Survey on energy consumption in wireless IOT

Mahesh Patil
DYPIET Ambi,
Talegaon
maheshrpatil486@gmail.com

Mahesh Sutar
DYPIET Ambi,
Talegaon
msutar13@gmail.com

Sachin Waghmare
DYPIET Ambi,
Talegaon
sachuwagh@gmail.com

Prof. Kirti Panmand
DYPIET Ambi,
Talegaon
kirtipanmand9@gmail.com

ABSTRACT-
This paper focuses the Internet of Things. Main enabling feature of this promising model is the integration of several technologies and communication solutions. Identification and tracking technologies, wired and wireless sensor and actuator networks, enhanced communication protocols (shared with the subsequently invention Internet), and distributed intelligence for smart objects are just the most appropriate. The Internet of Things represents a hallucination in which the Internet extends into the real world hypothesis everyday objects. Physical objects are no longer detached from the virtual world, but can be controlled remotely and can act as physical access points to Internet services. Internet of Things (IoT) is a theory that envisions all items around us as element of internet. IoT management is very wide and includes diversity of things like smart phones, tablets, and sensors. Once all these devices are linked to each other, they facilitate more and more smart processes and services that maintain our basic needs, surroundings and health. Such huge number of devices linked to internet provides many different services. They also generate enormous amount of data and information. To decrease the huge amount of data we need to use data mining algorithm to provide user only required and important information.

General Term-
Internet of things, Quality of information, Smart object, Wireless sensor networks

Keywords-
Energy efficiency, Bigdata, Machine learning, Data mining

I. INTRODUCTION

A. What is IoT?

The Internet of Things (IoT) is the interconnection of uniquely identifiable embedded computing devices within the existing Internet framework. Typically, IoT is expected to offer advanced connectivity of devices and systems, and services that goes beyond M2M i.e. machine-to- machine(M2M) communications and covers a variety of protocols, various domains, and applications. The interconnection of all these embedded devices which also includes smart objects, is expected to lead in automation in nearly all fields enabling advanced applications like a Smart Grid.

B. Benefits of IoT?

Objects or things communicate with each other and perform the required actions. Human does not need to interact with system. IoT system is made up of three components: sensor, actuator, connectivity devices.

C. Risks In IoT:

Despite these important benefits, there was broad agreement among participants that increased connectivity between devices and the Internet may create a number of security and privacy risks.

D. Security Risk

According to panelists, IoT devices may present a variety of potential security risks that could be exploited to harm consumers by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating safety risks. Although each of these risks exists with traditional computers and computer networks, they are heightened in the IoT, as explained further below.

First, on IoT devices, as with desktop or laptop computers, a lack of security could enable intruders to access and misuse personal information collected and transmitted to or from the device. For example, new smart televisions enable consumers to surf the Internet, make purchases, and share photos, similar to a laptop or desktop computer. Like a computer, any security vulnerabilities in these televisions could put the information stored on or transmitted through the television at risk. If smart televisions or other devices store sensitive

financial account information, passwords, and other types of information, unauthorized persons could exploit vulnerabilities to facilitate identity theft or fraud. Thus, as consumers install more smart devices in their homes, they may increase the number of vulnerabilities an intruder could use to compromise personal information.
Second, security vulnerabilities in a particular device may facilitate attacks on the consumer's network to which it is connected, or enable attacks on other systems. For example, a compromised IoT device could be used to launch a denial of service attack. Denial of service attacks are more effective the more devices the attacker has under his or her control; as IoT devices proliferate, vulnerabilities could enable these attackers to assemble large numbers of devices to use in such attacks. Another possibility is that a connected device could be used to send malicious emails. Third, unauthorized persons might exploit security vulnerabilities to create risks to physical safety in some cases. One participant described how he was able to hack remotely into two different connected insulin pumps and change their settings so that they no longer delivered medicine. Another participant discussed a set of experiments where an attacker could gain "access to the car's internal computer network without ever physically touching the car." He described how he was able to hack into a car's built-in telematics unit and control the vehicles engine and braking, although he noted that "the risk to car owners today is incredibly small," in part because "all the automotive manufacturers that I know of are proactively trying to address these things." Although the risks currently may be small, they could be amplified as fully automated cars, and other automated physical objects, become more prevalent. Unauthorized access to Internet-connected cameras or baby monitors also raises potential physical safety concerns. Likewise, unauthorized access to data collected by fitness and other devices that track consumers' location over time could endanger consumers' physical safety. Another possibility is that a thief could remotely access data about energy usage from smart meters to determine whether a homeowner is away from home. These potential risks are exacerbated by the fact that securing connected IoT devices maybe more challenging than securing a home computer, for two main reasons. First, as some panelists noted, companies entering the IoT market may not have experience in dealing with security issues. Second, although some IoT devices are highly sophisticated, many others maybe inexpensive and essentially disposable. In those cases, if vulnerability were discovered after manufacture, it may be difficult or impossible to update the software or apply a patch.
And if an update is available, many consumers may never hear about it. Relatively, many companies – particularly those developing low-end devices – may lack economic incentives to provide ongoing support or software security updates at all, leaving consumers with unsupported or vulnerable devices shortly after purchase.

E. Privacy Risks

In addition to risks to security, participants identified privacy risks flowing from the Internet of Things. Some of these risks involve the direct collection of sensitive personal information, such as precise geo location, financial account numbers, or health information –risks already presented by traditional Internet and mobile commerce. Others arise from the collection of personal information, habits, locations, and physical conditions over time, which may allow an entity that has not directly collected sensitive information to infer it. The sheer volume of data that even a small number of devices can generate is stunning: one participant indicated that fewer than 10,000 households using the company's IoT home automation product can "generate 150 million discrete data points a day" or approximately one data point every six seconds for each household. Such a massive volume of granular data allows those with access to the data to perform analyses that would not be possible with less rich data sets.61 According to a participant, "researchers are beginning to show that existing smart phone sensors can be used to infer a user's mood; stress levels; personality type; bipolar disorder; demographics (*e.g.*, gender, marital status, job status, age); smoking habits; overall well-being; progression of Parkinson's disease; sleep patterns; happiness; levels of exercise; and types of physical activity or movement." This participant noted that such inferences could be used to provide beneficial services to consumers, but also could be misused. Relatedly, another participant referred to the IoT as enabling the collection of "sensitive behavior patterns, which could be used in unauthorized ways or by unauthorized individuals." Some panelists cited to general privacy risks associated with these granular information-collection practices, including the concern that the trend towards abundant collection of data creates a "non-targeted dragnet collection from devices in the environment."
During the interconnection IoT is suffering from several security challenges and there are potential vulnerabilities due to complicated networks referring to heterogeneous target sensors and backend management system.

F. What is QoI?

Whatever information system providing to user should be as per users requirement and fit to use for his particular purpose. Sensor stores huge amount of data in database but user need only limited information so system should able to provide him only important information. We propose the relevancy of the sensor to task as the degree to which the sensor can satisfy tasks QoI requirements.

G. What is energy efficiency?

We need to create a set of task and find out each task which sensor is required, and for executing this task we will turn on sensor for particular time interval and after completion of task sensor will go to idle state. So, in this way we are trying to improve energy efficiency of system. This is called as duty cycling.

Efficient heterogeneous sensing of the urban environment needs to simultaneously meet competing demands of multiple sensing modalities. This has implications on network traffic, data storage, and energy utilization. Importantly, this encompasses both fixed and mobile sensing infrastructure as well as continuous and random sampling. A generalized framework is required for data collection and modeling that effectively exploits spatial and temporal characteristics of the data, both in the sensing domain as well as the associated transform domains.

II. RELATED WORK

A hybrid security and compressive sensing-based scheme for multimedia sensor data gathering is presented. It has light security mechanism and thus decreases the complexity and energy consumption of system [7]. However, given the fact that most wireless sensor devices are resource constrained and operate on batteries, the communication overhead and power consumption are therefore important issues for WSNs design. In order to efficiently manage these wireless sensor devices in a united manner, the industrial authorities should be able to provide a network infrastructure supporting various WSN applications and services that facilitate the management of sensor-equipped real-world entities [3].It is a method to select M2M gateway from a large number of possibilities in order to increase service availability while also obtaining better signal strength for higher QoS. The methods presented are evaluated in terms of their performance, including energy consumption, and a service deployment guideline is derived using real-world data collected at an exhibition, which gave encouraging results [5].An Energy-Efficient and Delay-Aware Wireless Computing System (E2DA-WCS). Since there is a tradeoff relationship between the power consumption and the delay for data collection, our proposed system controls the sleep schedule and the number of links to minimize the power consumption while satisfying an acceptable delay constraint [6].

Wireless sensor networks (WSN) behave as a digital skin, providing a virtual layer where the information about the physical world can be accessed by any computational system [8]. Wireless sensor networks (WSN) behave as a digital skin, providing a virtual layer where the information about the physical world can be accessed by any computational system [9].This paper depicts such challenges on technologies, applications, and standardization, and also proposes an open and general IoT architecture consisting of three platforms to meet the architecture challenge. Finally, this paper discusses the opportunity and prospect of IoT [10]. In this paper, we propose Mobile Sensor Data Processing Engine (MOSDEN), and plug-in-based IoT middleware for mobile devices, that allows collecting and processing sensor data without programming efforts. Our architecture also supports sensing as a service model. We present the results of the evaluations that demonstrate its suitability towards real world deployments. Our proposed middleware is built on Android platform [2]. A design an aggregated-proof based hierarchical authentication scheme (APHA) for the layered networks. Concretely, 1) the aggregated-proofs are established for multiple targets to achieve backward and forward anonymous data transmission; 2) the directed path descriptors, homomorphism functions, and Chebyshev chaotic maps are jointly applied for mutual authentication; 3) different access authorities are assigned to achieve hierarchical access control [4].We present a framework where IoT can enhance public safety by crowd management via sensing services that are provided by smart phones equipped with various types of sensors [11]. Our purpose is to minimize energy consume by sensor and improve its efficiency. Sensor collects the huge amount of data from environment which we are storing in database user always looking for short and important data or information from database so our purpose is to fulfill user's expectations by using data mining algorithm for accessing data from database. Data mining is technique used to extract short and important data from enormous amount of data. Keeping the sensor always in active [on] state required large amount of energy so to reduce this energy consumption we will switch sensor from active to idle and idle to active state as per user's request.. System should take decisions from its past experiences. That is system should behave rationally. Sensor daily collects the data and stores it in the cloud. Cloud is accessible only to the authorized user. Someone should not alter or change the data in the cloud. We are going to use strong authentication technique for this purpose.

III. FUTURE SCOPE

In the future work, a more robust and reliable device management system for IoT needs to be built. Especially, the following research issues need to be considered with higher priorities:

A. SMART CITY

Technically speaking, smart city is very much like a conceptualized blueprint, rather than actual services that have been implemented and put in use in people's everyday life. However, the development of the concept is booming while the urban population has expanded rapidly in recent year's .By 2025, with more than 60% of the

world population expected to live in urban cities. By 2023, there will be 30 mega cities globally, with 55% in developing countries, such as China, India, Russia and Latin America.

B. SMART HOME

The concept of smart home has existed for over 10 years. Although the related technologies are well mature, there are still barriers to populate a large scale adoption, such as expensive unit price, exaggerated advertising, fancy ideas but not practical, and lack of industry standards. The existing applications can be categorized into Following areas:

a) *Home Security and Monitoring:*

The applications include window/door control, gas/smoke detector, infrared sensor, remote control/emergency button and air conditioner control. It also provides alternative method to take care of children and elderly.

b) *Community Security:*

These applications include property management, community monitoring, electric patrol, security intercom and entrance guard.

c*) Multi-Service Home Gateway:*

The applications include broadband service, home multimedia system, IPTV and remote health monitoring.

c) *Home Devices Connectivity and Control:*

Including intelligent home appliances, such as smart bulb, high-end wash machine refrigerator, which are already available on the market.

C. SMART TRANSPORTATION

The development of smart transportation is generally led by governments or transportation authorities. Successful examples include real time traffic and public transportation information sharing, intelligent traffic control systems, incentive program to regulate transportation, largely promotion of electric vehicle and charging facilities, and dedicated short-range communication (DSRC) enabled vehicular communication system,

a) Navigation and Safety:

Utilizing the vehicles (e.g., cars, buses, trains) along with the roads and the rails equipped with sensors, actuators and processing power, important traffic information could be offered to the drivers or passengers of the vehicles to achieve better navigation and safety.

b) Road Planning and Route Optimization: Benefiting from the more accurate traffic information about road patterns, governmental authorities could better plan and design the roads. Particularly, intelligent roads can be performed, with warning messages based on climate conditions and unexpected events (e.g., accidents or traffic jams).

D. REAL TIME MANAGEMENT:

It is a challenging issue for resource constrained sensor networks. In this case, the IoT system needs to rely on efficient service gateway design to minimize the amount of data to be sent by constantly reviewing the data from users, and intelligent data oriented middleware design to only transmit real time information when a reading is out-of-threshold.

E. SECURITY AND PRIVACY:

Security, trust and privacy are also important issues to be considered in practical applications. There are both hard way and soft way methods to achieve different degrees of security. These security methods are appropriate for M2M deployments where there is an existing trust relationship between the devices and server.

IV. CONCLUSION

Thus we have concluded that it is possible to implement energy efficient system with the quality of data. All the system in existing mechanism implements either energy efficiency or providing quality of information. System which provides quality of information needs more energy for good performance. It is possible to implement data mining technique and machine learning algorithm for quality of performance of system with efficient energy consumption.

V. ACKNOWLEDGMENTS

We are thankful to our UG Prof. Kirti Panmand for guiding us and providing knowledge required for this project. We also Thanks our project co-coordinator for supporting us and allow us to work on this project.

.

VI. REFERENCES

[1] Chi Harold Liu,Jun Fan, Joel W. Branch2,And Kin K. Leung ,"Toward QoI and Energy-Efficiency in Internet-of-Things Sensory Environments", volume 2, no. 4, December 2014

[2] Charith Perera, Prem Prakash Jayaraman, Arkady Zaslavsky, Dimitrios Georgakopoulos, "MOSDEN: An Internet of Things Middleware for Resource ConstraineMobile"978-1-4799-2504-9/14 $31.00 © 2014

[3] Zhengguo Sheng, Chinmaya Mahapatra Chunsheng Zhu And Victor C. M. Leung, "recent advances in industrial wireless sensor networks toward efficient management in iot", volume 3, 2015.

[4] Huansheng Ning, Hong Liu and Laurence T. Yang "Aggregated- Proof Based Hierarchical Authentication Scheme for the Internet of Things", VOL. 26, NO. 3, MARCH 2015

[5] V. G. Tharinda Nishantha Vidanagama, Daisuke Arai, And Tomohiko Ogishi, "service environment for smart wireless devices: an m2m gateway selection scheme" ,volume 3, 2015.

[6] Katsuya Sutox, Hiroki Nishiyamax, NeiKatox, Chih-Wei Huang," an energy-efficient and delay-aware wireless computing system for industrial wireless sensor networks", 2169-3536 (c) 2015

[7] Jin Qi1, Xiaoxuan Hu, Yun Ma1, And Yanfei Sun ", a hybrid security and compressive sensing-based sensor data gathering scheme", volume 3, 2015.

[8] Cristina Alcaraz, Pablo Najera, Javier Lopez, Rodrigo Roman, "wireless sensor networks and the internet of things do we need a complete integration?",volume 2,2014

[9] Friedeman Mattern And Christian Floerkemeier," from the internet of computers to the internet of things" ,volume 3,2015

[10] Shanzhi Chen, HuiXu, Dake Liu, Bo Hu, And Hucheng Wang,"A Vision of IoT: Applications, Challenges, and Opportunities with China Perspective" vol. 1, no. 4, august 2014

[11] Burak Kantarci and Hussein T. Mouftah," Trustworthy Sensing for Public Safety in Cloud-Centric Internet of Things", vol. 1, no. 4, august 2014