DESIGN AND EVALUATION OF AN IMPROVED CONSTRAINT APPLICATION PROTOCOL (i-CoAP) BASED ON MOBILITY MANAGEMENT FOR INTERNET OF THINGS

[1]BISHIR ABDULLAHI, [2]SHAIFALI SHARMA

School of Advance Computing
Department Of Computer Science and Engineering
Alakh Prakash Goyal Shimla University, Shimla, HP, India.

***Abstract*: Internet of Things is a simple idea of connecting all identified objects through wireless connection, that they could communicate with each other and be able to identify themselves to other devices. In the Internet of Things (IoT) devices are mainly mobile nodes that require mobility management protocols to be in place, to provide transparent services without experiencing interruption or disconnections. The primary goal of the mobility management protocol is to maintain connectivity between networks. In a reliable and dependa ble environment, service continuity is supported in a scenario where the IoT resources/devices are mobile or can become unavailable due to handover delays or network disconnection. Constraint Application Protocol is a specialized internet application protocol for constrained devices. It enables those constraint devices called node to communicate with wider internet using similar protocols. CoAP is designed for use between devices on the same constrained network example low-power, lossy networks between devices and general nodes on the internet, and between devices on different constrained networks both joined by internet. There is significant problem in CoAP due to its handoff delay through double address detection. This research work investigated the existing Constraint Application protocol based on mobility management protocols and improved the protocol by proposing a novel i-CoAP mobility management that improved transmission of data packets between nodes of different locations. The improved constraint application protocol makes use of cache and tunneling modes to improve communication between nodes during handover operation.**

INTRODUCTION

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. (Safwan and Shamala, 2016)

IP Mobility Management

"In an earlier study, (Safwan and Shamala, 2016) had insisted that IP mobility management is utilized as a mechanism to resolve these issues. The management protocols introduced to support mobility have 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 (Akyildiz, 2002).

IoT in Wireless Sensors Networks

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. 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. 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 (Zinonos and Vassiliou, 2010). 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. In the IoT paradigm, WSNs are considered the most important elements which collect information from their surrounding environment. 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 industry is evident such as "Smarter Planet" IBM (IBM A Smarter planet, 2016).

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. 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 (Qin *et al.*, 2016). However, 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 (Sheng *et al.* 2013*).*

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. 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 (Sheng *et al.*, 2013).

Enabling IP Mobility Management

To provide IP mobility management, the IETF proposed and released the Mobile Internet Protocol IPv4 (MIPv4). 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) and network mobility (NEMO) approach 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. Several host-based protocols were released and designed by the IETF to alleviate the bottleneck in the MIPv6 such as Hierarchical MIPv6 (HMIPv6), Fast Handover for Hierarchical (FHMIPv6) and Fast Handover MIPv6 (FMIPv6. 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 (Koodli, 2016).

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). 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) (Yokota *et al.*,2015).

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. 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 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), cluster-based PMIPv6 for wireless mesh networks, and a cluster-based proxy mobile IPv6 (CSPMIPv6) 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 efforts to constantly enhance the IPv6 solutions for WSN-IP (Jabir, 2012).

Overview of Internet Protocol version 6 (IPv6)

IPv6 is an updated version of IPv4, proposed by IETF. IPv6 improves several features of IPv4, such as extend the address range, and 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. 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. 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 (Chauhan, 2014).

Meanings of Some Terms

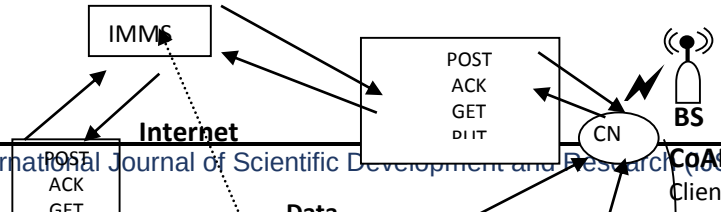
Terms	Descriptions
IMMS	IoT Mobility Management Server
P_Addr	Permanent Address
T_Addr	Temporary Address
Cur_T_Addr	Current Temporary Address
New_T_Addr	New Temporary Address
ACK	Acknowledgement
WSN BS	Wireless Sensor Network Base Station
H-Flag	Handover Flag
LBC	Local Binding Cache

Proposed Mobility Management Architecture of i-CoAP

Figure 1.0 shows the mobility management architecture using CoAP. The components of the architecture consist of a CoAP server and CoAP Client nodes and IoT Mobility Management System (IMMS) with a Mobility Management Table (MMT).

However it shows the detailed mobility management procedure for IoT i-CoAP mobility management. The CoAP consists of four procedures, *i.e.*, registration, discovery, binding, and notification, to provide mobility management for a moving CoAP node. The operation of CoAP is described in detail below. First, the CoAP client and CoAP node send the POST request message for registration to the IMMS in order to register their own P_Addr and Lifetime in the MMT of the IMMS. As the CoAP client attempts to communicate with the CoAP node, the CoAP client sends a GET request message to the IMMS for discovery. This message includes the CoAP client's destination IP address. In response, the CoAP client receives the current T_Addr for the CoAP node and it's Lifetime in the ACK response message for discovery. Then, the CoAP client stores the T_Addr and Lifetime for the CoAP node in the LBC. Subsequently, the CoAP client can exchange data with the CoAP node directly until the Lifetime of T_Addr expires.

Next, let us consider the case in which the CoAP node moves from the old base station (BS) such as router, access router to the new BS of the new WSN. As the CoAP node moves away from the old WSN BS and enters the network domain of the new BS, it requires the IP handover operation (as illustrated in Figure 3.4). In order to perform the handover operation, the CoAP node first detects the radio signal strength (RSS) from the old ER at the link layer. When the RSS from the old BS drops below a certain threshold value, the CoAP node prepares the handover operation. In order to prevent packet loss during the handover operation, the CoAP node notifies the CoAP client of its status—*i.e.*, handover mode—by sending a PUT request message to withhold access requests from the IMMS. The IMMS then updates the H_Flag of the CoAP node in the MMT to "1." It also forwards the PUT request message so that requests from the CoAP Client are withheld. In response, the CoAP client likewise updates the H_Flag in its LBC to "1." Because the H_Flag of a CoAP node indicates that the node is performing a handover operation—and consequently cannot be accessed. During a handover, the CoAP node resides in the overlapped region of two network domains: the old BS and the new BS. The CoAP node detects the movement of a CoAP node through the Router Advertisement (RA) and Router Solicitation (RS) messages. As soon as it detects the new BS network domain, the CoAP node attempts to secure a new temporary IP address—*i.e.*, T_Addr from the new ER—by using Neighbor Solicitation and Neighbor Advertisement.



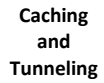


Figure 1.1 Proposed Improve Mobility Management Architecture for Caching and Tunneling Modes

Proposed IP Format of i-CoAP

In this subsection, we present the IP address format using i-CoAP. Figure 1.2 shows the IP address information during i-CoAP handover. We assume that the CoAP node moves from WSN BS1 to WSN BS2. In this situation, Cur_T_Addr and Cur_Lifetime of CoAP node are changed to New_T_Addr as a temporary IP address, *i.e.*, T_Addr, and New_Lifetime as Lifetime, respectively. However, P_Addr as the permanent IP address, *i.e.*, P_Addr, does not change. P_Addr, T_Addr, and Lifetime of CoAP nodes are cached on the IMMT of the IMMS. W_Addr indicates the IP address of the IMMS. The detailed information refers to the CoAP standard the RSS from the access point or base station connected to the old-ER is less than the threshold value, mCSN cannot send or receive data from old-ER, and disconnects a connection from the access point or base station connected to the old-ER. mCSN then discovers the new-ER. mCSN attempts to perform the connection attachment to the access point or base station connected to the new-ER. It then retrieves a new T_Addr through the DHCP server, which includes both Discovery and Offer procedures.

Step 4: After obtaining a new T_Addr, mCSN tunnel the temporary address for a PUT binding update request message to both the IMMS and CWC through new-ER, simultaneously, by referring to the T_Addr of CWC in the LBC, to inform them of the new T_Addr. The PUT binding update (BU) request message includes the P_Addr, T_Addr, and Lifetime of mCSN. After the IMMS and mCSN receive the PUT BU message, the T_Addr and Lifetime are updated in the MMT and LBC and the H_Flag is set to "0". Finally, CoMP node A can retrieve the data from mCSN. In this manner, the connection between CWC and mCSN can be seamlessly maintained during the handover operation.

Adding Caching and Tunneling to the Proposed Scheme.

To address the disruption issue, we proposes mobility management scheme for the service-enabled IoT scenarios. The scheme proposes two modes: a caching and a tunneling mode. The caching method is used to address the delay issues: Handover Delay and Coverage Loss. In the caching mode, the gateway caches the last reading from the sensor every time it is queried and also during the initial sensor association. The tunneling mode addresses the Inflexibility of SP to handle changes in the underlying topology or the case that SP has not been updated about the new location of a particular sensor node. In Figure 1.4 and 1.6, the scheme for the caching and tunneling modes is depicted. The association phase is the same for the both modes, tunneling mode and caching mode and described as follows. In the association phase between sensor and Sensor Gateway the sensor receives a beacon signal from SGW1 sent as Send Beacon () and thereupon requests authentication with Start Authentication (node ID). If the sensor is allowed to associate to the node, permission is granted Grant Permission (). The node requests a session from SGW1 Request Session Id () and a session ID is retrieved via Retrieve Session Id (). The session ID contains the name or address of the node's current associated gateway.

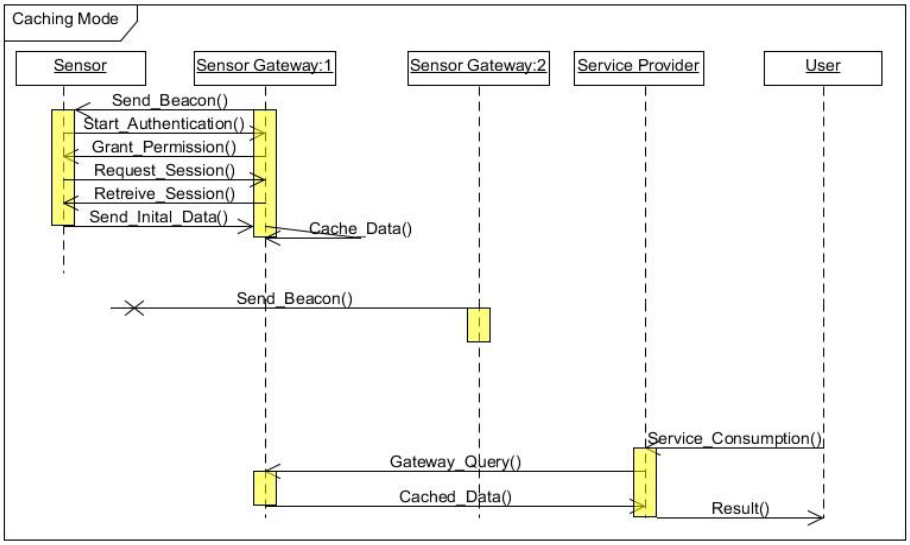


Figure 1.4: Caching Mode (Frieder *et al.*, 2012).

1) Caching Mode:

The proposed scheme introduces a cache, for each Sensor Gateway to store the latest data of each connected node cached on a gateway. This data is used during the handover delay to respond to the queries. The service remains available even during long sensor disconnection (i.e. moving in an area with no coverage to another SGW). If a user queries the SP and SP tries to access the sensor data via a SGW which cannot access the requested sensor, cached data is used to serve the query. After the association phase in Figure 1.6 the node sends its current data to SGW by Send Initial Data () and SGW caches this data. The cache is also updated during every successful sensor query with the latest sensor data. In the case that the sensor node starts to move and cannot receive a new beacon signal due to coverage issues, the caching mode will be applied. During the movement of the node, a user uses SP services by sending Service Consumption () request. SP forwards the queries to the responsible SGW1, which is not able to contact the particular node. SGW1 will use its latest cached reading to respond to the SP Cached Data () which will be also used to serve the request of the user via SP. The trade-off for this approach is the data freshness. In some critical scenarios where the latest data needs to be accessed, such as medical or surveillance scenarios this approach is not applicable.

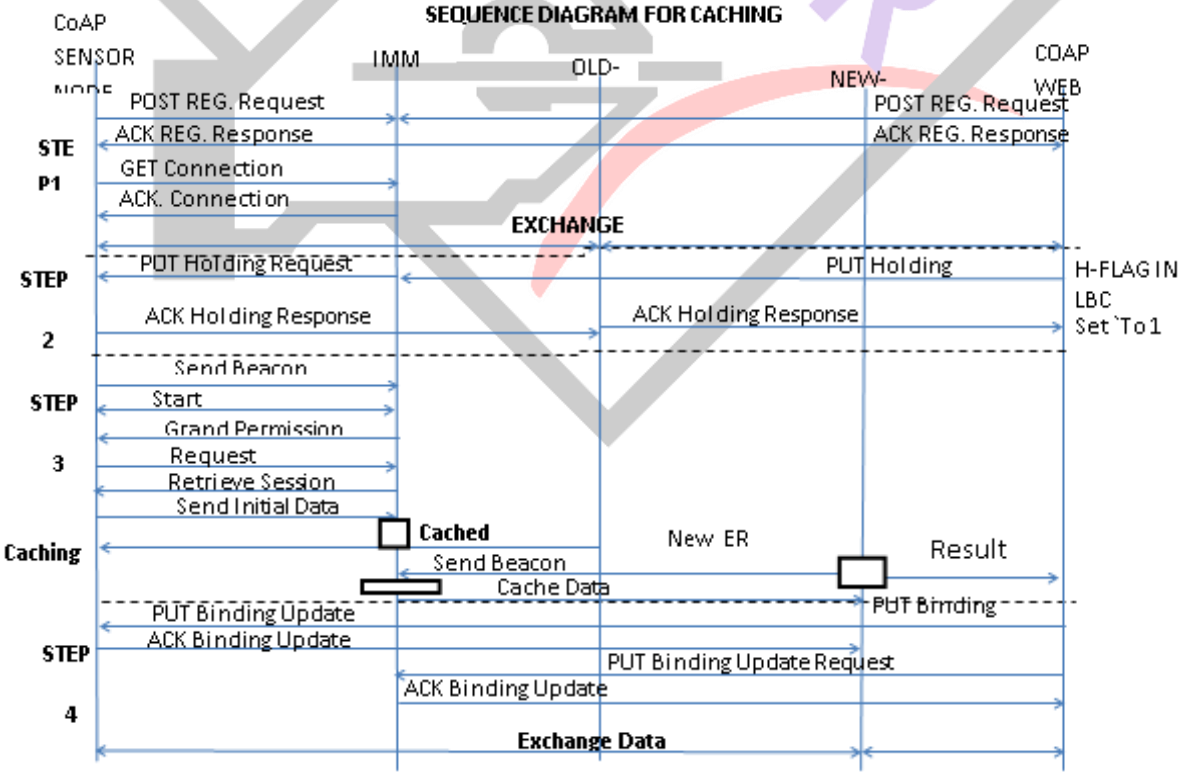


Figure 1.5. Proposed Sequence Diagram for Caching Mode

2) Tunneling Mode:

The Tunneling approach can be used during the handover while the CoAP node is already connected to the new SGW but the SP has not been updated with this movement information. This could be the case for static SPs which do not support the changes in the underlying topology. While SP is not updated with the new SGW information, the SGW can tunnel the request to the new SGW in

the tunneling mode of the proposed resource mobility scheme. This is possible because the sensor node can submit ID of the new SGW to the old one during the re-association phase.

Figure 1.6: Tunneling Mode (Frieder *et al.*, 2012)

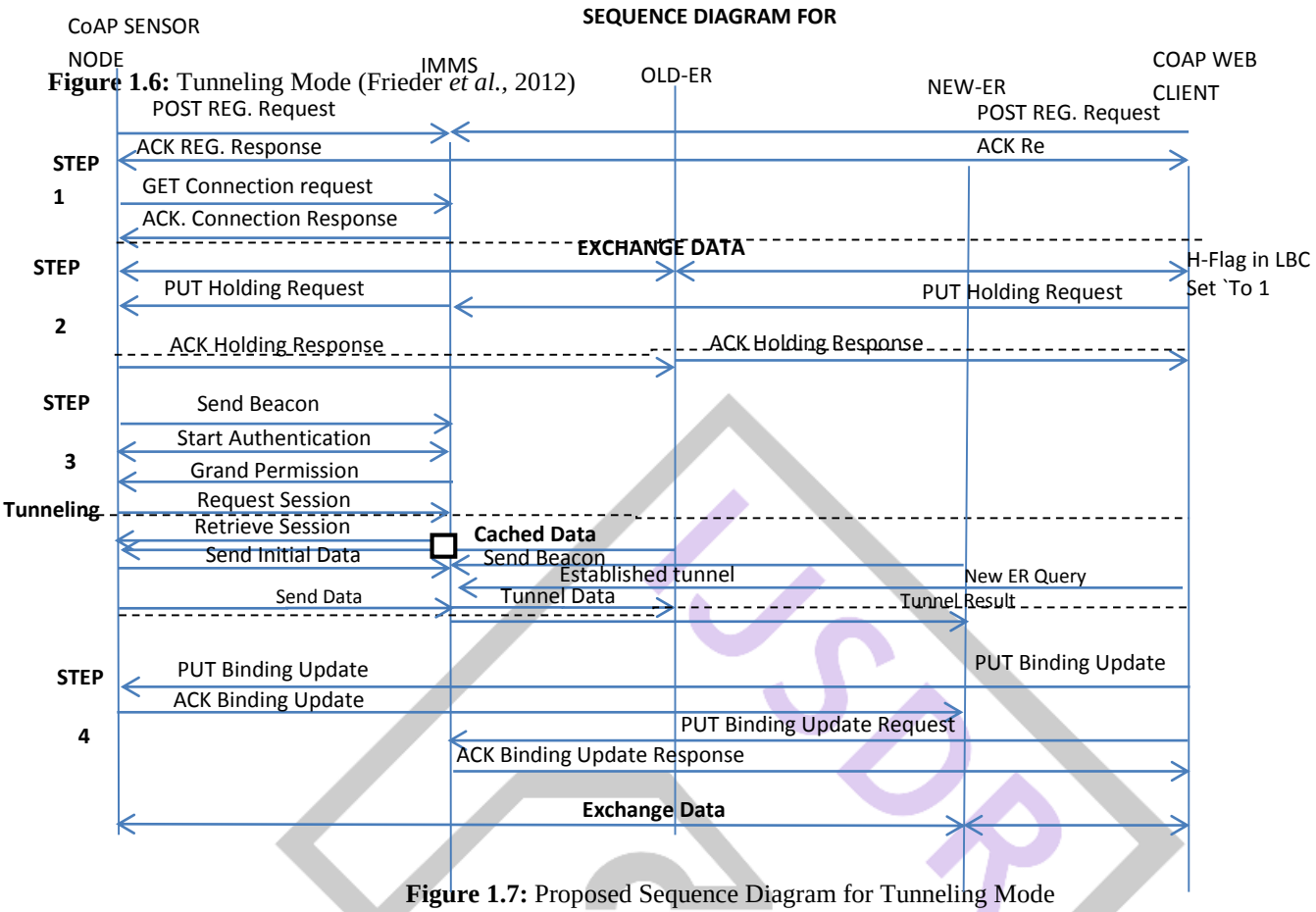


Figure 1.7: Proposed Sequence Diagram for Tunneling Mode

Proposed Algorithm for a Reliable Message Transmission

We describe the algorithm of signaling massage transmission for a reliable mobility management algorithm of i-CoAP based mobility management protocol and analyze the performance of the handover delay using caching mode. The i-CoAP extents the CON massage of the CoAP protocol to reliable transmit the signaling massage under an unreliable IoT network environment. In particular, the retransmission is instrumented by using a massage ID and CON massage of the CoAP protocol, using CoAP PUT, and caching mode. The massage ID is used to detect duplicate and for transmission reliability and the CON massage is retransmission using both default timeout and exponential back-off between retransmission until recipient sends an ACK with the same massage ID from corresponding endpoint. The algorithm shows the reliable transmission of i-CoAP massage where T, Rc, m, Ch, Tn and are timeout, retransmission count, maximum number of retransmission counts caching and Tunneling mode respectively.in case of packet loss the PUT massage are retransmission for binding update and holding.

Proposed Algorithm For Reliable_Signaling_Massage Transmission (*P, T, Rc, m, Ch,Tn*);
/*This algorithm describe the reliable transmission of i-CoAP message by using *T, Rc m*, and *Ch* ,*Tn**/
P: CoAP message
T: Timeout //T=ACK_TIMEOUT
Rc: Retransmission count/ /initially *Rc* = 0
M: Maximum number of retransmission count / / *m* = 4, *Ch*: caching/tunneling Mode // *Ch* >= *m*

```
1.    Begin
2.    If (T == 0 OR Rc == 0) Then {
3.       T = ACK TIMEOUT ;
4.       Rc = 0; m = 4; Ch >= m; }
5.    Else {
6.          If (Rc <  m) Then {
7.             Send the CoAP message to lower layer;
8.             While (T < Timeout) / / wait until T is expired
9.                If  (mCSN receives Acknowledgement)
10.               Then { T = 0; Rc = 0;Tn;
11.                        Call  CoAP_Retransmission (P + 1, T, Rc, Ch); }
```

12. **Else Call** CoAP_Retransmission (*P, T*2, Rc + 1 m <= Ch*) ; }
13. **Else** Discard P;} // is discard
14. **End**

Analytical Model

The packet loss of the signaling message can dramatically increase the handover latency, which may be caused by collision, congestion, and system failure in both wireless and wired communication links. The retransmission of signaling messages in the case of packet loss may greatly reduce the handover latency in constrained IoT networks.

The handover delay at a CoAP node side is the time interval during which the CoAP node cannot send or receive any packets during a handoff, and is composed of both L2 and L3 handover latencies. Figure 13 shows the handover delay timeline caused by executing the CoAPS. The white small circle indicates the time line during the handover of CoAP node between WSN BS1 and WSN BS2. The total handover delay, *i.e.*, the packet reception latency tp, consists of the link setup time t_{L2} which is caused by an L2 handover; the IP connectivity latency (tIP); and the location update latency (tBU). Here, tIP is the sum of tMD, tAC, and tBU, where tMD represents the movement detection delay; tAC, the address configuration; DAD, the delay; and tBU, the BU delay between the CoAP node and IMMS (Makaya and Pirre, 2008).

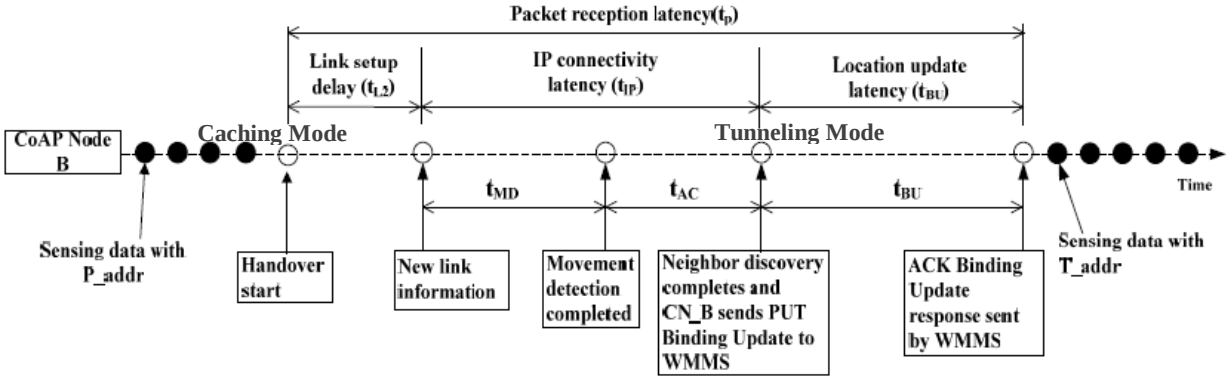


Figure 1.8: Handover Delay Timeline of i-CoAPs

To analyze the delay more precisely, in the following passage, we describe the delay caused by a signaling message between the CoAP node and IMMS. Let $t_{X,Y}$ be defined as a one-way signaling message transfer delay between nodes *X* and *Y*. One of the endpoints is a CoAP node, and $t_{X,Y}$ can be computed as follows as described (Makaya and Pierre, 2008)

$$t_{X,Y}(s) = \left(\frac{s}{B_{WL}} + l_{WL}\right) + \left[(d_{X,Y} - 1)\left(\frac{s + s_t}{B_W} + L_W + \varpi\right)\right] \quad \text{.....3.1}$$

Here, *S* is the size of the signaling message, and *Bwl* and *Bw* are the bandwidths of the wireless and wired links, respectively. L_{WL} and L_W are the link delays of the wireless and wired links, ϖ is the average queuing delay at each router on the Internet, $d_{x,y} - 1$ is the average number of hops in a wired link between nodes *X* and *Y*, and s_t is the tunneling packet size. In Equation (1), the first and second terms indicate a one-way signaling message transfer delay in a wireless and wired link, respectively, between nodes *X* and *Y*. For an analytic performance evaluation, a formula for the handover latency was derived for each mobility management protocol. The handover latency in MIPv6 is composed.

$$D_{MIPV6} = t_{L2} + t_{MD} + t_{AC} + t_{BU} + t_{rr} \quad \text{.....3.2}$$

Here, t_{BU} is the time delay incurred when the CN_B conducts a BU to the HA. t_{RR} is the time delay caused by executing a return rout ability procedure.

For $Dt_{BU} = 2(t_{CN\_B.HA} + t_{CN\_B.CN})$ 3.3

And $Dt_{rr} = 2(t_{CN\_B.CN} + t_{CN\_B..HA} + t_{HA.CN})$ 3.4

MIPv6 uses a bi-directional tunnel between the HA and CN_B.

Because CoAP is only used for local mobility management, a BU for either the or CN, *i.e.*, CN_A, is not necessary. However, instead of HA/CN, it requires a BU for the mobility management server (IMMS), and thus, binding update delay, *i.e.*, tBU incurs when sending signaling messages back and forth between CN_B and the IMMS. It creates a handover delay of 2CN_B, IMMS. In the case of CoAPs, the handover latency is composed of t_{L2}, t_{MD}, t_{AC}, and t_{BU}. Here, tBU represents a binding update signaling message delay, *i.e.*, a PUT binding update request message and an ACK binding update response message. Table 3 shows a summary of total handover delay for MIPv6, CoAP, and i-CoAP.

Table: Handover Latency

Protocol	Total Handover Latency
D_{MIPV6}	$t_{L2}+t_{MD}+t_{AC}+t_{BU}+t_{rr}$
D_{CoAP}	$t_{L2}+t_{MD}+t_{AC}+t_{BU}$
D_{i-CoAP}	$t_{L2}+t_{MD}+t_{AC}+t_{CN\_B+tn.IMMS}+t_{CN\_B.CN\_A}$

Packet loss is the amount of packets dropped, lost, or corrupted during transfer. Because the packet loss is proportional to the handover delay, the packet loss P*HOprotocol* of the handover protocol of *HO protocol* can be calculated as follows: (Makaya and Pierre 2008).

PHOprotocol = λp DHOprotocol

Here, λp is the packet arrival rate in packets per time units, and D*HOprotocol* is the handover delay of the handover protocol of *HOprotocol*. A summary of the total packet loss for MIPv6, CoAP, and i-CoAPs is shown below. In the case of i-CoAPs, a PUT holding request message and an ACK response message between the CoAP B and the IMMS are required during a handover to maintain the hold mode. Because it is assumed that during the hold mode, almost no packet loss occurs, packet loss during the handover operation is zero.

Performance Evaluation Metrics

The process of evaluating the performance of this algorithm, existing algorithm will be used to quantify the extent to which the research improved for constrained application protocol based mobility management protocol for IoT.

The objective of this research is to minimized handover latency and minimized packet loss.

(i). Handover Latency – The handover latency at CoAP node site is the time interval during which a CoAP node cannot send or receive any packet during handover, it is composed of L2 (link layer) and L3 (IP layer) handover latency. Link layer handoff is the sum of delay due to movement direction, IP layer addresses configuration and binding update.

(ii). Packet loss – is the amount of packet dropped, lost or corrupted during transfer, packet loss can be calculated as

Packet Loss = $\frac{Ns-Nd}{Ns}$ X 100%

Where, Ns = Number of packet generated at source

Nd = Number of packet received at destination

RESULT AND DISCUSSION

In this section, we conducted performance analysis of the two mobility management protocols using i-CoAPS. In particular, we compare the performance of the proposed mobility management with that of the IETF MIPv6 and CoAP mobility management protocols.

Analytical Analysis

We conducted analytical analysis to compare the proposed i-CoAPS mobility management with the existing protocols. We demonstrate some numerical result in order to analyze the proposed algorithm and compared with the existing algorithm. We demonstrate some numerical result in order to analyzed the proposed algorithm and compare with the existing algorithm; we set the values of parameters as shown in table 4.1 below. Most of the parameters in the analysis were set to typical values found in Makaya and Pirre (2008).

Table: Empirical Values

t_{AC} = 500ms	$\mathbf{t}_{MD}$ = 100ms	T_{l2} = 50ms	B_w = 10Mps	B_{wl} =20-250kbs	$\boldsymbol{\theta}$ = 0.1ms
l_{wl} = 15ms	l_w = 2ms	S = 50byte	S_t = 80byte	$\boldsymbol{\lambda}_p$ = 10p/s	No = 10

In Table the auto-configuration delay indicates the time interval during the duplicate address detection procedure, and the movement detection delay indicates the time interval during which the CoAP node recognizes whether the current network domain is in the same domain. The L2 handover delay indicates the time interval during the link layer handover procedure. Table provides further description of these parameters. It is assumed that the number of hops between the CoAP node and WSN BS, between the CN and HA, between the IMMS and WSN BS1 BS/WSN BS2, and between the HA/CN and IMMS are set to 1, 2, 2, and 2, respectively. In the performance evaluation, we used UDP-based Constant Bit Rate (CBR) traffic with bit rates of below 56 Kb/s, a packet size of 1024 bytes, and a packet arrival rate under 55 packets/s.

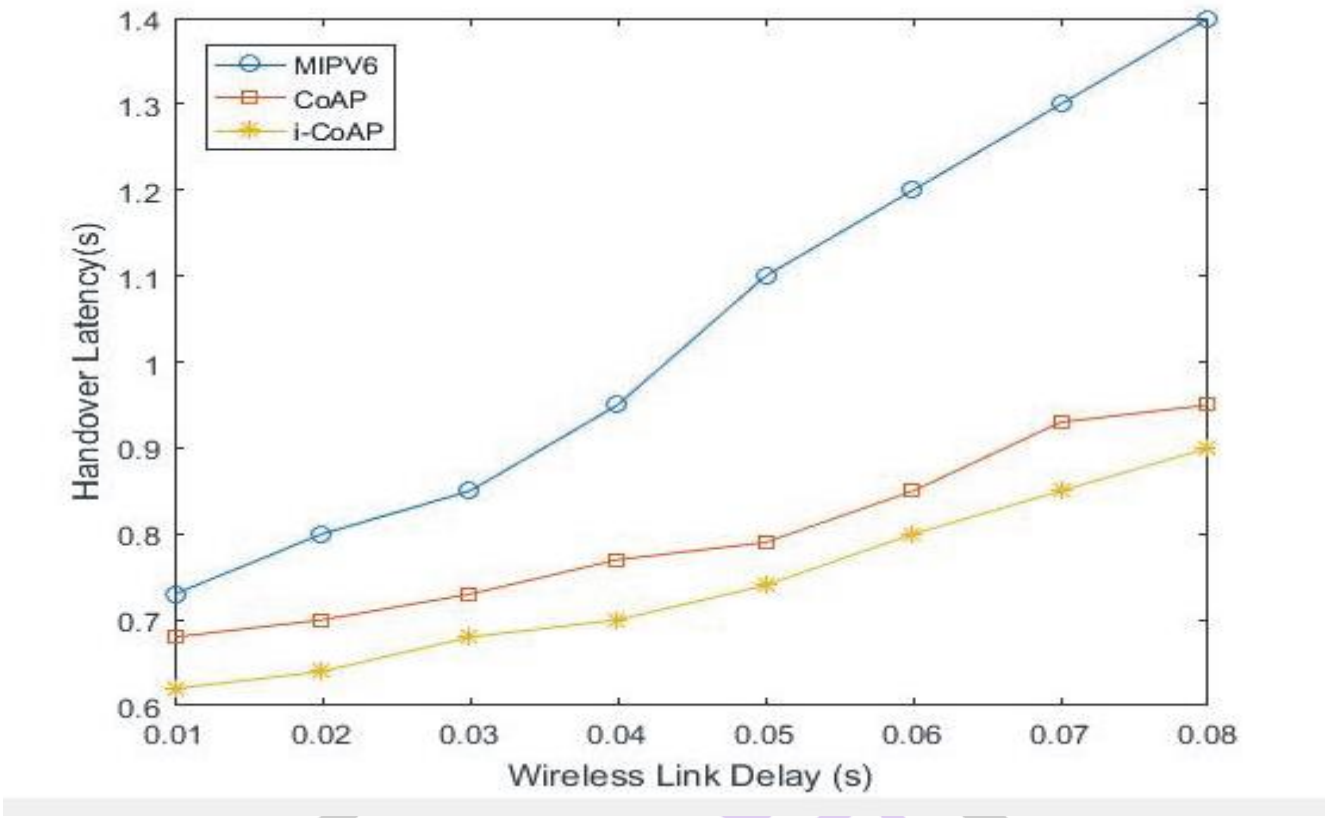


Figure 2.1 Impact of Wireless Link Delay on Handover Latency

Figure 4.1 shows the change in handover latency of the mobility protocol based on changes in the wireless link delay. The handover delay can be as large as the number of the control packets during the handover between the WSN BS and CoAP node increases. As Figure 4.1 shows, the handover latency of the proposed i-CoAPs is similar to the results of the CoAp. For CoAP, a BU message is exchanged between the CoAP node and MAP. In contrast, for i-CoAP, a PUT BU request message and an ACK BU response message are exchanged between the CoAP node and IMMS.

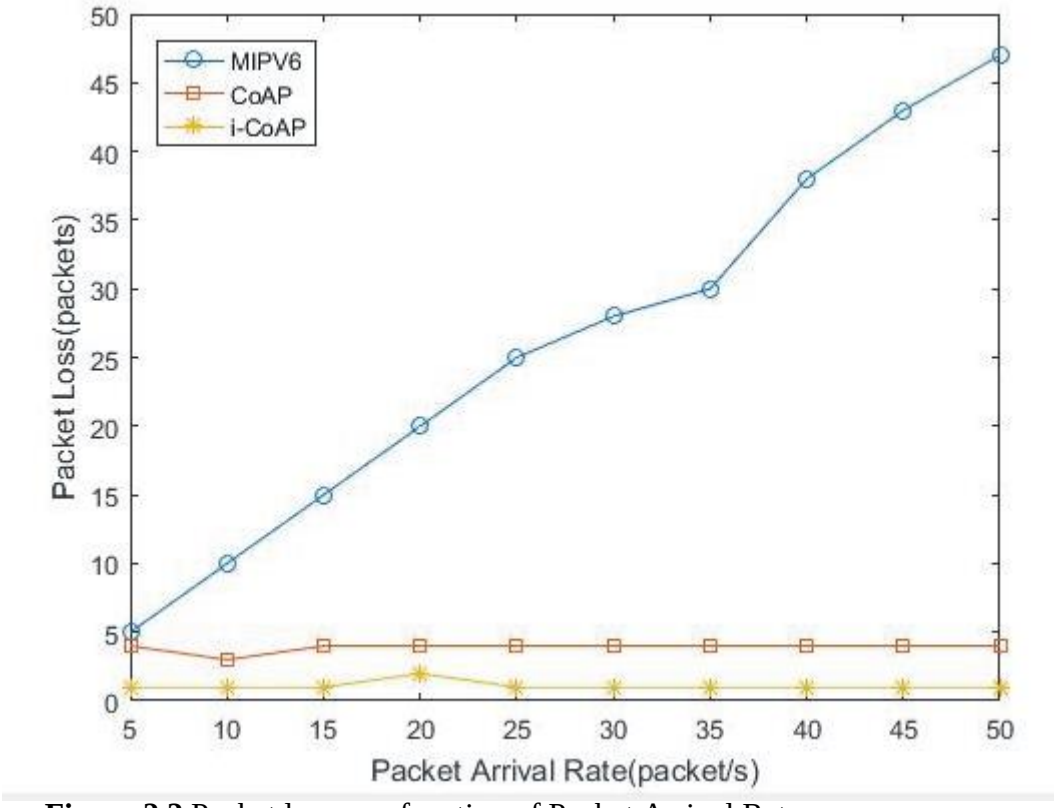


Figure 2.2 Packet loss as a function of Packet Arrival Rate

Figure 4.2 shows the change in packet loss in terms of the packet arrival rate. The packet loss rate is important in service reliability in the IoT. As Figure 4.2 shows, the packet loss of the proposed i-CoAPs is less than that of MIPv6 and CoAP. The packet loss of both MIPv6 and CoAP increases sharply as the packet arrival rate increases. In contrast, almost no packet loss occurs for i-CoAPs because the protocol uses the hold mode of operation.

Table: Packet Loss Analysis

Protocol	Total Packet Loss
MIPv6	λDMIPv6
CoAP	λPDCoAP
i-CoAPS	Zero

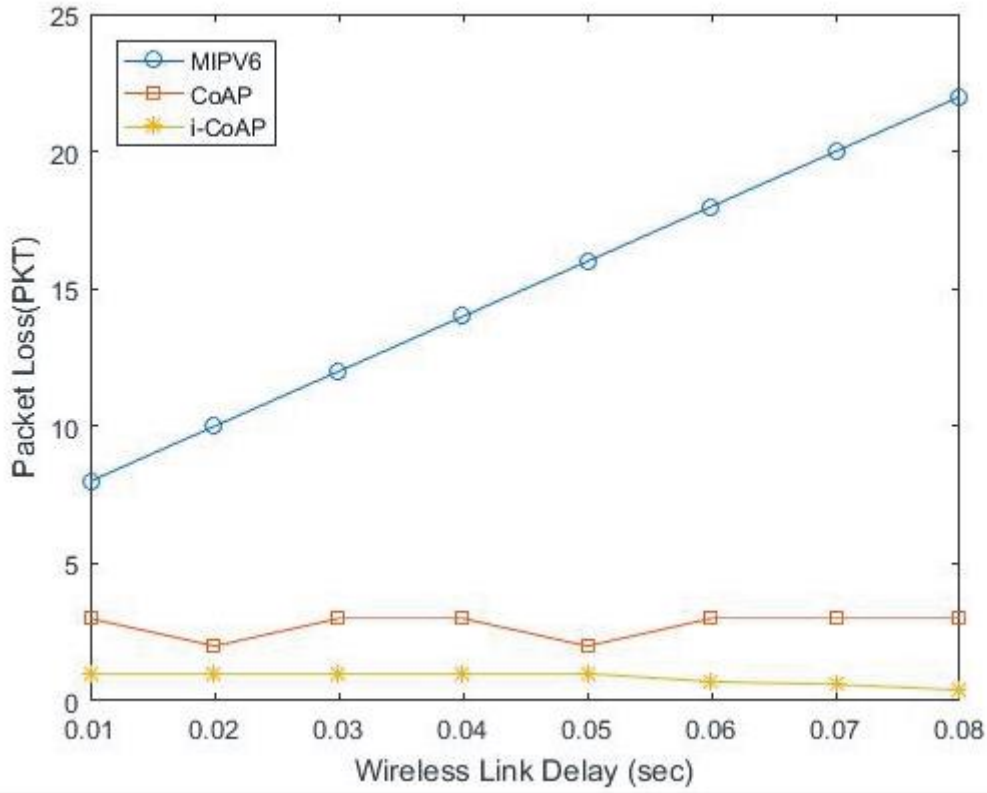


Figure 2.3 Impact of wireless link delay on packect loss

Figure 4.3 shows the impact of packet loss with regard to a variety of wireless link delays. To measure the packet loss with regard to the wireless link delay, the value of λp was set to 10 packets/s; *LWL* was set to 0.002 s; and *LW* was set to vary between 10 ms and 80 ms. In MIPv6 and CoAP, packet loss increases as *LW* increases. However, in i-CoAPs, the amount of packet loss is less than that of CoAP and MIPv6 under the conditions of varying wireless link delays. In i-CoAPs, the PUT holding mechanism can be dynamically reduced.

Contribution to the Body of Knowledge

In this research work we presented an improved constraint Application Protocol based mobility management for Internet of things by adding two mobility modes caching and tunneling during handover operation. The analysis results show that the proposed scheme outperformed the existing CoAP on efficiency in performance with regard to handover and packet loss.

Summary

The discussions in the previous sections show that the proposed improve algorithm outperforms the various mobility management protocols. The next chapter of this dissertation summaries and concludes the research.

SUMMARY, CONCLUSION AND FUTURE WORK

Summary

Internet of Things is a simple idea of connecting identified objects through wireless connection where they could communicate with each other and be able to identify themselves to other devices, most devices associated with IoT are mobile and therefore required special mobility management protocol to maintain and preserve IP mobility, such protocols are needed to provide mobile devices with uninterrupted access to mobile services while moving within networks and remaining interconnected. IoT devices can become unavailable due to handover delays or network disconnection. In this dissertation we improved the constraint application protocol by adding two modes, caching and tunneling during handover operation.

The analysis result show that the proposed i-CoAP comparing with the existing ones, demonstrates a high efficiency in performance with regard to handover latency and packet loss.

5.2 Conclusion

The research proposed method for reducing handover latency and packet loss for improving Constraint Application Protocol, it was observed from conducted analysis the performance of the proposed improve constraint application protocol is faster than the existing one based on the following:

1. Before disconnecting using old connection and attaching to the new one the node will establish a temporary address and creates a tunnel as soon as it detects a new link following this it will start sending packets when reconnected to the new point of attachment.
2. Analysis show that the propose scheme produces an enhancement in handover latency and packet loss.

Recommendation for Future Work

The objectives of this research were achieved. Future work may be required to be done on the security aspect of the proposed mechanism.

The proposed algorithm can be validated using simulation.

REFERENCES

Ahmad, A., Paul, A., Rathore, MM., Rho, S., (2015). Aware Mobility Management of M2M for IoT Communication. 1-14

Akyildiz, F., Weilian, Su., Sankarasubramanian, Y., Cayirci, F.(2002). A Survey on Sensor Networks Communication Magazine

Akylidiz, I. F.,. Altunbasak, Y. and Siva Kumar, R. (2004). An adaptive protocol suite for the next-generation wireless internet. IEEE communication magazine, Vol. 42, No. 3 March 2004, pp. 128-136.

Akyildiz, I. F., Xie, J. and Mohanty, S. (2004). A survey of mobility management in next-Generation, all IP-Based wireless system. IEEE wireless communication magazine, Vol. 11, No. 4 Aug. 2004, PP. 16-28.

Akyildiz, I. F., Xie, J. and Mohanty, S. (2005). A Ubiquitous mobile communication architecture for next heterogeneous wireless system. IEEE communication magazine Vol. 43. No.6 jun. 2005 pp.29-36.

Angelo, P., Castellami, Mattiam, Gheda., Michele, Zorzal., (2011). Web Services for Internet of things through CoAP and EXI, IEEE International Conference on Communication Workshop pp. 1-6.

Bauer, M., Riaz, A., (2016). A study of network based mobility management schemes 6LoWPAN mobility, open Issues and proposed Solution, Department of Electrical and communication engineering NIT, Kashimir

Bandoyo, S., Padhyay., Sengupta, M., Maiti, S., and Dutta, S.(2011). Role of Middleware for Internet of Things. *International journal of Computer Science and Engineering Survey* Vol. 2. No. 2, pp: 94-105

Bormann, C., and Shelby, Z.(2012). Blockwise Transfer in CoAP Internet Engineering Task Force. Constrained RESTFul Environment Group Internet Draft.

Bouaziz, M., and Rachedi, A., (2016). A Survey on Management Protocols in Wireless Sensor Networks Based on 6LowPAN Technology.

Brandt, A., (2011). Discovery of CoAP Servers Across Subnet Internet Engineering Task Force Constrained Restful Environment Group Internet Draft.

Chai, R., Zhao, YL., Chen, Q., Tang, L.(2009). Group Mobility in Wireless Sensor Network. *International Conference on Wireless Communication Signal Processing* (wcsp).

Chauhan, D., and Sharma, S.(2014). A Survey on Next Generation Internet Protocol IPv6 *International Journal Electron Industrial Engineering (IJEE)* ISSN 2. pp: 125-128

Chen, S., Hu, B., Sun, Q., Jiang, Y. (2009). A Performance Evaluation of IPv6-Based Network Mobility Management. *Proceeding of the 5th International Conference on Wireless Communication Networking and Mobile Computing*. pp: 1-4

Chun Seung-Man., Hyun-Su Kim,. And Jong-Tae Park (2015). COAP – Based Mobility Management for Internet of Things, School of Electronics Engineering, College of IT Engineering, Kyung Pook National University Daegu, Korea.

Chun, SM., Kim, HS., Park, J., (2015). CoAP- Based Mobility Management for Internet of Things. 16060-16032.

Constrained Application Protocol (CoAP). (Accessed on 2017) Available online *http://tool.ietf.org/html/rfc* 7252

Deering, SE., Hinden, R.,(2016). Internet Protocol Version 6 (IPv6) Specification, http://www.rfceditor.org/info/rfc2460

Deng, J., Heinzelman, Y., Varshney, P., (2005). Scheduling Sleeping nodes in high density cluster based sensor networks.

Devarapalli, V., Chowdhury, K., Gunarelli, S., Patil, B., Leung, K., (2013). Proxy Mobile IPv6 Available from http://tools.left.org/html/rfc213

Gundavelli,S., Leung, K., Devarapalli, V., Chowdhury, K., and Patil, B., (2017) Proxy Mobile IPv6 RFC 5213.

Frieder Ganz,. Ruidong Li,. Payam Barnaghi,. (2012) A Resource Mobility Scheme for Service-Continuity in the Internet of Things,. Centre for Communication System Research, University of Surrey Guildford, United Kingdom.

Gershenfield, Chan, H., and Liu, U., (2004). Requirement for Distributed Mobility Management, IETF RFC 7333.

Gundevelli, S., and Jeon, S., (2008). DMM Deployment Models and Architecture Consideration, Draft –ietf deployment models.

Harlke, K., and Shelby, Z., (2012). Observing Resource in CoAP Internet Engineering Task Force Constrained Resful Environment Group Internet Draf

Hierarchical Mobile IPv6 Mobility Management (2015). Available online http://toolsletf.org/htmlrfc4140

Haripriya, Y., Pavani, K., Lavanya, S., Viswanatham, VM., (2015). A Framework for detecting Malicious Nodes in Mobile Adhoc Network. *International Journal of Science and Technology*. pp:151

Jabir, AJ., Subramaniam, SK., Ahmed, ZZ., Hamid, N.,(2012). A Cluster-Based Proxy Mobile IPv6 for IP-WSNs. EURASIP *Journal on Wireless Communication Network* pp:1-17

Jani Puttonen,. (2006). Mobility Management in wireless networks,. University of JYVASKYLS 2006.
Jaydip Sen,. Mobility and Handoff management in wireless networks. (2006). Tata Consultancy Services, India pp. 45
Jeschke, S., Brecher, C., Song, H., Rawat, D.,(2016). Industrial Internet of Things, Cyber Manufacturing System, Springer Chan Switzerland.
IBM A Smarter Planet.(2016) http://www.ibm.com/smarterplanet/us/en.
Islam, MM., Huh EN., Sensor Proxy Mobile IPv6 (SPMIPv6). (2011). A Novel
Scheme for Mobility Supported IP-WSNs 1865-1887.
Jabir, AJ,. Ahmad ZZ, (2012). A Cluster- Based Proxy Mobile IPv6 for IP-WSNs. EURASIP. Wireless Communication Network.
Jaydip, Sen., (2004). Mobility and Handoff Management in Wireless Networks, Tata Consultancy Services, India. Pp 22-23.
Jong, Tea, Park., (2015). Hierarchical Mobile IPv6 Mobility Management Available online. http://tool/ietf/html/rfc4068.
Kai, C., Zhimin, Y., Rongyi, C., Chenghao, L., (2008). A Handoff Algorithm based on Care of Address Pool of Hierarchical Mobile IPv6 in Proceeding of *3rd International Conference on Pervasive Computing and Application*. pp: 302-306
Koodli, R., (2016). Mobile IPv6 Fast Handover IETF RFC 5568do.10.17487, http://www.rfc-editor.org/info/rfc5568.
Kushalnagar, Q., Zhour, R., and zheng., (2016). Proceeding of 2nd Internetional Conference on Logistic Informatics and Service Science PP.751-756 doi:10 1007/978.
Loong, Sye., Sardeep., (2014). Security in The Internet of Things A Standandization perspective, Internet of Things Journal IEEE, Vol. 1 Issue 3, pp. 265-275.
Makaya, Christian., Pierre, Samuel ., (2008). An Analytical Framework for Performance Evaluation of IPv6-Based Mobility Management Protocols. IEEE Transaction on wireless Communication vol.7 No. 3.
Maria, Rita, Palattella., Thomas, Wattey., Luigi Alferedo, Gree., (2013). CoAP Standardized Protocol Stack for the Internet of (Important) Things, Communication Surveyand Turtorials IEEE pp1389-1406.
Mobility Support in IPv6 (2015). Available Online. http://www.rfc-editor.org/html/rfc4068
Mohanty S., (2006). A new architecture for 3G and WLAN integration and inter-system handover management wireless networks, Vol. 42, No. 6, November 2006, pp. 733-745.
Narten, T., Simpson, W., (2016). Neighbor Discovery for IPv6. Rfc 246
Petersburg ST., 2012. Internet of Things, Smart Space and Next-Generation Networking,. Russia August 2012.
Perkins, C., Falowo, O., (2011). Distributed Mobility Management Scheme with Mobility Routing function as the Gateways. Proc of IEEE.
Qin, Y., Shen,QZ., Falkner,NJG.,Dustdar, S., Wang, H., Vasilakos, AU.,(2016). A Survey on Data-Centric Internet of Thing, *International Journal on Network Computer Application pp:137-153*
Rahaman, A., and Dijik, E.,(2012). Group Communication for Internet Engineering Task Force Constrained Restful Environments Group.
Safwan, Ghaleb., Shamala, Subramaniam,. Zuriat, Ahmed., Zukarnain, and Abdullahi, Muhammed., (2016). Mobility Management for IoT a survey. *EURASIP Journal on Wireless Communication and Networking.*
Safwan, G., Shamala, S.,(2016). Mobility Management for IoT a Survey EURASIP Wireless Communication and Networking
Seung-Man, C., Jong-Tae P., (2016). A mechanism for Reliable Mobility Management for Internet of Things Using CoAP
Seung, Man-Chun., Hyun, Su., and Jong, Tea Park., (2015) CoAP-Based Mobility Management for Internet of Things. School of electronics Kyung Pook National University Daegu Korea.
Seung, Man., (2015). Mobility Support in IPv6. Available online, http:www.rfc-editor/info/rfc3775.
Silva, R., Silva, JS., Boavida, F., (2012). A Proposal for proxy-Based Mobility in WSNs Computer Communication.
Solmaz, S., and Ramin Shamshiri., (2015) A Survey on Mobility Management Protocols in Wireless Sensor Network-Internet Protocol. *Indian Journal of Science and Technology Vol 8* ISSN 0974-5645
Soliman, H., Castellucciac, Malik, Bellier, L.,(2013). Hierarchical Mobile IPv6 Mobility Management (HMIPv6). Available http://www.left.org.rfc/rfc4140.
Shelby, Z., (2010). Embedded Web Services IEEE Wireless Communication pp:52-57