Ghaleb *et al. EURASIP Journal on Wireless Communications and Networking* (2016) 2016:165
DOI 10.1186/s13638-016-0659-4

EURASIP Journal on Wireless Communications and Networking

REVIEW Open Access

Mobility management for IoT: a survey

Safwan M. Ghaleb[1], Shamala Subramaniam[1,2*], Zuriati Ahmed Zukarnain[1] and Abdullah Muhammed[1]

Abstract

Internet of Thing (IoT) or also referred to as IP-enabled wireless sensor network (IP-WSN) has become a rich area of research. This is due to the rapid growth in a wide spectrum of critical application domains. However, the properties within these systems such as memory size, processing capacity, and power supply have led to imposing constraints on IP-WSN applications and its deployment in the real world. Consequently, IP-WSN is constantly faced with issues as the complexity further rises due to IP mobility. IP mobility management is utilized as a mechanism to resolve these issues. The management protocols introduced to support mobility has evolved from host-based to network-based mobility management protocols. The presence of both types of solutions is dominant but depended on the nature of systems being deployed. The mobile node (MN) is involved with the mobility-related signaling in host-based protocols, while network-based protocols shield the host by transferring the mobility-related signaling to the network entities. The features of the IoT are inclined towards the network-based solutions. The wide spectrum of strategies derived to achieve enhanced performance evidently displays superiority in performance and simultaneous issues such as long handover latency, intense signaling, and packet loss which affects the QoS for the real-time applications. This paper extensively reviews and discusses the algorithms developed to address the challenges and the techniques of integrating IP over WSNs, the attributes of mobility management within the IPv4 and IPv6, respectively, and special focus is given on a comprehensive review encompassing mechanisms, advantages, and disadvantages on related work within the IPv6 mobility management. The paper is concluded with the proposition of several pertinent open issues which are of high research value.

Keywords: Wireless sensor network, Mobility wireless sensor network, IPv6 protocol, IP-enabled wireless sensor network, Mobility management, Ubiquitous computing

1 Review

1.1 Introduction

Wireless sensor networks (WSNs) are tiny devices that are used to sense and collect the data from their surrounding environment in a periodic and continual manner. The data is collected via them and transmitted through the network to reach the sink node where the collected data is analyzed. Unfortunately, WSNs face many challenges due to resource-constrained in terms of memory size, power limitation, computational capability, and due to inconsistency during deployment [1]. These limitations which definitely affect the real-time applications motivating the researchers to propose frameworks that address energy efficiency, router optimization, and data reduction such as the works proposed in [2–8].

Extensive studies have attempted to integrate Internet Protocol (IP) with WSNs as a result to the advent of Internet of Things (IoTs) and ubiquitous computing. Ubiquitous computing is a scenario, where literally everything is connected with everything at anytime and anywhere. This facilitates to make respective decisions without any intervention from the user. The motivation of integrating WSNs with IP is to exploit the benefits of reusing the existing infrastructures and IP-based applications technology for cohesive connectivity with WSNs [9].

In the IoT paradigm, WSNs are considered the most important elements which collect information from their surrounding environment [10]. WSNs provide a remote access when connecting with IoT elements. Apart from this, the collaboration among heterogeneous information systems exhibit common services. This integration is not imaginary and exists in reality. The involvement of the

*Correspondence: shamala_ks@upm.edu.my.
[1] Department of Communication Technology and Network, Universiti Putra Malaysia, 43400 UPM, Serdang, Selengor D.E., Malaysia
[2] Sports Academy, Universiti Putra Malaysia, 43400 UPM, Serdang, Selengor D.E., Malaysia

industry is evident such as "Smarter Planet" [11]. To create the "central nervous system for the Earth," the (CeNSE) project by HP labs deployed tiny smart sensor nodes, worldwide. Similarly, another project developed by IBM considered the smart sensors to play the main role in intelligent cities and intelligent water management. Till date, there have been several technologies developed and tested to enable the integration between the WSNs and IoT. The enabling devices technologies, sustaining low bandwidth, and low power are among the main challenges of this integration. The enabling device technologies such as radio frequency (RF) are of essential importance [12, 13]. To address these challenges, the Internet Engineering Task Force (IETF) proposed many routing protocols and constrained application protocol (CoAP) that are suitable to the IoT; for more information about these protocols and their standards, challenges, and opportunities, see Sheng et al. [14]. The issue of mobility management is of critical importance and forms the focus of this paper.

The IP management protocols introduced to support mobility has evolved from host-based to network-based mobility management protocols. The presence of both types of solutions is dominant but depended on the nature of systems being deployed. The mobile node (MN) is involved with the mobility-related signaling in host-based protocols, while network-based protocols shield the host by transferring the mobility-related signaling to the network entities. The features of the IoT are inclined towards the network-based solutions. The wide spectrum of strategies derived to achieve enhanced performance evidently displays superiority in performance and simultaneous issues such as long handover latency, intense signaling, and packet loss which affects the QoS for the real-time applications.

This paper extensively reviews and discusses the algorithms developed to address the challenges and the techniques of integrating IP over WSNs, the attributes of mobility management within the IPv4 and IPv6, respectively, and special focus is given on a comprehensive review encompassing mechanisms, advantages, and disadvantages on related work within the IPv6 mobility management. The paper is concluded with the proposition of several pertinent open issues which are of high research value.

6LowPAN standard protocol was released by IETF [15]. It allows IP-based communication over computationally constrained networks. WSN nodes are capable of achieving mobility due to their shrinking size and enhancing portability, over the years. This goal can be accomplished through coupling the WSN nodes with mobility entities such as phone, people, or vehicles.

This paper is organized as follows. Firstly, in Section 1.2, an overview of IPv6 protocol and its features is demonstrated followed by a detail account of the mobility feature of IPv6. The challenges of IP-enabled over WSN, and the state of the art for enabling IP over constraints-resources WSNs is demonstrated in Section 1.3. The structure of MWSN, critical issues, advantages, and differences between MWSN and WSNs are presented in Section 1.4. An extensive comparative analysis of mobility management protocols based on several characteristics is made in Section 1.5. Section 1.6 deliberates the critical issues and subsequent open issues associated with the mobility protocol studies. Finally, Section 2 concludes the points of this article.

1.1.1 Enabling IP mobility management

To provide IP mobility management, the IETF proposed and released the Mobile Internet Protocol IPv4 (MIPv4) [16, 17]. The home agent (HA), foreign agent (FA), mobile node (MN), corresponding node (CN), care of address (CoA), visitor list (VL), and mobility binding table (MBT) network entities were introduced by MIPv4 protocol. HA is responsible for keeping the MN reachable when it moves in the Internet in the same domain and keeping their mobility information in MBT. A foreign agent is located in the foreign domain which supports the moving MN. When the MN reaches a foreign domain, the foreign domain assigns a CoA (temporary address based on the current position of the MN) to the MN and keeps the information of arriving MN in its VL and informs the HA about the MN movements. Then, the entry information on the local MBT will be updated by HA. CN is the mobile host being either in static or mobile node that communicates with the MN. As a result of the short range of IP address and high burden of network entity adverted, the Mobile Internet IPv6 (MIPv6) [18] and network mobility (NEMO) approach [19] were proposed by the IETF. This was done to overcome the aforementioned problems in MIPv4. However, the MIPv6 and NEMO protocols are not efficient for critical applications (real-time applications), due to high handover latency, packet ratio loss and signaling overhead [20].

Several host-based protocols were released and designed by the IETF to alleviate the bottleneck in the MIPv6 such as Hierarchical MIPv6 (HMIPv6) [21], Fast Handover for Hierarchical (FHMIPv6) [20] and Fast Handover MIPv6 (FMIPv6 [22]. Access router (AR) and access point (AP) are used to relieve the MN from any related signaling during handover in order to reduce handover latency. Due to the shortcomings of most host-based approaches, there is a constant need to enhance the solutions provided. This improvement will help to meet the key requirement of efficient mobility, communication support that is the major issue of host-based approaches. It causes a major bottleneck in node mobility.

In order to address the aforementioned bottleneck, a new protocol was released by IETF, namely, Proxy Mobile

IPv6 (PMIPv6) [23]. The main objective of this protocol is to ensure that the mobility-related signaling messages are exchanged between the mobile node, corresponding node (CN), and home agent (HA) which causes a high level of tunneled messages. The main target of the aforementioned host-based protocols is to keep all hosts in the mobile network to be accessible via their permanent IP address. It also maintains the ongoing session for all hosts while they are moving within the MIPv6 domain. However, these protocols suffer from associated problems. Recently, the PMIPv6, designed by the IETF, has become essentially a derivative of MIPv6 in terms of signaling and reusing many concepts such as the HA functionality. The PMIPv6 is a network-based mobility management protocol to provide an MN in a topological localized domain. Therefore, it makes the MN free from any mobility-related signaling issue during handover process.

To overcome the limitation associated with host-based protocols, the PMIPv6 adds two extra elements, namely, the local mobility anchor and mobility (LMA) and access gateway (MAG). The LMA takes the responsibility of maintaining the MN reachability while it moves between sub-networks in the local PMIPv6 domain. The serving network MAG takes the responsibility of Mobility management instead of MN. The MAG registers the MN with LMA after initiating the required signals to authenticate MN with authentication, authorization, and accounting (AAA) server. However, the PMIPv6 has similar limitations to the MIPv6 such as handover latency, signaling overhead, and packet loss during HO [24]. Although, several existing studies have tried to enhance the PMIPv6 in terms of handover latency, signaling overhead, and preventing packet loss, there still remains room for improvement. An enhancement of PMIPv6 is the Fast Proxy mobile IPv6 (PFMIPv6) protocol [25] which is a derivative from MIPv6. It is standardized by the IETF to reduce the handover latency. However, when the MN moves from previous MAG (PMAG) to the new MAG (NMAG), the FPMIPv6 protocol depends completely on PMAG to predict the NMAG, where the MN moves to; this dependency leads to false handover initiation.

On the other hand, some approaches like sensor proxy MIPv6 (SPMIPv6) [26–28], cluster-based PMIPv6 for wireless mesh networks [29], and a cluster-based proxy mobile IPv6 (CSPMIPv6) [24] employed clustering techniques to reduce the handover latency. The architectures of SPMIPv6 and cluster-based PMIPv6 for wireless mesh networks suffers from problems existing in PMIPv6 due to the centralizing the entire action via central and single LMA. The CSPMIPv6 protocol shows remarkable improvement in terms of handover latency, LMA load, and transmission cost performance compared to previous proposed solutions. The next section deliberates in detail the IPv6 essential components to enable the further deliberations on the numerous effort to constantly enhance the IPv6 solutions for WSN-IP.

1.2 Overview of Internet Protocol version 6 (IPv6)

IPv6 is an updated version of IPv4, proposed by IETF [30]. IPv6 improves several features of IPv4, such as extend the address range, provides support for real-time application (e.g., audio/video streaming), more control on level of QoS, and integrating IP security (IPsec) and support the mobility through the mobile [31, 32]. Despite all the benefits of IPv6, it still has a critical issue with respect to the actual deployment in complete. This is correlated to the time needed for mapping IPv4 to IPv6 which is largely attributed to the incompatibility with the old generation devices, for instance, the old generation infrastructure such as routers works on IPv4, which required changing their routing table [31]. The most common differences between IPv6 and IPv4 protocol in terms of their characteristics are discussed in the next subsection. It also describes a set of new features of IPv6, such as the header of IPv6, addresses of IPv6, ND, and IPv6 address auto-configuration.

1.2.1 Comparative analysis between IPv4 and IPv6

The distinct differences between IPv4 and IPv6 protocol are stated in Table 1 and explained as below.

1.2.2 IPv6 headers

The header in the IPv6 protocol is a very similar to the header in IPv4. However, some differences are made by dropping some fields in IPv4 or by making them optional in order to reduce the handling cost of the packet. This also limits the bandwidth cost of IPv6 header [30]. To learn more about the fundamental concepts of IPv6, please refer to Fig. 1.

1.2.3 IPv6 addresses

To make all nodes accessible in the network, a unique address must be assigned to each node. The length of assigned address of the IPv6 to every node in the network is 128 bits (16 bytes), whereas in the IPv4, it was 32 bits (4 bytes). This address is categorized into three subcomponents [30]: link-local address, site local address, and global address. The first one is used to limit the communication inside the node's link so the packet will not be routed outside the nodes. In the second one, a unique address is used to limit the interconnection within a specific geographical area. In the latter, a globally unique address is used to allow the packets to traverse anywhere. The address organization in IPv6 protocol is similar to IPv4 but with two main differences. The first is the length of an address in IPv6 is longer than the address of IPv4. The second is the concept of prefix used in IPv6 instead of the net-mask as in the IPv4 protocol.

Table 1 IPv4 and IPv6 comparison

Characteristics	IPv4	IPv6
Address space (source and destination address)	32 bits or 4 bytes length size of address	128 bits or 16 bytes length size of address
Checksum	Includes checksum which slows the process due to examine the IP header at each traverse router	dose not include checksum technique, which is replaced by an upper layer protocol and link layer technologies for error control and provide checksum mechanism
Header options	Header includes option	Any optional data moved to extension header
length of IP header	20–60 depending on IP option	Fixed length, which is 60 bytes and did not include IP header option
Self-configuration	Manual or use DHCP based IP configuration	Auto-configuration capability
Broadcast technique	Used broadcast to transfer the address to all nodes on its networks	Multi-cast address (link-local scope) used
Fragmentation	Applied by host and router (destination) and used the following fields for fragmentation ID, flag and offset	Just applied by the source
Mobility	Mobile IPv4 features used	Mobile IPv6 and its improvements for efficient hand-off
Map addresses	Use node addresses recorded in dynamic network services (DNS) for map node names	Use AAAA (Quad A) record in Domain Name System (DNS) to map node names to IPv6 addresses
Packet identification	Not supported	Use packets flow label field
Security	IPsec header used as a optionally service for protecting the packets	Compulsory use IPsec for safe data and control the packet
Lifetime of datagram	Used time to live (TTL) which is used to determine the lifetime of datagram on the network	Instead of TTL mechanism, hope limit used to determine the limit number of routers that must cross by the packet before it considered an invalid packet.

1.2.4 Neighbor discovery

Neighbor discovery (ND), which was proposed by [33] to discover the communication between the neighbors tethered to the same link. The ND mechanism is also used to discover the neighbor routers that are used to redirect the packet instead of nodes. An example of ND is the Internet control message protocol (ICMP) that is used for three objectives as follows: (1) to discover the neighbor routers that are attached to the same link; (2) to make the nodes learn that which neighbor routers are the best for forwarding the packet to its destination; and (3) to define and make the all the nodes and routers learn the way of mapping between the IPv6 interface and the link layer interface. This is achieved through using neighbor advertisement (NA) and neighbor solicitation (NS) messages.

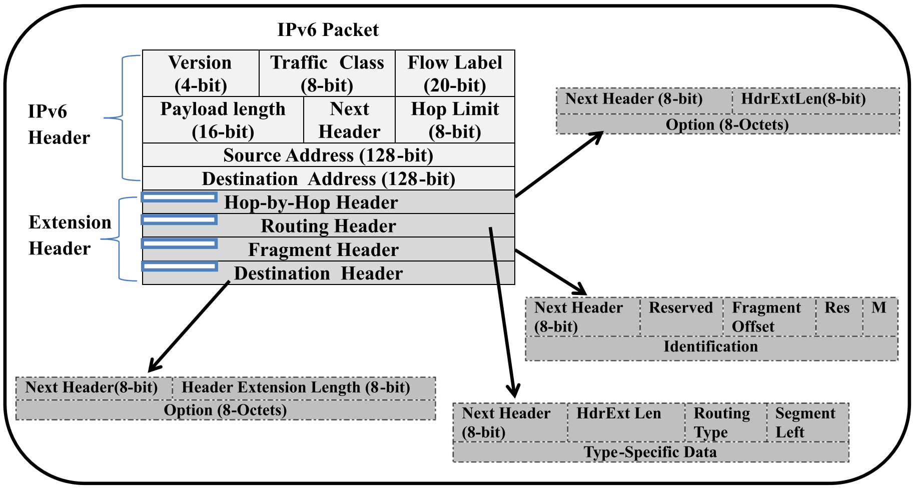

Fig. 1 Basic concepts of IPv6

1.2.5 IPv6 addresses auto-configuration

There are several new functionalities introduced in IPv6 protocol where addressing auto-configuration is considered as one of the major functionality, introduced by [30]. This functionality is used to teach the nodes the method to configure their address automatically in order to use this address as its interface to become accessible from the other nodes. This auto-configuration is divided into two types: stateful and stateless addresses. In the stateful auto-configuration, a server with database (e.g., DHCP) is used by the MN to get its address. In the stateless, that is considered a new feature for the IPv6 protocol, it allows the MN to generate its interface automatically through combining its identifier link layer prefix. This prefix address comes as a result to the advertising message from the router that is attached to the node's link.

1.2.6 Mobility in IPv6

All of these differences as mentioned earlier leads to an important question: what are the remarkable features of IPv6 regards mobility management? To answer this question, several features that make IPv6 preferable over IPv4 in mobility application is briefly listed below.

- Efficient routing is achieved by using flexible address (hierarchical) and fragmentation at source host and discover the path's of a maximum of transmission unit (MUT).
- Efficient packet processing is achieved by removing the checksum process and the options from the IP header. The checksum is put in the extension field to make IP header more flexible for mobility.
- Improved security by using the IPsec protocol achieves better security than IPv4.
- Auto-configuration helps in getting care of addresses.
- More addresses space: space to cover the high demands of addresses in the next 20 years. This is due to the vast growth of Internet devices.
- End-to-end transparency: as a result, to the vast address of IPv6, the nodes can communicate directly (end-to-end). It increases the security and performance.

  In addition to the aforementioned features, there are some other features such as easy managements, multi-cast process for using bandwidth in an efficient way (directed data flows), and scalability make the IPv6 more suitable for mobility applications.

1.3 Open issues of IP-enabled WSNs

In this section, before discussing the IP-enable evolution, the most critical challenges of integrating IP over WSNs are deliberated and demonstrated in this section.

1.3.1 Challenges of enabling IP over WSNs

In addition to the limited energy issue which is considered the main problem in WSNs either static or not static, several challenges arose, as a result to enabling IP over WSNs.

- Large size of header

  The IP messages in several routing protocols are composed of two parts: packet header and the payload (body of the message). As a result of composition (IP header and message payload in the same body), the IP header becomes as an overhead for protocol communication. As it is known, the most units in the smart sensor node hardware that consumes more power is wireless transceiver, which is used for communication. As a result, the power consumption is greatly affected when any transition or receiving occurs, even during the listening when the transceiver is idle. To solve this problem, the compression technique should be used to shorten IP header [34].
- Dedicated bandwidth

  In general, the IEEE 802.15.14 protocol used by the WSN nodes to communicate works with an approximate speed of 256 kbps. As a result of bandwidth limitation, many applications are greatly affected. It leads to the increase of the medium access delay as well as increases the time required for any other operation. To tackle this problem, the broadcast mechanism energy consumption must be minimized, if it is not possible to avoid it. The protocols must be able to transmit the primary information and drop the others. In addition, in order to make the TCP/IP optimized, the protocols should be made energy efficient [35].
- Global addressing scheme

  In order to make the node reachable from anywhere, the IP addressing for source and destination address should be acquired from a global addressing with a unique address. In the IPv4 protocol, the dynamic host configuration protocol (DHCP) server is used for generating the addresses, which cause overhead and huge traffic. However, in the IPv6 protocol, the stateless address, the auto-configuration (SSA) mechanism is used instead of DHCP [36].
- Implementation issues

  Many issues emerged during the implementation of IP over WSN, due to the limited hardware. The most critical issue is the memory, which is required to run whole IP operations. In addition, the reassembly process is needed after packet fragmentation, which is also a burden. Besides, in a wired network, the typical maximum transmission unit (MTU) of IP can easily transmit 1500 bytes. The transmission in MAC layer is 127 bytes for IEEE 802.15.14 protocol. This is because the physical layer (MAC layer) was designed for small packet size [34, 37].

- Transport protocol
  The IP routing protocol is considered a best-effort routing protocol. This means, the IP protocol does not provide a mechanism of QoS such as the guarantee of packet delivery. To achieve reliability and ensuring packet delivery, TCP protocol is used. However, the burst error rate is considered a big problem for TCP at wireless transmission on a sensor node. This is because the TCP protocol was not designed for this problem. Furthermore, the TCP was not designed for power consideration. The end-to-end communication at the TCP protocol is the reason to cause an overhead [38].

1.3.2 IP-enabled systems evolution techniques

WSNs are encompassed of hundreds or even thousands of tiny sensor nodes, which were initially used by critical such as military applications. These sensors sense and capture the data from their environment and transmit to sink node for data analysis. This network faces many barriers as a result to resource-constrained of sensor nodes. Furthermore, a huge number of contextual data are generated through sensing which require scalable and efficient technique for storage and retrieve [39]. Ubiquitous computing, where machines inter-connect with other machines to make a decision instead of human, becomes feasible and a reality as a result of using IP-WSN for sensing and collect the data on behalf of the user. In this section, we present an overview of IP-WSN approaches that have been recently presented. Methods and approaches for integrating the IP with WSNs are discussed to make the interconnection between the WSNs and other IP networks feasible. Benefits from the existing infrastructure and IP-application for cohesive connectivity with sensor networks are also covered [24]. Mainly, there are two main approaches used to connect WSN with IP networks, namely, sensor node stack-based and proxy-based [40]. In the first approach, every sensor node has an IP protocol stack implemented as a routing protocol. It allows sensor nodes to send and receive the data from/to other networks. In the latter, the second approach uses serving network (sink node) as a gateway to exchange the data between the sensor nodes and Internet. The details of two aforementioned approaches are also reported herein. Recently, the network-based management has gained considerable attention and focus in the world of research. The main objective of network-based management is to reduce the HO latency when the MN moves between sub-networks. In order to reduce the HO latency, several protocols have been proposed. HO latency is the discipline which investigates the principles, protocols, and infrastructures for developing a convenience protocol to reduce the HO latency. In this section, we will discuss some related works related to IP-WSNs, beginning from the base works dedicated IP stack to recent works related to real deployment, passing through the IP-WSNs stack. The advantages and disadvantages of existing works will also be highlighted.

1.3.3 IP-enabled techniques

The micro IP (uIP) and lightweight IP protocol (LwIP) TCP/IP stack are the first works for implementation of a complete TCP/IP stack for smart sensor nodes which was proposed by Adam Dunkels [41]. The uIP protocol was proposed in general to gain benefits of an IP-enabled architecture by implementing a full TCP/IP stack for small memory size and low-processing power of WSNs. It integrates with 8-bit systems and 16-bit systems to connect the WSNs with IP networks, while the LwIP developed as a larger footprint to be convenient for more capable systems. Both introduced protocols are compatible with a subset of RFC1122 document [42] and the implementation of the feature Internet Protocol (IP), Transmission Control Protocol (TCP), and Internet Control Massage Protocol (ICMP). LwIP support changing the IP address dynamically and manage more than one local IP address per device with User Datagram Protocol (UDP) support. Nevertheless, the limits of an 8-bit micro-controller and 16-bit micro-controller, a possible implementation a full TCP/IP, was not easier for tiny WSNs. Intrusion mentoring is the first approach to implement IP-based WSN with low-processing and tiny smart sensor nodes, which was presented by Adam Dunkels et al. [43]. The infrastructure network uses the embedded sensor board (ESB), produced by Freie Universitt Berlin (FU) as a platform [44]. The applications used the FU Berlin mote platform, a full uIP stack, and the Contiki operating system developed by SICS which runs on each node [45]. The objective of this protocol is movement detection. The authors used sensor location coordinator a unique IP address assignment for WSN address configuration. The smart WSN transmits alert message to the central station, which is a PDA in this work when the intrusion is detected. The PDA replicates and distributes the events to all nodes in the network to provide them with logs for all recent alarm events, so every node will have a complete knowledge of all recent events of all other nodes within its network as well as keep the building under monitoring continuously.

Body sensor network (BSN) protocol is used in a network where smart sensor nodes are deployed on a human body to monitor body signals in an unobtrusive scenario. It can also take advantage of IP-based motes [46]. A BSN plays an important role to envision the notion of mobile health (M-health). During daily routines in an individual's life, sensor networks can be used to capture one's activities and movements, hence, enabling the health in motion

[47, 48]. A platform integration of a true ubiquitous mobile health system requires a technology that may be provided by integrating mobile computing and body sensor networks. The smart node makes use of the TinyOS operating system that uses IEEE802.15.4 under uIP stack. They are also characterized by constrained flash memory which enable continuous disconnected operation. The traditional BSNs are not suitable for all applications due to using application-dedicated data transmission protocols. Besides, electromagnetic interference (EMI) will arise during the transmission of radio frequency between the medical sensors [49].

Due to the shortcomings in the traditional BSNs, the scholars at HP labs introduced on-body sensing data networks that used a full TCP/IP stack and TinyOS over IEEE 802.15.4 wireless [47]. This network connects the smart sensor nodes, which are deployed in a human body with aggregators as shown below in Fig. 2. The aggregator that has more capability acts as an access point used to receive the captured data from the low-power WSN and transmit it to the global Internet when the connection becomes available. As a result to using the BSNs technology, several challenges are bring out such as energy efficiency, scalability, interference mitigation, QoS, and security, which are highlighted in [49]. Various algorithms proposed to achieve energy efficient, security, and routing optimization [50–56]. Moreover, the authors in [57] proposed protocol to solve the interference issue during the channel assignment with topology preservation.

Camilo T. et al. [58] developed an IP-enabled model named IPSens for wireless mish sensor networks (WMSN) to enhance mobility. In this paper, the authors exhibit clearly the various myths associated with the use of IP over WSNs. The proposed IPSens model used access point (AP), access router (AR), and sensor node (SN) concepts used in the IPSens model. While the sensor nodes grouped into clusters, each cluster managed by the AR that has complete information about the membership of it. The AR acts as a gateway between sensors members and the AP. Here, the AP acts as an edge router to connect the sensor nodes with other IP networks as demonstrated in Fig. 3.

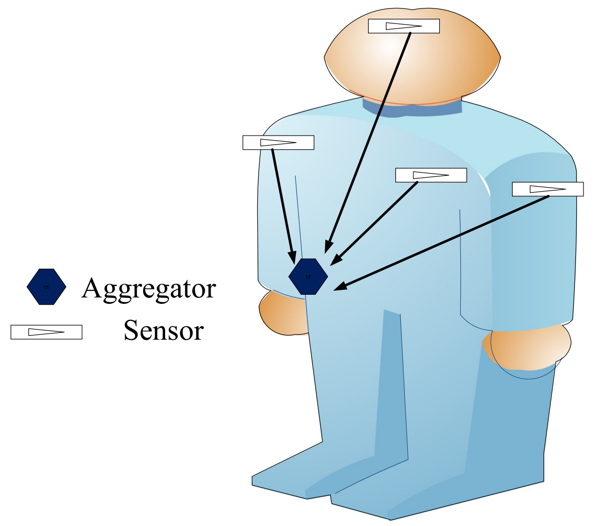

Fig. 2 Body sensor nodes (BSN) configuration

In [59], the authors made comparison between IPv4 and IPv6 to address the issue of IP in WSN. The comparison made was based on the Contiki operating system over ESB nodes. Despite the IPv6 has a large range of IP address space, however, it may cause a lot of overhead when compared with IPv4 as a result to its fixed length 128 bits addresses with 40 byte header. Moreover, they demonstrate that the IPv6 have a trivial effect than IPv4, and that IPv6 is preferable, and beneficial to use as a result of its higher functionality and the simplicity of header compression. To enhance mobility and take advantages of IP-enabled technology for connecting WSNs with IP networks, it is essential that protocol should be lightweight. This will consume less resources for WSNs.

IPv6 over low-power wireless personal area networks working group (6LoWPAN WG) prototype is introduced by 6LoWPAN working group from IETF [15]. 6LoWPAN play a key role to facilitate the use of IPv6 functionality over IEEE802.15.4 standard. The key characteristic of 6LowPAN is to allow connectivity among limited power devices by mapping the IPv6 capability (e.g., ND) with low capacity devices. The physical (PHY) and media access control (MAC) layer defined in IEEE802.15.4 standard are adopted by 6LoWPAN protocols to make them as its PHY and MAC layer. The main objective behind the 6LoWPAN development is to reduce bandwidth consumption, packet size, power expenditure, and processing requirements [60]. Due to adopting the IEEE802.15.4 standard under IPv6, two problems arise: header overhead of IPv6 and low payload IEEE802.15.4. To solve these issues, adaptation layer has been added between the network layer and MAC layer. 6LWPAN uses compression mechanism to solve the first problem mentioned before. And the latter, fragmentation mechanism, used to divide the IPv6 datagram into suitable IEEE802.15.4 frames.

Another work introduced by [61] used a full IPv6/6LoWPAN architecture network over a tiny, low-computational, and low-memory WSN. The authors of this work made several considerations on the use of a complete IPv6 over low-power WSN which was implemented on a real-world application. There are three basic services in the IP-network layer: (1) configuration and management, (2) forwarding and and (3) routing which are explained by the authors in this work to provide valuable knowledge. The authors also used TinyOS 2.x

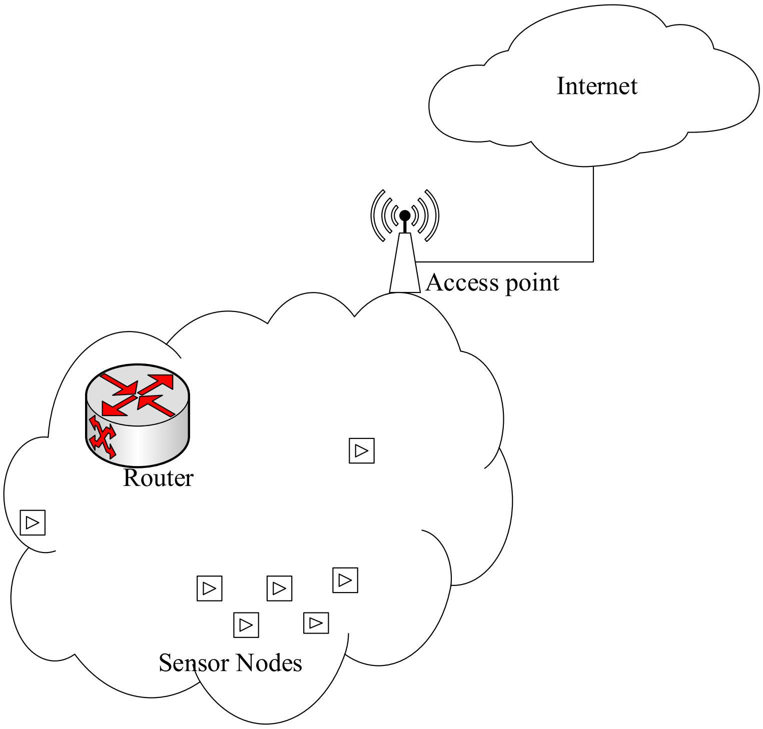

Fig. 3 Sensor router concepts [58]

operating system [62] on TelosB motes from Crossbow technology [63] to evaluate the IPv6 architecture for low-power WSNs. Approximately, 23.5 kB of memory and 3.5 kB of RAM is consumed to implement a UDP socket and a TCP connection. The implemented IPv6-based architecture outperforms the existing architecture systems that does not conform any particular architecture or standard regarding efficiency.

Another protocol is uIP (IPv6) which is proposed by [64] to leverage the micro uIP (IPv4). The major aim of implementing a full IPv6-based protocol for tiny, low-power, and low-memory WSNs is to design a uIPv6 protocol for inter-operable end-to-end communication between IPv6-enabled smart sensor nodes and any IPv6 capable host, connected to the Internet. The uIPv6 is implemented and integrated into ContikiOS similar to uIPv4 protocol. The TCP/IP stack, integrate IP packet datagram on IEEE 802.11 or IEEE 802.15.4, and link layer protocol (Ethernet) are services provided by this software layer to the applications in the context platform. Regardless of the MAC and link layer types, the uIPv6 protocol can by be applied efficiently. The uIPv6 stack required less than 2 kB of RAM and 11.5 kB of code size to present Transfer Control Protocol (TCP), User Datagram Protocol (UDP), IPv6 addressing, Internet Control Message Protocol (ICMPv6) and Neighborhood Discovery (ND). Based on the analysis and evaluation of interconnection between IP networks for both inter and intra-communication with 6LoWPAN, significant overhead is noticed when the data is transferred between various networks [65]. This is generally a result of fixed address.

6GLAD architecture presents a twice-network address translation (NAT) plus reverse network address translation in order to overcome the aforementioned problem of the fixed address [65]. This is particular when the IPv6 world-wide addressing was needed and this new architecture was proposed, named, 6GLAD by [65]. Avoiding overhead and exploiting the 6LoWPAN functionalities are major benefits from the 6GLAD architecture. The total of overhead communication reduced up to 88.89 %, due to the integration of 6LoWPAN architecture and 6GLAD architecture. The reduction provided by twice-NAT comes as a result of amendments of both IP source addresses and IP destination addresses. WSNs gateway between IPv6 global address and link-local address enables the use of short range addresses in low-memory and low-power sensor nodes. In addition, it allows the external hosts on the Internet to reach the internal nodes. For validation purposes the network simulator-2 (NS2) was used to deploy the respective experiments.

In addition to the aforementioned protocols, there are several other works and standards which were proposed such as dual addressing scheme (DAS) [66], ZigBee-based [67], tree-based routing algorithm (ETRA) [68], the LoWPAN Network Management Protocol (LNMP) management architecture [69] and a configurable tiny TCP/IP protocol stack featuring Session Initiation Protocol (SIP) [70]. Moreover, the protocol in [71] designed a new method to facilitate wireless connectivity based on the IEEE 802.15.14. The main aim of this protocol is to enable communication and data transformation between IP-WSN devices and IP-network.

These protocols have served as a foundation and motivation for the integration of WSN-IT further harnessing the IoT terminology to become evident and prominent. However, these protocols still suffer from several challenges as a result to the constraint of the WSNs. Limited bandwidth, limited power, header overhead, addressing space scheme, and transport protocol are considered as among the most important challenges of using IP-WSN. These challenges must be taken into account when IP-WSN is used. Many researches have been proposed to addressed these challenges such as IP-Header compression, which reduce the packet address overhead as well as the power transmission. Another research direction focuses on using UDP instead of TCP in order to reduce the power consumption and bandwidth overhead by removing the required acknowledgement that notify the transmission point about the successful reception [72]. Besides, in [73] stateless auto-configuration is suggested instead of DHCP in IPv4 to preserve the power consumption. Moreover, these protocols lead to the consumption of the MNs power in fast manner especially, in the large network. This is due to using the multi-hop communication to send the packet to the destination [74]. Thus, the authors in [75] proposed an approach to maximize end-to-end throughput in multi-hop WSNs with special consideration to spatial reusability of the WSNs communication media or clustering technique as in [76] in order to limit the barriers of using multi-hop WSNs. These challenges keep the door open for the future researchers to enhance the aforementioned protocols and make them appropriate for high-level degree of QoS.

All these protocols are designed in order to adopt IPv6 stack over tiny, dedicated memory, and low-power WSNs efficiency. These constraints greatly effect the security, due to moving the data through slower, less secure wireless media [77]. The aforementioned solutions make ubiquitous computing a reality. IP-based smart tiny WSNs have made their impact in WSN future IoT and ubiquitous computing. This is due to the evolving WSNs towards IP-WSNs. Mobility within the IoT is experiencing rapid growth due to the proliferation of the applications. Therefore, mobility management protocols has become an essential part to manage the hosts while roaming between sub-domains. This roaming may be intra-communication when hosts moving inside the same domain or intercommunication when hosts moving between different domains. The mobility management protocol can be divided into two different parts: host-based mobility (implemented in the host itself) and network-based mobility management (implemented in the proxy-router) depending on the application scenario at hand. In resource-constrained WSN, proxy-based mobility is more suitable, since it releases the sensor nodes from any mobility-related signaling which extends the network lifetime.

The MIPv4 architecture is the first breakthrough to address, the IP management, and was designed and produced by the IETF [32]. The main aim of developing this protocol is to make the nodes continue connecting to the networks, even when they are in movement mode. The HA, FA, CoA, CN, MN, MBT, and VL are new terminologies introduced by MIPv4 which are already stated in the previous section as shown in Fig. 4. The key role of HA ensures that the local MN continue connecting to CN even when the MN is roaming. This is done by keeping the MN information on its MBT. The CN located on the global Internet is the node that MN communicates with. The FA located in a different network in which MN moves to, the FA assign CoA to MN when it arrives, keeping the information about the registered MN in its VL. When a datagram to an MN arrives on HA via IP routing protocol, the HA fetches on its MBT, to check whether the target MN is on its domain. If yes, the HA directly sends the datagram to the MN, else the MN CoA used by the HA to encapsulate the datagram and deliver it to the FA, through the IP routing protocol. After the datagram is delivered by the FA, the FA fetches the CoA on its VL, the FA de-encapsulate the datagram and forwarding the received packets to the MN. In the opposite direction, the FA sends the datagram coming from the MN to the CN using conventional IP routing protocol or using a directed tunnel between FA and HA (FA-HA tunnel).

Router advertisement messages (RA) are periodically broad-casted by the HA and FA to detect any changes in their existing MNs inside their networks. Whenever, the MN changes its point of attachment, it can wait for a router advertisement message. In the other case, MN periodically broadcasts router solicitation (RS) rather than waiting for router advertisement messages from the new FA.

Despite there are benefits occurring as a result of using the MIPv4, however, there exist several drawbacks, such as long communication routing protocol (triangular routing) due to the dependency on the HA to send and receives the packets through it between MN's CN and MN. Therefore, extra time is needed to deliver the packets to their destination, due to the triangular routing problem, putting extra burden on the network entities. Furthermore, all the packets on-the-fly will be lost during the handover process because the new visited network cannot

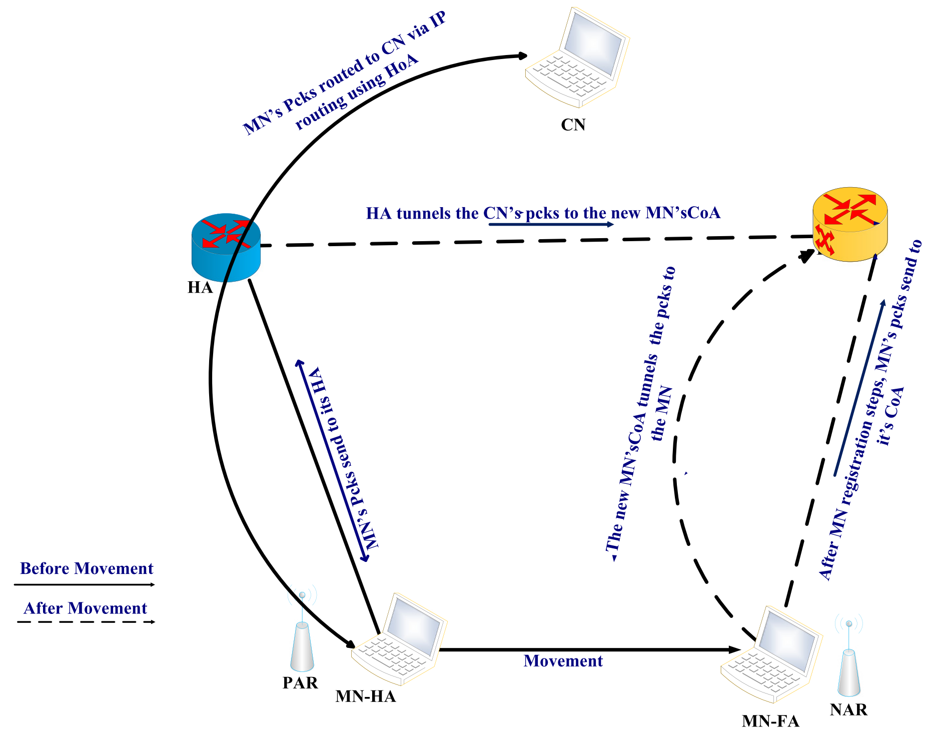
MN's Pcks routed to CN via IP routing using HoA
CN
HA tunnels the CN's pcks to the new MN'sCoA
HA
MN's Pcks send to its HA
The new MN'sCoA tunnels the pcks to the MN
After MN registration steps, MN's pcks send to it's CoA
Before Movement
After Movement
PAR
MN-HA
Movement
MN-FA
NAR

Fig. 4 Operation of MIPv4

inform the old visited network about the movement of the MN.

MIPv6 protocol, developed by the IETF working group [18], helps to resolve the issues that arise in MIPv4. MIPv6 is derived from MIPv4 architecture. The functionality of IPv6 is more capable and easier to implement and solves numerous limitations existing in MIPv4 limitations, supporting the efficient mobility management for MN. MIPv6 allows a MN to roam within the MIPv6 domain without losing or corrupting any of its connections with CN, whereas MIPv4 protocol suffers from the long routing protocol due to the dependency on the HA and FA to deliver the datagram between the MN and its CN. This is due to the fixed address home of address (HoA) given by the HA to the MN, to maintain the MN accessible by its CN at anytime, anywhere. Moreover, all the packets will reach to the MN by the normal routing protocol without any modification if the MN is still in its home network. The MN will be reachable by the provisional CoA given by the new visited network that MN moves to, and the MN will not be accessible any more by the HoA. Moreover, in the MIPv6 the HA intercept all the flying packets to the MN's HoA and redirects the packets to the current MN's CoA. Thus, the MN must update its HA on its current visited network (CoA). Accordingly, all the MN's packets which are received by the HA are redirected via tunnel to the MN's HoA to its visited network (CoA). Therefore, directly tunnel ends used to transfer the data between the MN and the MN's HA, unlike the MIPv4 that used the FA. Additionally, the MIPv6 solve several limitations in MIPv4 such as a triangular routing problem and enhance the performance of the network by introducing route optimization scheme. This can be done through exchange message query response between the MN and its CN, to establish a secure and direct connection, to improve the routing between the MN and its CN in the MIPv6. Thus, no more interception is experienced by the packets traveling between the MN and its CN by the HA. This improvement makes the network more secure and reliable and minimizes the network load [18]. Furthermore, the packets that are sent by the MN to its CN are delivered to the MN'sCN address directly.

In spite of the benefits associated with this protocol, it is still not appropriate and desirable to be deployed in real implementation due to the following factors, including intense packet loss, intense signaling, and long handover latency. Furthermore, every time the MN moves to a new sub-domain, it must update its CoA to its HA and MN's CN without any consideration to the mobility if its local or global. Moreover, building an IPv6 tunnel cause extra overhead and as a result requires an additional IPv6 header [78]. Due to these limitations, that make the users dissatisfied, especially for the real-time applications such as VoIP and audio /video streaming, so several investigations [79] and mobility enhancement protocol appeared such as FMIPv6 [22] and HMIPv6 [21] to improve the MIPv6 performance.

To overcome the weaknesses of MIPv6, an enhanced protocol was introduced by [22] and named, fast handover for MIPv6. This protocol prevents the service disruption when the MN in motion and also helps to minimize the needed time for MN to move between the sub-domains during the handover associated with MIPv6 (handoff operation time). In the FMIPv6, the MN's are relieved from any mobility signaling by carrying out the handover signaling burden through the FMIPv6 entities which are previous/old access point (PAR), new access point (NAR), and HA. The FMIPv6 have two kinds of handover operation, namely, predictive handover and reactive handover. In predictive handover, when the MN's change the link layer of attachment between the two access points, they are triggered by the link layer , whereas reactive handover is triggered by the network layer and it happens when the MN's moved out the current access network range (L3 handover). In general, the main idea behind the development of FMIPv6 protocol is that when the MN initiates the L2 handover with NAR, the NAR will initiate the L3 handover with PAR. So, a bidirectional tunnel will be established between the NAR and PAR before completion of the L2 handover between the MN and the NA. This reduces significant time in the handover process. In the latter, a bidirectional tunnel will be established between the NAR and PAR, but this will happen after the completion of handover between the MN and NAR. In addition, to reduce the packet loss during the handover operation, buffering technique is used in either NAR or PAR or both of them together. Thus, after completion of handover process, the buffered packets are forwarded into the MN.

Despite all the issues related to MIPv6 which are resolved by the FMIPv6, the FMIPv6 still suffers from some limitations such as reordering the packets due to using multi-paths to forward the packets into the MN. Despite the fact that packet tunneling and buffering techniques minimize the packet loss during MN's movement, particularly for constant bit rate (CBR) services, however, they add extra processing and increases the load on the network link between NAR and PAR. This is due to the consecutive tunneling and de-tunneling of the buffered packets. The reliable and accurate tunneling between the NAR and PAR is dependent on the availability of a trigger and the appropriate handover decision timing. Some other well-known problems associated with this protocol include high handover latency and intense signaling.

NEMO is another protocol extends the MIPv6 [19]. The main objective of this protocol is to support the mobility for all MNs in the mobile network, by the mobile router (MR), as well as keep the MN's in the mobile network continuity accessible even when they are in movement. So, all the signaling and tunnel configuration related to mobility management is taken care by the MR instead of the MNs. The nodes have their IP addresses associated with the mobile network prefix (MNP) of the NEMO which is located at the home agent of the mobile router. For route optimization support, NEMO basic support (B.S) has no specific standards. With respect to mobility, the NEMO B.S is based on mobility functionality comprised in the mobile node which is a router in this scenario. In order to minimize the signaling cost between the 6LoWPAN MR and the 6LoWPAN access gateway, a compressed mechanism used by the Lightweight NEMO protocol was introduced by [80] to compress the mobility header. Nested [81] has been introduced to solve the MN movement, where it moves to another mobile or static network.

A new scheme protocol called the HMIPv6 local mobility management was proposed by [21]. The aim of this protocol is to enhance the MIPv6 architecture so as to reduce the signaling overhead and handover latency that occur during the handover mechanism. For this reason, the HMIPv6 architecture added a new entity named, mobility anchor point (MAP). This new local entity which addressed by a regional CoA (RCoA) has the capability to support several access routers (ARs). These ARs are responsible for determining the coverage area of the MAP and using the broadcast mechanism to announce itself continuously. Two CoAs associated with the MNs in the HMIPv6 protocol: RCoA and local care of address (LCoA). The RCoA address is used to make the MNs accessible, while MNs roam within the MAP network. On the other hand, the LCoA address is used to make the MNs accessible when the MNs are inside the visited network. Roams inside the MAP domain is called intracommunication (local mobility), whereas roams between different MAP domains is called the intercommunication (global mobility). The hierarchical addressing allows MNs to roam within the MAP domain, without the need to inform neither their HAs nor CNs.

The sequence processes of the HMIPv6, as depicted in Fig. 5, are illustrated as follows. A handover process will be applied by a MN to disconnect from a previous AR (PAR) and connect to a new AR (NAR). The MN must send a binding update (BU) message to its HA and CN to inform them with its new CoA, this message will go through a MAP to reach the HA/CN. The response message of BU from the HA/CN also will go through the same way to reach the MN. If the MAP located far away from the HA/CN, this will definitely cause time delay that required to deliver the BU message in both directions between the MAP and HA/CN. Due to the aforementioned drawback, it is logical to have a provisional HA on the MAP. Thus, when the MN roams in the same MAP domain, it only needs to update the MAP, then the address of the MNs in this case is LCoA. The time that was needed for traveling

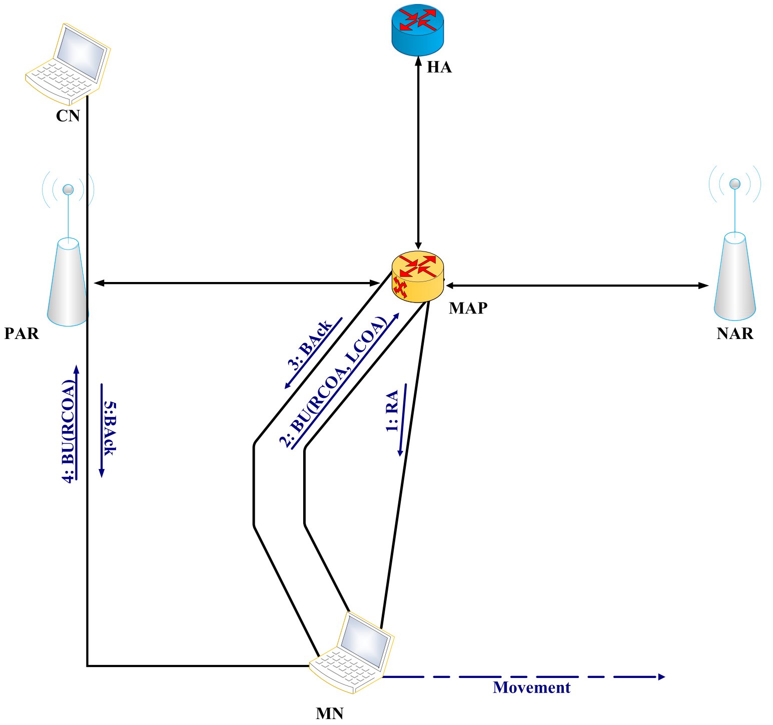

Fig. 5 HMIPv6 signaling scenario

a BU message between the MAP and HA/CN is eliminated. In general, the HMIPv6 is more efficient and more desirable for intra-communication than the MIPv6. Due to this, the hierarchical addressing handles the MN registration rather than the global IP communication in the MIPv6 network.

In general, all the host-based protocols would not be a preference in selection for the IoT especially as the devices are highly constrained in terms of power, memory size, and the processor. The lack of preference comes as a result of the involvement of MN in the mobility process which leads to increase the MN complexity and wastage on air resources. Furthermore, these protocols suffer from several issues such as intense signaling, long handover, and high packet loss which lead to degradation in the level of QoS.

To overcome the drawbacks associated with host-based protocols, proxy-based protocols are presented and proposed by the IETF working group such as PMIPv6 and its extension schemes and protocols such as SPMIPv6 and CSPMIPv6. To meet energy efficiency requirements, proxy-based protocols relieve the sensor nodes from any mobility-related management in handoff process, in order to reduce the signaling overhead, signaling costs, and handoff registration during the HO process. These protocols are covered in this section.

PMIPv6 is implemented and designed by IETF to settle mobility challenges associated with network management at the network layer [23]. The standardized protocol is created to support network-based localized mobility management, which makes the MN free from any IP-mobility-related signaling when the MN roams, hence, the proxy mobility functionality take the burden of all the mobility-related signaling instead of MN, unlike the MIPv6 protocol. PMIPv6 is derived from MIPv6 by reusing some functionality (ex. HA) and extending the signaling. To make the MN free from any involvement in mobility-related signaling when the MN in motion, the PMIPv6 added two novel entities named, LMA and MAG. The key characteristic of LMA is to maintain the IP-interface of MN to continue connecting with the ongoing session even when the MN roams between sub-domains. From the viewpoint of MN, the PMIPv6 domain seems it as home network, while the key role of the MAG which has some capability is to support the interface connectivity in the PMIPv6 domain. Once the MN attaches the MAG domain to the PMIPv6 domain, the MAG (serving network) triggering the required signals to register and authenticate the MN and allocates a unique home network prefix (HNP) to every MN using per-MN-Prefix addresses model as illustrated in [23] documents. The good thing of using this prefix address is to make the MN feel always that the entire PMIPv6 domain is a home network and can get its home-of-addresses (HoA) on any access network. This is achieved by making the MN prefix following the MN wherever the MN roams in the PMIPv6 domain. It is unlike the MIPv6 in which there is no need to configure the CoA in the MN. For more details about the PMIPv6 works and its terminologies the work by [23] can be reviewed.

Despite the benefits that the PMIPv6 gives, like reducing the handover and reducing the time needed for signaling update comparing to MIPv6, still, it suffers from several limitations due to the triangle routing protocol between the MN, LMA, and CN [82]. This centralization leads to degradation of the quality of services (QoS) that is a necessity for sensitive applications such as video/audio applications and VIOP. Furthermore, PMIPv6 suffers from another barrier which is the limitation of MN on its domain. This could be a problematic for IoT equipment which uses diverse applications [83, 84].

1. LMA: All the datagrams that are sent/received between the MN and the CN must pass through the LMA. In other words, the key target of the LMA is to keep the MN reachable during the handoff process through updating the binding cash entry (BCE) for each new MN registered. Furthermore, to complete the PMIPv6 registration domain, the LMA is responsible to register and authenticate every MAG in the PMIPv6 domain.
2. MAG: the MAG plays an important role to manage the MN connection on behalf of the MN. The MAG is responsible for detecting the MN attachment/detachment process.
3. MN: the MN is every node that communicates through LMA in the PMIPv6 domain.
4. CN: the CN is the node that receives and sends the datagrams to the MN through LMA entity.
5. Proxy binding update (PBU) and proxy binding acknowledge (PBA) are used by the MAG and the LMA to update the LMA's BCE table to authentication the register/de-register of the MN. For more details, see Fig. 6.

The SPMIPv6 protocol, proposed by [26–28], is the first protocol that works on smart sensor network-based localized mobility management (SLMA), particularity focusing on energy efficiency. The SPMIPv6 is derived from the MIPv6 architecture with the ability to make the distinct WSN interconnecting via shared backbone architecture. In this work, the main objective of sensor localized mobility anchor (SLMA) is to maintain mobile node reachability when the MN roams between the SPMIPv6 domains. This reachability is achieved by maintaining information in the binding cash entry (BCE) for every MN registered. Additionally, SLMA exhibit authorization, authentication, and accounting (AAA) services to reduce the number of messages needed for MN registration, while the sensor mobile gateway (SMAG) acts as an edge router to detect the MN movement and interchanges the messages required with SLMA instead of a sensor MN. This solution is slightly improved regarding packet transmission cost and signaling cost when compared with MIPv6 and PMIPv6. Despite the benefits offered, the SPMIPv6 still suffers from limitation such as long handoff latency, LMA overhead, router optimization, and central point failure as a result of relying on single and center LMA [24].

The protocol [24] presents an enhanced architecture to SPMIPv6 named, cluster sensor PMIPv6 (CSPMIPv6) architecture. This enhancement attempts to tackle the bottleneck issues in SPMIPv6 and PMIPv6 protocols by dividing the proxy mobile domain into sub-local domains as shown in Fig. 7. Each sub-domain groups MAGs into clusters, each cluster being managed and controlled by cluster head (HMAG). This architecture consists of an LMA, MAG, HMAG, MN, and CN. In the CSPMIPv6 architecture, the LMA and MAG functionality are similar to LMA and MAG in PMIPv6 protocol, while the key characteristic of the head MAG (HMAG) is to relive the LMA from any local mobility management. Furthermore, the HMAGs provide the AAA technique to reduce the signaling cost for mobile node registration. Also, the HMAGs reduce the handoff latency and provide rout-optimized path in intra-communication mobility. Regarding the handoff latency, LMA dependency and packet transmission cost the CSPMIPv6 is superior to PMIPv6 and SPMIPv6 protocols. Figure 7 depicts the operations that are needed to register the MN within the CSPMIPv6 protocol as well as the movement scenarios. The MN goes one or more of the three scenarios, during its movement within the CSPMIPv6 sub-domains.

The first scenario is called initial registration. The steps of the MN initial registration are illustrated as follows:

1. When the MN1's attachment is detected by the MAG1 in the CSPMIPv6 domain, the MAG1 triggers the access authentication procedure by using the MN1 Identifier (MN-ID).
2. The MAG1 sends a request message local proxy binding update (LPBU), on behalf of the MN1, to the HMAG1 to inform it about the new location of the MN1.
3. Then, the authentication is performed by the HMAG1. Upon authentication success, the HMAG1 sends a request proxy binding update (PBU) message to the LMA containing the MN1-ID and the HMAG1 address.
4. When the LMA receives the PBU message, the binding cash entry (BCE) will be updated by entering the new MN1 information. After that, the LMA

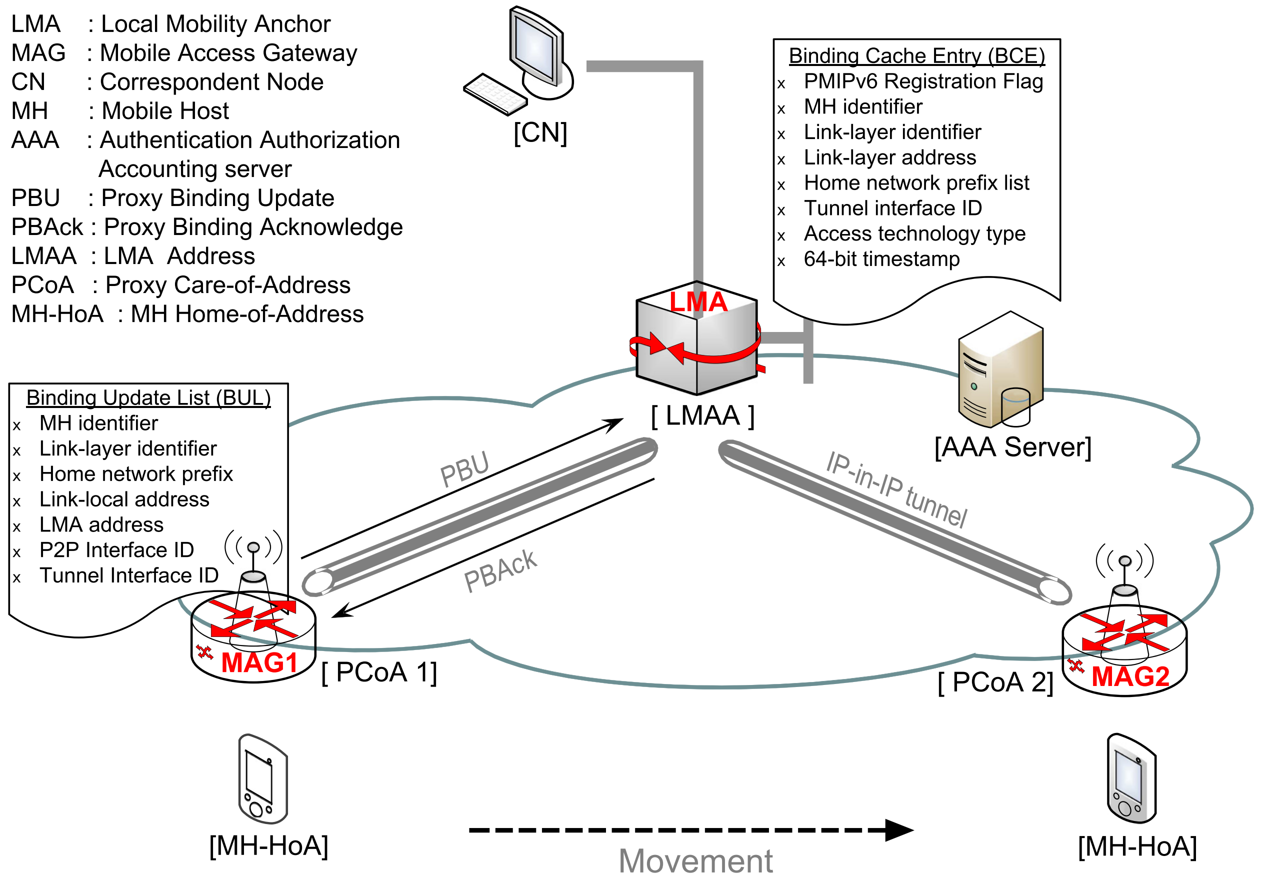

Fig. 6 Basic concepts in PMIPv6 [135]

sends a proxy binding acknowledgement (PBA) message to the HMAG1. The PBA message contains the MN1-HNP which will be used by the MN1 to keep its connection. Then, the LMA establishes a bidirectional tunnel with the HMAG1.

5. Upon receiving the PBA by the HMAG1, a binding update list (BUL) table is created in order to register the MN1. Afterwards, the HMAG1 sends a local proxy binding acknowledgement (LPBA) message to the MAG1 which provides the prefix address of the MN1.
6. Once the MAG1 receives the LPBA message, a BUL table will be created by the MAG1 to maintain the MN1 information and to register the MN1 as well. Furthermore, the MAG1 emulates the new prefix address to the MN1 through an RA message.
7. Finally, when the MN1 receives the RA message successfully, it will re-configure its IP address based on the new MN1-HNP address using either stateless or stateful configuration. Then, the MN1 will be able to send and receive the packets using this address.

In the second scenario which is named an intra-HMAG mobility is explained as follows:

1. When the MN1's attachment is detected by the MAG2 in the CSPMIPv6 domain, the MAG2 triggers the access authentication procedure by using the MN1 Identifier (MN1-ID).
2. This step remains the same as in scenario one.
3. In this step, once the HMAG1 receives a LPBU message, it checks its BUL table to see if the MN1 is a member on its list. If the HMAG1 find the MN1 entry, it sends a LPBA message to the MAG2 without any intervention from the LMA.
4. The MAG2 emulate the MN1-HNP which is the same to the previous one to the MN1 through a RA message.
5. In the final step, the MN1 re-configure its IP address and use this IP address to continuously send/receive the packets.

In the third scenario which is called, inter-HMAG mobility is performed as follows:

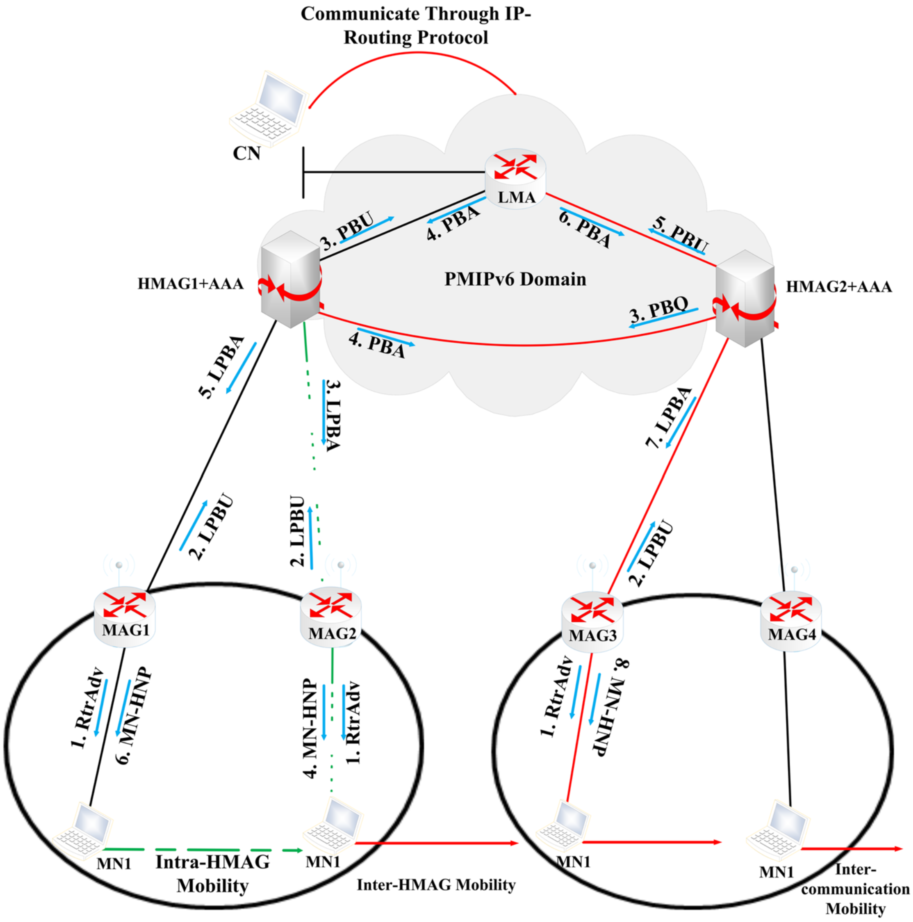

Fig. 7 Registration scenarios in CSPMIPv6 domain

1. When the MN1's attachment detected by the MAG3 in the CSPMIPv6 domain, the MAG3 triggers the access authentication procedure by using the MN1 Identifier (MN1-ID).
2. This step remains the same as in scenario one.
3. In this step, once the HMAG2 receives a LPBU message, it checks its BUL table to see if the MN1 is a member of its list. Since the MN1 does not exist in its list, so it will send a proxy binding query (PBQ) message to the whole HMAGs neighbors.
4. The HMAG1 in this step, when receives the PBQ, sends a PBA replay message to the HMAG2, including all the information about the MN1 connection.
5. Finally, a tunnel is created between the HMAG1 and the HMAG2 once the HMAG2 receives the PBA.
6. In this Step and Step (7) the HMAG2 sends a LPBA to the MAG3 as well as sending a PBU message to the LMA to inform it about the new location of the MN1.
8. In this step, upon receiving the LPBA by the MAG3, the MAG3 sends the MN1-HNP to the MN1 through an RA.
9. Finally, this Step is similar to Step (7) of the first scenario.

Although, the CSPMIPv6 suffers from several limitations including single point of failure and handoff latency, as well as its derived the aforementioned bottlenecks in SPMIPv6 due to relying on single and center LMA for the CN while establishing the tunnels. Furthermore, this solution is not appropriate to be applied in large-scale networks due to its static tree-based structure networks [85]. Moreover, adding a new entity leads to increase the signaling and the end-to-end delay, especially in the inter-domain mobility. Finally, the message broadcast between the HMAG to identify the new location of the MN wastes the air resources, especially in such networks where their MNs move all the time such as the highway roads and trains.

Despite all the improvement that evolved from one protocol to another, still the required level of QoS is not achieved. This is due to the intense signaling, point of failure, and handover delay during the MN motion. Some of these barriers degrade the network performance such as HO delay and point of failure, whereas high signaling leverage the power consuming, which demands extra handling from the network side, as well as with slight intervention of IP-WSN as possible.

Moreover, when the MN moves between sub-domains, its prefix is changed to specify the new location of the MN. Thus, the broadcasting RA sends in a periodic manner to discover this movement which increases the signaling in the network. Besides, using the buffering technique during the MN movement prevents the packet loss and leads to extra overhead on the network entities. The buffered packets should be tunneled to the MN through the new point of attachment. This tunneling process leads to increase in the power expenditure and signaling cost due to using a lot of control information by the MN [86]. These protocols also do not consider the duty cycle when the MN state in the hibernation mode to leverage the power. Furthermore, the network-based protocols do not consider the multi-hop communication between the edge router and its node, and thus the MN consumes high power to send the packets to the edge router, especially when the router is so far from its node.

1.3.4 Mobility-related works

The work by [87, 88] was introduced to enhance the mobility by minimizing the time needed by the MN to change point of attachment between two local domains (PMIPv6-domains). This enhancement was done using the overlap function of MAG, named overlap-MAG, to fill the overlap area between two PMIPv6 local domains in order to maintain the MN session continue without any service disruption. The main aim of the overlap-MAG function is to detect the MN movement and do registration on behalf of the MN (inter-domain handover).

In order to achieve the lowest signaling costs, the PA-NEMO protocol proposed by [89] combines the PMIPv6 network-based protocol with NEMO protocol. Address mapping approach is used by the PA-NEMO protocol to support an efficient mobility even with nested scenario. In synchronously fashion, the mapping cash list (MCL) was kept by both MR and MN's HA.

The destined packets to the MN should pass through a MN's HA. Firstly, to execute the mapping address, then the packets redirected through a tunnel between LMA and MAG to reach the MR's MN to execute the inti-mapping. Finally, the packets are forwarded to their destination. in order to reduce the cost of devices. This protocol started transmission tunnels out of 6LoWPAN region.

Another work to improve mobility has been presented by [90], called overlay enhanced mobility for the IoT. To achieve this enhancement, the researchers leveraged the sensor as endpoints. This is applied to support the sensor and host-mobility separately. DHT-based chord [91] is used to implement this strategy. Furthermore, it is used to store the mapping of IDs and location of sensor nodes.

Another recent protocol which is compatible and suitable for IoT-devices is presented by [92], called lightweight MIPv6 with IPSec support protocol. The main goal of this protocol is to present an optimal solution for dynamic ecosystems in terms of efficiency and security integrated with resource-constrained devices (IoT-devices). Furthermore, this protocol has awareness about the IoT requirement. It concludes and proofed that the integration between MIPv6 and IPsec for restricted-devices is feasible despite all the cons of this protocol in terms of intense overhead and large memory requirement.

1.4 Mobility in wireless sensor network (MWSNs)

To understand the differences between static WSNs and MWSNs, a brief description is provided in this section about MWSN architecture and the advantage behind adding mobility scenario.

1.4.1 MWSNs architectures

MWSNs can be classified into three classes, flat, two-tier, or three-tier architecture [93]. These architectures are presented in Fig. 8, and they are explained below. In the first hierarchical which is called a flat, the architecture network contains a set of nodes that used the ad hoc manner to communicate. This node can be stationary, PDA, or mobile node, but all the communication was done over the same network. Example of this architecture is shown in Fig. 8a which is used by the basic navigation system [94].

In the second one, which is called two-tier, its architecture consists of a set of mobile nodes and one or more stationary node as shown in Fig. 8b. The mobile nodes act as a data mule to assist the flow of data over the network, as well as from the overlay network. The mobile node in this network has more capability such as longer covering distance, higher processing, and higher bandwidth. In addition, the overlay network, in a density scenario, always all nodes maintained connected, or the network will become disconnected. In the disjoint case for ensuring arrive data to their destination, the mobile entities have the ability to locality themselves, so as to re-establish the connection. Example of this system is NavMote system [95].

In the third one, which is called three-tier, the network architecture consists of a set of stationary nodes that are used to pass the data to a set of mobile nodes, which in turn forward the data to a set of base stations (ex. APs) as represented in Fig. 8c. This overlay network generally designed to cover enormous areas suitable with a large number of applications at the same time. For example, consider you have a parking for cars with a lot of available places, and the sensor node applications are used to monitor the parking lot to determine

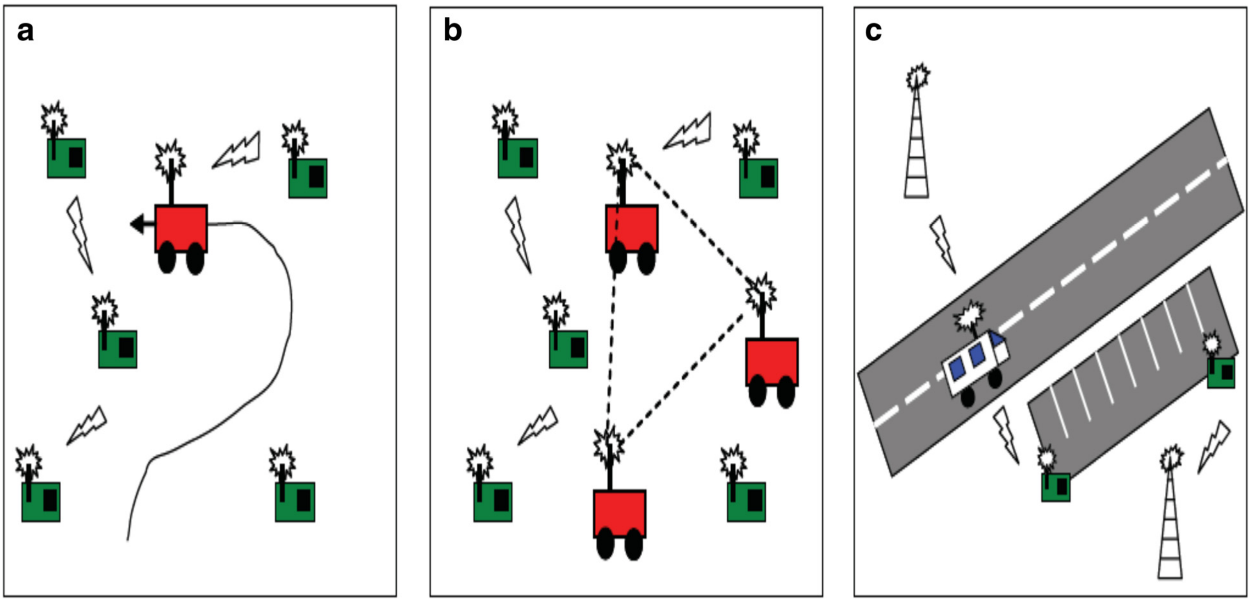

Fig. 8 a Flat, **b** three-tier, and **c** three-tier architectures of MWSN [140]

the availability areas. As a first tier, the sensor node in this network has a responsibility to sense and collect the data from their areas and forward this data in a broadcast manner to the sink node (ex. cell phone, PDA). This base station represents the second tier, which in turn forward the received data to the AP (cell towers) which is representing the third-tier architecture. After that, a centralized database is used to store the data. Users can access the database to discover the availability of places in this parking lot. At the node level, and according to their functions within the network, the mobile WSN can be classified:

- Mobile embedded sensor: In this type of sensor, their movement is controlled by external force, like wildlife tracking [96] or tracking cooperative nodes [97]. Another typical example for embedded sensors can be found in [98–100].
- Mobile actuated sensors: In this type, the mobile sensors are capable to change their position throughout the sensing area (locomotion) [94]. The management, in this type is used the pre-defined deployment, the target area can be increased. Some example of this type of sensors can be found in [101–103].
- Data mule: Predominantly, in this kind which is called a data mule [96], the sensor nodes do not work as mobile; they just collect the data and sent the collected data to the base station.
- Access point: In this network, the mobility nodes behave as an access point to keep the network connectivity by re-positioning themselves within the sensing area [104, 105].

1.4.2 *Advantage of adding mobility*

Most of the time, the deployments of sensor nodes are dedicated to the application. The sensor nodes can be deployments in a huge number of arrangements such as surrounding of the target area, grid, or randomly. In several cases, the optimal deployment remains unknown till the sensor nodes begin to sense, gather, and processing data. In the larger region, or remote areas, redeployment the nodes is infeasible. However, the rearranging nodes when they are mobile is actually possible. The work in [105, 106] showed the benefits of adding the mobility to the WSNS such as improving the coverage area, and as a consequence, it improves the sensor node deployments. This improvements are able to adapt to many different applications as well [107]. For example, sensor node in wildfire system can keep a safe distance from the fire, simultaneously measures the variation of its environment during the firing, and sends it to the fire fighters. Furthermore, in the sparse network or in disjoint network, the mobile node can be re-positioned itself to keep the network connected. In addition, some nodes die fast like stationary nodes because the data must transfer through it which leads to the consumption of its energy. But, this problem is solved using mobile node, as well as prolonging the network lifetime [108]. Another interesting advantage is improving the data integrity and extending the capacity by using multiple routing path for communication or reliable multi-cast protocol [109, 110]. Moreover, integrating the mobility into WSNs leads to shortening of the routing path by reducing the hops between the source and its destination to complete the delivery of packets [111].

1.4.3 Differences between MWSNs and WSNs

There are several differences between MWSNs and WSNs. A few examples are illustrated as follows:

- Power consumption. There is a big difference between WSNs and MWSNs as mentioned in [112] models. The energy consumed from both networks and all of them demands using the energy in an efficient way. But, the mobile entities consume more energy to enable the mobility. Green mobile techniques are introduced by many researchers to minimize the energy expenditure and carbon dioxide (CO_2) emissions in the mobile networks [113, 114].
- Dynamic network topology. In traditional WSNs, routing table or routing history, it uses a map to transfer the data to the destination as described in traditional WSNs protocols [115]. In contrast, the dynamic topologies, table routing, is no longer used, and rout discovery must be used instead of routing tables with considerable cost, regarding to energy, bandwidth and time. Fortunately, there is an active area of research dedicated to routing in mobile ad hoc networks (MANETs) and MWSNs can borrow from this work [116, 117].
- Network sink. In centralized traditional WSNs applications, sensor node data are delivered to a sink node which is used to process it using intensive resources functions. Remarkable overhead is noticed as a result to data aggregation, analysis, and routing [118]. On the other hand, dynamic network uses base station to cover a wide area to collect data and can alter their position to reduce the transmission hops for sensor nodes. Furthermore, data mining algorithms used to analyze and discover the hidden knowledge from a massive data in order to reduce the data that is routed which in turn reduces the energy consumption [119].
- Localization. Difficult if it is not impossible to change the sensor node position in statically network; however, in the dynamic network when the nodes are mobile, it is required to change their positions continuously. This is to cover the sensing environment and maintain the network connect. As a rapid re-positioning that is happening in the dynamic network, extra energy demand and time is needed.

1.4.4 Critical issues in MWSNs

Localization: Several works have been presented in the past decade on WSN [120–122], and most of them can be applied on mobile WSNs. As a result of integrating mobility over constraints-resources sensor, the implementation of lightweight algorithms for localization has become a necessity. This necessity leads to several reasoners to enhancing the location discovery [123, 124].

Coverage: Despite all the efforts and attention by researchers to increase coverage in SNs (static, mobile) [125], however, this effort is still not enough specially on mobile sensor and how to use the mobile node to make the network adopted with varying coverage dynamically.

Deployment calibration: Deployment calibration is another problem which is considered an important problem. For example, when the sensor node depends on mobile nodes to cover its geographical area, as well as its deployment depends on its neighborhood.

Network repair: The most interested in the mobile sensor network maintains the connectivity. The mobile nodes have the ability to reposition themselves on the points of disconnected to repair the network. However, this procedure increases the power expenditure. Consequently, this led to study to find an optimal algorithm for mobile movements.

Massive reprogramming: Another interested challenge for enabling mobility is massive reprogramming [126]. There is a possibility to consider solutions using locomotion nodes in overlay networks, reprogramming portion of it.

1.5 Analysis of mobility management protocols

In this section, a comparative analysis is made between several mobility protocols in terms of various characteristics (see Table 2 for more details). As mentioned earlier, the mobility management protocol is classified into two classes: host-based and network-based depending on their goals. Designing these protocols, whether host-based or network-based should take into consideration their characteristics and the suitable environment [127]. Based on our classification, a comparison between the common characteristics of mobility management protocols are discussed as follows:

Packet reordering: refers to a mechanism to reorder the received packets that reach out of order. This phenomenon comes as a result of using either buffering technique or some kind of parallelism. The network performance and packet receiver are affected by this phenomenon.

Handover category: refers to a method of mobility management that keep the MN reachable during the MN movement which in turn enhance the mobility management QoS. HO is classified into two classes, proactive and reactive. In the first one, the HO performed before change the MN association from the old access point, while in the latter, the HO performed after change the MN it position across or within a domain.

Table 2 A comparative analysis between several mobility protocols in terms of various characteristics

Characteristics	MIPv4	MIPv6	FMIPv6	HMIPv6	NEMO	PMIPv6	SMIPv6	CSMIPv6	Ovelab-MAG	OMAG
Author	[16, 17]	[18]	[22]	[21]	[19]	[23]	[26–28]	[24]	[87]	[88]
Packet reordering	No	No	Yes	No	No	No	No	Yes	No	Yes
Handover category	Reactive	Reactive	Reactive / Proactive	Reactive	Reactive	Reactive	Reactive	Reactive	Reactive	Reactive
Support of QoS	No	Yes (partial)	Yes (partial)	Yes (partial)	NO	Yes	Yes	Yes	Yes	Yes
Additional infrastructure	HA,FA	NO	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Scope of Mobility	Global	Global	Global/Local	Local	Local	Local	Local	Local	Global/Local	Global/Local
handover Latency	Long	Long	Moderate	Moderate	Long	Moderate	Moderate	Moderate	Moderate	Moderate
Scalability	No	Yes	Limited	Limited	Yes	limited	limited	limited	limited	limited
Router optimization support	Not-support	Support	N/A	support	Not-support	Not-support	Not-support	Intra-domain support	Not-support	Not-support
Mobility class	Host-based	Host-based	Host-based	Host-based	Host-based	Network-based	Network-based	Network-based	Network-based	Network-based
Mobile node modification	Yes	Yes	Yes	Yes	No	No	No	No	No	No
Power consumption	High	High	High	High	Low	Low	Low	Low	Low	Low
overhead on MN	High	High	High	Medium	Non	Non	Non	Non	Non	Non
DAD	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No
Multi-homing	Not-support	Not-support	Not-support	Not-support	Not-support	Support	Support	Support	Support	Support

QoS: refers to the ability to manage the network traffic in order to satisfy the user requirement. In other words, it is the ability to introduce a different QoS for a various services (sensitive, non-sensitive application) in the mobility protocols.

Additional infrastructure: refers to add an extra element or elements over the network entities in order to enhance the mobility.

Scope of mobility: as mentioned before, the mobility can be categorized into two categories: global mobility and local mobility according to their scope of operation. The former one, the MN moves within a differ sub-domains, while in the local, the MN moves within a domain.

Handover latency: refers to the time that elapsed starting from the last packet received from the PAR till receiving the first packet from the NAR. This time actually differs according to the protocol scope and HO techniques.

Scalability: refers to the capability of the systems or the networks for adding several MNs when needed without affecting the performance of the network.

Router optimization support: refers to the ability of protocols to shorten the path between the MN and its CN by routing the packet directly between them without any intermediate entity.

Mobility class: the mobility management was divided into two categories: host-based and network-based. In the former one, the mobility protocol requires some modification of the IP stack protocol of MN to perform the mobility, whereas the network-based does not require any modification on the MN because the mobility-related signaling done by the network entity.

Mobility node modification: to support the mobility in the host-based protocols, it is necessary to make some modification of the IP stack protocol and change the IP address on the MN. This modification leads to some extra overhead on the MN due to its limitation (power, memory, etc.). Moreover, a lot of power is consumed due to involving the MN in the mobility-related signaling, while in the network-based, the MN does not involve any mobility-related signaling which make the network mobility, better and suitable to be used in the mobility scenario.

DAD: refers to the ability of the nodes to check whether an address is unique or not-unique (already in use) [128]. This procedure consumes a significant time, which leads to increase the HO delay.

Multi-homing: refers to the ability of the MN to be connected through two interfaces. This ability leads to support ubiquitous access to the Internet at anytime and anywhere to provide reliability and fault tolerance.

From the comparative analysis in Table 2 discern the usability of network-based protocol. Meanwhile, the characteristics of PMIPv6 and its improvements provide an efficient mobility management, which supports mobility for both of IPv4 and IPv6 with transparency the MN from any mobility-related signaling. Furthermore, the network-based protocols, which are localized mobility management, reduce the handover by shortening the time needed to update the location as well as reduce the signaling overheads over the wireless networks. These enhancements are done by moving all the mobility-related signaling into the network entities instead of MN. Moreover, dispense with the DAD and movement detection when the MN moves within the PMIPv6 domain can be observed. In the host-based mobility protocols, the MN should be involved supporting the mobility during the MN motion within a domain or a sub-domain networks. Moreover, the DAD and the movement detection process must apply in host-based protocols. This, definitely, leads to extra overhead on MN and increases the HO delay which affect the service delivery.

The aim of this comparative study is to better understand the capability and the suitability of protocol among the existing mobility protocols for IP-enabled constraint devices in terms of functionalities, technique, and enhanced services.

1.6 Open research issues

Analyzing the mobility issues, the reasons that motivate the mobility should be understood first. The common definition of the mobility is a change of the MN association regardless whoever initiates it. Several reasons could cause this change such as point of failure (e.g., MAG), network performance (e.g., low signal, delay, packet loss, etc.), and physical movement [129]. This change may lead to modification in the topology which in turn needs a topology control in order to characterizes the way of monitoring the sensing field and the rules of connecting each pair of WSNs in that field [129, 130]. Unfortunately, changing the MN association leads to loosing the connectivity which causes service interruption, data loss, and serious impact on the application functionality [131]. Designing a protocol that meets the key requirements of mobility management QoS for all IP-based WSN, notably, for real-time applications, several challenges in mobility management, must be taken into consideration. These issues and challenges will be demonstrated in this section. Moreover, a comparative analysis between several mobility management protocols is made in the next section for better understanding of mobility protocols.

To enhance the mobility management, several works have been presented in the last few years. Most of this researches focused on common issues such as: minimizing HO latency, packet loss, mobility signaling costs, end-to-end delay, and power consumption [132]. These issues which considered main challenges in mobility may take place/occur in L2, L3, or both L2 and L3. HO is the major challenge in these issues which triggered by L2 and L3 handoff. The L2 delays are caused by authentication process, channel detection, and association delay, while L3 delay is affected by CoA, movement detection, registration and duplicate address detection. The researchers in [133, 134] demonstrated that the most time consuming is the channel scanning and improves the scanning delay. Moreover, a list of issues for IP-enabled related to mobility management will be investigated besides the common issued discussed early [135].

- Fault tolerance: refers to the ability of the protocol to continue work or operate even under some faults or failures properly. This can be done through adding new entities (multi-LMA or multi-home-agent) to prevent the point of failure.
- Balancing scheme: refers to distributing the nodes or the work evenly between the network entities, the absence of load-balancing lead to overhead which in turn lead to packet loss and service disruption (disconnect IP session). Also, this can be done through adding a new entity takes responsibility of attaching the nodes to the correct domain based on factors or by implement extra methods in the protocol.
- Scalability: this scheme refers to increase the number of the nodes without affecting the network performance or disrupting the services during the connectivity.
- Triangle routing: this refers to the mechanism of destined the packet indirectly to the MN as in [16]. So, router optimization must be taken into consideration in mobility management to make the MN able to receive the packet directly from CN association [32].
- Security: refers to the mechanism of protecting data against security attacks and detecting any possible security threats to make the protocol management more secure. However, the most arguable point between the researchers is how to provide a security protection and privacy in terms of location's transparency during the MN motion into sub-domains. Trust management (TM) for IoT has proven to enhance privacy and security, for a deeper understanding of the TM see [136, 137].
- Buffering technique: this an effective technique, when implemented can avoid packet loss during MN motion. This is done by buffering the packets in the network entities (ex. MAG) until finishing handover. This technique is applied by using the host-based principle which needs a MN participating in mobility-related signaling (handover initiation). The MN Involving leads to adding extra burden on the MN, because of its bounded resources (e.g., memory, processor, power, etc.). Furthermore, this mechanism adds extra overhead in order to reorder the buffering packets and scheduling mechanism to deliver the packets to the destination based on its ordering and priority.
- Multi-homing: this refers to connecting the node to one or more different interfaces in order to get a seamless HO without services disruption.
- Inter-mobility and intra-mobility cooperation: refers to the capability of cooperating between the inter-mobility (e.g., MIPv6) and intra-mobility localized mobility management (e.g., PMIPv6) in order to enhance the mobility [138].
- QoS: refers to the ability of introducing different services for a different QoS for all the next-generation IP-based WSN. Example of this is when the MN used for carrying critical services which is sensitive to delay (e.g., audio/video streaming) or non-sensitive services. A new challenge in mobility management is how to provide QoS for a homogeneous and heterogeneous [139].

2 Conclusions

Future wireless networks have gained great interest from the research community. This interest occurred as a result of its importance in the mobile networks of the next generation, therefore, as a consequence of the tremendous growth of the mobile devices on the Internet that triggered the IP management issue. This paper provides an overview of IPv6 protocol. Furthermore, a comparison between the IPv4 and IPv6 has been made. The IPv6 turned out to be more efficient and suitable for IP mobility management. This is due to the functionality provided by the IPv6 protocol to make the mobility efficient.

The analysis provided in this paper provides depth and demonstrates the evolution of IP-enabled technology and the constantly emerging challenges. This evolution leads to the distinct feature of having a wide spectrum of options for connectivity. Although WSNs equipped with IPs has long researched, the constantly evolving properties of innovative applications in IoT is constantly pressing for new findings to accommodate the new mechanism. Striking a balance between accommodating the growing complexity, sophistication and the constrained properties of the physical dimensions of the network is a constant challenge. The power of IoT resides in the ability to cater and make the demands of mobility seemless. The orientation between fostering responsibilities to the network from the host will constantly provide an evolving provision of ideal solutions.

Thus, these protocols are constantly challenged to support seamless mobility service in an efficient manner. This deficiency is a result of little back-end support provided in the IP stack for MN and also due to changing its interfaces. Furthermore, also due to an intense signal to update the MN location, IP interfaces re-configuration, and MN access authentication. Such lack of functionality leads to increased complexity for the MN, increased power expenditure, and a waste of air resources. Moreover, it also introduced some well-known problems such as HO latency, packet loss, and intense signaling. Therefore, the network-based protocols such as PMIPv6 are considered the best solutions for the mobility management. This enables the MN to roam freely within the PMIPv6 domains, as well as shields it from any mobility-related signaling. This shield leads to improved MN communication by reducing the wireless overhead and shortens the time needed to update the MN location. The essence of research are the open issues in developing solutions to enable the mobility management for the IoT to be seamless, energy efficient and secure. Determining the governing policies can stretch from being host-based to network-based. The emergence of new components in isolation or encompassed within an entity provides a rich repository of new solutions.

Received: 19 March 2016 Accepted: 16 June 2016
Published online: 11 July 2016

References

1. IF Akyildiz, Su Weilian, Y Sankarasubramaniam, E Cayirci, A survey on sensor networks. Communications Magazine, IEEE. **40**(8), 102–114 (2002). doi:10.1109/MCOM.2002.1024422
2. Y Zeng, D Li, AV Vasilakos, Real-time data report and task execution in wireless sensor and actuator networks using self-aware mobile actuators. Computer Communications. **36**(9), 988–997 (2013). doi:10.1016/j.comcom.2012.07.016. Reactive wireless sensor networks
3. Y Song, L Liu, H Ma, AV Vasilakos, A Biology-Based Algorithm to Minimal Exposure Problem of Wireless Sensor Networks. IEEE Transactions on Network and Service Management. **11**(3), 417–430 (2014). doi:10.1109/TNSM.2014.2346080
4. XY Liu, Y Zhu, L Kong, C Liu, Y Gu, AV Vasilakos, MY Wu, CDC: Compressive data collection for wireless sensor networks. IEEE Transac. Parallel. Distrib. Syst. **26**(8), 2188–2197 (2015). doi:10.1109/TPDS.2014.2345257
5. J Wan, C Zou, K Zhou, R Lu, D Li, IoT sensing framework with inter-cloud computing capability in vehicular networking. Electron. Commer. Res. **14**(3), 389–416 (2014). doi:10.1007/s10660-014-9147-2
6. N Javaid, MR Jafri, ZA Khan, N Alrajeh, M Imran, A Vasilakos, Chain-based communication in cylindrical underwater wireless sensor networks. Sensors (Basel, Switzerland). **15**(2), 3625–49 (2015). doi:10.3390/s150203625
7. A Dvir, AV Vasilakos, Backpressure-based routing protocol for DTNs. SIGCOMM Comput. Commun. Rev. **40**(4), 405–406 (2010). doi:10.1145/1851275.1851233
8. Y Yao, Q Cao, AV Vasilakos, EDAL: An energy-efficient, delay-aware, and lifetime-balancing data collection protocol for heterogeneous wireless sensor networks. IEEE/ACM Transac. Netw. **23**(3), 810–823 (2015). doi:10.1109/TNET.2014.2306592
9. Z Zinonos, V Vassiliou, in *GLOBECOM Workshops (GC Wkshps), 2010 IEEE*. Inter-mobility support in controlled 6lowpan networks, (2010), pp. 1718–1723. doi:10.1109/GLOCOMW.2010.5700235
10. Y Jiang, L Zhang, L Wang, Wireless Sensor Networks for the Internet of Things. Int. J. Distrib. Sensor Netw. **1** (2013)
11. IBM: A Smarter Planet. http://www.ibm.com/smarterplanet/us/en/. Accessed 3 Mar 2016
12. Y Qin, QZ Sheng, NJG Falkner, S Dustdar, H Wang, AV Vasilakos, When things matter: a survey on data-centric Internet of Things. J Netw Comput Appl. **64**, 137–153 (2016). doi:10.1016/j.jnca.2015.12.016
13. L Xie, Y Yin, AV Vasilakos, S Lu, Managing RFID Data: challenges, opportunities and solutions. IEEE Commun. Surv. Tutorials. **16**(3), 1294–1311 (2014). doi:10.1109/SURV.2014.022614.00143
14. Z Sheng, S Yang, Y Yu, AV Vasilakos, JA Mccann, KK Leung, A survey on the IETF protocol suite for the Internet of Things: standards, challenges, and opportunities. IEEE Wirel Commun. **20**(6), 91–98 (2013). doi:10.1109/MWC.2013.6704479
15. N Kushalnagar, G Montenegro, DE Culler, JW Hui, Transmission of ipv6 packets over ieee 802.15. 4 networks (2007). http://www.rfc-editor.org/info/rfc4944. Accessed 15 Feb 2016
16. C Perkins, IP mobility support for IPv4 (2002). http://www.rfc-editor.org/info/rfc3344. Accessed 12 Feb 2016
17. C Perkins, IP mobility support for IPv4, revised (2010). http://www.rfc-editor.org/info/rfc5944. Accessed 1 Jan 2016
18. C Perkins, D Johnson, J Arkko, Mobility Support in IPv6. Technical report, RFC 6275, July (2011). http://www.rfc-editor.org/info/rfc6275. Accessed on 13 Mar 2016
19. A Petrescu, R Wakikawa, P Thubert, V Devarapalli, Network Mobility (NEMO) Basic Support Protocol. IETF RFC. 4063 (2005). RFC 3963, doi 10.17487/RFC3963, http://www.rfc-editor.org/info/rfc3963. Accessed 15 Nov 2015
20. M-C Chuang, J-F Lee, in *Consumer Electronics, Communications and Networks (CECNet), 2011 International Conference On*. FH-PMIPv6: A fast handoff scheme in Proxy Mobile IPv6 networks, (2011), pp. 1297–1300. doi:10.1109/CECNET.2011.5768193
21. H Soliman, L Bellier, KE Malki, Hierarchical mobile IPv6 mobility management (HMIPv6). IETF, RFC 4140 (2005). RFC 4140, doi 10.17487/RFC4140, http://www.rfc-editor.org/info/rfc4140. Accessed 14 Jan 2016
22. R Koodli, Mobile IPv6 fast handovers. IETF, RFC 5568 (2009). RFC 5568, doi 10.17487/RFC5568 http://www.rfc-editor.org/info/rfc5568. Accessed 18 Feb 2016
23. V Devarapalli, K Chowdhury, S Gundavelli, B Patil, K Leung, Proxy Mobile IPv6. IETF, RFC 5213 (2008). RFC 5213, doi 10.17487/RFC5213, http://www.rfc-editor.org/info/rfc5213. Accessed 12 Oct 2015
24. AJ Jabir, SK Subramaniam, ZZ Ahmad, NAWA Hamid, A cluster-based proxy mobile IPv6 for IP-WSNs. EURASIP J. Wirel. Commun. netw. **2012**(1), 1–17 (2012). doi:10.1186/1687-1499-2012-173
25. H Yokota, K Chowdhury, R Koodli, B Patil, F Xia, Fast handovers for PMIPv6. Int. Eng. Task Force. (2010). RFC 5949, doi 10.17487/RFC5949 http://www.rfc-editor.org/info/rfc5949. Accessed 1 Dec 2015
26. MM Islam, E-N Huh, Sensor proxy mobile IPv6 (SPMIPv6)-A novel scheme for mobility supported IP-WSNs. Sensors. **11**(2), 1865–1887 (2011). doi:10.3390/s110201865
27. MM Islam, S-H Na, S-J Lee, E-N Huh, in *Future Generation Information Technology: Second International Conference, FGIT 2010, Jeju Island, Korea, December 13–15, 2010. Proceedings*, ed. by T-h Kim, Y-h Lee, B-H Kang, and D Ślęzak. A Novel Scheme for PMIPv6 Based Wireless Sensor Network (Springer, Berlin, Heidelberg, 2010), pp. 429–438. doi:10.1007/978-3-642-17569-5_42
28. MM Islam, TD Nguyen, AA Al Saffar, S-H Na, E-N Huh, in *Computational Collective Intelligence. Technologies and Applications: Second International Conference, ICCCI 2010, Kaohsiung, Taiwan, November 10–12, 2010. Proceedings, Part III*, ed. by J-S Pan, S-M Chen, and NT Nguyen. Energy Efficient Framework for Mobility Supported Smart IP-WSN (Springer, Berlin, Heidelberg, 2010), pp. 282–291. doi:10.1007/978-3-642-16696-9_31. http://dx.doi.org/10.1007/978-3-642-16696-9_31. Accessed 12 Nov 2015
29. H-N Nguyen, C Bonnet, in *Mobile Ad Hoc and Sensor Systems, 2008. MASS 2008. 5th IEEE International Conference On*. Proxy Mobile IPv6 for Cluster Based Heterogeneous Wireless Mesh networks (IEEE, 2008), pp. 617–622. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4660097&tag=1
30. SE Deering, R Hinden, Internet protocol, version 6 (IPv6) specification (1998). http://www.rfc-editor.org/info/rfc2460. Accessed 24 May 2016
31. D Chauhan, S Sharma, A survey on next generation Internet Protocol: IPv6. Int. J. Electron. Ind. Eng. (IJEEE), ISSN. **2**(2), 125–128 (2014)
32. D Johnson, C Perkins, J Arkko, Mobility support in IPv6. Technical report (2004). http://www.rfc-editor.org/info/rfc3775. Accessed April 2016
33. T Narten, E Nordmark, W Simpson, Neighbor Discovery forIPversion6 (IPv6). RFC2461, December (1998). http://www.rfc-editor.org/info/rfc2461. Accessed 22 Apr 2016
34. Q Zhou, R Zhang, ed. by Z Zhang, R Zhang, and J Zhang. LISS 2012: Proceedings of 2nd International Conference on Logistics, Informatics and Service Science (Springer, Berlin, Heidelberg, 2013), pp. 751–756. doi:10.1007/978-3-642-32054-5_105. http://dx.doi.org/10.1007/978-3-642-32054-5_105. Accessed 27 Mar 2016

35. BK Maharrey, AS Lim, S Gao, Interconnection between IP networks and wireless sensor networks. Int. J. Distrib. Sensor Netw. **2012**, 15 (2012). doi:10.1155/2012/567687

36. S Ziegler, C Crettaz, I Thomas, in *Advanced Information Networking and Applications Workshops (WAINA), 2014 28th International Conference On*. IPv6 as a Global Addressing Scheme and Integrator for the Internet of Things and the Cloud, (2014), pp. 797–802. doi:10.1109/WAINA.2014.157

37. P Agrawal, TS Teck, AL Ananda, in *Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE,* vol. 2. A lightweight protocol for wireless sensor networks (IEEE, 2003), pp. 1280–12852. doi:10.1109/WCNC.2003.1200557

38. O Gasser, TCP/IP communication in a WSN. Sensor Nodes–Operation, Network and Application (SN). **75**, 75–82 (2011)

39. G Fortino, G Di Fatta, M Pathan, AV Vasilakos, Cloud-assisted body area networks: state-of-the-art and future challenges. Wirel. Netw. **20**(7), 1925–1938 (2014). doi:10.1007/s11276-014-0714-1

40. JJ Rodrigues, PA Neves, A survey on IP-Based wireless sensor network solutions. Int. J. Commun. Syst. **23**(8), 963–981 (2010). doi:10.1002/dac.1099

41. A Dunkels, in *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services*. MobiSys '03. Full TCP/IP for 8-bit Architectures (ACM, New York, NY, USA, 2003), pp. 85–98. doi:10.1145/1066116.1066118. http://doi.acm.org/10.1145/1066116.1066118. Accessed 11 Oct 2015

42. R Braden, Requirements for Internet hosts-communication layers. INTERNET STANDARD Network Working Group (1989). <http://www.rfc-editor.org/info/rfc1122>. Accessed 28 Jan 2016

43. A Dunkels, T Voigt, N Bergman, M Jönsson, in *Swedish National Computer Networking Workshop*. The design and implementation of an IP-based sensor network for intrusion monitoring (Citeseer, Karlstad, Sweden, 2004)

44. KTH Royal Institute of Technology: Scatterweb Embedded Sensor Board. http://www.csc.kth.se/~ronniej/project/Scatterweb/ESB.html. Accessed 13 June 2016

45. The DTN/SN Project. http://www.sics.se/cna/dtnsn/ Accessed 1/2015

46. P Neves, M Stachyra, J Rodrigues, Application of wireless sensor networks to healthcare promotion. J. Commun. Softw. Syst. **2**(3), 181–190 (2008)

47. A Christian, et al., in *IEEE International Symposium on Wearable Computing, Workshop on On-Body Sensing, Osaka, JP*. Gathering Motion Data Using Featherweight Sensors and TCP/IP over 802.15. 4, Cambridge Research Laboratory, (2005), pp. 18–21. Available from: http://www.hpl.hp.com/techreports/2005/HPL-2005-188.pdf. Accessed 25 June 2016

48. M Chen, S Gonzalez, A Vasilakos, H Cao, VCM Leung, Body area networks: a survey. Mob. Netw. Appl. **16**(2), 171–193 (2011). doi:10.1007/s11036-010-0260-8

49. D Lin, X Wu, F Labeau, A Vasilakos, Internet of Vehicles for E-Health Applications in View of EMI on Medical Sensors. **2015** (2015). doi:10.1155/2015/315948

50. L Xiang, J Luo, A Vasilakos, in *Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2011 8th Annual IEEE Communications Society Conference On*. Compressed data aggregation for energy efficient wireless sensor networks, (2011), pp. 46–54. doi:10.1109/SAHCN.2011.5984932

51. Z Zhang, H Wang, AV Vasilakos, H Fang, Ecg-cryptography and authentication in body area networks. IEEE Transac. Inf. Technol. Biomed. **16**(6), 1070–1078 (2012). doi:10.1109/TITB.2012.2206115

52. N Chilamkurti, S Zeadally, A Vasilakos, V Sharma, Cross-layer support for energy efficient routing in wireless sensor networks. J. Sensors. **2009** (2009). doi:10.1155/2009/134165

53. Y Yao, Q Cao, AV Vasilakos, EDAL: An energy-efficient, delay-aware, and lifetime-balancing data collection protocol for wireless sensor networks, 182–190 (2013). doi:10.1109/MASS.2013.44

54. MM Ghaleb, S Subramaniam, M Othman, Z Zukarnain, Static and mobile data gathering techniques in wireless sensor networks: A Survey. Int. J. Adv. Comput. Tech. **6**(3), 47–60 (2014)

55. A Vasilakos, C Ricudis, K Anagnostakis, W Pedryca, A Pitsillides, in *Fuzzy Systems Proceedings, 1998. IEEE World Congress on Computational Intelligence., The 1998 IEEE International Conference On,* vol. 2. Evolutionary-fuzzy prediction for strategic qos routing in broadband networks, (1998), pp. 1488–14932. doi:10.1109/FUZZY.1998.686339

56. D He, C Chen, S Chan, J Bu, AV Vasilakos, Retrust: Attack-resistant and lightweight trust management for medical sensor networks. IEEE Transac. Inf. Tech. Biomed. **16**(4), 623–632 (2012). doi:10.1109/TITB.2012.2194788

57. H Cheng, N Xiong, AV Vasilakos, LT Yang, G Chen, X Zhuang, Nodes organization for channel assignment with topology preservation in multi-radio wireless mesh networks. Ad Hoc Networks. **10**(5), 760–773 (2012). doi:10.1016/j.adhoc.2011.02.004. Special Issue on Cognitive Radio Ad Hoc Networks

58. T Camilo, JS Silva, F Boavida, Some Notes and Proposals on the use of IP-based Approaches in Wireless Sensor Networks. Ubiquit. Comput. Commun. J., 627–633 (2007)

59. JS Silva, R Ruivo, T Camilo, G Pereira, F Boavida, in *Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference On*. IP in wireless sensor networks Issues and lessons learnt, (2008), pp. 496–502. doi:10.1109/COMSWA.2008.4554464

60. D Singh, S Singh, M Singh, H-P Kew, D-U Jeoung, US Tiwary, H-J Lee, in *Multimedia, Signal Processing and Communication Technologies, 2009. IMPACT '09. International*. IP-Based Ubiquitous Sensor Network for In-home Healthcare Monitoring, (2009), pp. 201–204. doi:10.1109/MSPCT.2009.5164210

61. JW Hui, DE Culler, in *Proceedings of the 6th ACM Conference on Embedded Network Sensory Systems.* SenSys '08. Ip is dead, long live ip for wireless sensor networks (ACM, New York, NY, USA, 2008), pp. 15–28. doi:10.1145/1460412.1460415. http://doi.acm.org/10.1145/1460412.1460415. Accessed 23 Nov 2015

62. University of California at Berkeley: TinyOS. https://www.dmoz.org/Computers/Software/Operating_Systems/Network/TinyOS.. Accessed 12 Oct 2015

63. J Polastre, R Szewczyk, D Culler, in *Information Processing in Sensor Networks, 2005. IPSN 2005. Fourth International Symposium On*. Telos: enabling ultra-low power wireless research, (2005), pp. 364–369. doi:10.1109/IPSN.2005.1440950

64. M Durvy, J Abeillé, P Wetterwald, C O'Flynn, B Leverett, E Gnoske, M Vidales, G Mulligan, N Tsiftes, N Finne, A Dunkels, in *Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems.* SenSys '08. Making Sensor Networks IPv6 Ready (ACM, New York, NY, USA, 2008), pp. 421–422. doi:10.1145/1460412.1460483. http://doi.acm.org/10.1145/1460412.1460483. Accessed 11 Jan 2016

65. A Zimmermann, J Sa Silva, JBM Sobral, F Boavida, in *Next Generation Internet Networks, 2008. NGI 2008*. 6GLAD: IPv6 global to link-layer ADdress translation for 6LoWPAN overhead reducing, (2008), pp. 209–214. doi:10.1109/NGI.2008.35

66. S Yang, S Park, EJ Lee, JH Ryu, B-S Kim, HS Kim, Dual addressing scheme in IPv6 over IEEE 802.15. 4 wireless sensor networks. ETRI J. **30**(5), 674–684 (2008)

67. J-H Kim, D-H Kim, H-Y Kwak, Y-C Byun, in *Multimedia and Ubiquitous Engineering, 2007. MUE '07. International Conference On*. Address Internetworking between WSNs and Internet supporting Web Services, (2007), pp. 232–240. doi:10.1109/MUE.2007.63

68. Y-S Kim, EJ Lee, BS Kim, HS Kim, in *Convergence Information Technology, 2007. International Conference On*. Extended tree-based routing algorithm in IPv6-enabled wireless sensor networks, (2007), pp. 1269–1274. doi:10.1109/ICCIT.2007.333

69. H Mukhtar, K Kang-Myo, SA Chaudhry, AH Akbar, K Ki-Hyung, S-W Yoo, in *Network Operations and Management Symposium, 2008. NOMS 2008. IEEE.* LNMP- Management architecture for IPv6 based low-power wireless Personal Area Networks (6LoWPAN), (2008), pp. 417–424. doi:10.1109/NOMS.2008.4575163

70. G Han, M Ma, in *Information, Communications Signal Processing, 2007 6th International Conference On*. Connecting sensor networks with IP using a Configurable tiny TCP/IP protocol stack, (2007), pp. 1–5. doi:10.1109/ICICS.2007.4449652

71. G z. Cui, H b. Li, in *Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference On*. The design of localization in wireless sensor network node based on jennic platform (IEEE, 2010), pp. 45–48

72. V Tsaoussidis, I Matta, Open issues on TCP for mobile computing. Wireless Communications and Mobile Computing. **2**(1), 3–20 (2002). doi:10.1002/wcm.30

73. PAC da Silva Neves, JJPC Rodrigues, Internet Protocol over Wireless Sensor Networks, from Myth to Reality. J. Commun. **5**(3), 189–196 (2010). doi:10.4304/jcm.5.3.189-196

74. M Youssef, M Ibrahim, M Abdelatif, L Chen, AV Vasilakos, Routing metrics of cognitive radio networks: a survey. IEEE Commun. Surv. Tutorials. **16**(1), 92–109 (2014). doi:10.1109/SURV.2013.082713.00184
75. T Meng, F Wu, Z Yang, G Chen, AV Vasilakos, Spatial reusability-aware routing in multi-hop wireless networks. IEEE Transac. Comput. **65**(1), 244–255 (2016). doi:10.1109/TC.2015.2417543
76. Y Liu, N Xiong, Y Zhao, AV Vasilakos, J Gao, Y Jia, Multi-layer clustering routing algorithm for wireless vehicular sensor networks. IET Commun. **4**(7), 810–816 (2010). doi:10.1049/iet-com.2009.0164
77. Q Jing, AV Vasilakos, J Wan, J Lu, D Qiu, Security of the Internet of Things: perspectives and challenges. Wirel. Netw. **20**(8), 2481–2501 (2014). doi:10.1007/s11276-014-0761-7
78. AJ Jara, L Ladid, A Skarmeta, The Internet of everything through IPv6: An analysis of challenges, solutions and opportunities. J. Wirel. Mob. Netw. Ubiq. Comput. Dependable Appl. **4**, 97–118 (2013)
79. C Makaya, S Pierre, An analytical framework for performance evaluation of IPv6-based mobility management protocols. Wirel Commun. IEEE Transac. **7**(3), 972–983 (2008). doi: 10.1109/TWC.2008.060725
80. JH Kim, CS Hong, T Shon, A lightweight NEMO protocol to support 6LoWPAN. ETRI J. **30**(5), 685–695 (2008)
81. M Shin, T Camilo, J Silva, D Kaspar, Mobility support in 6LoWPAN. draft-shin-6lowpan-mobility-01 (2007). (work in progress, May 29 2007, Network Working Group, Internet-Draft ETRI) https://tools.ietf.org/html/draft-shin-6lowpan-mobility-00. Accessed 10 May 2016
82. AJ Jabir, S Shamala, Z Zuriati, N Hamid, A comprehensive survey of the current trends and extensions for the proxy mobile IPv6 protocol. IEEE Syst. J. **PP**(99), 1–17 (2015). doi:10.1109/JSYST.2015.2497146
83. JH Kim, R Haw, CS Hong, in *Consumer Electronics (ICCE), 2010 Digest of Technical Papers International Conference On*. Development of a framework to support network-based mobility of 6LoWPAN sensor device for mobile healthcare system, (2010), pp. 359–360. doi:10.1109/ICCE.2010.5418817
84. J Kim, R Haw, EJ Cho, CS Hong, S Lee, A 6LoWPAN sensor node mobility scheme based on proxy mobile IPv6. IEEE Transac. Mob. Comput. **11**(12), 2060–2072 (2012). doi:10.1109/TMC.2011.240
85. R Silva, JS Silva, F Boavida, Mobility in wireless sensor networks—survey and proposal. Comput. Commun. **52**, 1–20 (2014). doi:10.1016/j.comcom.2014.05.008
86. M Bouaziz, A Rachedi, A survey on mobility management protocols in wireless sensor networks based on 6LoWPAN technology. Comput. Commun. **74**, 3–15 (2016). doi:10.1016/j.comcom.2014.10.004. Current and Future Architectures, Protocols, and Services for the Internet of Things
87. S Ro, VH Nguyen, Inter-domain mobility support in Proxy Mobile IPv6 using overlap function of mobile access gateway. Wireless Networks. **21**(3), 899–910 (2014). doi:10.1007/s11276-014-0828-5
88. I Joe, H Lee, in *Computing, Networking and Communications (ICNC), 2012 International Conference On*. An efficient inter-domain handover scheme with minimized latency for PMIPv6, (2012), pp. 332–336. doi:10.1109/ICCNC.2012.6167438
89. K Xiong, Y Zhang, Z Zhang, S Wang, Z Zhong, PA-NEMO: Proxy mobile IPv6-aided network mobility management scheme for 6LoWPAN. Elektronika ir Elektrotechnika. **20**(3), 98–103 (2014)
90. K Victor, J Ulf, G Mikael, Overlay Enhanced Mobility for the Internet of Things. J. Netw. **10**(7) (2015). doi:10.4304/jnw.10.7.420-430
91. I Stoica, R Morris, D Liben-Nowell, DR Karger, MF Kaashoek, F Dabek, H Balakrishnan, Chord: a scalable peer-to-peer lookup protocol for Internet applications. IEEE/ACM Transac. Netw. **11**(1), 17–32 (2003). doi:10.1109/TNET.2002.808407
92. AJ Jara, D Fernandez, P Lopez, MA Zamora, AF Skarmeta, Lightweight mipv6 with ipsec support. Mobile Inform. Syst. **10**(1), 37–77 (2014). doi:10.3233/MIS-130171
93. SA Munir, B Ren, W Jiao, B Wang, D Xie, J Ma, Mobile wireless sensor network: architecture and enabling technologies for ubiquitous computing. Adv. Inf. Netw. Appl. Workshops, Int. Conf. **2**, 113–120 (2007). doi:10.1109/AINAW.2007.257
94. I Amundson, X Koutsoukos, J Sallai, in *Proceedings of the First ACM International Workshop on Mobile Entity Localization and Tracking in GPS-less Environments*. MELT '08. Mobile Sensor Localization and Navigation Using RF Doppler Shifts (ACM, New York, NY, USA, 2008), pp. 97–102. doi:10.1145/1410012.1410034. http://doi.acm.org/10.1145/1410012.1410034
95. L Fang, PJ Antsaklis, LA Montestruque, MB McMickell, M Lemmon, Y Sun, H Fang, I Koutroulis, M Haenggi, M Xie, X Xie, Design of a wireless assisted pedestrian dead reckoning system—the NavMote experience. IEEE Transac. Instrum. Meas. **54**(6), 2342–2358 (2005). doi:10.1109/TIM.2005.858557
96. P Juang, H Oki, Y Wang, M Martonosi, LS Peh, D Rubenstein, Energy-efficient Computing for Wildlife Tracking: Design Tradeoffs and Early Experiences with ZebraNet. SIGARCH Comput. Archit. News. **30**(5), 96–107 (2002). doi:10.1145/635506.605408
97. B Kusy, A Ledeczi, X Koutsoukos, in *Proceedings of the 5th International Conference on Embedded Networked Sensor Systems*. SenSys '07. Tracking Mobile Nodes Using RF Doppler Shifts (ACM, New York, NY, USA, 2007), pp. 29–42. doi:10.1145/1322263.1322267. http://doi.acm.org/10.1145/1322263.1322267. Accessed 11 Mar 2016
98. J Polastre, R Szewczyk, D Culler, in *Information Processing in Sensor Networks, 2005. IPSN 2005. Fourth International Symposium On*. Telos: enabling ultra-low power wireless research, (2005), pp. 364–369. doi:10.1109/IPSN.2005.1440950
99. P Dutta, M Grimmer, A Arora, S Bibyk, D Culler, in *Proceedings of the 4th International Symposium on Information Processing in Sensor Networks*. IPSN '05. Design of a Wireless Sensor Network Platform for Detecting Rare, Random, and Ephemeral Events (IEEE Press, Piscataway, NJ, USA, 2005). http://dl.acm.org/citation.cfm?id=1147685.1147772. Accessed 11 Apr 2016
100. MOOG: Crossbow MICAz (MPR2400) Radio Module. http://www.moog-crossbow.com. Accessed 14 June 2015
101. K Dantu, M Rahimi, H Shah, S Babel, A Dhariwal, GS Sukhatme, in *Proceedings of the 4th International Symposium on Information Processing in Sensor Networks*. IPSN '05. Robomote: Enabling Mobility in Sensor Networks (IEEE Press, Piscataway, NJ, USA, 2005). http://dl.acm.org/citation.cfm?id=1147685.1147751. Accessed 17 May 2016
102. J Friedman, D Lee, I Tsigkogiannis, S Wong, D Chao, D Levin, W Kaiser, M Srivastava, in *Proceedings of the First IEEE International Conference on Distributed Computing in Sensor Systems*. DCOSS'05. RAGOBOT: A New Platform for Wireless Mobile Sensor Networks (Springer, Berlin, Heidelberg, 2005), pp. 412–412. doi:10.1007/11502593_43. http://dx.doi.org/10.1007/11502593_43. Accessed 19 Apr 2016
103. S Bergbreiter, KSJ Pister, in *Intelligent Robots and Systems, 2003. (IROS 2003). Proceedings. 2003 IEEE/RSJ International Conference On,* vol. 2. CotsBots: an off-the-shelf platform for distributed robotics, (2003), pp. 1632–16372. doi:10.1109/IROS.2003.1248878
104. RC Shah, S Roy, S Jain, W Brunette, Data MULEs: modeling and analysis of a three-tier architecture for sparse sensor networks. Ad Hoc Networks. **1**(2–3), 215–233 (2003). doi:10.1016/S1570-8705(03)00003-9. Sensor Network Protocols and Applications
105. G Wang, G Cao, TL Porta, W Zhang, in *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE,* vol. 4. Sensor relocation in mobile sensor networks, (2005), pp. 2302–23124. doi:10.1109/INFCOM.2005.1498517
106. B Liu, P Brass, O Dousse, P Nain, D Towsley, in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*. MobiHoc '05. Mobility Improves Coverage of Sensor Networks (ACM, New York, NY, USA, 2005), pp. 300–308. doi:10.1145/1062689.1062728. http://doi.acm.org/10.1145/1062689.1062728. Accessed 13 Mar 2016
107. E Ekici, Y Gu, D Bozdag, Mobility-based communication in wireless sensor networks. IEEE Commun. Mag. **44**(7), 56–62 (2006). doi:10.1109/MCOM.2006.1668382
108. SR Gandham, M Dawande, R Prakash, S Venkatesan, in *Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE,* vol. 1. Energy efficient schemes for wireless sensor networks with multiple mobile base stations, (2003), pp. 377–3811. doi:10.1109/GLOCOM.2003.1258265
109. P Li, S Guo, S Yu, AV Vasilakos, Reliable Multicast with Pipelined Network Coding Using Opportunistic Feeding and Routing. IEEE Transac. Parallel Distrib. Syst. **25**(12), 3264–3273 (2014). doi:10.1109/TPDS.2013.2297105
110. P Li, S Guo, S Yu, AV Vasilakos, in *INFOCOM, 2012 Proceedings IEEE*. CodePipe: An opportunistic feeding and routing protocol for reliable multicast with pipelined network coding, (2012), pp. 100–108. doi:10.1109/INFCOM.2012.6195456
111. A Kansal, AA Somasundara, DD Jea, MB Srivastava, D Estrin, in *Proceedings of the 2Nd International Conference on Mobile Systems,*

Applications, and Services. MobiSys '04. Intelligent Fluid Infrastructure for Embedded Networks (ACM, New York, NY, USA, 2004), pp. 111–124. doi:10.1145/990064.990080. http://doi.acm.org/10.1145/990064.990080. Accessed 11 Jan 2016

112. Q Wang, M Hempstead, W Yang, in *Sensor and Ad Hoc Communications and Networks, 2006. SECON '06. 2006 3rd Annual IEEE Communications Society On*, vol. 1. A Realistic Power Consumption Model for Wireless Sensor Network Devices, (2006), pp. 286–295. doi:10.1109/SAHCN.2006.288433
113. X Wang, AV Vasilakos, M Chen, Y Liu, TT Kwon, A Survey of Green Mobile Networks: Opportunities and Challenges. Mob. Netw. Appl. **17**(1), 4–20 (2012). doi:10.1007/s11036-011-0316-4
114. Y Zeng, K Xiang, D Li, AV Vasilakos, Directional routing and scheduling for green vehicular delay tolerant networks. Wirel. Netw. **19**(2), 161–173 (2013). doi:10.1007/s11276-012-0457-9
115. JN Al-Karaki, AE Kamal, Routing techniques in wireless sensor networks: a survey. IEEE Wirel. Commun. **11**(6), 6–28 (2004). doi:10.1109/MWC.2004.1368893
116. M Abolhasan, T Wysocki, E Dutkiewicz, A review of routing protocols for mobile ad hoc networks. Ad Hoc Netw. **2**(1), 1–22 (2004). doi:10.1016/S1570-8705(03)00043-X
117. Y-S Yen, H-C Chao, R-S Chang, A Vasilakos, Flooding-limited and multi-constrained QoS multicast routing based on the genetic algorithm for {MANETs}. Mathematical and Computer Modelling. **53**(11–12), 2238–2250 (2011). doi:10.1016/j.mcm.2010.10.008. Recent Advances in Simulation and Mathematical Modeling of Wireless Networks
118. M Ghaleb, S Subramaniam, M Othman, Z Zukarnain, Predetermined path of mobile data gathering in wireless sensor networks based on network layout. EURASIP J. Wirel. Commun. Netw. **2014**(1), 1–18 (2014). doi:10.1186/1687-1499-2014-51
119. F Chen, P Deng, J Wan, D Zhang, AV Vasilakos, X Rong, Data Mining for the Internet of Things: Literature Review and Challenges. Int. J. Distrib. Sen. Netw. **2015**, 12–121212 (2015). doi:10.1155/2015/431047
120. J Hightower, G Borriello, Location Systems for Ubiquitous Computing. Computer. **34**(8), 57–66 (2001). doi:10.1109/2.940014
121. G Mao, B Fidan, BDO Anderson, Wireless sensor network localization techniques. Comput. Netw. **51**(10), 2529–2553 (2007). doi:10.1016/j.comnet.2006.11.018
122. MZA Bhuiyan, G Wang, AV Vasilakos, Local area prediction-based mobile target tracking in wireless sensor networks. IEEE Trans. Comput. **64**(7), 1968–1982 (2015). doi:10.1109/TC.2014.2346209
123. MZA Bhuiyan, G Wang, AV Vasilakos, Local Area Prediction-Based Mobile Target Tracking in Wireless Sensor Networks. IEEE Transac. Comput. **64**(7), 1968–1982 (2015). doi:10.1109/TC.2014.2346209
124. G Wei, Y Ling, B Guo, B Xiao, AV Vasilakos, Prediction-based data aggregation in wireless sensor networks: combining grey model and Kalman Filter. Comput. Commun. **34**(6), 793–802 (2011). doi:10.1016/j.comcom.2010.10.003
125. MA Batalin, GS Sukhatme, Coverage, Exploration and Deployment by a Mobile Robot and Communication Network. Telecommun. Syst. **26**(2), 181–196. doi:10.1023/B:TELS.0000029038.31947.d1
126. JW Hui, D Culler, in *Proceedings of the 2Nd International Conference on Embedded Networked Sensor Systems*. SenSys '04. The Dynamic Behavior of a Data Dissemination Protocol for Network Programming at Scale (ACM, New York, NY, USA, 2004), pp. 81–94. doi:10.1145/1031495.1031506. http://doi.acm.org/10.1145/1031495.1031506. Accessed 22 Nov 2015
127. KS Kong, W Lee, YH Han, MK Shin, H You, Mobility management for all-IP mobile networks: mobile IPv6 vs. proxy mobile IPv6. IEEE Wirel. Commun. **15**(2), 36–45 (2008). doi:10.1109/MWC.2008.4492976
128. S Thomson, T Narten, T Jinmei, IPv6 stateless address autoconfiguration, RFC 4862 (1998). doi:10.17487/RFC4862, September 2007 <http://www.rfc-editor.org/info/rfc4862>. Accessed 12 December 2015
129. Z Shelby, C Bormann, *6LoWPAN: The wireless embedded Internet*, vol. 43. (John Wiley & Sons Ltd, Hoboken, NJ, USA, 2009), p. 91
130. M Li, Z Li, AV Vasilakos, A Survey on Topology Control in Wireless Sensor Networks: Taxonomy, Comparative Study, and Open Issues. Proc. IEEE. **101**(12), 2538–2557 (2013). doi:10.1109/JPROC.2013.2257631
131. A Achour, L Deru, JC Deprez, Mobility Management for Wireless Sensor Networks A State-of-the-Art. Procedia Comput. Sci. **52**, 1101–1107 (2015). doi:10.1016/j.procs.2015.05.126. The 6th International Conference on Ambient Systems, Networks and Technologies (ANT-2015), the 5th International Conference on Sustainable Energy Information Technology (SEIT-2015)
132. RA Khan, AH Mir, A Study of Network Based Mobility Management Schemes, 6LoWPAN Mobility, Open Issues and Proposed Solutions. **45** (2014). 1408.2632
133. P-J Huang, Y-C Tseng, K-C Tsai, in *Vehicular Technology Conference, 2006. VTC 2006-Spring. IEEE 63rd*, vol. 2. A Fast Handoff Mechanism for IEEE 802.11 and IAPP Networks, (2006), pp. 966–970. doi:10.1109/VETECS.2006.1682968
134. YS Chen, MC Chuang, CK Chen, DeuceScan: Deuce-based fast handoff scheme in IEEE 802.11 Wireless Networks. IEEE Transac. Veh. Technol. **57**(2), 1126–1141 (2008). doi:10.1109/TVT.2007.907027
135. I Al-Surmi, M Othman, BM Ali, Mobility management for IP-based next generation mobile networks: review, challenge and perspective. J. Netw. Comput. Appl. **35**(1), 295–315 (2012). doi:10.1016/j.jnca.2011.09.001
136. Z Yan, P Zhang, AV Vasilakos, A survey on trust management for Internet of Things. J. Netw. Comput. Appl. **42**, 120–134 (2014). doi:10.1016/j.jnca.2014.01.014
137. D He, C Chen, S Chan, J Bu, AV Vasilakos, A distributed trust evaluation model and its application scenarios for medical sensor networks. IEEE Transac. Inf. Tech. Biomed. **16**(6), 1164–1175 (2012). doi:10.1109/TITB.2012.2199996
138. J Kempf, Goals for network-based localized mobility management (NETLMM) (2007). http://www.rfc-editor.org/info/rfc4831. Accessed 30 Dec 2015
139. IF Akyildiz, J Xie, S Mohanty, A survey of mobility management in next-generation all-IP-based wireless systems. IEEE Wirel. Commun. **11**(4), 16–28 (2004). doi:10.1109/MWC.2004.1325888
140. I Amundson, XD Koutsoukos, in *Mobile Entity Localization and Tracking in GPS-less Environnments: Second International Workshop, MELT 2009, Orlando, FL, USA, September 30, 2009. Proceedings*, ed. by R Fuller, XD Koutsoukos. A Survey on Localization for Mobile Wireless Sensor Networks (Springer, Berlin, Heidelberg, 2009), pp. 235–254. doi:10.1007/978-3-642-04385-7_16. http://dx.doi.org/10.1007/978-3-642-04385-7_16. Accessed 14 Apr 2016