Internet of Things: Usage of LiFi and Need for Flow Control Protocol

B R Vatsala
Dept of Computer Science and Engineering
The National Institute of Engineering
Mysore, India
vat_mys@yahoo.com

Dr. Vidya Raj C
Dept of Computer Science and Engineering
The National Institute of Engineering
Mysore, India
vidya_rajc@yahoo.com

Abstract**—**The Internet of Things (IoT) is the future of Internet. It is the network of physical objects accessed through Internet. The objects have embedded sensors that will capture potentially enormous amounts of data, A processing system inside the object processes the captured data and these processed data are to be transmitted as quickly as possible. Thus there is a requirement for high bandwidth network and appropriate data transfer protocols.

Keywords*-IOT;Bandwidth;LiFi;Flow control protoco;Flow Completion Time*

*****

I. Introduction

The Internet of Things (IoT) is part of the Internet of the future and will comprise billions of intelligent communicating " things" or Internet Connected Objects (ICOs) that will have sensing, actuating, and data processing capabilities [1]. Each ICO will have one or more embedded sensors that will capture potentially enormous amounts of data, which need to be transmitted as quickly as possible requiring more bandwidth. LIFI is one potential solution for this.

LiFi can be thought as a light based Wi-Fi. That is, it uses light instead of radio waves to transmit information providing large bandwidth, it is eco friendly and low cost compared to WiFi[13][15]

If ICOs are connected using LiFi, it means that they communicate fast utilizing high bandwidth only in the local area. When the information is to be transmitted to or received from Internet, which has comparatively low bandwidth there is a need for a flow control protocol that synchronizes LiFi and Internet, but at present no such protocol exists implicating a need to design and implement a new protocol for the above said purpose.

This paper is organized as follows. Section II elaborates on Internet of Things and its requirements Section III discusses the LiFi Technology. Section IV discusses the need for flow control protocol for IOT.

II. Internet of things

The IoT will consist of billions of digital devices, people, services and other physical objects having the potential to seamlessly connect, interact and exchange information about themselves and their environment. It will combine the power of universal network connectivity with embedded systems, sensors and actuators in the physical world. It allows devices to communicate with each other, access information over the Internet, store and retrieve data and interact with users, smart, pervasive and always connected environments.

The main strength of the IoT idea is the high impact it will have on several aspects of everyday-life and behavior of potential users. From the point of view of a private user, the most obvious effects of the IoT introduction will be visible in both working and domestic fields. In this context, e-commerce, e-health, enhanced learning are only a few examples of possible application scenarios in which the new paradigm will play leading role in the near future. Similarly, from the perspective of business users, the most apparent consequences will be equally visible in fields such as, automation and industrial manufacturing, logistics, business/process management, intelligent transportation of people and goods. the US National Intelligence Council foresees that ‘‘by 2025 Internet nodes may reside in everyday things – food packages, furniture, paper documents, and more”. It highlights future opportunities that will arise, starting from the idea that ‘‘popular demand combined with technology advances could drive widespread diffusion of an Internet of Things (IoT) that could, like the present Internet, contribute invaluably to economic development [2] Fig 1 gives the application of IoT in day to day life.

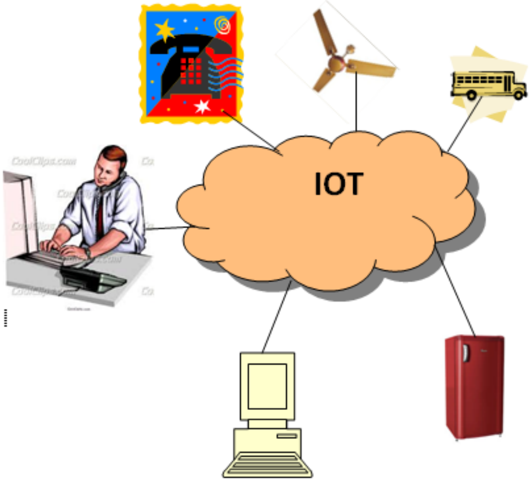

Figure 1. IoT Scenario

The vision of IoT can be seen from two perspectives— ‘Internet’ centric and ‘Thing’ centric. The Internet centric architecture will involve internet services being the main focus while data is contributed by the objects.

From a technical point of view,The capabilities of the Internet of Things include: Communication and cooperation, Addressability, Identification, Sensing, Actuation, Embedded information processing and Localization and User interfaces.

The demands placed on the IoT technology are substantial. In addition to the expectation that the technology must be available at low cost if a large number of objects are actually to be equipped, many challenges exist such as:

* *Scalability:* An Internet of Things potentially has a larger overall scope than the conventional Internet of computers. But then again, things cooperate mainly within a local environment. Basic functionality such as communication and service discovery therefore need to function equally efficiently in both small-scale and large-scale environments.

* *Arrive and operate:* Smart everyday objects should not be perceived as computers that require their users to configure and adapt them to particular situations. Mobile things, which are often only sporadically used, need to establish connections spontaneously, and organize and configure themselves to suit their particular environment.

* *Interoperability:* Since the world of physical things is extremely diverse, in an Internet of Things each type of smart object is likely to have different information, processing and communication capabilities. Different smart objects would also be subjected to very different conditions such as the energy available and the communications bandwidth required. However, to facilitate communication and cooperation, common practices and standards are required. This is particularly important with regard to object addresses. These should comply with a standardized schema if at all possible, along the lines of the IP standard used in the conventional Internet domain.

* *Discovery:* In dynamic environments, suitable services for things must be automatically identified, which requires appropriate semantic means of describing their functionality. Users will want to receive product-related information, and will want to use search engines that can find things or provide information about an object's state.

* *Software complexity:* Although the software systems in smart objects will have to function with minimal resources, as in conventional embedded systems, a more extensive software infrastructure will be needed on the network and on background servers in order to manage the smart objects and provide services to support them.

* *Data volumes:* While some application scenarios will involve brief, infrequent communication, others, such as sensor networks, logistics and large-scale "real-world awareness" scenarios, will entail huge volumes of data on central network nodes or servers.

* *Data interpretation:* To support the users of smart things, we would want to interpret the local context determined by sensors as accurately as possible. For service providers to profit from the disparate data that will be generated, we would need to be able to draw some generalizable conclusions from the interpreted sensor data. However, generating useful information from raw sensor data that can trigger further action is by no means a trivial undertaking.

**Security and personal privacy:* In addition to the security and protection aspects of the Internet with which we are all familiar (such as communications confidentiality, the authenticity and trustworthiness of communication partners, and message integrity), other requirements would also be important in an Internet of Things. We might want to give things only selective access to certain services, or prevent them from communicating with other things at certain times or in an uncontrolled manner; and business transactions involving smart objects would need to be protected from competitors' prying eyes.

* *Fault tolerance:* The world of things is much more dynamic and mobile than the world of computers, with contexts changing rapidly and in unexpected ways. But we would still want to rely on things functioning properly. Structuring an Internet of Things in a robust and trustworthy manner would require redundancy on several levels and an ability to automatically adapt to changed conditions.

* *Power supply:* Things typically move around and are not connected to a power supply, so their smartness needs to be powered from a self-sufficient energy source. Although passive RFID transponders do not need their own energy source, their functionality and communications range are very limited. In many scenarios, batteries and power packs are problematic due to their size and weight, and especially because of their maintenance requirements. Unfortunately, battery technology is making relatively slow progress, and "energy harvesting", i.e. generating electricity from the environment (using temperature differences, vibrations, air currents, light, etc.), is not yet powerful enough to meet the energy requirements of current electronic systems in many application scenarios. Hopes are pinned on future low-power processors and communications units for embedded systems that can function with significantly less energy. Energy saving is a factor not only in hardware and system architecture, but also in software, for example the implementation of protocol stacks, where every single transmission byte will have to justify its existence. There are already some battery-free wireless sensors that can transmit their readings a distance of a few meters. Like RFID systems, they obtain the power they require either remotely or from the measuring process itself, for example by using piezoelectric or pyroelectric materials for pressure and temperature measurements.

* *Interaction and short-range communications:* Wireless communication over distances of a few centimeters will suffice, for example, if an object is touched by another object or a user holds their mobile against it. Where such short distances are involved, very little power is required, addressing is simplified (as there is often only one possible destination) and there is typically no risk of being overheard by others. NFC is one example of this type of communication. Like RFID, it uses inductive coupling. During communication, one partner is in active mode and the other can be in passive mode. Active NFC units are small enough to be used in mobile phones; passive units are similar to RFID transponders and are significantly smaller, cheaper and do not need their own power source.

* *Wireless communications:* From an energy point of view, established wireless technologies such as GSM, UMTS, Wi-Fi and Bluetooth are far less suitable; more recent WPAN standards such as ZigBee and others still under development may have a narrower bandwidth, but they do use significantly less power.

Wireless technology requirement is the main challenge in IoT.

III. Li-fi

Li-Fi (Light Fidelity) can be thought of as a light-based Wi-Fi. That is, it uses light instead of radio waves to transmit information and instead of Wi-Fi modems, Li-Fi would use transceiver-fitted LED lamps that can light a room as well as transmit and receive information. Since simple light bulbs are used, there can technically be any number of access points [15]. This technology uses a part of the electromagnetic spectrum that is still not greatly utilized- The Visible Spectrum (which is unlicensed) . Light is in fact very much part of our lives for millions and millions of years and does not have any major ill effect. Moreover there is 10,000 times more space available in this spectrum and just counting on the bulbs in use, it also multiplies to 10,000 times more availability as an infrastructure, globally[13]

It is possible to encode data in the light by varying the rate at which the LEDs flicker on and off to give different strings of 1s and 0s. The LED intensity is modulated so rapidly that human eyes cannot notice, so the output appears constant.

More sophisticated techniques could dramatically increase VLC(visible light communication) data rates. Teams at the University of Oxford and the University of Edinburgh are focusing on parallel data transmission using arrays of LEDs, where each LED transmits a different data stream. Other groups are using mixtures of red, green and blue LEDs to alter the light's frequency, with each frequency encoding a different data channe.

Li-Fi has already achieved blisteringly high speeds in the lab. Researchers at the Heinrich Hertz Institute in Berlin, Germany, have reached data rates of over 500 megabytes per second using a standard white-light LED. Haas has set up a spin-off firm to sell a consumer VLC transmitter that is due for launch next year. It is capable of transmitting data at 100 MB/s - faster than most UK broadband connections [13].

Visible light communication is a potential solution to the global wireless spectrum shortage. LiFi is a fast and cheap optical version of Wi-Fi, the technology of which is based on Visible Light Communication .VLC is a data communication medium, which uses visible light between 400 THz (780 nm) and 800 THz (375 nm) as optical carrier for data transmission and illumination. It uses fast pulses of light to transmit information wirelessly. Since it uses visible light rather than radio waves it is eco friendly and cheap[15].

LiFi Can be used in the places like operation theatres in hospitals, traffic signals, aircraft, smart nuclear plants and chemical plants etc figure 2 depicts IOT based on LiFi

Figure 2. IOT using LiFi

LiFi can be a potential solution for low power, high bandwidth requirement of IoT. The main limitation of light waves is that it can not penetrate walls and LiFi has a small range of coverage compared to WiFi. Thus IoT can be deployed using LiFi in local area with Internet as backbone. When IoT is deployed in this way a need for flow control protocol exist to synchronize the speed of LiFi and present Internet which uses comparatively low bandwidth network technology.

IV. FLOW CONTROL PROTOCOL

At present the congestion control is done through TCP using Slow-Start and AIMD (Additive Increase Multiplicative Decrease) Each TCP connection starts with a pre-configured small initial congestion window (no larger than 4 Maximum Segment Size (MSS) [4] and probes the network for available bandwidth using the Slow-Start procedure. Slow-Start increases the congestion window by one MSS for each new acknowledgment received, which results in the window doubling after each window's worth of data is acknowledged. A connection enters Slow-Start on newly starting or on experiencing a packet retransmission timeout, and exits Slow-Start when it detects a packet loss or when the congestion window has reached a dynamically computed threshold, ssthresh. Which is set to half of the current congestion window when packet loss was detected.

TCP exits Slow-Start to enter the Congestion Avoidance phase, where it continues to probe for available bandwidth. During periods when no packet losses are observed, TCP performs an Additive Increase of the window size, by 1 MSS each time a full window is acknowledged and decreases window size by half when congestion is detected[14] The reaction to congestion indication (packet loss) varies across different flavors of TCP as follows:

♦ *TCP Tahoe*: Tahoe congestion control was introduced by Van Jacobson in 1987. A Tahoe sender records the ssthresh as cwnd 2 value (the initial value of ssthresh is usually set to the receiver window size), sets cwnd to 1 MSS and enters Slow-Start, in response to a series of "congestion collapse" events (a state where the network is live-locked, performing little useful work) or on detecting a packet loss (either through retransmission timeout or three duplicate acknowledgment packets), It continues Slow-Start so long as cwnd < ssthresh, and is in Congestion Avoidance beyond that [5].

a) ♦ *TCP Reno:* This is the second version which differs from TCP Tahoe when detecting packet loss through three duplicate acknowledgment packets (an indication of a milder congestion). TCP Reno reduces the cwnd by half (as opposed to reducing the window to one like in Tahoe) to achieve a higher sending rate after loss recovery. The procedure implementing this is called Fast Recovery. Also whenever 3 duplicate ACKs are received a segment is transmitted without waiting for time out this procedure is called 'Fast-Re-Transmit [6].

♦ *TCP NewReno:* NewReno also reduces cwnd by half on detecting a packet loss through three duplicate acknowledgments, but NewReno improves upon Reno when retransmitting multiple packet losses. Reno fails to recover efficiently from multiple packet losses in a window. After transmitting the first lost segment, it typically waits for the retransmit timer to expire, in order to recover the remaining lost segments. When a received acknowledgment does not acknowledge all outstanding segments, NewReno retransmits the missing segment [7].

♦ *TCP SACK:* A TCP extension called Selective Acknowledgment improves further on NewReno's retransmission mechanisms. SACK allows the receiver to indicate up to four non-contiguous blocks of sequence numbers received correctly, thus allowing the sender to retransmit lost data more efficiently. This is currently the most widespread TCP version in the Internet [11].

There are other flow control protocols such as STCP [8] and fast TCP [9] which are designed for high bandwidth wide area netwoks but they work well for long flows but not for short flows

There exists many flow control protocols which are based on explicit feedback from the network to minimize flow completion time such as:

♦ *XCP:* XCP (Explicit Control protocol) works by involving the routers in congestion control. The network explicitly tells the receiver the state of congestion and how to react to it. This allows senders to adjust their windows based on the precise feedback information [10].

♦ *RCP:* RCP (Rate Control Protocol) involves explicit feedback from routers along the path. Here a router maintains a single rate, R(t), for every link. The router “stamps” R(t) on every passing packet (unless it already carries a slower value). The receiver sends the value back to the sender so that it knows the slowest (or bottleneck) rate along the path. In this way, the sender quickly finds out the rate it should be using (without the need for slow-start). The router updates R(t) approximately once per roundtrip time (RTT), and strives to emulate processor sharing among flows [11].

♦ *Three level ECN :* three-level ECN (Explicit congestion notification scheme aggravates TCP over wireless links. Using three-level ECN as the congestion feedback mechanism and the “congestion coherence” in consecutive packets, this scheme avoids majority of end-to-end retransmissions, unnecessary slowdowns and timeouts caused by wireless errors and hence improves the performance of TCP over wireless links [12].

All these protocols are designed for Internet with homogeneous environment. No flow control protocol has been designed for IoT where “things” are connected using LiFi which has very high bandwidth and want to access Internet which has comparatively very low bandwidth constituting heterogeneous environment.

V. Conclusion

The future of IOT lies in meeting its requirements and thus the paper provides an idea to use LiFi for the high bandwidth requirement of IOT and also emphasize on the need to identify an appropriate flow control protocol when IoT uses LiFi.

Acknowledgment

We acknowledge the support of the National Institute of Engineering in the completion of this work and also acknowledge authors whose paper has been referenced

References

[1] Charith Perera, Arkady Zaslavsky, Chi Harold Liu, Michael Compton, Peter Christen, and Dimitrios eorgakopoulos, “Sensor Search Techniques for Sensing as a Service Architecture for the Internet of Things”, IEEE SENSORS JOURNAL, VOL. 14, Feb 2014.

[2] L. Atzori, A. Iera, and G. Morabito, “The Internet of things: a survey”, Computer Networks, vol. 54, no. 15, pp. 2787-2805, 2010.

[3] Friedemann Mattern and Christian Floerkemeier ,“From the Internet of Computers to the Internet of Things” Informatik- Spektrum 33 (2): 107–121. Retrieved 3 February 2014.

[4] M. Allman, S. Floyd and C. Partridge, “Increasing TCP’s Initial Window,” RFC 3390 , Oct 2002.

[5] V. Jacobson, “Congestion Avoidance and Control,” SIGCOMM Symposium on Communications Architectures and Protocols , pages 314-329, 1988.

[6] V.Jacobson “Modified TCP Congestion Control and Avoidance Alogrithms”.Technical Report 30,Apr 1990.

[7] S.Floyd, T.Henderson “The New- Reno Modification to TCP’s Fast Recovery Algorithm” RFC 2582, Apr 1999.

[8] T. Kelly, “Scalable TCP: improving performance in highspeed wide area networks,” Comput. Commun. Rev. vol. 32, no. 2, Apr. 2003.

[9] C. Jin, D. X. Wei, S. H. Low, “FAST TCP: Motivation, Archi tecture, Algorithms, Performance,” Proceedings of IEEE Infocom 2004, Hong Kong, Mar 2004.

[10] D. Katabi, M. Handley, C. Rohrs, “Internet Congestion Control for High Bandwidth-Delay Product Networks,” Proceedings of ACM Sigcomm , Pittsburgh, Aug 2002.

[11] Nandita Dukkipati: “Rate Control Protocol (RCP): Congestion Control to Make Flows Complete Quickly”, phd thesis university of Stanford, Oct 2007.

[12] Mohammad Usman Ali Khan, Shahid Khan, Yasir Ali Rasheed, “Optimization of TCP over Wireless Networks” , International Journal of Electrical & Computer Sciences IJECS-IJENS,Oct 2011.

[13] Haas, Herald "Wireless data from every light bulb",TED Global. Edinburgh, Scotland, Jul 2011

[14] Larry L. Peterson and Bruce S. Davie,” Computer Networks – A Systems Approach” , 4th Edition, Elsevier, 2007

[15] www.lificonsortium.org/