Social Web of Things: A Survey

[a,*]Tein-Yaw Chung, [a]Ibrahim Mashal, [a]Osama Alsaryrah, [a]Van Huy, [b]Wen-Hsing Kuo and [c]DHARMA P. AGRAWAL

[a] Department of Computer Science and Engineering, Yuan Ze University, Taoyuan, Taiwan

[b] Department of Electrical Engineering, Yuan Ze University, Taoyuan, Taiwan

[c] OBR Research Center for Distributed and Mobile Computing, ECECS Department, University of Cincinnati, Cincinnati, OH 45221-0030, USA

*csdchung@saturn.yzu.edu.tw

***Abstract*— Recently, Wireless Sensor Networks (WSNs) are spread all over the world, and are commonly used to collect physical information from the surrounding world. WSNs play a central role in the Internet of Things (IoT) vision. IoT is a new paradigm that aims to integrate and connect anything at anytime, anyplace, with anything and by anyone. However, addressing objects is the main challenge for IoT. IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) has been introduced to cope with this issue. The emerging paradigm Social web of thing (SWoT) enables users to manage, access, share, and integrate smart objects with Social Network Site (SNS). This paper investigates different SWoT platforms and architectures, provides an overview of the current state-of-the-art on WSN communication standards.**

Keywords*— Internet Of Things; IPv6 over Low-power Personal Area Networks; Social Web of Things; Web of Things; Wireless Sensor Network; ZigBee.

I. Introduction

Today, wireless sensor networks (WSNs) are commonly being used and deployed in many locations for different applications. WSN consists of thousands of small, power-limited, inexpensive, and limited processing power sensor devices, which collect data for indefinite period of time[1-2]. WSN applications range from military applications to health-care monitoring, environmental observation, structural and industrial monitoring, remote monitoring, control networks, habitat monitoring, surveillance, tracking, and many others [3-4].

In a WSN, sensors connect with each other using wireless proprietary protocols, such as, Bluetooth or Zigbee. However, the main challenge is establishing a connection between sensors and the Internet. Nowadays, this communication is feasible due to IPv6 over Low-power Personal Area Networks (6LoWPANs). Sensors, actuators, and RFID are key components of Internet-of-Things (IoT) [5-7] and have created an important new trend in pervasive computing. A generic vision of IoT is to interconnect smart devices and objects anytime and anywhere throughout the world.

IoT has given rise to Web of things (WoT). While the IoT addresses the mechanisms to connect smart objects, the WoT addresses the integration of embedded systems into the Web. Currently, Social Web of Things (SWoT) can be considered as a convergence paradigm of Social Network Sites (SNS) and WoT. The concept is to bring SNS services and features, such as social graphs into an integrated system.

The rest of the paper is organized as follows. Section II presents commonly used WNS communication standards. Section III illustrates SNS architectures and describes underlying functionalities and basic elements. Section IV describes both IoT and WoT and presents major differences between them. SWoT is presented in in section V and different platforms and architectures are also discussed. Finally, Section VI concludes the paper.

MACHINE TO MACHINE INTEGRATION

Currently, WSN have become popular in home and building automation (HBA). Many terms like Smart Homes, intelligent buildings, integrated home systems are used to refer to the same concept. HBA goes beyond turning devices on and off. The goal of HBA is to enable smart objects communicate with each other and transport information between them so as to control and monitor the environment.

HBA allows leveraging emerging machine-to-machine (M2M) technologies in performing large scale automation. As M2M devices communicate with each other without any or with limited human intervention, this is called machine-type-communication (MTC). Nowadays, M2M has become the main pattern of Internet of Things (IoT) which envisions interconnection of all smart objects across the whole world anytime and anywhere. Objects could include computers, mobile phones, tablets, RFID tags, and sensors. In order to get most of WSNs, they must share and exchange sensed data. In other words, different WSNs must interact with each other and with the Internet. Sensors connect to each other using communication protocols such as Bluetooth, 802.15.4, Zigbee, etc. These protocols have been designed for low data rate with low power consumption.

To connect objects to the Internet and form a heterogeneous network, all objects must have a unique Internet protocol (IP) address. The integration of IP-enabled devices is a big challenge of IoT. Originally, using IP protocol in low power and resource-constrained objects was not considered, because IP is heavy for these tiny devices. Thanks to IPv6 over Low-power Personal Area Networks (6LoWPANs), it is possible now to realize IoT and M2M. In this section, we describe several WSN communication standards.

IEEE 802.15.1 – Bluetooth: Bluetooth IEEE 802.15.1 is a short-range, low power consuming communication protocol used in Wireless Personal Area Networks (WPAN). Bluetooth is widely used in cellular phone, PDAs, printer, digital camera, headsets, PC keyboards, mice, and many other devices. Bluetooth is popular for voice, data, and audio applications for limited distance of 10 meters. However, Bluetooth data rate range from 1 to 3 Mbps. Bluetooth uses a frequency hopping spread-spectrum technology. It operates in the unlicensed 2.4 GHz Industrial Scientific Medicine (ISM) band. Bluetooth devices can be either a master or up to 7 slaves where slaves can communicate only with their master. Bluetooth devices are connected dynamically and form self-organizing wireless ad-hoc networks. Before data can be exchanged, a connection between master and slaves must be established.

Bluetooth specification includes both link layer and application layer definitions. The foundation is the media access control (MAC) (L2CAP, LMP, and baseband) and the physical layer (PHY) radio. The Bluetooth protocol stack supports IP addressing and therefore design of Bluetooth restricts its performance and limits its applicability to WSN. Bluetooth works well for a limited number of nodes and a Piconet with up to seven slaves with a master can be simultaneously established and maintained.

In 2011, low energy (BLE) Bluetooth technology was launched to support ultra-low power communication. Unlike classical Bluetooth, BLE is a connectionless protocol; it does not need to establish a connection before data transmission, and thus decreases power consumption. BLE consumes 10-20 times less power and is able to transmit data 50 times quicker than a classical Bluetooth.

IEEE 802.15.3a – Ultra-Wide Band (UWB): is a short-range high-speed wireless communication technology for an indoor environment. It was developed for extremely high data rates applications, such as, multimedia applications. UWB bandwidth ranges from 110 Mbps up to 480 Mbps for a distance of about 10 m. UWB signals use the spectrum from 3.1 GHz to 10.6 GHz [8]. UWB characteristics include low-power consumption, low complexity, low cost, good localization and tracking, good security, and multipath environments. The main drawback of UWB that it is no more supported since IEEE 802.15.3a task group was dissolved in 2006.

IEEE 802.15.4: is standard for low rate wireless personal area networks (LRWPAN) [9]. 802.15.4 was designed for low data-rate, low-duty short range communication applications. The IEEE 802.15.4 standard defines the PHY layer and MAC sub-layer protocols for the WPAN. Physical layer supports 27 channels spread across three different free license ISM frequency bands: 868 MHz with data rates of 20 kbps, 915 MHz with 40 kbps, and 2.40 GHz with 250 kbps. Maximum frame size is 127 bytes. Coverage distance for IEEE 802.15.4 is about 10 m to 100 m. Within IEEE 802.15.4 network, a device can have either a 64-bit address or a 16-bit short IEEE address. In other word, a PAN can supports up to 64,000 nodes.

The MAC layer uses carrier sense multiple access with collision avoidance (CSMA/CA) mechanism to manage channel access. Guaranteed time slot (GTS) is another mechanism supported by the MAC which provides fixed communication slots to devices. The MAC is also responsible for beacon generation, synchronization and security mechanisms.

The standard allows two types of topologies star topology and peer-to-peer topology. In star topology, devices communicate with a central coordinator. In peer-to-pee topology, each device is able to communicate directly with peer devices in an ad hoc manner. IEEE 802.15.4 defines two types of device. Full Function Device (FFD) and Reduced Function Device (RFD). FFD devices are more complex since it supports all network functionalities and multi-hop communication, and thus, can be used in a peer-to-peer topology. Only FFD devices can be a PAN coordinator and they can talk to both FFD and RFD. RFD support partial network functionalities, and do not support multi-hop communications. RFD is intended for simple applications that require infrequently communicate. RFD is implemented using minimal resources and memory capacity. An RFD can be associated with a single FFD at a time and they cannot talk to an RFD. Several efforts have been made to employ 802.15.4. Next paragraphs describe ZigBee and 6LOWPAN.

ZigBee: As mentioned earlier, IEEE 802.15.4 only defines the physical and MAC layers. Many upper layer protocols were proposed. However, The ZigBee is the most popular one. ZigBee was developed by ZigBee Alliance for low-data rate and short-range applications. ZigBee devices use very low power and battery operated for long life time. ZigBee devices use two addresses, the unique 64 bit physical address and 16 bit short address. Short address is used to reduce packet size and to route packets within the network. ZigBee defines the upper layers, namely, the network layer (NWK) and application layer (APL).

The NWK layer is responsible for addressing, routing, both discovery and maintenance, processing and transmitting packets, and forming and building ZigBee network, in addition to security. Thousands of ZigBee devices can form mesh networks. Mesh topology is more complicate and robust than other topologies because of the redundant routes between two nodes. To establish and select a route when old routes are absolute ad hoc on-demand distance vector (AODV) routing protocol is used. The ZigBee also allows tree and star topologies. In a star topology all communications between end devices have to go through the coordinator. All these topologies must include a coordinator device. ZigBee coordinator is a device responsible for forming, managing, and maintaining the Zigbee network, in addition to store information.

Besides to coordinator, Zigbee defines another two types of devices, namely, ZigBee routers and ZigBee end device. Devices are grouped together by ZigBee routers, it also provide multi-hop communication across devices using a routing. ZigBee end device which collect data, is only able to communicate with the router or the coordinator. FFD or RFD can be used as the end device, while, Only FFD can be used by the coordinator and the router.

APL layer adds services discovery and application protocol profiles. It consists of Application Support Sub-layer (APS), Application Framework (AF), ZigBee Device Object (ZDO), the ZigBee device profile (ZDP). APS provides services to interface the NWK layer to AF and ZDO. ZDO provides an interface to the user as it initializes APS and NWK. AF provides an environment for the application object.

6LoWPAN: Neither IEEE 802.15.4 nor ZigBee can support direct interworking with an IP network. A simple solution is to use IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) which is a specification that supports IPv6 communication over the IEEE 802.15.4 network [10]. It is intended for low data rate, short range, low power, low memory usage and low cost applications. 6LoWPAN stack consists of IEEE 802.15.4 PHY and MAC layers, adaptation layer, network layer, transport layer and application layer.

The 6LoWPAN supports two kinds of routing, namely, mesh-under and route-over. The difference between both is how and where packets are forwarded. Mesh-under routing occurs in the 6LoWPAN adaptation layer, while route-over routing occurs in the 6LoWPAN network layer.

The 6LoWPAN standard allows sensor devices to be addressable using IPv6 addresses. The communication between 6LoWPAN sensors and IP-enabled device is quite simple. Sensor sends its data to a router, which in turn forward it to 6LoWPAN gateway. When routing data is inside WSN, there is no need to send full IP addresses, thereby reducing the overhead. The 6LoWPAN gateway uses the destination IP address to forward packets to the destination. Communication from IP-enabled device to 6LoWPAN sensors is done in the same manner. However, IP-enabled device must know IP addresses of the destination sensor.

In order to support IPv6, 6LoWPAN standard adds adaptation layer between data link and network layers. The main responsibility of the adaptation layer is fragmentation and reassembly of packets. The 1280 bytes IPv6 packet is much larger than the IEEE 802.15.4 frame which is 102 bytes of payload or 81 bytes when consider Link Layer security header. In other word, IPv6 packet that needs to be transmitted is unable to be encapsulated in one IEEE 802.15.4 frame and has to be divided into a number of fragments. Another problem adaptation layer has to deal with is address management. Despite the huge address space provided by the IPv6, it is not designed to be used on sensors.

By using 6LOWPAN, it is now possible to integrate WSNs with heterogeneous IPv6 networks. However, implementing network layer protocol is complicated and difficult. Moreover, 6LOWPAN cannot be applied to WSN using other communication protocol, such as ZigBee protocol, since they are not compatible. 6LoWPAN is still not standardized yet.

Z-Wave: is a wireless communications protocol designed especially for home automation [11]. It uses low-power radio waves around 900 MHz ISM bands and operates at data rate of 9.6 kbps. Nowadays, Z-Wave supports the 2.4 GHz and 200 kbps bit rates. A single network may contain up to 232 devices. Z-Wave protocol stack composed of five layers: the PHY, MAC, transfer, routing, and application layers. Two types of devices are defined in Z-Wave. Controllers send commands to the slaves which execute commands and reply to the controllers.

The Z-Wave performs routing by using source routing approach. In order to be aware of the network topology, controller maintains a table that represents full topology of the network. When a controller transmits a packet, it requests the path from the table and includes it in the packet. Slave which performs the roll of a router, forward the packet from one device to another towards the destination. The main drawback of Z-Wave is that it is susceptible to interference, since Z-Wave devices use the same RF channel with the same frequency. This may limit the spread of Z-Wave.

X10: All standards mentioned before are wireless standards. However, M2M is built on both wireless and wired systems, and the most known home automation protocol, X10, is wired. X10 is a standard home automation communication protocol which uses existing power line. X-10 is able to address up to 256 unique devices. X10 is inexpensive since no additional cabling is required, easy to use, widely deployed specially in North America. However, X10 possess a number of drawbacks. Firstly, X10 devices installation locations are limited since they are plugged into the power outlets. Secondly, nearby devices signals may interfere and may get lost.

II. SOCIAL NETWORK PLATFORM

Social Network Sites (SNSs) are online platforms that help individuals publish, collaborate and share information and experiences with other individuals or groups on that same network, and build social relationships with them. SNSs are emerging area of Web 2.0, where content and information are provided by the users. However, SNSs vary greatly in their features and user base.

SixDegrees.com is the first recognizable social network site launched in 1997, since that, SNSs have passed through number of development waves and they are constantly evolving. As the popularity of SNS has grown, many organizations start using it to facilitate its job in sales, marketing, research, and customer service. Today, numerous SNS are available such as Facebook, Flickr, Google+, MySpace, Twitter, Friendster, Orkut, YouTube, and LinkedIn are popular social networking sites.

When users join a SNS, they create and publish profiles and relevant content. Users can also create and maintain social relationships to other users with whom they associate or share common interests. Moreover, they can view and traverse other user's relationships. The knowledge about the relationship is used to improve efficiency and effectiveness of SNS. SNSs are free and powerful means of communication. Individuals can stay in touch with each other using communication services like emails, chats, instant messaging. To understand SNS, basic elements are presented in the following paragraphs.

Social actors: Actors are social entities. People or users are the most obvious example of actors. Users must register with SNS and provide some information to complete registration. This information is added to the user's profile. However, some sites allow browsing of some data without sign-up. To extend coverage to other entities, SNS support other collective social entities, such as corporations, organizations, institutes, or even events [12-13]. Most sites enable users to create and join special interest groups. Users can post messages to groups and upload shared content to the group [14].

Profiles: Profiles are the backbone of SNS [15]. Profiles are unique pages created using answers to questions asked to users when they join a SNS. In another word, profiles are self-expression. Profiles include user personal details, such as, name, age, location, interests, hobbies, personal achievements, pictures. This profile information is shared among the users. Users must determine how they want to present themselves and who may view their profile. Profiles visibility and accessibility vary among different SNSs and user discretion [17].

Social Relations: After the user join a SNS, users identify who they wish to connect with or establish some kind of relations with different users. This is done by maintaining links to other users sharing same interest. This is a core feature for every SNS. Some SNS maintain groups of users with same interests, so users can join these groups rather than creating links to individual users. SNSs support different types of relations. Unidirectional relations do not need confirmation or consent from the target user. For example, Follow is a popular case of unidirectional relation. On contrast, bidirectional relations need confirmation from both users before creating the link. Users must be able to organize and manage their contacts, this feature is contacts management. Contact management settings can also be used to grant permissions to certain groups of contacts at the same time. A related concept is a tie [16]. A tie is the set that aggregates all different types of relations that exist between two internet identities. A tie provides more comprehensive and coherent view on users' interactions.

Communication tools: SNSs provide communication tools and technologies to exchange messages between users. An important feature is commenting feature that display conversations on a user's profile. SNSs also have a private messaging feature, chat, video-conferences and system notifications. System notification is used by the system to alert users of some types of events. New communication tools were developed by SNSs to allow users to post a short message sharing what they think, do or how they are feel. This is called the status update.

Content: SNSs do more than just allow user to have a profile and a social relations and it allow users to share information. SNSs support different types of content, such as, text comments, pictures, videos, events and external links to other sites. Text comments are the most basic type. The more types of content SNSs support, the more channels actors have to interact between them.

Other features SNSs support: More recent actions performed as an activities timeline are organized and ordered in activities timeline as one or several actors. It helps users to be aware of the activities and actions of other users, and have a sense of what is happening in the social network. They can appear in several parts of the site. Home page is another feature in SNSs where actors can access more relevant information in the SNS. User can post, add, or create new content to his own profile or to other actor in the SNS using a Wall.

Despite all the advantages of SNSs, users are bound to a given SNS and it is hard to migrate to another SNS. Interoperability between platforms is very limited, when users modify data on one SNS as they have to update the data on every SNS, otherwise diverse information will be present. Another problem with SNS is losing control over user's personal information and data once they have published it.

OpenSocial is a set of common application programming interfaces (APIs) for building social applications that run on the web. It defines specifications to build applications that run on different multiple SNS, using the data stored by that SNS. The goal of OpenSocial is to enable SNS share their data to be accessed on the web from anywhere. It was developed by Google along with MySpace and a number of other social networks. Gadgets can be developed to run on websites that have implemented the OpenSocial APIs. Open Social's API is based entirely on HTML and JavaScript. Some web sites currently using OpenSocial include Friendster, hi5, iGoogle, Yahoo, LinkedIn, MySpace, Orkut, Salesforce.com.

III. INTERNET AND WEB OF THINGS (IOT) AND (WOT)

Currently, Internet is the most important elements in our daily life. Millions of users use Internet to browse the web, play games, and use SNS and applications all over the world. This global platform is capable of providing an interconnection between machines and objects in order to create smart environments, leading to IoT paradigm.

The vision of IoT is enabling things to be connected anytime, anyplace, with anything, and anyone using any network and any service. The term IoT was first used in 1999. However, there is still no standard definition of IoT [18] [19]. We understand the IoT as the use of world-wide network to provide an interconnection between smart objects, which are enabled by various technologies, such as, RFID, wireless sensor to provide a new services and applications.

The IoT only focuses on networking layer and to establish connections between physical world objects, giving them a transport capability. In contrast, Web of Things (WoT) only focuses on application layer. WoT attempts to reuse and adapts existing web technologies to build new applications and services. In other words, WoT is integrating smart objects to become a part of the web and make them available as resources via standard web mechanism [20].

In order to integrate smart objects with the web, smart objects must be first connected to the Internet using specified addresses. Then, objects have to understand the web language by adding web server or web service interface to the objects (web enabled objects). There are two types of integration: the first one being an direct object integrated with the web by making the object addressable and embedded in a web server on it. The Second type deals with objects that cannot be web enabled, such as RFID. In this case a proxy server or a smart gateway must be implemented.

IV. SOCIAL WEB OF THINGS (SWOT)

The Social web of things paradigm enables users to manage and access web-enabled devices and give the user an ability to share these devices with other users [21]. SNS increase the popularity of Web 2.0 technology, it enables users to communicate and exchange contents between each other, and SNS has been extended by an interactive and open web services in the recent years. These web services can extend the social relation between people to relation between them and their web enabled devices [22].

In our research, we reviewed a number of proposed platforms and architectures which aim to share smart object data and make them usable by SNS or using some of offered features by SNS. In the next few paragraphs, we provide an overview of what has already been done by researchers to integrate SNS with smart objects.

A system is proposed in [23] that allow users to share their sensor data by offering REST API which make the recorded data of smart objects available for any other web application. This system uses a SNS open API authentication services. In this approach, the sensors sent data directly to a web server which processes this data and share the user's preferred information.

Another example is presented in [24] where the researchers proposed architecture to integrate body sensor networks (BSNs) and social networks through an IP multimedia subsystem (IMS), where Authorized social network members can monitor real-time BSN data of other users.

Another system called SenseFace [25] integrates BSN with SNS. SenseFace consist of a four-tier network that passes sensory data from a mobile BSN to a cellular network, and then to the Internet and finally to the overlay network which produce different data visualization formats suitable for existing social networks such as Facebook.

In [26], web enabled objects communicates with SNS through the API provided by the SNS itself, each object and the service is associated with its own dedicated SNS where the sensory data will be published, e.g., Twitter as proposed.

As another example, application called SenseShare [27], use Facebook API's and make it as main front end user interface. SenseShare use authentication, privacy, and security setting offered by SNS to select who can see information we want to share.

Social Access Controller (SAC) [28] is another example of integrating smart object with SNS. SAC is an application responsible for creating a link between web enabled devices and SNS through RESTful Web API. It works as an authentication and a proxy sharing component for web enabled object and manage the access control to the SNS. Figure 1 shows the architecture of SAC.

Similar to SAC system, another system is proposed in [29] to share smart home data through social network. The system connect the web enabled devices to Web server or a RESTful gateway, a Web server hosts the Web application which enables the Smart Home to be integrated to the SNS using Web-based APIs which are mostly REST-based.

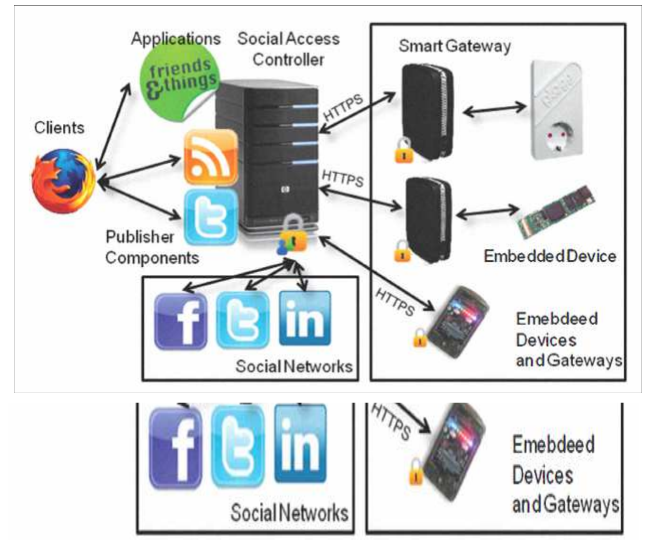

Figure 1: SAC General Architecture

WoT make things accessible and usable as web resources and make it able to work with web 2.0 technologies. In order to reach convergence and to have integration between physical objects and social networks, a few elements and concepts must be considered. Researchers in [22] have defined those elements. The first element is the availability of Open Web API to access the internal structures of SNS. The second element is the SNS must allow building Applications through the provided open API. The third element is availability of the Web-enabled Physical Device to make it accessible by SNS. Using Web Services is the fourth element for the physical and SNS convergence.

Integration between SNS and physical objects under Web of Things can occur by using some of the SNS features. SNS can be used as authentication server, monitoring tools, or a place to share smart objects data. For authentication, SNS credentials can be used to login to WoT servers. SNS support using Oauth protocol which allows a user to use their SNS credentials to login other sites. To use SNS as a monitoring tool, WoT allows web enabled objects to be connected to the WoT system, and then create dashboard visualizations as Facebook applications which allow users to share and monitor the smart object data.

V. CONCLUSION

In this paper, we have summarized an overview of available WSN standards and protocols. 6LOWPAN is considered a better solution for connecting WSN with IP networks. However, X10 protocol is inexpensive since it uses existing power line. SNS is discussed in details to cover its main features. WoT aims to integrate Web-enabled objects. Indeed, socializing WoT is a recent trend in computing and is called SWoT. We defined SWoT and introduce it basic elements. Different SWoT architectures and frameworks have also been presented in the paper.

ACKNOWLEDGMENT

This work was supported by the Industrial Technology Research Institute (ITRI) Taiwan, R.O.C.

REFERENCES

[1] Neha Jain and Dharma P. Agrawal, “Current Trends in Wireless Sensor Network Design,” *International Journal of Distributed Sensor Networks*, Taylor & Francis Publishers, vol. 1, no. 1, 2005, pp. 101-122.

[2] Yick, Jennifer, Biswanath Mukherjee, and Dipak Ghosal. “Wireless sensor network survey,” *Computer networks*, 52.12 (2008): 2292-2330.

[3] L. M. L. Oliveira and J. J. P. C. Rodrigues, “Wireless Sensor Networks: a Survey on Environmental Monitoring,” *Journal of Communications (JCM)*, Academy Publisher, Vol 6, No 2, pp. 143-151, April 2011.

[4] Ning Xu, “A survey of sensor network applications,” *IEEE Communications Magazine*, 40.8 (2002): 102-114.

[5] Delphine Christin, Andreas Reinhardt, Parag S. Mogre, and Ralf Steinmetz, “Wireless sensor networks and the Internet of Things: Selected challenges,” *Proceedings of the 8th GI/ITG KuVS Fachgespräch Drahtlose Sensornetze* (2009): 31-34.

[6] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Future Generation Computer Systems*, (2013).

[7] L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” *Computer Networks*, 54, 15 (2010), 2787–2805.

[8] Ian F. Akyildiz, Tommaso Melodia, and Kaushik R. Chowdhury. “A survey on wireless multimedia sensor networks,” *Computer networks*, 51.4 (2007): 921-960.

[9] J. T. Adams, “An introduction to IEEE STD 802.15.4,” 2006 IEEE Aerospace Conference, pp. 8, doi: 10.1109/AERO.2006.1655947

[10] G. Mulligan, “The 6LoWPAN architecture,” *in Proceedings of the 4th Workshop on Embedded Networked Sensors,* (EmNets ’07), pp. 78–82, June 2007.

[11] Gomez, Carles, and Josep Paradells, “Wireless home automation networks: A survey of architectures and technologies,” *Communications Magazine*, IEEE 48.6 (2010): 92-101.

[12] Antonio Tapiador and Diego Carrera. “A survey on social network sites' functional features,” *arXiv preprint* arXiv:1209.3650 (2012).

[13] A. Tapiador, D. Carrera, and J. Salvachua, “Social Stream, a social network framework,” *Future Generation Communication Technology (FGCT)*, 2012 International Conference on , vol., no., pp.52,57, 12-14 Dec. 2012 doi: 10.1109/FGCT.2012.6476557

[14] Alan Mislove, Massimiliano Marcon, Krishna P. Gummadi, Peter Druschel, and Bobby Bhattacharjee, “Measurement and analysis of online social networks,” *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, ACM, 2007.

[15] Nicole B. Ellison, “Social network sites: Definition, history, andscholarship,” *Journal of Computer‐Mediated Communication*, 13.1 (2007): 210-230.

[16] Katarzyna Musiał and Przemysław Kazienko, “Social networks on the internet,” *World Wide Web* 16.1 (2013): 31-72.

[17] Danah Boyd, “Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications,” *In Networked Self: Identity, Community, and Culture on Social Network Sites* (ed. Zizi Papacharissi), (2010), pp. 39-58.

[18] *The Internet of Things 2012 - New Horizons*, (European Research Cluster on the Internet of Things) IERC Books.

[19] Lu Tan, and Neng Wang, “Future internet: The Internet of Things,” *International Conference on Advanced Computer Theory and Engineering (ICACTE*), 2010, 3rd, vol. 5, pp. V5376-V5380, 20-22 Aug. 2010

[20] D. Guinard, V. Trifa, and E. Wilde, “A resource oriented architecture for the Web of Things,” *Internet of Things (IOT)*, 2010 , vol., no., pp.1,8, Nov. 29 2010-Dec. 1 2010

[21] Andrei Ciortea, Olivier Boissier, Antoine Zimmermann, and Adina Magda Florea, “Reconsidering the social web of things,” position paper. *In Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication* (UbiComp '13 Adjunct), 2013.

[22] A. Kamilaris, D. Papadiomidous, and A. Pitsillides, “Lessons Learned from Online Social Networking of Physical Things,” *2011 International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA*), pp.128,135, 26-28 Oct. 2011

[23] M. Shoaib, W.-C. Song, R. Ahamd, and D.-H. Kim, “Architecture of Push Service Based on SNS for Sharing Sensor Information,” in *Green and Smart Technology with Sensor Applications*, vol. 338, H.-s. Cho, T.-h. Kim, S. Mohammed, H. Adeli, M.-k. Oh, and K.-W. Lee, Eds., ed: Springer Berlin Heidelberg, 2012, pp. 342-346.

[24] M. C. Domingo, “A context-aware service architecture for the integration of body sensor networks and social networks through the IP multimedia subsystem,” *IEEE Communications Magazine*, vol. 49, no. 1, pp. 102-108, January 2011

[25] M. A. Rahman, A. El-Saddik, and W. Gueaieb, “Data visualization: From body sensor network to social networks,” *IEEE International Workshop on Robotic and Sensors Environments*, 2009, ROSE 2009, pp.157-162, 6-7 Nov. 2009

[26] M. Baqer, “Enabling collaboration and coordination of wireless sensor networks via social networks,” *6th IEEE International Conference on Distributed Computing in Sensor Systems Workshops (DCOSSW*), 2010, pp. 1-2, 21-23 June 2010

[27] Exploiting Social Networks for Sensor Data Sharing with SenseShare http://escholarship.org/uc/item/4919w4vh .

[28] D. Guinard, M. Fischer, and V. Trifa, “Sharing using social networks in a composable Web of Things,” *2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops* (PERCOM Workshops), pp. 702-707, March 29, 2010-April 2, 2010.

[29] A. Kamilaris and A. Pitsillides, “Social networking of the Smart Home,” *IEEE 21st International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC*), 2010, pp. 2632-2637, 26-30 Sept. 2010.