of Things vision because of low cost and strong existing support from business community. RFID together with Near Field Communications (NFC) and Wireless Sensor and Actuator Networks (WSAN) are recognized as "the atomic components that will link the real world with the digital world" [10]. As an example, RFID technology is composed of a reader and several remote tags. Tags are characterized by unified 64-96 bit identifiers. These tags can be active or passive depending on energy consumption. Tags are small chips placed on different objects. There are four different kinds of tags commonly in use: low frequency tags (125 kHz or 134.2 kHz), high frequency tags(13.56MHz), UHF tags (868 MHz to 956MHz), and microwave tags (2.45GHz). WSAN is starting to play important role in deploying new services in Internet of Things technology. New application scenarios include healthcare, environment monitoring, agriculture. Another trend is moving from traditional sensor networks toward 6LoPAN/IPv6 standard that allows native connectivity of sensors to the Internet.

As mentioned earlier in the paper, ***Standardization*** is the first and still unsolved problem that needs to be solved if IoT is to take off as a technology. Many proposals already exist but none is globally accepted and adopted. Standardization proposals are provided by institutions like Auto-ID lab, ETSI, ISO, and ITU. Figures 1 and 2 illustrate all the details than need to be standardized and agreed upon.

Situation is similar with ***Addressing*** of IoT devices. Again many proposals and solutions already exist, but none has majority acceptance across the industries. Regarding the number of devices which will use Internet addressing, addressing problem becomes essential. Since IPv4 addressing space is exhausted, IPv6 is to be employed. IPv6 gives solution for existing internet devices intended for use in regular internet surroundings. The problem is that the IPv6 is still not adapted to work with Internet of Things. Essentially, IPv6 allows for 128 bits for addressing. This will be enough for RFID which uses only 64-96 bit identifiers and this possibility has been investigated. Out of IPv6 128 bits, it is proposed that first 64 bits are used for RFID identification and the last 64 for gateway between RFID and Internet. Proposed solutions for this issue are given in [8], [12], [13], [22].

Gathering of information is next issue related to Internet of Things. Here we deal with "big data" issue. Regarding enormous number of devices which will be connected to the network (as stated earlier up to 50 billion by 2020), gathered information will be massive. Problems which arise with this amount of data are transmission, storage and processing of "big data". Transmitted amount of data varies from few kb up to several Mb. Today storage of information delivered through Internet costs around 10^{-9} euro per byte. Counting total number of devices which will be connected and amount of information retrieved, delivered and stored, leads to a conclusion that very demanding resources will be required to handle demanding IoT requirements[6].

Security and privacy of IoT are also very questionable since major problems come from wireless communications which is vulnerable to attacks. Concept of privacy is closely related to authentication and authorization. More about this is discussed in [2]. Hence IoT systems need to be designed and implemented with adequate security and privacy protection. The threat to security and privacy may not be recognized to be as significant as in other types of networks since IoT devices have limited functionality and connectivity. But there are more points of possible intrusion and vulnerability in an IoT system. A system failure or hacker attack could have serious consequences, for example in energy or other utility infrastructure. For example, a hacker could target sensors at a water treatment facility to cause false readings on whether water is potable. Most utility infrastructure IoT systems will have only security concerns but there will also be some privacy issues. Hacking into a smart utility meter, for example, could reveal whether or not a family is at home. Consumer IoT systems will need to protect both privacy and security. There will be liability issues if the IoT system fails or makes a wrong determination. Liability insurance will be needed by IoT components and systems vendors. Limiting liability by contract with a utility, state or local government or business may be feasible in the same way as for other equipment and software but contracts may not be possible in many consumer applications.

The way that IoT physical components are combined into a system and the related data analytics software can have significant business value. Intellectual property (IP) and patent protection is important. IoT system designers need to think both offensively and defensively in creating an IP strategy so they have the freedom to operate without a license from a third party and also provide a barrier to entry by a competitor. There already exist several thousand patent applications and over 100 patents issued in which the term "Internet of Things" appears when the US Patent and Trademark Office (USPTO) data base is searched. A flood of application is probably to follow both in USA, Europe and other parts of the world.

4. APPLICATIONS

There are several application domains which will be impacted by Internet of Things. New domains and areas where IoT applications will likely improve quality of our lives are home, health, work, and agriculture in many different ways.

The Home of Internet of Things

In personal and home use sensors can be used for controlling refrigerators, washing machines, air conditioner, surveillance system, etc. Another example are smart utility meters that one can read online on the utility's web site. There are pilot programs of smart meters and related technology that already rolled out USA and Europe. Utilities consumption is measured hourly and data is transmitted on a wireless basis to the utility center several times a day. Both the utility and customers can track the use. Currently, however, only few percent of developed countries customers are equipped with such smart devices and the overall implementation is slow.

The Agriculture of Internet of Things

One specific application of Internet of Things is in food supply chain. In today's world food supply is critical for human kind. In order to provide enough food, efficient management of food need to be done. Management is very complex and starts from the production, processing, storage, distribution and consumption. In this chain it is very important to provide certain level of quality. IoT can help in proper traceability, visibility and controllability of agriculture. Sensors embedded in fields can control field conditions, collect information and send data using WiFi, mobile or some other technology to the main center where the overall food chain is managed. More on this is given under Utility IoT bellow.

The Industrial Control of Internet of Things

Next type of applications are in industrial control. For example, employees monitoring, work of elevators in a building, use of lightning, heating and other industrial or building systems. Using ZigBee technology wireless sensors and passive tags, a variety of indoor locations and employees can be monitored. Sensor can also be employed for monitoring level of toxic gas and oxygen levels inside closed rooms (chemical plants for example) to ensure safety of workers.

The Traffic Control Internet of Things

Further application in IoT area is in traffic control. Here, traffic and road condition data would be collected using sensors and communicated to traffic control centers and to drivers in a form of information and traffic advice. Same can be done at traffic intersections to control smartly traffic lights and reduce accidents, traffic jams and traffic casualties. Car generated pollution can be reduced, as well as car fuel consumption. Traffic information can be provided by sensor network to determine the best route.

The Smart Cities of Internet of Things

The application of the Internet of Things paradigm to the urban context is of particular interest, for forming Smart Cities. This will bring benefits in many areas like management and optimization of traditional public services, such as transport and parking, lighting, surveillance and maintenance of public areas, parks, preservation of cultural heritage, garbage collection, maintenance of hospitals, and schools. By 2020 more of the 60 percent of world population will live in urban cities. Development of this idea has already started through FP7 Smart Santander project as well as OUTSMART project. A smart city is defined as a city that monitors and integrates conditions of all of its critical infrastructures, including roads, bridges, tunnels, rail/subways, airports, seaports, communications, water, and power, even major buildings, the city that can better optimize its resources, plan its preventive maintenance activities, and monitor security aspects while maximizing services to its typically numerous citizens. So called "Padova" city plan for smart city development is described in [14]. According to Pike research (www.pikeresearch.com) smart city market is estimated at hundreds of billions of dollars by 2020. Reference [15] summarizes a project where 77 cities were analyzed based on different criteria like economy, mobility, environment, governance, people, living conditions, etc. This is all taken into account for defining and building a smart city. The project is supported by "Technische Universitat in Wien" and started in 2007, financed by public and private stakeholders.

The Utilities of Internet of Things

Specifically for a smart home we would need a smart utility meter (water, electricity, gas) that generates usage data. This is communicated wirelessly to the utility center for the software on their computers to analyze the data and report results on the web site for a user to view. In some pilot programs, the customer can view the data as it comes in, as well as compare their numbers with past use and city averages. The usage numbers should eventually alert the user to, say, water leak plus utility status could also be measured with another device which could identify a leak immediately, rather than letting water to be wasted. To find the location for repair, however, we would need to add sensors to measure pressure at various locations in home's water system. The sensors would be connected to data analytics software in the cloud that would analyze the data transmitted in order to identify the location of the leak between two sensing points in my water system. This is a much more complex application than simply tracking water usage and illustrates the importance of the software applications needed in order to make sense of the transmitted data. The IoT can't make it rain or snow or fix leaky pipes but it can help the supply problem by making water usage more efficient and less wasteful, particularly in places where water is scarce. The IoT can also help

water be transported to the point of need with greater precision.

More Utility Applications of Internet of Things

To further expand on the utility example, the universe of utility IoT systems can be divided into infrastructure, governmental, business and consumer. The water infrastructure IoT will help improve a utility's quality, supply, treatment, transportation and storage facilities such as reservoirs. The priority for action should be to deploy the IoT at the infrastructure level since the water savings will be the greatest and action should be the fastest. A utility should be able to justify the expenditure on the water savings particularly on the basis of planning for scarcity. State and local governments can save money and also have a major impact on supply by implementing the IoT for buildings and other uses like landscape irrigation. An IoT water management system for a large building or office park can help the manager monitor and manage water use more efficiently. Water cost savings and forced conservation will help drive adoption by businesses (including often related and important agricultural industry) and consumers but they will be looking for a clear return on investment.

A utility can use an IoT system to remotely determine the status and working condition of equipment (open or closed, on or off, full or empty, etc.). A gate can be opened or closed or a pump turned on or off remotely to adjust the flow of water through a water transportation system. Pumps, gates and other equipment with moving parts in the water infrastructure can be monitored for vibration and other indications of failure. If a water pump is about to fail, the utility can be prompted to repair or replace it. An IOT-enabled water treatment plant can report if its filters are clean and functioning properly. The IoT can measure water pressure in pipes to find leaks faster in the water transportation system or the presence of certain chemicals in the water supply and maybe even organic contaminants like the ecoli which is often found especially in undeveloped areas.

Agriculture consumes lots of freshwater available in a country, with a large amount being wasted by leaky irrigation systems, inefficient field application methods and the planting of water intensive crops in the wrong growing location. The IoT has great potential to make water use smarter for the agricultural industry particularly in irrigation efficiency.

Another focus for water savings should be landscape irrigation in parks, medians and elsewhere. This is a major use of water in cities. Nationwide in USA, it is estimated to be nearly one-third of all residential water use and as much as half of this water is wasted due to runoff, evaporation or wind. An IoT landscape irrigation system is available in the market for public or private use which applies sophisticated data analytics to a wide variety of objects. Current weather data is combined with sensors for moisture and heat and other data such as the slope of the land, type of soil and the relative exposure to sunshine at a particular time.

The Retail of Internet of Things

This segment encompasses a broad range of services for end users. For example paying service can be accomplished using NFC technology, or intelligent shopping where based on your location your receive information about sales in shopping malls near you with special attention to customers habits. Also sensors can control shelves in stores signaling when shelf is empty and needs to be restocked.

The Environment of Internet of Things

In this area sensors play important role. Their functions include monitoring level of gases in preventing forest fire, or monitoring level of CO2 emission of factories, cars in defining a level of air pollution, or for monitoring level of snow preventing avalanche or landslide.

The Health of Internet of Things

Today modern society is responsible for changing healthcare model from hospital oriented toward home oriented. Including Internet of Things capabilities in this segment many effective solutions can be implemented. Some of the most important are in the area of tracking and monitoring patient status using WSN technology, in the area of remote service where diagnosis can be delivered through the Internet, patient information management where all data about patient are stored at one central place and can be reached through the Internet anytime, anywhere.

Additional Area for Internet of Things

Other application areas include: smart parking of parking places free for car parking in the city, monitoring of vibrations and conditions of material in building or some special places and monuments, controlling level of noise in the cities, in particular in centers and densely inhabited city parts, monitoring of congestion and optimization of driving and pedestrian routes, suggestions for shopping in shopping malls in a form of an advice based on customer habits, goods availability, etc.

5. SENSORS

Sensors play important role in Internet of Things technology, making it almost human with their "eyes" and "ears" features. It is not surprising that global companies are planning to invest huge amounts of money into smart sensors development. The sensor production worldwide will expand next few years, especially in area of energy and mining (33%), power and utilities (32%), automotive (31%) since many sensors are going to be embedded in the road and car for accident avoidance and hands free driving. Plans are that production of sensors in area of industrial will rise up to 25%, hospitality 22%, retail 20%, [16].

As an example of a company working in smart sensors, Omron Company is working on developing sensors as a part of smart face-recognition cameras. The sensors will be used as a part of smart home. Possible application can be in area of management lights in home. For example, sensor can detect a man sleeping at smart home and reduce level of light, possibly turning it down.

Another example is several manufacturers which started production of multi-sensor platforms integrating several sensing elements. For example, one self-tracking sensor contains several sensing elements like GPS sensor for positioning, temperature sensor for temperature of a body, heart rate sensor for measuring heart rate and blood pressure, accelerometer etc. This kind of sensor is already used in casual and professional sports, and sold by Nike, Run Keeper, Fitbit and other. In addition, "smart-watches" and "smart-glasses" are developed by Google and Apple and are expected to be widely used, [17].

In this paper (see Appendix) we also present a quick introduction of our own and new low power wireless sensor network which may be a future candidate for an IoT for certain sensor applications. We will elaborate on this in details in the subsequent paper.

6. CURRENT TRENDS IN INDUSTRY

Potential benefits from Internet of Things are almost endless. Internet of Things applications are changing the way people live, habits opening new opportunities for knowledge collecting and sharing as well as improving quality of life. These benefits are recognized by significant companies like Google, Apple, Intel and Cisco that positioned them in Internet of Things landscape, considering the Internet of Things biggest growth area as well as IP and innovation. Today many telecom operators consider that Internet of Things is becoming a core business focus measured by number of users connected in the network. Also part of this business is given to manufactures of mobile devices toward wider adoption of Internet of Things.

Computer Chips for Internet of Things

Industry Internet of Things leaders AT&T, Cisco, GE, Dell, and IBM are working with Intel to create solutions that give developers and customer flexibility to help drive market adoption, [18]. This decision is based on prediction that by the end of 2020, 50 billion of devices will be connected which will bring multi-trillion dollars of benefit for companies. Cisco even now offers solutions for smart cities, manufacturing, mining oil and gas as well as in physical security solutions, industrial networking and embedded networks [19]. IBM is also part of big alliance approaching Internet of Things vision. IBM is investing linkages between Information of Things and IBM Smarter Commerce, IBM Smarter Analytics [20]. Launching of new technology brings revolution in all parts of information and communication industry. Companies like Intel and AMD are challenged to design new chips that will conform to the requirements of the new technology. AMD has unveiled "company's embedded chip roadmap for 2014". Chips for embedded system are a key growth area intended for need of Internet of Things. After this message sent from AMD, Intel's CEO responded with their vision announcing that company is in a phase of developing a new set of chips called Quark. Quark will be one-fifth of the size of use one-tenth of the power in comparison with their best existing chips. Cisco as a market leader launched nPower X1, processor that contains 4 billion of transistors offering 400Gbps throughput. These new technologies are expected to bring huge profits to these companies. AMD and ARM have already announced that they expect grow from $11.6 billion in 2014 to $15.5 billion in next two years. All brought by the prospects of IoT.

Looking beyond simple vision of Internet to Things are Cognitive IoT, Cloud Connectivity for Internet of Things and Cloud-Assisted remote sensing CARS, that already have some features of Internet of Things.

Cognitive Internet of Things

Current research in cognitive area focuses on how to make sensors to see, hear smell and connect physical things around. This leads to development of new paradigm called Cognitive Internet of Things. New idea brings "brain" in the system which means that objects can learn about behavior, think about processes and understand different worlds around. Possible applications of this new concept can be in home, safety, health, all in order to enhance "intelligent life". The author in paper [21] gives definition of Cognitive Internet of Things and proposes architecture, where system relays on four layers: sensing control layer, data-semantic-knowledge layer, decision-making layer, and service evaluation.

Cloud Connectivity for Internet of Things

Number of devices connected to the Internet is rising every day. Most devices connect usingWiFi and WLAN solutions. Since Bluetooth and WLAN are two commonly used technologies for connecting to Internet, authors in paper [7] propose new Bluetooth technology for "things" connecting. Bluetooth 4.0 has a special extension for Bluetooth Low Energy which makes this technology suitable for low power sensors in the network. Constrained Application Protocol is protocol developed on application layer intended to be used for web services working with very simple devices with low power consumption. Using Constrained Application Protocol (CoAP) and Service Oriented Architecture (SOA) makes it possible to connect devices through different places in order to access local sensor cloud.

Cloud-Assisted Remote Sensing (CARS)

Another new concept in IoT paradigm is Cloud-Assisted Remote Sensing (CARS). CARS enable connection of distributed data, sharing of resources on global scale, real-time and remote access to data as well as pay-as-you-go

concept. With development of CARS concept there is a big potential for development Internet of Everything (IoE) concept. IoE is a new trend in communication and Internet technologies that tries to connect everything on the Internet. Recent Cisco study has shown that this trend can give 14 trillion of dollars of net-profit value in the near future. CARS concept can bring benefits in remote tracking and monitoring category where possible applications can help in preventing environmental pollution, tracking of some rare species of animals, monitoring in health care, etc. Next category is real-time resource optimization and control where possible applications are in the area of traffic control and congestion avoidance, finding place for car parking. The last category is smart troubleshooting where we need to identify, diagnose and repair certain processes, with applications in many industries [8].

7. CONCLUSION

The Internet has changed dramatically the way we live. IoT idea pushes the Internet much further. This paper is a current review of basic aspects and concepts of new IoT paradigm, as well as an introduction of a NEW IoT based low power wireless sensor network protocol. Going back to 1999 when this term is used for the first time and then going in the future of 2025 and beyond, current IoT status and thinking is represented. Since the main vision is in providing "easy life" in "smart cities", this new concepts completely corresponds to the new requirements of modern society. This new trend is recognized by big companies like who have been most vocal in expressing their interest, which encompasses hardware (the things themselves), embedded software, communication and information services associated with the "things".

During the next five years, smart antennas, new IoT related wireless technologies, low power sensors and new and efficient wireless protocols will be further developed, security and privacy issues will be addressed, reducing power of wireless devices would be resolved. During the 2020s questions regarding large scale wireless networks, self adaptive services, cloud storage and algorithms for intelligent systems will be implemented and around 2025 and beyond, new autonomous IoT systems will be developed and will be able to perform independently and in mutual interaction, culminating with a plug and play smart IoT objects and things.

8. APPENDIX

NEW LOW POWER SENSOR NETWORK PROTOCOL

In this paper, we also propose a wireless sensor network which is divided into sub-nets which account for sensor geographical "congregation" due to a prescribed or ad-hoc deployment (see Figures 3, 4). The network is suitable for low power wireless sensor networks such as contemplated in IoT.

Proposed Networking Terms:

$\mathbf{LN_m}$ – Local Network number **m,** which is a collection of fixed number of sensors forming a sensor locale, where **m = 1,2,…,N**.

$\mathbf{S_{n,m}}$ – Sensor **n** within a particular $\mathbf{LN_m}$**.** Sensor may have limited local intelligence and memory, and a specific physical protocol as considered in Section 4.3.

GN – Global Network, which is a collection of all **LN**'s hence comprising of all the deployed sensors, performing a common data reporting activity.

$\mathbf{LN_mC}$ – Local Network **m** Control sensor is "in charge" (a Master) of communication within and outside of $\mathbf{LN_m}$**.** This function is negotiable by the other sensors in $\mathbf{LN_m}$**.** An event may trigger (based on some metrics) this to be renegotiated.

GNC – Global Network Control sensor node, in charge of the overall data reporting and communication. This may also be a negotiable function.

Proposed Wireless Communication Protocols Terms:

LP_m – Local Wireless Sensor Protocol is a communication protocol internal to $\mathbf{LN_m}$**,** i.e. between any sensor $\mathbf{S_{n,m}}$ and $\mathbf{LN_mC}$**.** It needs to be as simple as possible, employed as infrequently as possible, with the lowest energy possible.

$EP_{p,q}$ – External Wireless Local Sensor Protocol is a communication protocol between $\mathbf{LN_p}$ and $\mathbf{LS_q}$**.** It may implement relay and repeat functions.

GP_p – Global Protocol between $\mathbf{LN_p}$ and **GNC.**

Network Operation

We will consider a fixed and static (not-moving-sensors) network but it will be a dynamic one in a sense that the relationships between the sensor nodes will be dynamic (such as which sensor is "in charge" at any given time; see also bellow).

The network will be self organizing. We envision the following basic situations:

1. Network Initialization (sensors not collecting data yet).
   a. Synchronize (time, etc.) sensors throughout the network. This functionmay be performed periodically to maintain network integrity. Simulation will be a reliable tool in determining how often to repeat this function.
   b. Establish relationships (Master/Neighbor/Slave) among sensors based on a pre-assigned criteria, such as sensor physical layer consideration, accuracy, battery life, memory, etc.
   c. Forming of $\mathbf{LN_m}$ and "Master" sensor "in charge", i.e. $\mathbf{LN_mC}$. This may be simply pre-determined.
   d. Test communications throughout the network to make sure that all the sensor nodes are responding and are "healthy". This is a responsibility of G**NC.**
   e. All of the above Initialization functions will be integrated into our LP_m, $EP_{p,q}$ and GP_p protocols.

2. Following initialization, the network will go silent until an event triggers data gathering and reporting.

3. An event will trigger a short network activity and data reporting traffic (causing "event network trail" in Figure 5) after which the network will go back to a quiet mode. During the event reporting the following functions will be performed:

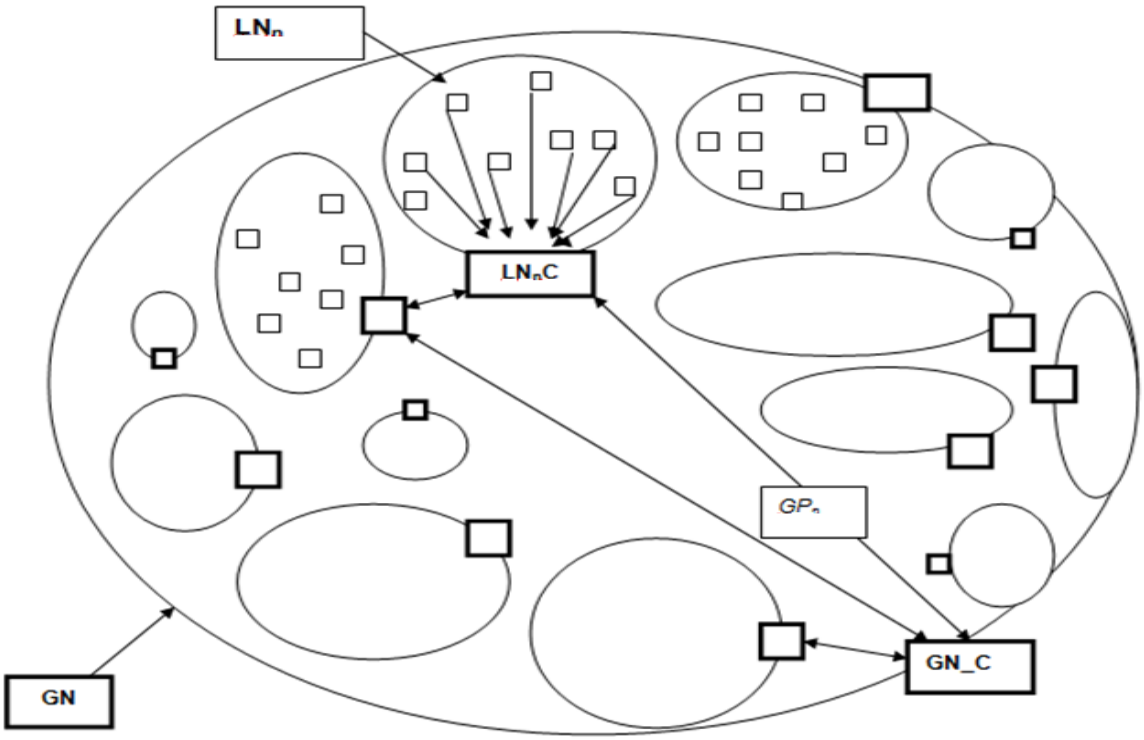

Figure 3. Global Wireless Sensor Network Topology (GN)

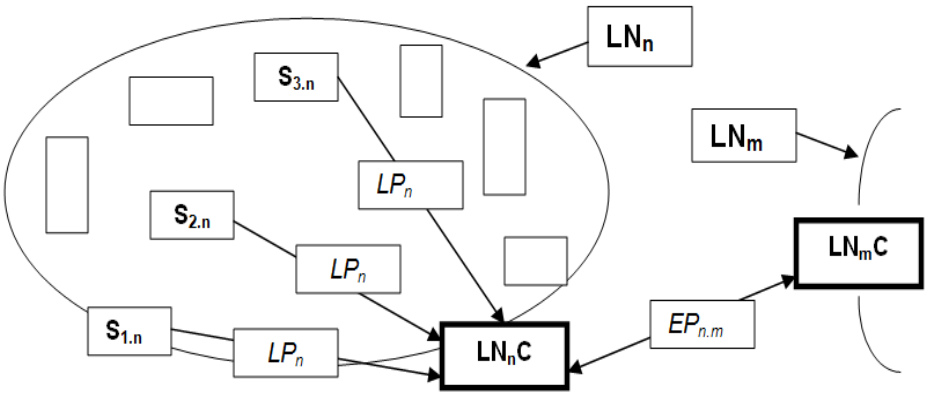

Figure 4. A Local Wireless Sensor Network Topology (**LN_n**)

a. All the reporting sensors will route their communications from within sub networks, i.e. $\mathbf{LN_m}$, through sensors in-charge, $\mathbf{LN_mC}$, to G**NC** using short packets and LP_m, $EP_{p,q}$,GP_p protocols.

b. Depending on the type of trigger event and resulting communications and reporting (number of sensors alarmed, sensor signal strength, etc.), the network may re-adjust internal structure to address the next event more effectively.

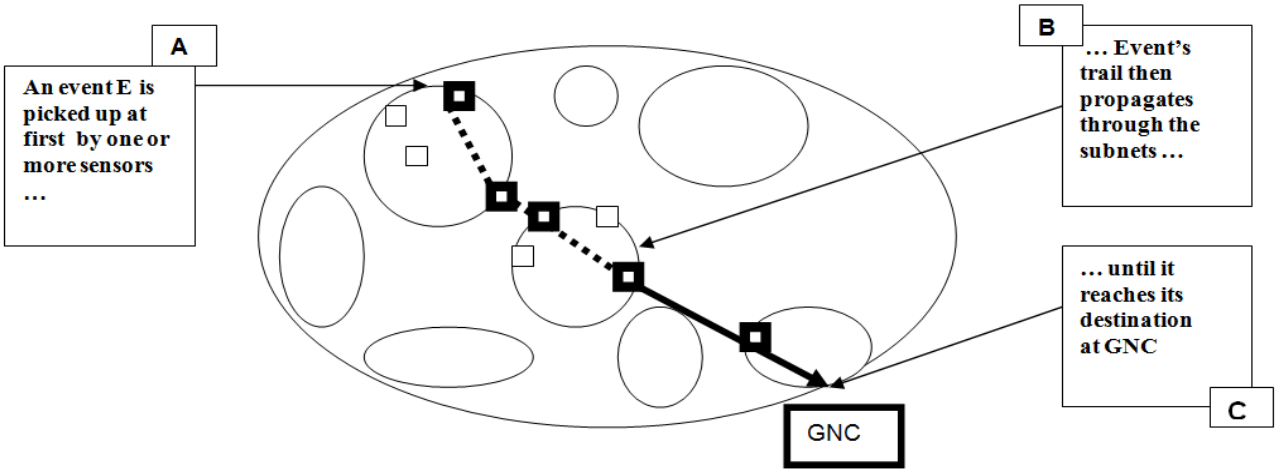

Figure 5. Event E Network Trail

Wireless Protocol Description

The design of the *LP*, *EP* and *GP* protocols came from a synthesis of our own ideas and ideas gleaned from existing successful network protocols.

The need for conserving power and greatly limiting message traffic will make the protocol quite different from existing protocols. The following is a description of our initial considerations as far as the structure of these protocols. We will use a generic description for *LP* protocol as an illustration as to how a particular subnet $\mathbf{LN_m}$ is formed and how individual sensor nodes are given roles (such as Master $\mathbf{LN_mC}$) within the subnet (see also Figure 4). The details of *LP*, as well as *EP* and *GP* will be discussed in our future work.

Sensor Node Acquisition

Initially, it is assumed that all nodes are Master's of themselves and Neighbors of themselves. There may be two general situations:

1. Node has no neighbors in the protocol tables
   a. Broadcast request for Slaves
      i. If another Master's request received
         * Negotiate Master-hood domain number
            - Generated Random domain number
            - Highest domain number becomes Master
         * If it becomes a Slave
            - Transmit neighbor list to new Master

(Which may be just itself)

2. Node has neighbors
   a. It is Master
      i. All of his neighbors are Slaves of his domain
   b. It is Slave
      i. To only one Master
      ii. May be connected to other Slaves & Masters
         * Some neighbors may belong to other Master domains
         * Another Master will consider him an ambassadorial Slave
            - Able to forward messages to and from different Master domains

In any case, the above scheme results in a particular sensor node in a subnet $\mathbf{LN_m}$ becoming a Master or $\mathbf{LN_mC}$ control node. As stated earlier, this can be re-negotiated following some network event that can trigger it.

Basic Relative Time Domain Description

1. Time is divided arbitrarily into Time Divisions (TD's). A TD belongs to one or more Master domains (i.e. one or more $\mathbf{LN_m}$'s). As Slave sensor units are added or lost, the time division of an $\mathbf{LN_m}$ domain is adjusted accordingly.

2. TD's are divided into equal size blocks. These blocks represent intervals when a sensor may transmit. Masters ($\mathbf{LN_mC}$'s) arbitrate duration assignments.

3. Time in the TD is always relative and is marked by a numerical time stamp by each sensor unit that broadcasts.

4. Everyone listens when not transmitting, and adjusts their internal time to the time in the last block received. Since each next block is clock relative to a predecessor (without absolute time reference), it insures message sequencing will undergo the **least possible** collision and boundary failures. This will **maximize** overall energy efficiency by eliminating excessive synchronization transmissions due to high traffic collisions.

5. A time block belongs to a Master domain (i.e. $\mathbf{LN_m}$). When two domains overlap, the $\mathbf{LN_mC}$'s will negotiate time block sequences and they will coalesce intoa single mutually inclusive TD such as shown in Figure 6.

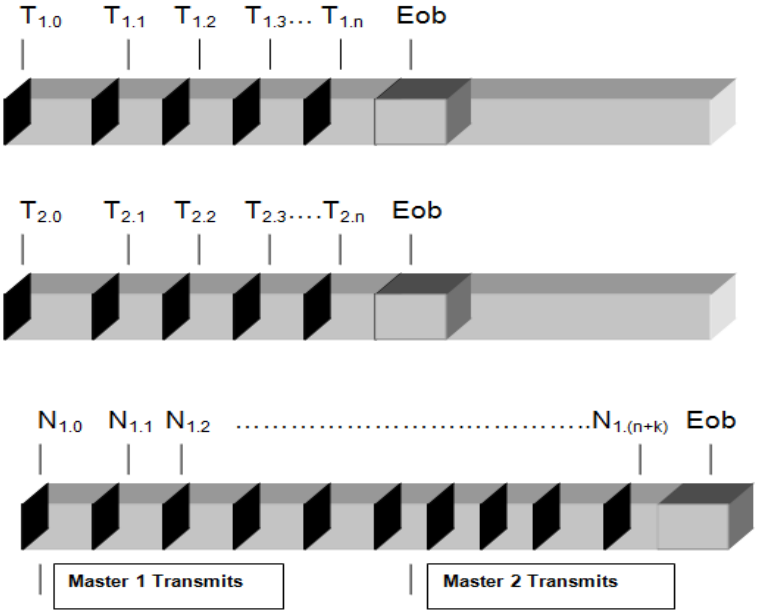

Figure 6. Simplified relative Time Domain Structure of LP protocol

REFERENCES

1. European Research Cluster on Internet of Things (2014) http://www.internet-of-things-research.eu/
2. De-Li Yang Feng Liu Yi-Duo Liang (2010) A survey on Internet of Things, Atlantis Press
3. D. L. Brock (2001) The electronic product code (epc) a naming scheme for physical objects, Auto-ID Center, White Paper
4. Ingo Friese, Challenges from the Identities of Things, Discussion group within Kantara Initiative
5. Auto-ID Laboratories, http://autoidlabs.org
6. Omar Said (2013) Towards Internet of Things: Survey and Future Vision, International Journal of Computer Networks (IJCN), Volume 5. Issue 1
7. Pablo Punal Pereira (2013) Enabling Cloud-connectivity for Mobile Internet of Things Applications 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering
8. Sherif Abdelwahab (2014) Enabling Smart Cloud Services Through Remote Sensing: An Internet of Everything Enabler IEEE Internet of Things Journal, Vol. 1, No. 3
9. Gs Global standards http://www.gs1.org/gsmp/kc/epcglobal/architecture
10.Luigi Atzori (2010) The Internet of Things: A survey Elsevier Computer Networks 54 (2010) 2787–2805
11. Bernhard H.Walke IEEE802 Wireless systems Willey 2006
12. Jayavardhana Gubbi (2013) Internet of Things (IoT): A vision, architectural elements, and future directions Elsevier Future Generation Computer Systems 29 (2013) 1645–1660
13. Prajakta Pande (2014) Internet of Things –A Future of Internet: A Survey International Journal of Advance Research in Computer Science nd management Studies Volume 2 Issue 2
14.Andrea Zanella (2014) Internet of Things for Smart Cities IEEE Internet of Things Journal Vol.1 No 1.
15. European Smart Cities http://www.smart-cities.eu/
16. PwC 6th annual digit IQ 2014, http://www.pwc.com/us/en/advisory/digital-iq-survey/assets/sensor-technology.pdf
17.Melanie Swan (2012) Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0Journal of Sensors and Actuator Networks
18. Official Intel web site www.intel.com
19. Official Cisco web site www.cisco.com
20. Official IBM web site www.ibm.com
21.Qihui Wu (2014) Cognitive Internet of Things: A New Paradigm beyond Connection
22. Treffyn Lynch Koreshoff (2013) Internet of Things: a review of literature and products