International Journal on Advanced Science Engineering Information Technology

Vol.7 (2017) No. 2
ISSN: 2088-5334

Investigation of Home Agent Load Balancing, Failure Detection and Recovery in IPv6 Network-based Mobility

Anshu Khatri[#], Senthilkumar Mathi[#]

[#]*Department of Computer Science and Engineering, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, Amrita University, India*
E-mail: cb.en.p2cse16004@cb.students.amrita.edu, m_senthil@cb.amrita.edu

***Abstract*— Mobile IPv6 came as an extensively acknowledged technology to support mobility in networks. Home agents are in charge for the registration of mobile devices and act as a key entity for the tunneling of data packets to the corresponding registered mobile nodes. A single home agent has administrative control over the critical tasks including home agent registration management, maintenance of cache data and tunneling of data packets to the mobile nodes that are away from their home networks and so on. However in this approach, home agent act as the sole failure point, which gave rise to the placement of multiple home agents to overcome this issue. The load balancing mechanism for multiple home agent deployment faces the problem of improper load sharing, signaling overhead and synchronization issues. Moreover, failure detection and recovery mechanism are inefficient in nature. It experiences a significant delay in tunneling of data packets and suffers from disconnection making it incompetent for the use in real time applications. Most of the existing methods for load sharing and failure detection use the concept of exchange of router advertisement message named as "heart beat messages" at a constant rate. The reduction in the interval of router advertisement can result in signaling overhead and synchronization issues. Hence, this paper investigates and analyzes the various load balancing mechanisms of mobile IPv6. In addition, it presents the comparative study of the failure detection and recovery mechanism of existing methods. Finally, it concludes that future work can be extended in the domain of distributed active load sharing mechanism and proactive failure detection.**

***Keywords*— distributed load balancing; binding update; IPv6 mobility; binding acknowledgement; route optimization**

I. INTRODUCTION

The Internet Protocol (IP) is the fundamental communication protocol for the delivery of datagrams across the network. Its routing function enables internetworking, and actually establishes the internet connection. The task of delivering packets from the source host to the destination host is merely based on the concept of IP addresses in the packet headers [1]. The IP specifies the format of packets that encapsulates the data to be delivered and the addressing scheme that is used to label the datagram with source and destination data.

Every device that is connected to the Internet has a unique IP address. It provides the identification and location information of the device which is required to send data to or receive from other devices in the network. IPv4 uses 32-bit addressing format which limits the address space to 4294967296 (2^{32}) addresses. The explosive rate of people all over the world connecting to the Internet and the stupendous number of new devices that are getting connected every day causes the global IPv4 pool to deplete to a critically low level. It is suffering from scalability issue, lack of proper routing, network instability and incapability to offer new IP for present and future devices resulted in exhausting of all IP's. The decreasing availability of IPv4 addressing space led to the incorporation of IPv6 into the networks [2]. IPv6 is a 128-bit addressing format, theoretically allowing 2^{128} compared to 2^{32} IPv4 address. The salient features of IPv6 are: extended addressing capabilities, ordered hierarchy for managing growth of routing table, stateless autoconfiguration, streamlined header format and flow identification, enhanced support for extensions, security, well-built IP layer encryption and authentication, mobility, Quality of Service (QoS), privacy extensions for stateless address auto configuration and source address selection etc. It is easy to understand the addressing scheme of IPv6. Any global address can be accessed on the network [3], [4].

Mobile IP was initially defined as an expansion to IPv4 to support mobility, which suffers from the problem of routing, only point of failure of Home Agent (HA) in mobile IPv4, multiple HAs support, route optimization, and IP security. Mobile IPv6 (MIPv6) solved these problems and evolved as a widely recognized technology to support mobility in networks [5]. Each Mobile Node (MN) in the mobile IP

networks has a specific IP home addressing associated to the home network. MN acquires a temporary care-of address using stateless auto-configuration or DHCP when it visits a new foreign network as illustrated in Fig. 1. It sends a registration message to its HA to inform about the new location [3]–[8], [40]. After receiving and accepting the registration, the HA captures all the packets that are coming to the MN's home address. While MN are roaming, one single HA takes care of forwarding IP datagrams, manages HA registration, maintains caches and tunneling of data packets for MNs that are away from their home networks, resulting in unfavourable impact on the robustness and overall performance of the network [43],[44], [46], [60], [62], [70].

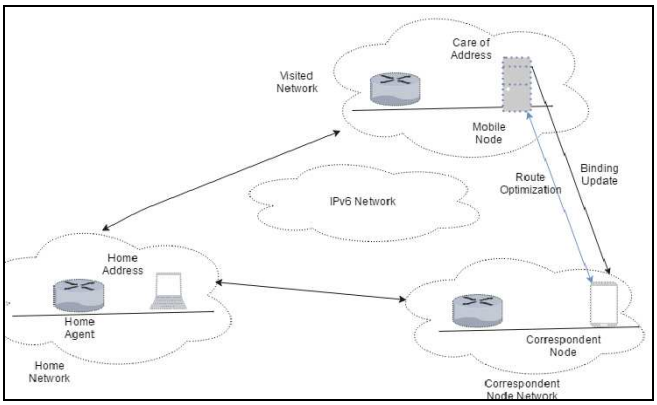

Fig. 1 Mobile IPv6 operation

The two main approaches: the centralized approach and the distributed approach are present for HA load balancing. The centralized approach provides more administrative control; only one HA is accountable for gathering load sharing parameters from all the nearby HAs and takes decision for HA load assignment. The distributed approach overcomes the problem of single point of failure in centralized mechanism because in this each and every HA shares its information with other HAs. Many investigations in the direction of deployment of multiple HAs have been suggested to solve the problem of the single point of failure [7], [58], [63], [71]. But these are susceptible to issues such as increased flow of message exchange, disconnection between HA and MN and a longer period for the HA registration. The centralized approach is predominantly used in the existing mobile networks which have an improper load on one HA. The load sharing and failure detection use the concept of exchange of router advertisement message named as *"heart beat messages"*. Each router sends these messages through multicasting at a constant rate. However, issues related to signaling overhead and synchronization would increase with the reduction in the time interval of router advertisement [9], [10].

The rest of the paper is organized as follows. Section II describes the previous works carried out in this domain. Section III discusses the comparative analysis of the existing methods. Lastly, conclusions and future work are discussed in Section IV.

II. Material and Method

Dynamic Home Agent Address Discovery (DHAAD) protocol follows the mechanism of distributed approach. Each and every HA manages a list of all HAs present in the network. An address discovery request is transmitted by the MN on the anycast address of an HA and wait for the reply. Basically, anycast addressing is used to enable the router to select different anycast destination for every packet. If MN doesn't receive the reply message within the time limit, the MN may retransmit the registration request to the same anycast address. Every succeeding retransmission is delayed twice the time interval of the previous retransmission. This protocol is majorly used by the most of the load sharing mechanism for the HA registration process [10], [11]. Another example of distributed approach is Inter Home Agent (HAHA) protocol. It pursues few features of DHAAD as each HA maintains a list of HA located on the network and shares the binding table as well. In the case of HA failure or overloading, HA switch message is transmitted either by the same HA or backup HA to the affected MN. The MN drop off its present binding after the reception of the switch message and sends a BU to the preferred HA which is sent along the switch message. If no preferred HA is sent, MN uses DHAAD request message on HA's any cast address [12], [13].

Home Agent Handoff (HAH) scheme is also similar to DHAAD and HAHA, maintains a list of HAs [10]. This list is extended to support load sharing parameters and is dependent on router advertisement to update the entries where HA bit is set. Each and every HA shares the information that helps to take HA reassignment decision. HA uses HAH message to signal the MN regarding the HA failure or overloading. Upon reception of HAH message, the MN follows the same steps as discussed in HAHA method. The current binding to the failed HA is deactivated, and BU is directed to the preferred HA. In the case of absence of preferred HA details, the affected MN follows DHAAD mechanism. The method presented in [10] considers load as a combination of MNs registered to HAs plus network traffic through the network. The network contains set of HAs and a gateway router with the assumption that there is a sort of redundancy for gateway routers. HA registration can have two situations: MN is aware of its HA, and MN doesn't know its HA. In the first situation, MN can send BU to its HA, whereas in the second situation, it uses either DHAAD or DNS protocol to obtain the HA's IP address. The failure detection mechanism uses the concept of *"heart beat messages"* to detect the failure and it is transparent to MN. The messaging overhead is reduced because the MN does not perform any activity in the failure detection. The gateway router maintains a binding table that contains all the MN registration on the network. During HA failure, re-registration request would be issued to the affected MNs after consulting the binding table.

Load balancing mechanism allows MN to get registered to only one HA over the Home link. The servicing HA sends HA switch message along with the preferred HA to some of its registered MNs in the case of overloading. These MNs deregister their present binding and re-register again with the preferred HA [14]. Inter HA's protocol reliability and load balancing mechanism are also discussed which is said to be

transparent to the MN whereas it is not entirely transparent in every possible situation. When the binding expiration and failure of serving HA occur at the same time, the MN has no information about its new serving HA. Consequently, the MN sends all the data packets to the failed HA and waits for the reply. The MN will infer that HA has failed based on the no-reply from the failed HA and should get registered to a new HA. The pretentious MN initiates HA re-registration process again to establish the connection with a new HA. This mechanism is not transparent to MN and leads to the service interruption because MN having no information of its new serving HA continues to tunnel the packets destined for the Correspondent Node (CN) through failed HA's IP address only [15].

Subsequently, a load sharing is suggested for both IPv4 and IPv6 HAs [9], [10]. Each HA maintains a queue along with the defined upper and lower thresholds. When the sub-threshold value is crossed, HA broadcasts its queue length and makes policy table on each HA. Upon crossing the threshold value, HA selects one MN and register it to another HA after inspecting the policy table followed by a re-evaluation of the queue length to check the results. If it is not successful, then another MN is selected to move to another HA. The HA failure detection is not handled by this mechanism.

Many HAs are deployed over different home links in a mechanism discussed in [11], [16]. An MN connects to one or more HAs in which any one of the HA is preferred as a primary HA by the MN. Tunneling of packets from CN to MN can be either through the primary HA or any other HA. The failure of the primary HA is not transparent in nature. After primary HA failure, the MN switches to any other HA on the same home link as its primary HA's home link. This method adds extra overhead on the MNs and causes service interruption as well. Moreover, delayed failure detection problem is not addressed. The hybrid load balance mechanism suggested in [11] comprises of multiple MIPv6 based HAs and MNs. Each HA is attached to an access router as shown in Fig. 2 and manages a traffic load table that is sorted in descending order of the traffic load field. Each HA broadcasts its traffic table to other HAs in the network to take HA reassignment decisions. Each entry in the binding update table has a timer associated with it and is taken for HA reassignment once the timer goes out.

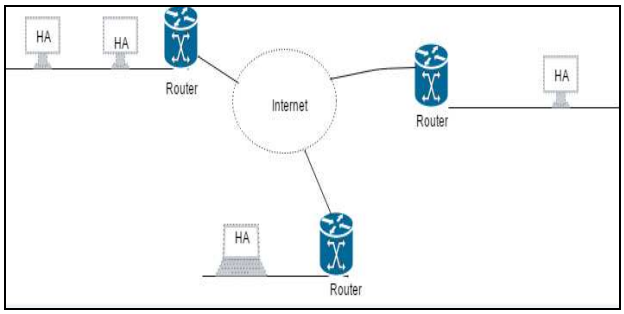

Fig. 2 Hybrid load balance architecture

Virtual Home Agent Reliability Protocol (VHARP) architecture is same as MIPv6 with few extensions to it. In this method, one home link comprises of multiple HAs having different link-local IP addresses. The home link has one global IP address taken as global HA address [17]. This address is used for all the communication between CN and any HA in a home link providing a single virtual view of all the HAs on the home link. Each HA can take any of these three states: active HA, backup HA, and inactive HA. The failure detection is based on *"heart beat messages"* and recovery is performed either as active HA or backup HA recovery based on the recovery procedure [68]. Failure detection and recovery mechanism are transparent to MN; therefore it does not result in any service interruption and latency [18], [19].

Virtual Home Link (VHOL) follows the same architecture and working as VHARP discussed in [17] and integrates home link redundancy to address the issue of a single home link failure of VHARP as presented in Fig. 3. The load balancing and failure detection mechanism follows the message exchange technique and is transparent to MN. The rate of exchanging messages is less as compared to VHARP; therefore VHOL has less signaling overhead. This method is efficient in resource utilization as it utilizes all the secondary links in addition to the primary link. There is no service interruption in VHOL, and each HA in the home links has fewer loads overhead as compared to VHARP [19].

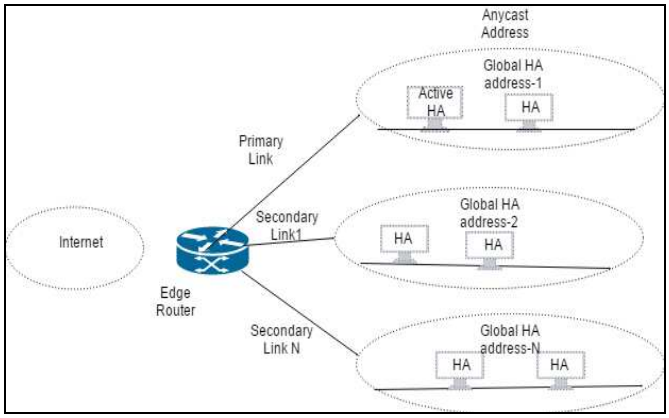

Fig. 3 VHOL architecture

Web services load balancing techniques are discussed in [20], [51], [69]. It suggests to add more hardware resources and to make web server improvement with respect to changing demands. This approach is not cost effective and does not provide a long lasting solution. Distributed web servers with multiple nodes can be deployed to provide a better solution. These distributed web servers are loosely coupled and act as a single server from the client's perspective. A load balancer is presented that contains two modules: mobility agent and regular load balancer device. MN initiates registration request in order to set up the optimized route with the servers and sends packets once the connection is established. TCP slicing load balancing and packet rewriting are compatible with MIPV6's registration request, whereas MIPv6's registration request compatibility is not provided by mobility agents in case of packet forwarding technique and MN interact through sub-optimal route with the server. The sub-optimal path suffers from many limitations; it increases infrastructure to load and packet overhead. It is also not much capable of addressing link failures.

Multiple HA deployment scheme (MHADS) enhances service availability and improves performance. It comprises of a dynamic load balancing and faults tolerance procedure in order to provide a single HA mirror image for transparent load balancing and failure detection mechanism. The edge router in the home link acts as a BM (Balancer and Monitor). It works as a balancer in case of load sharing and as a monitor in the detection of HA failure and recovery mechanism. In addition, it performs active load sharing by selecting the best HA during the registration process itself. The load parameters of every HA is calculated using dynamic weight load evaluation algorithm. The HA-failure detection and recovery procedure is based on the widely used concept of *"heart beat messages"*. Every HA updates BM and sends these messages in regular interval of time. The BM uses failure detection request and answer during the absence of acknowledgement from HA for a period of time along with ring backup chain for failure takeover and recovery process [7]. Network segmentation is used in the backup quorum management mechanism [21]. It has a circular architecture in nature in which each HA equally segments its network. Every HA has a backup quorum to store the details of MNs. During HA failure, least loaded backup quorum provides services to the MNs. A number of backup bindings can be reduced by using the small quorum size. This method does not add extra hardware cost and has low registration overhead as well [22].

Virtual Private Network based Home Agent Reliability Protocol (VHAHA) defines a network having multiple home links [23]. Each home link contains multiple HAs that can take any state out of these three states: active HA, backup HA and inactive HA [17], [18]. Virtual Private Network (VPN) is created out of the set of some selected HAs and is assigned the Global HA address. Each HA knows the status of other HA inside the VPN due to the periodical announcement of "Heat Beat Messages". Each HA that is part of global HA address get notified when a packet reaches the global HA address. The HA that is nearest to the MN has less overhead and receives the packet. The failure detection and recovery mechanism are transparent to the MNs; hence over the air (OTA) messaging is reduced. Each HA has a defined load that is used to set the priority among the HAs. The assigned priority is dynamic in nature and gets updated corresponding to every change in mobility binding. This method adds up some overhead and complexity, but it is negligible in nature. It provides better reliability because it is functioning even when the entire home link fails [72].

The solution presented in [24] assumes that multiple HAs, called as "Home Agents Group" (HA Group), can work concurrently to overcome the difficulty of HA as the only failure point. All the mobility management tasks are handled by the main HA and are taken over by stand-by HA when the main HA fails. The signaling mechanism is used to detect HA failure and is followed by HA switch to recover from it. The switching between main HA and stand-by HA can either be soft or hard switching. The performance of HA failure recovery depends on the destruction of the tunnel with the failed HA and creation of a new tunnel with another HA.

Global HAHA method follows the distributed mechanism to overcome the single point of failure and triangular routing problems that occur in centralized mobility handling. Fig. 4 presents the architecture in which multiple HAs are grouped under one Global HA representation. MNs use anycast messages to notify these HAs regarding MN's current location. HA nearer to the MN will respond to the message and act as the primary HA for the MN [25], [26].

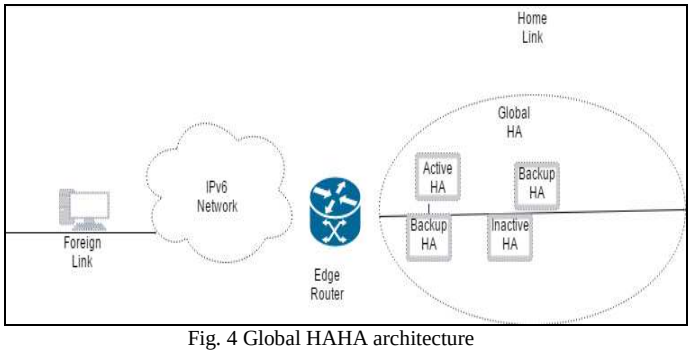

Fig. 4 Global HAHA architecture

The connection establishment of an MN with the nearest HA results in a reduction of the probability of HA handoff failure. Reliable HA delivery (RHAD) method discussed in [27] uses this connection establishment technique. Its network architecture has edge router which is basically a router at the boundary that inspects the BU from MN and maintains a router list. This BU information stays in router list till BU lifetime becomes zero. RHAD uses gateway protocol to transmit packets between the edge router and HAs. When an MN broadcasts BU, it is transmitted through the edge router, and the HA that is nearest is selected as active HA. The stand-by HA is selected by the active HA based on the preference levels and maintains a synchronized binding between active, and standby HAs. The failure detection and recovery technique follow the similar procedure as discussed in VHARP; therefore it is transparent to MN.

The Multihomed Mobile Network Architecture (MMNA) presented in [28] discusses the benefits of multihoming and provides multihoming management mechanism. It comprises of two main components: multihomed tree establishment and gateway discovery as given in Fig. 5. Its extension includes multiple care-of addresses to support multiple gateways within the tree [29], [39], [59]. The information is advertised by each gateway to the mobile routers, and the selection process can take place at different levels. The gateway selection can either be flow based or network based [64]-[67].

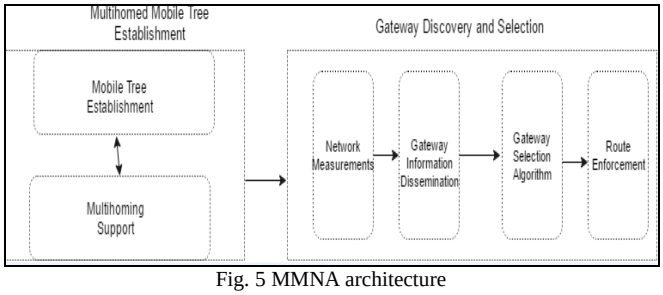

Fig. 5 MMNA architecture

The hierarchical MIPv6 is discussed in [30], [31] to address mobility issues. A new MIPv6 node named as

mobility anchor point can be situated at any level in the foreign network. It also has two new addresses to take into consideration: regional and on-link care-of-address. When the MN receives these addresses, it sends the BU to the anchor point to establish the connection between the two addresses. The attributes of the anchor point, MN, and network topology determines the selection process of mobility anchor point in the foreign network [45], [49], [61]. Another extension to MIPv6 is Proxy MIPv6, which act as a core network mobility management protocol [32], [33]. The two main elements in this approach are local mobility anchor and mobility access gateway. The network prefix of the MN has the local mobility anchor as the anchor point and the access gateway act as the router for the MN [34]–[38], [41]. An access link is provided by the gateway to which MN attaches when it gets into the network. The gateway checks the authorization of using services with the help of authentication, authorization and accounting server [42], [47], [48], [50]-[57].

III. Results and Discussion

In this section, the analysis and comparison of the various existing methods for load balancing and failure detection mechanisms are discussed. The parameters considered for comparison of the existing methods include throughput, signaling overhead, the number of MNs registered and latency for failure detection and recovery.

In redundant HA, registration of MNs to the HAs can have two situations: MN is aware of its HA, and MN does not know its HA. In the first situation, MN can send BU to its HA, whereas in the second situation, it uses either DHAAD or DNS protocol to get the HA's IP address. VHARP and VHOL suffer high registration overhead due to the updating and synchronization of binding cache entries among active, backup and inactive HAs. HA Group method uses the concept of BU/BA for the HA registration process. Each HA maintains a traffic load table and monitor its queue size for the registration of an MN to an HA in the case of the Hybrid method. It uses traffic load advertisement for the reassignment of HAs when the timer that is associated with the corresponding entry expires. The MHADS uses BM which maintains home agent tables for active load sharing by selecting the least loaded HA during the HA registration process itself. The RHAD and VHAHA methods have low overhead as compared to the other methods given in Table 1.

TABLE I
Comparison of HA Registration Overhead

Metrics	HA registration overhead
Redundant HA	Either BU/BA messaging or DHAAD
VHARP	High
HA Group	BU messaging
MHADS	Low
VHOL	High
Hybrid	Traffic load table and ICMP Messaging
RHAD	Low
VHAHA	Low

Although MHADS and VHAHA provide active load balancing, yet most of the existing load sharing mechanism uses the concept of passive load sharing. The load sharing mechanism is not transparent to the MN and adds to the OTA signaling overhead in case of redundant HA method. VHARP and VHOL also suffer more loads sharing overhead due to its complex architecture and centralized approach. The traffic load table maintenance and load advertisement in Hybrid method add to the load sharing overhead. In this method, HA is reassigned to an MN when the timer associated with the corresponding MN expires. The MHADS experiences low overhead as compared to the other existing methods represented in Table 2. It has BM which dynamically collects and maintains the load details of every HA and selects the least loaded HA during the registration process itself.

TABLE II
Comparison of Load Balancing Mechanism of Existing Methods

Metrics	Load sharing mechanism (active /passive)	Load sharing overhead
Redundant HA	Passive	High
VHARP	Passive	High
MHADS	Active	Low
VHOL	Passive	High
Hybrid	Passive	High
VHAHA	Active	Less than VHARP

VHARP failure detection and recovery mechanism are restricted to only one home link. This method fails in case of complete failure of the home link, therefore to overcome this issue VHOL method is used which uses the pair of one primary home link and one or more secondary home links. The redundant HA method uses the concept of *"heart beat messages"* for failure detection which adds to the signaling overhead and takes more time in detecting HA failure. MHADS uses messaging same as redundant HA plus failure detection request and answer to detect failure which adds to the failure detection time and signaling overhead. RHAD uses the concept of VHARP and BGP. It has low signaling overhead and failure detection time than VHARP.

Mostly methods that are listed in Table 3 and 4 have transparent failure detection and recovery mechanism. Therefore, the OTA signaling overhead is negligible except redundant HA method in which recovery is not transparent to the MNs and adds to the OTA signaling. The redundant HA suffers more failure recovery time in which HA re-registration request is sent to the affected MNs which results into OTA signaling. VHOL experiences more recovery time than VHARP as it takes time for the synchronization of the updates among active, backup and inactive HAs through a pair of a primary home link and one or more secondary home links. HA recovery method in HA Group considers failure recovery time plus tunnel destruction and construction time. MHADS uses a pair of signals of service restoration request and takeover in the ring backup chaining process which increases the time for the HA failure recovery. VPN is constructed in VHAHA mechanism in which the selected HAs are assigned Global HA address. It has low

failure recovery time because recovery process is confined to this VPN.

TABLE III
COMPARISON OF FAILURE DETECTION

Metrics	Fault tolerant range	Failure detection Time	Fault detection signaling overhead
Redundant HA	Covers entire range	High	High
VHARP	Limited to Home Link	Moderate	High
HA Group	Covers entire range	Low	Low
MHADS	Covers entire range	High	High
VHOL	Covers entire range	More than VHARP	Less than VHARP
RHAD	Covers entire range	Less than VHARP	Low
VHAHA	Covers entire range	Less than VHARP	Comparable to VHARP

TABLE IV
COMPARISON OF FAILURE RECOVERY

Metrics	Transparency	Failure Recovery Time	OTA messages exchanged for recovery
Redundant HA	Recovery is not transparent to MN	High	Low
VHARP	Yes	Low	Nil
HA Group	Yes	High	Nil
MHADS	Yes	High	Nil
VHOL	Yes	Moderate	Nil
RHAD	Yes	Low	Nil
VHAHA	Yes	Low	Nil

A. Impact of Number of Registrations of MNs on HA's Throughput

As shown in Fig. 6, the throughput increases with the increase in the number of registered MNs, but as the number of MNs becomes more, it starts decreasing. In HA Group method, it is showing a great fall as compared to other methods due to the overhead of tunneling mechanism. The throughput of VHOL is more as compared to VHARP because all the primary links, as well as the secondary links, are properly utilized. The re-registration request to the MN in the redundant HA method during the load sharing and failure recovery leads to the OTA overhead. The MHADS performs better due to active sharing of the load during the HA registration process itself. It uses the concept of *"heart beat messages"* for active failure detection followed by an exchange of a pair of messages of failure detection request and response for ensuring HA failure. MHADS throughput performance is comparatively low than hybrid model due to the use of ring backup chain concept used for failed HA takeover. The hybrid model makes use of traffic load tables in which HA re-assignment is performed only when there is a significant load difference and has less re-assignment overhead.

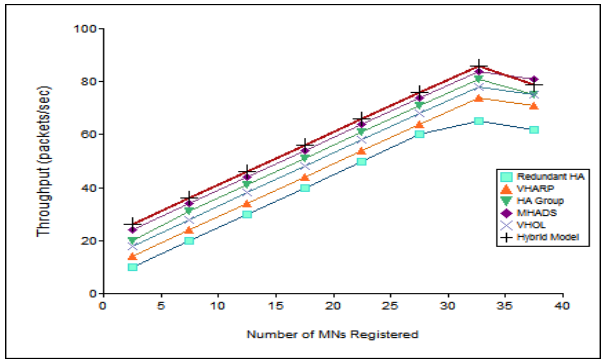

Fig. 6 Effect of number of MNs registered on the throughput

B. Signaling Overhead and Throughput

The predominantly used approach in the existing methods for load sharing and failure detection is through the exchange of *"heart beat messages"*. Each router multicasts these message at a constant rate. However, signaling overhead and synchronization issues increases with the decrease in the time interval of advertisement of messages. Therefore, more signaling results in the reduction of throughput.

As shown in Fig. 7, for a given throughput, the redundant HA suffers the most because it uses re-registration request by MN for the load sharing and failure recovery which adds to the OTA messaging. VHOL has low signaling overhead as compared to VHARP because time interval of the router advertisement messages is more in comparison to VHARP. Signaling is reduced in the case of the Hybrid model as it only advertises messages when traffic load table is in an overloaded state. The hybrid model performs better than MHADS because in the case of later *"heart beat messages"* is periodically advertised to maintain the connections but it advertises HA transfer request only when HA is overloaded, therefore has low overhead as compared to the other methods.

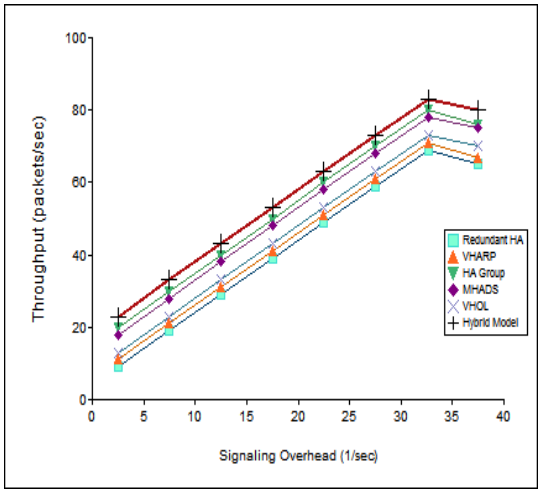

Fig. 7 Throughput vs signaling overhead

C. Failure Detection Time

Although failure detection in redundant HA method is transparent to the MN, recovery scheme is not transparent in nature. Each HA sends *"heart beat messages"* to the gateway and absence of this periodic messages is taken as an HA failure by the gateway. These messages are broadcasted at a constant rate. If the advertisement of messages is done at a longer time interval, then signaling overhead can be taken in control but failure detection takes more time. The VHOL is an extension to VHARP method and overcomes the limitation of the single home link failure. The rate of the interval for the router advertisement messages is taken more in VHOL leading to the increase in failure detection time. As shown in Fig. 8, failure detection time for RHAD and VHAHA is comparable in nature and less than VHARP. MMNA provides fast failure detection and recovery scheme. The stand-by HA in HA Group method detects the failure instantly by means of signaling packet. MHADS uses the concept of *"heart beat messages"* for the failure detection in addition to failure detection request and answer which adds to the failure detection time.

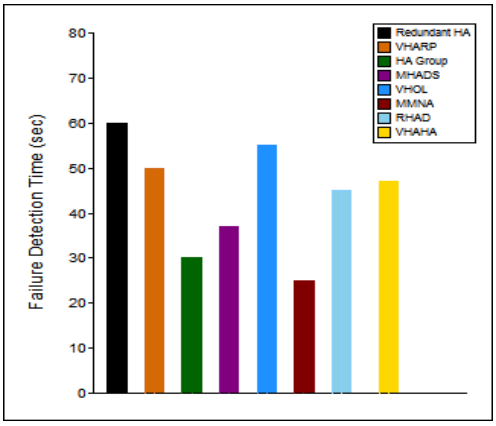

Fig. 8 Comparison of failure detection time

D. Signaling Overhead for the Given Number of MN's Registrations

Fig. 9 shows that the number of messages exchanged in VHAHA is higher as compared to others, but it is comparable to VHARP protocol. The number of recovery messaging is less in RHAD; therefore it has less signaling overhead. The VHARP causes notable message exchange and suffers more signaling overhead as compared to VHOL due to less time interval rate for the advertisement of router messages. The redundant HA also suffers considerable signaling overhead. It suffers OTA signaling in addition of periodic *"heart beat messages"* as the number of registered MNs increases and failure recovery process takes place. Although MHADS and HA Group , both uses the concept of *"heart beat messages"*, MHADS has more signaling overhead because of the presence of failure detection request/answer and service takeover request/answer messages.

E. Failure Recovery Time Vs Number of MNs

The procedure of tunnel destruction from the failed HA to the creation of tunnel to a new HA in the case of HA Group method adds to the failure recovery time. In MHADS, service takeover request / answer messaging plus reconstruction of ring backup chain contributes to the failure recovery time. The VHARP, VHOL, and VHAHA provide a comparable amount of time in recovery. HA re-registration message overhead is reduced because failure recovery is completely transparent to the MNs. The VHOL has one primary home link and one or more secondary home links whereas VHARP has only one home link. Therefore, the VHOL consumes more recovery time in comparison to VHARP after detection of the HA failure as shown in Fig. 10. The VPN is constructed in the VHAHA method in which selected HAs are assigned one global HA address. It has less failure recovery time because recovery process is confined to VPN only.

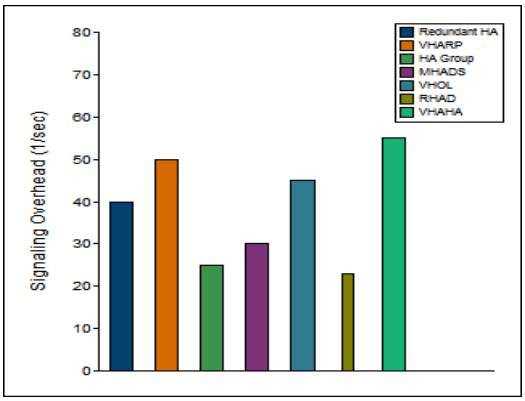

Fig. 9 Comparison of signaling overhead of various methods

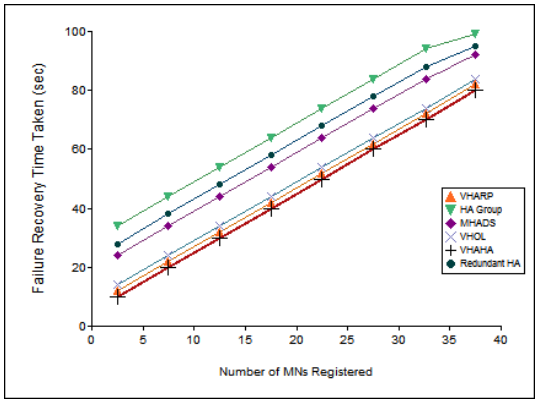

Fig. 10 Failure recovery time vs. number of MNs

E. Registration Time Vs. Number of MNs

In redundant HA method, MN either knows its HA or does not know. If it does not know, it follows DHAAD mechanism, which provides less registration time for the MN-HA registration. The VHAHA inherits the architecture from VHARP with few modifications. In this method, few HAs are selected to construct VPN, and one Global HA is assigned to the VPN. It provides better registration time as compared to VHARP. The VHARP and VHOL both uses the list of active, backup and inactive HAs and has comparable HA registration time. MN selects the nearest HA as active HA for the registration in RHAD. It selects the stand-by HA from the redundant list of HAs and maintains synchronization among them. The MHADS uses the function module of BM which receives the registration request from the MNs and selects the best HA for the

registration process. The HA overloading is actively prevented in this method because it selects the best HA at the time of registration itself. In comparison to RHAD, it takes more registration time due to the overhead involved in HA list maintenance and selection at BM as shown in Fig. 11.

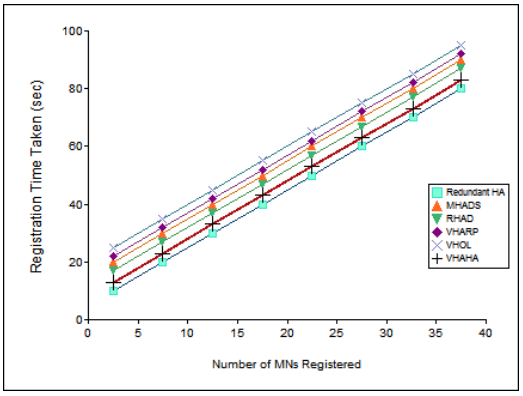

Fig. 11 Registration time vs number of MNs

G. OTA Interface Messaging Overhead

The Failure recovery procedure is not transparent to the MNs in redundant HA method, although failure detection is transparent in nature. This leads to the OTA message overhead. Other discussed methods have failure detection and recovery mechanism transparent to the MN, therefore has negligible OTA signaling overhead as represented in Fig. 12.

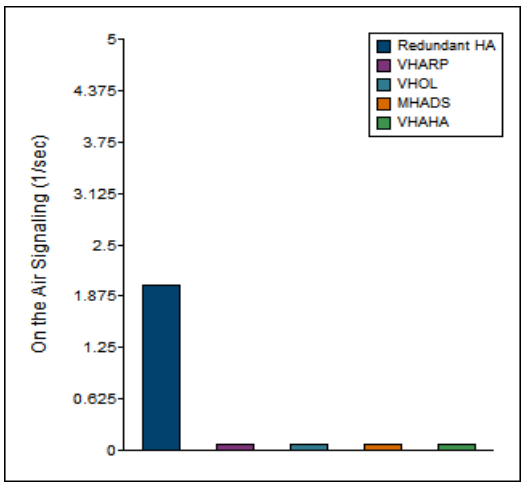

Fig. 12 Comparison of OTA signaling overhead

H. Failure Detection Signaling Overhead

The failure detection signaling overhead is almost same in VHARP and VHAHA as given in Fig. 13. Although VHAHA has more signaling overhead as compared to other mechanisms, yet it outperforms other methods and provides reliability even when the entire home link fails. The failure detection signaling overhead is less in VHOL in comparison to VHARP because the rate at which router advertises signaling messages is more than that of VHARP messaging rate.

The redundant HA also uses the "*heart beat messages*" and adds to the signaling overhead. The MHADS method follows the same mechanism as the redundant HA with additional messaging of "*failure detection request*" and "*failure detection answer*", therefore faces more signaling overhead as compared to the redundant HA. Whereas in HA group, advertisement messaging takes place between primary HA and stand-by HA resulting in less signaling overhead with respect to the redundant HA.

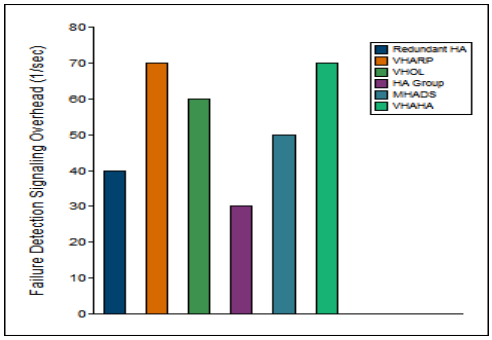

Fig. 13 Comparison of signaling overhead for failure detection

I. Load Sharing Signaling Overhead

The redundant HA faces more signaling overhead as compared to other load sharing methods. The load sharing process is initiated by sending HA re-registration request by the HA to the MNs when HA is in over loaded state. It includes the preferred HA address, and MN initiates the new registration process. It is not transparent to the MN and adds to the OTA messaging leading to increased signaling overhead. The complex architecture of VHOL adds more signaling overhead as compared to VHARP.

The hybrid model uses the concept of traffic load tables in which a timer is associated with each entry in the table. HA re-assignment occurs only when there is a significant load on an HA or when the timer expires. HA sends the ICMP reply message by itself without the reception of the ICMP request, if it selects the new HA for the affected MNs, therefore has less signaling overhead in comparison to previously discussed methods. The load balance performance and the handoff frequency determine the rate of selection of a new HA. Fig. 14 shows that load sharing signaling overhead is least in MHADS method that actively selects the best HA using single HA mirror image. HA sends the load transfer request to the BM only when it is in the overloaded state, and BM again selects the best HA for the re-registration process.

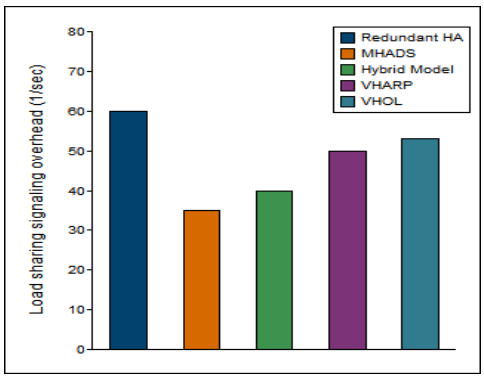

Fig. 14 Comparison of signaling overhead for load sharing

IV. CONCLUSIONS

In this paper, the comparative study of various load balancing, failure detection and recovery mechanisms in MIPv6 based network is presented. Many investigations in the direction of deployment of multiple HAs have been suggested to solve the single failure point problem of an HA. But these are susceptible to issues such as increased flow of message exchange, disconnection between HA and MN and a longer period for the HA re-registration. The centralized approach is predominantly used in the existing mobile networks which have improper load on one HA. The load sharing and failure detection use the concept of exchange of router advertisement message named as *"heart beat messages"*. Each router multicasts these message at a constant rate. However, issues related to signaling overhead and synchronization would increase with the reduction in the interval of router advertisement. The MN experiences a significant delay in tunneling of data packets and suffers from the disconnection making it inefficient for the real-time applications. It can be inferred that most of the methods use passive load sharing mechanism in which load distribution takes place only after the HA registration process. There are few methods like MHADS which performs active load sharing but the process used is implicitly centralized in nature. The extensive use of *"heart beat messages"* in the case of failure detection and recovery in most of the existing methods, limits the performance by increasing the signaling overhead. Future work can be extended in the domain of distributed active load sharing mechanism. The proactive failure detection and recovery while maintaining less signaling overhead can be directed for further research.

REFERENCES

[1] Terli, Venkata Krishna Kishore, et al. "Software implementation of IPv4 to IPv6 migration," Long Island Systems, Applications and Technology Conference (LISAT), 2016 IEEE. IEEE, 2016.

[2] C. Perkins, "IP Mobility Support", IETF-RFC (Proposed Standard) 3344, August 2002.

[3] Johnson, David, Charles Perkins, and Jari Arkko. "Mobility support in IPv6." No. RFC 3775. 2004.

[4] Perkins, Charles, David Johnson, and Jari Arkko. "Mobility support in IPv6." No. RFC 6275. 2011.

[5] Yen, Yun-Sheng, Chia-Chang Hsu, and Han-Chieh Chao. "Distributed balancing with application-layer anycast for home agent discovery on the mobile IPv6." 2005 International Conference on Wireless Networks, Communications and Mobile Computing. Vol. 2. IEEE, 2005.

[6] Mathi, Senthil Kumar, and M. L. Valarmathi. "A Secure and Efficient Binding Update Scheme with Decentralized Design for Next Generation IP Mobility." Artificial Intelligence and Evolutionary Algorithms in Engineering Systems. Springer India, 2015. 423-431.

[7] Zhang, Hanwen, et al. "A multiple home agent deployment scheme to enhance service availability for MIPv6." Communication Systems, 2008. ICCS 2008. 11th IEEE Singapore International Conference on. IEEE, 2008.

[8] Mathi, Senthil Kumar, M. L. Valarmathi, and G. Ramprasath. "A secure and efficient registration for IP Mobility." Proceedings of the First International Conference on Security of Internet of Things. ACM, 2012.

[9] Vasilache, Adrian, Jie Li, and Hisao Kameda. "Load balancing policies for multiple home agents mobile IP networks.' Web Information Systems Engineering, 2001. Proceedings of the Second International Conference on. Vol. 2. IEEE, 2001.

[10] Khan, Shoaib, et al. "Home agent load balancing in mobile ipv6 with efficient home agent failure detection and recovery." 2006 International Conference on Emerging Technologies. IEEE, 2006.

[11] Deng, Hui, et al. "A hybrid load balance mechanism for distributed home agents in mobile IPv6." Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003. 14th IEEE Proceedings on. Vol. 3. IEEE, 2003.

[12] Wakikawa, R., Devarapalli, V. and P.Thubert, "Inter Home Agents Protocol (HAHA)," IETF Draft, draft-wakikawamip6-nemo-haha-00.txt (work in progress), October 2003.

[13] Lee, Jong-Hyouk, and Tai-Myoung Chung. "Performance evaluation of distributed multiple home agents with HAHA protocol." International Journal of Network Management 17.2 (2007): 107-116.

[14] F. Heissenhuber, W. Fritsche, and A. Riedl, "HA Redundancy and Load Balancing in Mobile IPv6," in Proc. 5th International Conf. Broadband Communications, HongKong, 1999

[15] Heissenhuber, Florian, Wolfgang Fritsche, and Anton Riedl. "Home agent redundancy and load balancing in Mobile IPv6." Broadband communications. Springer US, 2000.

[16] Deng, H., Zhang, R., Huang, X. and K. Zhang, "Load Balance for Distributed HAs in Mobile IPv6", IETF Draft, draft-deng-mip6-ha-loadbalance-00.txt (work in progress), November 2003.

[17] Faizan, Jahanzeb, Hesham El-Rewini, and Mohamed Khalil. "VHARP: Virtual home agent reliability protocol for mobile IPv6 based networks." 2005 International Conference on Wireless Networks, Communications and Mobile Computing. Vol. 2. IEEE, 2005.

[18] Faizan, Jahanzeb, Hesham El-Rewini, and Mohamed Khalil. "Efficient dynamic load balancing for multiple home agents in mobile IPv6 based networks." ICPS'05. Proceedings. International Conference on Pervasive Services, 2005. IEEE, 2005.

[19] Faizan, Jahanzeb, Hesham El-Rewini, and Mohamed Khalil. "Introducing reliability and load balancing in home link of Mobile IPv6 based networks." 2006 ACS/IEEE International Conference on Pervasive Services. IEEE, 2006.

[20] Cabellos-Aparicio, Albert, and Jordi Domingo Pascual. "Load Balancing in Mobile IPv6's Correspondent Networks with Mobility Agents." 2007 IEEE International Conference on Communications. IEEE, 2007.

[21] C.K.Shyamala and R.R.Sharanya; A dual quorum-reed solomon coded protocol handling hybrid failures in distributed storage, International Journal of Control Theory and Applications, Vol. 9 , No.10, pp. 4257-4267, September 2016.

[22] Chen, Yeong-Sheng, Chien-Hsun Chen, and Hua-Yin Fang. "An efficient quorum-based fault-tolerant approach for mobility agents in wireless mobile networks." Sensor Networks, Ubiquitous and Trustworthy Computing, 2008. SUTC'08. IEEE International Conference on. IEEE, 2008.

[23] Rathi, S., and K. Thanushkodi. "Design and Performance Evaluation of an Efficient Home Agent Reliability Protocol." (2009).

[24] Abdelgadir, Abdelgadir Tageldin, et al. "Performance analysis of a highly available home agent in mobile networks." Proceedings of the 14th Communications and Networking Symposium. Society for Computer Simulation International, 2011.

[25] Dayaratna, H. R. O. E., Kunitake Kaneko, and Fumio Teraoka. "Multiple home agent placement considerations based on internet service provider perspective in MobileIPv6." Computer Software and Applications Conference (COMPSAC), 2013 IEEE 37th Annual. IEEE, 2013.

[26] Wakikawa, Ryuji, Guillaume Valadon, and Jun Murai. "Migrating home agents towards internet-scale mobility deployments." Proceedings of the 2006 ACM CoNEXT conference. ACM, 2006.

[27] Diana, A. Avelin, K. Sundarakantham, and S. Mercy Shalinie. "Alleviation of Binding Update Re-registration Handoff Latency at Home Agent Failure in MIPv6 Network." International Journal of Computers Communications & Control 10.4 (2015): 463-470.

[28] Alsukayti, Ibrahim S., and Christopher Edwards. "Multihomed mobile network architecture." IFIP Networking Conference (IFIP Networking), 2015. IEEE, 2015.

[29] McCarthy, Ben, Christopher Edwards, and Martin Dunmore. "Advances in MANEMO: Definition of the Problem Domain and the Design of a NEMO-Centric Approach." Applications and the Internet Workshops, 2007. SAINT Workshops 2007. International Symposium on. IEEE, 2007.

[30] Baek, Jinsuk, et al. "On a moving direction pattern based MAP selection model for HMIPv6 networks." Computer Communications 34.2 (2011): 150-158.

[31] Kusin, Zulkeflee, and Mohamad Shanudin Zakaria. "Dynamic load control mechanism in hierarchical MIPv6." Electrical Engineering

and Informatics (ICEEI), 2011 International Conference on. IEEE, 2011.
[32] Anbarasi, P. N., and Senthilkumar Mathi. "A Tokenized Binding Update Scheme for Next Generation Proxy IP Mobility." Artificial Intelligence and Evolutionary Computations in Engineering Systems. Springer India, 2016. 193-207.
[33] Raza, Syed M., et al. "Dynamic Load Balancing of Local Mobility Anchors in Software Defined Networking based Proxy Mobile IPv6." Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication. ACM, 2016.
[34] Nguyen, Tien-Thinh, and Christian Bonnet. "Considerations of IP multicast for load balancing in Proxy Mobile IPv6 networks." Computer Networks 72 (2014): 113-126.
[35] Jeon, Seil, Rui L. Aguiar, and Namhi Kang. "Load-Balancing Proxy Mobile IPv6 Networks with Mobility Session Redirection." IEEE Communications Letters 17.4 (2013): 808-811.
[36] Mathi, Senthilkumar, and P. N. Anbarasi. "A Secure and Efficient Location Update Scheme for Next Generation Proxy Mobile IP in Distributed Environment." Procedia Computer Science 57 (2015): 942-951.
[37] Ernest, Petro P., Olabisi E. Falowo, and H. Anthony Chan. "Network-based distributed mobility management: Design and analysis." 2013 IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob). IEEE, 2013.
[38] Qutub, Syed, and Tricha Anjali. "Load sharing mechanism for Mobile Access Gateways in PMIPv6." Electro/Information Technology (EIT), 2012 IEEE International Conference on. IEEE, 2012.
[39] Mitra, Sulata, and Sumanta Pyne. "Distributed Route Selection Algorithm in Nested Multihomed Mobile Networks." Advances in Computing, Control, & Telecommunication Technologies, 2009. ACT'09. International Conference on. IEEE, 2009.
[40] Zhang, Yujun, and Hanwen Zhang. "A Mobile Agent Fault-Tolerant Method Based on the Ring Detection & Backup Chain for Mobile IPv6 Networks." Communications (ICC), 2011 IEEE International Conference on. IEEE, 2011.
[41] Nguyen, Tien-Thinh, and Christian Bonnet. "Considerations of IP multicast for load balancing in Proxy Mobile IPv6 networks." Computer Networks 72 (2014): 113-126
[42] Aman, Azana Hafizah Mohd, et al. "Parametric Comparison of Multicast Support for Network Mobility Management: A Qualitative Analysis." International Journal of Multimedia and Ubiquitous Engineering 11.9 (2016): 203-210.
[43] Mathi, Senthilkumar, M. Lavanya, and R. Priyanka. "Integrating dynamic architecture with distributed mobility management to optimize route in next generation internet protocol mobility." Indian Journal of Science and Technology 8.10 (2015): 963.
[44] Tran, Phuoc Nguyen, and Nadia Boukha Tem. "Extension of multiple care-of-address registration to support host multihoming." Information Networking, 2008. ICOIN 2008. International Conference on. IEEE, 2008.
[45] Kawano, Keita, Kazuhiko Kinoshita, and Koso Murakami. "Multilevel hierarchical mobility management scheme in complicated structured networks." Local Computer Networks, 2004. 29th Annual IEEE International Conference on. IEEE, 2004.
[46] Zhang, Yu-Jun, et al. "Mobile agent fault-tolerant method based on ring detection & backup chain." Journal on Communications 9 (2011): 004.
[47] Jeon, Seil, Rui L. Aguiar, and Namhi Kang. "Load-Balancing Proxy Mobile IPv6 Networks with Mobility Session Redirection." IEEE Communications Letters 17.4 (2013): 808-811.
[48] Nguyen, Tien-Thinh, and Christian Bonnet. "Load balancing mechanism for proxy mobile IPv6 networks: An IP multicast perspective." Computing, Networking and Communications (ICNC), 2014 International Conference on. IEEE, 2014.
[49] Barkoosaraei, Ana Mirsayar, A. Hamid Aghvami, and Paul Pangalos. "Adaptive quality of service aware multi-mobility anchor point registration in hierarchical mobile IPv6 wireless access networks." IET Networks 3.3 (2014): 176-186.
[50] Kalyanaraman, Madhavan, Swaminathan Seetharaman, and S. Srikanth. "Integrated approach for proxy-mobile-IPv6 (PMIPv6) based IP Flow Mobility and offloading." Communications (NCC), 2015 Twenty First National Conference on. IEEE, 2015.
[51] Alawi, M. A., Alsaqour, R. A., Sundararajan, E., & Ismail, M "Prediction Model for Offloading in Vehicular Wi-Fi Network." International Journal on Advanced Science, Engineering and Information Technology 6.6 (2016): 944-951.
[52] Kalyanaraman, Madhavan, Swaminathan Seetharaman, and S. Srikanth. "Dynamic and integrated approach for proxy-Mobile-IPv6 (PMIPv6) based IP Flow Mobility and offloading." Computing and Communications Technologies (ICCCT), 2015 International Conference on. IEEE, 2015.
[53] Meneguette, Rodolfo I., et al. "A flow mobility management architecture based on proxy mobile IPv6 for vehicular networks." Computers and Communication (ISCC), 2016 IEEE Symposium on. IEEE, 2016.
[54] Kong, Hyunjin, et al. "Load balancing of local mobility anchors in proxy mobile IPv6 networks." Proceedings of the Second Asia-Pacific Symposium on Internetware. ACM, 2010.
[55] Viswanathan, Murlikrishna, et al. "A novel local mobility anchor selection scheme for proxy mobile IPv6 networks." Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication. ACM, 2012.
[56] Raza, Syed M., et al. "Dynamic Load Balancing of Local Mobility Anchors in Software Defined Networking based Proxy Mobile IPv6." Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication. ACM, 2016.
[57] Nguyen, Tien-Thinh, and Christian Bonnet. "Considerations of IP multicast for load balancing in Proxy Mobile IPv6 networks." Computer Networks 72 (2014): 113-126.
[58] ZHAO, Lei, et al. "A routing selection algorithm based on a multi-attribute decisionfor the IPv6 mobile network." Journal of Harbin Engineering University 7 (2014): 014.
[59] Alsukayti, Ibrahim S., and Christopher Edwards. "Efficient mobility and multihoming support for mountain rescue." IFIP Wireless and Mobile Networking Conference (WMNC), 2015 8th. IEEE, 2015.
[60] Erunika, Oshani, Kunitake Kaneko, and Fumio Teraoka. "Impact of multiple home agents placement in mobile IPv6 environment." IEICE Transactions on Communications 97.5 (2014): 967-980.
[61] Seo, Jae Kwon, and Kyung Geun Lee. "Hierarchical mobility management for fast handoff and load distribution in IPv6 networks." Wireless Communications and Mobile Computing 8.10 (2008): 1345-1353.
[62] Goswami, Subhrananda, and Chandan Bikash Das. "A Survey on Various Route Optimization Techniques in Network Mobility." Journal of Uncertain Systems 10.2 (2016): 91-107.
[63] Vasilache, Adrian, Jie Li, and Hisao Kameda. "Threshold-based load balancing for multiple home agents in mobile IP networks." Telecommunication Systems 22.1-4 (2003): 11-31.
[64] Kong, Ruoshan, Jing Feng, and Huaibei Zhou. "The Combination of Multiple Care-Of Addresses Registration and Reverse Routing Header in Nested Network Mobility." Internet Technology and Applications (iTAP), 2011 International Conference on. IEEE, 2011.
[65] Ng, C., et al. Analysis of multihoming in network mobility support. No. RFC 4980. 2007.
[66] Thubert, P. "MIP6/NEMO Working Group V. Devarapalli Internet-Draft Nokia Expires: September 6, 2006 R. Wakikawa WIDE." (2006).
[67] Devarapalli, Vijay, et al. Network mobility (NEMO) basic support protocol. No. RFC 3963. 2004.
[68] Khalil, Mohamed, et al. "Virtual distributed home agent protocol." U.S. Patent No. 6,430,698. 6 Aug. 2002.
[69] Abidin, H. Z., Din, N. M., Radzi, N. A. M., & Rizman, Z. I. "A Review on Sensor Node Placement Techniques in Wireless Sensor Networks." International Journal on Advanced Science, Engineering and Information Technology 7.1 (2017): 190-197.
[70] Busaranun, Adisak, Panita Pongpaibool, and Pichaya Supanakoon. "Simple Implement of Home Agent Reliability for Mobile IPv6 Network." TENCON 2006-2006 IEEE Region 10 Conference. 2006.
[71] Lin, Jenn-Wei, and Ming-Feng Yang. "Fault-tolerant design for wide-area Mobile IPv6 networks." Journal of Systems and Software 82.9 (2009): 1434-1446.
[72] Rathi, S., and K. Thanuskodi. "A Secure and Fault tolerant framework for Mobile IPv6 based networks." arXiv preprint arXiv:0909.4858 (2009).