*Communications and Network*, **2013, 5, 44-48**
doi:10.4236/cn.2013.51B011 Published Online February 2013 (http://www.scirp.org/journal/cn)

# A Green and Reliable Internet of Things

**Shyam Sundar Prasad[1], Chanakya Kumar[2]**
[1]Deptment of ECE, National Institute of Technology, Jamshedpur, India
[2]Deptment of ECE, Sam Higginbottom Institute of Agriculture, Technology & Science, Allahabad, India
Email: ssprasad@ieee.org, chankyajha@yahoo.co.in

Received 2012

## ABSTRACT

Internet of Things (IoT) is innovation in the field of Communication where a number of intelligent devices are involved sharing information and making collaborative decision. IOT is going to be a market-changing force for a wide variety of real-time monitoring applications, such as E-healthcare, homes automation system, environmental monitoring and industrial automation as it is supporting to a large number of characteristics and achieving better cost efficiency. This article explores the emerging IoT in terms of the potential Energy Efficiency Reliability (EER) issues. This paper discusses the potential EER barriers with examples and suggests remedies and techniques which are helpful in propelling the development and deployment of IoT applications.

**Keywords:** Energy Efficiency Reliability; Internet of Things; Machine to Machine Communication

## 1. Introduction

Internet of Things is a new research in the field of Internet. IoT is the advance version of Machine to Machine (M2M) Communication, where each object connects with another object, without human intervention.

In IoT, billions of objects can communicate, recognize and respond without human intervention. IoT may be explained with the following example: When a car goes to a petrol pump station, it will refill petrol in the car. A sensor at the pump will read the registration number of the car, and pass the information to the credit card swapping machine, which will deduct the amount for the petrol filled, automatically. Similarly, plants in a field may communicate to a sprinkler system, when they need to be watered. A runner's shoes may communicate time, speed and distance to him or her. Current research projections estimate that within 5-10 years, 100 billion devices will be connected to the internet [1].

Previously, computers communicated via Electronic Data Interchange (EDI). With the advent of internet, all computers are now able to connect and communicate. Their ability is not only limited to communication but they can also control and monitor another device. Thus devices start talking. With the revolution of wireless communication, mobile devices can also be easily connected. Evolution of Internet of Things has made it possible for objects to get information about their position in the world, to interact with other objects, and to have access to information for data gathered in their vicinity.

Internet of Things first started in the 1990s, with Industrial automation systems. Slowly, internet and internet protocols became widely used between embedded devices and Back End Servers (BS). The vision behind Internet of Things is that embedded devices, also called smart objects, will universally become IP enabled with the help of IPV6.

Hence, they will also slowly become an integral part of the internet. M2M serves as a base for IoT. The basic components of internet of things are a node sensor and its connection strategy – i.e. how this sensor will transfer data to a collecting device. Gradually IoT will lead to all objects surrounding us that are connected to the Internet in some way or the other. Thus, Energy Efficiency Reliability-EER becomes an issue of concern.

This paper technically discusses the energy efficiency and reliability issues in emerging IoT communications, and suggests introduction of efficient activity scheduling schemes for providing an energy efficient and reliable IoT communications environment.

## 2. Overview of IoT Communication Architecture

As shown in **Figure 1**, architecture of Internet of Things consists of sensor nodes, network domain, and application domains [2].

Sensor Node domain is same as M2M node domain in M2M communication [2]. In the node domain, an area network is potentially formed by a large number of IoT nodes {$N0$, $N1$ …} and an IoT Gate Way (GW). Each IoT node $N_i$ is a very flexible and smart device equipped with some specific sensing technology for real-time monitoring. Once monitoring data are sensed, IoT nodes

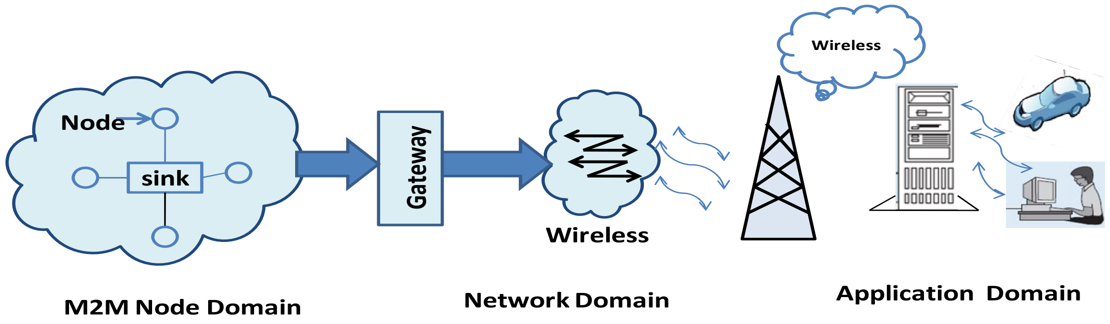

**Figure 1. The structure of M2M communication.**

will make intelligent decision and transmit the sensory data packets to the GW in single-hop or multihop patterns.

The Gateway GW is an integrated device. After collecting the packets from nodes, it is able to intelligently manage the packets and provide efficient paths for forwarding these packets to the remote back-end server (BS) via wired/wireless networks.

Network Network domain provides cost-effective and reliable channels for transmitting sensory data packets from the Sensor domain to the application domain.

Application domain is the last part of the architecture. In the application domain, BS is the key component for the whole IoT communication paradigm, which not only forms the data integration point for storing all sensory data from the IoT domain, but also provides these real-time data to a variety of IoT applications for remote monitoring management.

## 3. The EER Requirements in IoT Communication

Despite the real –time application and lots of benefits, research in M2M communication still in its infancy and faces many technical challenges. These challenges include M2M Architecture, M2M communication's Green issues, M2M cost effectiveness, M2M reliability, M2M Privacy, Persistency, Security [3].

Recently, much attention has been paid to the deployment of architecture and software challenges in M2M communications not only from the IT industry but also from academia [3].

However, the energy efficiency, reliability, and security issues in M2M Communications have not been well explored. According to a recent report on global carbon emissions [4], information and communication technology (ICT) accounts for 2–2.5 percent of all harmful emissions, which is almost equal to the global aviation industry. Therefore, to protect global environments, green communication has been widely advocated for achieving energy efficiency in communication networks.

All IoT communication systems may have unique features in a rapidly growing environment, and they are generally organized in an architecture similar to that shown in **Figure 2**, with the following common characteristic: a massive number of sensor nodes are deployed in the IoT domain to collect useful monitoring data by sensing technologies and real-time processes, and to transmit sensory data to the BS in the application domain without direct human intervention. This characteristic can benefit users from fast growing IoT communications in many promising applications; however, it also brings new EER challenges.

To successfully deploy IoT communication systems for the next generation, real-time monitoring applications are required and Energy-efficiency and Reliability (EER) requirements must be satisfied.

### 3.1. Efficient

Since a mass of Sensor nodes {$N0$, $N1$…} are deployed in the IoT sensor domain, IoT communication should focus on energy saving by optimizing sensor nodes-sensing, processing, and transmissions, and ultimately

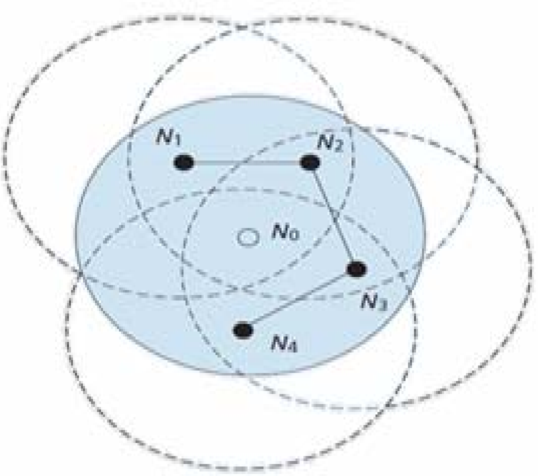

**Figure 2. An example that node N0 may switch to sleep mode because its sensing range is fully covered by the connected neighbors N1… N4.**

prolong the lifetime of the whole IoT communication. In addition, since the BS is also a power-con- suming component in IoT communication, great efforts should also be made on the BS to achieve environment friendly, green IOT communication.

### 3.2. Reliability

Reliability is critical for Efficient IoT communication, because unreliable sensing, processing, and transmission can cause false monitoring data reports, long delays, and even data loss, which would reduce people's interest in IoT communication. Therefore, the rapid growth of IoT communication demands high reliability.

Now, let us discuss the EER issues in IoT communication by surveying several potentially useful solutions to shed light on this research line.

## 4. Energy Efficiency in IoT Communication

IoT communication system is dependent upon the massive sensor nodes to intelligently collect monitoring data in the IoT domain. It is also dependent on the wired/ wireless network to relay the collected sensory data to the BS in the network domain, and on the BS, to support various IoT applications on the network in an application domain. This is because a massive number of devices are involved in IoT. The Energy Efficiency (green) becomes a challenging issue especially in the IoT sensor domain. IoT Communication dominates energy consumption. Energy Efficiency can be increased by wisely adjusting transmission power (to the minimal necessary level), and carefully applying algorithms and distributing computing techniques to design efficient communication protocols (e.g., routing protocols) [5].

It can be further improved by activity scheduling, the objective of which is to switch some nodes to low-power operation ("sleeping") mode so that only a subset of connected nodes remain active while the functionality (e.g., sensing and data gathering) of the original network is preserved. In [6] an activity scheduling scheme is proposed for sensing coverage, which appears to be the best in the literature. This scheme requires time to be slotted, and activity scheduling is then done in rounds. In each round, a node selects a random timeout and listens to messages from neighbors before it expires. These messages contain the activity decision (i.e., whether to be active or not) of their senders.

When the timeout expires, which is solely based on the received information, the node makes its own activity decision and announces it to the neighbors by transmitting a message. A node decides to be active if its sensing range (coverage circle) is fully covered by the sensing ranges of a connected set of active neighbors.

The decision on full coverage is in turn grounded on a well-known geometric theorem (illustrated in **Figure 2**, together with the connectivity consideration): if there are at least two coverage circles, and any intersection point of the two circles inside the sensing area is covered by a third coverage circle, the sensing area is fully covered. Some nodes may have announced themselves as active, and later, after receiving new announcements from neighbors, find that they are fully covered. In this case, they may change their previous decisions and enter sleep mode after announcing their new decisions.

The scheme involves local communication only and generates a very small number of control messages, thus being Energy Efficient. Simulations based on ideal and realistic physical layers reveal its advantages over other similar algorithms. Therefore, the scheme can be applied to achieve Green communication in the IOT domain.

## 5. Reliability in IoT Communication

For achieving Green IoT, since not all sensor nodes are expected to simultaneously be active in the IoT domain, Reliability is a challenging issue. In order to improve the Reliability of IoT communication, exploiting redundancy technologies, including information redundancy, spatial redundancy, and temporal redundancy, can be an efficient approach for IoT communication. Below, let us discuss three major Reliability issues in IoT communication with different redundancy technologies.

## 6. Reliability in Sensing and Processing

Due to component faults and so on, a single IoT node may not be sufficient to accurately sense and process monitoring data. Therefore, a majority vote in green IoT communication is desirable to improve reliability. In [7], a local vote decision fusion (LVDF) algorithm is presented, which can be directly applied in IoT communication. In LVDF, each IoT node $Ni$ first independently senses, processes, and makes an initial single-bit decision $di \in \{0, 1\}$ on some event in a specific IoT application, and shares the decision $di$ with its neighbors $NB(i)$. Given a set of decisions $\{di : j \in NB(i)\}$, node $Ni$ adjusts initial decision $di \rightarrow z_i \in \{0, 1\}$ based on the majority voting strategy. In the end, all updated decisions $z_i$ are communicated to the GW, which again uses majority voting to make a decision based on $z_i$. Since LVDF is a corrected decision strategy, it can improve the sensing and processing reliability in IoT communication with additional information and temporal redundancy.

## 7. Reliability in Transmission

Consider that there are $n$ total positive monitoring data on the same event in the IoT domain, and the GW will report the decision to the BS only if it can collect more than *k* distinct monitoring data packets. These positive monitoring data can first be aggregated and then forwarded to the GW together for achieving communication efficiency. However, in green IoT communication, not all nodes are active, which may result in unreliable transmission in the IoT domain.

To improve transmission reliability, spatial redundancy technology can be adopted [7]. Specifically, each monitoring data packet is independently transmitted to the GW. Assume that each transmission has an equal transmission reliability *p* in the IOT domain, where 0 < *p* ≤1. Then the reliability of more than *k* out of *n* packets can reach the GW for making the correct decision, $\sum_{i}^{n} = K\binom{n}{i}p^{i}(1-p)^{n-i}$. Obviously, at the cost of redundant transmissions, the reliability in this strategy is higher than that in the aggregation transmission.

## 8. Reliability at BS

The BS receives sensory and decisional data packets from the GW. These are processed one by one in the application domain and only one server is used to process them as this saves energy (power). But when there is considerable increase in the data packets, which may happen during peak hours, one single server is not adequate to deal with the situation. In such a case, reliability and QoS degrade. Therefore, to solve this issue a pair of servers, i.e. a primary and secondary server is deployed at the application domain. (Shown in **Figure 3**) So, when there are a large number of data packets, the second server will automatically be activated [2].

We model both the primary and second servers as M/M/1 queuing systems, where the means of service time are $1/\mu_p$ and $1/\mu_s$, respectively. Let λ be the arrival rate at the BS. If λ is small, all packets will be served by the primary server for energy saving. However, when λ increases, a fraction λ, where0 ≤ α <λ, of the packets will be served by the second server, and the rest, 1–α packets, will still be served by the primary server for guaranteeing the QoS in terms of average service delay. Therefore, the total average delay can be expressed as

$$E(D) = \frac{\alpha}{\mu_p - \lambda.\alpha} + \frac{1-\alpha}{\mu_p - (1-\alpha)\lambda}$$

where and

By calculating the derivative

$$\frac{dE(D)}{d\alpha} = 0$$

We have

$$\alpha = \frac{\sqrt{\mu_p\mu_s} - \sqrt{\mu_s\mu_p} + \sqrt{\mu_s\lambda}}{\left(\sqrt{\mu_p + \sqrt{\mu_s}}\right)\lambda}, \qquad (1)$$

which indicates that, all packets are served by the primary server; when the second server will be adaptively active, and serve a fraction α of packets. Therefore, the reliability issues in IOT communication can be addressed by redundancy technologies; however, they will incur additional redundancy costs. How to balance greenness and reliability in IOT communication needs further exploration.

To transfer secure data with reliability and efficiently is an important issue for IOT communication. To achieve this there are many research paper has been published -for example by using the optimal allocation method of the message shares onto multiple paths in terms of security, and the multipath discovery techniques in a mobile ad hoc network [8].

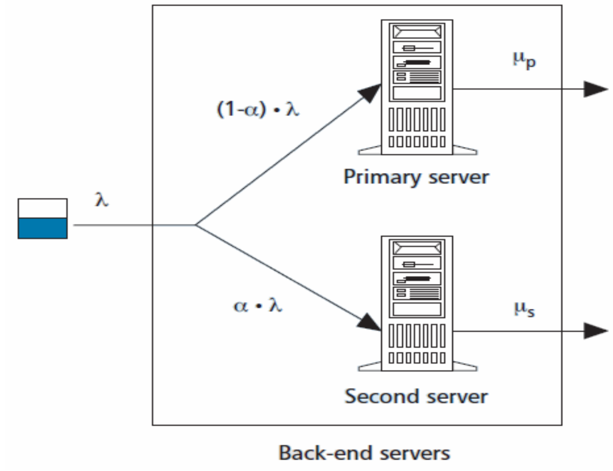

**Figure 3. The deployments of primary and second servers to achieve reliability [2].**

## 9. Conclusions

In this article, we have studied the issues to achieve green IoT communication by employing efficient activity scheduling techniques for energy saving. We have also offered several approaches to address the reliability issues in IoT. Although we have discussed the EER issues in the general IoT paradigm to shed light on this research line, further efforts are needed to identify the EER issues in specific IoT communication contexts.

## REFERENCES

[1] Source: Michael Nelson, IBM IT director.

[2] R. S. Lu, “GRS: The Green, Reliability, and Security of Emerging Machine to Machine Communication” *IEEE Communication Magazine,* April 2011.

[3] S. Hattangady, “Wireless M2M the Opportunity is Here!(Part1),”http://emblazeworld.com/AttachmentsArticles/2009-MayCellular WhitepaperPart 1.pdf

[4] R. Hodges and W. White, “Go Green in ICT,”

http://www.nascio.org/committees/green/whitepapes/bdna.pdf¸ 2008

[5] I. Stojmenovic, "Localized Network Layer Protocols in Wireless Sensor Networks based on Optimizing Cost Over Progress Ratio," *IEEE Network*, Vol. 20, No. 1,2006, pp. 21-27. doi:10.1109/MNET.2006.1580915

[6] A. Gallais *et al.*, "Localized Sensor Area Coverage With Low Communication Overhead," *IEEE Trans. Mobile Computing*, Vol. 7, No. 5, 2008, pp. 661-672. doi:10.1109/TMC.2007.70793

[7] N. Katenka, E. Levina and G. Michailidis, "Local Vote Decision Fusion for Target Detection in Wireless Sensor Networks," *IEEE Transactions on Signal Processing*, Vol. 56, No. 1, 2008, pp. 329-338.
doi:10.1109/TSP.2007.900165

[8] W. Lou *et al.*, "Spread: Improving Network Security by Multipath Routing in Mobile Ad Hoc Networks," *Wireless Networks*, Vol. 15, No. 3, 2009, pp. 279-294. doi:10.1007/s11276-007-0039-4