Exploration of Existing Frameworks for Connecting Wireless Sensor Networks (WSNs) with Current Internet

Renuka Roselin Kujur
School of Information Technology,
MATS University, Raipur, C.G., India - 493447,

A.K. Dwivedi
School of Information Technology,
MATS University, Raipur, C.G., India - 493447

ABSTRACT

Wireless Sensor Network (WSN) is an emerging area of research and gaining worldwide attraction. Through this work, the objective is to explore all existing and ongoing research works related to connect an emerging network, i.e., Wireless Sensor Networks (WSNs) with existing Current Internet. This paper evaluates different approaches to integrate WSNs into the Internet and outlines few set of challenges. As well as with this exploration, the objective is to provide an educts or conclusion on the most suitable solutions in this regard.

Keywords

Wireless Sensor Network, IP-enabled wireless sensor networks, IP, IPv6, TCP/IP Networks, Internet connectivity on wireless sensor networks.

1. INTRODUCTION

WSNs are rapidly attaining a major significance both in computer science and networking, and in many fields of physical and biological sciences. These WSNs are composed of small, low-power devices with extremely limited computation capability, memory space and communication means, such networks clearly differ from the more familiar networks. Several important questions still remain, however: How should sensor networks be integrated into, and addressed from, the wider, future internet? And what special challenges do they present to designers and implementers? This paper presents some views on these questions. Wireless sensor networks are constructed with various hardware sensors based on MEMS (Micro-Electro Mechanical System) [1] and NANO technologies, and have been recognized as one of core technologies for the future ubiquitous sensor networks. Because it is possible to recognize, collect, and process the various events that occur in the real life using wireless sensor networks, there will be an increasing demand for the sensor network applications in the present and future ubiquitous environments such as watching the movement of enemies in battlefields, monitoring rainfall and geological conditions, and long-term observation of ecological adaptation. The main goal of a sensor network is to provide sensing facilities to the user or other systems. The Internet has around 1 billion users worldwide, so it makes sense to provide WSN services to this ever-growing community.

2. SENSOR PROTOCOL STACK

A generalized protocol stack for WSNs basically consists of 5 layers. These are as given in the Figure 1.

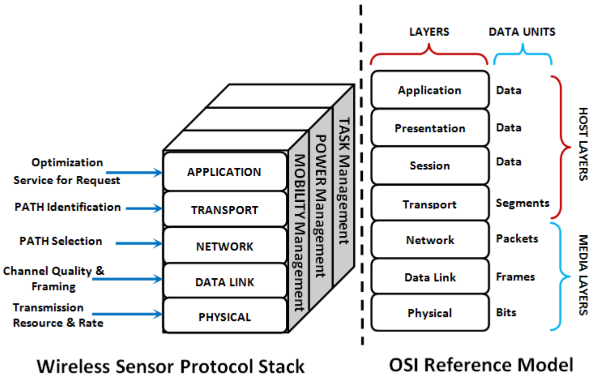


Fig 1: Generalized WSN-Specific Protocol Stack vs. OSI Reference Model [2] [3]

The generalized WSN-specific protocol stack is slightly different from the OSI Reference model. The generalized WSN-specific protocol stack combines the power and routing decisions, integrates data with different networking protocols, lead into power-efficiently through the wireless medium and promotes efforts of sensor nodes. The generalized WSN-specific protocol stack consists of the five layers and some management specific planes like power maintenance, mobility management, and task control. Depending on the sensing tasks, different types of software can be made and used on the application layer. Sensor nodes can be used for continuous sensing, event detection, identification and location sensing. The concept of these wireless connections of sensor nodes promises many new application areas of integrating WSNs with current Internet.

3. CHARACTERISTICS OF WSN

3.1 Data Flow Patterns

The most basic use of sensor networks is to treat each node as an independent data collection device. Periodically, each node in the network sends its readings to a central warehouse/data sink. Alternatively, it is possible to treat sensor networks as essentially distributed databases - users interested in specific information insert a query into the network through a node (or nodes) usually called the sink. This query is transmitted into the network. Then nodes with the data are known as sources in WSN jargon responds with the relevant information. Thus one-to-many and many-to-one data flows dominate the communications in sensor networks. This can be distinguished with the one-to-one addressable flows that are typical of most IP-based networks.

3.2 Energy Constraints

The nodes in unattended large-scale sensor networks are likely to be battery powered, with limited recharging capabilities. Under these conditions, the primary network performance metric of interest is the energy efficiency of operation (a related metric is the lifetime of the network -

measurable in terms of the time when a significant portion of nodes in the network fail due to energy depletion). Typically, communication is significantly more energy-expensive than computation. The Berkeley motes, for example, can process 100 instructions with less energy than the amount needed to transmit a single bit.

3.3 Application-Specific Networking and Data-Centric Routing

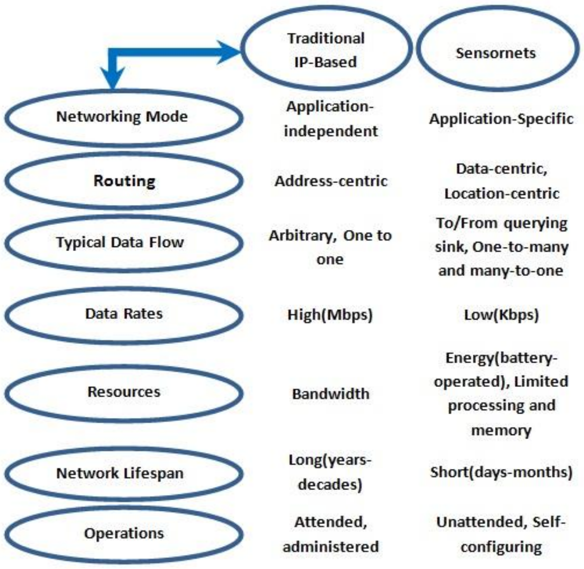
Traditional IP-based networks follow the layering principle which separates the application level concerns from network layer routing. This is essential because of applications are expected to run over a common networking substrate. By contrast, sensor networks are likely to be quite limited in the applications they perform. This calls for cross-layer optimizations and application-specific designs. One design principle that exploits application-specificity to significantly reduce communication energy is the use of in-network processing to filter out irrelevant and redundant information. For example, intermediate nodes may be allowed to look at the application-level content of packets in order to aggregate them with information originating from other sources.

Related to this is the distinction between address-centric and data-centric routing. The Internet was designed around an address-centric ideology, which works when data is usually attached to a specific host. It requires a prior knowledge of which host to contact. Almost all communications (ftp, http, email etc.) in the Internet have this characteristic – it is known *a* priori where the data is located. For this reason, communication on the Internet is usually point-to-point, and this requires the ability to uniquely identify each host through IP addresses.

4. DIFFERENCING TRADITIONAL IP-NETWORK FROM WIRELESS SENSOR NETWORK

In recent years there has been a great surge of interest in SN, which is focused on developing networking architectures. The task of joining WSN to the existing Internet brings with it several challenges. Any network that wishes to be connected to the Internet needs to address the question of how it will interface with the standard protocols like the Internet Protocol (IP). This paper describes the characteristics of WSN that differentiate them from traditional IP-based networks.

The key differences [4] are presented as follows (as given in the Figure 2):



	Traditional IP-Based	Sensornets
Networking Mode	Application-independent	Application-Specific
Routing	Address-centric	Data-centric, Location-centric
Typical Data Flow	Arbitrary, One to one	To/From querying sink, One-to-many and many-to-one
Data Rates	High(Mbps)	Low(Kbps)
Resources	Bandwidth	Energy(battery-operated), Limited processing and memory
Network Lifespan	Long(years-decades)	Short(days-months)
Operations	Attended, administered	Unattended, Self-configuring

Fig 2: Differences between traditional IP-network and WSN

The task of joining WSN to the existing infrastructure i.e. Internet brings with it several experiments [5].WSN are large-scale systems consisting of resource-constrained nodes that are best-suited to application and data-centric routing. Such features form a set of challenges on the interconnection approaches are explained as follow and the following points make differences and can be describes as:

4.1 Limited capabilities of WSN nodes

Sensor nodes have limited abilities in dealing out, computing, memory and most importantly in power intake. As focusing to TCP/IP, energy consumption is an important in WSN protocols.

4.2 Possibility of absence of Global Unique IDs

Sensor Motes do not usually have predefined global unique Identification or addresses as in IP-networks. For example, the Directed Diffusion protocol performs data-centric querying and routing without the use of globally unique IP-like addresses.

4.3 Different Routing Protocols in both networks

WSN basically uses specific routing protocols that are appropriate for it. They are not the same from the Internet protocol. Hence, WSN routing protocols uses addressing systems that are not IP-compliant.

4.4 Data-Centric routing rather than Address-Centric

It is public in WSN to issue a query to many “unknown” nodes by using named data. In associate, the popular of TCP/IP transactions assume prior knowledge of location of data and hence the destination address.

4.5 Data flow pattern

The most common data flow in TCP/IP networks is one-to-one data flow. In WSN, other data flow patterns are very common. For example, a user can issue a query by broadcasting it from sink to some or all sensor nodes (i.e. one-to-many). Yet, retrieving query results takes a different form. This is due to many sensor nodes have the queried information and so send the required results to the sink in many-to-one flow pattern.

5. PROBLEM FORMULATION

Traditionally, Wireless sensor networks (WSNs) are not IP-enabled, but for networking other mechanisms are deployed in the sensor nodes. Hence, their integration into IP-based Wide Area Network (WAN) infrastructures requires the deployment of alternatives at the edge of both networking domains that transform between non-IP communication in the sensor network and IP communication in the Internet (as given in the figure 3).

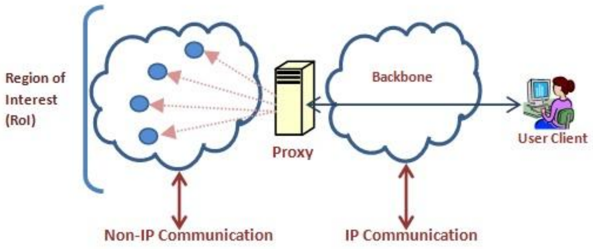


Fig 3: Integration of a Non-IP-Enabled Sensor network in the Internet

Transformation is performed usually at application level. A potential method is an application process in the proxies that make queries to sensor nodes for sensor data via non-IP communication process (e.g. Zigbee) and stores the received sensor data in a local database. The proxy application process could apply aggregation on the data before storage. After that, the user clients in the Internet retrieve the data from the proxy database via TCP/IP. An alternative way would be a proxy process that performs communication protocol transformation, e.g. transformation between IP and Zigbee at network level.

Connecting WSNs to the Internet by way of proxies is not seamless. Proxies break the end-to-end communication accompanied by problems similar to Network Address Translation (NAT) as given in [5]. Therefore, research and standardization activities are emerging [6], [7], [8] that explore and specify IP networking in wireless sensor. WSN with IP support would enable a seamless integration of sensor networks with WAN infrastructures since the IP-enabled sensor network would just be another part of the Internet. It is clear that Gateways would be required and have to be deployed that interconnect WAN infrastructures and wireless sensor nodes but these can function on IP level and are usual routers with at least one WAN interface and at least one interface that supports the link technology of the sensor network, (as given in the figure 4).

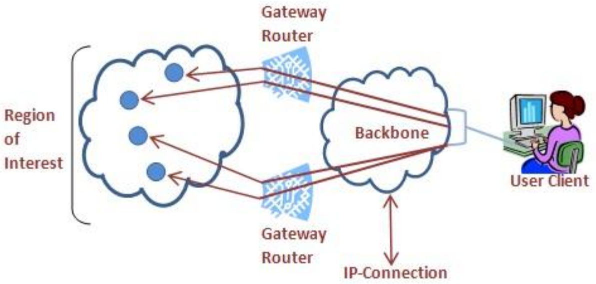


Fig. 4: Integration of IP-enabled Sensor Networks in the Internet

6. IP OVER WSN

This part provides an outline with the motivation and challenges for implementing the IP protocol over Wireless Sensor Network.

6.1 Challenges

There were a number of reasons that supported the idea that IP cannot be used directly at the sensor level, reserving the routing for dedicated protocols. This section provides the main challenges with some discussion.

6.1.1 Header Overhead

IP adds important amount of data on the header block of the packet, introducing undesirable overhead. A lot of energy is spent on wireless communication; this may be a very restrictive factor for the use of IP on the smart sensor node. The least IPv4 header has 20 bytes plus the payload. Further extensions can be used for enlarging the size of the header. IPv6 uses a different tactic, where a fixed 40 bytes header (which is double in IPv4) is used. The header size increases is mostly due to 128-bit addresses instead of 32-bit addresses of IPv4, even though IPv6 header is more elevated, improved and optimized. As a result header overhead may increase. To overcome this problem, header compression technique must be used. The mechanism can be applied to the addresses (by using link-local addresses for instance) or even applying the compression mechanisms defined by the 6LoWPAN specification.

6.1.2 Addressing Scheme

IP addressing method relies on the understanding of the source address and a destination address, and it must be unique inside a given network. Whereas IPv4 can use dynamic host configuration protocol (DHCP) for addressing, it adds for more protocol overhead; while IPv6 provides key mechanism for stateless auto-configuration. In IPv6 the two: unicast and multicast addresses also make it promising to address a group of nodes with a single address. Unicast provides a packet to the nearest interface of the identified group alone, while multicast delivers to the entire network Interfaces of the identified group.

6.1.3 Limited Bandwidth

Small sensors have limited wireless bandwidth; 250kbps is common in IEEE 802.15.4 applications [9], the longer the data transmission will take. With limited bandwidth one do not wants to waste bits overhead problem, even if it is for header, error control, or others. To overcome this, header compression mechanisms can be used.

6.1.4 Limited Energy

One of the different factors of WSNs is the limited energy of the WSN nodes, as motes need to be very small and cost-effective. Wireless Network Communications on the nodes consume the enormous amount of energy, involving both transmitting and receiving of datagrams. In some cases the energy cost of 1 bit transmission corresponds to 1000 processor instructions or more. In many states it is not viable to provide battery charging or battery replacement. Thus, when a sensor node loses its power it dies. Also often when a given number of nodes in a network die, the network concludes to provide sensing amenities, interpreting it unusable. This test is overcome with header compression. The stateless configuration of IPv6 allows the association of an IPv6 link-local address to an interface.

6.1.5 IPv4 or IPv6

IPv4 currently still manages to satisfy the great majority of computer communication needs across the Internet, mainly due to several methods like network address translation (NAT). However, IP addresses are becoming short, so IPv6 rises as a solution. The IPv6 protocol may even aggravate the expected overhead of IP for WSN.

7. CONNECTING WIRELESS SENSOR NETWORK WITH EXISTING ARCHITECTURES

Most of the WSN applications aim at watching, gathering or finding of external/internal phenomenon. Few examples of these are as follows: Building environment monitoring, wild-Life Habitat Monitoring, Forest fire-detection etc. For such kind of applications, the sensor networks cannot function in complete isolation. There must be a way for a monitoring these so as to gain access to the data produced by the sensor network. This can be done by connecting the sensor network to an existing network infrastructure such as a local-area network, the global Internet, or a private intranet, remote access can be achieved to the sensor network. There are three ways suggested to connect sensor networks with existing infrastructure of TCP/IP. These are Proxy Architectures, Delay Tolerant Networks, and TCP/IP for Sensor Networks.

7.1 Proxy Architectures

A very simple way to connect two networks is by deploying a special proxy server between the sensor network and the TCP/IP network. The proxy can operate in either of two ways: as a relay, or as a front-end. In relay, the proxy will simply relay data coming from the sensor network to clients on the TCP/IP network. The user clients must register to a particular data interest with the proxy, and the proxy will then relay data from the sensor network to the registered clients (as given in the Figure 5).

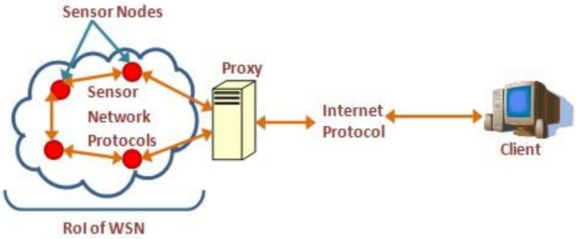


Fig 5: Proxy Architecture

7.1.1 Advantage of Front-End-Proxy

A front-end proxy can also be used to deploy security features such as user and data authentication, the proxy acts as a front-end for the sensor network; it pro-actively collects data from the sensors and stores the information in a database. The clients can query the proxy for specific sensor data through SQL-queries or web-based interfaces. One advantage of the proxy based approach to connect sensor and TCP/IP networks is that the proxy completely decouples the two networks. This naturally allows for specialized communication protocols to be implemented in the sensor network.

7.1.2 Drawbacks of Proxy Approach

Among the drawbacks of the proxy approach are that it creates a single point of failure. If the proxy fails, all the communication to and from the sensor nets is impossible. One solution would be to deploy redundancy in the form of a set of back-up proxies. Such a solution decreases the simplicity of the proxy approach. Other difficulties are that a proxy implementation usually is for a specific task or a particular set of protocols. Such a proxy implementation requires special proxies for each application.

7.2 Delay Tolerant Networks

DTN is based on the TCP/IP protocol suite which is built on a number of implicit conventions that do not hold true in challenged communication environments. In particular, the underlying assumptions of TCP/IP are as:

- An end-to-end path must occur between source and destination during data interchange.
- The max round trip-time for packets must be relatively small and stable.
- The end-to-end packet harm is relatively small.

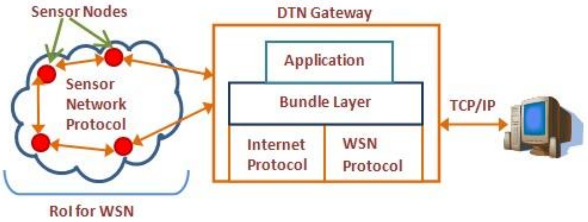


Fig 6: Connecting using the DTN-Architecture

The DTN architectural design (As given in the Figure 6), contains numerous principles to provide service in these Environments as mentioned in [10]. A DTN consists of set of *areas* which share a common layer called the bundle layer that resides above the transport layer. The bundle layer stores messages in storage if no link available. Layers are chosen dynamically based on the specific communication features. The DTN gateway frontwards bundles between those areas, and takes care of delivering messages from other regions to hosts within the local region. A fully DTN enabled sensor network would effortlessly be stretched to a TCP/IP network, simply by connecting one or more of the DTN gateways to the TCP/IP network.

7.3 TCP/IP for Sensor Networks

Directly employing the TCP/IP protocol suite as the communication protocol in the sensor network would enable seamless integration of the sensor network and any TCP/IP network. No special midway nodes or gateways would be needed for connecting a sensor network with a TCP/IP network. TCP/IP in the sensor network would also provide the possibility to route data to and from the sensor network over standard technologies such as General Packet Radio Service (GPRS) [5]. It leads to architecture:

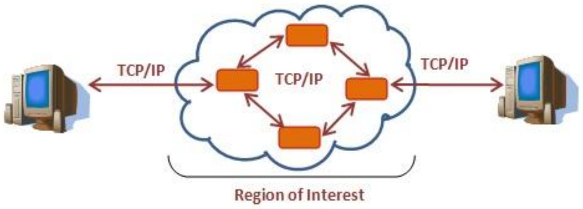


Fig 7: Connecting using TCP/IP in the Sensor Network

The size of TCP/IP packet headers is ranges between 28 and 40 bytes, and limited bytes of sensor data are sent in a datagram, the headers consist of nearly 90% of each packet. Energy efficiency is of crucial significance for WSNs, a header overhead of 90% is not acceptable. Hence, most protocols developed for sensor networks try to keep the header overhead as low as possible. For instance, the TinyOS [11] message communication header overhead is only 5%. The header overhead in TCP/IP can be reduced using various forms of header compression approaches [12], [13], [14], [15]. These mechanisms or techniques were designed to work with single-hop-link, but now it also being done with multi-hop-links. Methods for improving TCP performance in wireless networks have been proposed [16], [17], [18], but these are often targeted towards the case where the wireless link is the hopped last, and not for WSN with multiple wireless hops. In addition, traditional methods assume that the routing nodes have significantly larger amounts of resources than what limited sensor nodes have.

8. RELATED WORKS

8.1 Gateway-Based Integration

The gateway-based integration [19] operates the gateway systems between the wireless sensor networks and the Internet; it is of two kinds. One is application-level gateway, and the other is a DTN (Delay-Tolerant Networking)-based gateway [20]. Application-level gateway is implemented on the function which enables protocol transformation. This method is easy to implement, has low positioning cost, and provisions the internetworking efficiently on heterogeneous networks because the isolated operation between the wireless sensor networks and Internet, is possible [21]. The DTN is defined as a network constructed with regional networks. Here, region implies a network that employs same technology. So, the DTN-based gateway internetworks between the regional networks which employ the same technology using application-level gateway. This method controls the delay time, transforms the protocol efficiently and provides the interoperability between the regional networks.

8.2 Overlaying-Based Integration

IP overlay network [20], [22] based on overlaying-based integration [19] is a structure which can send and receive the data through IP packets after applying the IP protocol and assigning the IP address to the sensor nodes on wireless sensor networks. This method deals with two issues. One is how IP address is given to the sensor node and how to combine the address-based and data-based routing efficiently according to network stream. The location of the sensor node was introduced in IP address assignment and the Directed Diffusion and ACQUIRE were proposed in routing protocol. On the other hand, overlay sensor networks [23] based on overlaying-based integration combine the sensor networks with the Internet outspreading the data centric routing on the sensor networks to application-level overlay sensor networks on the Internet. Now the collected data from the sensor networks is forwarded to the host on the Internet after encapsulating the payload of the IP packet on the gateway. Therefore, this method can be easily implemented and interconnected via program on the host because data of the sensor networks can be processed with an application message of the Internet protocol.

8.3 6LoWPAN

A task force named 6LoWPAN Working Group from the Internet Engineering Task Force (IETF) is working on a standard protocol definition: 6LoWPAN[24]. The main goal of the 6LoWPAN is defining the transmission method of the IPv6 packet on LoWPAN which is constructed with IEEE 802.15.4 devices, supporting small/Pico sensor network. These devices have features such as low power, less prices, low bandwidth, great density, and star or mesh topology. Therefore, 6LoWPAN implements the routing that considers available cyclic sleep, low overhead, small size routing table, and extensions in constructing the IP and TCP/UDP environments over MAC/PHY layer. Due to the given causes, 6LoWPAN expects re-use of the verified legacy technologies, exchange of the data and association to non-IEFT Corporation like ZigBee Alliance. At present, 6LoWPAN uses verified and well-known IP technologies, has a viewpoint that can use the legacy network infrastructure and save the additional cost, but this scheme which adopts IPv6 on ZigBee, is not good because it spends more memory (64K), incurs high costs, and is difficult to implement.

8.4 IPv6 DDNS (Dynamic DNS)

Dynamic DNS updates (DDNS) which is a standard mechanism for dynamically updating the DNS. Unlike DNS that only works with static IP, DDNS works with dynamic IP, such as assigned by an ISP or other DHCP server. DDNS is common with home networkers, who typically receive dynamic, most-often-changing IP addresses from their service provider. To use DDNS, individual simply signs up with a provider and connect/install network software on their host to monitor its IP address. Thus, it works equally well with Stateless Address Auto Configuration (SLAAC), DHCPv6, or manual address configuration. It is important to study how each of this work, if IP address-based confirmation, instead of stronger mechanisms (RFC3007), was used in the updates. As relying on IP addresses for DDNS is rather uncertain at best, stronger authentication should always be used; still, this requires that the authorization will be explicitly configured using unspecified operational methods [25].

9. CONCLUSION

As WSNs gaining popularity in its application dimensions, it becomes a necessity to connect this Ad-Hoc wireless network to the infrastructure based Internet. This integration can be fruitful to retrieve gathered environmental data from Region of Interest (RoI), remotely and wirelessly. This data can be useful and supportive to achieve many things in present as well as in future. Since WSNs & Current Internet differ in various aspects so it is not possible that a single technological solution fulfills or covers all integration related programs. The objective of this research contribution is to present or explore each and every aspects of existing frameworks concepts and projects used or focused on integration of WSNs & Current Internet.

10. REFERENCES

[1] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y. and Cayirci, E. 2002. Wireless Sensor Networks: a Survey. Computer Networks, vol. 38, 393–422.

[2] Emara, K.A.A.E.S. 2009. Integrating Wireless Sensor Networks with IP-based Network. Master's Thesis. Department of Computer Science, Ain Shams University, Cairo.

[3] Zimmermann, H. April 1980. OSI Reference Model-The ISO Model of Architecture for Open Systems Interconnection. IEEE Transactions on Communications, vol. 28, no.4, pp.425-432. doi: 10.1109/TCOM.1980.1094702.

[4] Zamalloa, M.Z. and Krishnamachari, B. 2003. Integrating Future Large-scale Wireless Sensor Networks with the Internet. USC Computer Science Technical Report CS03-792, Department of Electrical Engineering, University of Southern California, CA.

[5] IETF working group 6lowpan. IPv6 over Low power WPAN (6lowpan). Available at: http://www.ietf.org/html.charters/6lowpancharter.html.

[6] Available at: http://www.sciencedaily.com/releases/2006/02/060210090229.htm.

[7] IETF working group 6lowpan. IPv6 over low power wpan (6lowpan). Available at: http://www.ietf.org/html.charters/6lowpancharter.html.

[8] Dunkels, A. The Contiki Operating System. Available: https://www.sics.se/search/content/contiki.

[9] IEEE Computer Society. 2006. Part 15.4: Wirless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-rate Wireless Personal Area Networks (WPANS) - IEEE std802.15.4-2006.

[10] Dunkels, A., Alonso, J., Voigt, T., Ritter, H. and Schiller, J. 2004. Connecting Wireless Sensornets with TCP/IP Networks. In Proceedings of the Second International Conference on Wired/Wireless Internet Communications (WWIC2004).

[11] Hill, J., Szewczyk, R., Woo, A., Hollar, S., Culler, D., and Pister, K. November 2000. System Architecture Directions for Networked Sensors. ACM SIGPLAN Notices, vol. 35, no. 11, pp. 93-104. Doi:10.1145/356989.356998.

[12] Jacobson, V. February 1990. Compressing TCP/IP Headers for Low-speed Serial Links. Internet Engineering Task Force. RFC 1144.

[13] Degermark, M., Engan, M., Nordgren, B., and Pink, S. 1997. Low-loss TCP/IP header compression for wireless networks. ACM/Baltzer Journal on Wireless Networks.

[14] Pink, S., Degermark, M. and Nordgren, B. February 1999. IP header compression. Internet Engineering Task Force. RFC 2507.

[15] Casner, S. and Jacobson, V. February 1999. Compressing IP/UDP/RTP Headers for Low-Speed Serial Links, Internet Engineering Task Force, RFC 2508.

[16] Intanagonwiwat, C., Govindan, R. and Estrin, D. 2000. Directed diffusion: a scalable and robust communication paradigm for sensor networks. In Proceedings of the ACM's Conference on Mobile Computing and Networking (ACM MobiCom), pp. 56-67.

[17] Jacobson, V. February 1990. Compressing TCP/IP headers for low-speed serial links. Internet Engineering Task Force, RFC 1144.

[18] Liu, J. and Singh, S. 2001. ATCP: TCP for mobile ad hoc networks. IEEE Journal on Selected Areas in Communications, vol. 19 (7), pp.1300-1315.

[19] Kim, J.-H, Kim, D.-H, Kwak, H.-Y and Byun, Y.-C. 2008. Integration between WSNs and Internet based on Address Internetworking for Web Services. Computing and Informatics, vol. 27, 707–718.

[20] Dunkels, A., Alonso, J. and Voigt, T. January, 2004. Making TCP/IP viable for Wireless Sensor Networks. SICS Technical Report T2003:23, ISRN:SICS-T{2003/23-SE, Swedish Institute of Computer Science. Sweden. ISSN 1100-3154.

[21] Zamalloa, M. Z. and Bhaskar, K. 2003. Integrating Future Large-Scale Wireless Sensor Networks with the Internet. USC Computer Science Technical Report CS, pp. 03-792.

[22] Dunkels A., Alonso, J., Voigt T., Ritter H. and Schiller J., February, 2004. Connecting Wireless Sensornets with TCP/IP networks. In Proceedings of the Second International Conference on Wired/Wireless Internet Communications.

[23] Dai, H. and Han, R. November. 2004. Unifying Micro Sensor Networks with the Internet via Overlay Networking. In Proceedings of the IEEE Emnets-I, pp. 571–572.

[24] Mulligan, G. and Group, W. 2007. The 6LowPAN Architecture. In Proceedings of 4th Workshop on Embedded Networked Sensor, Cork, Ireland, pp. 78-82.

[25] Comcast, A.D., Autonomica, J.I., and Savola, P. April 2006. Operational Considerations and Issues with IPv6 DNS. RFC 4472. Internet Society.