Fault Tolerant Distributed and Fixed Hierarchical Mobile IP

Paramesh C. Upadhyay*, and Sudarshan Tiwari**
*Deprtment of Electronics & Communication Engineering
Sant Longowal Institute of Engineering & Technology
Longowal-148106, INDIA
E-mail: pcu_001@yahoo.co.uk
**Deprtment of Electronics & Communication Engineering
Motilal Nehru National Institute of Technology
Allahabad-211004, INDIA
E-mail: stiwari@mnnit.ac.in

Abstract: *To several mobility management protocols proposed for IP-based mobile networks, fault tolerance aspect of mobility agents is a primary requirement to sustain continuous service availability to the mobile hosts. For a localized or micro- mobility management solution, the local mobility agent i.e. gateway is a single point of failure because it is responsible for enforcing the signaling and data packets in its domain. Such failures may severely disrupt the communications among the failure-affected users. The problem becomes even more severe for mobility agents in a distributed mobility management scheme with overlapping registration areas.*

This paper proposes a fault tolerance scheme for Distributed and Fixed Hierarchical Mobile IP (DFHMIP) and evaluates its performance in terms of data transmission cost and blocking probability.

Keywords: *DFHMIP, Fault tolerance, micro-mobility.*

******Corresponding Author*

1. Introduction

During last decade, the mobile communications and Internet technologies have gained tremendous popularity among the users throughout the world. This has led towards the convergence of mobile communications and Internet technologies together so as to achieve their fullest advantages. Mobile IP (MIP) [1] is a base protocol for IP mobility that uses home agents (HA) and foreign agents (FA) as mobility agents to facilitate mobility in IP-based mobile networks. However, MIP is not suitable for fast mobility users, as it incurs high signaling burden on the network and results in longer handover delay for mobile hosts (MH) staying away from their HA. Several micro-mobility protocols, centralized [2, 3, 4] and distributed [5, 6], have been proposed in literature to alleviate the inherent limitations of Mobile IP.

Fault tolerance of mobility agents in IP-based mobile networks is an important issue to be addressed. The failure of a mobility agent interrupts the communications among the affected users. Therefore, the researches in the field of fault tolerant IP mobility management schemes have gained substantial momentum during the past decade. For a localized or micro- mobility management solution, the local mobility agent i.e. gateway is a single point of failure because it is responsible for enforcing the signaling and data packets in its domain. Such failures may severely disrupt the communications among the failure-affected users [7]. The problem becomes even more severe for

10.5121/iju.2010.1204

mobility agents in a distributed mobility management scheme with overlapping registration areas. In this paper, a fault tolerance scheme is suggested for such a mobility management scheme, Distributed and Fixed Hierarchical Mobile IP (DFHMIP). The performance metrics for this scheme include signaling cost, blocking probability, and data transmission cost. To the best of knowledge, this is the first work for fault tolerant distributed mobility management solution having overlapping registration areas.

This paper is structured in following way. Section 2 is dedicated to related works in the arena of fault tolerance. In section 3, an overview of DFHMIP is presented. Section 4 explains the proposed fault tolerance scheme for DFHMIP, and mathematical model for the proposition is developed in section 5. Performance analysis has been carried out in section 6 and, finally, section 7 gives concluding remarks on this proposal.

2. Related works

In Mobile IP, HAs and FAs are single points of failure and potential bottlenecks. If a HA crashes it can lead to communication failure if the mobile is away from home. Fault tolerance for IP-based mobile networks is relatively new topic and only few proposals are available in literature. Most of them focus on fault tolerance for MIP. These schemes suggest maintaining a dedicated back-up or a secondary mobility agent for each primary mobility agent (i.e. HA or FA), which takes over when later fails to work. Such schemes suffer from two drawbacks. First, back-up mobility agents need to be updated, leading to increase in signaling cost. Second, maintaining a back-up mobility agent for each primary agent results in higher system cost.

HARP [8] is an optional extension to Mobile-IP to address the fault tolerance of home agents. It is a simple protocol based on the notion of one or more HARP peers that act as a single shared Home Agent. Each HARP peer is configured with information about its HARP peers and forwards any Mobile-IP registration messages it receives to its peers. HARP peers act in parallel to create or delete tunnels to the Mobile Node's remote COA according to the last registration message received.

In [9], authors propose fault tolerance mechanisms which allow multiple redundant home and foreign agents in the network. In the event of failure, these agents takeover from each other and split load balancing among them. The primary HA (FA) forwards the registration messages received from an MH to its peer HAs (FAs) and sends the registration reply message to the MH only after receiving acknowledgement messages from its peers. This makes the registration delay longer when the number of MHs is large and they are highly mobile.

The fault tolerance schemes for Mobile IP can also be found in [10, 11]. H. Omar et al [12] have proposed a fault tolerance scheme for the failure of any of the FAs along the path between the root FA and the leaf FA in HMIP.

In [13]**,** the authors suggested a novel protocol with multiple mobile agents (MA) where only double mobility bindings are maintained in the whole system. When an HA fails, its backup HA can takeover in a short time without fetching the bindings from other places. Besides, authors also consider the load balancing between these HAs during HA takeover and recovery. Simulation results show that this method has less registration overheads, better MH scalability, less sensitivity on MH mobility, more fault tolerance robustness, and less takeover time than others.

The efficient fault tolerance scheme presented in [14] attempts to overcome these drawbacks. But, remapping of failure-affected radio access networks (RANs) seems to be inappropriate for large mobile networks because, to avoid the disruption in service during the failure, the RANs may be connected with FAs, which are at very long distances. In such situations, if the frequent packets arrive for a mobile host, it may cause large data transmission delay. It is undesirable from the user viewpoint. The situation will even worsen with increasing call arrival rate. A similar approach is available in [15] also.

3. An Overview of DFHMIP

DFHMIP [16], like MIP, uses two mobility agents, viz. Home Agent (HA) and Foreign Agent (FA), to make user mobility possible from one subnet to another in the network. Each mobile host is permanently registered with a subnet where it started its mobility services first time. This subnet is called the home subnet of the host. Any other subnet in the network is a foreign subnet for the host. The HA, located at the home subnet, assigns a permanent IP address to the MH, called its home address. Similarly, when a mobile host leaves its home subnet and enters a foreign subnet, the FA, located at the foreign subnet assigns a temporary address, also known as care-of-address (CoA) of the host. The proposed scheme is based on having neighbors' information, wherein each FA is assumed to be aware of the IP addresses of its neighboring FAs.

The FA_x is said to be the neighbor of FA_y if a mobile host moves from area covered by FA_x to another area covered by FA_y. This means that the neighbors are located at a single hop-distance only. The neighboring information of each FA is assumed to have been embedded in the FA advertisement messages. This assumption does not have significant impact on data rate in the network [17]. Also, unlike the scheme proposed in [18] wherein the entire domain list is broadcast in the coverage area of an AR through the advertisement messages, in our proposed scheme, each FA broadcasts the list of neighboring FAs only in its coverage area. An MH, residing in the coverage area of the FA, listens the advertisement messages, and uses it solely to decide if a registration is necessary.

An FA, in this proposal, can concurrently work in three modes of operation: a Gateway FA (GFA), a Regional FA (RFA), or simply as an FA. The FA acts as a GFA whenever a mobile host requests it to perform a registration with its HA. This registration is termed as a macro-registration. Having performed a macro-registration, a mobile host can freely roam from one subnet to another until the next macro-registration is requested with the visiting FA of the mobile host. At this moment, the visiting FA of the mobile host becomes its new GFA. The group of the subnets, wherein a mobile host can move without a macro-registration, constitutes a registration area, called as macro-registration area (MacRA). The GFA resides at the center of a MacRA and any two consecutive MacRAs overlap with each other. The size of a MacRA is subnet or FA-specific rather than the user-specific.

A MacRA consists of a number of FA-specific smaller regions. These FA-specific regions are called micro-registration areas (MicRA). In fact, each FA is surrounded by its neighboring FAs, with the FA being at the center. This FA together with its neighboring FAs constitutes MicRA. The center FA acts as an RFA for itself as well as for the neighboring FAs. Thus, the size of MicRA depends upon the number of neighboring FAs only. When a mobile host leaves a MicRA, the visiting FA becomes its new RFA, and a new MicRA is formed. This makes two successive MicRAs overlapping with each other. When a mobile host changes its MicRA, it registers with its GFA via its RFA. This registration is called a micro-registration. A host can move in its MicRA without any registration with the GFA. Thus, the movement of a mobile host within MicRA is transparent to its GFA. Based on the algorithm given in [16], a mobile host can decide to perform a macro, micro, or a local registration.

When a mobile host registers an FA as an RFA, the registered FA and its neighboring FAs simply act as FAs for the host. While moving from one FA to another within the MicRA, the host registers with its RFA locally. This registration is referred as a local registration. Note that when a host registers an FA as a GFA, at that moment, the registered FA behaves like the GFA, RFA, and the

FA for the mobile host. Similarly, if the host registers an FA, other than the GFA, as its RFA, the registered FA acts as an FA for the host, as well.

A macro-registration is performed at MacRA level, a micro-registration at MicRA level, and a local registration at subnet level. Thus, the scheme uses three level hierarchies in the network, the GFA being at the highest level, RFA at the intermediate level, and the FA at the lowest level. The size of a MacRA or a MicRA for all the mobile hosts using same FA as a GFA or a RFA, respectively, is fixed. The traffic load in the network is evenly distributed at each FA. Therefore, the scheme has been given a name: Distributed and Fixed Hierarchical Mobile IP, abbreviated as DFHMIP. The formation of overlapping MacRAs and MicRAs with host movement is shown in Figure 1.

Each FA maintains three visitor lists namely, GFA visitor list, RFA visitor list and FA visitor list to keep location records of each mobile host at its GFA, RFA and an FA, respectively. The packets intended for a mobile host are first intercepted by the HA, which then tunnels them to the GFA. The GFA forwards these packets to the RFA, which forwards them to the mobile host via itself or through one of its neighboring FAs, if necessary.

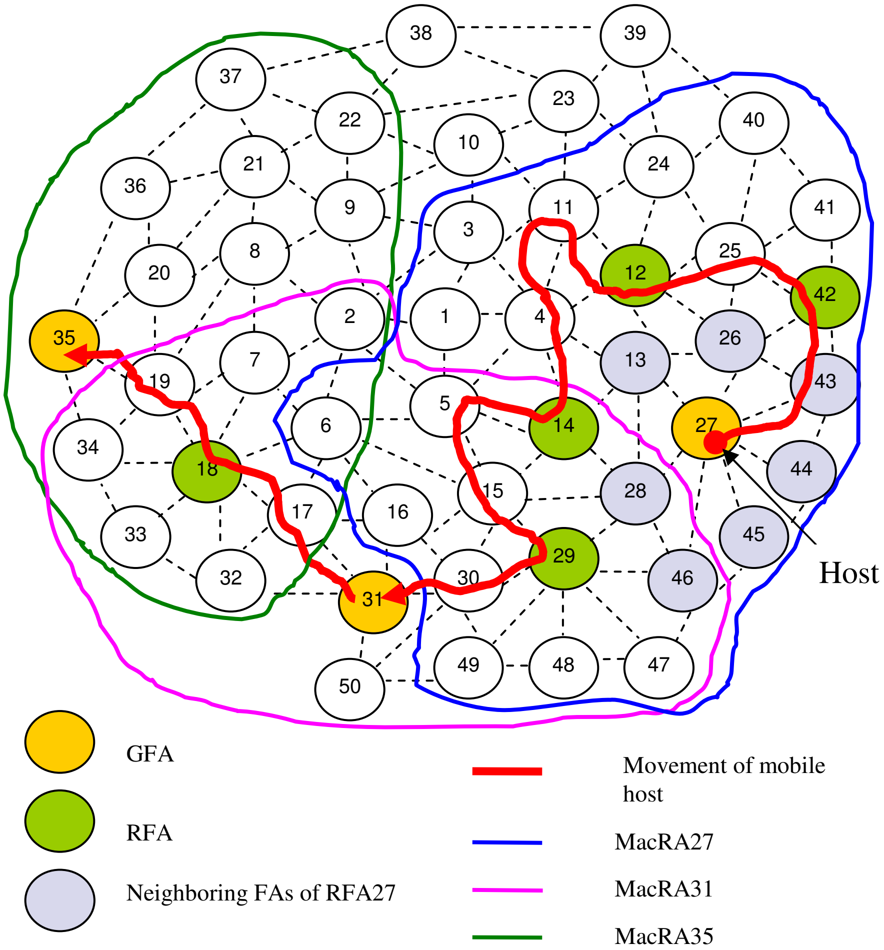


Figure 1. Formation of overlapping Macro- and Micro-registration areas

A MacRA, in proposed DFHMIP, can be considered as consisting of four layers namely, layer 0, layer 1, layer 2, and layer 3, as shown in Figure 2. Layer 0 consists of a single FA only, and lies in the interior most vicinity of a MacRA. This FA is referred as a GFA. A mobile host performs a macro-registration in two situations. First, when it moves to an FA at layer 4 and second, when it moves to an FA at layer 3 and finds that it has changed its MicRA. Under both the circumstances, the visiting FA becomes the new GFA of the host, and a new MacRA is formed. A mobile host experiences a change of MicRA or RFA at an FA in layer 3 only when it's current RFA is located at either layer 1 or layer 2. This is due to the fact that, in proposed DFHMIP, the layer 3 FAs in a MacRA can act as general FAs only.

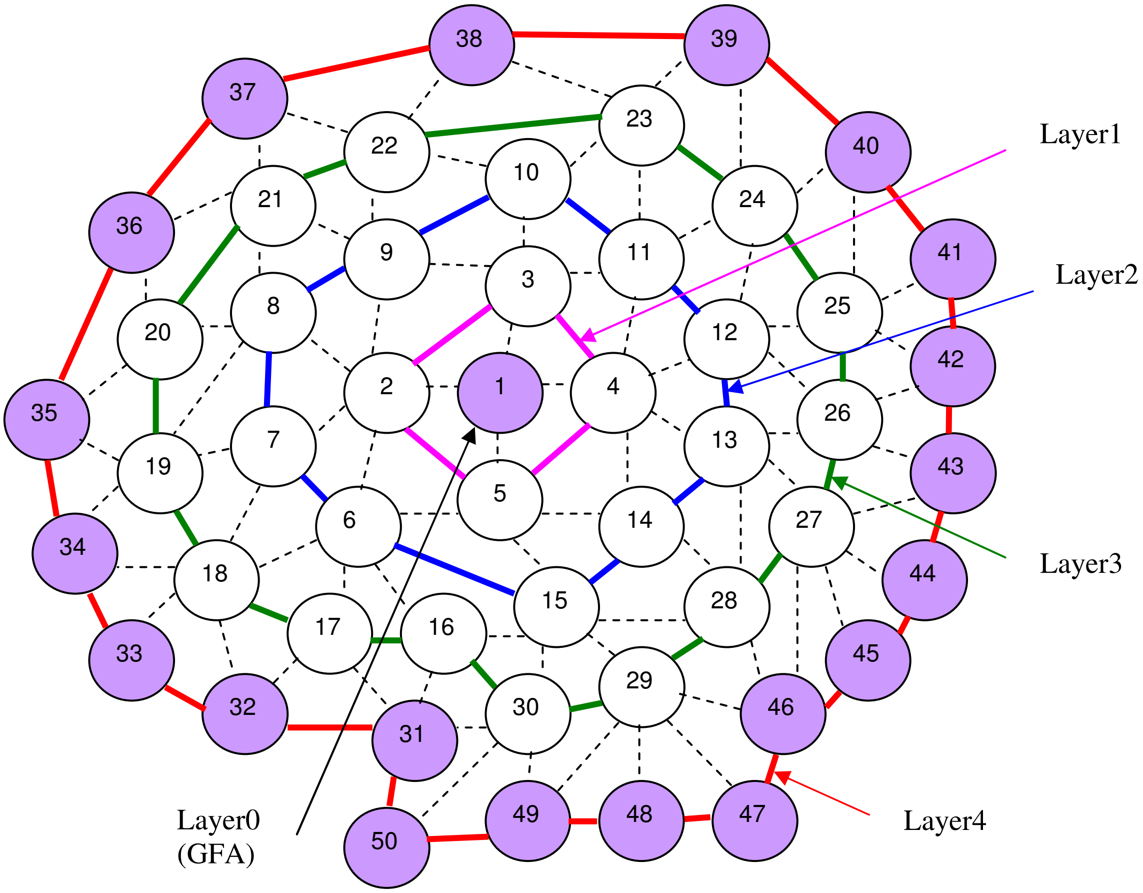


Figure 2. Layered network architecture for DFHMIP

To implement DFHMIP, each mobile host maintains three buffers R_1, R_2 and R_3, for storing the IP addresses from GFA, RFA and FA, respectively. Now onwards, these IP addresses are referred as an identifier of a GFA, RFA and an FA, respectively. A GFA identifier consists of IP addresses of GFA and its neighboring FAs. Similarly, the RFA identifier includes the IP addresses of RFA and its neighboring FAs, and the FA identifier is the IP address of the visiting FA and those of its neighboring FAs. A mobile host receives these identifiers from advertisement messages from its GFA, RFA and FA, respectively. When a mobile host enters a foreign subnet, it uses following steps to perform a macro-registration, a micro-registration, or a local registration:

1. The host listens the FA identifier from the agent advertisement messages from the visiting FA, and stores in its buffer R_3 .
2. The visiting FA becomes the GFA and RFA of the mobile host. In this particular case, the GFA, RFA, and FA identifiers are same. Therefore, the FA identifier, in buffer R_3, is copied into the buffers R_1 and R_2 , i.e.
$$R_1 \xleftarrow{identifier} R_3 ; \qquad R_2 \xleftarrow{identifier} R_3$$
3. At each subnet crossing, the visiting FA identifier and previous FA identifier have at the most 4 IP addresses in common. Therefore, the mobile host computes $R_1 \cap R_2$ and $R_2 \cap R_3$.
4. IF $R_2 \cap R_3 \geq 4$ and $R_1 \cap R_2 \neq \{\}$, then local-registration occurs. Here, $\{\}$ represents a null set.
5. IF $R_2 \cap R_3 < 4$ and $R_1 \cap R_2 \neq \{\}$, a micro-registration occurs. At this moment, visiting FA becomes, the new RFA. Therefore, the FA identifier, in buffer R_3, is copied to buffer R_2 , i.e.
$$R_2 \xleftarrow{identifier} R_3$$
6. ELSE IF $R_1 \cap R_2 = \{\}$, then macro-registration takes place.
7. Go To step 1.

4. Proposed Fault Tolerance Scheme for DFHMIP

4.1 System Description

The following assumptions are made for the fault tolerance scheme for DFHMIP:

- The HA of a mobile host is failure-free and faults may occur at FAs only as a failure-free HA is necessary for user authentication.
- Only single fault occurs in a MacRA at a particular time, as the probability of occurrence of multiple faults in the same MacRA is very less.
- The mobile hosts registered at a GFA are uniformly distributed among the underlying RFAs.

The failure of an FA, in DFHMIP, can be noticed in the same way as the user movement is detected in Mobile IP. In Mobile IP, the movement detection that a mobile host has crossed a subnet boundary is made in either of the two ways: first, when the host's registration lifetime expires, and second, when it receives no agent advertisement messages from its registered FA. The registration timeouts are, generally, higher (usually, 2-3 minutes) than the agent advertisement intervals, which is of the order of few seconds only [9]. Therefore, DHMIP primarily considers FA advertisement messages to detect the failure of an FA in seconds. In addition, a mobile host can, also, detect the failure of its registered FA under any of the following conditions:

(i) If a mobile host requests its registered FA for a local, micro or macro registration and it does not receive any response from the FA.
(ii) If the HA sends data packets to the failure-affected FA, when it acting in GFA mode.
(iii) If mobile hosts attempt to send the packets via its registered FA and the FA does not respond due to failure.

When a fault occurs at an FA, this FA is considered to be located at layer0. This faulty FA is referred to as FA0. As FA0 fails, its other two functionalities i.e. GFA and RFA are also failure-affected. The faulty GFA and RFA are called as GFA0 and RFA0 respectively. For GFA0, any of the FAs at layer0, layer1, and layer2 can act as RFA. Thus, the mobile hosts that have registered GFA0 as a gateway may stay with any of the RFAs at layer0, layer1, and layer2, as shown in Figure

3(a). These RFAs can be classified into two categories. One is RFA0 located at layer0, and the other belongs to that of failure-free RFAs located at layer1 and layer2. The failure-free RFAs are called as healthy RFAs.

Further, due to overlapping nature of MacRAs, the RFA0 acts as an RFA not only for GFA0, but also for all GFAs located at layer0, layer1, and layer2. Considering layer0 GFA i.e. GFA0 as faulty and GFAs at layer1 and layer2 as healthy GFAs, the mobile hosts in DFHMIP scheme arrive at RFA0 from both faulty and healthy GFAs. The mobile hosts that register RFA0 as an RFA are characterized in two ways. First belongs to mobile hosts which stay with FA0 i.e. RFA0 itself, and second is that of the mobile hosts, which have moved to neighboring FAs of RFA0 i.e. layer1 FAs. These FAs are referred to as healthy FAs. It is to be noted that FA0 acts as an FA not only for RFA0, but also for RFAs at layer1. The flow diagram for mobile hosts from/to different category of GFAs, RFAs, and FAs is shown in Figure 3.

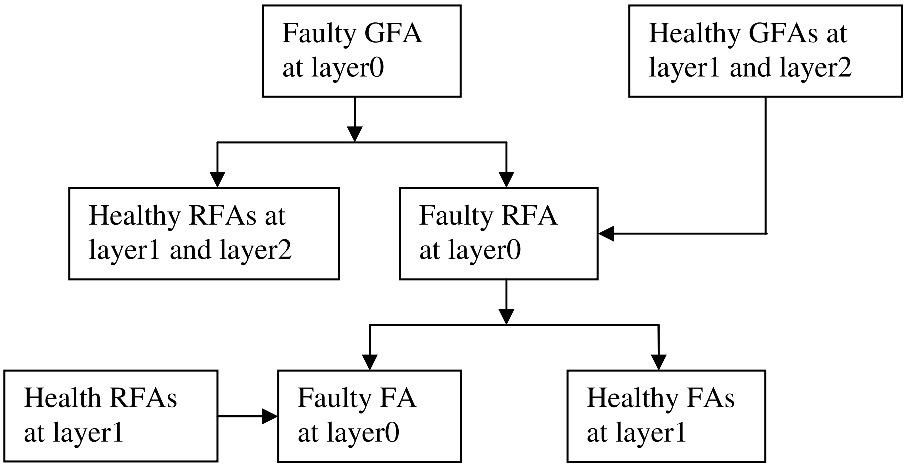
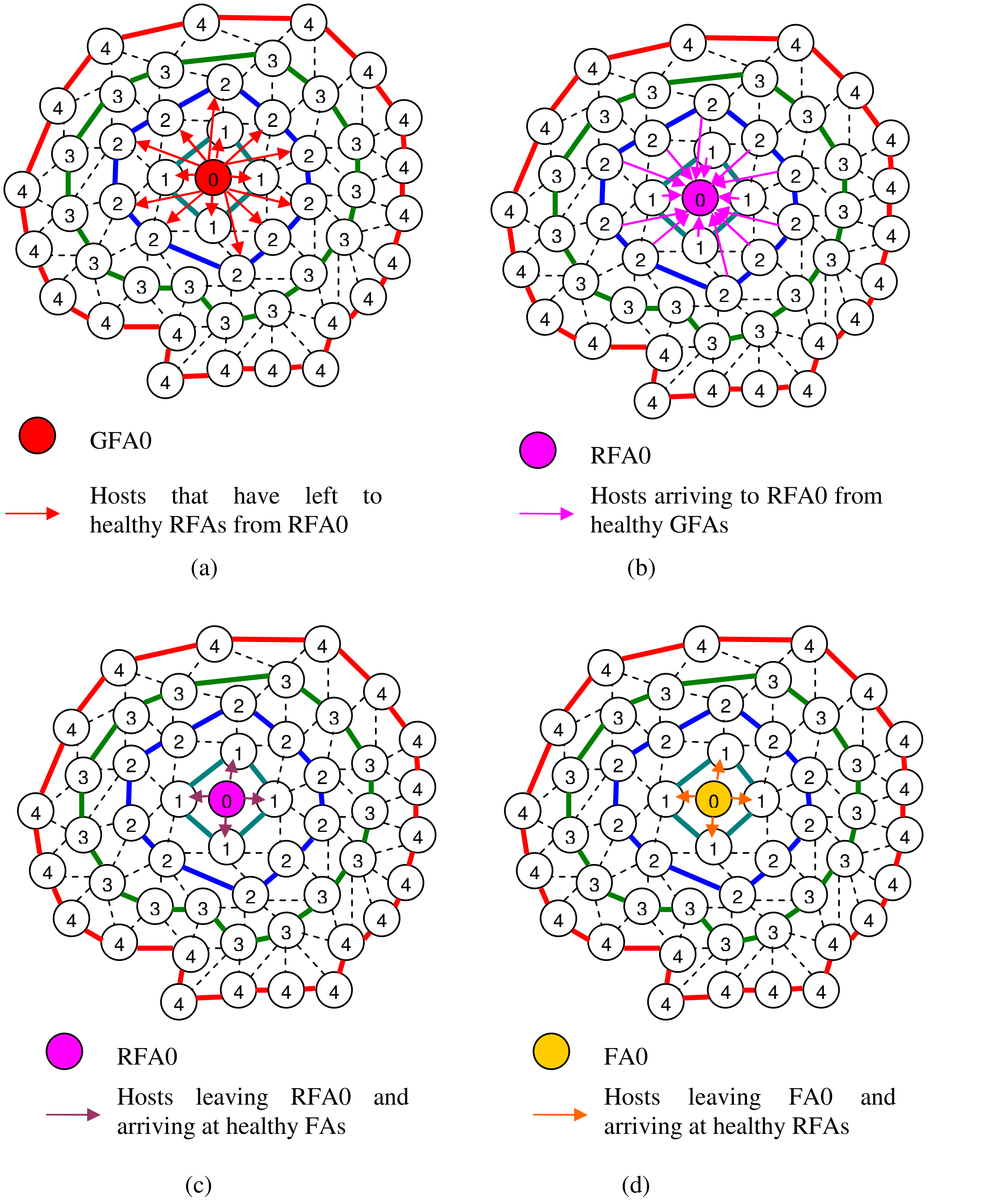


Figure 3. Flow diagram for mobile hosts from/to different category of GFAs, RFAs, and FAs

The pictorial view of different categories of mobile hosts is shown in Figures 4.(a)-(d).


GFA0
Hosts that have left to healthy RFAs from RFA0
RFA0
Hosts arriving to RFA0 from healthy GFAs
RFA0
Hosts leaving RFA0 and arriving at healthy FAs
FA0
Hosts leaving FA0 and arriving at healthy RFAs

(a)

(b)

(c)

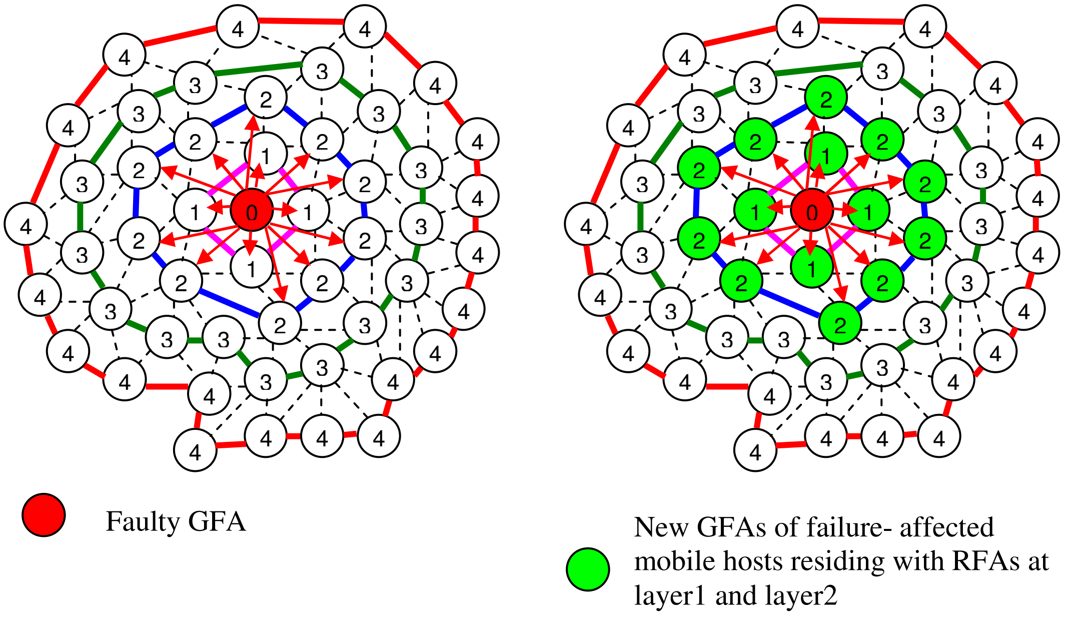
(d)

Figure 4. (a) Healthy RFAs at layer1 and layer2 for GFA0; (b) Healthy GFAs at layer1 and layer2 for RFA0; (c) Healthy FAs at layer1 for RFA0; (d) Healthy RFAs at layer1 for FA0.

4.2 Fault tolerance of a foreign agent

The GFA0 can neither receive data packets from the HAs of failure-affected mobile hosts, nor can it forward them to the registered RFAs of the hosts. Therefore, the mobile hosts that have registered GFA0 as a gateway need to be assigned new GFA(s) so as to maintain continuous packet delivery to them.

The fault tolerance of GFA0, having healthy RFAs, can be achieved by reconfiguring the visitor lists of healthy RFAs. The healthy RFAs add the entries of the failure-affected mobile hosts from respective RFA visitor lists to their GFA visitor lists. Then, these RFAs become the new GFAs for the hosts residing with each of them, as shown in Figure 5. This requires that the new GFAs should perform macro-registrations for the failure-affected hosts. Thus, the HAs of the hosts become aware of their new GFAs. The HAs of the affected hosts will tunnel all the future data packets to new GFAs for their successful delivery. Note that this does not pose any additional traffic burden on healthy RFAs, as these were already serving the failure-affected hosts prior to failure had occurred at the GFA. The overhead involved in this process is the increased signaling cost due to macro-registrations.


Faulty GFA
New GFAs of failure- affected mobile hosts residing with RFAs at layer1 and layer2

(a)

(b)

Figure 5. Allocation of new GFAs to the hosts with faulty GFA (GFA0), but healthy RFAs

To attain the fault tolerance of RFA0, it should be recalled that the mobile hosts to RFA0 reach from faulty GFA0, and the healthy GFAs of RFA0. For the mobile hosts registered at RFA0, and having GFA0 as gateway, it is necessary that a new gateway(s) should be assigned to them to facilitate packet delivery from their respective HAs. Such hosts may either be staying with FA0 or with healthy FAs. For the mobile hosts, residing with healthy FAs, it is proposed that their corresponding FAs should act as new RFAs and GFAs for them. These FAs add the entries of their respective hosts from their FA visitor list to their RFA and GFA visitor lists. These hosts perform macro-registrations with their HAs to make them aware of new GFAs. Assigning new GFAs to the hosts that have arrived at healthy FAs from RFA0 with GFA0 is shown in Figure 6. It should be noted this transformation will not increase any extra traffic burden on the FAs, as these hosts were already registered at the FAs and were getting the services from them only.

On the other hand, for the mobile hosts residing with FA0, achieving fault tolerance of FA0 is a little cumbersome. To accomplish this, a system-initiated handoff, similar to [14], is proposed. The system-initiated handoff is used to redirect the workload of faulty FA0 to selected failure-free FAs. However, it does not change the location of failure-affected mobile hosts. In this approach, failure-affected mobile hosts are virtually moved to serving areas of the selected failure-free FAs. These FAs add the entries in their GFA, RFA, and FA visitor lists for the mobile hosts that have been redirected to them. The FAs, then, perform macro-registration for the hosts, redirected to them, with their respective HAs to make them aware of new GFAs of the hosts.

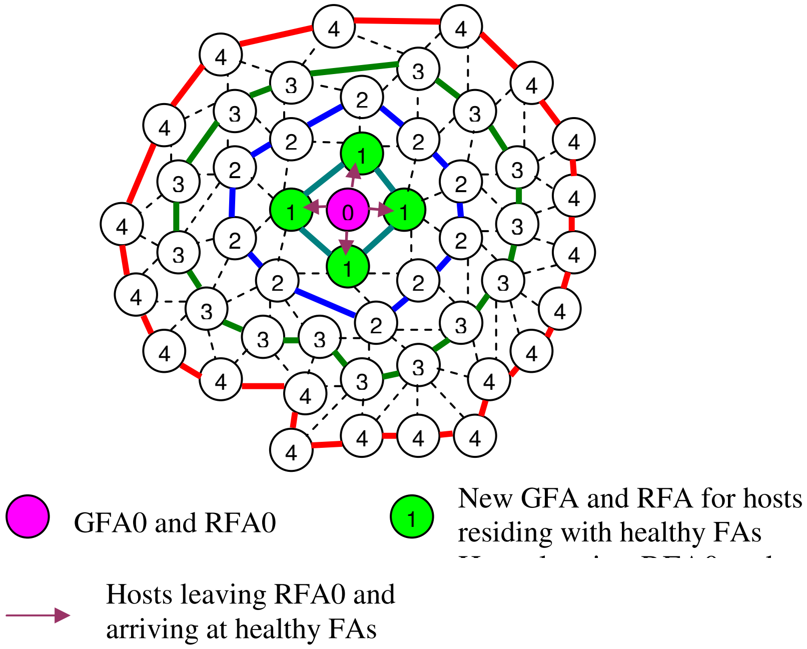


Figure 6. New GFA and RFA for hosts residing with healthy FAs

The traffic load of faulty FA0 is redirected to the failure-free FAs. This can be achieved by modifying the relationship between failure-affected radio access networks (RAN) with FAs, as shown in Figure 7. This becomes possible with the help of an interconnection that connects RANs with FAs. Usually, each RAN is connected with a single FA. But, when a failure occurs, one or more FAs are selected as backup FAs for the faulty FA. The failure-affected mobile hosts are now served by the backup FAs, without changing the location of radio coverage area of the hosts. The mobile hosts registered at RFA0, and having healthy GFAs may, also, stay either with FA0 or with healthy FAs. It is noteworthy that FA0 lies either at layer 1 or layer 2 of healthy GFAs depending upon whether a healthy GFA is at layer 1 or layer 2 of GFA0, respectively.

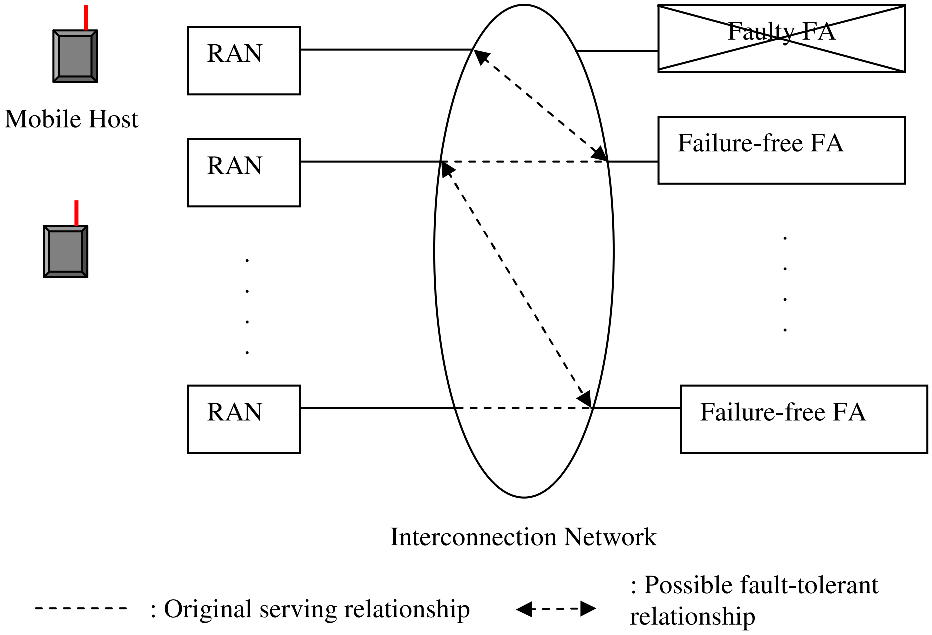


Figure 7. Remapping the relationship between RANs and FAs for fault tolerance [14]

Here, it is assumed that the mobile hosts registered at a healthy GFA have not moved beyond its layer 2 when a failure has occurred at FA0. Under this assumption, the mobile hosts residing with healthy FAs will request for micro-registrations with their healthy GFAs, via their corresponding healthy FAs. The healthy FAs will become new RFAs for their failure-affected hosts. All future packets to such a mobile host, from its healthy GFA, will be routed via its new RFA. For the hosts residing in the coverage area of FA0 and that have reached FA0 from healthy GFAs, and registered at RFA0, the fault tolerance of FA0 can be obtained using system-initiated handoff, as in the case of mobile hosts residing with FA0 and have arrived from GFA0, via RFA0. Here, it is assumed that each healthy GFA has contributed same number of mobile hosts at FA0. In this case, the healthy GFAs are used as backup members for FA0, and the RAN of failure-affected hosts is connected with these backups. Each backup GFA adds the entries of its failure-affected hosts from its GFA visitor list to its RFA and FA visitor lists. This accomplishment neither involves any additional traffic load, nor any signaling overhead on healthy GFAs.

5. Mathematical Analysis

We use following notations for analytical analysis of the proposed scheme:

N_{FAs}	Total number of FAs in the network
N	Number of MHs registered at a GFA
$N_{failure\_affected\_MHs}$	Number of failure-affected MHs
n_i	Number of FAs at i^{th} layer

n	Number of layers in the network
λ_{FA}	Arrival rate of data requests to a failure-free FA.
μ_{FA}	Service rate of data at a FA
c_{FA}	Number of resource units for handling data at an FA
w_{FA}	Traffic overhead at each FA at layer 1 and 2

5.1 Signaling Overhead

Signaling overheads involved in proposed fault tolerance scheme are due to macro and micro registrations. These registrations take place when new GFAs and new RFAs are allocated to failure-affected mobile hosts due to their faulty GFA (GFA0) and RFA (RFA0) respectively. Assume that N hosts are registered at each GFA in the network. Therefore, with GFA0, RFA0 and FA0, each host requires a macro-registration. Further, assuming that MacRA formed by GFA0 and healthy GFAs are alike, and considering RFA0 at layer 0, if the number of healthy GFAs at layer 1 is n_1 and at layer 2 is n_2, then the number of hosts that have moved to RFA0 from healthy GFAs, denoted as $N_{Hosts\_RFA0\_HealthyGFAs}$, can be written as:

$$N_{Hosts\_RFA0\_HealthyGFAs} = \frac{(n_1 + n_2)N}{(1 + n_1 + n_2)} \qquad (1)$$

These, hosts require a micro-registration at their respective healthy GFA, therefore, total registration cost in the event of a failure at an FA, represented as $\mathrm{Re}\,gCost_{failure\_affected\_hosts}$, is given by

$$\mathrm{Re}\,gCost_{failure\_affected\_hosts} = NC_{macro} + \frac{(n_1 + n_2)N}{(1 + n_1 + n_2)}C_{micro} \qquad (2)$$

5.2 Data transmission cost between RAN and the backup FAs

5.2.1 For efficient fault tolerance scheme for MIP

For data transmission cost in efficient fault tolerance scheme for MIP [66], consider layered architecture of the entire network with faulty FA being at layer 0. In efficient scheme for MIP, the workload of a faulty FA is distributed among rest of the FAs in the network. The failure-affected RAN is connected with healthy FAs so as to sustain the services to its affected users. In large mobile networks, when healthy FAs are far way from the failure-affected RAN, the data transmission delay from/to a mobile host may become longer. This will incur a considerable amount of data transmission cost on the network. The situation may become severe if the packet arrival rate at a failure-affected host is very high. If total number of FAs in the network is N_{FAs}, then the number of failure-affected hosts per healthy FA is given by:

$$N_{Host\_perFA} = \frac{N}{(N_{FAs} - 1)} \qquad (3)$$

Therefore, average data transmission cost, denoted as $Cost_{Trans\_MIP}$, can be written as:

$$Cost_{Trans\_MIP} = \frac{C\,N\,\lambda_a}{(N_{FAs} - 1)} \sum_{i=1}^{k} in_i \qquad (4)$$

where,

C Data Transmission Cost per unit distance between a healthy FA and a failure-affected RAN

λ_a Packet arrival rate

k Number of layers in the network

n_i Number of FAs at i^{th} layer

For hexagonal network architecture, number of FAs at i^{th} layer is $n_i = 6i$, and total number of FAs in network is, $N_{FAs} = 1 + 6k$. Therefore, average data transmission cost becomes:

$$Cost_{Trans\_MIP} = \frac{CN\lambda_a}{k} \sum_{i=1}^{k} i^2 \qquad (5)$$

5.2.2 For proposed fault tolerance scheme for DFHMIP

The average data transmission cost for proposed scheme can be written as:

$$Cost_{Trans\_proposed} = CN\lambda_a \left[\sum_{i=1}^{n_1} \frac{1}{FA_{i,1}^{1} + 1} + \left(\frac{n_1 + 2n_2}{1 + n_1 + n_2} \right) \right] \qquad (6)$$

where, $FA_{i,1}^{1}$ is the number of FAs at layer 1 of i^{th} FA which is at layer 1 of FA0.

For hexagonal network architecture,

$$n_1 = 6,\ n_2 = 12$$

Therefore, expression for data transmission cost reduces to

$$Cost_{Trans\_proposed} = CN\lambda_a \left(\frac{6}{7} + \frac{30}{19} \right) \qquad (7)$$

5.3 Blocking Probability

When a failure occurs at an FA, its workload is distributed among the healthy FAs in the MacRA. Therefore, the resources of a healthy FA are now contended by the failure-affected mobile hosts moved from the faulty FA and the mobile hosts originally located at the healthy FA. This degrades the performance of healthy Fas in terms of increasing blocking probability, which causes a new data request to be more possibly blocked at a healthy FA in comparison to prefailure. Total traffic overhead on each FA at layer 1 or 2 can be written as:

$$w_{FA} = \frac{N}{(n_1 + 1)} \qquad (8)$$

From Erlang's loss formula, blocking probability of each FA at layer 1 and layer 2, prior to fault had occurred, is given as:

$$P_{FA\_Blocking\_beforefailure}= \frac{\dfrac{\left(\dfrac{\lambda_{FA}}{\mu_{FA}}\right)^{c_{FA}}}{c_{FA}!}}{\displaystyle\sum_{i=0}^{c_{FA}} \dfrac{\left(\dfrac{\lambda_{FA}}{\mu_{FA}}\right)^{i}}{i!}} \qquad (9)$$

$\frac{\lambda_{FA}}{\mu_{FA}}$ is called as traffic intensity for a foreign agent.

The blocking probability of each FA at layer 1and layer 2, after failure, is given as:

$$P_{FA\_Blocking\_afterfailure} \frac{\dfrac{\left(\dfrac{\lambda_{FA}+\lambda_{FA}*w_{FA}}{\mu_{FA}}\right)^{c_{FA}}}{c_{FA}!}}{\displaystyle\sum_{i=0}^{c_{FA}} \dfrac{\left(\dfrac{\lambda_{FA}+\lambda_{FA}*w_{FA}}{\mu_{FA}}\right)^{i}}{i!}} = \frac{\dfrac{\left(\dfrac{\lambda_{FA}(1+w_{FA}}{\mu_{FA}}\right)^{c_{FA}}}{c_{FA}!}}{\displaystyle\sum_{i=0}^{c_{FA}} \dfrac{\left(\dfrac{\lambda_{FA}(1+w_{FA}}{\mu_{FA}}\right)^{i}}{i!}} \qquad (10)$$

Therefore, the increase in blocking probability on each FA becomes:

$$P_{FA\_Blocking}=\left(\frac{\dfrac{\left(\dfrac{\lambda_{FA}(1+w_{FA}}{\mu_{FA}}\right)^{c_{FA}}}{c_{FA}!}}{\displaystyle\sum_{i=0}^{c_{FA}} \dfrac{\left(\dfrac{\lambda_{FA}(1+w_{FA}}{\mu_{FA}}\right)^{i}}{i!}}\right)-\left(\frac{\dfrac{\left(\dfrac{\lambda_{FA}}{\mu_{FA}}\right)^{c_{FA}}}{c_{FA}!}}{\displaystyle\sum_{i=0}^{c_{FA}} \dfrac{\left(\dfrac{\lambda_{FA}}{\mu_{FA}}\right)^{i}}{i!}}\right) \qquad (11)$$

6. Performance Evaluation

The Figure 8 shows the effect of varying distance between faulty agent and healthy agents on data transmission cost. The figure shows that in the case of proposed scheme for DFHMIP, the data transmission cost in proposed scheme for DFHMIP is very small as compared to the efficient scheme for MIP. It is also observed that the data transmission cost in efficient scheme increase rapidlr with increasing distance between faulty FA and healthy FAs. However, the cost is almost constant in the proposed scheme. This is because with increasing distance in the efficient scheme, the packets take longer time to reach at the failure-affected RAN, whereas in the proposed scheme, failure-affected RANs are connected locally with FAs at layer 1 and layer 2 only. Therefore the packet delivery, in the event of a failure, is much faster than the efficient scheme for MIP. As shown in Figure 9, the data transmission delay or cost in efficient scheme is highly affected with increasing packet arrival rate at the failure-affected mobile hosts. However, there is very slow and smooth increase in the cost for the proposed scheme. The reason is that the packets, in the case of efficient scheme will have to traverse a longer distance with every packet arrival at the failure-affected host.

The Figure 10 shows that the blocking probability of an FA in proposed fault tolerance scheme becomes higher as compared to the efficient scheme. This happens because in MIP, the failure-affected hosts are uniformly distributed among all the FAs in the network, whereas for DFHMIP, the distribution of affected users is done only among the healthy FAs at layer 1 and layer 2 locally.

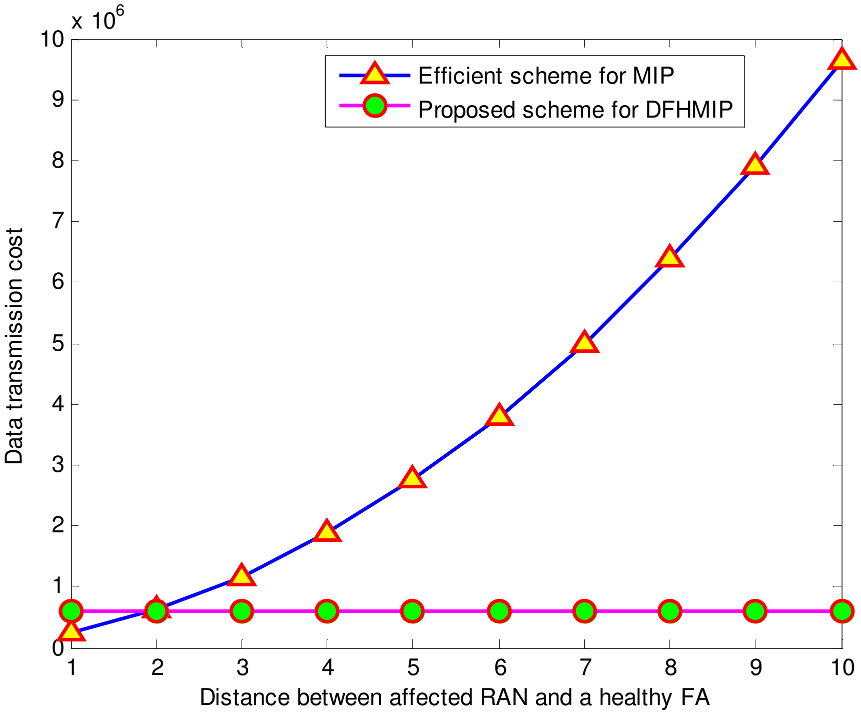


Figure 8 Variation of data transmission cost with distance between healthy FAs and faulty FA

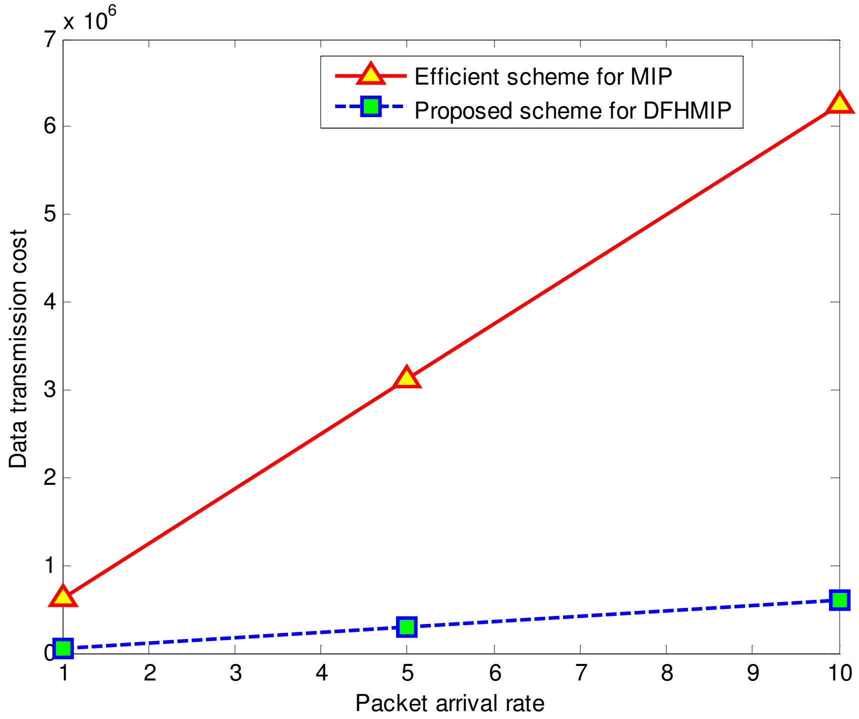


Figure 9. Data transmission cost vs. packet arrival rate

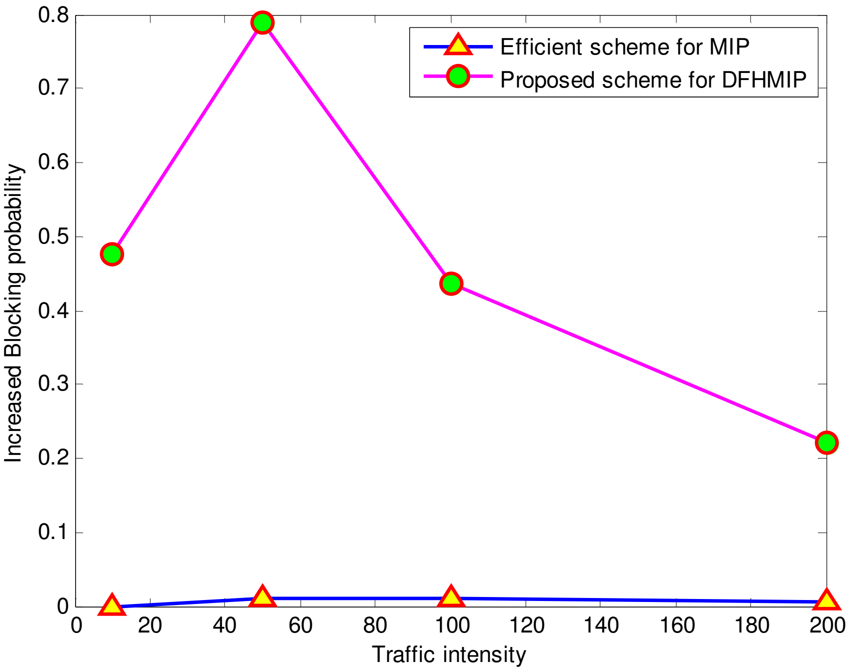


Figure 10. Variation of blocking probability with traffic intensity

7. Conclusions

This chapter suggests a fault tolerance scheme for foreign agents in DFHMIP. Though, no fault tolerance scheme for distributed and fixed architecture is reported in literature, this scheme is compared with an efficient scheme for MIP [14]. It has been observed that the data transmission delay in proposed scheme is much lower as compared with the MIP. However, proposed scheme results in higher blocking probability at each FA. This limitation is tolerable because higher data transmission delay during an ongoing session is more annoying as compared to increased blocking probability of newly starting sessions.

References

[1] Charles E. Perkins, " Mobile IP," IEEE Communications Magazine, May 1997, pp. 84-99.

[2] R. Ramjee, K. Varadhan, L. Salgarelli, S. R. Thuel, Shie-Yuan Wang, and T. La Porta, "HAWAII: A Domain-Based Approach for Supporting Mobility in Wide-Area Wireless Networks," IEEE/ACM Transactions on Networking, vol. 10 , no. 3, June 2002, pp. 396 – 410.

[3] Andras G. Valko, "Cellular IP: A New Approach to Internet Host Mobility," Computer Communication Review, January 1999, vol. 29, no. 1, pp. 50-65.

[4] Eva Gustafsson, Annika Jonsson, and Charles E. Perkins, "Mobile IPv4 Regional Registration," Internet Draft, draft-ietf-mip4-reg-tunnel-01, November 2005, work in progress.

[5] Jiang Xie, and Ian F. Akylidiz, "A Novel Distributed Dynamic Location Management Scheme for Minimizing Signaling Costs in Mobile IP," IEEE Transactions on Mobile Computing, vol., no.3, July-September 2002, pp.163-175.

[6] Wenchao Ma, and Yuguang Fang, "Dynamic Hierarchical Mobility Management Strategy for Mobile IP Networks," IEEE Journal on Selected Areas in Communications, May 2004, vol. 22, no. 4, pp. 664-676.

[7] Theo Pagtzis, Carl Williams, Charles Perkins, and Peter Kirstein, "Requirements for Localised IP Mobility Management," Proceedings IEEE Wireless and Networking Conference, 16-20 March 2003, WCNC 2003, vol. 3, pp. 1979-1986.

[8] Bjorn Chambless, and Jim Binkley, "HARP- Home Agent Redundancy Protocol," Internet draft, draft-chambless-mobileip-harp-00.txt, October 27, 1997, work in progress.

[9] Rajib Ghosh, and George Varghese, "Fault-Tolerant Mobile IP," Technical Report WUCS-98-11, Washington University, April 1998.

[10] JinHo Ahn, and ChongSun Hwang, "Low-Cost Fault-Tolerance for Mobile Nodes in Mobile IP based Systems," Proceedings International Workshop on Distributing Computing Systems, 2001, pp. 508-513.

[11] JinHo Ahn, Sung-Gi Min, and Chong-Sun Hwang, "Scalable and Efficient Fault-Tolerant Protocol for Mobility Agents in Mobile IP-based Systems," Future Generation Computer Systems, Vol. 18, 2002, pp. 613-625.

[12] H. Omar, T. Saadawi, and M. Lee, "Supporting Reduced Location Management Overhead and Fault Tolerance in Mobile IP Systems," Proceedings 4th IEEE Symposium on Computers and Communications, July 199, ISCC'99, pp. 347-353.

[13] Yin-Fu Huang, and Min-Hsiu Chuang, "Fault Tolerance for Home Agents in Mobile IP," Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 50, no. 8, December 2006, pp. 3686-3700.

[14] Jenn-Wei Lin, and Joseph Arul, "An Efficient Fault-Tolerant Approach for Mobile IP in Wireless Systems," IEEE Transactions on Mobile Computing, vol. 2, no. 3, July-September 2003, pp. 207-220.

[15] Sangheon Pack, Taewan You, and Yannghee Choi, "Performance Analysis of Robust Hierarchical Mobile IPv6 for Fault-Tolerant Mobile Services," IEICE Trans. Commun., May 2004, vol. E87-B, no. 5, pp. 1158-1165.

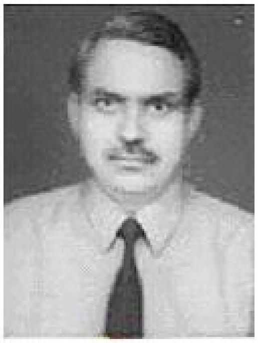
[16] Paramesh C. Upadhyay, and S. Tiwari, "Distributed and Fixed Mobility Management Strategy for IP-based Mobile Networks," IET Communications Journal (Communicated).

[17] Wenhui Zhang, Juergen Jaehnert, and Klaus Dolzer, "Design and Evaluation of a Handover decision Strategy for 4th Generation Mobile Networks," Proceedings 57th IEEE Semiannual Vehicular Technology Conference, 22-25 April 2003, VTC 2003, Vol. 3, pp. 1969-1973.

[18] Chang Woo Pyo, Jie Li, and Hiroyuki Morikawa, "Distance-Based Localized Mobile IP Mobility Management," Proceedings 8th International Symposium on Parallel Architectures, Algorithms and Networks, ISPAN 2005.

Biography

Paramesh C. Upadhyay received his B. E. Degree in Electronics & Communication Engineering from Regional Engineering College Srinagar (now, National Institute of Technology, Srinagar), J&K, India, in year 1989, and M. E. Degree in Electronics Engineering from Punjab University, Chandigarh, India, in year 2001. He earned his Doctorate Degree in Electronics & Communication Engineering from Motilal Nehru National Institute of Technology, Allahabad, India, in year 2007. He is currently serving as Associate Professor in Department of Electronics & Communication Engineering, Sant Longowal Institute of Engineering & Technology, Longowal. His current research interests are in the areas of Mobility Management, Performance Evaluation, and Mobile-IP Networks. He has been reviewer of Elsevier's Computers and Electrical Engineering Journal and IEEE ICNSC'06, and TPC member of IEEE GLOBECOM'06.



Sudarshan Tiwari did his B. Tech. in Electronics Engineering, and M. Tech. in Communication Engineering from Institute of Technology, BHU, Varanasi, India, in year 1976 and 1978, respectively. He received his Ph. D. Degree in Electronics and Compter Engineering from

University of Roorkee (now, Indian Institute of Technology) Roorkee, India in year 1993. He is Professor in Department of Electronics & Communication Engineering at Motilal Nehru National Institute of Technology, Allahabad, India, since year 1999, where he undertook the responsibilities of Head of department and Dean (Research & Consultancy). He was visiting Professor at J. M. Liverpool, U.K., during year 1998-99 under Indo-UK joint research project. He has been reviewer of several International/National journals and conferences. He has published more than 50 research papers in reputed International journals and Conferences, and has guided 4 Ph. D. students in the area of Communications & Networking. He has successfully completed research projects sponsored by AICTE/MHRD/DST, Govt. of India, and Govt. of U. K. His current research areas are Communication Engineering, Wireless Communications & Networks, WDM Optical Networks, ATM Networks, and Broadband ISDN.