Mobility Management of Internet of Things: Protocols, Challenges and Open Issues

Muneer Bani Yassein
Computer Science Department
Jordan University of Science and Technology
Irbid, Jordan,
masadeh@just.edu.jo

Shadi Aljawarneh, Walaa Al-Sarayrah
Computer Science Department
Jordan University of Science and Technology
Irbid, Jordan
saaljawarneh@just.edu.jo, Wtalsarayrah14@cit.just.edu.jo

***Abstract*—Present day applications and technologies are continuing to drive the growth and demand in existing, and emerging fields of research. The largest change encouraging many researchers and academics to study and businesses to invest in, is the Internet of Things (IoT). IoT devices are mainly Mobile Nodes (MNs) that require Mobility Management Protocols (MMPs) to be in place, to provide transparent services to users without experiencing interruptions or disconnections. Several issues and challenges impact the communication existing between mobile nodes within a mobile IP enabled network such as packet loss, end-to-end delay, increased handover latency, increased signalling costs and power consumption. Some of the issues can be minimised by implementing new mobile IP protocols or through enhancing existing ones. This paper discusses and examines some of the important issues and challenges along with a comparative analysis and comparison of mobility management protocols and characteristics in common.**

Keywords— IoT; Mobile IP; Mobility Management; Datagrams; Handover.

I. Introduction

The significant and rapid increase of mobile devices connected to the Internet has led to the emergence of a new field of research and knowledge for researchers and businesses. Reported by the International Telecommunication Union (ITU): "there will be a rise from 6 billion to 7.3 billion mobile users by the year 2014". This number is fast exceeding the world's population.

The Internet of Things (IoT) [1] and Wireless Sensor Networks (WSN) cover a large number of mobile nodes interacting and exchanging data with each other. By 2020, the number of IOT devices is estimated to grow 50 billion times [2]. IoT is considered as being a machine to machine communication in which all physical devices are connected via the Internet. Most devices like laptops, mobile phones or any other gadgets associated with the IOT are mobile, and therefore, require special mobility management protocols to maintain and preserve IP mobility. Such protocols are needed to provide users of mobile devices with uninterrupted access to mobile services while moving within networks and remaining interconnected [29-32].

Furthermore, this massive increase in the use of mobile devices can no longer be managed and supported using older and out-dated Internet Protocols (IP). In providing sufficient IP address space for all network devices, newer versions based on previous protocols have appeared, i.e. IP version 6 (IPv6).

The Internet Engineering Task Force (IETF) created a standard set of protocols for communication purposes between mobile nodes called Mobile IP (MIP) [3]. The primary goal of the protocol is to maintain connectivity between networks, and having a permanent IP address for each mobile device, especially with WSN having low power sensors, such as 6LoWPAN [4].

The remainder of this paper is structured as follows. In Section II, Mobile IP general operations and models are discussed, including several important terminologies. Five of the greatest challenges facing mobility management are identified along with brief descriptions and causes in Section III. In Section IV, several mobility management protocols are proposed and illustrated, including a comparative analysis of mobility management protocols based upon common characteristics and finally, Section V, presents the final conclusions.

II. Mobile IP

When sudden changes in an IP address occur in applications, (e.g. voice and video over IP) potential problems with lost connectivity may emerge. Mobile IP ensures the continuous connectivity across the Internet. Both wired and wireless devices use mobile IPs when moving from one network to another while maintaining the Transmission Control Protocol (TCP) connection.

A. Mobile IP: Terminology.

The definitions of some terms are found in this section:

978-1-5090-6778-7/17/$31.00 ©2017 IEEE

- Mobile IP: a standard used to maintain connectivity while moving between networks by users of mobile nodes whose IP address is attached to a network.
- Mobile Node (MN): an internet connected device that moves from the home network to a foreign network.
- Home Network: an original network that a mobile node associates with before accessing a foreign network.
- Home Address: a permanent address used to communicate with a mobile node located within the home network.
- Home Agent (HA): an entity responsible for performing mobility functions on behalf of a mobile node and forwarding messages to a mobile node while existing outside the home network.
- Care-of Address (COA): a new address of a mobile node in a foreign network.
- Foreign Network: a new visited network.
- Foreign Agent (FA): an entity responsible for performing mobility functions on behalf of a mobile node in a foreign network.
- Correspondent Node (CN): any node attempting to communicate with a mobile node while existing outside the home network.
- Handover: the changing point of attachment from one network to another.
- Tunnel: the followed path of an encapsulated packet.
- Datagrams: the basic unit transferred between mobile nodes within a network.
- Route optimisation: sending datagrams directly from a mobile node using its permanent IP address to another node without passing through the home agent.
- Tunnelling: sending datagrams from a private network to a public network via an encapsulation process.
- Previous Access Network (PAN): a mobile node's access point before performing a handover operation.
- New Access Network (NAN): a mobile node's access point after performing a handover operation.
- Previous Access Router (PAR): a mobile node's default router before performing a handover operation.
- New Access Router (NAR): a mobile node's default router after performing a handover operation.

B. Mobile IP: Basic Model

A transparent and location-independent routing of datagrams to mobile nodes is conducted by a Mobile IP [3]. When the location of a mobile node changes, it will remain identified by its home network address. In the instance of moving away from the home network, the mobile node is associated with its home address using a care-of address. The care-of address provides the mobile node with all required information relating to its current point of attachment to the network. Following this, for each mobile node, the mobile IP will register its care-of address with the home agent. Datagrams are redirected from the home network to its associated care-of address by the home agent which reconstructs a new IP header holding the care-of address of the mobile node as its destination IP address.

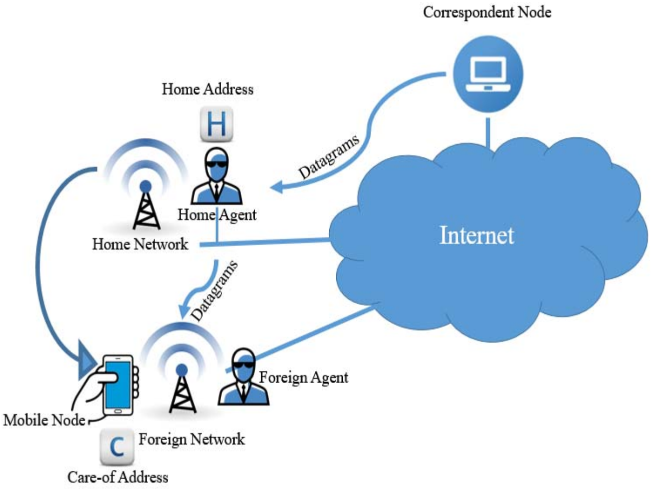

Fig.1. Mobile IP Model

A tunnelling mechanism is used by a mobile IP, where the new header encapsulates the original message packets sent by the correspondent node. After the datagrams arrive at the care-of address, they are de-encapsulated and delivered to the mobile node. Refer Figure 1.

III. Challenges and Open Issues

Over the past few years, most studies have focused on identifying common problems and challenges existing in mobility management. These include; mobility signalling costs, power consumption, packet loss, HO latency and end-to-end delay. Several studies have focussed mainly on protocols and the enhancement of existing protocols to solve and reduce challenges. Several of these protocols will be discussed later in this study. Before proposing solutions and alternatives, the problems need to be well understood. In this section, brief descriptions are presented for each problem and some of the potential causes.

Mobile nodes use wireless links to attach themselves to the Internet, and by using such links, many limitations may appear, such as a higher error rate and lower bandwidth. Also, mobile nodes are battery powered, with their primary purpose, to minimise energy consumption. In addition, two important factors should be considered in reducing the number of sent messages and decreasing their size.

1) Reducing mobility signalling costs [5]

The tremendous number of IoT signalling traffic results from billions of mobile nodes which can place the network at risk and become congested. Each mobile node will send data periodically. A signalling Tsunami may result from adding these messages and multiplying these with the number of all mobile nodes. This issue will cause resources to be used in an inefficient manner, thereby creating additional load and stress on the current network, leading consequently to a diminished Quality of Service (QoS).

2) *Reducing packet loss [6]*

Packet loss occurs when a message fails to reach its destination while travelling across the network. It is measured by calculating the percentage of lost packets and comparing these to the number of total packets sent. Network congestion is a common cause relating to this very issue and packet loss has a significant impact on user experience and reducing the overall QoS.

As discussed, network congestion is the leading cause in lost packets. When packets are sent at a higher rate than the capacity at which the link may handle, it will eventually drop off or lose some of these packets. Other possible reasons that exist are attributed to weak radio signals, corrupted hardware and harmful if not destructive, cyber-attacks. Any throughput is reduced as a side effect of packet loss and increased latency resulting from the extra time required to retransmit lost packets.

3) *Minimising HO latency [7]*

Changing the point of attachment from one network to another is referred to as the Handover Mechanism (HM), where delays can occur while being performed. Several reasons cause delays such as channel detection, authentication, process movement, Duplicate Address Detection (DAD), registration association and channel scanning. Handover latency is measured by taking the last datagram received from the old point of attachment to that of the first datagram received by the newer one.

4) *Minimising End-to-End Delay [8] [9]*

The time required to transmit a datagram across a network from its source to its destination is referred to as End-to-End Delay. It is considered an important issue, especially with time-sensitive applications that are dependent on event-driven sensor networks. It's hard to bind the end-to-end delay and anticipate when the traffic load will occur in response to an event. Time sensitive applications demand a guarantee on end-to-end latency.

5) *Minimising Power consumption [10]*

Improving energy efficiency and reducing energy demand are both widely acknowledged as critical challenges in society today, but also for IoT applications. Reducing power and energy consumption is a major focus area and is key to building energy efficient systems, providing adequate storage (i.e. batteries and cells), and in power sources supported by the adoption of power-efficient protocols.

IV. Mobility Management Protocols

Several mobility management protocols have been proposed over the past few years to support various applications and services, such as real-time applications. In this section, general descriptions are provided for each mobility management protocol.

A. *An Overview of Existing Mobility Management Protocols*

1) *Mobile IPv4 [11]*

Each node has a unique IP address; this IP address identifies the node's current point of attachment to any network. For a node to receive datagrams, it must be located on the same network as identified by its IP address, otherwise, the node's datagrams are not received. There are two possible choices for a node wishing to change its point of attachment without losing its communications capability. The first choice is to force the node to change its IP address every time it changes its current point of attachment. The second choice is to propagate all possible routes for each node throughout the network. Obviously, both choices are not feasible. In the first choice, each time a node changes a location, it's impossible to maintain connectivity with both the transport and higher layer. On the other hand, scaling problems will emerge when applying the second choice, especially given the enormous growth of mobile devices.

In Mobile IPv4, nodes within the Internet can change their point of attachment without the need to change their IP address. How IPv4 manages to accommodate node mobility is summarised into three key steps, as listed below: (also refer to Figure 1).

a) The correspondent node sends datagrams to the mobile node on the home network.

b) The home agent intercepts datagrams and then tunnels these datagrams to the corresponding care-of address.

c) A de-tunnelling mechanism of the datagrams is undertaken by a foreign agent and datagrams delivered to the mobile node.

Mobile IPv4 suffers from fragility or being broken and arises when a mobile node has a single home agent. Having more than one home agent is conducive to being more functional. Major extensions have been added to mobile IPv4 towards enhancing its mobility performance such as route optimisation, hierarchal tunnelling, and reverse tunnelling.

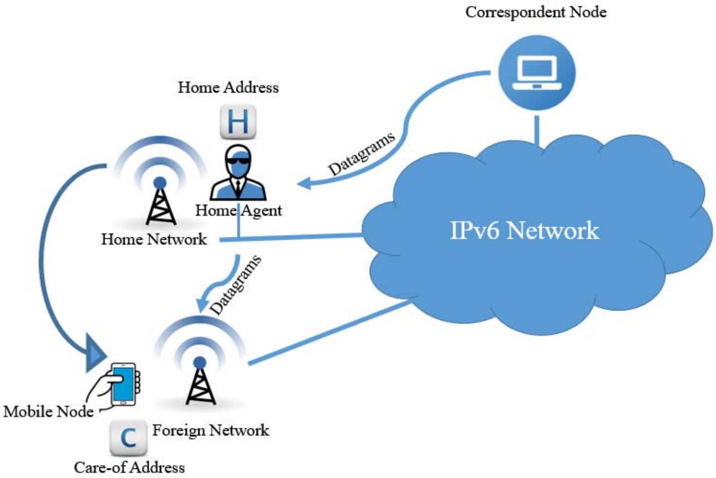

Fig. 2. Mobile IPv6

2) *Mobile IPv6 [12] [13]*

As shown in Figure 2, the principle to maintain the capability to reach another mobile device while moving around and changing points of attachment remain preserved in the mobile IPv6. Mobile IPv6 is an improved version of mobile IPv4 and provides larger address spaces, given that the fundamental operations remain the same, and except for the need to use a foreign agent. Furthermore, mobile IPv6 uses a binding cache mechanism to register each mobile node's home address with its corresponding care-of address on its home link. The home agent manages the registration process after receiving a binding update request from a mobile node which the home agent then sends back a binding acknowledgement reply to the mobile node. This finalises the registration process and any datagrams directly sent to its mobile node care-of address.

Although mobile IPv6 solves the issues surrounding changing locations of the mobile node, some more general problems still exist, i.e. having a link that can only be achieved in part or via unidirectional connectivity, hidden terminal problems, and determining the reason behind lost packets, whether due to network congestion or bit errors.

Many features shared with mobile IPv4 and mobile IPv6 provide various improvements on mobile IPv4. For example, foreign agents are not required in mobile IPv6 as in mobile IPv4. The datagrams are sent using a routing header rather than using encapsulation as this modification will reduce the overhead amount.

Mobile IPv6 uses a neighbour discovery mechanism [14] to intercept sent datagrams destined to a mobile node's home address from the correspondent node, tunnelling these to the node's care-of address. Another important mechanism uses a route optimisation technique opening the possibility of using shorter paths and eliminating congestion at the home agent of the mobile node. Finally, any failures on the path to or from the home agent are somewhat reduced as the mobile node, and the correspondent node, communicate without the need to pass datagrams via the home agent.

Mobile IPv6 supports multiple home agents to a mobile node where the mobile node can obtain the IP address of its home agent/s by initiating "dynamic home agent address discovery".

3. *Hierarchical MIPv6 (HMIPv6) [15]*

The performance of mobile IPv6 is impacted due to all signalling processes between a mobile node, its home agent, and its correspondent node forming a burden on the handover speed. Hierarchical mobility management for mobile IPv6 (HMIPv6) is introduced as an extension to mobile IPv6, reducing the amount of signalling and improving the performance of mobile IPv6.

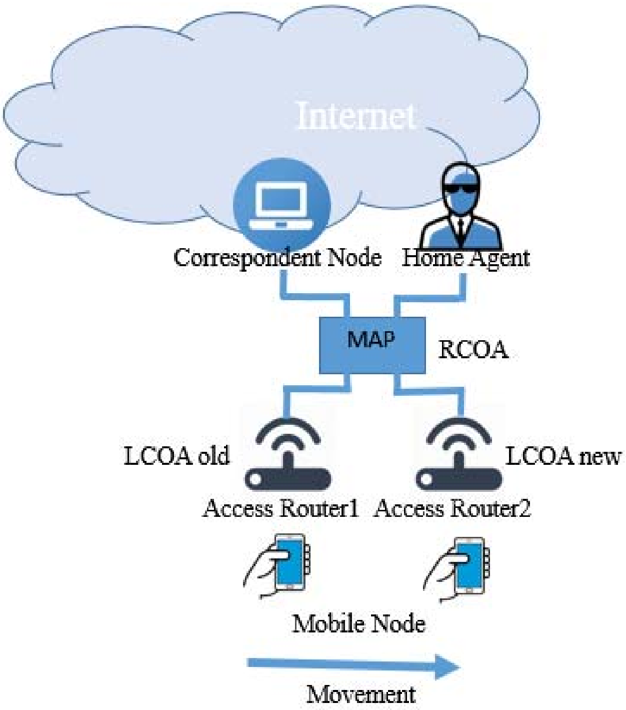

Fig. 3. HMIPv6

To maintain connectivity and the ability to reach other mobile devices moving in mobile IPv6, binding updates are sent from a mobile node to its home agent and its correspondent node. A best-case scenario is not having any lost packets for each mobile node at the time identified for 1.5 round-trips needed to authenticate the binding update between a mobile node and each correspondent node. In updating the home agent, the time for one round trip is required. An active connection to the network is disrupted every time a handoff is performed due to such round-trip delays. By eliminating these delays from the handover period, the performance of mobile IPv6 is significantly improved.

HMIPv6 uses a new node called a Mobility Anchor Point (MAP) which solves the resulting delays from signalling. Binding updates are sent to a local MAP, acting mainly as a local home agent for a mobile node instead of sending them to the home agent and correspondent nodes. The MAP intercepts all datagrams destined for the mobile node retransmitting these to the mobile node. Refer Figure 3.

The MAP distinguishes between the movement within the region and the interdomain region. A mobile node has two addresses when located in a MAP's domain; local-care of address (LCoA) and regional care-of address (RCoA). If a mobile node moves only within the MAP region, it will only be registered with a new LCoA. The RCoA remains the same, with no need to send binding updates to the home agent and the correspondent nodes. Therefore, signalling overload and packet loss are reduced over the network, and eventually, the handover delay reduced.

4. *Fast Handover for Mobile IPv6 (FMIPv6) [16]*

Using several applications like voice and video conferencing creates a challenge over mobile IP enabled networks given handover latency. The protocol targets handover latency and packet loss problems with its implementation based on mobile IPv6. Before disconnecting using the old connection and attaching to the new one, the mobile node will establish a temporary address and create a tunnel as soon as it detects a new link. Following this, it will start sending datagrams when reconnected to the new point of attachment.

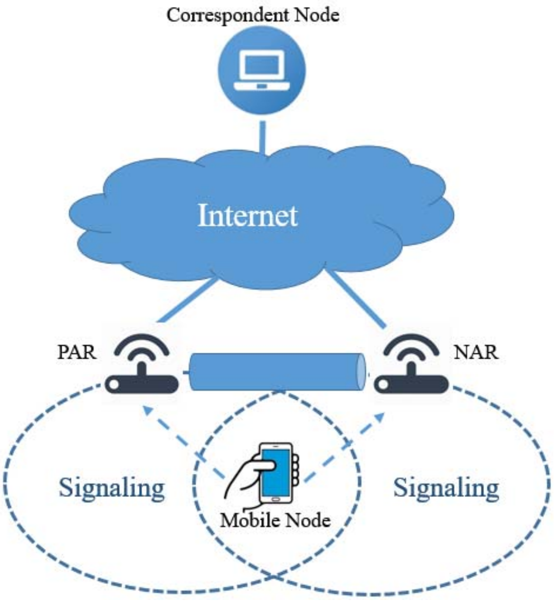

Fig. 4. Fast handover MIPv6

As shown in Figure 4, scanning of surrounding access points is performed by the mobile node before initiating the handover. The mobile node then sends a message to its Previous Access Router (PAR) to start initiating the tunnel between it and the Next Access Router (NAR) in the new location.

5) *Network Mobility (NEMO) [17]*

This protocol targets the overhead associated with signalling by using a compressed mobility header. It is an extension of mobile IPv6 allowing mobile nodes to move freely within the Internet. In previous mobility management protocols, the mobile node was responsible for all mobility management functions, whereas this is not the case for NEMO. A new entity called a Mobile Router now manages all mobility services, such as sending binding updates to mobile nodes' home agents.

6) *Proxy Mobile IPv6 (PMIPv6) [18] [19]*

PMIPv6 mobile nodes do not participate in any signalling, but rather, are a network based class mobility management scheme. There are dedicated mobility entities i.e., Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG), which monitor all movements of mobile nodes and manage mobility operations. Nevertheless, PMIPv6 suffers from having a handover process limitation given it's only performed within a local domain by the mobile nodes.

There are several problems regarding the Local Mobility Anchor (LMA), where a non-optimal path is used to exchange datagrams, thus creating the potential for bottlenecks. Problems will occur, as well as having a potential single point of failure. Furthermore, an issue may arise where the load is not distributed evenly among the MAGs, causing the MAGs to become overloaded.

7) *Sensor Proxy Mobile IPv6 (SPMIPv6) [20]*

Signalling and mobility costs, including energy consumption, are reduced using SPMIPv6 compared to MIPv6 and PMIPv6. Unfortunately, SPMIPv6 does suffer from several problems, such as the long handover latency, bottleneck issues and using non-optimised paths. These problems are inherited from PMIPv6 resulting from using one single Local Mobility Anchor (LMA).

8) *Clustered SPMIPv6 (CSPMIPv6) [21]*

CSPMIPv6 is an enhanced protocol. CSPMIPv6 consists of clusters of Mobility Access Gateways (MAGs) where for each cluster, there is a unique cluster head (HMAG). Cluster heads are responsible for all handover signalling and providing optimised paths. Thus, the load located on LMA is significantly reduced.

9) *Overlapping Mobile Access Gateway (OMAG) [22]*

The mobile nodes capability in PMIPv6 is extended to cover the inter-domain level using an OMAG protocol. Handover latency is reduced by using a Pseudo code Generation & Verification Algorithm (PGVA) which provides faster generation and verification for the IPv6 address.

10) *Constrained Application Protocol (CoAP) [23] [24]*

This protocol is proposed to address low power and noisy networks. An example of constrained networks is Power Wireless Personal Area Networks (6LoWPANs) [4]. CoAP is specially designed for the web-enabled transfer and is easily integrated with HTTP supporting URLs and different media types. CoAP excels in handling handover latency, signalling overload and packet loss [24] compared to all previous mobility management protocols.

B. *Comparative Analysis regarding Addressed Issues*

Table 1, shows a comparison between some of the mobility management protocols regarding issues and challenges mentioned in this study with further discussion continuing in the following section.

Mobility Protocols	**Issues**				
	Signalling Cost	***Packet Loss***	***Handover Latency***	***End-to-End Delay***	***Energy Consumption***
MIPv4	Not Addressed	Not Addressed	Not Addressed	Not Addressed	Not Addressed
MIPv6	Not Addressed	Less	Less	Less	Not Addressed
HMIPv6	Less	Less	Less	Less	Not Addressed
FMIPv6	Not Addressed	Less	Less	Less	Not Addressed
NEMO	Less	Less	Less	Less	Not Addressed
PMIPv6	Less	Less	Less	Less	Not Addressed
SMIPv6	Less	Less	Less	Less	Less
CSMIPv6	Less	Less	Less	Less	Less
OMAG	Not Addressed	Less	Less	Less	Not Addressed
CoAP	Less	Less	Less	Less	Less

TABLE 1 MOBILITY PROTOCOLS AND ISSUES ADDRESSED

Using a binding update process in MIPv6, handover latency, packet loss and end-to-end delays are reduced compared to MIPv4 [25]. The HMIPv6's [15] using a mobility anchor point (MAP) will lessen the amount of signalling traffic with handover latency reduced. Furthermore, fast handover MIPv6 targets packet loss and handover latency, and is performed before disconnecting old connections, and attaching to newer connections. The mobile node will establish a temporary address, creating a tunnel as soon as it detects a new link, and then starts sending datagrams when reconnected to the new point of attachment. However, the signalling cost is a barrier. [26].

Signalling overheads are reduced in the NEMO protocol by using a compressed mobility header. Moreover, [27] proposed an enhanced version of NEMO called SINEMO, to measure the throughput after the handoff but it remained the same while using NEMO, but resulted in a decline in performance due to bidirectional tunnelling.

Although MIPv6 enhances the overly long handover latency and packet loss problem in MIPv4, the issues continue to remain in MIPv6 compared to proxy mobile IPv6. The problems are solved in PMIPv6 in addition to signalling overheads. In MIPv6 using dedicated mobility entities, i.e. Local Mobility Anchor (LMA) and Mobile Access Gateways (MAGs), will monitor all movement of mobile nodes and manage mobility operations.

PMIPv6 remains impacted from having a long handover time resulting from handling all authentications and registration operations in the binding updates process. This delay leads to packet losses and end-to-end delays. Clustered PMIPv6 (CPMIPv6) solves these problems in PMIPv6 as it uses a one Top-level MAG (TMAG) for each group of MAGs. TMAG reduces the overhead on LMA by conducting all mobility operations (i.e. handoff signalling, load distribution among the MAGs and providing optimised communication paths). Thus, it reduces packet loss by providing a buffer for each mobile node within each cluster. It also reduces the signalling cost resulting from all authentications and registration operations in the handover processes. [28]

C. A Comparative Analysis of Common Characteristics

This section presents a comparison between several mobility management protocols mentioned in this study based on a number of common features. Refer Table 2.

Important definitions:

- Scalability.

  The ability to add several mobile nodes to the network when required without any changes in network performance.

- Router optimisation support.

  The ability of protocols to route the datagrams directly between the mobile node and its correspondent node without the need to use any intermediate nodes (uses a shorter path).

- QoS.

  The ability of protocols to satisfy the requirements of the user by providing a different QoS for various applications.

- Additional infrastructure.

  The need to add additional elements to network entities for improving mobility.

- Packet reordering.

  The ability to reorder received datagrams received out of order. Using either buffering or parallelism techniques may cause the datagrams to become out of order.

- Handover types.

  The ability to keep mobile nodes reachable while moving. Handover may be classified as Reactive Handover, which occurs after changing the point of attachment of the mobile node, and Proactive Handover, which is undertaken prior to the mobile node changing its point of attachment.

- Mobility scope.

  The ability of a mobile node to move either within subdomains or within a domain. The first is called Global Mobility, while the second is called Local Mobility.

- Handover latency.

  The elapsed time starting from the last datagram received from the previous access router (PAR) to the first datagram received from the new access router (NAR).

Characteristics	**Mobility Protocols**								
	MIPv4	***MIPv6***	***FMIPv6***	***HMIPv6***	***NEMO***	***PMIPv6***	***SMIPv6***	***CSMIPv6***	***OMAG***
Scalability	No	Yes	Limited	Limited	Yes	Limited	Limited	limited	limited
Router optimisation	Not Supported	Supported	Supported	Supported	Not Supported	Not Supported	Not Supported	Intra-Domain support	Not Supported
QoS	Not Supported	Supported (partial)	Supported (partial)	Supported (partial)	Not Supported	Supported	Supported	Supported	Supported
Additional infrastructure	HA, FA	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Packet reordering	No	No	Yes	No	No	No	No	Yes	Yes
Handover Type	Reactive	Reactive	Reactive/ Proactive	Reactive	Reactive	Reactive	Reactive	Reactive	Reactive
Mobility Scope	Global	Global	Global/ Local	Local	Local	Local	Local	Local	Global/ Local
Handover Latency	Long	Long	Moderate	Moderate	Long	Moderate	Moderate	Moderate	Moderate
Mobility management class	Host based	Host based	Host based	Host based	Host based	Network based	Network based	Network based	Network based
MN Modification	High	High	High	Medium	None	None	None	None	None
Power consumption	High	High	High	High	Low	Low	Low	Low	Low
DAD	Yes	Yes	Yes	Yes	Yes	No	No	No	No

TABLE 2 CHARACTERISTICS OF SEVERAL MOBILITY MANAGEMENT PROTOCOLS

- Mobility management class.

Mobility Management is categorised as host-based mobility, and network-based mobility. A mobile node's IP address is modified to perform mobility as host-based while if network-based, no modifications via the mobile nodes are required. Network entities manage the mobility.

- Mobility node modification.

Mobility in host-based protocols require support by making changes to the IP stack protocol and changing a mobile node's IP address as mentioned previously in the two classifications for mobility management. Due to possible power and memory limitations with mobile nodes modifications, additional overhead results in consuming more power by host-based protocols when signalling. Alternatively, network-based protocols are better since mobile nodes do not involve any signalling operations.

- DAD.

Duplicate Address Detection (DAD) is the ability to determine whether a given address is unique or already in use. This procedure creates an additional overhead and increases the handover delay.

The purpose of discussing these comparison helps to provide a better understanding of the suitability and capability of each mobility protocol, especially in IP enabled and often constrained devices, to ensure services are provided efficiently.

V. CONCLUSION

In the age of IoT, where machines communicate and interact with other devices (and gadgets), particular focus and consideration must be acknowledged to manage the mobility of all mobile nodes. This paper discussed some of the mobility management protocols, issues and challenges and common characteristics of these protocols that are necessary to understand and acknowledge.

REFERENCES

[1] Gubbi, J., Buyya, R., Marusic, S. & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7),1645-1660.

[2] Evans, D. (2011) The internet of things how the next evolution of the internet is changing everything. CISCO White papers.

[3] Perkins, C.E. (1997). Mobile ip. IEEE communications Magazine, 35(5), pp.84-99.

[4] Achour, A., Deru, L. & Deprez, J.C. (2015). Mobility Management for Wireless Sensor Networks *A State-of-the-Art. Procedia Computer Science, 52*,.1101-1107.

[5] Ki-Sik, K., MoonBae, S., Kwang Jin, P.A.R.K. & Hwang, C.S. (2006). A comparative analysis on the signaling load of Mobile IPv6 and Hierarchical Mobile IPv6: Analytical approach. *IEICE Transactions on Information and Systems*, 89(1), 139-149.

[6] Wikipedia contributors. (2016). Packet loss. *Wikipedia.* Date of retrieval December 25, 2016. Available: https://en.wikipedia.org/wiki/Packet_loss.

[7] Kong, K.S., Lee, W., Han, Y.H. and Shin, M.K., 2008, May. Handover latency analysis of a network-based localized mobility management protocol. In 2008 IEEE International Conference on Communications (pp. 5838-5843). IEEE.

[8] Wikipedia contributors. (2016, December 25). End-to-end_delay. [Online]. Available: https://en.wikipedia.org/wiki/End-to-end_delay

[9] Xu, Y., 2010. Minimize end-to-end delay through cross-layer optimization in multi-hop wireless sensor networks.

[10] Hwang, H.Y., Kwon, S.J., Chung, Y.W., Sung, D.K. and Park, S., 2011. Modeling and Analysis of an Energy-Efficient Mobility Management Scheme in IP-Based Wireless Networks. Sensors, 11(12), pp.11273-11294.

[11] Perkins, C., 2002. IP mobility support for IPv4 (No. RFC 3344).

[12] Johnson, D., Perkins, C. and Arkko, J., 2004. Mobility support in IPv6 (No. RFC 3775).

[13] Jora, N., 2015. Mobile IP and Comparison between Mobile IPv4 and IPv6. Journal of Network Communications and Emerging Technologies (JNCET) www. jncet. org, 2(1).

[14] Narten, T., Simpson, W.A., Nordmark, E., and Soliman, H., 2007. Neighbor discovery for IP version 6 (IPv6).

[15] Soliman, H., Bellier, L. and Malki, K.E., 2005. Hierarchical mobile IPv6 mobility management (HMIPv6).

[16] Koodli, R., 2008. Mobile IPv6 fast handovers.

[17] Devarapalli, V., Wakikawa, R., Petrescu, A. and Thubert, P., 2004. Network mobility (NEMO) basic support protocol (No. RFC 3963).

[18] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K. and Patil, B., 2008. Proxy mobile ipv6 (No. RFC 5213).

[19] Joe, I., & Lee, H. (2012) . An efficient inter-domain handover scheme with minimized latency for PMIPv6. In Computing, Networking and Communications (ICNC). Proceedings of International Conference on IEEE,(pp.332-336)

[20] Islam, M.M. and Huh, E.N., 2011. Sensor proxy mobile IPv6 (SPMIPv6)—A novel scheme for mobility supported IP-WSNs. Sensors, 11(2), pp.1865-1887.

[21] Jabir, A.J., Subramaniam, S.K., Ahmad, Z.Z. and Hamid, N.A.W.A., 2012. A cluster-based proxy mobile IPv6 for IP-WSNs. EURASIP Journal on Wireless Communications and networking, 2012(1), pp.1-17.

[22] Ro, S. and Nguyen, V.H., 2015. Inter-domain mobility support in Proxy Mobile IPv6 using overlap function of mobile access gateway. Wireless Networks, 21(3), pp.899-910.

[23] Shelby, Z., Hartke, K. and Bormann, C., 2014. The constrained application protocol (CoAP) (No. RFC 7252).

[24] Chun, S.M., Kim, H.S., and Park, J.T., 2015. CoAP-Based Mobility Management for the Internet of Things. Sensors, 15(7), pp.16060-16082.

[25] Kumar, K.R., Sharath Babu, M.D. and Thyagarajan, M.K., 2013, May. Comparison Of Mobility Management In Mobileipv4 & Mobileipv6 Networks. In International Journal of Engineering Research and Technology (Vol. 2, No. 5 (May-2013)). ESRSA Publications.

[26] Pack, S. and Choi, Y., 2003, September. Performance analysis of fast handover in mobile IPv6 networks. In IFIP International Conference on Personal Wireless Communications (pp. 679-691). Springer Berlin Heidelberg.

[27] Rahman, M.S., Bouidel, O., Atiquzzaman, M. and Ivancic, W., 2008, November. Performance Comparison between NEMO BSP and SINEMO. In IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference (pp. 1-5). IEEE.

[28] Shamala, S. and Jabir, A.J., 2016. Mobility Management for Internet of Things. World Scientific News, 41, p.313.

[29] Aljawarneh, Shadi A., Raja A. Moftah, and Abdelsalam M. Maatuk. "Investigations of automatic methods for detecting the polymorphic worms signatures." Future Generation Computer Systems 60 (2016): 67-77.

[30] Aljawarneh, Shadi A., Ali Alawneh, and Reem Jaradat. "Cloud security engineering: Early stages of SDLC." Future Generation Computer Systems (2016).

[31] Aljawarneh, S.A. and Yassein, M.O.B., 2016. A Conceptual Security Framework for Cloud Computing Issues. International Journal of Intelligent Information Technologies (IJIIT), 12(2), pp.12-24.

[32] Aljawarneh, Shadi, and Muneer Bani Yassein. "A resource-efficient encryption algorithm for multimedia big data." Multimedia Tools and Applications (2017): 1-22.