CRHA: An Efficient HA Revitalization to Sustain Binding Information of Home Agent in MIPv6 Network

A. Avelin Diana, V. Ragavinodhini, K. Sundarakantham and S. Mercy Shalinie

Abstract Home agents (HAs) maintain the binding information of mobile node (MN). The binding cache of HA stores the associated data of MN. It represents a single point of failure in Mobile IPv6 networks. An efficient fault-tolerant method is essential to defend these information without any loss. This paper focuses on the revitalization of HA at the time of failure. The standby HAs are formed as clusters within the redundant HA set. Every home agent synchronize its bindings to the next highest preference value home agent. In this paper, we propose clustered redundant home agent (CRHA) protocol to maintain the binding association within the cluster. The simulation results show that our approach is better than the existing recovery schemes.

Keywords MIPv6 · Fault tolerance · Home agent · Binding update · Preference value

1 Introduction

In MIPv6 network, when the Mobile node (MN) gets away from the home and changes its point of attachment to the Internet, home agents (HA) maintain current location (IP address) information of MN [1]. Correspondent node (CN) is the

A. A. Diana (✉) · V. Ragavinodhini · K. Sundarakantham · S. M. Shalinie
Department of Computer Science and Engineering, Thiagarajar College of Engineering, Madurai, India
e-mail: dianaavelin@gmail.com

V. Ragavinodhini
e-mail: raga.cse.34@gmail.com

K. Sundarakantham
e-mail: kskcse@tce.edu

S. M. Shalinie
e-mail: shalinie@tce.edu

G. S. S. Krishnan et al. (eds.), *Computational Intelligence, Cyber Security and Computational Models*, Advances in Intelligent Systems and Computing 246,
DOI: 10.1007/978-81-322-1680-3_25,

network entity on another end for communication, i.e., any node that communicates with MN is called CN. HA is a router on MN's home network, which tunnels datagram for delivery to MN when it is away from home network. In Mobile IPv6, MN should assign three IPv6 addresses to their network interfaces, when they are roaming away from their home network. First is its home address (HoA), which is a stable IP address assigned to the MN. It is used for two reasons: (1) allows a MN which is having a stable entry in the DNS and (2) to hide the IP layer mobility from upper layers. The second is MN's current link, i.e., local address, and the third address is care-of-address (CoA) which is related with MN only when it visits foreign network. The association between the MN's HoA and its CoA along with the remaining life time is known as binding. The central data structure used in MIPv6 is binding cache (BC), a volatile memory consisting of number of bindings for one or more MNs. BC is maintained by both CN and HA. Each entry contains the MN's HoA, CoA, and life time. The life time is valid, if the MN does not refresh the BC entry; the entry is deleted after the lifetime expiry. After configuring its CoA, the MN has to register its binding with HA to determine the current location of MN.

The remainder of this paper is organized as follows: Sect. 2 comprises of related work. The MIPv6 network architecture is described in Sect. 3. Section 4 briefly illustrates the proposed clustered redundant home agent (CRHA) scheme, and its performance analysis with the existing approach is described in Sect. 5. The conclusion is provided in Sect. 6.

2 Related Work

The HA in MIPv6 network transmits packet via tunneling to the MN. The network comprises of active home agent (AHA) and redundant standby home agents (SHAs). The HAs are identified via DHAAD mechanism [2], and the selection of HA is based on the highest preference value [3]. Every HA must maintain a separate HA list [4]. The binding update (BU) is retained to hold this list between MN and HA [5]. This list contains the binding information of MN, and if the AHA gets failed, it is transferred to one of the SHA.

In Mobile IPv6, fault-tolerant methods can be classified into three categories. Central management method is difficult to deploy and least expandable [6, 7]. Passive failure detection and recovery method MN detects HA failure during registration and produces long service break time, and the signaling cost is high. In binding backup, AHA backup its bindings with SHA. At the time of HA failure, one of the SHA will take over the service from AHA. This method deploys different solutions. Full backup method [8] deploys every home agent in a network to maintain all MN bindings. The stable storage method [9] is used to keep all MN bindings in the network. In partial backup method [10], each home agent in a network selects a SHA. All the HAs in virtual home agent method [11] share one global address, and only one home agent is active. IETF draft proposes redundant home agent set (RHAS) method [12, 13] in which every AHA has a SHA from

RHAS. If the AHA fails, the SHAs in the RHAS are responsible for failure detection and service takeover. This method comprises of two switch methods, namely RHAS virtual and RHAS hard which works with HARP protocol [14].

In all the discussed approaches, the recovery duration of a HA at the time of AHA failure is high. Even though it has a selected SHA, the continuous failure of AHAs will lead to loss of binding information. If the replaced new AHA gets failed suddenly without selecting a new SHA, the information in such failed HA will be lost and cannot be recovered. Our approach provides an efficient solution to overcome such issue, and we have also compared our method with other existing approaches.

3 Network Architecture

In Internet topology, the movement of MN can be identified by unique prefix of each network. If the network has one or more prefix, it can be advertised by the neighbor discovery. The global address of the router in *R*-flag depicts that the network has different routers with same prefix and the MN is connected to one router among them. Too many MNs for a single HA cause overload problem. To mitigate this problem, MIPv6 provides DHAAD mechanism that determines the HA address and permits the HA to distribute the load between multiple HAs in a same network by using higher preference value. The network architecture is described in Fig. 1.

4 Proposed Clustered Redundant Home Agent Scheme

4.1 HA Access and Handover Mechanism

The flow chart Fig. 2 illustrates the HA access mechanism in our network. Initially, the incoming BU message from MN is authenticated by its respective AHA. If the BU message is successfully authenticated, AHA sends the registration reply

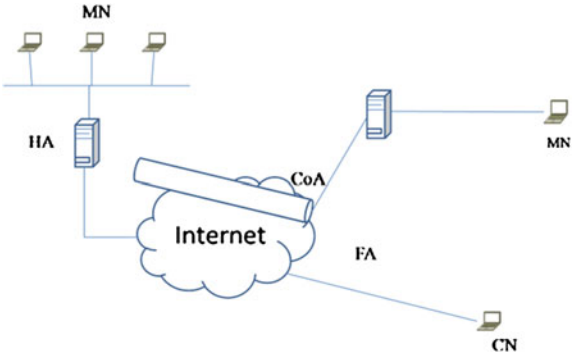

Fig. 1 Network architecture

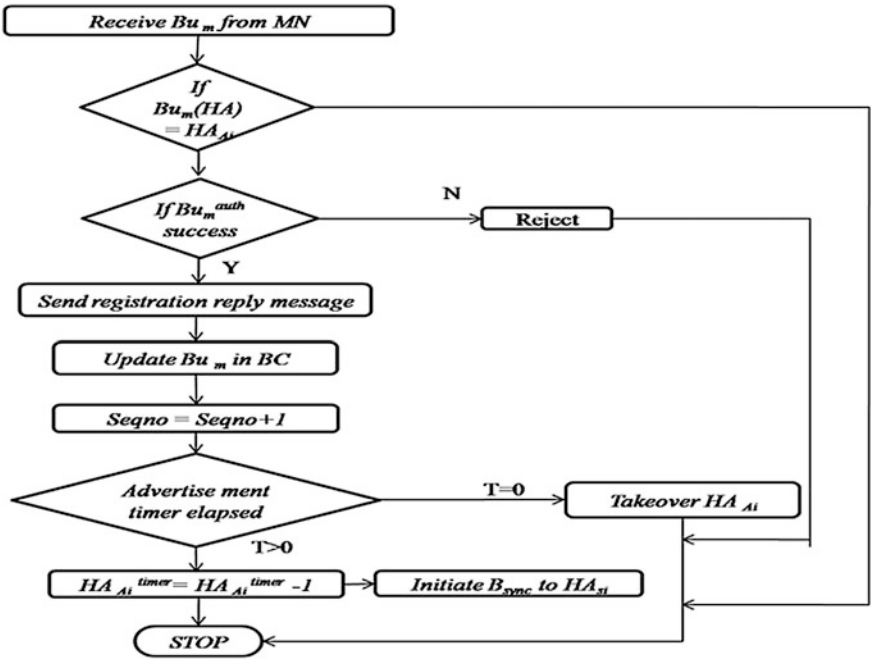

Fig. 2 HA access and handover in MIPv6 network

message to MN else it rejects the MN. Then, the MN updates BU message in BC. The sequence number is incremented by one based on the incoming BU. If the advertisement timer of AHA has elapsed, two cases are to be noticed

- Case 1 ($T = 0$): SHA takeover the AHA.
- Case 2 ($T > 0$): Timer of AHA gets decrement by one and the binding synchronization to SHA is initiated.

4.2 CRHA Mechanism

The network consists of a cluster of SHAs in a RHAS as shown in Fig. 3. Each cluster of virtual SHAs in RHAS serves a single AHA. A single SHA with highest preference value is connected to AHA, and other SHAs within the cluster are connected among themselves and updated from connected SHA. When the SHA knows that AHA fails, it converts itself as an active one and SHA with highest preference value in RHAS is connected to new AHA.

HA–HA protocol is used for the communication between HAs. In RHAS, we propose a new protocol named CRHA protocol for HA communication as in Fig. 4. The number list field indicates the total number of HAs in a cluster. The

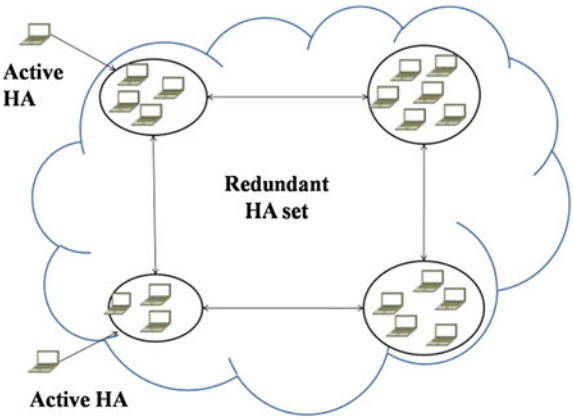

Fig. 3 Clustered redundant HA set

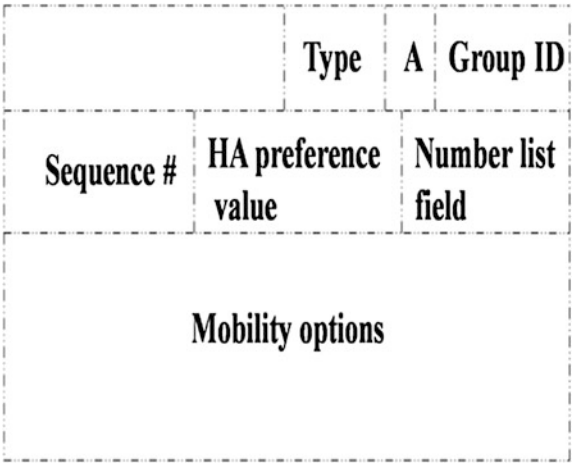

Fig. 4 CRHA protocol

preference value of SHA is based on the nearest distance from AHA. If a SHA from the cluster is removed, the number list field gets decremented.

The type field is to identify the type of HA in a network. Mobility options field consists of any option other than the specific section of message precised to mobility.

Type 0	Assigned for SHA which is directly connected with the AHA
Type 1	Denotes the cluster HA in a redundant HA set
Group ID	Determines the ID for each cluster
A (acknowledgement flag)	Verifies the sender is AHA through the cluster hello message
Sequence	Confirms that the incoming cluster hello message is a most recent one

HA preference value	Based on the highest preference value, SHA from the cluster is set as AHA at the time of AHA failure
Number list	This field indicates the total number of HAs in a cluster.

When the number list field value of cluster gets reduced to ≤ 2, the AHA relieves from older cluster and binds with a new cluster in RHAS. The left HAs batch up with a cluster constituting least number of HAs which is nearer. Figure 5a shows that two AHAs are batched up with two clusters, i.e., serving clusters. Consider AHA2 with cluster preference value 3 as in Fig. 5a. It gets failed, and one of the SHAs in cluster serves as AHA as depicted in Fig. 5b. Now, the cluster consists of only two standby virtual HAs, and so, it finds a new non-serving cluster with number list 6 and joins it as in Fig. 5c. Finally, the remaining two HAs get attached to the serving cluster with 4 HAs to make it as 6 as shown in Fig. 5d.

5 Performance Analysis

We have compared CRHA scheme with the existing RHAS hard and virtual switching methods. Registration delay of a HA means the delay variation in registration between before and after AHA failure. In all the other approaches,

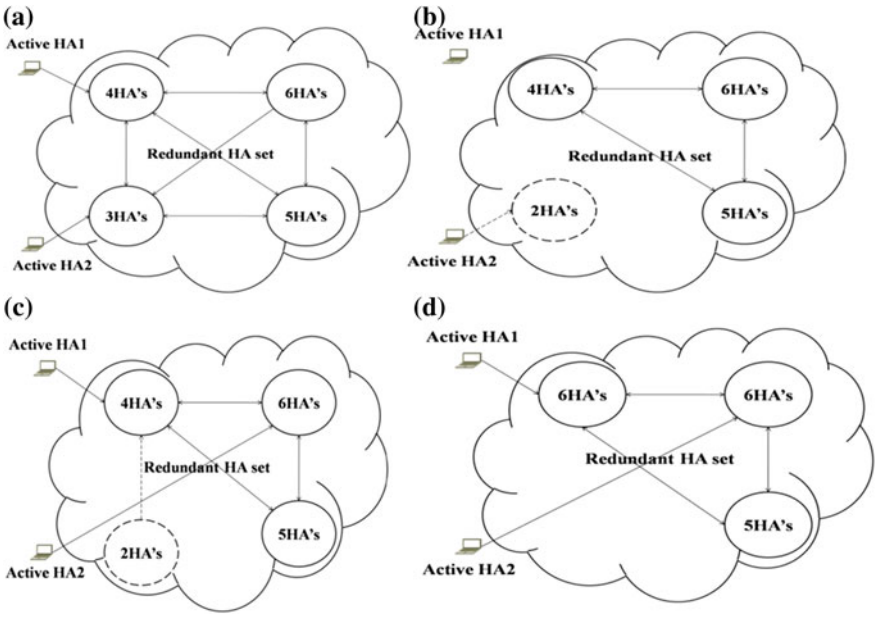

Fig. 5 HA handoff in CRHA method **a** CRHA cluster **b** Active HA2 cluster with one HA decremented **c** Active HA2 joins new cluster **d** Newly formed CRHA cluster

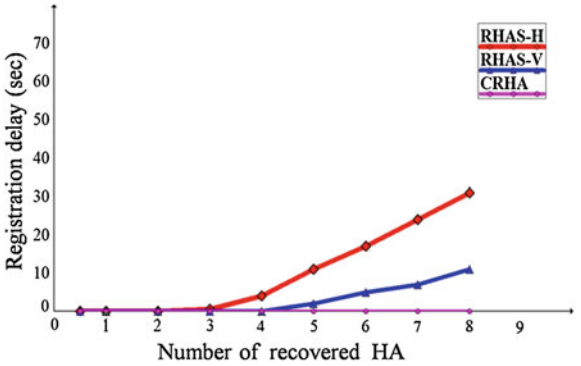

Fig. 6 BU registration delay at HA

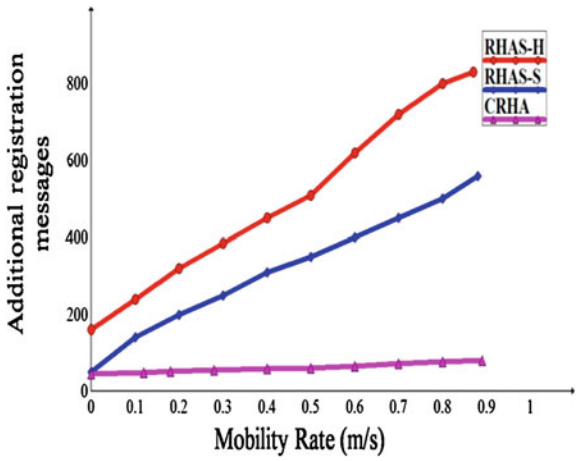

Fig. 7 Additional registration messages

SHAs take time to switch position as AHA at failure, but in CRHA, the failure is not transparent to MN since we use virtual address, and hence, there is no registration delay variation. Figure 6 illustrates the registration delay with recovery HAs of different approach. Figure 7 depicts the additional registration message with the mobility rate of MN. The registration delay is mitigated to negligible count in CRHA approach. Figure 8 shows variations in registration delay with the increased mobility rate. There is no need of exploring time for SHA in CRHA method as it is within the cluster. Figure 9 shows the exploring time of SHA to the number of SHAs explored. Since the AHA failure is not transparent and the exploring time of SHA is negligible, the registration delay variation is constant in CRHA.

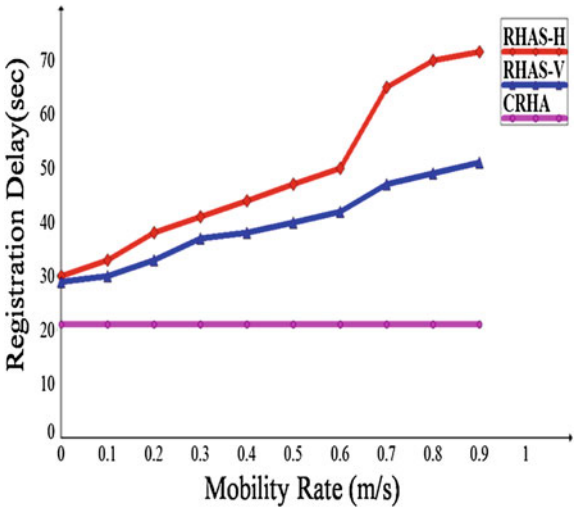

Fig. 8 Registration delay variations

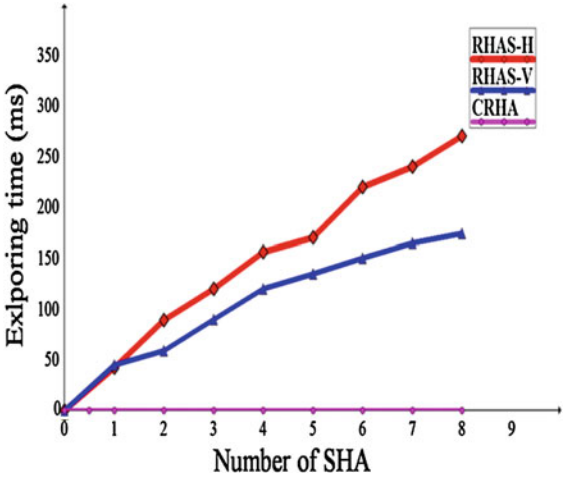

Fig. 9 SHA exploring time

6 Conclusion

This paper proposes CRHA scheme with a protocol for an effective fault-tolerant mechanism. The key point is to reduce the exploring time of SHA and registration delay. Since the SHAs share binding information in the form of a chain within cluster, the exploring time is unnecessary during AHA failure. In CRHA method, registration delay is negligible, and hence, the binding information remains secure. The simulation results reveal that CRHA method shows a better performance when compared with the existing RHAS switching approaches.

References

1. D. Johnson, C. Perkins, J. Arkko. Mobility Support in IPv6. IETF RFC 3775. 2004
2. Qian Sun., et al., "Security Issues in Dynamic Home Agent Address Discovery", draft-sun- mipv6-dhaadsecurity-00.txt, November 2004.
3. Cisco IOS IPv6 Command Reference, ipv6 mobile home-agent (global configuration) through ipv6 ospf database-filter all out. Available FTP: http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_07.html
4. IP Mobility: Mobile IP Configuration Guide, Cisco IOS Release 15 M&T, Available FTP: http://www.cisco.com/en/US/docs/ios-xml/ios/mob_ip/configuration/15-mt/ip6-mobile-home-agent.html#GUID-9156DE37-F1F6-489C-BF4D-65B366A2D782
5. Yujun Zhang, Hanwen Zhang, A Mobile Agent Fault-Tolerant Method Based on the Ring
6. JW. Lin, J. Arul. An Efficient Fault-Tolerant Approach for Mobile IP in Wireless Systems. IEEE Transactions on Mobile Computing. 2(3):207–220. 2003.
7. S. Bose, C. Hota. Efficient Fault Tolerant Mobile IP in Wireless Networks Using Load Balancing Approach. Information Technology Journal. 6(3):463–468. 2007.
8. J. Lee, TM. Chung. Performance Evaluation of Distributed Multiple Home Agents with HAHA Protocol. International Journal of Network Management. 17:107–115, 2007.
9. JH. Ahn, CS. Hwang. Efficient Fault-Tolerant Protocol for Mobility Agents in Mobile IP. International Parallel and Distributed Processing Symposium (IPDPS). Pp.1273–1280. 2001.
10. YS. Chen, CH. Chen, HY. Fang. An Efficient Quorum-Based Fault-Tolerant Approach for Mobility Agents in Wireless Mobile Networks. IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing (SUTC). Pp.373–378. 2008.
11. J. Faizan, HE. Rewini, et al. Introducing Reliability and Load Balancing in Mobile IPv6 Based Networks. Journal of Wireless Communications and Mobile Computing. 6:1–19. 2006.
12. R. Wakikawa. Home Agent Reliability Protocol. IETF Draft of MEXT Working Group, July 2009.
13. R. Wakikawa. Home Agent Reliability Protocol. IETF Draft of MEXT Working Group, May 2011
14. S. Rathi, and K. Thanushkodi, Design and Performance Evaluation of an Efficient Home Agent Reliability Protocol, International Journal of Recent Trends in Engineering, Vol 2, No. 1, November 2009