ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 8(10), 963-974, May 2015* DOI: 10.17485/ijst/2015/v8i10/58213

Integrating Dynamic Architecture with Distributed Mobility Management to Optimize Route in Next Generation Internet Protocol Mobility

Senthilkumar Mathi*, M. Lavanya and R. Priyanka

Amrita School of Engineering, Amrita Vishwa Vidyapeetham (University), Coimbatore, Tamilnadu, India;
msenthil_cse@yahoo.co.in, mlavanya005@gmail.com, rpriyanka.2312@gmail.com

Abstract

Increasing population of mobile users has lead to the demand of higher mobility support. Many protocols have been standardized for mobility management such as Mobile Internet Protocol version 6, hierarchical mobile IPv6 and proxy mobile IPv6 and so on. The predominantly used approach in the existing mobile networks is the centralized mobility management. In this, the messages transferred between mobile node and correspondent node must pass through each level due to the hierarchical architecture. When a mobile network is implemented with the centralized architecture, the messages are routed to the MN irrespective of its location using mobile IP for continuing services during the handover. But this approach is susceptible to issues such as single point of failure, non-optimized routes, latency issues, wastage of resources and security threats which affect the performance and scalability, demanding a flatter architecture with an efficient mechanism to face the traffic overload from the mobile users. Hence, the paper proposes a new scheme to form a flatter architecture by distributing the mobility management functionalities as distributed access point at the access level. The resistance against security threat such as man-in-the-middle attack, replay attack and false binding update attack has been achieved. Finally, numerical results show that the proposed scheme provides significant reduction in signaling cost and improves efficiency in route optimization.

Keywords: Binding Acknowledgement, Binding Cache, Binding Update, Distributed Access Point, Distributed Mobility Management

1. Introduction

The congregation of the mobile devices with the Internet usage is enlarged at a rapid rate increasing the demand to the service providers to supply advanced network functionalities. The available mobility protocols are not sufficient to meet the challenges of advancements in the mobile internet. The extensions have been made to the base protocols but it faces deployment issues[1,11]. In order to ease the deployment, further approaches have been proposed. The Distributed Mobility Management (DMM) allows the distribution of the mobility functions which provides flattened network architecture[3]. It incorporates additional extensions required to yield efficiency and provide better performance.

Currently the flat architecture is the obligatory development of mobile Internet for reducing the cost and improving performance. At the same time mobile usage traffic capacity is mounting greater than the revenue. Offloading the traffic selectively poses to be an issue to the service providers which in turn is solved by the dynamic mobility management. The main idea of Dynamic mobility management is to distribute the mobility functions with dynamic user traffic anchoring in access level[2,4].

*Author for correspondence

In the existing mobility protocols, the MIPv6 allows the Mobile Node (MN) to be reachable and maintains ongoing connections while moving in the topology. It uses the redirection function in which the HA redirects packets addressed to an MN's home address to its current location after MN notifies their current location to HA[13]. Mobile IPv6 allows an MN to communicate with another node through the optimized path by using IP routing.

Mobility management functionalities are distributed at different locations in a network so that the MN can communicate with CN using the nearest access point in the network. The functionalities of the entities in the network can be copied to multiple locations as Mobility Anchor Point (MAP) so the packet can be sent to the CN through the nearest MAP in the network and avoid the security threats[14]. The pictorial view of the DMM environment is shown in Figure 1.

level provides a simple flat architecture. The proposed architecture avoids the different levels in the DMM and allows the traffic to provide optimal mobility support to the MN.

The rest of the paper is organized as follows. Section 2 describes about the previous works carried out in the DMM domain. Section 3 discusses the proposed architecture with the scheme. The security analysis is discussed in Section 4. Section 5 emphasizes on performance evaluation. Section 6 concludes the paper.

2. Related Works

Chan et al. investigates various possible approaches to implement DMM by topologically distributing the mobility anchors in different levels like distribution in mobile core network, access network and distribution in host. It

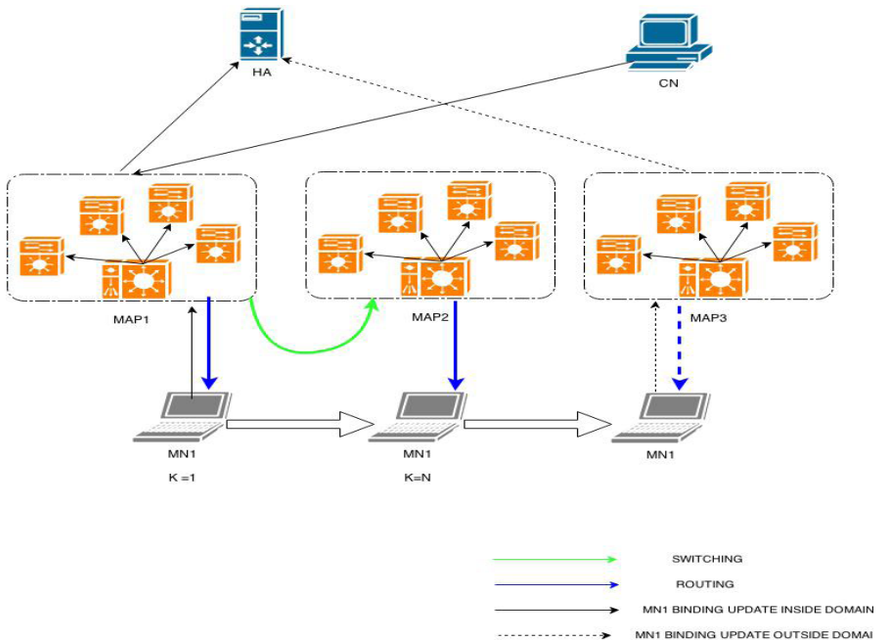

Figure 1. Generalized distributed architecture of IPv6 mobility.

Even though the distribution is done in different levels, it forms a centralized and hierarchical architecture. Thus it demands a flattened architecture in which the mobility functionalities are distributed and they can be used from the nearest access point[5].

Hence, this paper proposes a mechanism to combine DMM with dynamic user's traffic anchoring in access also emphasizes on the needs and the issues faced in integrating the dynamic mechanism with DMM architecture.

In the DMM environment, the MAPs are distributed at different levels in a tree structure[2]. The MAPs at the higher level of the hierarchy is the Root MAP (RMAP) and the MAPs at lowest level of hierarchy are the Leaf MAPs (LMAP). When MN switches from one network to

the other, it updates its LCOA to the LMAP. The LMAP in turn checks for MN's entry in binding list and the packet gets transferred to the higher level MAP. This procedure has to be executed every time when a packet passes through each level since it is carried by all level's MAPs. But this approach results in higher costs since the packet has to go through more intermediate MAPs. If one node fails it affects the entire tree structure. The overall structure of the system is shown in Figure 2.

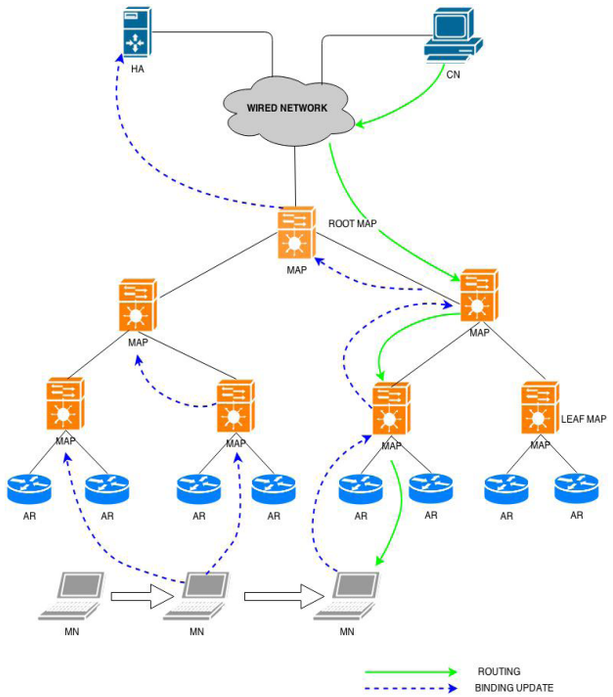

Figure 2. Message flow in HMIPv6.

To overcome this issue, a method has been formulated in4 that have two levels of MAP dynamically where each acts as both the root MAP and leaf MAP. Depending on the user mobility, the types of MAP changes dynamically which reduces the bottleneck of the traffic load at the MAP. Thus, the functionalities are evenly distributed that enhances the efficiency of the scheme. Due to the dynamicity of the system, the MN has no boundary limitations within the network.

Though this scheme creates levels dynamically among the MAPs, the levels may be prone to the single point of failure attack. The packets that are routed from the MN to the CN must pass through the logical levels of the network architecture. But it also faces the issue of centralized architecture at some level[5].

3. Proposed Scheme

The proposed system introduces a new scheme in which all the mobility functionalities and the HA functionalities are integrated as a single unit as Distributed Access Point (DAP) in the access level itself. By this, the route is optimized since the number of levels is reduced and the DAP is distributed. The proposed architecture is shown in Figure 3.

In the proposed system, whenever the MN enters into a network it communicates with the CN through the DAP1. When the MN moves from one network to

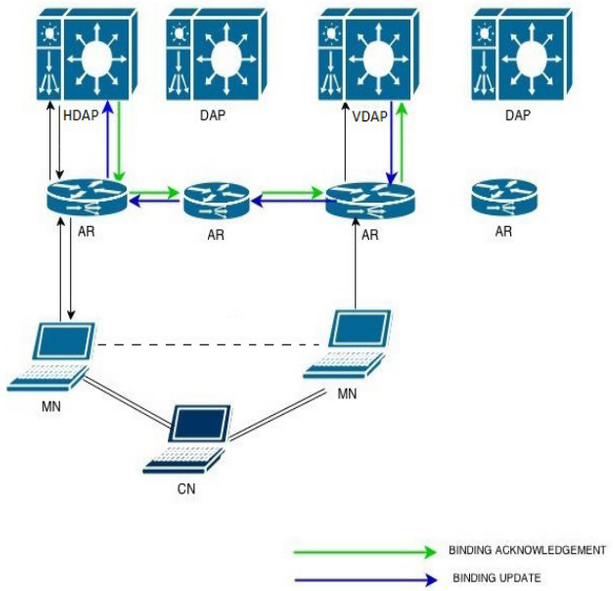

Figure 3. Message flow of the proposed architecture.

the other network, the AR sends Router Advertisement (RA) message to all the DAP in the network. When any of the DAP, say DAP2 accepts the RA message, it forwards the RA message to the DAP1 notifying it that the MN is now connected to the DAP2. The DAP1 notifies the CN that the connection between the MN and DAP1 is ended. MN sends a BU to the DAP2. It accepts the BU and stores the message in the BC returns BA message to the MN. This process registers MN in the new network. Subsequently, MN sends a connection request to CN. The bidirectional tunnel is established between MN and CN and the communication starts. But when a large number of MN switches from one network to the other constantly, handling the BU poses an issue and the BC overflows. To

solve this issue, an alternate dynamic buffer is added to the DAP so whenever the BC overflows the BU with LLT is chosen and inserted into the dynamic buffer to store it temporarily[6]. Once when the BC entry is free and the LT of the BU is not expired, the BU is again send back to the BC for further processing. This mechanism solves the signaling overhead issue in distributed environment.

3.1 Scheme Description

The notations that are used in the proposed scheme are mentioned in Table 1. The nonce values and the public keys are pre-shared values during the initial registration without any trusted third party.

- **Initial Registration of MN**

When the MN enters into a network, it connects with the nearest DAP and becomes its HDAP. It sends the IPv6 subnet prefix of that network to MN. The process is shown in Figure 4. MN receives the message from HDAP and it authenticates using $Nonce_{HDAP}$. Thus, when HDAP communicates with MN, it should send the new nonce value to avoid security attacks. Then the bidirectional connection is established between MN and CN and the packet transfer starts.

Step1. HDAP → MN: $IDPrefix_{MN}$, $Nonce_{HDAP}$

- **MN Registration in Different Network**

Step2. DAP → AR: RA_{DAP}

Table 1. Notations used in the proposed scheme

Notations	Description
HDAP, VDAP	DAPs in home and visitor network respectively.
$IDPrefix_{MN}$	Address prefix of MN
RA_{DAP}	Router advertisement to DAP
KU-MN	Public key of MN
E_{KU-MN}	Encryption using public key of MN
CT_{MN}	Cipher Text of MN
LT	Lifetime
$Nonce_{MN}$, $Nonce_{CN}$, $Nonce_{HDAP}$	Nonce of MN, CN and HDAP respectively
$Nonce'_{MN}$, $Nonce'_{HDAP}$	New Nonce of MN, CN and HDAP respectively

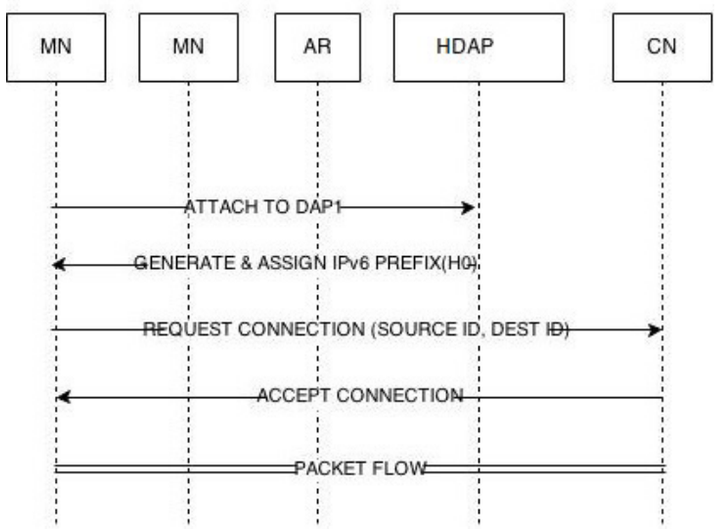

Figure 4. Initial registration of MN in the home network.

where RA_{DAP} = $IDPrefix_{MN}$, $Nonce_{MN}$, LT.

When MN moves from one network to the other, it has to register in the new network. All the DAPs in the network send Router Advertisement (RA) message to the AR periodically. Upon receiving RA message from the DAPs, the AR accepts any one of them and forwards it to MN. The overall process of MN in different network is shown in Figure 5.

Step3. MN→HDAP: CT_{MN}, Hash[CT_{MN}]

where CT_{MN} = $E_{KU\text{-}MN}$ [BU, $IDPrefix_{MN}$, $Nonce_{MN}$]

BU= $IDPrefix_{MN}$, ID_{VDAP}, LT.

When RA is received from AR, MN sends a BU and it is encrypted using public key of MN ($E_{KU\text{-}MN}$ [BU, $IDPrefix_{MN}$, $Nonce_{MN}$]). Then the hash function is applied on the encrypted message and sent to HDAP. HDAP receives the message and authenticates MN using the new nonce value. It validates the message with the received

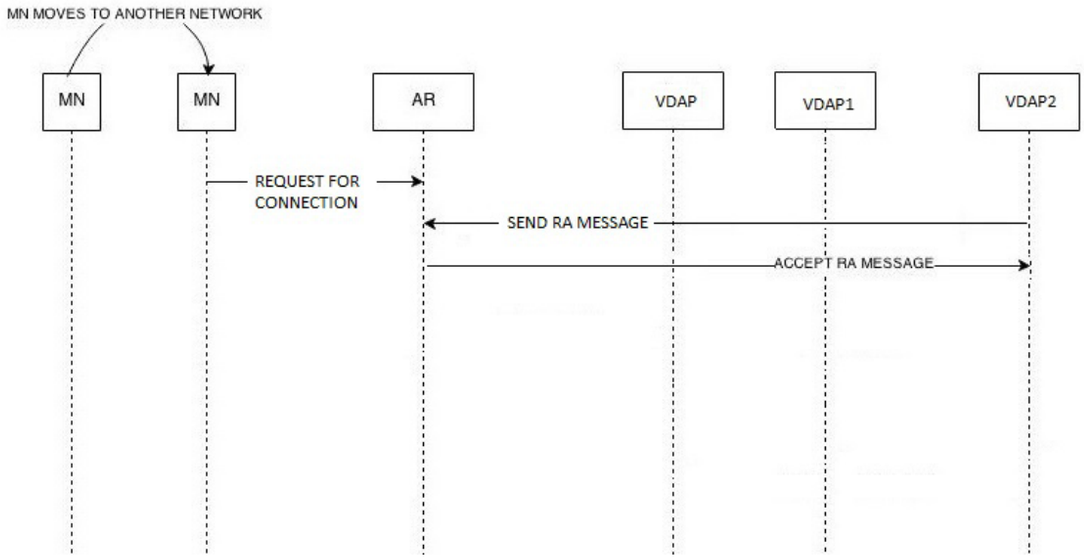

Figure 5. Router advertisement in the visitor network.

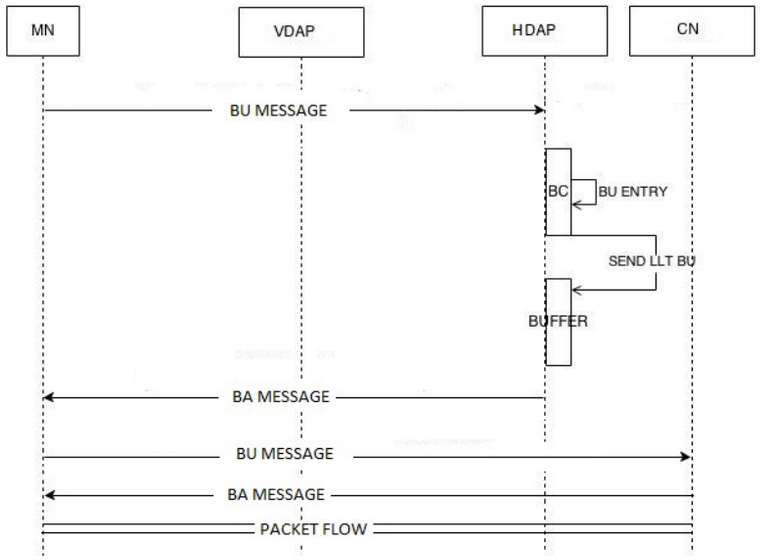

Figure 6. BU transfer from BC to buffer.

Hash value and decrypts it using private key of HDAP. The BU is retrieved from the decrypted message. In order to avoid the intruder attacks, a new nonce $Nonce'_{MN}$ is generated by MN and updates it to HDAP. The working of this module is shown in Figure 6.

- **Message Transfer from Bc to Buffer**

Step4. HDAP: Upon receipt of BU from MN

HDAP enters BU to the BC and it stores the message. When many MN send BUs at the same time, BC overflows and discards the messages that incur the loss of packets. MN has to resend a new BU message to HDAP which causes extra signaling cost. Thus an alternate dynamic buffer is embedded into the DAPs in the network. It sends the BU with LLT to the alternate dynamic buffer present in the DAP and store them temporarily till BC has space for new entry. The insertion process is depicted in Figure 7. The procedure for transferring the BU from binding cache to dynamic buffer at DAP[6] is shown in Figure 8.

- **Binding Acknowledgement**

Step5. HDAP→MN: BA, $Nonce'_{MN}$

where BA= $IDPrefix_{MN}$, ID_{VDAP}, LT

when HDAP validates BU it accepts the message and updates the location of the MN. Then it sends BA message to MN. Upon receiving the message from HDAP, MN authenticates HDAP using the new nonce value $Nonce'_{MN}$.

- **Location Update between MN and CN**

Step6. MN→ CN: CT_{MN}, Hash[CT_{MN}]

where $CT_{MN} = E_{KU\text{-}MN}$ [BU, $IDPrefix_{MN}$, $Nonce'_{MN}$]

Step7. CN→MN: BA

The MN and CN authenticate each other using the ID and the nonces. The location update of MN is sent to CN through which the MN and CN can communicate directly.

4. Security Analysis

In this section, the analysis of security attributes such as confidentiality, integrity and authentication are discussed and the attack prevention of the existing and the proposed schemes are also addressed

4.1 Confidentiality

The messages transferred over a communication link needs to be secured from gaining unauthorized access of the unknown entity[9]. Confidentiality ensures the privacy of the messages from the interception by the attackers. When the MN sends the BU to HDAP in step 3 of the proposed scheme, it is enciphered ($E_{KU\text{-}MN}$[BU, $IDPrefix_{MN}$, $Nonce_{MN}$, $Nonce_{HDAP}$]) using the public key of the MN (KU-MN) and HDAP decrypts the message using private key of HDAP. Thus, the intruder cannot obtain the content when the message is intercepted because the message can be opened only by the private key of HDAP which ensures confidentiality. The confidentiality of various existing schemes with the proposed scheme is tabulated in Table 2.

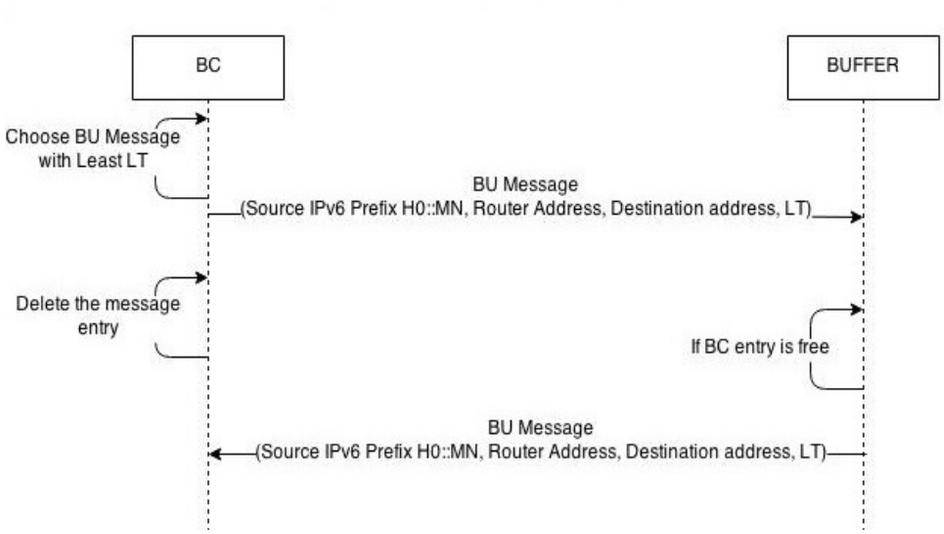

Figure 7. Insertion of BU into the buffer.

```
PROCEDURE: BU MESSAGE TRANSMISSION FROM BC TO BUFFER

Initialize Timer T, Session variable S.
Set Threshold value of T
Input:BU(ID prefix, ID_VDAP, Lifetime)
        if T is less than or  equal to S and LT is not ZERO
        When both the conditions are TRUE ,Execute section 1.
        Step 1: Insertion of BU into BC
                Check for BC entry vacancy to insert BU message
                If BC entry is AVAILABLE ,then
                INSERT BU message into BC.
                else  Execute section 2.
        Step 2 : Transmission of BU from BC to Buffer
                Choose the BU with  Least LT and send to buffer and Execute section 3.
                Delete the entry of the transferred BU message from the BC .
        Step 3:Insertion of BU into Buffer
                Check if Buffer Flag is set ON  to update the BU entry from BC, then
                Pick the BU message from the BC and INSERT into Buffer
                else End the process.
                 if  Next-Entry in Buffer is NULL, then
                Set Buffer Flag as OFF and Timer as 0
        Step 4: Re-transmission of BU from Buffer to BC
                Check for BC entry vacancy to insert BU message
                If BC entry is AVAILABLE ,then
                Choose the BU with  Higher LT and resend to BC
                Delete the entry of the transferred BU message from the buffer.
        else Repeat the process
        End Process
```

Figure 8. Insertion of the binding update into the buffer at DAP.

Table 2. Comparative analysis of confidentiality.

Scheme	Confidentiality		
	MN-CN	MN-MAP/ DAP	MN-HA
Taleb et al. 2005	Yes	Yes	Not supported
Wakikawa et al. 2006	Yes	No	No
Hasan et al. 2012	No	Not supported	No
Chen et al. 2014	No	Yes	No
Proposed	Yes	Yes	Yes

4.2 Integrity

Integrity assures the receiver that any message sent over a communication channel remains unaffected[9]. In the proposed scheme, the integrity of the messages is achieved by using hash function. In step 6, when the cipher text CT_{MN} transferred from MN to CN, the hash function is applied on the message Hash[CT_{MN}]. If the message from the MN is intercepted, the intruder will not be aware of the type of hash function used since it is pre-shared and agreed upon the two communicating parties only. But, if the intruder tries to open the message then the computed hash value on the receiver side alters. Thus, the recalculated hash value becomes different and the modified message can be identified at CN. From Table 3, it shows that the integrity is provided between all the correspondent pairs MN-CN, MN-DAP and MN- HA in the proposed scheme

Table 3. Comparison of integrity

Scheme	Integrity		
	MN-CN	MN-MAP/ DAP	MN- HA
Taleb et al. 2005	No	Yes	Not supported
Wakikawa et al. 2006	Yes	Not supported	Yes
Hasan et al. 2012	No	Not supported	No
Chen et al. 2014	Yes	No	Yes
Proposed	Yes	Yes	Yes

4.3 Authentication

Authentication is the process of claiming an entity's identity and ensuring its validity through any proof such as user credentials. The mutual authentication between the communicants MN, CN, VDAP and HDAP is achieved by using the cryptographic hash function. In step 3, when MN exchanges BU message with HDAP, the type of the hash function used is agreed upon both the communicating parties. Thus, the information is known only to MN and HDAP. The use of same hash function at the sender and receiver should remain the same. Consequently, the proposed scheme authenticates MN and HDAP. The mutual authentication analysis is shown in Table 4.

Table 4. Comparative analysis of mutual authentication

Scheme	Mutual Authentication		
	MN-CN	MN-MAP/ DAP	MN-HA
Taleb et al. 2005	Yes	Yes	Not supported
Wakikawa et al. 2006	No	Not supported	Yes
Hasan et al. 2012	No	Not supported	Not supported
Chen et al. 2014	Yes	No	Yes
Proposed	Yes	Yes	Yes

4.4 Man-in-the-middle Attack Prevention

In the man-in-the-middle (MITM) attack, the attacker seizes the communication link and performs malicious activity in the link. In the steps 3 and 6 as mentioned in section 5, the MITM attack between MN and HDAP is prevented in the proposed scheme by using hash function for the exchange of messages between the communicating parities. If the attacker intercepts and modifies the message transferred, the hash value differs from the received value at HDAP. Thus, the message is discarded and the attack is prevented. The message is also encrypted with the public key of MN (KU-MN) which can be decrypted only by using the private key of HDAP. As a result, it is impossible for the intruder to alter the contents of the message.

4.5 Replay Attack Prevention

Replay attack happens when an unauthorized entity poses as an authorized entity by using any user credentials and gain access over the system for replaying the message. It is avoided in the proposed scheme by attaching nonce to each of the messages between the two nodes such as MN and CN ($Nonce_{CN}$, $Nonce_{MN}$) and HDAP and MN ($Nonce_{MN}$, $Nonce_{HDAP}$). In the step 3 MN renews the nonce value as $Nonce'_{MN}$ and sends it to HDAP which then replaces the older nonce value ($Nonce_{MN}$) with the new nonce value ($Nonce'_{MN}$). When HDAP does further communication with MN, it authenticates HDAP with $Nonce'_{MN}$. If the intruder tries to send a bogus message then it is rejected since the nonce does not match. As a result, the replaying of the message is prevented in the proposed scheme.

4.6 False BU Attack Prevention

The BU messages are vulnerable to the false BU attack in which an attacker resides in the channel between the communicants and changes the content such as ID Prefix of the subnet, LT of the BU message. When the attacker intercept the BU message sent between the MN and CN, it is possible that the intruder can modify the content of BU message and send a false BU message to CN. But in the proposed scheme, it is prevented since the BU message is encrypted using the KU-MN ($E_{KU\text{-}MN}$[BU, $IDPrefix_{MN}$, $Nonce'_{MN}$, $Nonce_{CN}$]) which in turn requires the private key of CN to decrypt the message as mentioned in step 6.

The analysis of attack prevention in existing and proposed scheme is tabulated in Table 5.

Table 5. Attack prevention analysis

Scheme	Prevention against		
	MITM	Replay attack	False BU attack
Taleb et al. 2005	Yes	Yes	No
Wakikawa et al. 2006	No	No	No
Hasan et al. 2012	No	No	No
Chen et al. 2014	Yes	No	No
Proposed	Yes	Yes	Yes

5. Performance Evaluation

In this section, the performance analysis of the proposed scheme with existing schemes is discussed based upon the total signaling cost. When MN moves from one network to other network, the following are taken into consideration for computing signaling cost; binding update, binding refresh and packet delivery. The total signaling cost is denoted as follows,

$$C_T = TC_{BU} + TC_{BR} + TC_{PD} \quad (1)$$

where TC_{BU}, TC_{BR} and TC_{PD} are the total costs for binding update, binding refresh and packet deliver respectively. The notations and the system parameters used for the performance analysis are listed in Table 6 and 7 respectively. Some of the distinctive parameters are set based upon the assumptions found in[8,10].

5.1 Binding Update Cost

The location of MN is updated to DAP and CN each time it moves into a different network and hence it involves the binding update cost for MN. In the analytical model of10 for MIPv6, the location information of MN is achieved by updating the address at HA and CN irrespective of the MN's mobility. In HMIPv6, the MN performs the local and global binding update when it moves within the MAP domain and vice versa respectively. Due to the high mobility nature of MN, it is essential to measure binding update cost which is estimated as per the formulations[7] as follows,

$$C_{BU} = E(N_l)C^l + E(N_d)C^g \quad (2)$$

where $E(N_l)$ and $E(N_d)$ is the ratio of the packet arrival rate to the number of subnets that MN crosses but still remains within the access level for intra domain and inter domain respectively. The eqn. (2) can be rewritten as,

$$TC_{BU} = \frac{1}{\lambda_s}(\mu_l C^l + \mu_d C^g) \quad (3)$$

Here, μ_l is the difference of the rate at which the packets move within the subnet (μc) and DAP domain μd respectively.

In the proposed scheme, the binding update cost is estimated based on the processing cost at DAP, since all the mobility functions including the functionalities of HA is integrated within the DAP. Initially, the MN sends solicitation among the DAPs in the network through AR .Thus, the processing cost of AR for initial registration is PC_{AR} . The HDAP generates a subnet prefix and forwards it to MN. Upon receiving the prefix, the MN sends the

Table 6. Notations used in the performance analysis

N_c	number of subnets crossing during intra-AN/MAP handoffs
N_d	number of AN/MAP domain crossing during inter-AN/MAP handoffs
C^g	global binding update cost to HA/CNs
C^l	local binding update cost to MAP
N_{CN}	number of CNs having a binding cache entry for an MN
$D_{x,y}$	average number of hops between nodes *X* and *Y*
$C_{x,y}$	transmission cost of control packets between nodes *X* and *Y*
PC_x	processing cost of control packet at node *X*
T_D	binding update lifetime of MN at DAP

BU message to the HDAP. The HDAP creates an entry for BU message into the alternate dynamic buffer with the processing cost (PC_{HDAP}).

$$C^{l}_{Proposed-BU} = 2\left(C_{MN,AR} + PC_{AR}\right) + PC_{HDAP} + PC_{VDAP} + C_{AR,HDAP} + C_{HDAP,VDAP} \quad (4)$$

The transmission cost of packets transferred between two nodes is termed as, $C_{X,Y} = \tau d_{X,Y}$ where is the distance between nodes X and Y. τ is the unit transmission cost over wired link. The transmission cost between MN and AR is $C_{MN,AR} = \tau\rho$ where ρ is the weighing factor of the wireless link.

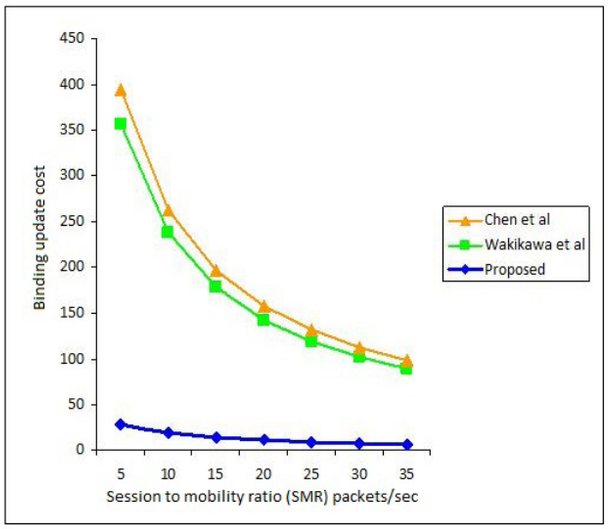

Figure 9. Effect of SMR on binding update cost.

Figure 9 depicts the efficiency in terms of Session to Mobility Ratio (SMR) with the binding update cost. In the proposed scheme, there is no transmission cost at HA and thus the processing and the transmission cost of the DAP is considered which is relatively lower than the cost at HA. Comparing the cost variation of analytical models in10, MIPv6 has lower binding update cost as it does not follow any hierarchies.

5.2 Binding Refresh Cost

The binding refresh cost is added up when the lifetime of the binding update gets expired and the lifetime is refreshed. Each time when BU message is transferred from BC to buffer, the process of updating the lifetime of BU consumes certain amount of cost in terms of time. The binding refresh cost in the proposed scheme is formulated as

$$TC^{BR}_{Proposed} = 2\left(\left[\frac{1}{\mu_d T_D}\right] C_{MN,DAP}\right) + 2\left(\left[\frac{1}{\mu_d T_C}\right] N_{CN} C_{MN,CN}\right) \quad (5)$$

As per equation (5), TD and TC which denotes the lifetime of the binding update of MN at DAP and CN respectively. $C_{MN,DAP}$ is the BU message lifetime refresh cost at the DAP. The average rate of sending BU message from BC to buffer is the inversely proportional to the product of μd and T_D. Hence, the transmission cost $C_{MN,CN}$ is proportional to the number of CNs N_{CN} to which the MN is connected.

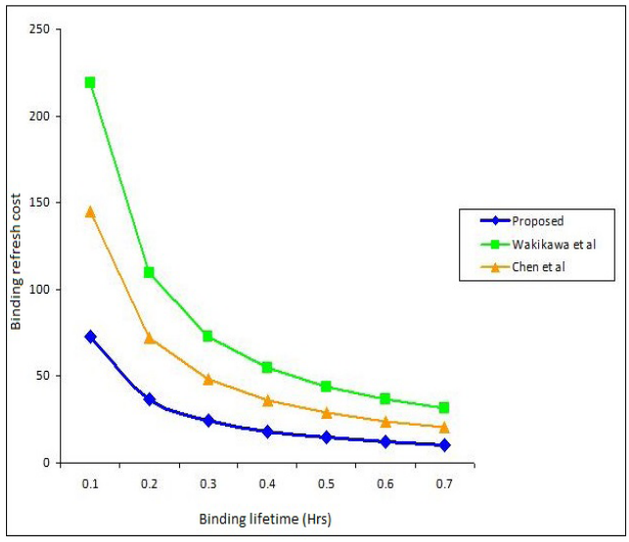

Figure 10. Binding refresh cost vs binding lifetime.

The variation of the binding refresh cost depends on the binding lifetime parameters namely T_D and T_C whose values range from 0.4 to 0.7 hours. The cost remains stable between the series because the time is optimized to execute the refresh process when the lifetime expires. If the binding lifetime deviates from the range, it leads to frequent or infrequent refresh of the BU message which results in increase of cost[10]. From the Figure 10. the proposed system shows consistent outcome in terms of binding refresh cost when compared to the existing works.

5.3 Packet Delivery

Once when the binding of MN is done, the packets are delivered to the destination through the IP channel which includes transmission cost for the delivery of packets when it is moved from one location to another. The total delivery cost is represented as,

$$C_{PD} = \alpha C_{tun} + \beta C_{loss} \quad (6)$$

where α and β are the weighing factors and $\alpha + \beta = 1$. C_{tun} and C_{loss} are the costs of a successful and failed connection respectively. The value of the successful tunneling cost becomes zero ($C_{tun} = 0$) since the forwarding of packets during handover in MIPv6 and HMIPv6 occurs. Upon the failure of the connection, the scheme incurs a packet loss. Hence, the packet loss for the proposed scheme can be written as,

$$C_{loss} = \lambda_p C^f (T_{LS} + T_{IP} + T_{LU}) \quad (7)$$

where λ_p is the rate at which the packets arrive at a node and C^f is the transmission cost for transferring data packets from MN to AR in the previous network and from that AR to CN. The link switching delay (T_{LS}) is the time taken for MN to move from one link to the other[15]. When the link switching is finished, the IP connectivity takes place and TIP is the duration rate of sending the IP packets. The location update delay (T_{LU}) is the time to forward the packets to the MN's new IP address.

The delivery of packets in the proposed model need not pass through the levels as in HMIPv6 or MIPv6. As a result, the delay components as in the equation (7), T_{LS}, T_{IP} and T_{LU} are low when compared to the existing models. Figure 11 illustrates that the packet delivery cost of the existing and the proposed schemes, which increases proportionally with packet arrival rate and there is a delay in the delivery of packets before MN receives directly through previous AR. The packet delivery cost in the proposed model sustains during the IP forwarding session.

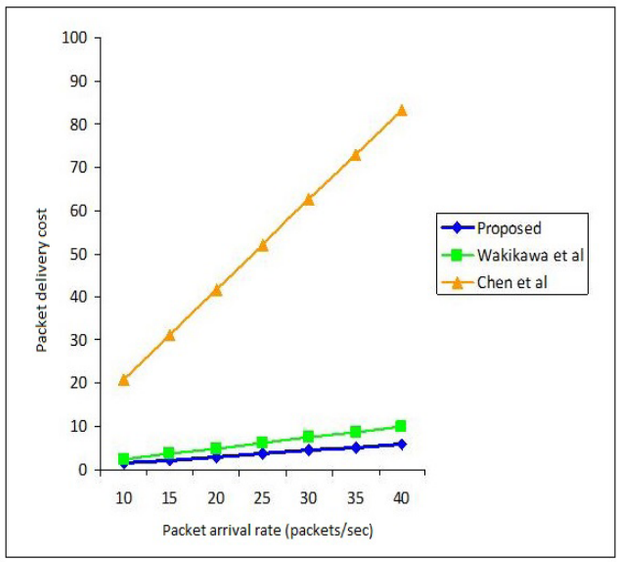

Figure 11. Packet delivery cost on varying packet arrival rate.

From Figure 12, the proposed scheme shows a significant reduction in the total signaling cost compared to the existing schemes. The MIPv6 involves more BU cost since the transmission cost of the HA is higher than HMIPv6. The proposed scheme shows lower BU cost but the packet delivery cost and the binding refresh cost shows marginal variation when compared to MIPv6 and HMIPv6. The efficiency of the system gets deteriorated mainly due to more signaling consumption for BU. Thus in the proposed scheme, this issue is resolved by reducing BU update cost which improves the overall performance. The comparative investigation on cost assessment of the existing and the proposed model depicts that the proposed scheme enhances the optimization of the total signaling cost as shown in Figure 12.

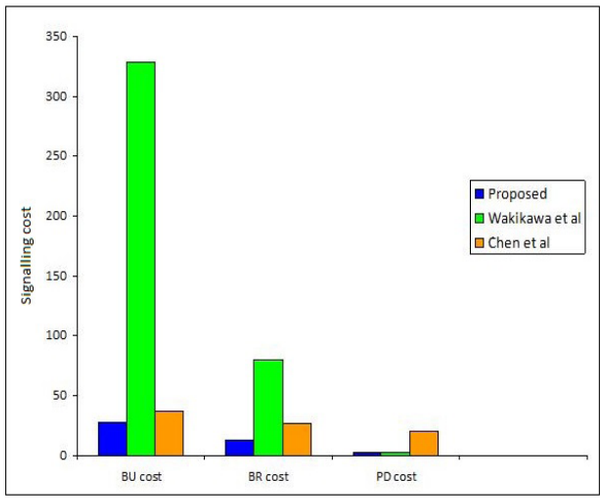

Figure 12. Comparison of total signaling cost on different parameters.

6. Conclusion

The expansion of high end mobile users requires mobility support which is efficient in terms of cost, security and performance. It is achieved in this paper by dynamically switching the mobility functions wherever the MN moves. This paper highlights the reduction of signaling overhead of the system by using alternative dynamic buffer thus optimizing the route, reducing the packet loss

and generating a secured binding update scheme. The numerical results of binding update, binding refresh and the packet delivery costs shows that the signaling cost of the proposed scheme comparatively reduces the total cost. The DMM paradigm proposes to relocate the nodes closer to the users thus flattening the network providing optimized route. The distribution of the functionalities eliminates the levels in the mobile network. In addition, the security threats are handled by the appropriate preventive measures in the proposed scheme.

7. References

1. An X, Pianese F, Widjaja I, Acer GU. DMME: A Distributed LTE Mobility Management Entity. Bell Labs Technical Journal. 2012; 17(2):97–120.
2. Bertin P, Lee JH, Seite P. Distributed Mobility Anchoring; 2013.
3. Chan HA, Yokota H, Xie J, Seite P, Liu D. Distributed and dynamic mobility management in mobile internet: current approaches and issues. J Comm. 2011; 6(1):4–15.
4. Chen J, Xiong Z, Yang P, Zheng Y, Liu C, Li G. A dynamic architecture for mobility management in hierarchical mobile IPv6. J Comput. 2014; 9(5):1168–76.
5. Condeixa T, Sargento S. Centralized, distributed or replicated IP mobility? IEEE Communications Letters. 2014; 18(2):1–4.
6. Hasan SS, Hassan R, Abdalla FE. A new binding cache management policy for NEMO and MIPV6. J Theor Appl Inform Tech. 2012; 36(1):113–7.
7. Hussien LF, Aisha-Hassan AH, Habaebi MH, Khalifa OO, Hameed SA. Development of Analytical Approach to Evaluate (DiffServ-MIPv6) Scheme. Res J Appl Sci Eng Tech. 2014; 7(12):2529–38.
8. Lai WK, Chiu JC. Improving handoff performance in wireless overlay networks by switching between two-layer IPv6 and one-layer IPv6 addressing. IEEE Journal on Selected Areas in Communications. 2005; 23(11):2129–37.
9. Makaya C, Pierre S. An analytical framework for performance evaluation of IPv6-based mobility management protocols. IEEE Transactions on Wireless Communications. 2008; 7(3):972–83.
10. Mathi SK, Valarmathi ML. A secure and decentralized registration scheme for IPv6 network-based mobility. IJET. 2013; 5(5):.
11. Caytiles RD, Park B. A study of an integrated security handover scheme for hierarchical mobile IPv6 based multimedia convergence networks. Int J Contr Autom Syst. 2013; 6(2):367–72.
12. Takacs A, Bokor L. A distributed dynamic mobility architecture with integral cross-layered and context-aware interface for reliable provision of high bitrate mhealth services. In: Godara B, Nikita K, editor. Wireless Mobile Communication and Healthcare. 2013; 6;369–79.
13. Taleb T, Suzuki T, Kato N, Nemoto Y. A dynamic and efficient MAP selection scheme for mobile IPv6 networks. IEEE Conference on Global Telecommunications, GLOBECOM'05; 2005. p. 5.
14. Wakikawa R, Valadon G, Murai J. Migrating home agents towards internet-scale mobility deployments, Proceedings of the 2006 Conference on ACM CoNEXT; 2006.
15. Xie J, Akyildiz IF. A novel distributed dynamic location management scheme for minimizing signaling costs in Mobile IP. IEEE Transactions on Mobile Computing. 2002; 1(3):163–75.