Mobile Networks and Applications
https://doi.org/10.1007/s11036-018-1007-1

A Route Optimized Distributed IP-Based Mobility Management Protocol for Seamless Handoff across Wireless Mesh Networks

Peer Azmat Shah[1] · Khalid Mahmood Awan[1] · Zahoor-ur-Rehman[2] · Khalid Iqbal[2] · Farhan Aadil[1] · Khan Muhammad[3] · Irfan Mehmood[4] · Sung Wook Baik[3]

Abstract
A Wireless Mesh Network (WMN) can provide Internet connectivity to end users through heterogenous access network technologies. However, the mobility of mobile nodes across these access networks in WMNs results in service disruption. Existing mobility management protocols are designed for single hop networks and are centralized in nature. A Distributed IP-based Mobility Management Protocol (DIMMP) is proposed in this paper that provides seamless mobility with service continuation for mobile nodes when they roam across WMNs. Instead of relying on a centralized mobility anchor, the mobility functionality is distributed at multiple nodes in the WMN, in order to reduce the chances of potential single point of failure. The proposed protocol manages both types of mobilities i.e. intra-WMN and inter-WMN and uses a new enhanced route optimization procedure. Simulation results show that this work has contributed by improving the performance of handoff procedure with respect to handoff latency, packet loss and signalling overhead, as compared to the existing protocols.

Keywords Wireless mesh network · Route optimization · Distributed mobility management · Handoff latency · Signalling overhead

1 Introduction

With the proliferation of mobile devices, wireless connectivity has become ubiquitous. Hence, due to an increase in the variety of mobile devices, the classical opinion of having wired connectivity in the Internet is now changed and new scenarios of mobile applications have emerged. In this regard, more and more Internet services of both conventional and novel types are being smoothly accessed using various mobile devices through wide deployment of wireless networks. The Internet is extending its coverage area, which brings more opportunities for the service providers and the network operators to expand their network. For users, this means more benefits and conveniences in their work and daily life.

In addition, the evolution of 4G wireless networks, all-time access and seamless mobility across different networks, like WLAN, WiMAX, UMTS and WWAN etc., are desirable [1, 2]. For example, mobility from a cellular network to a satellite-based network or to a high bandwidth WLAN is possible. Utilizing this attribute, users will benefit from features like access to different services, increased coverage, and all-time access with more reliable wireless access that will work even in the failure of one or more networks. Due to this versatility, the Internet users want to use the best access network, according to their preferences network characteristics or their own preferences. This leads to the deployment of Wireless Mesh Network (WMN), which allows self-healing [3], fast, easy and affordable network deployment due to its adhoc nature and provides all-time Internet access to mobile devices using the heterogeneous access networks [4].

The WMNs are multi-hop wireless networks that have the capabilities of self-healing and self-configuration. Just like

✉ Irfan Mehmood
irfanmehmood@ieee.org

[1] Internet, Communication & Networks (ICNet) Research Lab, Department of Computer Science, COMSATS Institute of Information Technology, Attock 43600, Pakistan

[2] Pattern Recognition, Images and Data Engineering (PRIDE) Research Lab, Department of Computer Science, COMSATS Institute of Information Technology, Attock 43600, Pakistan

[3] Digital Contents Research Institute, Sejong University, Seoul, Republic of Korea

[4] Department of Software, Sejong University, Seoul, Republic of Korea

Published online: 15 February 2018

mobile adhoc network (MANET) and wireless sensor network (WSN), the hosts of a WMN may rely on each other to maintain network connectivity in adhoc manner. Unlike MANET and WSN, in WMNs according to functionalities and roles the nodes can be divided into two types: wireless mesh routers and wireless mesh clients. Mesh clients are the end nodes which can enter or leave the WMN at any time. These are the mobile nodes having user applications running on them and connect to the Internet through the connection provided by the WMN. Example of these devices includes smart phones, laptops, PDAs and sensor nodes etc. Whereas, wireless mesh router performs some additional routing functions for supporting mesh networking in addition to the routing functionalities as a simple wireless router, as discussed by Akyildiz et al. [5]. These WMN routers can be categorized into three main categories: router with gateway functionality, relay routers and access routers. The mesh routers that are connected to the backbone Internet are termed as Mesh Border Gateways (MBG). Relay routers are used to forward data between gateway routers and access routers. The access routers usually provide the last hop connectivity to the mesh clients in WMN. On the basis of functionality of nodes, [5] has discussed that the WMN can be divided into three types. Focus of this this work is the Infrastructure WMN (IWMN) which is shown in Fig. 1.

In the last two decades, research community started working to resolve the issues related to interoperable wireless networks such as access, handoff, location and resource coordination, quality of service, wireless security and authentication, in order to provide the Internet services through different access technologies. To address these issues for implementing the features required, the vital role will be of network architectures. When using this architecture of Internet with heterogeneous access networks, a Mobile Node (MN) can move from one access network to another. Hence, the communication that was established previously with a Correspondent Node (CN) remains no longer active due to change in its point of attachment, which results in its Internet Protocol (IP) address change. Since the IP addresses of communicating nodes are used for the association between them, hence all on-going communications will be inactive when IP address of one of the communicating parties changes due to mobility [5]. Hence, mobility management process is essential for service continuation.

The paper is planned as follows. In Section 2, motivation of doing research in this area is discussed. Section 3 analysed the related work and highlighted the shortcomings in the literature. In Section 4, the working of proposed protocol DIMMP is given. Section 5 modelled the signalling overhead of DIMMP and Section 5.2.1 presents the performance analysis. Finally, Section 6 draws the conclusion along with future research directions.

2 Motivation

A mobility management protocol allows users to roam across heterogeneous access networks while simultaneously offering them incoming session requests and supporting sessions in progress [6]. To achieve this objective, mobility management can be further classified into two categories: traditional mobility management in single hop networks and mobility management in multi-hop networks. The problem of mobility is also faced in the multi-hop WMNs, just like traditional wireless networks. The reason is that, the transmission range of wireless antennas used in WMNs is still limited. In a mobile environment, the mesh clients will have free mobility; therefore, the question of how to maintain connectivity of network applications active is very important in the mobile environment.

The performance of existing solutions for mobility management protocols like Mobile IP and its variants is not good in WMNs. A simulation based evaluation was carried in [7] for Mobile IPv4 in the WMNs. Their findings disclosed significant increase in the handoff latency when number of wireless hops were increased between MN and wired Internet [7]. It was also shown through simulation that handoff latency of the network layer is more affected than the link-layer handoff latency due to multi-hop nature of WMN. It is due to the latency of route discovery and amount of global signalling messages propagation.

The reason for this degraded performance of existing mobility management protocols is that they are based on a centralized architecture which rely, to a certain extent, on centralized entity for mobility signalling and data forwarding. Due to this centralized architecture, mobility management protocols are vulnerable to several limitations, as discussed in [8] and [9]:

- Less or non-optimal and long routes.
- Signalling overhead (that results in handoff latencies).
- Higher vulnerability due to the presence of a probable single point of failure and potential bottleneck.

In comparison to the traditional mobility management, multi-hop wireless networks, require connection management in addition to the basic mechanisms of mobility management, as presented by [10] and [11]. It refers to the route reconfiguration and resource management. Also, the mobility of mesh terminal nodes (clients) may be intra-WMN or it may be inter-WMN (from one operator's mesh network to another operator's mesh network) [12]. Unfortunately, the mobility management approaches in literature either try to solve the intra-WMN mobility or the inter-WMN mobility. Even in some cases both types of mobility are handled, however the inter-WMN mobility is usually achieved

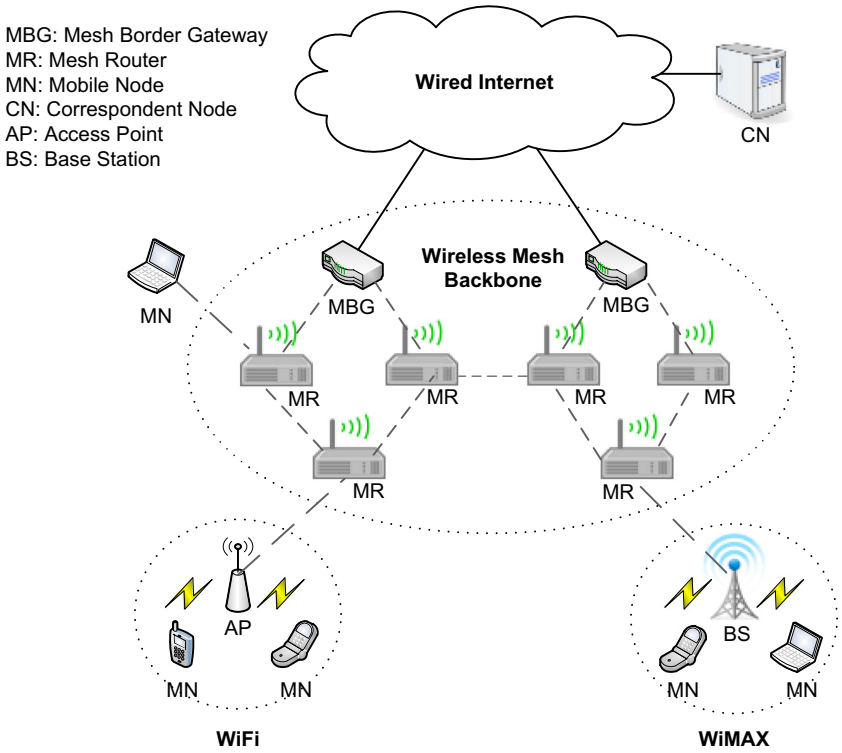

Fig. 1 Infrastructure wireless mesh network

through Mobile IPv6 that practices global signalling using return routability based route optimization. The return routability introduces high handoff latency, overhead of signalling and packet loss in the handoff [13].

Because of the above discussed complications in handover process, design and development of a new mobility management mechanism is desirable that exploits the features of the WMN for multi-hop and have no dependence on a central network entity, rather is distributed in nature. The goal is to minimize the handoff latency by maximizing the mobility anchor points availability without producing coordination overhead.

3 Related work

For the last several years, research community is working on mobility management in WMN and they have proposed many solutions to manage this problem. Some of the well-known solutions from literature, their pros and cons are debated here.

3.1 Mobility management solutions for WMN

Boukerche and Zhang [14] and Majumder et al. [15], discussed that the mobility management protocols for WMNs can be categorized into three major categories, that is, tunnelling-based, routing-based, and multicasting-based.

3.1.1 Tunnelling-based solutions

These solutions support the mobility by managing the IP address change of MNs. These solutions use a hierarchical architecture in the WMN, where a high-level mobility anchor node adds an additional IP header, encapsulates the packet and then forwards to a lower anchor node in the hierarchy. The low-level anchor node removes the extra IP header by decapsulation and forwards to the destination MN. Usually, the new wireless mesh router to which MN attached after mobility serves as low-level anchor node and the previous mesh router from which MN moved serves as the high-level anchor node. Some of the well-known tunnelling-based mobility management solutions for WMN are proposed in [16–22]. Major problems with these solutions are the overhead of encapsulation and decapsulation and dependence upon some centralized mobility anchor up in the network hierarchy.

3.1.2 Routing-based solutions

These solutions modify the multi-hop routing protocol to facilitate the handoff. The routing tables are updated for the re-establishment of connection after the handoff. Usually, such solutions work with the assumption that MN does not change its IP address due to mobility and are deployed for intra-WMN mobility. In this situation, the routing information is updated in the mesh routers for the new location of

MN. Some of these solutions are discussed in [23–30] and [31]. Problem with these solutions is that, these can only be used in scenarios where MN does not change its IP address while mobility and are restricted to intra-WMN mobility only.

PaRtIal path establishment based handover Management tEchnique (PRIME) [23] aims to catch a node (crossover node) from the old path, having a route to the target Base Station (BS) of the MN with the required bandwidth. To process the handoff, the routing tables of crossover node are updates accordingly. The IMeX [32] is a routing-based solution that supports both intra and inter-WMN mobility. It facilitates parallel execution of handoff from multilayers, and uses a data caching procedure in order to ensure minimum packet loss during the handoff. The proposed IMeX uses the Mesh Routers (MRs) and groups them into linked groups which are rooted at each gateway MR. Each group corresponds to a different subnet and MRs have a different IP address prefix belonging to different groups. The Xcast-based Group Routers (XGRs), which are special MRs, belong to more than one subnets and are furnished with multiple IP addresses and each IP corresponding to a different subnet. The handoff for intra-WMN mobility is performed efficiently in PRIME and IMeX, however, in the case of inter-WMN mobility there is no common crossover node or XGR between the old and the new subnet that can manage the L3 delays. In such case, Mobile IPv6 will be used that causes delays and overhead and consequences to possible bottleneck and single point of failure.

Pointer forwarding based solutions are also discussed in literature [33–37] that are the variants of routing-based solutions. In these mobility solutions, the entire routing information is not updated in the mesh network rather a pointer is forwarded for each handoff from one access mesh router to another.

3.1.3 Multicast-based solutions

The mobility management protocols which use multicast are proposed in [38] and [39] for WMN. These solutions assign the access routers (old and new) to the multicast group and data is received by both access routers for smooth handoff. These solutions have a general problem of multicast overhead and restrict the mobility to intra-WMN.

3.2 Distributed mobility management solutions

In 2010 research community realized the problem of potential bottleneck and single point of failure for existing mobility management solutions and started working on distributed mobility management. In this context, the Internet Engineering Task Force (IETF) renamed and re-chartered the Mobility Extensions for IPv6 (MEXT) working group as the Distributed Mobility Management (DMM) working group in 2011 in the IETF82 meeting. The work being done in this working group is at initial stages and only the requirements for distributed mobility management have been standardized [40]. The other solutions being proposed as individual drafts are not mature and need a lot of work.

Some distributed mobility management solutions have also been proposed in literature. These include [41–49] and [50]. Majority of these solutions provide local mobility services within a domain. Even in the case that some provide global mobility service, they are based on tunnelling and have not provided any route optimization mechanism that results in handoff latency and signalling overhead. Also, these solutions are proposed for single hop networks and are based of existing Mobile IPv6 and its variants, hence suffers for performance degradation when used in the WMNs, as discussed by [7].

4 Protocol operation

To address the problems of mobility management protocols discussed in previous section, this section attempts to propose a new fully distributed mobility management protocol for WMN. For this purpose, Distributed IP-based Mobility Management Protocol (DIMMP) with six components is proposed. Each component of DIMMP is discussed in detail in the upcoming sub-sections. Using these components, the mobility functionality is distributed to multiple wireless MBGs, Mobility Anchor Routers (MARs) and at the end nodes in the network without relying on a centralized network entity. The aim is to minimize the service disruption (handoff latency) and Single Point of Failure (SPOF), signalling overhead (Sig_ovrehead), packet loss (Pkt_loss) and to maximize the security. The objective function is defined as per [51, 52] in Eq. 1.

$$F_{DIMMP} = \mathcal{F}(\text{Latency}, \text{SPOF}, \text{Sig\_overhead}, \text{Pkt\_loss}, \text{Security}) \quad (1)$$

4.1 MBG discovery and registration

After entering an access network in the WMN, MN first gets an IP address. MN must keep record of the MBGs through which it is connected to the Internet in the WMN, so that MN can interact with these MBGs for session continuity. To keep this record, MN performs the MBG discovery process.

For MBG discovery, MN sends the Gateway Solicitation message M_j towards MBGs which are part of a multicast group in the WMN. This message is just like Home Agent (HA) Discovery message used in the Mobile IPv6. The source address of the Gateway Solicitation message is typically the Home Address (HoA) of the MN if MN is being attached to the WMN for the first time or it may be the MN's Care-of

Address (CoA) if the MN has already done mobility from its home network earlier.

The MBGs must respond back to the MN's Solicitation message and unicast the encrypted Solicitation Acknowledgement (ACK) message to the respective MN directly on the source address that MN has chosen for Solicitation. The MN, upon receiving, decrypts the Solicitation ACK message and keeps record of the IP address of each MBG from which it has received an ACK by updating its MBG list. Each MN maintains a data structure, MBG list, to keep a record of the serving MBGs. In case of intra-WMN mobility, MN will be depending on these MBGs for its session continuity. The reason to encrypt the messages and to authenticate the MBGs by the MN is to avoid the intruders to get control of the MNs and the MBGs. Algorithm 1 describes the wireless MBG Discovery and Registration procedure. It is assumed that access to Public Key Infrastructure (PKI) through the WMN is available.

Algorithm 1: Mesh border gateway discovery and registration

```
1.  START
2.  MN j ∈ N multicasts the Gateway Solicitation message Mj:
    j → multicast : Mj= E_PR(j) (ts, Certj)
3.  IF wireless MBG i ∈ G receives Mj
4.      i verifies Mj with public key PKj of j
5.      IF the signature is verified
6.          i unicasts the response Gateway Solicitation ACK Mi:
            i→ j : Mi = E_PK(j) (IPi, Certi)
7.      ELSE
8.          Error is returned
9.      END IF
10. END IF
11. IF j receives Mi from i
12.     j checks that any request Mj was sent earlier
13.     IF any request was sent
14.         j verifies Mi with public key PKi of i
15.         IF Mi is verified
16.             j updates MBG list
17.         ELSE
18.             Error is returned
19.         END IF
20.     ELSE
21.         Discard the message
22.     END IF
23. END IF
24. END
```

4.2 Correspondent node compatibility

The CN compatibility test is performed for the calculation of shared secret *Token*, and to check whether CN supports DIMMP or not. For this purpose, signalling is performed at the start of communication between MN and the CN. This compatibility status of CN will help to reduce the handoff latency and signalling overhead during the handoff process.

Algorithm 2 shows this procedure where the shared secret key K is computed from public keys k, which are computed using the Complex Conversion Routine Encoding (CCRE) and the permutation function applied on 128 bits (P128). The process is done through Elliptic Curve Diffie-Hellman key exchange through the option negotiation. The protocol messages for the proposed CN compatibility, Node Status Request (NS_REQ) and Node Status Response (NS_RES), are carried within the IPv6 Mobility Header [53]. The CN compatibility details can be read from [54] and the Algorithm 2 defines this process for the initiator and responder sides separately and Fig. 2 shows the message exchange.

4.3 Link status classification & data caching

DIMMP employs the fuzzy logic based link status classification mechanism as explained in our previous works [55, 56]. The link status classification system uses fuzzy input variables Received Signal Strength Indicator (RSSI), velocity, distance and bit error rate and classifies the link status as active, about-to-break and broken. Based on link status, the data caching of DIMMP is triggered. Using this procedure, if the link status is about-to-break and MN has no option for connectivity to any alternate access network, means MN is present in a non-overlapping coverage access region, then the MN sends *Cache Request* message to the serving MBGs in order to buffer the incoming packets for the particular IP address that may not be available after some time. The MBGs which are receiving data for that MN from the Internet start buffering the incoming packets destined to that IP address, mentioned in the *Cache Request* message, and respond with *Cache ACK* message.

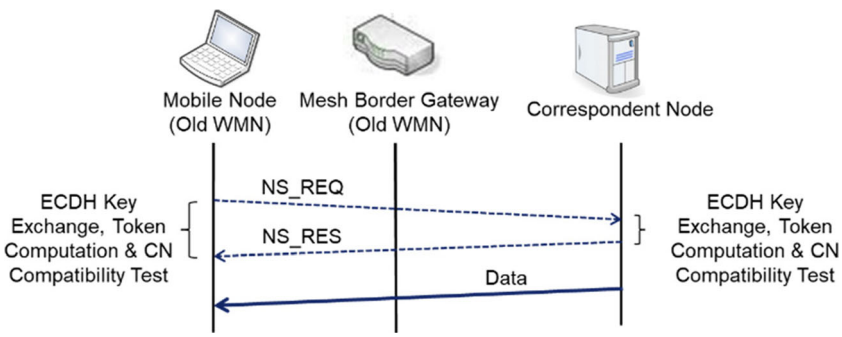

Fig. 2 CN compatibility message exchange

In case of broken link status, MN does not send the *Cache Request* message as it is not reachable at its previous location. Similarly, when MN is present in overlapping access region of two or more access networks, then MN has already performed the Layer 2 connectivity and can get a new IP address (Layer 3 connectivity) in the new network. As MN is still reachable through old network and can receive data, hence there is no need to send the *Cache Request* message.

Algorithm 2: Correspondent node compatibility procedure

Initiator side:

```
START
Initialize Xi= Random{1,2,3,……..,n-1}
ki= P128[CCRE(Xi * a)]
Send NS_REQ to other node
Receive message from responder node
IF(Received NS_RES)
    K= ki*Xj
    Token= SHA1(Xi,Xj,K)
    Update CN compatibility list as True
ELSE
    Update CN compatibility as False
END IF
END
```

Responder Side:

```
START
Receive NS_REQ from initiator side
IF (DIMMP compatible)
    Initialize Xj= Random{1,2,3,……..,n-1}
    kj= P128[CCRE(Xj * a)]
    K=kj*Xi
    Token=SHA1(Xi,Xj,K)
    Update CN compatibility list as True
    Send NS_RES
ELSE
    Send ICMPv6 error message
END IF
END
```

4.4 IP-layer handoff management

Handoff management by DIMMP is performed in a distributed manner which is achieved through multiple MBGs, MARs and the end nodes. It is assumed that the link-layer handoff follows the legacy handoff procedures in the client network. However, to trigger the IP-layer handoff, link status classification and gateway discovery and registration procedures are used. The intra-WMN and inter-WMN handoff are executed in a different manner.

4.4.1 Intra-WMN handoff management

In case of MN's mobility across access networks within the administrative domain of a single WMN, the entry and exit points (MBGs) for all access networks with the rest of the Internet remains unchanged. Hence, Mobile IPv6's return routability and route optimization procedure to update the binding entries at the CNs create extra signalling overhead. The reason is that, there is no direct path between the MN and the CN except the path through the MBGs. The only way to perform handoff with an optimal cost, in this case, is to update the binding entry at the MBGs.

In the case of MN's mobility across non-overlapping coverage access regions, when the MN moves out of the old access network for which the *Cache Request* was sent to the gateways, then the old IP address remains no longer active for communication and the link status becomes broken. After entering a new access network, MN performs the layer 2 connectivity and gets a new IP address (layer 3 connectivity). Now, MN sends the *Add IP Request* message to the MBGs from its new IP address (CoA), to record a binding entry between the old IP (HoA) and the new IP address (CoA). The MBG sends back the *Add IPACK* to the MN. This is just like the Binding Update (*BU)* message used in Mobile IPv6 and its variants, but the difference is that it is sent to all the serving MBGs. Figure 3 shows the sequence diagram for the intra-WMN handoff execution in non-overlapped coverage access regions.

However, only an *Add IP Request* message is sent by MN to the MBG in case two where MN is moving across overlapping access regions. An *Add IPACK* message is received from the MBG. This process is explained in Fig. 4. The control packets are encrypted using the public private key pair to ensure secure communication between MN and the MBG [57]. The control packets sent from MN to the MBG are encrypted first using the MN's private key and then MBG's public key, which guarantees that only authenticated MN has sent the message and integrity of message is assured.

4.4.2 Inter-WMN handoff management

The DIMMP executes optimal inter-WMN handoff using an enhanced route optimization procedure. This process utilizes the status of CN compatibility determined through Algorithm 2. When a MN receives a new *Gateway Solicitation ACK* message with a new MBG IP address that it has not received earlier, then MN concludes that it has entered in a new access network which is part of a new WMN. In this case, MN checks the status of CN's compatibility for DIMMP.

In the case, when CN does not support the DIMMP or to receive the buffered data from the old WMN gateway, MN sends Add IP Request Forward (FWD) message to the new gateway, containing the IP addresses of old serving mesh gateways. New MBG, upon receiving this message, sends Add IP Request to gateways previously serving the MN in the old WMN. This procedure will decrease the handoff control signalling as compared to the Mobile IPv6, where control signalling is also performed between HA and the CN for return routability based route optimization. Figure 5 shows the sequence diagram for the handoff execution in this case.

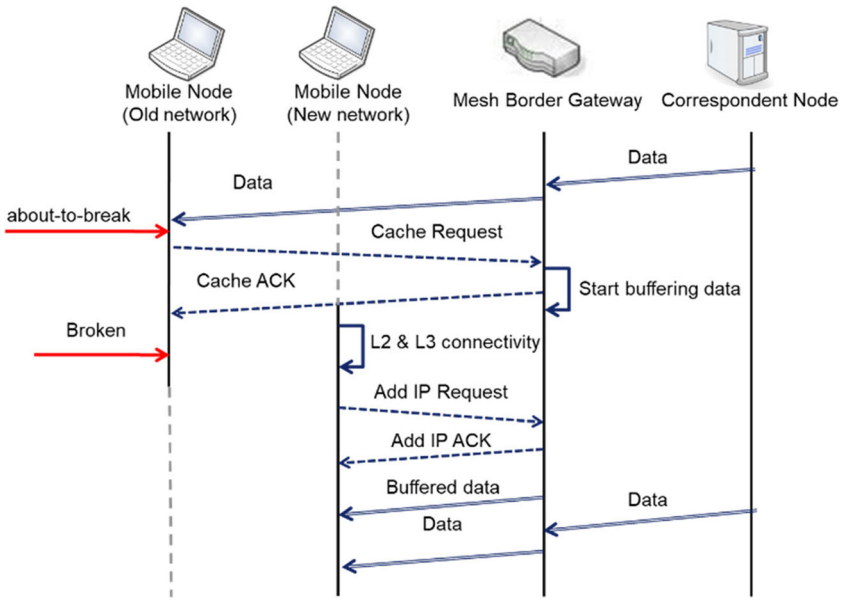

Fig. 3 Intra-WMN handoff execution across non-overlapped coverage access regions

In the other case, when CN also supports DIMMP then there is no need to route the packets through the old MBGs, rather Time based One-Time Password Route Optimization (TOTP-RO) is done. Here, MN interacts with the CN directly as explained next in the enhanced route optimization procedure.

4.4.3 Enhanced route optimization

In the Time based One-Time Password Route Optimization (TOTP-RO) enhancement, two phases are used. In the first phase, signalling is performed at the start of communication between MN and the CN. This signalling is used to check the compatibility of CN for DIMMP and for the calculation of shared secret Token, as already explained in Algorithm 2. In the second phase, MN communicates with the DIMMP compatible CNs directly by sending *Modified Binding Update* (MBU) message. The *MBU* message contains the authentication information as well in addition to the original binding update information. This authentication information includes a One-Time Token (*OTT*) and *Timestamp*. Figure 6 shows the header format for *MBU* message. The details of the enhanced route optimization are discussed in our previous work [13].

The *MBU* header contains additional fields *Timestamp*, *OTT* and *OTT Lifetime* in comparison to standard BU header. *Timestamp* is the timestamp, *OTT* is a 3 Bytes field that contains the OTT value and *OTT Lifetime* is the lifetime for the OTT value contained in the preceding field.

The *OTT* in Eq. 2 is generated using the time based one-time password (TOTP) technique [58] by concatenating the shared secret *Token*, MN's HoA, CoA and the *Timestamp* [13, 54].

$$OTT = TOTP[MD5(Token|HoA|CoA|Timestamp)] \quad (2)$$

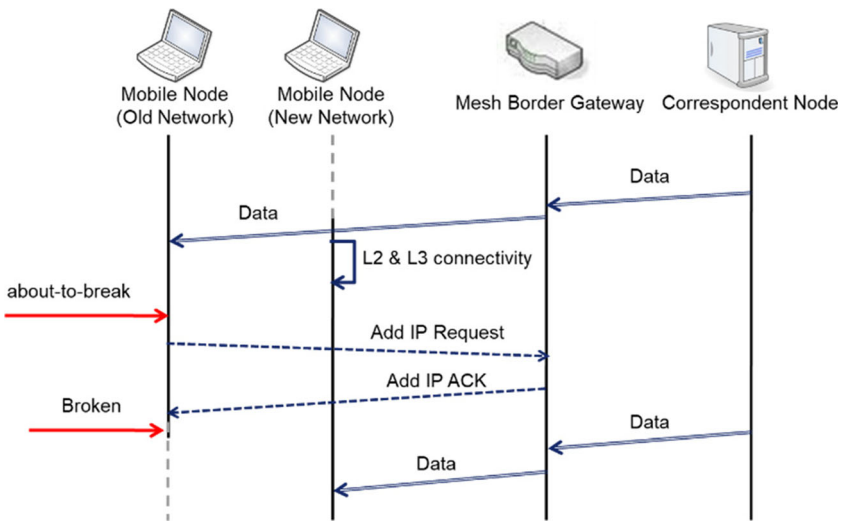

Fig. 4 Intra-WMN handoff execution across overlapped coverage access regions

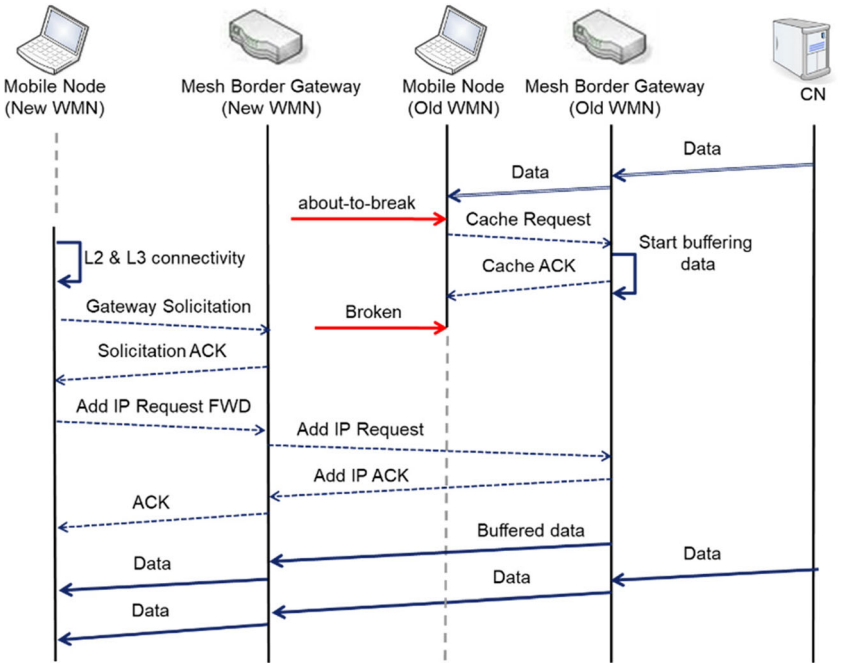

Fig. 5 Inter-WMN handoff execution when CN has no support for DIMMP

Upon receiving the *MBU* message from a MN, the CN computes its own *OTT* taking the HoA and timestamp from the received packet and shared secret *Token* value from its local CN compatibility list. The verification is performed by comparing the computed *OTT* with the received *OTT* value. If both *OTT* values are matched, CN updates the Binding Cache with a binding entry for MN's HoA and CoA and sends the *Binding ACK*, if the Acknowledge (A) bit is set by the sending MN. The HoA is not communicated through the *MBU* header; rather it is mentioned in the home address option which is carried in the Destination Option extension header [53] in the base IPv6 packet. Also, the CoA in not explicitly mentioned in the *MBU* message and it is taken from the source address field of the received IPv6 packet. After successfully updating the binding entry, the CN sends data to the MN's new location (CoA) directly using Type 2 Routing header [53]. Figure 7 shows the sequence of message flow inter-WMN handoff execution with enhanced TOTP-RO procedure when CN supports DIMMP.

To achieve signalling optimization, in the proposed TOTP-RO the Route Optimization signalling are performed only once for a handoff unless there is any need to authenticate the other party. To keep the binding entries at the CN alive, the DIMMP compatible CN does not perform the periodic Binding Refresh Request (BRReq) procedure such as performed by Mobile IPv6, rather the CN and the MBG determine the life of binding entry. When the binding lifetime expires at the CN then it monitors the network traffic for that particular binding entry. If there is no network traffic for a particular MN, for which there exists a binding entry and binding lifetime has expired, then CN sends BRReq to MN. In case, there exists traffic then CN simply updates the binding lifetime to its previous value without sending any Binding Refresh Request to the MN. The MN, upon receiving the Binding Refresh Request message will perform the route optimization procedure in which MBU message is sent to the CN directly.

To handle the binding lifetime at the MBG, while MN sends Add IP Request message to the MBG it adds a flag in it that whether any MBU message has also been sent to the CN or not. In case, option states that a MBU message has also been sent to the CN then the MBG will forward the buffered data to MN's new location and will delete the binding entry

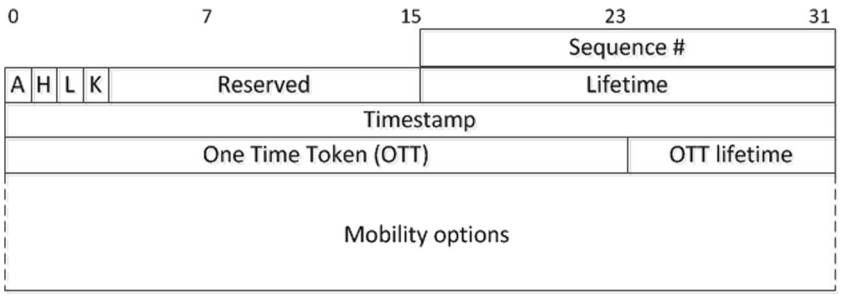

Fig. 6 Modified binding update header format [13]

after forwarding all the buffered data. In the other case, when option states that the MN has not sent any MBU message to CN, the MBG keeps the binding entry and handles it just like handled by the CN. Hence, no additional control traffic is introduced by the DIMMP to keep the binding entries alive at the CN and at the MBG. Algorithm 3 shows the overall handoff process at different nodes.

Algorithm 3: Handoff execution using DIMMP

On mobile node:

```
START
Initialize M = set of MNs, N = set of CNs
MN i ϵ M moves
IF i is present in non-overlapping coverage access regions
    Send Cache Request and receive Cache ACK
    i enters the new network
    Perform Layer2 and Layer3 connectivity in new network
END IF
i performs Gateway Discovery and Registration using Algorithm1()
Check type of mobility by examining the Gateway Solicitation ACK
IF mobility is intra-WMN
    Send Add IP Request and receive Add IP ACK
ELSE
    Send Add IP Request FWD and receive ACK
    IF CN j ϵ N supports DIMMP
        Send MBU and receive Binding ACK
    END IF
END IF
i receives data in new network
END
```

On mesh border gateway:

```
START
Initialize M = set of MNs, G = set of MBGs
MBG i ϵ G receives message from MN j ϵ M
Check type of message
IF message is Cache Request
    Send Cache ACK to j
    Start buffering incoming packets for j
ELSE
    IF message is Add IP Request
        Send Add IP ACK
    ELSE
        IF message is Add IP Request FWD
            Send Add IP Request to old gateway and receive ACK
            Send Add IP ACK to j
        END IF
    END IF
END IF
Start Data flow control to j's new location
END
```

On correspondent node:

```
START
Initialize M = set of MNs, N = set of CNs
CN i ϵ N received MBU
Compute the OTT
IF Received OTT == Computed OTT
    Update Binding Cache
    Send Binding ACK
    Start data flow control
ELSE
    Discard the message
END IF
END
```

4.5 Connection management

Once the MN successfully performs Layer2 and Layer3 connectivity after moving into new network, mobility control messages are forwarded to MBGs and CN. For sending these messages, WMN requires a route from MN to the wired Internet. The routing protocols for different types of adhoc networks are evaluated in previous works [59, 60]. The two main types of protocols, proactive and reactive have their own certain pros and cons. Using these protocols, mobility creates significant coordination overhead and signalling traffic which results in the increased handoff latency and overhead.

The connection management in the context of mobility management in WMN refers to the path maintenance with minimum cost in the adhoc part of the WMN. To avoid the problem of broadcast and delay in route discovery and establishment, the MARs are used in the Infrastructure WMN, for transferring the packets to/from MN's new location. The concept of dividing the WMN into subnets [32] was used and the WMN is divided into clusters in our technique. Each MAR serves as the cluster head. The MAR has some additional functionality as compared to the traditional cluster head described in [61]. This additional function of MAR is to handle the MN's mobility within the WMN. The new mechanism works in a similar manner as described in [61] except that the MN's does not belong to any cluster because MN is attached to the last mesh router (AP or BS) in the infrastructure mode. So, MN's movement information is not being populated in the WMN. For this purpose, the last mesh router (to which MN is attached) notifies the MAR that it has a route to the MN. The MAR assumes that this mesh router has path or link to the other MAR or MN itself.

When the MN moves to a new network and attaches itself to a mesh router (AP/BS), it does not perform any route discovery process. Rather, it just sends the handoff control message (Add IP Request or MBU) to the attached mesh router. The first mesh router which is part of some cluster, instead of broadcasting the route request generates the route request to its MAR. If the MAR knows the path to the destination or is itself the destination, then it responds with a route reply, otherwise it forwards the route request to all neighbour MARs. Passing the route request to neighbour MARs reduces the broadcast in the WMN to save the scarce wireless resources, as the other nodes which are not the MARs will not further broadcast the message and will discard it. If the MAR knows the path to destination, it will generate a route reply on the backward path, otherwise it will pass the route request to the neighbour MAR, until it reaches the destination (MBG) and responded back with a route reply on the same path.

The route request message also contains additional information about MN's previous location. If a MN has changed its

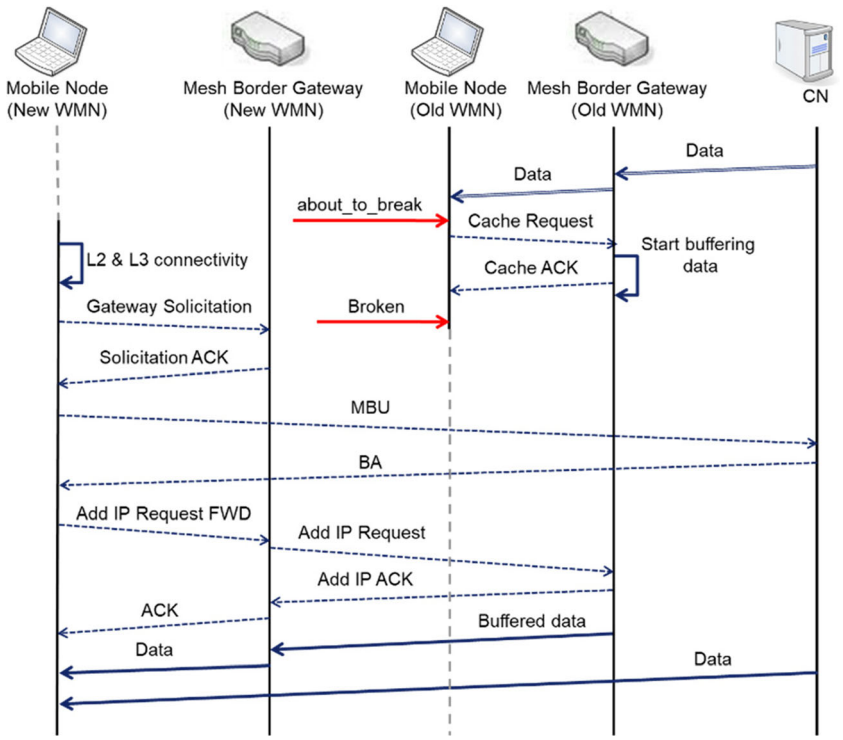

Fig. 7 Inter-WMN handoff execution when CN supports DIMMP

network location and is going through the handoff, then the route request message will also contain the information of its previous network's IP address (HoA). When a MAR receives such route request and if it was involved in any routing of packets to MN's previous location, then it generates a Route Error message. Before forwarding the route request message further, MAR sets the MAR Route Error bit in the message. The purpose of setting this bit in route request message is to avoid generation of further Route Error messages by the other MARs on the path to the MBG.

The Route Error message generated by the MAR also contains additional information of MN's new and old IP addresses as compared to the traditional Route Error message. This Route Error message is for the intra-WMN CNs which were communicating with the MN. When a CN inside the WMN receives such Route Error message, it generates a new route request for the MN but this time with the new IP address. Hence, intra-WMN communications are restored without any additional control signalling between the MN, CNs and the MBGs. For Internet-based communication, the Add IP Request and MBU messages still work in the similar manner as described in the IP-layer handoff management sub-section.

4.6 Distributed location management

The proposed protocol DIMMP also distributes the location information to local location databases and global location database. Local location database resides in the MBGs and global location database resides in the Internet. Location update depends upon the type of mobility, the MN is currently going through. In the case of intra-WMN mobility, MN updates the local location database in the gateway through the Add IP Request message. No additional control signalling is being introduced by the DIMMP for location update. In the case of outward mobility from WMN, the MN should inform the global location server about its location change. This global location update is done with Domain Name System (DNS) dynamic update.

After the mobility of the MN, if a session request for MN is initiated from inside the same WMN in which MN is residing, then local location database serves the request and informs the initiator node the IP address of responder node. This decreases the delay in session delivery time, as location request query is handled locally.

5 Signalling overhead of DIMMP

There are two main classes of mobility related signalling overhead in in wireless networks: 1) One is for mobility and the other is 2) when MN exchanges control messages without moving out.. In the first case, the overhead is generated when a MN performs handoff updates. In the latter one, to refresh the binding entries at the mobility anchor points overhead is for the advertisement messages periodically broadcasted by the mobility anchor points and for the control messages exchanged.

5.1 Signalling overhead due to mobility

Mobility of a node results in the exchange of signalling messages by the mobility management protocol. These signalling messages are exchanged to resume the communication at MN's new location and usually involve interaction between MN, CN and the mobility anchor points. Similarly, to deliver data at MN's new location also requires addition of some extra header bytes with the original packet. It also causes the overhead. Hence, using the model of Makaya and Pierre [62] and Makaya et al. [63], total mobility based signalling overhead for DIMMP, $C_{Mobility}$, can be modelled as the sum of overhead generated for mobility control messages (C_{IP_Update}) and the overhead for data delivery at new location (C_{DD}).

$$C_{Mobility} = C_{IP\_Update} + C_{DD} \tag{3}$$

where:

C_{IP_Update} is the control signalling overhead for updating binding at MBG (*Add IP Request*) and at CN (*MBU*).

(C_{DD}) is the data packets delivery overhead at MN's new location. Symbols used in this section are shown in Table 1.

5.1.1 IP update or modified binding update overhead

Using the model of [63] which is developed for mobility of a MN across subnets of a given access network, changes have been made to model the behaviour of a MN moving across WMNs. Let μ_A be the access network crossing rate and μ_M represents the WMN crossing rate. In case of crossing the WMN by a MN, the access network is also crossed, hence the access network crossing rate when MN performs intra-WMN mobility can be modelled as:

$$\mu_L = \mu_A - \mu_M \tag{4}$$

Let A equally divided sub access networks are there in a WMN and all of them covers such regions that form a contiguous area, then the WMN crossing rate according to [64] is:

$$\mu_M = \frac{\mu_A}{\sqrt{A}} \tag{5}$$

Putting the value of μ_M in Eq. (4):

$$\begin{aligned} &\mu_L = \mu_A - \frac{\mu_A}{\sqrt{A}} \\ &\text{Or} \\ &\mu_L = \frac{\mu_A{}^{*}\left(\sqrt{A}-1\right)}{\sqrt{A}} \end{aligned} \tag{6}$$

A MN can perform two types of binding updates, based on the type of mobility: IP Update at MBG (*Add IP Request*) and IP Update at CN (*MBU*). The *MBU* is performed to update CN for inter-WMN mobility when CN has support for DIMMP. For intra-WMN mobility or CN do no support DIMMP, *Add*

Table 1 Notations used for modelling protocol signalling overhead due to mobility

Notation	Description
μ_A	Access network crossing rate
μ_M	WMN crossing rate
A	No. of sub access networks in a WMN
M	No. of WMNs
$C_{Mobility}$	Total signalling overhead due to mobility
C_{IP_Update}	Signalling overhead to update binding entries at MBG and the CN
C_{MBU}	Signalling overhead to update binding entry at the CN
C_{Add_IP}	Signalling overhead to update binding entry at the MBG
C_{DD}	Data delivery overhead at MN's new location
N_{GW}	No. of MBGs
N_{CN}	No. of CNs
$E(N_A)$	Average no. of access networks crossed
$E(N_M)$	Average no. of WMN crossed
SMR	Session-to-mobility ratio
λ_S	No. of sessions
P_{ho}	Probability of handoff signalling completion
n	No. of retries to send control message if it is lost
S_x	Size of message x
DT_X	Data delivery overhead for protocol X
$DT_{A\text{-}B}$	Data delivery overhead from node A to node B
	Ratio between data and control packets during the handoff process

IP Request is only performed. The binding entry at the MBG is updated in any to receive the buffered data from old MBG. The average binding update overhead cost for Mobile IPv6 was modelled by [62] and [63] using the cost of local and global signalling. Using those models, the IP Update average overhead is:

$$C_{IP\_Update} = N_{GW}{}^{*}[E(N_A){*}CAdd_{IP}] + N_{CN} \qquad [E(N_M){*}C_{MBU}] \tag{7}$$

where:

$E(N_A)$ is the average no. of access networks crossed while residing inside a single WMN.

$E(N_M)$ is the average no. of WMNs crossed by a MN during an on-going session.

N_{GW} and N_{CN} are the no. of MBGs and no. of CNs with which MN must communicate for handoff.

C_{MBU} is the overhead of updating the binding at the CN.

C_{Add_IP} is the overhead of updating the binding entry at the MBG.

To perform the signalling overhead analysis, [62] has presented Session-to-Mobility Ratio (SMR). It is defined as the ratio between the no. of sessions (λ_S) and the mobility rate (μ_A) crossing access networks (no. of handoffs).

$$SMR = \frac{\lambda_S}{\mu_A} \tag{8}$$

Using the model of [63], the average number of access networks crossed while residing inside a WMN and while crossing the WMN are:

$$E(N_A) = \frac{\mu_L}{\lambda_S} \text{ and } E(N_M) = \frac{\mu_M}{\lambda_S}$$

Hence, C_{IP_Update} as a function of SMR from Eq. (7), will be:

$$C_{IP\_Update} = N_{GW}{}^{*}\left[\frac{\mu_L}{\lambda_S}{*}C_{Add\_IP}\right] + N_{CN}{}^{*}\left[\frac{\mu_M}{\lambda_S}{*}C_{MBU}\right]$$

Putting the values of μ_L and μ_M from Eq. (5) and (6):

$$C_{IP\_Update} = N_{GW}{}^{*}\left[\frac{\mu_A{}^{*}\left(\sqrt{A}-1\right)}{\lambda_S{}^{*}\sqrt{A}}{*}C_{Add\_IP}\right] + N_{CN}{}^{*}\left[\frac{\mu_A}{\lambda_S{}^{*}\sqrt{A}}{*}C_{MBU}\right]$$

From Eq. (8)

$$\frac{1}{SMR} = \frac{\mu_A}{\lambda_S}$$

Hence,

$$C_{IP\_Update} = N_{GW}{}^{*}\left[\frac{\left(\sqrt{A}-1\right)}{SMR{*}\sqrt{A}}{*}C_{Add\_IP}\right] + N_{CN}{}^{*}\left[\frac{1}{SMR{*}\sqrt{A}}{*}C_{MBU}\right]$$

$$C_{IP\_Update} = \frac{1}{SMR{*}\sqrt{A}}{*}\left[N_{GW}{}^{*}\left(\sqrt{A}-1\right){*}C_{Add\_IP} + \left(N_{CN}{*}C_{MBU}\right)\right] \tag{9}$$

In the case of intra-WMN mobility or inter-WMN mobility when the CN do not support DIMMP, no control signalling is done with the CN for *MBU*. Hence, the overhead reduces to:

$$C_{IP\_Update} = \frac{1}{SMR{*}\sqrt{A}}\left[N_{GW}{}^{*}\left(\sqrt{A}-1\right){*}C_{Add\_IP}\right] \tag{10}$$

To calculate the C_{Add_IP} and C_{MBU}, let P_{ho} represents the probability that a handoff signalling will complete successfully, then the *Add_IP* update and *MBU* signalling overhead for DIMMP can be expressed as:

$$C_{Add\_IP} = P_{ho}{}^{*}\left(\sum_{i=1}^{N_{GW}}\left(S_{Add\_IP\_Req_i} + S_{Add\_IP\_ACK_i}\right)\right) + (1-P_{ho}){*}\left(n\sum_{j=1}^{N_{GW}} S_{Add\_IP\_Req_j}\right) \tag{11}$$

$$C_{MBU} = P_{ho}{}^{*}\left(\sum_{i=1}^{N_{CN}}\left(S_{MBU_i} + S_{BA_i}\right)\right) + (1-P_{ho}){*}\left(n\sum_{j=1}^{N_{CN}} S_{MBU_j}\right) \tag{12}$$

where:

C_X is the overhead cost for process X.

N_{CN} is the no. of CNs.

n is the no. of retries in case of failure of send the message.

S_X is the size of message X.

The first terms in the Eq. (11) and (12) represent the successful packet delivery cost and the second terms represent the cost for number of failures. For inter-WMN mobility, *Add IP Request FWD* overhead is also added.

$$C_{Add\_IP} = P_{ho}{}^{*}\left[\sum_{i=1}^{N_{GW}}\left(S_{Add\_IP\_Req_i} + S_{Add\_IP\_ACK_i} + S_{Add\_IP\_Req\_FWD_i} + S_{ACK_i}\right)\right] + (1-P_{ho}){*}\left[n\sum_{j=1}^{N_{GW}} S_{Add\_IP\_Req_j}\right] \tag{13}$$

From Eqs. (11) and (12) total *IP Update* overhead is:

$$C_{IP\_Update} = C_{Add\_IP} + C_{MBU} \tag{14}$$

5.1.2 Data delivery overhead

To deliver the data at MN's new location also introduces additional overhead. The mechanism adopted for data delivery during the handoff process results in data delivery overhead [62]. This overhead is of two types: successful packet delivery overhead and packet loss overhead. Packet loss may cause retransmissions that causes an additional use of scarce wireless resources [63].

Let $DT_{A\text{-}B}$ is the overhead for delivering a data packet from node A to node B and DT_X represents the data delivery overhead for protocol X. As no data packet is sent to the MN's old network, hence there will be no data delivery cost except the delivering of first data packet to MN in the new access network.

$$DT_{DIMMP} = DT_{CN-MN_{new}} \tag{15}$$

Let η be the ratio between the data and control packets during the handoff process, then the data delivery overhead for transferring data at MN's old location is:

$$DT_{CN-MN_{old}} = \eta(DT_{CN-MBG} + DT_{MBG-MN_{old}}) \tag{16}$$

For intra-WMN and inter-WMN mobility, the overhead for delivering data to MN's new location is shown in eqs. (17) and (18) respectively.

$$DT_{CN-MN_{new}} = \eta(DT_{CN-MBG} + DT_{MBG-MN_{new}}) \tag{17}$$

$$DT_{CN-MN_{new}} = \begin{cases} \eta(DT_{CN-MBG_{old}} + DT_{MBG_{old}-MBG_{new}} + DT_{MBG_{new}-MN_{new}}) \\ \eta(DT_{CN-MN_{new}}) \end{cases} \tag{18}$$

5.2 Signalling overhead without mobility

Even if MN does not move, it performs signalling to keep track of mobility anchor points. Usually this overhead is for the announcement messages periodically broadcasted by the mobility anchor points and also for the control messages to refresh the binding entries. The notations used in this section are shown in Table 2.

Total additional overhead cost when MN is not going through any handover, is:

$$Ad\_oh_X = C_{\mathrm{Reg}\_X} + C_{BR\_X} \tag{19}$$

where:

C_{Reg_X} is the cost of registration (HA or MBG registration) for protocol X.

C_{BR_X} is the cost of performing binding refresh operation for protocol X.

These two costs are calculated in the next sub-sections.

5.2.1 HA/MBG registration overhead

The MBGs in DIMMP do not perform periodic broadcast for the advertisement messages. Hence, the overhead for DIMMP Gateway Discovery and Registration is just for the multicast signalling performed only once by each MN to discover the MBG and then response from the MBG. Hence, the overhead cost of DIMMP MBG discovery with N_{MN} number of MNs in a particular time interval is:

$$C_{MBG\_\mathrm{Reg}\_DIMMP} = \sum_{i=1}^{N_{MN}} \left(S_{GW\_Sol_i} + \sum_{j=1}^{N_{GW}} S_{Sol\_Ack_{i,j}} \right) \tag{20}$$

where:

SGW_Sol is the size of *Gateway Solicitation* message.
SSol_Ack is the size of *Solicitation ACK* message.
NGW is the no. of MBGs.

5.2.2 Binding refresh overhead

To keep the binding entries at the CN alive, Mobile IPv6 uses *Binding Refresh Request* (*BRReq*) message. When the binding lifetime of a MN's CoA expires and Binding Cache entry is still active, then the CN sends *BRReq* message to the MN. As a result, MN initiates a full return routability procedure that results in signalling overhead.

When using DIMMP, the CN does not perform any procedure like Mobile IPv6 in which there are sent periodic binding refresh messages, rather the CN and the MBG determines the life of binding entry. When a binding lifetime expires at the CN, then it monitors the network traffic for that particular binding entry. If there is no network traffic for a particular MN, for which there exists a binding entry and binding lifetime has expired, then the CN sends *BRReq* to MN. In the case, there exists traffic then the CN simply updates the binding lifetime to its previous value without sending any *BRReq* to the MN. The MN upon receiving the *BRReq* message will perform the route optimization procedure in which *MBU* message is sent to the CN directly.

To handle the binding lifetime at the MBG, while MN sends *Add IP Request* message to the MBG it adds an option in it that whether any *MBU* message has also been sent to the CN or not. In the case, option states that a *MBU* message has also been sent to the CN then the MBG will forward the buffered data to MN's new location and will delete the binding entry after forwarding all the data. In the other case, when option states that MN has not sent any *MBU* message to the CN, the MBG keeps the binding entry and handles it just like handled by the CN. Hence, no additional control traffic has

Table 2 Notations used for modelling protocol signalling overhead without mobility

Notation	Description
Ad_oh_X	Total overhead cost when MN does not execute handover
C_{Reg_X}	Cost of registration (HA or MBG registration) for protocol X
C_{BR_X}	Cost of performing binding refresh operation for protocol X
S_{HA_Adv}	Size of HA advertisement message
SGW_Sol	Size of *Gateway Solicitation* message
$SSol\_Ack$	Size of *Solicitation ACK* message
S_{BR_X}	Size of binding refresh message sent from protocol X
n	No. of HA advertisements in a particular time interval
N_{MN}	No. of MNs
N_{GW}	No. of MBGs
T	Time interval for which MN does not move again
t	Binding lifetime
x	No. of times MN found the traffic for the particular binding entry for which binding lifetime has expired
N_{BR_X}	No. of binding refresh messages for protocol X
int	Function that generates the integer value for given input

been introduced by the DIMMP to keep the binding entries alive at the CN and at the MBG.

Consider a MN that moved from one network to another and performed the route optimization procedure. Let the binding lifetime be t seconds and the MN does not move again in a given time interval T. The number of binding refresh messages can be approximated as discussed by [65]:

$$N_{BR\_DIMMP} = \text{int}\left(3*\left(\frac{T}{t} - x\right)\right) \tag{21}$$

where:

int is a function that returns the integer value of a given input.

x is the number of times the CN found network traffic of the particular binding entry for which the binding lifetime is about to expire.

The value 3 represents the three messages (*BRReq*, *MBU* and *Binding ACK*) that will be exchanged to update the binding entry at the CN.

Assuming that one fourth of the times when binding lifetime was expired, the MN has not found any traffic for that particular binding entry, then three fourth of the times it found the network traffic:

$$x = \text{int}\left(\frac{3}{4}*\frac{T}{t}\right) \tag{22}$$

The number of binding refresh messages for DIMMP N_{BR_DIMMP} in Eq. (21) is for the mobility scenarios when MN moves from one WMN to another and the CN also supports DIMMP. In the case of intra-WMN mobility or inter-WMN mobility when CN has no support for DIMMP, there will be no binding entry at the CN that needs to be refreshed. Hence, there will be no message exchange in these scenarios.

$$N_{BR\_DIMMP} = 0$$

The overhead of binding refresh in a particular time interval, is:

$$C_{BR\_DIMMP} = \sum_{j=1}^{N_{BR\_DIMMP}} S_{BR\_DIMMP_j} \tag{23}$$

where:

C_{BR_X} represents the cost of binding refresh for protocol X.

S_{BR_X} is the total size of all message exchanged to refresh the bindings.

So, the total additional overhead for Mobile IPv6 and the DIMMP without any mobility is:

$$Ad\_oh_{DIMMP} = \sum_{i=1}^{N_{MN}} \left(S_{GW\_Sol_i} + \sum_{j=1}^{N_{GW}} S_{Sol\_Ack_{i,j}} \right) + \sum_{j=1}^{N_{BR\_DIMMP}} S_{BR\_DIMMP_j} \tag{24}$$

6 Performance analysis and discussions

In this section, the simulation setup details and results are discussed in three different contexts for the three features of the proposed DIMMP. The results are presented considering three perspectives: 1) for distributed mobility anchors, 2) for managing intra and inter-WMN mobility separately and 3) for

the enhanced route optimization and are compared with the Mobile IPv6 and the IMeX.

6.1 Simulation setup

To evaluate the performance of DIMMP, simulations are carried out in the NS-2 version ns-2.33. The simulations are performed on a Dell machine having Intel Core i5–3470 CPU@3.2GHz processor with installed memory (RAM) of 4.0 GB. Linux Fedora core 13 64-bit was used as the Operating System with kernel version 2.6.33.3–85.fc13.x86_64. For the mobility management, the MobiWAN implementation of RFC 3775 for ns-2.33 was used. For the simulation of WMN, the IEEE 802.16 Wireless Mesh Networks patch for ns-2.33 was used. Simulation configurations are shown in Table 3.

Nandiraju et al. [66] discussed in details the Internet traffic between the mesh clients and the MBG, and highlighted dominance of the peer-to-peer traffic in the WMNs as WMNs are expected mainly to be a solution for providing last-mile (to end node) broadband Internet access, resulting most of the background traffic and the MN's traffic for handoff was configured to be with the CNs in the wired Internet. The average values are plotted after running the simulation 10 times.

6.2 Performance evaluation for distributed mobility anchors

As per the problem discussed in the motivation section, the existing mobility management protocols were based on the centralized architecture which resulted in SPOF and performance degradation. This section discussed the analysis of the DIMMP for distributed mobility anchors with respect to handoff latency, signalling overhead, throughput and packet loss.

Table 3 Simulation parameters and values

Parameter	Value
Simulation area	1600 × 1600 m^2
Default transmission range of wireless node	150 m
Wireless channel bandwidth	10Mpbs
Wired links bandwidth	100Mbps
No. of terminal nodes in each WMN	4–53 (varying)
No. of MNs in each WMN	1–50 (varying)
No. of WMNs	2–5 (varying)
No. of MBGs in each WMN	2
No. of MRs in each WMN	10–25 (varying)
No. of FTP traffic sessions	3–10 (varying)
No. of CBR traffic sessions	1–53 (varying)
Simulation time	500 and 1000 s
Simulation time without any data traffic	First 15 s
Speed for infrastructure MRs	0 m/s
Speed for MNs	10 m/s
Interface queue type	DropTail/PriQueue
Interface queue length	50
Antenna model	Antenna/OmniAntenna

6.2.1 Handoff latency comparison

Figure 8 shows the handoff latency as a function of the number of MNs. For Mobile IPv6 and the IMeX, only a single HA was configured and all the MNs were attached to that HA. When all the MNs started the handoff process, they exchanged the signalling for handoff using home test and CoA test. The signalling messages of all the MNs for home test were routed to the CN via the central HA. This created an overhead to process the home test of all the MNs at the single HA. Also, the scarce wireless resources of WMN were being requested by all the MNs. Hence, as the number of MNs initiating the handoff at the same time increased, the handoff latency also increased.

The handoff latency of the IMeX has the same behaviour just like the Mobile IPv6. It also increased with an increase in the number of the MNs. The only difference of IMeX from the Mobile IPv6 is that, the IMeX has devised a new mechanism that attempted to reduce the pre-handoff latencies like: new access point discovery and attachment delay, IP address acquisition delay, DAD delay and route discovery delay. Using this mechanism, the IMeX reduced the handoff latency to some extent as compared to the standard Mobile IPv6, but the overall handoff latency is still very high. The reason for this high handoff latency is that, the IMeX used the Mobile IPv6 as the network layer mobility management protocol for session redirection where a single HA was handling the mobility signalling. Thus, the signalling done using the Mobile IPv6 with the IMeX resulted in the higher handoff latency with an increase in the number of MNs.

The work done by Jiang Xie [7] and Zhao and Xie [32] discussed that the handoff latency of mobility management

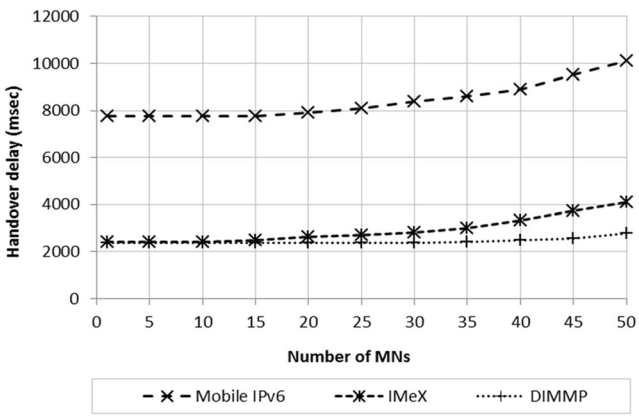

Fig. 8 Handoff latency comparison with varying number of MNs

protocols increases with the increase in the number of wireless hops. To analyse this effect of the number of hops on the handoff latency performance, results are plotted in Fig. 9. The result shows that the handoff latency of Mobile IPv6 is most affected by the increase in the number of wireless hops as compared to the other two protocols.

The high effect of the number of wireless hops on the handoff latency of Mobile IPv6 is due to the reason that, with Mobile IPv6 the Adhoc On-Demand Distance Vector (AODV) routing protocol was used. As Mobile IPv6 has nothing to do with the routing protocol, hence the AODV broadcasted the route discovery messages for the discovery of new path from the MN's new location to the wired Internet. The delay in the discovery of the new path is directly proportional to the number of wireless hops. As the number of wireless hops increased, the path discovery time also increased with the AODV that resulted in an increase in the overall handoff latency for the MN. The handoff latency for the DIMMP also increased with an increase in the number of hops, but this increase is less as compared to the standard Mobile IPv6. The route discovery procedure from the MN's new location in DIMMP was handled by the MARs in the WMN. This reduced the route discovery delay and hence the handoff latency for the DIMMP. The IMeX devised a mechanism that overcame the broadcasting of route discovery messages using the Xcast that reduced the delay involved in the WMN but the delay involved in updating the binding entries at the HA and at the CN are still there, that resulted in high handoff latency. The slight increase in the handoff latency with the increase in the number of wireless hops is due to the increase in the propagation delay on multiple hops.

6.2.2 Signalling overhead comparison

The distribution of mobility anchors controls the signalling exchange to be either at the local or at the global level. Without the distribution of mobility anchors, global signalling is always performed with the centralized mobility anchor point. The result of cumulative signalling overhead generated by the mobility management protocols is shown in the Fig. 10. As the mobility of MN is within the WMN, hence the distribution of mobility anchors resulted in the local handoff signalling exchange by the DIMMP. On the other hand, Mobile IPv6 and the IMeX executed the global signalling with complete route optimization using the return routability procedure.

The signalling overhead generated by the DIMMP is high at start as compared to the other two protocols. This high overhead is due to the fact that all the MNs using DIMMP used gateway discovery and registration procedure to keep the record of the MBGs.

After performing the handoff, the signalling overhead of IMeX has increased as compared to the Mobile IPv6. The IMeX has higher overhead because it used the Mobile IPv6 for session redirection and also generated its own notify signalling messages to communicate with the XGRs in the WMN, in addition to the signalling messages of the Mobile IPv6.

6.2.3 Throughput comparison

The throughput at the MN is affected due to the mobility. To analyse this effect, a single handoff was executed at time $t =$ 274 s. During the simulation, the mobility anchor was made down and at the same time handoff was also triggered. The purpose of making the mobility anchor down is to observe the impact of distributed mobility anchors.

The mobility of MNs caused the throughput to be dropped to zero for all the protocols, as MN became unreachable at the old location. Figure 11 shows the throughput comparison of mobility management protocols for distributed mobility anchors in case of non-overlapping coverage access regions. At 274 s the HA was made down and the MN's movement for handoff was also started at the same time. So, at 275 s, zero throughputs can be observed for all the protocols.

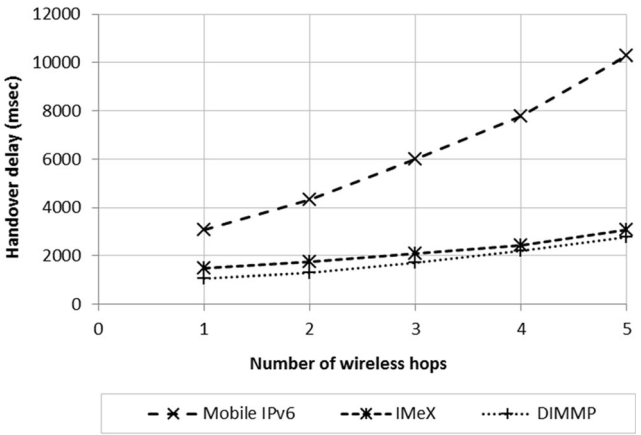

Fig. 9 Handoff latency comparison with varying number of wireless hops

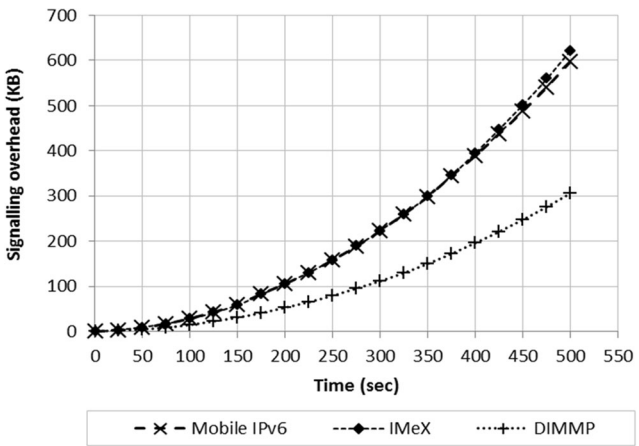

Fig. 10 Signalling overhead comparison for distributed mobility anchors

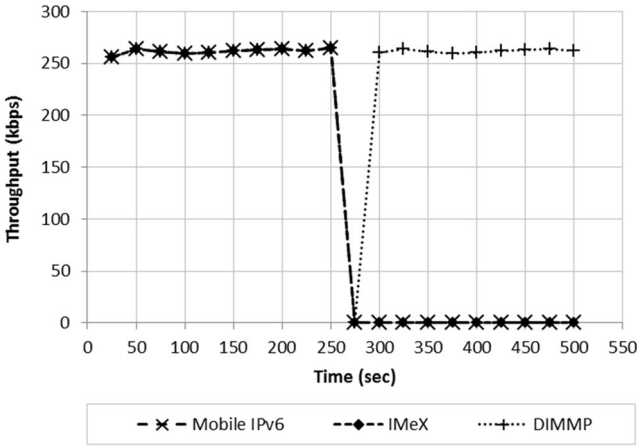

Fig. 11 Throughput comparison for distributed mobility anchors in non-overlapping coverage access regions

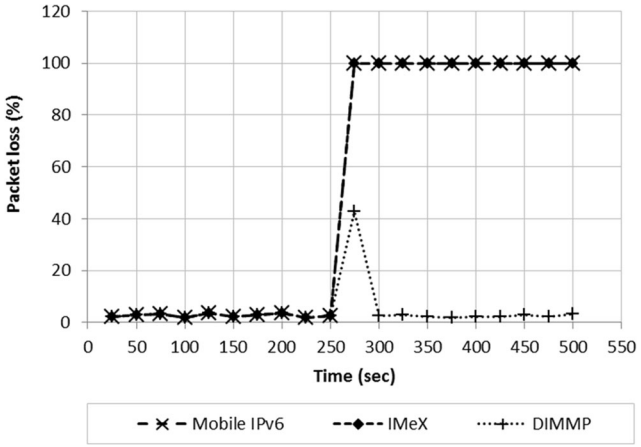

Fig. 12 Packet loss comparison for distributed mobility anchors in non-overlapping coverage access regions

As the Mobile IPv6 and the IMeX were having dependence on the central HA (mobility anchor point) for the signalling of handoff control messages, hence all the messages sent to the HA were lost. Also, the home test messages which were supposed to reach the CN via the HA were not reached. Thus, the route optimization procedure was not completed and the transmission was not restored, resulting in zero throughput at the MN for the rest of the simulation time after 275 s.

On the other hand, the throughput at the MN while using the DIMMP also dropped to zero at time 275 s, but due to distributed mobility anchors the binding update operation was also performed at the second MBG through the Add IP Request. The traffic was then routed through the second MBG and the MN became reachable at the new location. Hence, the throughput at the MN once again reached to its normal position.

6.2.4 Packet loss comparison

The number of packets lost during the handoff process depends upon the time the MN spends in the handoff. The higher the handoff latency is higher will be the packet loss. But in the case of centralized mobility anchor point failure, all packets destined to the MN will be lost. When MN moved out of the access network then for a certain period the MN was not having connectivity in any access network. Also, the mobility anchor node was unable to forward packets to the MN. Hence, all the packets destined to the MN in the WMN were lost. This can be observed from Fig. 12. At time $t = 275$ s the packet loss for all the mobility management protocols increased to the maximum. The packet loss for the Mobile IPv6 and IMeX remained at the same level, that is, was equal to the data arrival rate and all the packets were lost. As both Mobile IPv6 and the IMeX are dependent on the HA, which is down, hence it cannot forward the data. Although, the IMeX has devised Xcast-based data caching and forwarding mechanism but that mechanism can only be helpful for the intra-WMN mobility with a common XGR in the old and candidate subnets.

On the other hand, the packet loss for the DIMMP also increased to some extent but it can be observed that at time t = 275 s the packet loss is low as compared to the other two protocols. The reason is that, the WMN was configured with two MBGs and all the traffic sessions for the MN were not passing through the single MBG that was failed at $t = 274$ s. Some of the traffic sessions were passing through the second MBG and packets from CN's were successfully delivered to nodes which did not move and were residing in their attached access network. The packets which were passing through the MBG that has failed were lost. Hence at time t = 275 s a high packet loss is observed. It can also be observed from Fig. 12 that the packet loss for the DIMMP was decreased after some time. As DIMMP used distributed mobility anchors, hence the other MBG was notified about the MN's mobility through Add IP Request message.

6.3 Performance evaluation for handling intra and inter-WMN mobility separately

Mobility across WMNs is of two types: either across access networks within the WMN or across WMNs. As discussed in the motivation section that the existing mobility management protocols handle intra and inter-WMN mobility in the similar manner which resulted in higher handoff latency and signalling overhead. When the MN moves across networks inside a single WMN, then the entry and exit points with the wired Internet remains unchanged. So, utilizing this feature, the DIMMP managed the intra-WMN mobility with local signalling, while for inter-WMN mobility global signalling in the wired Internet was performed.

6.3.1 Handoff latency comparison

The handoff latency results for the simulation are shown in Fig. 13. The handoff latency caused while using the Mobile IPv6 as the mobility management protocol is highest and

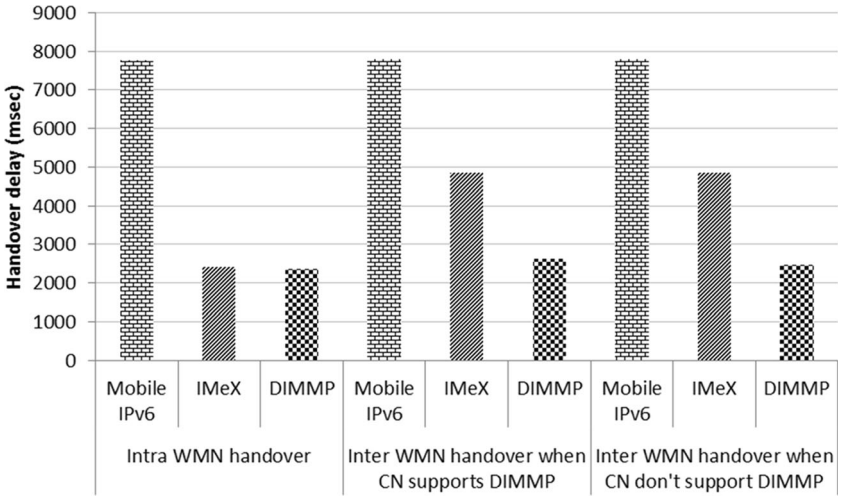

Fig. 13 Handoff latency comparison for the handling of intra and inter-WMN mobility separately

remains same in all the scenarios. The major factors for Mobile IPv6's higher delay are: the use of return routability based route optimization procedure and having no mechanism to reduce the route discovery delay in the WMN from MN to the MBG. The handoff latency for IMeX is high as well, because it also used the basic Mobile IPv6 mechanism for informing the CN about the MN's mobility. The only delays that have been reduced by the IMeX are: L2 scanning delay, L3 handoff detection delay, DAD delay and path discovery delay from the MN to the MBG in the WMN. In case of intra-WMN mobility, the reduction or elimination of these four delay components by the IMeX caused the handoff latency to decrease as compared to the standard Mobile IPv6. However, the delay caused due to the Mobile IPv6's signalling has still not been improved in the IMeX.

Another problem of managing mobility with IMeX is that, for inter-gateway based handoff if there is no corresponding XGR that belongs to both the old and new subnets, as in the case of inter-WMN mobility scenario, then the handoff latency will be increased. Thus, in case of inter-WMN mobility, increased handoff latency for the IMeX can be observed from Fig. 13. Here, the XGRs in the new WMN were not having information about the mobility of MN, hence they were unable to perform the IP address configuration, DAD detection and routing path discovery in advance.

On the other hand, the handoff latency caused by the DIMMP is lowest as compared to the other two protocols in all the three scenarios. For intra-WMN mobility case, the reduced handoff latency of DIMMP is due to the fact that DIMMP only performed local signalling inside the WMN and there was not signalling exchanged with the CN for the route optimization procedure. Only the Binding Cache entries were updated at the MBGs and MBGs started to forward the data to the MN's new location using data flow control procedure. In the case of inter-WMN mobility, the DIMMP implementation at the MN checked the status of the CN. When the CN was not DIMMP compatible then the binding entries were updated at the MBGs of the old WMN only, without communicating with the CN. In the other case, when CN was DIMMP compatible, then the enhanced route optimization procedure was executed.

6.3.2 Signalling overhead comparison

To analyse the signalling overhead of mobility management protocols, overhead was calculated as a function of the SMR [63]. The SMR is the ratio between the number of sessions running at MN to the number of handoffs MN executed during the simulation.

Figure 14 shows the signalling overhead comparison for intra-WMN mobility. The signalling overhead with the IMeX is highest in comparison to the other two protocols. The reason for this high signalling overhead is the messages exchanged by the IMeX protocol for notifying the old access point and the XGR in addition to the standard messages of Mobile IPv6 for updating the binding entries at the HA and at the CN. The

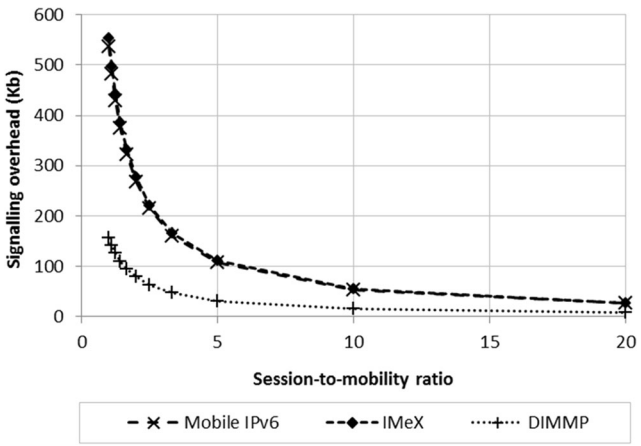

Fig. 14 Signalling overhead comparison for intra-WMN mobility

signalling overhead of Mobile IPv6 is also high as it used the route optimization procedure with return routability. On the other hand, the signalling overhead of DIMMP is lowest. The reason is that, the MN with DIMMP has not communicated with the CN rather the mobility was handled locally by the MBGs.

To evaluate the signalling overhead in the case of inter-WMN mobility, simulations were performed two times while making the CN as DIMMP compatible in one setup and non-compatible in the second setup. The results were obtained using the signalling overhead model [63]. Figure 15 shows the signalling overhead comparison for the inter-WMN mobility scenario.

The signalling overheads while using the IMeX and Mobile IPv6 are same as were in the scenario of intra-WMN mobility. The reason for this same overhead is that, both protocols attempted to handle the two types of mobility in the similar manner irrespective of the type of movement of the MN. On the other hand, the signalling overhead of the DIMMP, in this scenario, was dependent on the compatibility of the CN. When the MN was communicating with a DIMMP compatible CN, then the signalling overhead was higher as compared to the case when the MN communicated with a non-compatible CN.

6.3.3 Packet loss comparison

To analyse the performance of the DIMMP in terms of packet loss for the handling of intra and inter-WMN mobility separately, packet loss is calculated in the form of percentage and represents the percentage of packets lost in one second.

Figure 16 shows the packet loss comparison for the three mobility management protocols in the case of intra-WMN mobility. The packet loss for the DIMMP and the IMeX was observed minimum. The reason was that, both the DIMMP and the IMeX used the gateway based and Xcast-based data caching mechanism respectively that resulted in zero packet loss due to mobility. On the other hand, the packet loss for the Mobile IPv6 went high during the handoff.

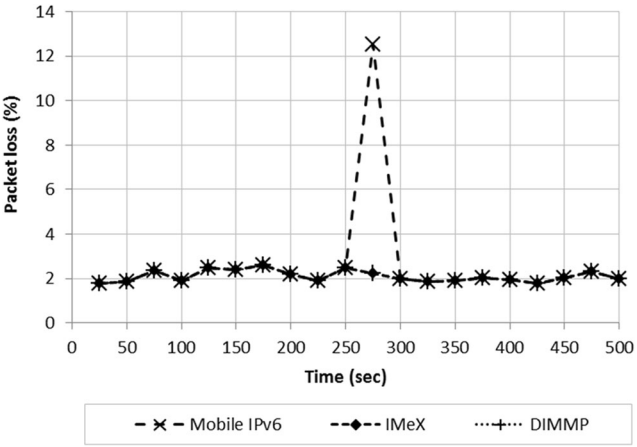

Fig. 16 Packet loss comparison for intra-WMN mobility

In the case of inter-WMN mobility, the Mobile IPv6 behaved in the similar manner just like discussed above for the case of inter-WMN mobility. However, the behaviour of the IMeX was changed and a high packet loss was observed at t = 275 s that can be observed from Fig. 17. The reason for this high packet loss for the IMeX in this scenario of inter-WMN is the fact that IMeX's Xcast-based caching mechanism only worked in the case of intra-WMN mobility or when there were some common XGRs in the old and the visited subnets. As in this case of inter-WMN mobility, there was no common XGR between the old and new subnets hence all the packets destined to the MN's previous location were lost during the handoff process.

6.4 Performance evaluation for the enhanced route optimization

As discussed in the motivation section, the Mobile IPv6 used a return routability based route optimization procedure for

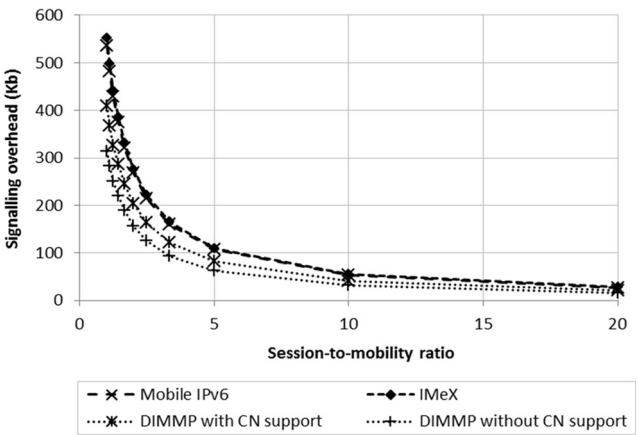

Fig. 15 Signalling overhead comparison for inter-WMN mobility

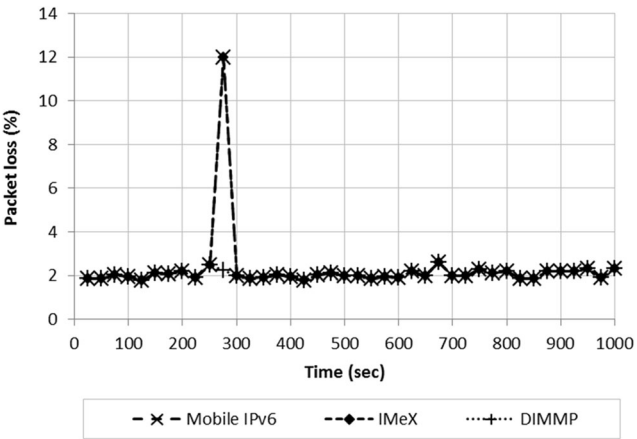

Fig. 17 Packet loss comparison for inter-WMN mobility

direct communication between the MN and CN. This route optimization results in higher handoff latency and signalling overhead. To overcome this problem, the DIMMP has proposed a TOTP route optimization procedure. This sub-section discussed the results of improvements due to enhanced route optimization.

6.4.1 Handoff latency comparison

To analyse the handoff latency performance of the DIMMP with enhanced route optimization, we have given a number to each packet received at the MN in ascending order starting from 1. So, for each successful packet received at the MN the counter increased by 1. As the MNs were having CBR traffic sessions, so the data was arriving at the MN with a constant rate and the packet arrival rate was not changed until there became some bottleneck in the network or the MN moved. In the case of mobility, packets were not received for the time period the MN was executing the handoff thus resulting in the disruption of service.

As it is clear from Fig. 13 that the handoff latency for the DIMMP in the WMN is not affected too much with the status of CN's compatibility, hence we can use either the scenario for compatible CN or non-compatible CN. In the simulation we have considered the case that CN supported the DIMMP. Figure 18 shows the result for the increasing number of packets with time.

The handoff was triggered at time $t = 274$ s, so at time 275 s, we can observe that the packets were not being received at the MN. The handoff latency of the IMeX is low as compared to the Mobile IPv6, but it is still high as compared to the DIMMP. The reason for the reduction in the handoff latency of the IMeX as compared to the Mobile IPv6 is that, the IMeX used Xcast-based routing and caching mechanism that decreased the route discovery delay from the MN's new location. The reason for the high handoff latency of IMeX as compared to the DIMMP is that, the IMeX used Mobile IPv6 as the network layer mobility management protocol for the session redirection. As DIMMP used the enhanced route optimization process in which the home test and CoA test of return routability based route optimization has been removed, hence the low handoff latency is observed.

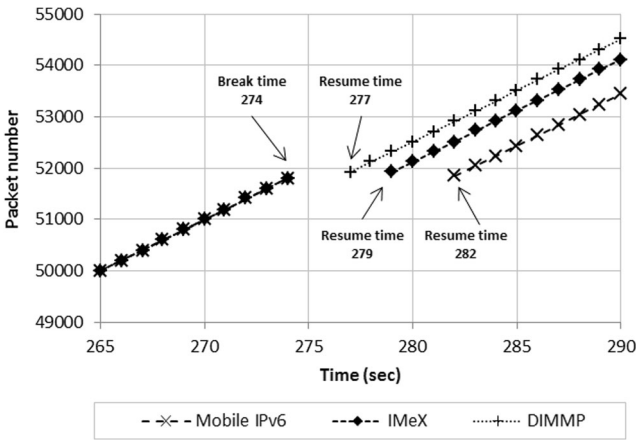

Fig. 18 Handoff latency comparison for enhanced route optimization

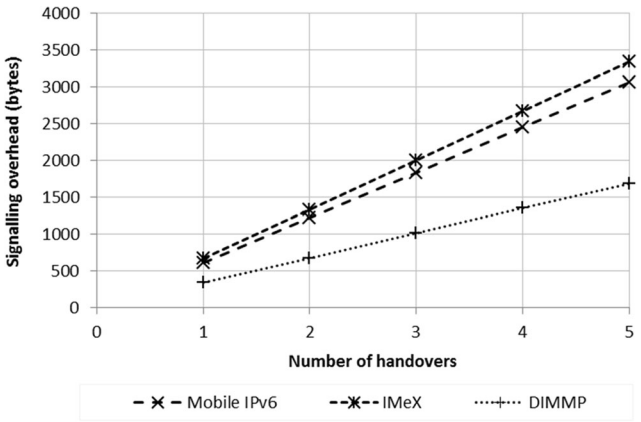

Fig. 19 Signalling overhead due to mobility comparison for enhanced route optimization

6.4.2 Signalling overhead comparison

The enhanced route optimization procedure has also reduced the signalling overhead for the DIMMP. There are two types of signalling overheads a mobility management protocol experiences, that is, the signalling overhead due to mobility and the signalling overhead without mobility.

Signalling overhead due to mobility When a MN moved across WMNs then the signalling messages exchanged for the mobility management created overhead. This signalling overhead due to mobility of MN as a function of the number of handoffs is shown in Fig. 19. The highest signalling overhead is generated by the IMeX. The reason for this high overhead of the IMeX as compared to the Mobile IPv6 is that,

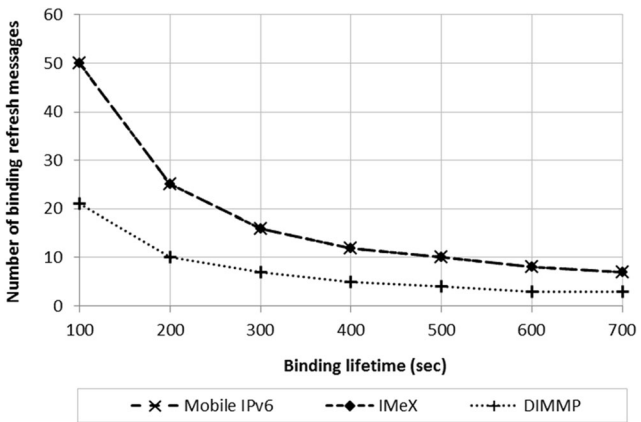

Fig. 20 Signalling overhead without mobility comparison for enhanced route optimization

Table 4 Pros and Cons of DIMMP

DIMMP Features	Pros	Cons
Distributed	Avoids single point of failure	May result in signalling overhead at attachment and registration time
Managing intra and inter-WMN mobility separately	Decreases signalling overhead and handoff delay for intra-WMN mobility	–
Enhanced route optimization	Decreases handoff delay for inter-WMN mobility	Computational overhead for security
Link status classification and caching	Decreases packet loss	Computational overhead
Gateway discovery and registration	No broadcast rather solicitation based discovery	Computational overhead for security
CN compatibility test	Decreases signalling overhead and handoff delay for intra-WMN mobility	Additional signalling overhead at the start of session
Connection management	No broadcast for route discovery	Overhead of clustering

the IMeX used the additional signalling messages to inform the XGRs about the mobility of the MN. These notification messages were additional to the standard route optimization messages of the Mobile IPv6.

Signalling overhead without mobility When a MN executes handoff, then after the handoff the MN has to keep the binding entry active at the CN so that the data can be redirected to its new location. For this purpose, mobility management protocols perform the binding refresh operation. The signalling done for this purpose creates additional overhead in the network without any mobility of that specific MN.

Figure 20 shows the overhead of the binding refresh messages generated by the mobility management protocol with varying values of binding lifetime. The Mobile IPv6 and the IMeX generated high signalling overhead message with the decrease in the binding lifetime.

The contribution of this work in the form pros and cons for each feature of DIMMP is shown in Table 4.

7 Conclusion & future research directions

Due to low performance of existing mobility management protocols in WMN the concept of distributed mobility management was envisioned. A new Distributed IP-based Mobility Management Protocol (DIMMP) for service continuation of MNs when they roam across access networks inside a WMN or across WMNs is proposed. DIMMP distributed the mobility functionality to multiple Mesh Border Gateways (MBG), Mobility Anchor Routers (MAR) and at the end nodes, thus reducing chances for a potential single point of failure. The DIMMP also utilizes the multi-hop routing to handle the problems of broadcast, route discovery delay and intra-WMN mobility. An enhanced route optimization procedure is also proposed to reduce the handoff latency and signalling overhead. Simulations were performed in ns-2 and obtained results showed that handoff latency and signalling overhead have been reduced when DIMMP is used in comparison to Mobile IPv6 and the IMeX in different scenarios. These improvements are due to the facts that DIMMP distributed the mobility anchors, used MARs to overcome the problems of broadcast and route discovery delay and the enhanced TOTP-based route optimization.

As this protocol only covers one aspect of distribution of mobility functionality to MBGs, MARs and end nodes, hence research community can extend this distribution to other wireless networks or for a generalized solution. In the case of multi-hop path failure, the existence of multi-paths in the WMN can also be utilized with the help of Fuzzy Logic based link status classification and multipath routing to further improve the performance [67–69]. This will also increase the overall performance for handoff execution in WMNs. Work can also be done in the area of simultaneous mobility handling when the two communicating nodes move simultaneously. Here, the two nodes can use TOTP-based direct communication between them and may also take help from the distributed name resolution servers to know the location of each other.

Acknowledgments This research was supported by the MIST (Ministry of Science and ICT), Korea, under the National Program for Excellence in SW supervised by the IITP (Institute for Information & communications Technology Promotion) (2015-0-00938).

References

1. Loumiotis I, Adamopoulou E, Demestichas K, Remoundou C, Kosmides P, Asthenopoulos V, Theologou M (2016) Road to next generation mobile networks: an evolutionary dynamics approach. Mob Networks Appl 21(2):237–246
2. Shah PA, Yousaf M, Qayyum A, Malik SA (2009) An analysis of service disruption time for TCP applications using end-to-end mobility management protocols. In: Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia, pp. 360–364
3. Zamanifar A, Nazemi E, Vahidi-Asl M (2017) A mobility solution for hazardous areas based on 6LoWPAN. Mob Networks Appl 1–16. https://doi.org/10.1007/s11036-017-0918-6
4. Akyildiz IF, Wang X (2009) Wireless mesh networks. Wiley

5. Akyildiz IF, Wang X, Wang W (Mar. 2005) Wireless mesh networks: a survey. Comput Netw 47(4):445–487
6. Al-surmi I, Othman M, Mohd B (2012) Mobility management for IP-based next generation mobile networks: review, challenge and perspective. J Netw Comput Appl 35(1):295–315
7. Xie J, Wang X (2008) A survey of mobility management in hybrid wireless mesh networks. Network, IEEE 22(6):34–40
8. Chan HA, Yokota H, Xie J, Seite P, Liu D (2011) Distributed and dynamic mobility management in mobile internet: current approaches and issues. Aust J Commun 6(1):4–15
9. Bokor L, Faigl Z, Imre S (2011) Flat architectures: towards scalable future internet mobility. In: SpringerLink The Future Internet, LNCS, vol. 6656, pp. 35–50
10. George A, Kumar A, Cavalcanti D, Agrawal DP (2008) Protocols for mobility management in heterogeneous multi-hop wireless networks. Pervasive Mob Comput 4(1):92–116
11. George A, Kumar A, Srinivasan S (2009) A multi-hop mobility management protocol for heterogeneous wireless networks: other article. Int J Pervasive Comput Commun 5(2):187–207
12. Rivera N (2008) Seamless connectivity and mobility in wireless mesh networks. Johns Hopkins University, Baltimore
13. Shah PA, Hasbullah HB, Afghan SA, Jung LT, Lawal IA, Mu'azu AA (2013) An enhanced procedure for mobile ipv6 route optimization to reduce handover delay and signaling overhead. In: International Multi Topic Conference. Springer, Cham, pp. 216–226
14. Boukerche A, Zhang Z (2008) A hybrid-routing based intra-domain mobility management scheme for wireless mesh networks. In: Proceedings of the 11th international symposium on Modeling, analysis and simulation of wireless and mobile systems, ACM, Oct 2008, pp. 268–275
15. Majumder A, Deb S, Roy S (2016) Classification and performance analysis of intra-domain mobility management schemes for wireless mesh network. In: Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies. ACM, Chicago, March 2016, p. 113
16. Huang R, Zhang C, Fang Y (2007) A mobility management scheme for wireless mesh networks. Proceedings of Global Telecommunications Conference, 2007 (GLOBECOM '07) 93241:5092–5096
17. Huang L, Yan Z, Liu Z, Huang H (2012) A strategy for mesh client mobility support in wireless mesh networks. In: Networking and Distributed Computing (ICNDC), 2012 Third International Conference on (pp. 69–71). IEEE, OCt 2012
18. Jang SH, Lee GS (2011) Mobility management scheme for the wireless mesh network using location server. Grid Distrib Comput Commun Comput Inf Sci 261:179–186
19. Tran M, Kim Y, Le J (2011) Load balancing and mobility management in multi-homed wireless mesh networks. KSII Trans Internet Inf Syst 5(5):959–975
20. Wang H, Huang Q, Xia Y, Wu Y, Yuan Y (2007) A network-based local mobility management scheme for wireless mesh networks. In: Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE, March 2007, pp. 3792–3797
21. Couto L, Barraca JP, Sargento S, Aguiar RL (2009) FastM in WMN: a fast mobility support extension for wireless mesh networks. In: proceedings of IEEE Second International Conference on Advances in Mesh Networks, pp. 90–96
22. Houyou AM, De Meer H, Esterhazy M (2006) P2P-based mobility management for heterogeneous wireless networks and mesh networks *. SpringerLink Lect Notes Comput Sci Wirel Syst Netw Archit Next Gener Internet 3883:226–241
23. Rajya Lakshmi L, Ribeiro VJ, Jain BN (2015) PRIME: a partial path establishment based handover management technique for QoS support in WiMAX based wireless mesh networks. Comput Netw 83:217–234
24. Yamarthy MR, Subramanyam MV, Prasad KS (2016) A multi-layer routing protocol for mobility management in wireless mesh networks. Procedia Comput Sci 89:51–56
25. Khasawneh FA, BenMimoune A, Kadoch M, Alomari A, Al-Khrayshah M (2015) Multihoming admission and mobility management in wireless mesh network. In: Computer, Information and Telecommunication Systems (CITS), 2015 International Conference on (pp. 1–5), IEEE, July 2015
26. Navda V, Kashyap A, Das SR (2005) Design and evaluation of imesh: an infrastructuremode wireless mesh network. In: World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a (pp. 164–170), IEEE, June 2005
27. Yang SH, Bao L (2011) Scalable mobility management in large-scale wireless mesh networks. In: Wireless Communications and Networking Conference (WCNC), 2011 IEEE (pp. 1230–1235), IEEE, March 2011
28. Zhang Z, Pazzi RW, Boukerche A (2010) A mobility management scheme for wireless mesh networks based on a hybrid routing protocol q. Comput Netw 54(4):558–572
29. Ren M, Liu C, Zhao H, Zhao T, Yan W (2007) MEMO: an applied wireless mesh network with client support and mobility management. In: Global Telecommunications Conference, 2007. GLOBECOM'07. IEEE (pp. 5075–5079), IEEE, Nov 2007
30. Sabeur M, Al Sukkar G, Jouaber B, Zeghlache D, Afifi H (2007) Mobile party: A mobility management solution for wireless mesh network. In: Wireless and Mobile Computing, Networking and Communications, 2007. WiMOB 2007. Third IEEE International Conference on (pp. 45–45), IEEE, Oct 2007
31. Huang D, Lin P, Gan C (2008) Design and performance study for a mobility management mechanism (WMM) using location cache for wireless mesh networks. IEEE Trans Mob Comput 7(5):546–556
32. Zhao W, Xie J (2012) IMeX: intergateway cross-layer handoffs in internet-based infrastructure wireless mesh networks. IEEE Trans Mob Comput 11(10):1585–1600
33. Majumder A, Roy S (2013) Design and analysis of a dynamic mobility management scheme for wireless mesh network. Sci World J 2013:16
34. Majumder A, Roy S (2016) Implementation of Forward Pointer-Based Routing Scheme for Wireless Mesh Network. Arab J Sci Eng 41(3):1109–1127
35. Li Y, Chen I (2011) Design and Performance Analysis of Mobility Management Schemes Based on Pointer Forwarding for Wireless Mesh Networks. IEEE Trans Mob Comput 10(3):349–361
36. Majumder A, Roy S (2012) A forward pointer based mobility management scheme for multi-hop multi-path wireless mesh network. In: Data Science & Engineering (ICDSE), 2012 International Conference on (pp. 194–197), IEEE, July 2012
37. Song J, Liu Q, Zhong Z, Li X (2012) A cooperative mobility management scheme for wireless mesh networks. In: Consumer Communications and Networking Conference (CCNC), 2012 IEEE (pp. 672–676), IEEE, Jan 2012
38. Amir Y, Danilov C, Musuăloiu-Elefteri R, Rivera N (2010) The SMesh wireless mesh network. ACM Trans Comput Syst (TOCS) 28(3):6
39. Amir Y, Danilov C, Hilsdale M, Musăloiu-Elefteri R, Rivera N (2006) Fast handoff for seamless wireless mesh networks. In Proceedings of the 4th international conference on Mobile systems, applications and services, ACM, June 2006, pp. 83–95
40. Chan H, Liu D, Seite P, Yokota H, Korhonen J. Requirements for distributed mobility management. Internet Engineering Task Force (IETF) RFC 7333
41. Motoyoshi G, Leibnitz K, Murata M (2010) Function-distributed mobility system for the future internet. In: Network Operations and Management Symposium Workshops (NOMS Wksps), 2010 IEEE/IFIP, IEEE, April 2010, pp. 28–35

42. Wakikawa R, Valadon G, Murai J (2006) Migrating home agents towards internet-scale mobility deployments. In: Proceedings of the 2006 ACM CoNEXT conference, ACM, Dec 2006, p. 10
43. Yu L, Zhijun Z, Tao L, Hui T (2010). Distributed mobility management based on flat network architecture. In: Wireless Internet Conference (WICON), 2010 The 5th Annual ICST, IEEE, March 2010, pp. 1–6
44. Bertin P, Bonjour S, Bonnin JM (2008) A distributed dynamic mobility management scheme designed for flat IP architectures. In: New Technologies, Mobility and Security, 2008. NTMS'08, IEEE, Nov 2008, pp. 1–5
45. Bertin P, Bonjour S, Bonnin JM (2009) An evaluation of dynamic mobility anchoring. In: Vehicular Technology Conference Fall (VTC 2009-Fall), 2009 IEEE 70th, IEEE, Sept 2009, pp. 1–5
46. Ernest PP, Chan HA (2011) Enhanced handover support and routing path optimization with distributed mobility management in flattened wireless networks. In: Wireless Personal Multimedia Communications (WPMC), 2011 14th International Symposium on (pp. 1–5), IEEE, Oct 2011
47. Kawano K, Kinoshita K, Yamai N (2008) A distributed mobility management scheme for large-scale Mobile Networks. In: Local Computer Networks, 2008. LCN 2008. 33rd IEEE Conference on (pp. 500–501), IEEE, Oct 2008
48. Song M, Huang J, Feng R, Song J (2006) A distributed dynamic mobility management strategy for mobile ip networks. In: ITS Telecommunications Proceedings, 2006 6th International Conference on (pp. 1045–1048), IEEE, June 2006
49. Fischer M, Andersen FU, Kopsel A, Schafer G, Schlager M (2008) A distributed IP mobility approach for 3G SAE. In: Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on (pp. 1–6), IEEE, Sept 2008
50. Giust F, De la Oliva A, Bernardos CJ (2011) Flat access and mobility architecture: An IPv6 distributed client mobility management solution. In Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on (pp. 361–366), IEEE, April 2011
51. Liu S, Cheng X, Fu W, Zhou Y, Li Q (2014) Numeric characteristics of generalized M-set with its asymptote. Appl Math Comput 243: 767–774
52. Liu S, Pan Z, Fu W, Cheng X (2017) Fractal generation method based on asymptote family of generalized Mandelbrot set and its application. J Nonlinear Sci Appl 10(3):1148–1161
53. Perkins EC, Johnson D, Arkko J (2011) Mobility Support in IPv6. Internet Engineering Task Force (IETF) RFC 6275
54. Shah PA, Hasbullah HB, Lawal IA, Mu'azu AA, Jung LT (2014) a totp-based enhanced route optimization procedure for mobile IPv6 to reduce handover delay and signalling overhead. Sci World J 2014(1):16
55. Aldabbagh G, Shah PA, Hasbullah HB, Aadil F, Awan KM, Marwat F (2017) Fuzzy Logic Based Enhanced AOMDV with Link Status Classification for Efficient Multi-Path Routing in Multi-Hop Wireless Networks. J Comput Theor Nanosci 14(1): 620–630
56. Shah PA, Hasbullah HB, Rafique S, Rehman SU, Jung (LT) Fuzzy logic based link status classification for efficient multipath routing in multi-hop wireless mesh networks. In: in proceedings of 2nd IEEE International Conference on Computer & Information Sciences (ICCOINS 2014)
57. Salomaa A (2013) Public-key cryptography (texts in theoretical computer science. An EATCS Series), 2nd Edition. Springer
58. M'Raihi D, Machani S, Pei M, Rydell J (2011) TOTP: Time-Based One-Time Password Algorithm. Internet Eng Task Force RFC 6238:1–17
59. Boukerche A, Turgut B, Aydin N, Ahmad MZM, Bölöni L, Turgut D (2011) Routing protocols in ad hoc networks: A survey. Comput Netw 55(13):3032–3080
60. Tarique M, Tepe KE, Adibi S, Erfani S (2009) Survey of multipath routing protocols for mobile ad hoc networks. J Netw Comput Appl 32(6):1125–1143
61. Jiang M, Tay YC (1999) Cluster Based Routing Protocol (CBRP). Internet Eng Task Force Draft Draft 1–13
62. Makaya C, Pierre S (2008) Enhanced fast handoff scheme for heterogeneous wireless networks. Comput Commun 31(10):2016–2029
63. Makaya C, Member S, Pierre S, Member S (2008) An Analytical Framework for Performance Evaluation of IPv6-Based Mobility Management Protocols. IEEE Trans Wirel Commun 7(3):972–983
64. Baumann FV, Niemegeers IG (1994) An evaluation of location management procedures. In: proceedings of Third Annual International Conference on Universal Personal Communications, 1994 (UPC '94), pp. 359–364
65. Li F (2005) A novel haleness and efficiency method for return routability procedure in mobile IPv6. In: Communications and Information Technology, 2005. ISCIT 2005. IEEE International Symposium on (Vol. 1, pp. 470–473), IEEE, Oct 2005
66. Nandiraju N, Nandiraju D, Santhanam L, He B, Wang J, Agrawal DP (2007) Wireless mesh networks: current challenges and future directions of web-in-the-sky. IEEE Wirel Commun 14(4):79–89
67. Liu S, Lu M, Liu G, Pan Z (2017) A Novel Distance Metric: Generalized Relative Entropy. Entropy 19(6):269
68. Liu S (2016) Recent Research and Application in Multimedia Part II. Recent Advances in Electrical & Electronic Engineering (Formerly Recent Patents on Electrical & Electronic Engineering) 9(2):82–82
69. Yang G, Liu S (2014) Distributed cooperative algorithm for k-M set with negative integer k by fractal symmetrical property. Int J Distrib Sens Netw 10(5):398583