The Journal of Systems and Software 82 (2009) 1434–1446

Contents lists available at ScienceDirect

The Journal of Systems and Software

journal homepage: www.elsevier.com/locate/jss

Fault-tolerant design for wide-area Mobile IPv6 networks

Jenn-Wei Lin *, Ming-Feng Yang

Department of Computer Science and Information Engineering, Fu Jen Catholic University, 510 Chung-Cheng Road, Hsinchuang 242, Taiwan

ARTICLE INFO

Article history:
Received 31 October 2007
Received in revised form 24 July 2008
Accepted 25 July 2008
Available online 6 August 2008

Keywords:
Mobile IPv6
Fault tolerance
Home agent

ABSTRACT

Mobile IPv6 provides the mobility management for IPv6 protocol. To establish a reliable Mobile IPv6 network, fault tolerance should be also considered in the network design. This paper presents an efficient fault-tolerant approach for Mobile IPv6 networks. In the proposed approach, if a failure is detected in the home agent (HA) of a mobile node, a preferable survival HA is selected to continuously serve the mobile node. The preferable survival HA is the HA that does not incur failure and is neighboring the current location of the mobile node. The proposed approach is based on the preference of each mobile node to achieve the fault tolerance of the HA. Finally, we perform simulations to evaluate the performance of the proposed approach.

1. Introduction

With the rapid development of Internet, IPv6 has been designed to overcome some problems within IPv4 (Deering and Hinden, 1998) (e.g. shortage of IPv4 address space, the explosion of routing tables, and security problem, etc.). In the other aspect, there is also a growing demand for accessing data using the wireless technology. To achieve the wireless Internet, mobility support should be taken into Internet. Mobility support in IPv6 (Mobile IPv6) has been standardized by IETF RFC 3775 (Johnson and Perkins, 2004).

Mobile IPv6 is designed to allow a mobile node (MN) to continuously sustain its ongoing sessions while changing its location in a Mobile IPv6 network. To meet this requirement, each MN is identified by its home address, regardless of its current point of attachment. While an MN at its home network, it operates like a fixed node by using the normal routing to send or receive packets through the access router (AR) of its home network. When the MN moves to a foreign network, it will inform its home agent (HA) of such movement by sending a binding update message. In such case, if a correspondent node (CN) sends a packet to the MN, the packet will be intercepted by the MN's HA and then tunneled to the MN. Here, the packet routing through the HA may introduce the triangle routing problem. To avoid the triangle routing problem, Mobile IPv6 also proposes a route optimization mechanism that allows a CN to directly send packets to the MN by caching the location information of the MN in the CN.

From the above execution scenario of Mobile IPv6, we can know that if a failure occurs in an HA, its responsible MNs cannot perform binding updates again. In such case, if some packets are required to go through the faulty HA, such packets will be lost. The fault tolerance of Mobile IP has been discussed in the literature (Ghosh and Varghese, 1998; Ahn and Hwang, 2001; Cisco Co. Ltd., 2002; Faizan et al., 2005, 2006; Pack and Choi, 2004; Lin and Arul, 2003). The proposed approaches in Ghosh and Varghese (1998), Ahn and Hwang (2001), Cisco Co. Ltd. (2002), Faizan et al. (2005, 2006), Pack and Choi (2004) and Lin and Arul (2003) can be divided into the following two main categories: the redundancy-based scheme and the redirection-based scheme. The redundancy-based scheme (Ghosh and Varghese, 1998; Ahn and Hwang, 2001; Cisco Co. Ltd., 2002; Faizan et al.,2005, 2006) is based on the hardware redundancy to achieve fault tolerance. The redirection-based scheme (Pack and Choi, 2004; Lin and Arul, 2003) is based on the workload redirection. In this scheme, the workload of the faulty mobility agent is taken by the survival mobility agent. Although the approaches of Pack and Choi (2004) and Lin and Arul (2003) do not incur the significant hardware overhead, the workload redirection is required to be assisted by the network architecture (e.g. the hierarchical Mobile IP architecture and a centralized OAM center in the network).

In this paper, we propose a new fault-tolerant approach for Mobile IPv6. Compared to the previous approaches (Ghosh and Varghese, 1998; Ahn and Hwang, 2001; Cisco Co. Ltd., 2002; Faizan et al., 2005, 2006; Pack and Choi, 2004; Lin and Arul, 2003), there are two features in the proposed approach. The first feature is that the proposed approach does not adopt the hardware redundancy and not need the assistance of the network architecture (e.g. the hierarchical Mobile IP architecture and the centralized OAM center Pack and Choi, 2004; Lin and Arul, 2003). The proposed approach is based the *home address regeneration* to tolerate the HA failure. When an HA fails, each of its responsible MNs (*failure-affected MNs*) generates a new home address to associate with its preferable survival

* Corresponding author.
E-mail address: jwlin@csie.fju.edu.tw (J.-W. Lin).

0164-1212/$ - see front matter © 2008 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2008.07.021

HA. Due to using the new home address, the failure-affected MN can continue to perform the binding update. In addition, the failure-affected MN can also continuously send packets to a CN. The other feature of the proposed approach is that it particularly considers how to recover the lost packets due to the HA failure. This also solves the problem how to make a CN send packets to a failure-affected MN when an HA fails. Unlike the previous approaches (Ghosh and Varghese, 1998; Ahn and Hwang, 2001; Cisco Co. Ltd., 2002; Faizan et al., 2005, 2006; Pack and Choi, 2004; Lin and Arul, 2003), the recovery of the lost packets is not dependent on the TCP layer, which can avoid incurring the long recovery latency. In the proposed approach, the packet recovery is integrated into the binding update of an MN. To examine the effectiveness of the proposed approach, we perform extensive simulation experiments to evaluate the performance of the proposed approach.

The remainder of this paper is organized as follows: Section 2 introduces the background of this paper. Section 3 proposes our approach. Section 4 evaluates the overhead of the proposed approach. Section 5 makes the comparison between the proposed approach and previous approaches. Section 6 performs simulations to quantify the performance of the proposed approach. Finally, we make conclusions and discuss future work in Section 7.

2. Background

This section describes the background knowledge of this paper. First, a wide-area Mobile IPv6 network model is given. Then, we briefly introduce the Mobile IPv6 protocol. Next, we describe the methods used for detecting the HA failure. Last, related work is reviewed.

2.1. Network model

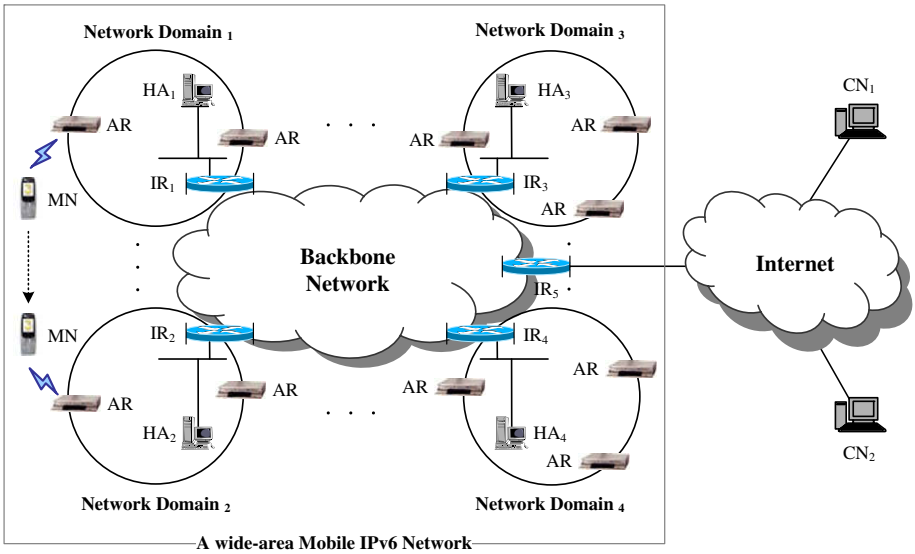
The network model referred in this paper is a wide-area mobile network (not Mobile Internet), as shown in Fig. 1. The Telecom carrier usually establishes a wide-area mobile network for its mobile users. In the wide-area mobile network, it has a number of network domains which are divided based on the geographic locations. Initially, each MN is located in a network domain as its home network. In a network domain, there are several access routers (ARs), a home agent (HA), and an interconnection router. The AR assists the MNs to forward packets within its located network domain. The HA provides the mobility support for its responsible MNs.

The details of the mobility support will be given in the next section. As for the interconnection router, it is used to transmit packets from a network domain to another one. Among the network domains, there is a high-speed fixed network as the backbone for connecting all the network domains.

2.2. Mobile IPv6

Initially, each mobile node (MN) is assigned a permanent address as its home address. The mobility of an MN is fixedly served by the HA in its home network. When the MN moves from its home network domain to another network domain, it will obtain a "care-of-address" to reflect its current point of attachment. Next, the MN sends a binding update message to its serving HA to store the address mapping between the home address and care-of-address in the binding cache of the HA. Then, the HA will respond to the MN with a binding acknowledgment message. Thereafter, the HA can intercept any packets destined to the home address of the MN and tunnel such packets to the care-of-address of the MN. However, the packet transmission through the HA may cause a long transmission delay, especially when the MN and CN are located in the same network domain. This is called the triangle routing problem. To solve the possible triangle routing problem, Mobile IPv6 supports the route optimization to forward packets by using the shortest path between the CN and MN. The route optimization is achieved by maintaining a binding cache in the CN to store the addresses of the communicating MNs (Johnson and Perkins, 2004).

For the security of binding update, Mobile IPv6 uses IPsec (Kent and Seo, 2005) and Return Routability (Johnson and Perkins, 2004) to ensure the secure binding update execution between the MN and HA and between the MN and CN. In this paper, the proposed approach is also based on the original Mobile IPb6 security mechanisms to achieve fault tolerance. As for how to provide more secure mechanisms for the Mobile IPv6 network, it is another research topic, which is now discussed in Fathi et al. (2005) and Ren et al. (2006).



MN: Mobile Node AR: Access Router HA: Home Agent IR: Interconnection Router CN: Correspondent Node

Fig. 1. Network model.

2.3. Failure assumption and detection

This paper only concerns the fault tolerance of the HA entity. For other main entities in the Mobile IPv6 network system (see Fig. 1), they are all the router equipment. The hardware redundancy technique has been extensively adopted to handle the fault tolerance of the router (Srivastava, 2003).

The MN and CN can detect the HA failure with the help of the interconnection router. As shown in the network model (Fig. 1), the interconnection router acts as the packet forwarder of an HA. Before a packet to an HA, the packet is first received by a corresponding interconnection router. In Lin and Arul (2003), it also stated that a router is usually collocated with an HA on a LAN of the same network domain to be the packet forwarder of the HA. If a failure occurs in an HA, the corresponding interconnection router can detect the failure by introducing the concept of "Heartbeat" (Khalil, 2002). Each HA will periodically send a heartbeat message to its corresponding interconnection router. Based on Hinden (2004), the default heartbeat interval (the default time between two sending heartbeat messages) is set to 1 s. In Kuo et al. (2005), it indicated that the heartbeat messages with once per second introduce a little bandwidth overhead. If the interconnection router does not receive the heartbeat message for a certain period of time, it can assume that there is a failure in its corresponding HA. Therefore, while an MN performs a binding update to a faulty HA, the corresponding interconnection router will respond to the MN with an ICMP error message (Conta et al., 2006). Then, the MN is also aware of the HA failure. Similarly, the corresponding node (CN) can also know the HA failure by the interconnection router. If a CN would like to send data packets to an MN through a faulty HA, the CN will also receive the ICMP error message from the interconnection router.

2.4. Related work

A lot of fault-tolerant approaches have been proposed for Mobile IP (Ghosh and Varghese, 1998; Ahn and Hwang, 2001; Cisco Co. Ltd., 2002; Faizan et al., 2005, 2006; Pack and Choi, 2004; Lin and Arul, 2003). The approaches (Ghosh and Varghese, 1998; Ahn and Hwang, 2001; Cisco Co. Ltd., 2002; Faizan et al., 2005, 2006) belong to the redundancy-based scheme. The basic idea of the redundancy-based scheme is to equip with one or more redundant HAs for each working HA as its backup set. In the approach of Ghosh and Varghese (1998), the redundant HAs are configured in the standby or load-sharing mode. If a working HA fails, one member of its redundant HAs will be selected to be the new working HA. This is done by using the Address Resolution Protocol (ARP) (Plummer, 1982) to map the IP address of the faulty HA onto the network link-layer address of the selected backup member. Other backup members can continuously co-work with the new working HA in the standby or load-sharing mode. However, in the approach of Ghosh and Varghese (1998), it has the binding synchronization problem. Whenever an MN performs a binding update to its primary HA, the binding update message is also sent to the corresponding redundant HAs. It may introduce a long registration delay.

To avoid the long registration delay, the approach of Ahn and Hwang (2001) uses the checkpoint and log techniques to store the binding update information in stable storage. Basically, the approach of Ahn and Hwang (2001) is similar to the approach of Ghosh and Varghese (1998). In Ahn and Hwang (2001), after an HA fails, one of its backup members can acquire the binding update information from stable storage. However, the access to the stable storage is a time-consuming operation.

In the approach of Cisco Co. Ltd. (2002), it uses the Hot Standby Router Protocol (HSRP) to ensure that the redundant HA can immediately take over the faulty HA. The HSRP is developed by Cisco (Li et al., 1998), which enables two or more HAs on a LAN as a single HA group by sharing the same IP address and MAC (Layer 2) address. Similar to the approach of Ghosh and Varghese (1998), this approach also has the binding synchronization problem.

Unlike the above redundancy-based approaches, the approach of Faizan et al. (2005) aims at Mobile IPv6, not Mobile IPv4. In Faizan et al. (2005), it proposes a Virtual Home Agent Reliability Protocol (VHARP) to allow that multiple HAs coexist on the same network domain (home link) and have the same Global IP address. Based on VHARP, all the communication between the MN (CN) and the HAs is based on the Global HA address. For each MN, its binding update information is stored on at least two HAs. One is the active HA, and others are the backup HAs. Each HA periodically sends a heartbeat message over the home link. If a failure occurs in the active HA, other HAs can detect this event since they do not receive the heartbeat message for a period of time. In such case, all other HAs simultaneously execute a procedure to select the HA with the lowest load as the new active HA. The approach of Faizan et al. (2006) enhances the approach of Faizan et al. (2005) to further consider the home link failure, not only the HA failure. In the approach of Faizan et al. (2006), multiple HAs on the same network domain are equipped with several home links. Similarly, if an active home link fails, the new active home link will be selected from other home links.

For the approaches of Pack and Choi (2004) and Lin and Arul (2003), they belong to the redirection-based scheme. The main idea of this scheme is to perform the workload redirection. In the approach of Pack and Choi (2004), its proposed fault-tolerant method is only suitable for the Hierarchical Mobile IPv6 (HMIPv6) architecture, not available for the general Mobile IPv6 architecture. The HMIPv6 is designed to reduce the registration overhead and handoff latency by introducing a local home agent entity called the mobility anchor point (MAP). The approach of Pack and Choi (2004) mainly copes with the MAP failure, not the HA failure. In the proposed fault-tolerant method, it assumed that each MN can receive two or more router advisement messages from different MAPs whenever it moves to a new network domain. Then, the MN selects a primary MAP (P-MAP) and a secondary MAP (S-MAP). Next, the MN performs the primary and secondary binding updates. The primary binding update notifies the P-MAP, HA, and communicating CNs of the following information: the MN current location and the MN's located MAP. The secondary binding update is executed after completing the primary binding update, which main purpose is to make the communicating CNs know the alternate reachable MAP of the MN (the MN's S-MAP). When a CN (MN) detects the failure of the P-MAP, the S-MAP will be instead of P-MAP to forward (send) packets to the MN (CN). From the above description, the fault-tolerant capability of Pack and Choi (2004) is dependent on the two-MAPs selection algorithm, but the algorithm is not clearly described in Pack and Choi (2004). If there is only one MAP in a network domain or the P-MAP and S-MAP fail simultaneously, the approach of Pack and Choi (2004) cannot work successfully. For the fault tolerance of the HA, the approach of Pack and Choi (2004) described that the redundancy-based scheme should be used since the HA contains very important binding update information.

The approach of Lin and Arul (2003) is our previous work on the fault tolerance of Mobile IPv4. It redirects the workload of the faulty HA to survival HAs without the hardware support. Based on the approach, the twice-tunneling transmission technique is used to assist the packet transmission after the HA failure. Compared to the pre-failure, the packet destined to an MN may incur a potentially long delay. In the execution of the workload redirection, the centralized OAM center is involved to collect the loading status of all failure-free HAs for evenly assigning the workload of

the faulty HA to the failure-free HAs. The centralized OAM center also needs to commend all the foreign agents (FAs) in the Mobile IPv4 network to collect the binding information of the faulty HA. However, unlike the Mobile IPv4, the Mobile IPv6 has no FAs. In such case, the binding information restoration must be done by all the failure-affected MNs to actively perform the binding updates with their respective new serving HAs. However, the approach of Lin and Arul (2003) does not discuss how to make each failure-affected MN know its new serving HA. Therefore, the approach of Lin and Arul (2003) is not suitable to be used in the Mobile IPv6 network architecture for tolerating the HA failure since the binding information cannot be restored.

3. The proposed approach

This section presents a new fault-tolerant approach for Mobile IPv6. The proposed approach is also based on the workload redirection by using survival (failure-free) HAs to serve the failure-affected MNs. The failure-affected MNs indicate the responsible MNs of the faulty HA. Unlike the previous redirection-based approach Lin and Arul (2003), the proposed approach can be applied in the Mobile IPv4 and IPv6 networks, and it is not required the support of the centralized OAM center. In addition, the selection of failure-free HAs is from the viewpoint of the failure-affected MN. It makes each failure-affected MN select its preferable failure-free HA as its new serving HA to reduce the fault-tolerant overhead. Therefore, when an HA fails, a failure-affected MN can continuously send packets to a CN. The details are described in Sections 3.1 and 3.2. The other feature of the proposed approach is that it does not rely on the end-to-end TCP layer to perform the lost packet recovery. When an HA fails, the packets sent from a CN can be delivered to a failure-affected MN. The details are described in Section 3.3. In addition, when a faulty HA is recovered from failure, the failure-affected MN can be served back by its original HA. This recovery procedure is also described in Section 3.4.

3.1. Fault tolerance of HA

If an HA fails, its responsible MNs (the failure-affected MNs) cannot continuously perform binding updates to it. Furthermore, the faulty HA is also unable to assist CNs to send packet to its responsible MNs. To tolerate the HA failure, the proposed approach assigns more than one HA for each MN. Unlike the redundancy based approaches (Ghosh and Varghese, 1998; Ahn and Hwang, 2001; Cisco Co. Ltd., 2002; Faizan et al., 2005, 2006), the proposed approach does not configure one or more redundant HAs for each working HA. As shown in Fig. 1, there is only one HA in each network domain. In the proposed approach, the multiple HA assignment is from the logical viewpoint to make that each HA in the Mobile IPv6 network system can serve any MNs. Fig. 2 illustrates the basic idea of the proposed approach.

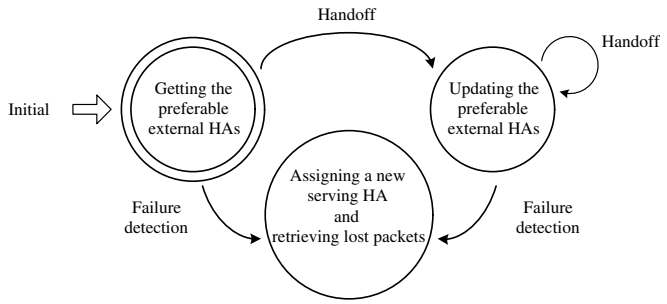


Fig. 2. The basic idea of the proposed approach.

Initially, each MN in its home network domain can know the identity of its default HA. The default HA is the HA in the MN's home network domain, which is fixed without changing as the MN moves. In addition, the MN can also know its preferable external HAs by actively sending a solicited binding update message to the default HA. The external HAs are the HAs having 1-hop network domain distance, 2-hop network domain distance, and so on with the home network domain, as shown in Fig. 3a. The reason why the external HAs can be known from a default HA is explained as follows. In this paper, the network model is under a wide-area mobile network, not Mobile Internet. The following information can be known while establishing the Mobile IPv6 network: the number of HAs, the distance relationship between an HA and another one, and the addresses of all the HAs in the system. (Note that the addresses of all the HAs can follow an addressing rule to assign them.) Therefore, it is reasonable for an HA to store the addresses of all other HAs in its external HA list based on the order of their location distances with the HA. In practice, the number of the HA addresses stored in the external HA list is dependent on the given fault-tolerant capability, which will be further discussed in Section 6. In this section, we are based on the highest fault-tolerant capability to elaborate the proposed approach. Therefore, if there are n HAs in the network system, the external HA list of an HA is required to store the addresses of $n-1$ external HAs.

If the large number of the external HAs is concerned, the addresses of the external HAs can be abstracted as *a meta-address* form since the addresses of the HAs can be pre-specified by following an addressing rule. By using the meta-address form and itself address of a default HA, the default HA can infer the addresses of its corresponding external HAs. For example in Fig. 3a, the interface identifiers (host-portion addresses) of all the HAs are fixedly specified as "0:0:0:1".

Additionally, the network domains in a Mobile IPv6 network system usually have the contiguous network-prefix addresses. With these two characteristics, in Fig. 3a, the addresses of the external HAs for HA_4 are simplified as the meta-address form (3, 2, and 4). In the meta-address form, the value of the *pre-domains* field is 3. It represents there are three network domains (1, 2, and 3) which network prefix addresses are smaller than the located network domain (4) of the MN. The value of the *post-domains* field is two which represents there are two network domains (5 and 6) which network-prefix addresses are larger than the located network domain (4) of the MN. As for the prefix-piece field, it is set to four which represents the prefix address of the network domain occupies four pieces. In the IPv6 protocol, the address is 128 bits, which is further divided into eight pieces and each piece has 16 bits. For the Mobile IPv6, the network-prefix portion of the address is usually 64 bits and the interface identifier (the host portion of the address) is also 64 bits (Jelger and Noel, 2005).

As mentioned above, the default HA will receive a solicited binding update message from each of its responsible MNs. Then, the default HA will respond to the MN with a binding acknowledgment message. Before sending this message, the default HA attaches the addresses of its known external HAs on the mobility options field of the binding acknowledgment message. Note that the mobility options field already exists in the binding acknowledgment message (Johnson and Perkins, 2004), which is used for extension. Several Mobile IPv6 research work (Takahashi et al., 2003; Lu et al., 2005) has also utilized the mobility options field to carry necessary information. However, if the size of the attached addresses is concerned, the meta-address form of the external HAs is attached on the binding acknowledgment message. Upon receiving the binding acknowledgment message, the MN can know the information about its preferable external HAs from the message. Next, the preferable external HA information is changed whenever the MN moves to a foreign network domain.

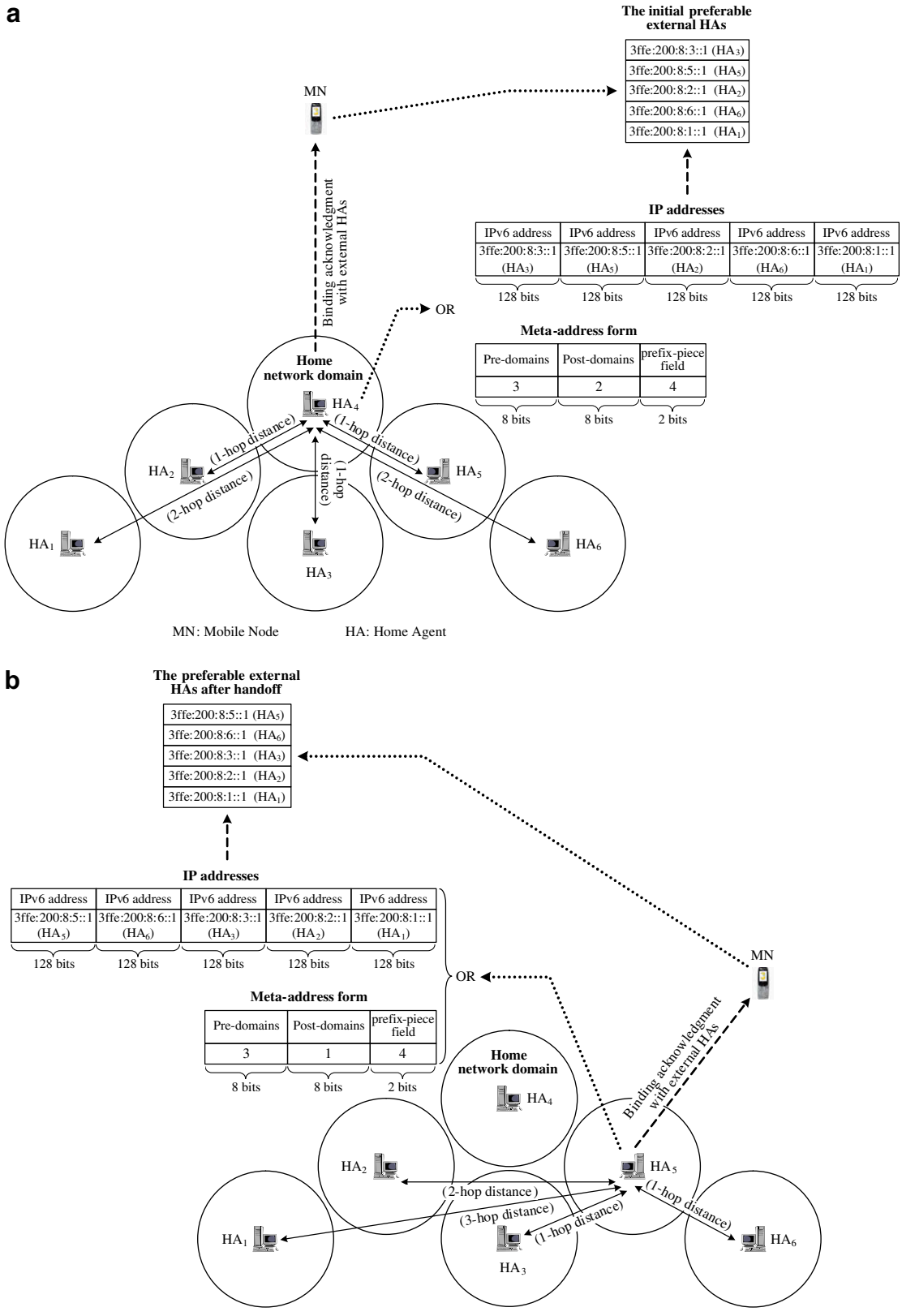


Fig. 3. The variation of the preferable external HAs. (a) MN in the home network domain. (b) MN in the foreign network domain.

When an MN moves to a foreign network domain, the MN also needs to send a binding update message to its default HA. After receiving the binding update message, the default HA will attach the new preferable external HA information on the binding acknowledgment message since the MN has changed its location. The new preferable external HA information is found as follows. First, the new located network domain of the MN is inferred from the MN's care-of-address. Then, the new preferable external HAs

are also found from the external HA list of the default HA. The new preferable external HAs have 0-hop network domain distance, 1-hop network domain distance, 2-hop network domain distance, and so on with the new located network domain of the MN. Next, the default HA attaches the addresses of the new preferable external HAs or their meta-address form on the binding acknowledgment message and then sends the message to the MN. Upon receiving the binding acknowledgment message, the MN updates the preferable external HA information, as shown in Fig. 3b. In Fig. 3b, if the default HA fails, the first preferable external HA of the MN is HA_5, not HA_3 since HA_5 is nearest to the new located network domain of the MN.

Thereafter, if a default HA fails, this failure event can be detected by its corresponding MNs (see Section 2.3). Each of these failure-affected MN will utilize its pre-obtained preferable external HA information to perform the fault tolerance of its default HA, as shown in Fig. 4. First, the failure-affected MN selects the first preferable external HA as the new serving HA since it is nearest to the MN's current location in comparison with other external HAs (see (2) of Fig. 4). Then, the failure-affected MN generates a unique external home address by using the address of the first preferable external HA and itself address. Note that the Mobile IPv6 protocol allows an MN to have more than one home addresses. The detailed address generation process will be given in next subsection. Next, the failure-affected MN performs a new binding update to the first preferable external HA by using the address pair (the generated external home address, the current care-of-address). If the first preferable external HA is in the faulty or overloading status (see (6) of Fig. 4), the binding update will be unsuccessful. In such case, the failure-affected MN will select next preferable external HA to repeat the above same operations until a suitable preferable external HA is met. Fig. 5 illustrates the detailed steps for tolerating multiple HA failures. After meeting a suitable preferable external HA, the failure-affected MN also needs to perform a binding update with each of its communicating CNs (see (7) of Fig. 4) by using the new address pair (the generated external home address, the current care-of-address). The above binding update is considered for the route optimization between the MN and the CN (see Section 2.2).

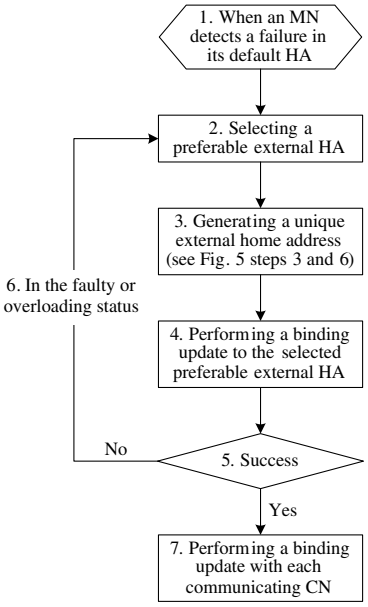


Fig. 4. The fault-tolerant process of the HA.

3.2. New home address generation

In the proposed approach, each failure-affected MN is required to generate a new home address for being served by its selected preferable external HA. The new home address is generated as follows: first, the prefix of the preferable external HA is used as the prefix of the new home address. Then, the suffix of the new home address is based on RFC 4291 (Hinden and Deering, 2006) and RFC 3041 (Narten and Draves, 2001) to generate it. If the failure-affected MN has a MAC address, the MAC address is transformed as the suffix of its new home address (Hinden and Deering, 2006). If the failure-affected MN has not the MAC address, it uses the MD5 hash function to generate the suffix of the new home address (Narten and Draves, 2001). Note that MD5 is usually implemented in an IPv6 node (Touch, 1995), which is used in the authentication for computing the digest of a message. By combining the generated prefix and suffix, the new home address of the MN is obtained. Then, the failure-affected MN will perform dupli-

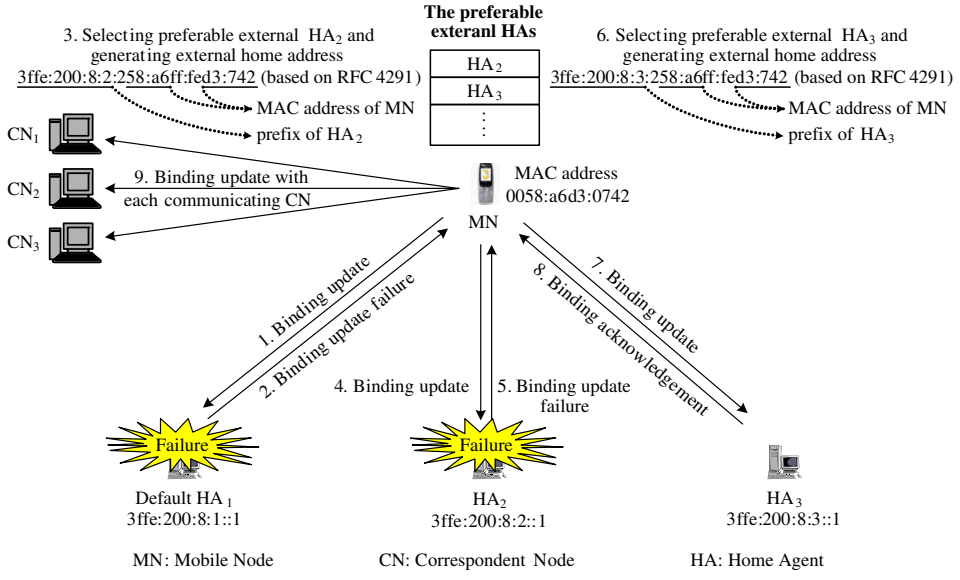


Fig. 5. Example of two HA failures in the system.

cate address detection (DAD) (Narten and Draves, 2001) for the generated new home address. In Soliman (2004), it claimed that the generated new home address has a very small duplicate probability with other home addresses. If the generated new home address is already in use, its suffix-portion address is re-generated by using a random number.

3.3. Lost packet recovery

The packet delivery from a CN is also affected by the HA failure. This subsection mainly solves the problem that a CN can continuously send packets to a failure-affected MN when an HA fails. The route optimization is supported in the Mobile IPv6. Therefore, unlike the Mobile IPv4, if an HA fails, the packets destined to a failure-affected MN are affected only when a CN would like to send a packet to the MN, but it has not the MN's binding information in its binding cache. In this situation, the packet will be forwarded through the faulty HA, and it will be lost. Furthermore, if the service session between the MN and the CN is TCP, the packet cannot be retransmitted successfully unless the faulty HA is recovered. To recover lost packets and avoid long recovery latency, the interconnection router that is located within the network domain of the faulty HA will be used to assist the packet delivery recovery. As mentioned in Section 2.3, when an HA fails, the CN will receive an ICMP error message from the interconnection router. To make the undeliverable packet be sent to the desired failure-affected MN, the proposed approach first asks the interconnection router to keep track the sent ICMP error messages for the faulty HA. These tracking messages will form an undeliverable packet list (see (2) of Fig. 6).

The proposed approach also asks the CN to store the undeliverable packets in its buffer (see (4) of Fig. 6). The buffer mechanism is also used to perform the packet recovery. To clearly understand the lost packet recovery of the proposed approach, Fig. 6 illustrates the assistance of the undeliverable packet list and buffer as well as the formats of these two data structures. With the support of the two data structures, the recovery process of the undeliverable packets can be integrated into the binding update, as shown in Fig. 7.

Based on the above description, when a default HA fails, each failure-affected MN will select its preferable failure-free HA as the new serving HA to perform its binding update. For recovering the lost packets at the faulty HA, the proposed approach asks the failure-affected MN to additionally send a binding update message to the faulty default HA in addition to the new serving HA (see (1.a) and (1.b) of Fig. 7). The binding update message to the faulty HA is also first received by the corresponding interconnection router of the faulty HA. In such case, the interconnection router checks whether there are undeliverable packets addressed to the failure-affected MN by using its undeliverable packet list (see (2.b) of Fig. 7). If so, the interconnection router sends an ICMP error message containing the relative CN list (see (3) of Fig. 7). Note that the ICMP message has a general message body field to include the required information with a variable length (Conta et al., 2006). The relative CN list is a list of addresses of relative CNs.

After receiving the ICMP error message containing the relative CN list, the failure-affected MN can know the relative CNs which previously sent undeliverable packets to it. Next, the failure-affected MN solicits the relative CNs to re-send the undeliverable packets. Here, the retransmission of the undeliverable packets can be integrated into the binding updates between the failure-affected MN and relative CNs. This is done by the failure-affected MN to send solicited binding update messages with its previous home address to the relative CNs (see (4) of Fig. 7). In addition to performing the binding update, the relative CNs also find the undeliverable packets destined to the failure-affected MN from their respective undeliverable packet buffers based on the previous home address of the failure-affected MN (see (5) of Fig. 7). Then, the found undeliverable packets are directly sent to the failure-affected MN. Since the failure-affected MN has registered its new binding information (the new external home address, the care-of-address) on the relative CNs, if such CNs would like to send packets to the failure-affected MN again, the packets can be directly sent to the failure-affected MN without passing through the faulty default HA.

3.4. Failure recovery

For recovering the lost packet at the faulty HA, the failure-affected MN additionally sends the binding update message to its faulty default HA when it performs a binding update. Therefore, when a faulty HA is recovered from failure, each failure-affected

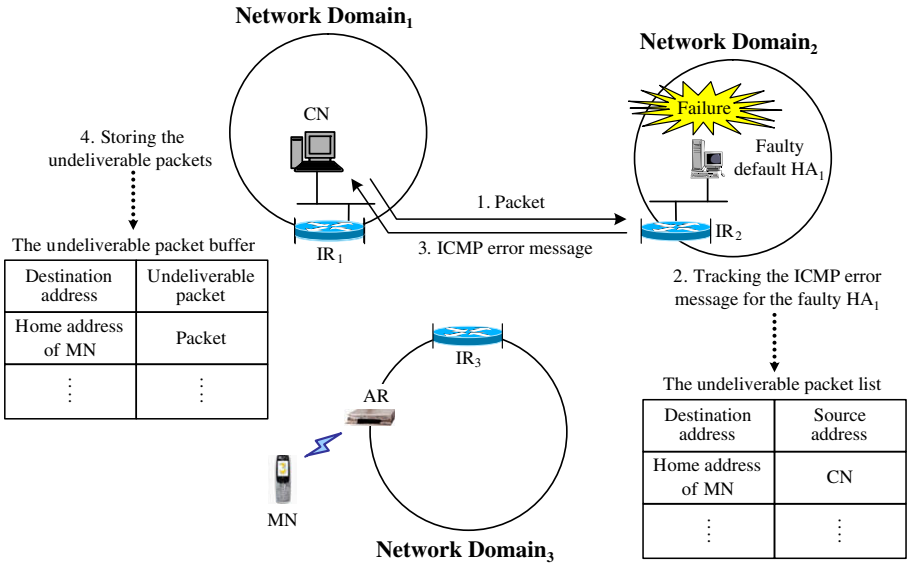


Fig. 6. The assistance of the undeliverable packet list and buffer.

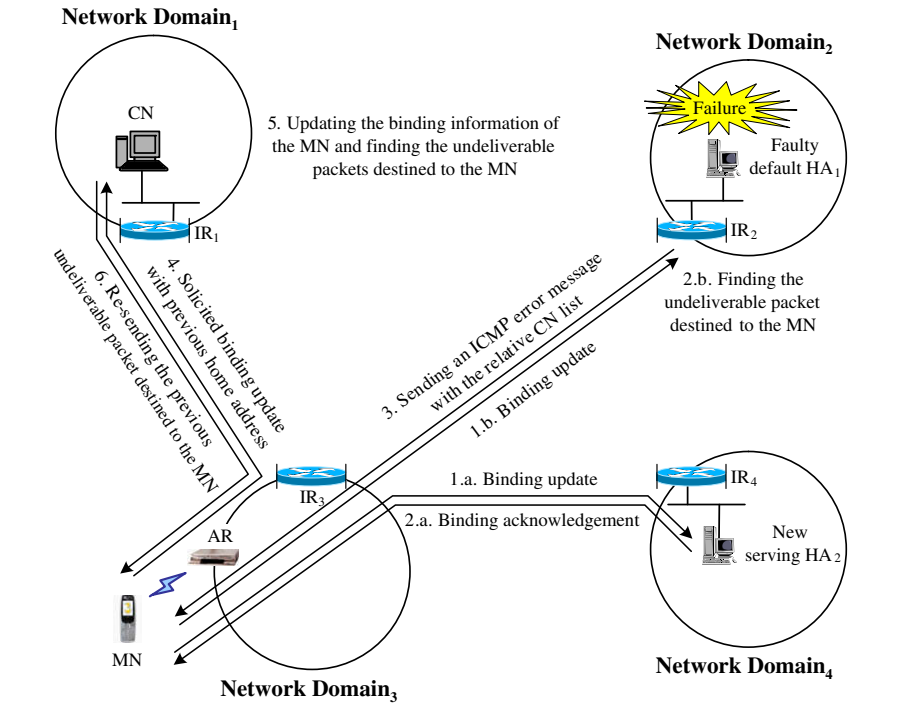


Fig. 7. Recovery of the lost packets due to the HA failure.

MN can detect this recovery event since its binding update to the default HA is successful, not failure. In such case, the failure-affected MN will receive a binding acknowledgment message from the recovered default HA. Next, the failure-affected MN uses its original home address to be served by the default HA, not the preferable external HA.

4. Evaluation

This section evaluates the failure-free and fault-tolerant overheads of the proposed approach. The recovery overhead of the lost packets is also evaluated in this section.

4.1. Failure-free overhead

In the proposed approach, each MN needs to maintain the preferable external HA information during the failure-free period for tolerating the HA failure. The cost for maintaining the preferable external HA information is counted into the failure-free overhead. In the proposed approach, the information maintenance is integrated into the binding update. When an MN moves to a new foreign network domain, the information about the new preferable external HAs is attached on the binding acknowledgment message. In reality, the additional size of this message is dependent on the number of the attached external HAs. However, if the preferable external HA information is converted into a meta-address form information (see Section 3.1), the size of the attached information is only 18 bits. As for the increasing transmission delay of the extended binding acknowledgment message (the binding acknowledgment message with the external HA information), it is dependent on the transmission delay of the attached external HA information. By simulation experiments, the transmission delay of an extended binding acknowledgment is almost same as that of the normal binding acknowledgment message (see Section 6). From the above description, we can know that the failure-free overhead of the proposed approach is very small.

4.2. Fault-tolerant overhead

The proposed approach is based on the workload redirection to tolerate the HA failure. In Lin and Arul (2003), we have mentioned that the fault-tolerant overhead of the redirection-based scheme is mainly determined on the performance degradation of a failure-free HA and the transmission latency of the fault-tolerant control messages (the transmission latency of the control messages issued for fault tolerance). Similar to Lin and Arul (2003), the performance degradation of a failure-free HA is also represented as the increasing blocking probability of a failure-free HA. Unlike the approach of Lin and Arul (2003), the proposed approach is from the MN viewpoint to tolerate the faulty HA. The increasing blocking probability formula in Lin and Arul (2003) can be directly applied in the proposed approach, which is derived as follows. Before an HA failure, the blocking probability that an HA has no sufficient binding entries for a working responsible MN can be derived by using the $M/G/c/c$ queuing model (Gross and Harris, 1985):

$$P_{\text{Before\_Blocking}} = \frac{\frac{\left(\frac{\lambda_{\text{HA}}}{\mu_{\text{HA}}}\right)^{c_{\text{HA}}}}{c_{\text{HA}}!}}{\sum_{i=0}^{c_{\text{HA}}} \frac{\left(\frac{\lambda_{\text{HA}}}{\mu_{\text{HA}}}\right)^{i}}{i!}} \tag{1}$$

where λ_{HA} is the arrival rate of working MNs, $\frac{1}{\mu_{\text{HA}}}$ is the mean service time of a working MN, and c_{HA} is the number of binding entries in an HA.

After an HA fails, the average number of the failure-affected MNs in the faulty HA can be also obtained by using the $M/G/c/c$ queuing model (Gross and Harris, 1985), as follows:

$$N_{MNs} = \sum_{n=0}^{c_{HA}} n \times \frac{\frac{\left(\frac{\lambda_{HA}}{\mu_{HA}}\right)^{n}}{n!}}{\sum_{i=0}^{c_{HA}} \frac{\left(\frac{\lambda_{HA}}{\mu_{HA}}\right)^{i}}{i!}} \quad (2)$$

These failure-affected MNs will respectively select their preferable failure-free HAs to serve them. For a failure-free HA, it may serve a portion of failure-affected MNs $f \times N_{MNs}$, where f is the fraction of the failure-affected MNs to be served by the failure-free HA. However, the proposed approach also considers the overloading situation. The number of the failure-affected MNs to be served by a failure-free HA is

$$N_{Serving\_Affected\text{-}MNs} = \text{Minimum}(f \times N_{MNs}, \text{Maximum}(N_{Threshold\_MNs} - N_{MNs}, 0)) \quad (3)$$

where $N_{Threshold\_MNs}$ is the overloading threshold of an HA. If the number of MN served by the HA is greater than or equal to this threshold, the HA is regarded to be in the overloading status. In such case, no failure-affected MNs can be served by the overloading HA.

During the HA failure period, the number of failure-affected MNs in Eq. (3) will additionally be served by a failure-free HA. For a failure-free HA, the number of the binding entries used for serving its responsible MNs becomes fewer. Therefore, the new blocking probability of a failure-free HA becomes:

$$P_{After\_Blocking} = \frac{\frac{\left(\frac{\lambda_{HA}}{\mu_{HA}}\right)^{(c_{HA}-N_{Serving\_Affected\text{-}MNs})}}{(c_{HA}-N_{Serving\_Affected\text{-}MNs})!}}{\sum_{i=0}^{(c_{HA}-N_{Serving\_Affected\text{-}MNs})} \frac{\left(\frac{\lambda_{HA}}{\mu_{HA}}\right)^{i}}{i!}} \quad (4)$$

From (1) and (4), the increasing blocking probability can be evaluated as

$$P_{HA\_Blocking} = \frac{\frac{\left(\frac{\lambda_{HA}}{\mu_{HA}}\right)^{(c_{HA}-N_{Serving\_Affected\text{-}MNs})}}{(c_{HA}-N_{Serving\_Affected\text{-}MNs})!}}{\sum_{i=0}^{(c_{HA}-N_{Serving\_Affected\text{-}MNs})} \frac{\left(\frac{\lambda_{HA}}{\mu_{HA}}\right)^{i}}{i!}} - \frac{\frac{\left(\frac{\lambda_{HA}}{\mu_{HA}}\right)^{c_{HA}}}{c_{HA}!}}{\sum_{i=0}^{c_{HA}} \frac{\left(\frac{\lambda_{HA}}{\mu_{HA}}\right)^{i}}{i!}} \quad (5)$$

For the aspect of the fault-tolerant control messages, The existing control messages of the Mobile IPv6 are used to be the fault-tolerant control messages, as follows:

- Binding update to an external HA.
- Binding acknowledgment from an external HA.

The first fault-tolerant control message is for the failure-affected MN to register its binding information with its preferable external HA. The second fault-tolerant control message is the corresponding binding acknowledgment message. As described in Section 3, the failure-affected MN may select the preferable external HA several times until a suitable external HA is met. Therefore, the above two fault-tolerant messages may be issued several times. The probability that a failure-affected MN will send i times the first (second) fault-tolerant control message is

$$(P_{HA\_Failure} + P_{HA\_Overload})^{i-1}(1 - (P_{HA\_Failure} + P_{HA\_Overload})) \quad (6)$$

where $P_{HA\_Failure}$ is the probability that an HA is in the faulty status at an instant of time. $P_{HA\_Overload}$ is the overloading probability.

From (6), we know that the transmission times of the first (second) fault-tolerant control message follow a geometric distribution. Therefore, the average number of sending the first (second) fault-tolerant control messages is:

$$\frac{1}{1 - (P_{HA\_Failure} + P_{HA\_Overload})} \quad (7)$$

From (7), the transmission latency of the issued first (second) control messages can be further inferred as

$$\frac{1}{1 - (P_{HA\_Failure} + P_{HA\_Overload})} \times d \quad (8)$$

where d is the average transmission delay for sending a binding update message (binding acknowledgment message) from an MN (HA) to an HA (MN).

Note that the above fault-tolerant control messages are sent from the failure-affected MN or the HA, not from the OAM center. Unlike the approach of Lin and Arul (2003), the transmission latency of the fault-tolerant control messages is not dependent on the bandwidth of the OAM network. In Lin and Arul (2003), it assumed that the OAM network can provide a high bandwidth for sending the fault-tolerant control messages, and it did not precisely evaluate the transmission latency of the fault-tolerant control messages. In addition, Lin and Arul (2003) also mentioned that the transmission latency of the issued fault-tolerant control messages is mainly dependent on the number of failure-affected MNs due to collecting their binding information. In contrast, the proposed approach can make each failure-affected MN simultaneously send and receive the first and second fault-tolerant control messages to select its preferable external HA as the fault-tolerant HA. The transmission latency of the issued fault-tolerant control messages is independent of the number of the failure-affected MNs.

4.3. Packet recovery overhead

To enable a failure-affected MN to retrieve the undeliverable packets destined to it, the interconnection router and the CN need to track and store the undeliverable packets by using the undeliverable packet list and buffer, respectively (see Section 3.3). The recovery overhead of the undeliverable packets can be measured as the memory spaces used to track and store the undeliverable packets. In Section 3.3, it also mentioned that the undeliverable packets will be retrieved by the corresponding failure-affected MNs whenever they periodically perform a binding update to the faulty HA (see Fig. 7). For an undeliverable packet, its stay time in an undeliverable packet list and that in the undeliverable packet buffer do not excess the interval of the corresponding MN's two binding updates. After the time elapsed, the occupied spaces in the list and buffer can be used to track and store another undeliverable packet. Therefore, the memory spaces (Mem_{UP_List}) required for an undeliverable packet list can be derived from the number of packets sent to the faulty HA during the binding update interval, as follows:

$$Mem_{UP\_List} = Int_{BA} \times \lambda_{Packet\_HA} \times E_{UP\_List} \quad (9)$$

where Int_{BA} is the time interval between two binding updates to the faulty HA, λ_{Packet_HA} is the arrival rate of packets to an HA, and E_{UP_List} is the size (the number of bytes) of an undeliverable packet list entry.

Similarly, the memory spaces (Mem_{UP_Buffer}) required for an undeliverable packet buffer can be also derived from the number of packets sent from a CN to failure-affected MNs during the binding update interval, as follows:

$$\mathrm{Mem}_{\mathrm{UP\_Buffer}} = \mathrm{Int}_{\mathrm{BA}} \times \lambda_{\mathrm{Packet\_CN}} \times P_{\mathrm{UP\_Buffer}} \quad (10)$$

where $\lambda_{\mathrm{Packet\_CN}}$ is the sending rate of packets from a CN, and $P_{\mathrm{UP\_Buffer}}$ is the average size (the average number of bytes) of an undeliverable packet sent from a CN.

5. Comparison

As described in Section 1, the traditional fault-tolerant approaches for Mobile IP are classified into the redundancy-based and redirection-based schemes. The comparison between the two schemes have been made in Lin and Arul (2003). The proposed approach and the approaches of Pack and Choi (2004) and Lin and Arul (2003) belong to the redirection-based scheme. Note that the approach of Pack and Choi (2004) mainly handles the fault tolerance of the MAP. In this section, we make detailed comparisons among the above three approaches, as shown in Table 1. The comparisons are in terms of fault-tolerant support, failure-free overhead, fault-tolerant overhead, fault-tolerant capability, and packet recovery.

- Fault-tolerant support: For the approach of Pack and Choi (2004), the MAP failure is tolerated by assuming that there are two or more MAPs in a network domain. With the aspect of the HA, it clearly indicated that HA contains very important binding information and its fault-tolerant approach should adopt the hardware redundancy. In the approach of Lin and Arul (2003), the OAM center is used to assist the workload redirection of a faulty HA. With the OAM center support, the workload of the faulty HA is distributed to multiple approximate failure-free HAs. As for the proposed approach, the fault tolerance is from the MN's viewpoint. If an HA fails, the failure-affected MNs individually select their preferable failure-free HAs to serve them. The OAM center is not involved to collect the workload of all the HAs for supporting the fault tolerance. In addition, the proposed approach is neither dependent on the hardware redundancy support.

Table 1
Comparison

Comparison Metrics	Approach of [8]		Approach of [9]		Proposed approach	
Fault-tolerant support	MAP	Multiple MAPs in a domain	HA	OAM center	HA	No
	HA	Hardware redundancy				
Failure-free overhead	MAP	One additional binding update	HA	No	HA	Generating the external HA information
	HA	Binding synchronization				
Failure-tolerant overhead	MAP	Binding update execution	HA	OAM assistance Performance degradation, Binding restoration, and Twice tunneling	HA	Performance degradation and Finding the suitable external HA
	HA	Switchover execution				
Fault-tolerant capability	MAP	Number of available MAPs in a network domain	HA	Number of available HAs in the network system	HA	Number of available HAs in the network system
	HA	Number of the redundant HAs in a network domain				
Packet recovery	No		End-to-end TCP		Binding update assistance	

- Failure-free overhead: For the approach of Pack and Choi (2004), an MN chooses two serving MAP while it moves to a foreign network domain. Then, two binding updates are performed to the two MAPs: the primary and secondary MAPs. The secondary MAP is only active when the primary MAP fails. With the HA aspect, its failure-free overhead is the binding synchronization between the primary HA and its redundant HA since the hardware redundancy is used. For the approach of Lin and Arul (2003), it does not take any actions against the HA failure during the failure-free period. For the proposed approach during the failure-free period, it requires to generate an up-to-date external HA information for each MN. The generation of the up-to-date external HA information can be integrated into the binding update. The increasing transmission delay on the binding update is trivial, which will be further validated in Section 6. As for the data structure used for the external HA information, it only takes 18 bits (see Section 3.1: meta-address form).
- Failure-tolerant overhead: For the approach of Pack and Choi (2004), it focuses on the fault tolerance of the MAP, not the HA. For making the secondary MAP take over the faulty primary MAP, each failure-affected MN needs to perform the binding updates to its HA and in communicating CNs for changing its default MAP as the secondary MAP. With the fault-tolerant overhead of the HA, it is determined by the switchover time since the hardware redundancy is adopted to tolerate the HA failure. For the approach of Lin and Arul (2003), the performance of a failure-free HA incurs certain degree degradation since some workload of the faulty HA is redirected to it. However, the workload redirection in the approach of Lin and Arul (2003) is based on the OAM center to issue several OAM control messages (see Section 5.2 of Lin and Arul (2003)). The cost of the issued OAM control messages is not trivial. Especially, the restoration of the faulty HA's binding information involves a lot of time-consuming operations (see Section 5.2 of Lin and Arul (2003)). Another main fault-tolerant overhead for the approach of Lin and Arul (2003) is the twice-tunneling transmission. The twice-tunneling transmission is used to redirect the packet transmission of the faulty HA. It may cause the triangle routing problem to be more serious. In contrast to the above two approaches, the proposed approach neither depends on the OAM center nor the hardware redundancy support. For the fault-tolerant overhead of the HA, its cost includes the performance degradation and the time for finding a suitable external HA, which have been evaluated in Section 4.2 (see Eqs. (5) and (8)).
- Fault-tolerant capability: For the approach of Pack and Choi (2004), its fault-tolerant range is restricted in a network domain. The faulty MAP (HA) can be tolerated by the secondary MAP (the redundant HA) in the same network domain. If no failure-free MAPs (redundant HAs) in the same network domain, the failure-free MAPs (redundant HAs) in other network domains cannot be used to achieve fault tolerance. The approach of Lin and Arul (2003) and the proposed approach have the same fault-tolerant capability. The workload redirection range is extended to the whole network system. If an HA fails, the failure-affected MNs can be served by anyone failure-free HA in the network system. However, the approach of Lin and Arul (2003) cannot be applied to Mobile IPv6 network system since it uses the foreign agent (FA) to assist the binding information restoration, but the FA does not exist in Mobile IPv6.
- Packet recovery: If an HA fails, the packets through it will be lost. The approach of Pack and Choi (2004) does not mention how to retransmit the lost packets. In the approach of Lin and Arul (2003), it clearly indicated that the lost packets due to the HA failure can be recovered only if the end-to-end TCP transmission mode is supported in the MNs and CNs (see Section 2.3 of Lin and Arul (2003)). As for the proposed approach, the recovery

of the lost packets is done by the binding update assistance (see Section 3.3) without relying on the TCP support, which avoids incurring the long recovery latency.

6. Experimental evaluation

To quantify the overhead comparisons among the proposed approach and the approaches of Pack and Choi (2004) and Lin and Arul (2003), we performed simulation experiments which are based on the given Mobile IPv6 module of the Network Simulator version 2 (NS-2) (Mobiwan, 2002). In the simulation environment, a Mobile IPv6 network system with 10 network domains is first deployed. Then, each network domain is equipped with a dedicated HA and three ARs. Among the network domains, the bandwidth and link delay of the backbone network are set to 100 Mbps and 10 ms, respectively. Then, 100 MNs are randomly distributed within the 10 network domains. For the mobility aspect of each MN, it is simulated based on the random waypoint model (Broch et al., 1998). In addition, 10 CNs are also set in the Mobile IPv6 network system to communicate with MNs by sending the consistent bit rate (CBR) traffic. Each CN periodically generates a 512-bytes packet by randomly choosing one of the following three intervals: 0.1 s, 0.05 s, and 0.001 s, and then sends the generated packet to one corresponding MN. Each packet of the CBR traffic adopts the UDP transport protocol. The time of the simulation run is 5000 s. During the simulation time, the HA failure is randomly occurred. In addition, we also perform another simulation run with 5000 s by using TCP traffic. For generating the TCP traffic, each CN performs the FTP application to transmit a data file with a random size to an MN.

In the above two simulation runs, we concern the failure-free overhead, fault-tolerant overhead, and packet recovery overhead. Based on Section 5, we can know that only the packet recovery overhead is dependent on the data traffic type and rate used in simulation experiments. For the failure-free overhead and fault-tolerant overhead, they are independent of the data traffic type and rate used since the two overheads are introduced due to issuing some control messages.

6.1. Overhead for tolerating faulty HA

Fig. 8a shows the comparison of the failure-free overhead. As mentioned above, the fault-tolerant approach of Pack and Choi (2004) for the HA adopts the redundancy-based approach. It needs to perform the binding synchronization during the failure-free period. The binding synchronization will take more time while performing the binding update. Correspondingly, the transmission delay of the binding acknowledgment message also increases. For the approach of Lin and Arul (2003), it does not take any actions against the HA failure during the failure-free period. However, the approach of Lin and Arul (2003) incurs a non-trivial fault-tolerant overhead. In addition, this approach is not really suitable to be used in the Mobile IPv6 network architecture. As for the proposed approach, the failure-free overhead is mainly determined by the number of the external HAs (backup HAs) attached on the binding acknowledgment message. Although the large number of external HAs can enhance the fault-tolerant capability, it also correspondingly increases the transmission delay of the binding acknowledgment message. However, if the addresses of the attached external HAs are represented as the meta-address form, the increasing transmission delay of the binding acknowledgment message is independent of the fault-tolerant capability. In addition, the average value is also very small as 7.7 μs. In Fig. 8a, the three approaches are all based on the heartbeat messages mechanism to detect the HA failure. In Fig. 8b, we also show the introduced failure-free overhead of the heartbeat messages by setting the heartbeat interval from 0.1 to 1 s with a step of 0.1 s. In Hinden (2004), the default heartbeat interval is 1 s. The size of the heartbeat message is set to 64 bytes. As shown in Fig. 8b, even if the heartbeat interval is very small as 0.l s, the bandwidth consumed by the heartbeat messages is 5 Kbps, which occupies 0.005% (5 Kbps/100 Mbps) of total bandwidth. The heartbeat messages introduce a little failure-free overhead.

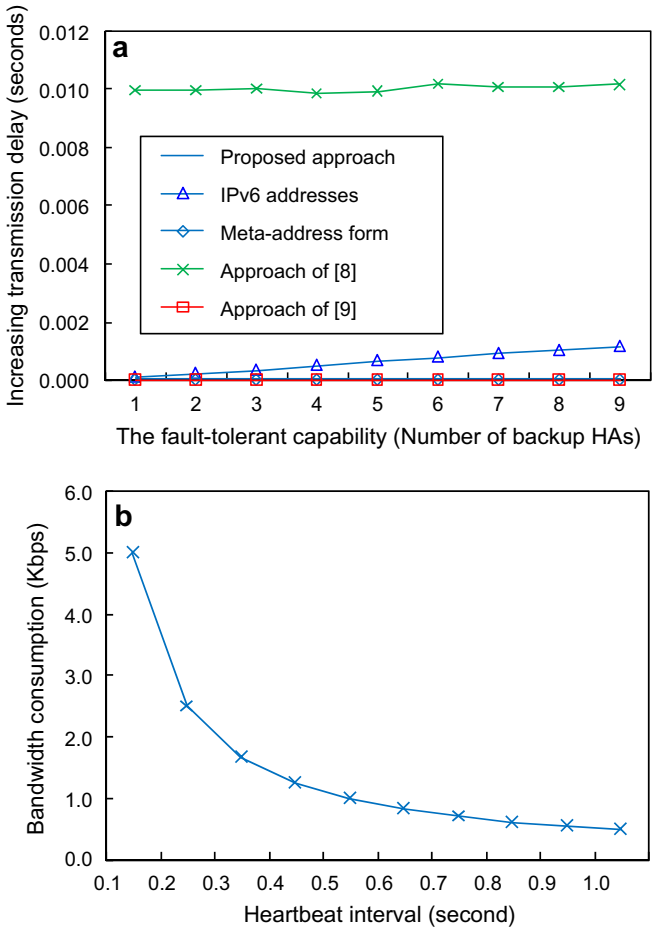


Fig. 8. The failure-free overhead. (a) The comparison. (b) The heartbeat overhead.

The comparison of the fault-tolerant overhead is shown in Fig. 9. As mentioned in Section 4.2, the fault-tolerant overhead concerns the following two sub-metrics: the increasing blocking probability and the transmission latency of the fault-tolerant control messages. In the aspect of the increasing blocking probability (see Fig. 9a), the approach of Pack and Choi (2004) has a very small value since it adopts the redundancy-based scheme to equip a redundant HA for each HA. However, the approach of Pack and Choi (2004) has the expensive hardware cost. For the approach of Lin and Arul (2003) and the proposed approach, they are based on the redirection-based scheme to redirect the workload of the failure-affected MNs to failure-free HAs. However, the approach of Lin and Arul (2003) does not consider the overloading situation. Therefore, the increasing blocking probability in the approach of Lin and Arul (2003) increases as the number of failure-affected MNs increases. Unlike the approach of Lin and Arul (2003), the proposed approach considers the overloading situation. For a failure-free HA, if it has been selected to be the preferable fault-tolerant HA for many failure-affected MNs, it will not act as the fault-tolerant HA for other failure-affected MNs again. Therefore, the increas-

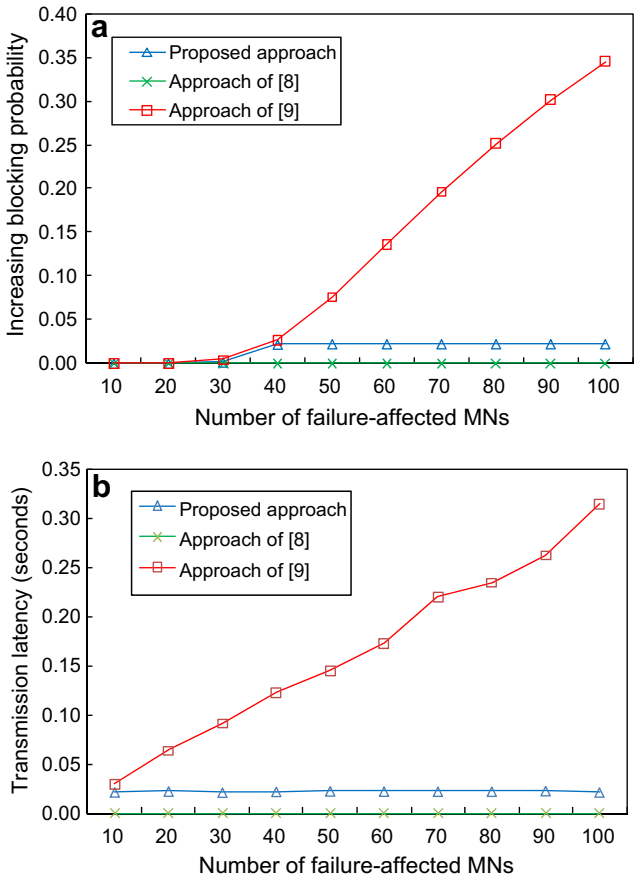


Fig. 9. The comparison of the fault-tolerant overhead. (a) The increasing blocking probability. (b) The latency of the fault-tolerant control message.

ing blocking probabilities are less than a threshold value (e.g. 0.022 in Fig. 9a).

For the other concerned metric of the fault-tolerant overhead, its comparison is shown in Fig. 9b. In the approach of Pack and Choi (2004), the faulty HA is switched over to the corresponding redundant HA by performing the ARP (Address Resolution Protocol). Although the cost of the ARP execution is trivial, the redundancy-based scheme has a limited fault-tolerant capability and an expensive hardware cost. For the approach of Lin and Arul (2003), it performs a complicated fault-tolerant procedure which needs to take more control messages. As for the proposed approach, it can make each failure-affected MN simultaneously select its preferable failure-free HA as its new serving HA. The transmission latency of the fault-tolerant message is independent of the number of the failure-affected MNs, and its average value is 0.02 s.

In addition, the proposed approach can make each failure-affected MN select its neighboring HA as its preferable fault-tolerant HA. To enhance this advantage, we further perform the comparison of the packet transmission latency through the fault-tolerant HA, as shown in Fig. 10. The proposed approach can provide the smallest packet transmission latency due to selecting the preferable fault-tolerant HA. For the approach of Pack and Choi (2004), the fault-tolerant HA is the equipped redundant HA of the faulty HA. The packet transmission latency through the fault-tolerant HA is nearly same as that before the HA failure. As for the approach of Lin and Arul (2003), the fault-tolerant HA is randomly selected from the failure-free HAs, the packet transmission latency has the largest value.

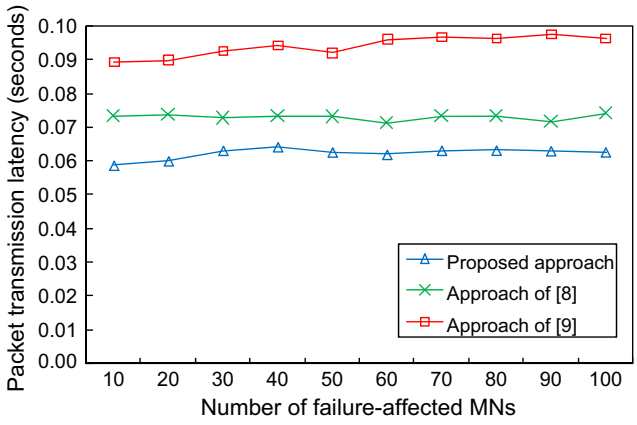


Fig. 10. The average packet transmission latency through the fault-tolerant HA.

6.2. Overhead for recovering lost packets

As for the packet recovery, Pack and Choi (2004) and Lin and Arul (2003) do not consider this issue in their fault-tolerant approaches. Fig. 11 only shows the packet recovery overhead of the proposed approach. As mentioned in Section 4.3, the packet recovery overhead is in terms of the sizes of the undeliverable packet list and buffer. As shown in Fig. 11, when adopting the CBR traffic, the both sizes increase as the binding update interval increases. The undeliverable packet buffer is larger than the undeliverable packet list since it is required to store the whole contents of the undeliverable packets. As mentioned in Section 3.3, the undeliverable packets due to the HA failure can be retrieved later from relative CNs when performing a binding update. Therefore, if there is a large interval between two binding updates, more undeliverable

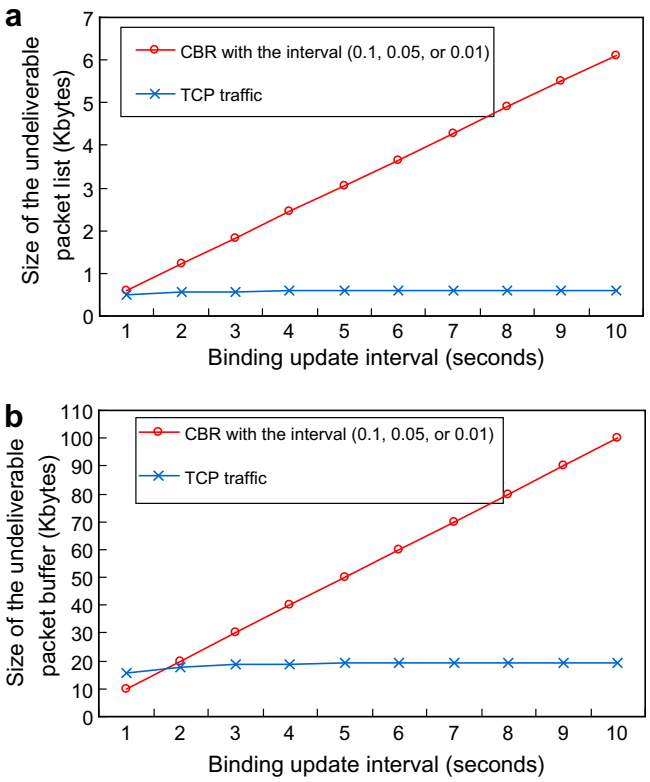


Fig. 11. The packet recovery overhead. (a) The size of an undeliverable packet list. (b) The size of an undeliverable packet buffer.

packets are generated during the binding update interval. Correspondingly, the undeliverable packet list and buffer need more memory spaces to track and store the undeliverable packets, respectively. In Mobile IPv6, the binding update interval is set between 1 and 10 s (Paik et al., 2004). From Fig. 11, we can see that the sizes of the undeliverable packet list and buffer (6.1 Kbytes and 100.0 Kbytes) in the CBR traffic are not large even if the binding update interval is set to 10 s.

When the TCP traffic is adopted in simulation experiment, the sizes of the undeliverable packet list and buffer are independent of the binding update interval. The reason is explained as follows: In the TCP protocol, it has the flow control and congestion control mechanisms which set a window to limit the number of sending packets. In the simulation experiments, the window size is set to 20 packets, which refers to the TCP module of Network Simulator version 2 (NS-2) (Mobiwan (2002)). Therefore, the maximum number of undeliverable packets is 20. Correspondingly, the maximum sizes of the undeliverable packet list and buffer are 0.6 Kbytes (20 packets $\times$ 32 bytes/per packet list entry) and 20 Kbytes (20 packets $\times$ 1 Kbytes/per packet), respectively.

7. Conclusion

This paper has presented an efficient approach to tolerating the HA failure in a Mobile IPv6 network system. The proposed approach is based on the home address regeneration to make each failure-affected MN be served by its preferable failure-free HA. Unlike the redundancy-based approaches (Ghosh and Varghese, 1998; Ahn and Hwang, 2001; Cisco Co. Ltd., 2002; Faizan et al., 2005, 2006), redundant HAs are not required to be equipped. Compared to the previous workload-redirection-based approaches (Pack and Choi, 2004; Lin and Arul, 2003), the proposed approach is more suitable to be used in the Mobile IPv6 network system since it is neither dependent on the hierarchical network architecture nor dependent on a centralized information provider (the centralized OAM center).

Furthermore, the proposed approach also considers how to recover the lost packets due to the HA failure. The packet recovery is not burdened on the TCP layer to avoid incurring long recovery latency. Finally, we performed simulations to evaluate the overheads for tolerating the faulty HA and recovering the lost packets. The simulation results show that the two overheads are small.

In addition to the fault tolerance, the security issue is also important for the Mobile IPv6 network. The proposed fault-tolerant approach is based on the Mobile IPv6 security mechanism. It is our future work for providing a more secure environment for the Mobile IPv6 network.

References

Ahn, J.H, Hwang, C.S., 2001. Efficient fault-tolerant protocol for mobility agents in Mobile IP. In: Proc. 15th Int'l Parallel and Distributed Processing Symp., 2001, pp. 1273–1280.

Broch, J., Maltz, D.A., Johnson, D.B., Hu, Y.-C., Jetcheva, J.G., 1998. A performance comparison of Mmulti-hop wireless ad hoc network routing protocols. In: Proc. ACM Int. Conf. Mobile Computing Networking (MOBICOM), pp. 85–97.

Cisco Co. Ltd., 2002. Mobile IP home agent redundancy. Available from <http://www.cisco.com/en/US/products/sw/iosswrel/ps1830/products_feature_guide09186a0080 087846.html>.

Conta, A., Deering, S., Gupta, M. (Eds.), 2006. Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6). RFC 4443.

Deering, S., Hinden, R., 1998. Internet protocol, Version 6 (IPv6) specification. RFC 2460.

Faizan, J., El-Rewini, H., Khalil, M., 2005. VHARP: Virtual home agent reliability protocol for Mobile IPv6 based networks. In: Proc. International Conf. on Wireless Networks, Communications, and Mobile Computing, Wireless Com 2005, Hawaii, USA.

Faizan, J., El-Rewini, H., Khalil, M., 2006. Introducing reliability and load balancing in home link of Mobile IPv6 based networks. In: Proc. of IEEE International Conference on Pervasive Services – ICPS 2006, Lyon, France.

Fathi, Hanane, Shin, SeongHan, Kobara, Kazukuni, Chakraborty, Shyam, Imai, Hideki, Prasad, Ramjee, 2005. Leakage-resilent security architecture for Mobile IPv6 in wireless overlay networks. IEEE Journal on Selected Areas in Communications (J-SAC) 23 (11), 2182–2193.

Ghosh, Rajib, Varghese, George, 1998. Fault-Tolerant Mobile IP. Washington University Technical Report WUCS-98-11, 1998.

Gross, D., Harris, C.M., 1985. Fundamentals of Queueing Theory. John Wiley & Sons Inc..

Hinden, R. (Ed.), 2004. Virtual router redundancy protocol (VRRP). RFC 3768.

Hinden, R., Deering, S., 2006. IP Version 6 addressing architecture. RFC 4291.

Jelger, C., Noel, T., 2005. Proactive address autoconfiguration and prefix continuity in IPv6 hybrid ad hoc networks. IEEE SECON 2005, 107–1175.

Johnson, D., Perkins, C., 2004. Mobility support in IPv6. RFC 3775.

Kent, S., Seo, K., 2005. Security architecture for the internet protocol. RFC 4301.

Khalil, M., 2002. Virtual distributed home agent protocol (VDHAP). US Patent 6 430 698.

Kuo, Jen-Hao, Te, Siong-Ui, Liao, Pang-Ting, Huang, Chun-Ying, Tsai, Pan-Lung, Lei, Chin-Laung, Kuo, Sy-Yen, Huang, Yennun, Tsai, Zsehong, 2005. An evaluation of the virtual router redundancy protocol extension with load balancing. In: IEEE 11th Pacific Rim International Symposium on Dependable Computing, Changsha, Hunan, China.

Li, T., Cole, B., Morton, P., Li, D., 1998. Cisco Hot Standby Router Protocol (HSRP).

Lin, Jenn-Wei, Arul, Joseph, 2003. An efficient fault-tolerant approach for Mobile IP in wireless systems. IEEE Transactions on Mobile Computing.

Lu, Weidong, Lo, Anthony, Niemegeers, Ignas, 2005. Session mobility support for personal networks using Mobile IPv6 and VNAT. In: Fifth Workshop on Applications and Services in Wireless Networks (ASWN'05), Paris, France.

Mobiwan, 2002. ns-2 extensions to study mobility in Wide-Area IPv6 Networks. Available from <http://www.inrialpes.fr/planete/pub/mobiwan>.

Narten, T., Draves, R., 2001. Privacy extensions for stateless address autoconfiguration in IPv6. RFC 3041.

Pack, Sangheon, Choi, Yanghee, 2004. Performance analysis of robust hierarchical Mobile IPv6 for fault-tolerant mobile services. IEICE Transactions on Communications E87-B (5), 7.

Paik, Eun Kyoung, Cho, Hosik, Ernst, Thierry, Choi, Yanghee, 2004. Design and analysis of resource management software for in-vehicle IPv6 networks. IEICE Transactions on Communications E87-B (7).

Plummer, D.C., 1982. Ethernet address resolution protocol: or converting network protocol addresses to 48.bit ethernet address for transmission on ethernet hardware. RFC 826.

Ren, Kui, Lou, Wenjing, Zeng, Kai, Bao, Feng, Zhou, Jianying, Deng, Robert H., 2006. Routing optimization security in mobile IPv6. Computer Networks 50 (13), 2401–2419.

Soliman, Hesham, 2004. Mobile IPv6 Mobility in a Wireless Internet, Addison-Wesley.

Srivastava, S., 2003. Redundancy management for network devices. In: The 9th Asia-Pacific Conference On, pp. 1157–1162.

Takahashi, Takeshi, Harju, Jarmo, Tominaga, Hideyoshi, 2003. Handover management in wireless networks based on buffering and signaling. In: Nineth EUNICE Open European Summer School and IFIP Workshop on Next Generation Networks, Budapest, Hungary.

Touch, J., 1995. Report on MD5 performance. RFC 1810.

Jenn-Wei Lin received the M.S. degree in computer and information science from National Chiao Tung University, Hsinchu, Taiwan, in 1993, and the Ph.D. degree in electrical engineering from National Taiwan University, Taipei, Taiwan, in 1999. He is currently an Associate Professor in the Department of Computer Science and Information Engineering, Fu Jen Catholic University, Taiwan. He was a researcher at Chunghwa Telecom Co., Ltd., Taoyuan, Taiwan from 1993 to 2001. His current research interests are fault-tolerant computing, mobile computing and networks, and distributed systems.

Ming-Feng Yang received the M.S. degree in the Department of Computer Science and Information Engineering from Fu Jen Catholic University in 2005, and is currently working towards Ph.D. degree in the Graduate Institute of Applied Science and Engineering at Fu Jen Catholic University. His current research interests are fault-tolerant computing, mobile computing and networks.