Indian Journal of Science and Technology, *Vol 9(10), DOI: 10.17485/ijst/2016/v9i10/88985, March 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Localization using GPS Coordinates in IPv6 Addresses of Wireless Sensor Network Nodes

Thomas O' Daniel, Mohammed Nazar Hussein and Raed Abdulla

Faculty of Computing, Engineering and Technology, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia; dr.thomas.odaniel@apu.edu.my, mohammed.nazarhussien@apu.edu.my, dr.raed@apu.edu.my

Abstract

Background/Objectives: This paper describes design considerations surrounding the implementation of a novel and standards-compliant scheme to incorporate GPS location information into the IPv6 address of Wireless Sensor Network (WSN) nodes. **Methods/Statistical Analysis:** A wide variety of localization protocols have been proposed which allow nodes to interpolate their location from their neighbors as an alternative to deploying more expensive WSN nodes with GPS receivers or other dedicated localization hardware. The scheme proposed here is similar to others in that it relies on ground-truth anchor nodes, and unique in that it uses the network address to convey this information. **Findings:** There are a number of interesting design considerations for location interpolation in a WSN that has a small number of sparsely distributed nodes with GPS ground-truth and a larger number of nodes that interpolate their location based on analysis of packets received with GPS coordinates and confidence intervals embedded in their addresses. Our calculations show that accurate GPS coordinates can be carried in the IPv6 address along with the transmission radius of the node, and this information is sufficient for a node to determine its location through triangulation. Additional flags can also be provided, such as an indicator of link quality, to refine this calculation and reduce the margin of error. The additional information can be different for each neighbor node, overcoming limitations on determining directionality in broadcast networks. Since the location information is carried in every packet header there is no overhead of a separate protocol and each node can do its calculations independently. **Applications/Improvements:** WSN nodes that report their geographic location in the address of every packet they send has obvious potential for refining information gathering in various types of deployments.

Keywords: GPS Coordinates, IPv6, Location-based Addressing, Wireless Sensor Networks

1. Introduction

Wireless Sensor Networks (WSNs) are a fundamental aspect of ubiquitous systems and the Internet of Things (IoT). WSNs are composed of low cost tiny devices with constrained processing and memory resources that are typically battery powered. Networks of these devices are characterized by small packet payload size, minimum bandwidth, unreliable radio connectivity, ad hoc deployment, dynamic topology changes, and nodes running in a power conservation mode to prolong battery lifetime. WSNs have applications in various fields such as structural health monitoring, energy monitoring, machine condition monitoring, transportation, and many other domains. Connecting networks of these devices directly to the Internet to achieve end-to-end communication where Internet users can retrieve and observe real-time data, is an active field of research across the globe.

Many types of WSN deployments, particularly for environmental surveillance[1] and disaster management[2] could benefit from constant reporting of the location where data was sensed. Nodes can be equipped with Global Positioning System (GPS), but this is a costly solution in terms of both money and energy consumption[3,4], and GPS typically fails inside buildings and under heavy vegetative cover[5]. Localization techniques reported in the literature use various combinations of metrics to develop measures of link quality, but inferring relative location

*Author for correspondence

from these measures is subject to assumptions about decrease in signal strength due to the distance between transmitter and receiver, type and height of antennas, and the presence of obstacles that disrupt the line-of-sight path[6,7].

This paper describes the major design considerations for a WSN that has a small number of sparsely distributed nodes with GPS ground-truth and a larger number of nodes that interpolate their location through inter-communication. As with all WSN localization techniques, a primary goal is to derive a satisfactory degree of accuracy from inconsistent radio communication while minimizing power consumption. Further design goals are Internet standards compliance and minimal modifications to standard implementations.

We begin with a brief description of the Internet standard 6LoWPAN protocol stack and IPv6 addressing. A novel scheme for using GPS coordinates as an IPv6 site-local address is presented, followed by consideration of the limits of GPS positioning accuracy and the implications for the addressing scheme. The question of optimal placement of sensor nodes programmed with GPS ground truth is posed, leading to an initial allocation of flag bits in the address. A promising algorithm from the literature for classifying link quality is explained, along with a brief overview of the implications of interference for localization in WSNs.

2. IPv6 and 6LoWPAN

2.1 The 6LoWPAN Protocol Stack

Internet standards are published as Requests for Comments (RFCs) by the Internet Engineering Task Force (IETF), and made available in a permanent archive at tools.ietf.org/. Ishaq, et al.[8] present an extensive overview of IETF standardization work and open issues being addressed in order to realize an all-encompassing IoT.

The IETF standard for extending the use of IPv6 to WSNs is known as 6LoWPAN, which stands for "IPV6 over Low Power Wireless Personal Area Networks". The 6LoWPAN protocol stack comprises IEEE 802.15.4 at the physical and Medium Access Control (MAC) layers, a 6LoWPAN adaptation layer, IPv6 at the network layer, and standard Internet protocols at the transport and application layers[9,10].

The IPv6 network works optimally with efficient links and high packet delivery rates, which is quite the opposite of the general characteristics of WSNs. IEEE 802.15.4 was developed for interconnection of data communication devices using short-range Radio Frequency (RF) transmissions in a wireless personal area network[11]. This standard defines a maximum physical-layer packet size of 127 bytes, while using IPv6 as the network layer protocol requires that a minimum MTU (Maximum Transmission Unit) of 1280 bytes must be supported over the link[12]. Furthermore, the IPv6 header is 40 bytes, leaving only 87 bytes for payload in the 802.15.4 frame. The 6LoWPAN adaptation layer provides header compression and packet fragmentation and reassembly mechanisms to manage these differences transparently[10,13].

2.2 IPv6 Addressing

When the IPv6 addressing architecture was originally standardized[14] "site-local" addresses were defined to be used for addressing inside a site without the need for a globally routable prefix. Site-local addresses were defined to serve the same purpose as IPv4 "private" address ranges[15] which had become quite popular and proven useful. Site-local addresses were subsequently deprecated[16] and replaced by "Unique Local IPv6 Unicast Addresses", a special-purpose address block and IPv6 unicast address format meant to be globally unique and intended for local communications, usually inside a site. These addresses are not expected to be routable on the global Internet[17,18,19].

Unique Local IPv6 unicast Addresses (ULAs) have the following general form:

- An 8 bit prefix, where FC00::/7 is used to identify Local IPv6 unicast addresses. The last bit is known as the L bit, and is set to one - use of addresses with the L bit set to zero are still undefined in 2015;
- A 40 bit Global ID set to a pseudo-random number using a standard algorithm;
- A 16 bit Subnet ID determined by the site;
- A 64 bit Interface ID that conforms to the current standard for the IPv6 Address Architecture.
- The subscript for the permeability of vacuum O_0, and other common scientific constants, is zero with subscript formatting, not a lowercase letter "o."

The standard specifies that the locally assigned Global ID must be generated with a pseudo-random algorithm. To ensure an extremely high probability of uniqueness, all sites generating Global IDs must use a functionally similar algorithm. RFC4193 specifies this as the least

significant 40 bits of a 160-bit SHA-1 digest generated from the concatenation of the current time of day and an EUI-64 identifier derived from the 48-bit MAC address of the system. Using this algorithm there is a theoretical risk of two independent sites generating identical prefixes, but the IETF is satisfied that this can be ignored for all practical purposes.

The Interface ID is supposed to be unique on the links reached by routing to that prefix, giving an IPv6 address that is unique within the applicable scope. Both the original standard for the IPv6 address architecture[14] and the updated standard[20] specified that Interface IDs are required to be constructed in Modified EUI-64 format. In the case of an IEEE 48 bit MAC identifier, two octets, with hexadecimal values of 0xFF and 0xFE, are inserted in the middle of the 48-bit MAC (between the company ID and vendor supplied ID), and the sixth bit in Internet standard bit-order (the "u" or "universal/local" bit) is inverted[21]. In the globally unique addresses assigned by the IEEE this bit has always been set to zero while locally created addresses set it to one, so when the bit is inverted, it maintains its original scope. The motivation was to allow development of future technology that could take advantage of interface identifiers with universal scope[10].

The standard for the IPv6 address architecture was updated in 2014 to remove the modified EUI-64 restriction, and clarify that the bits in an interface identifier have no generic semantics and that for the purposes of IP, the entire identifier must be treated as an opaque value by third parties[22].

This means it is now possible to create a standards-compliant method for using GPS coordinates as unique local IPv6 unicast addresses.

3. GPS Coordinates

GPS coordinates are based on dividing the perfect sphere of the world into 360 degrees of horizontal longitude and 180 degrees of vertical latitude. Each degree of latitude and longitude is divided into sixty minutes, and each minute is divided into sixty seconds, with fractions of a second offering finer-grained specification of a location. There are 3 common and equivalent formats for expressing location, ddd°mm'ss.ss", ddd°mm.mmm', and ddd.ddddd°, where d, m, and s stand for degrees, minutes, and seconds.

Degrees are expressed as a number between –180 and +180 for longitude, and a number between –90 and +90 for latitude. Zero degrees longitude is an arbitrary line, locations to the west of which are negative, and locations to the east are positive. Zero degrees latitude is the equator, with locations to the north as a positive number, and to the south as a negative number.

3.1 GPS in IPv6

The foundations of the scheme are IPv6 site-local addresses and GPS coordinates expressed in decimal degrees format. An IPv6 site-local address has a 16 bit Subnet-ID field and a 64 bit interface identifier field. The seventh decimal place of the GPS latitude and longitude numbers gives a location accurate to within about 1 centimeter, which is near the limit of what GPS-based techniques can achieve (see below).

For the purpose of embedding GPS coordinates in an IPv6 address, the coordinates can be shifted into positive integer space. The 360 degrees longitude and 180 degrees latitude form a grid of 360*180=64,800 zones. At seven-digit precision, within each of these zones there are 9,999,999 offsets in each direction[23]. In a common computer architecture representation, the latitude and longitude zone can be stored as an unsigned short integer (ushort, 16 bits), while the offsets each require 24 bits of a 32-bit unsigned integer (uint). The complete coordinates could be stored in an unsigned long integer (ulong, 64 bits).

While 64 bits is the required length for the interface identifier in an IPv6 unicast address, and thus the zone and offsets could be pushed whole into this space, there is a more interesting possibility. The 16 bit Subnet-ID field in the address allows for 65,536 subnets, which easily accommodates all of the latitude/longitude zones. The two 24-bit offsets can then be put in the interface identifier field, leaving 16 bits that could be used as flags. Interleaved bits (also known as Morton numbers) are useful for linearizing 2D integer coordinates, so x and y are combined into a single number that can be compared easily and has the property that a number is usually close to another if their x and y values are close[24,25].

So, given a set of coordinates like –33.1234567 and 88.7654321, the integer part would be mapped into the unsigned integer grid, and the zone concatenated with FD00 and the 40-bit Global-ID to form the first half of the address. The decimal parts of the two numbers would be interleaved into a single 48-bit number, and put into the Interface-ID field with the 16 low order bits initially set to zero, for subsequent use as flags.

Storing the decimal offsets within the grid in this fashion eliminates the need for a delimiter to separate the latitude and longitude offsets while making it easier to compare the relative location of points. The process of recovering the GPS coordinates is straightforward, as is the process for calculating relative distance between nodes. Using the zone as a subnet address facilitates routing, as does using the low-order bits as flags since the convention for routing tables is to calculate the longest match on the high-order bits. The flag bits in the interface address can be used to report a confidence interval based on how far removed a node feels it is from neighbors with ground truth, based on analysis of packets received and the confidence intervals contained in their addresses.

3.2 General Accuracy of GPS

As noted above, GPS coordinates are based on dividing the perfect sphere of the world into 360 degrees of horizontal longitude and 180 degrees of vertical latitude. The longitude lines, also known as meridians, are the same distance apart at the equator and converge at the poles. The meter was originally defined such that ten million of them would span the distance from the equator to a pole, so at the equator each degree of both latitude and longitude represents approximately 111.32 km. Because the meridians get closer together moving from the equator toward either pole, one degree of longitude is multiplied by the cosine of the latitude, decreasing the indicative physical distance as illustrated in Table 1.

In fact, the fourth decimal place is comparable to the typical accuracy of an uncorrected GPS unit with no interference, while accuracy to the fifth decimal place requires differential correction with commercial GPS units. The seventh decimal place is near the limit of what GPS-based techniques can achieve with painstaking measures[26].

These limitations establish bounds on the accuracy of both ground-truth and interpolated locations. Following the simple rule for determining the number of bits required to represent a decimal number, digits * 3.32 and round up, we could essentially choose a random pattern for the last 13 bits of the Morton code (the sixth and seventh digits of interleaved latitude and longitude) to locate a node within 0.8-1.1 square meter for typical locations – and even this assumes ground-truth is accurate at five decimal places.

This also helps us set expectations at the top end. A typical WSN transceiver, the TI CC2430 for example, has a reliable range of around 150 to 250 meters depending on the type of antenna[27,28], which is the in the range of the third decimal digit of the GPS coordinate readings. Thus the first 12 interleaved bits of the 48-bit Morton code for all neighbors will be either identical or vary within a narrow and predictable range, leaving only 23 bits of real variation. This simplifies the interpolation solution space significantly.

It is worth noting that the subnet may also vary within a narrow and predictable range at the edges of a GPS zone, a topic that is considered in more detail next

4. Location Interpolation

A node that has more than one ground-truth neighbor should be able to interpolate its location with a high degree of confidence (possibly even accuracy). Nodes that have no ground-truth neighbors will necessarily have lower confidence in their position estimates. A design consideration that can only be addressed using empirical data is the question of the confidence interval that should be associated with coordinates interpolated from reported locations that are hops away from ground truth. In other

Table 1. Precision of GPS decimal places of longitude and indicative locations at particular latitudes

Decimals	0	1	2	3	4	5	6	7
Equator	111 km	11 km	1 km	111 m	11 m	1 m	11 cm	1 cm
Quito, Ecuador; Maqcapa, Brazil; Kampala, Uganda; Thinadhoo, Maldives; Pontianak, Borneo								
23 N//S	102. 5 km	10.25 km	1 km	102.5 m	10.25 m	1 m	10.25 cm	1 cm
Havana, Cuba; Muscat, Oman; Shantou, China // Sao Paulo, Brazil; Windhoek, Namibia; Alice Springs, Australia								
45 N//S	78.7 km	7. 9 km	787 m	78.7 m	7. 9 m	78.7 cm	7. 9 cm	7. 9 mm
Portland OR USA; Limoges, France; Harbin, China // Rio Mayo, Argentina; Dunedin, New Zealand								
67 N//S	43. 5 km	4.35 km	435 m	43.5 m	4.35 m	43.5 cm	4.35 cm	4.35 mm
Coldfoot, AK USA; Repulse Bay, Canada; Inari Finland; Tomtor, Siberia // Adelaide, Casey Station, Antarctica								

words, when should confidence drop to zero? As an initial hypothesis, we posit that we will have little or no confidence in a position estimate when all neighbors are more than 2 hops away from a ground-truth node, but the real optimum could turn out to be more or less than that.

A particular case that deserves attention are the nodes at the edges, and especially the corners, of a GPS zone used in the Subnet-ID field of the address. As noted, a zone represents the integer latitude and longitude, which means 111 km square in real terms. In a WSN that spans zones, nodes at the edge of a zone will receive packets with different subnet addresses (in the case of a corner, up to four), even though they are physically quite close together.

In this special case interpolating location will require some extra processing, with a concomitant energy drain. Adjacent subnets will have a typical pattern, as will the offsets, since they are at the edge of a zone. The direction of the other zone can be determined (up, down, left, right) as well as the possible distance inside any zone (determined by the radio range) so margins of error for latitude and longitude can be calculated. The likelihood of putting oneself on the wrong side of the border must also be incorporated into the confidence interval. Since uncertainty propagates as distance from a ground-truth neighbor grows, the optimal placement of ground-truth nodes at these edges and decision criteria will have to be validated through experiments. Nonetheless, this special case determines the first use of the flag bits in the address.

4.1 Flag Bits in the Address

The edge case will require six of the 16 bits available for flags: Four bits to represent whether a neighboring subnet is up, down, left, right of the one in the address, and two bits to represent the number of neighbors outside the same subnet if any of the other four bits are set. Again, experiments will be necessary to determine if this is adequate information for a neighbor receiving this information to determine its location within a zone and distance from the edge, but it is a reasonable starting point. Four of these bits will remain unset if a node is confident it and all of its neighbors are in a single zone which means two bits could have different semantics in this case if it is necessary.

In the general case, the transmission radius of a node is essential information required for determining relative location. This could be done with a small set of bits that represent user-defined standard ranges, or a more exact number that is also pre-configured. Representing confidence means using the remaining bits available effectively. Two obvious states are "I have ground-truth" (complete confidence) and "I have no clue" (no confidence); other states could represent the number of neighbors with ground-truth, and the number of neighbors at a given number of hops away from a neighbor with ground-truth. Higher confidence would be associated with more neighbors close to ground truth, moderated by the quality of the link, which is discussed below. The exact patterns need to be formulated through experimentation.

It is important to note that since this is carried in the address of each packet, the values in the source address can be can be adjusted for each destination address. For example, if a node has a neighbour that reports its address as closer than it should be based on the transmission radii and signal quality, the nodes may infer that there is an interfering obstacle between them and adjust the transmission radius reported to other neighbours in the vicinity. This flexibility constitutes a unique low-cost way to address limitations on determining directionality in broadcast networks.

4.2 Link Quality

A very promising algorithm from the literature, dubbed the "Triangle Metric"[29], geometrically combines three readily available hardware indicators to identify the quality of links from a sample of as few as 10 packets.

Three relevant quantities can be directly observed using an IEEE 802.15.4-compliant transceiver: Packet Reception Rate (PRR), Received Signal Strength Indicator (RSSI), and the Link Quality Indicator (LQI). A fourth measure, the Signal to Noise Ratio (SNR), can be derived by sampling RSSI when there is no ongoing transmission and subtracting this value (known as the RSSI noise floor) from the RSSI associated with packets received.

Each of these metrics provide a different type of information, and each alone has strengths and weaknesses when it comes to classifying link quality. PRR cannot differentiate between good links that are resilient and good links that are susceptible to degradation from minor changes in shadowing or interference[30]. SNR can only differentiate between very good links and the rest, and combining these two is still inadequate to accurately classify a link as very good, good, intermediate, or bad. The characteristics of LQI are similar to those of PRR, but LQI

enables a better classification of bad, intermediate, and good links[31]. However, LQI does not distinguish between busy and slow links. Classification based on PRR requires a relatively large number of observations to obtain usable results, and approaches based on RSSI/SNR or LQI only partially map to PRR with any degree of accuracy.

The aim of the Triangle Metric is to estimate the quality of a link by combining the link state information of PRR, SNR, and LQI with small observation windows. The sum of the mean SNR and LQI values of the received packets is divided by the total number of transmitted packets to yield a "window mean". The advantage of the window mean over the statistical mean is that it includes reception rate information, effectively penalizing links with low reception rates. The reported experimental results show that this technique combines the information available from the physical layer in a way that leads to a more robust estimation compared to any one of these indicators alone. As is to be expected, the quality of the estimate increases with the size of the observation window since more data is available, but the reported results show that a window size of 10 packets is a reasonable trade-off between accuracy, cost, and estimation time.

5. Planning for Experiments

Our initial experimental environment must be founded on two key assumptions: The network will not span the edge of a zone, and there is no other network in radio range of any node. Having more than one network in an area poses the same complications with the Global ID as spanning the edge of one or more zones poses with the Subnet ID.

Further, all nodes will be running the same software, and none of the nodes will be equipped with GPS. Some nodes will be programmed with their actual GPS coordinates (ground-truth) when they are placed in the field, most will not.

Ground-truth nodes will be placed in a regular pattern on an unobstructed plain without direct intercommunication. Nodes that will interpolate their address will be placed in a pseudo random fashion within radio range of each other, to investigate patterns of flag bits and meaningful confidence intervals, especially for nodes that are hops away from ground-truth and nodes with fewer than two neighbors. This benchmark scenario will gradually be made more complicated with the addition of interferers that disrupt radio communication and mobile ground-truth nodes, to gauge the effect on confidence in and accuracy of interpolated location. Optimal location of ground-truth nodes will also be investigated, to confirm hypotheses of optimal placement described in the literature[32].

The benchmark scenario will also be used to test the limits of accuracy when there are multiple nodes within a small area. The granularity of GPS coordinates relative to the density of the sensor network could lead to address duplication, and pose a trade-off between using a simple ad hoc notification and tiebreaker protocol or drawing on the facilities of the 6LoWPAN neighbor discovery protocol[33].

A node that needs to interpolate its address will begin by collecting packets, parsing the address from the flags, and capturing the RSSI and LQI associated with them. Flags will be analyzed and the neighbors with the high confidence in their estimate of their location will be sent a series of packets in order to calculate PRR and SNR of the link. An initial confidence interval can then be calculated using the window mean of these links, which could be refined by sending packets to other neighbors and repeating the process.

Using the address means location and confidence information is passed with every packet, so this should only require modifying the stack to echo all packets received to an interpolator, which will return an address to be used in subsequent outgoing packets.

6. Conclusion

This approach to localization using GPS coordinates in IPv6 addresses of wireless sensor network nodes will meet our broad design goals of IETF standards compliance and minimal modification to standard implementations.

Using interleaved coordinates, flag bits, and the window means associated with links to neighbors will allow us to achieve the key design goal of deriving a satisfactory degree of accuracy from inconsistent radio communication while minimizing power consumption. Interleaved coordinates will simplify calculations and minimize power consumption; efficient calculation of link quality using a small number of packets to determine a window mean will allow formulation of confidence intervals that can be included in the address with simple bit-shifting operations, which, given the overall level of accuracy of GPS, will allow localization of a node within one square meter or so.

At this point we are able to describe the environment for our experiments that will provide the information necessary to configure the flag bits in the address that will be used to express the level of confidence in the interpolated address. These experiments are at a very early stage, with no concrete results to report as yet.

7. References

1. Yeon-Jun A, Do-Hyeun K. Sensor web based on multiple interface for public environmental surveillance. Indian Journal of Science and Technology. Aug 2015; 8(18):1–3.
2. Devasena A, Sowmya B. Wireless sensor network in disaster management. Indian Journal of Science and Technology. July 2015; 8(15); 1–6.
3. Cheng L, Chengdong W, Yunzhou Z, Hao W, Mengxin L, Maple C. A survey of localization in wireless sensor networks. International Journal of Distributed Sensor Networks 2012. 2012. p.12.
4. Stojmenovic I, Olariu S. Data-centric protocols for wireless sensor networks. In I. Stojmenovic (Ed.). Handbook of Sensor Networks: Algorithms and Architectures. 2005. p.417–56.
5. Maheshwari HK. Optimizing range aware localization in wireless sensor networks (WSNs). University of Leeds: UK; 2011.
6. Willis SL, Kikkert CJ. Radio propagation model for long-range wireless sensor networks. 6th International Conference on Wireless networks, Communications and Mobile Computing. 2005; 1:826–32.
7. Abd-Alhameed RA, Zhou D, See CH, Hu YF, Horoshenkov KV. Measure the range of sensor networks. Available from: http://mwrf.com/test-and-measurement/measure-range-sensor-networks. Date accessed: 10/15/2008.
8. Ishaq I, Carels D, Teklemariam GK, Hoebeke J, Van den Abeele F, De Poorter E, Moerman I, Demeester P. IETF standardization in the field of the Internet of Things (IoT): A survey. Journal of Sensor and Actuator Networks. 2013; 2(2):235–87.
9. Kushalnagar N, Montenegro G, Schumacher C. IPv6 over low-power wireless personal area networks (6LoWPANs): Overview, assumptions, problem statement, and goals. Network Working Group. 2007. p.1–12.
10. Montenegro G, Kushalnagar N, Hui J, Culler D. Transmission of IPv6 packets over IEEE 802.15.4 networks. Network Working Group. 2007. p.1–30.
11. IEEE Standard for local and metropolitan area networks - Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs). 2011. p.1–314.
12. Deering S, Hinden R. Internet Protocol, Version 6 (IPv6) Specification. Network working Group. 1998. p.1–39.
13. Hui J, Thubert P. Compression format for IPv6 datagrams over IEEE 802.15.4-based networks. Network Working Group. 2011. p.1–24.
14. Hinden R, Deering S. Internet Protocol version 6 (IPv6) addressing architecture. Network Working Group. 2003. p.1–26.
15. Rekhter Y, Moskowitz B, Karrenberg D, de Groot G. Address allocation for private internets. Network Working Group. 1996. p.1–9.
16. Huitema C, Carpenter B. Deprecating site local addresses. Network Working Group, 2004. p.1–10.
17. Hinden R, Haberman B. Unique local IPv6 unicast addresses. Network Working Group, 2005, 1–16.
18. Blanchet M. Special-use IPv6 addresses. Network Working Group. 2008. p.1–7.
19. Cotton M, Vegoda L, Bonica R, Haberman B. Special-purpose IP address registries. Internet Engineering Task Force (IETF). 2013. p.1–23.
20. Hinden R, Deering S. IP version 6 addressing architecture. Network Working Group, 2006. p.1–25.
21. IEEE Registration Authority. Guidelines for 64-bit global identifier (EUI-64). Available from: https//standards.ieee.org/develop/regauth/tut/eui64.pdf.
22. Carpenter B, Jiang S. Significance of IPv6 interface identifiers. Internet Engineering Task Force. 2014. p.1–10.
23. Dupuis L. Efficient WGS84 (aka GPS) coordinates compression. Available from: http://www.dupuis.me/node/35.
24. Giesen F. Decoding morton codes. Available from: https://fgiesen.wordpress.com/2009/12/13/decoding-morton-codes/
25. Hoedt A. Morton codes. Available from: http://asgerhoedt.dk/?p=276
26. Huber WA. How to measure the accuracy of latitude and longitude? Available from: http://gis.stackexchange.com/questions/8650/how-to-measure-the-accuracy-of-latitude-and-longitude/8674#8674
27. Huebner C, Cardell-Oliver R, Hanelt S, Wagenknecht T, Monsalve A. Long-range wireless sensor networks with transmit-only nodes and software-defined receivers. Wireless Communications and Mobile Computing. 2013; 13(7):1499–10.
28. Jonsrud GE. Texas Instruments application note AN040: folded dipole antenna for CC2400, CC2420, CC2430, CC2431, and CC2480. Texas Instruments Applications. 2008. p.1–26.
29. Boano CA, Zuñiga MA, Voigt T, Willig A, Romer K. The triangle metric: Fast link quality estimation for mobile wireless sensor networks. 2010 Proceedings 19th International Conference on Computer Communications and Networks (ICCCN), Zurich. Switzerland, Zurich. 2010. p.1–7.

30. Srinivasan K, Levis P. RSSI is under appreciated. 3rd Workshop on Embedded Networked Sensors (EmNets). Cambridge, MA, USA; 2006.
31. Polastre J, Szewczyk R, Culler D. Telos: Enabling ultra-low power wireless research. 4th International Symposium on Information Processing in Sensor Networks (IPSN'05). Los Angeles, USA, IPSN'09. 2005. p.364–69.
32. Kunz T, Tatham B. Localization in wireless sensor networks and anchor placement. Journal of Sensor and Actuator Networks. 2012; 1(1):36–58.
33. Shelby Z, Chakrabarti S, Nordmark E, Bormann C. Neighbor discovery optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs). Internet Engineering Task Force (IETF). 2012. p.1–55.