

SUPPORT FOR FAULT TOLERANCE IN LOCAL REGISTRATION MOBILE-IP SYSTEMS*

H. Omar, T. Saadawi and M. Lee
CUNY Graduate School, Department of Electrical Engineering
The City University of New York, City College
New York, NY 10031
{omar, eetns, mjlee}@ee-mail.engr.cuny.edu

ABSTRACT* - The Mobile-IP (M-IP) protocol allows IP hosts to move between different networks without the need to tear down established transport layer sessions. The Mobile-IP systems supporting local registration were introduced to reduce the number of times when home registration with the remotely located Home Agent is needed. The local registration systems consider requirements and assumptions that may affect other aspects of the Mobile-IP systems as the fault tolerance. In an environment where the probability of failure of mobility support stations is relatively high, as in the battlefield or where those stations are located in hazardous conditions, the issue of fault tolerance becomes of a particular interest. In this work we will present the issues associated with fault tolerance in local registration Mobile-IP systems and will suggest approaches to enhance the robustness of such systems against both Home Agent and Foreign Agent failures. Simulation results describing the performance of the suggested fault tolerance mechanisms will be presented.

I. INTRODUCTION

The Mobile-IP protocol as described in [1], and the associated specifications provide for a system that allows IP hosts to move between different sub-networks without the need to tear down established transport layer sessions. The mobility of the IP hosts is supported by two agents; the Home Agent (HA) and the Foreign Agent (FA). The Home Agent keeps track of the current location of its Mobile Nodes (MNs) and is trying to keep the Correspondent Nodes (CNs) communicating with those MNs updated with the current location information. The FA forwards packets to and from the MNs currently located and being serviced in its area.

The Mobile-IP with the route optimization extension [2] describes an arrangement where Correspondent Nodes have binding caches to store the location information for the MNs, while both HA and FA are trying to keep the CNs updated with the current MNs location information.

The basic idea of the local registration [3, 4] is to allow the Mobile Node to send registration requests to a regional FA, or an element willing to process such requests, that tracks regional movements but does not forward the MNs request to

the HA. As in [3] and [5], FAs are arranged hierarchically in a regional topology, and the MN is allowed to move from one serving area of the regional topology to another serving area of the same topology without requiring approval by or the need to bind location information at the HA.

In this work we present available approaches to support Mobile-IP using local registration, then we describe proposals to tolerate the failure of HAs and FAs. Failure characteristics of the local registration M-IP systems will be examined and accordingly mechanisms to enhance the performance of the system will be suggested. In particular, a simple mechanism to create or enhance HA redundancy will be described, and two options to provide FA fault tolerance will be presented and examined using simulation.

II. FAULT TOLERANCE IN MOBILE-IP

A. Home Agent:

In the current specification of Mobile-IP it is clear that the MN relies on the HA for connectivity and for cache maintenance when using the route optimization extension. The HA is expected to be responsible for the hosting of multiple MNs, representing a single point of failure for those mobile nodes. The HARP protocol presented in [6] allows two or more HAs to cooperate and share registration information associated with the MNs. Each HA element in the redundancy set is configured with information about the other peers. In this work, a simple mechanism to create HA redundancy will be described.

B. Foreign Agent:

All the MNs located in a service area with a faulty FA will be denied any connectivity with the outside world. In general, the failure of mobility support stations, or FAs in our context, may be tolerated by replication of the vital state information at one or several secondary support stations. In [7], the authors propose two schemes to tolerate mobile support station failure by replication. Another approach to tolerate the failure of Visitor Location Registers (VLRs) in PCS environment when using the forwarding scheme was presented in [8].

III. HIERARCHICAL LOCAL REGISTRATION MOBILE-IP OPERATION AND FAULT TOLERANCE

A. Architecture and Operation

* Prepared through collaborative participation in the Advanced Telecommunications & Information Distribution Research Program (ATIRP) Consortium sponsored by the U.S. Army Research Laboratory under the Federated Laboratory Program, Cooperative Agreement DAAL01-96-2-0002. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation thereon.

In this work we will consider local registration Mobile-IP systems where the FAs are strategically located on a hierarchy. For short we will call such system HLRM-IP (Hierarchical Local Registration M-IP). In an HLRM-IP as illustrated in Fig.1, the MN is trying to minimize the amount of tracking required to maintain its connectivity by identifying the smallest region for which the mobile node has not traversed any regional boundary. To accomplish this functionality, each ancestral FA considers the MN to be registered at the FA just below it in the hierarchy. The FA advertisements contain the complete regional hierarchy of FAs supporting the local registration. When moving to a new service area, the MN examines the hierarchical list of FAs in the new FA's advertisement in search for the nearest common ancestor to the care-of-addresses at the new and previous service areas. The local Registration Request generated by the MN is then relayed from the FA currently serving the MN to the next higher level of the hierarchy and towards the common ancestor FA. In this way, each FA in the hierarchy between the MN and the root FA will be able to maintain a binding for the MN. The registration replies follow the same path but from the root to the leaf FA direction allowing the intermediate FAs to examine the status of the Registration Request and update the binding accordingly.

The operation of the system may best be described by an example. Consider Fig. 1, the system has one HA and two root FAs, FA1 and FA2. The nodes named FAx are FAs supporting the HLRM-IP, while nodes named Rx are regular routers supporting no FA functionality. Each FA announces the higher part of the hierarchy that this FA is located on. For example FA4 will announce the chain FA4/FA3/FA1 while FA11 will announce FA11/FA7/FA5/FA3/FA1. Considering a MN moving from home to FA19, visiting the intermediate agents FA4, FA8, FA11 and FA14. It is clear that it is only when MN moves to FA19 (step 4), then the MN will need to send the Registration Request to the HA. As long as the MN is moving within the area served by the same root FA (FA1 is the root FA for the FAs visited in steps 0 through 3), the HA need not to be involved in the MN registration.

B. FA Fault Tolerance in HLRM-IP

In the case of Non-Hierarchical Mobile-IP, the failure of a FA will cause the loss of network connectivity to all MNs currently serviced by this faulty FA. This is different from the case of HLRM-IP where the failure of a FA will prevent the packets flowing through the hierarchical system from reaching this FA and any other FA in a lower level on the tree. It is clear that a FA failure has more negative effect in the HLRM-IP case as described later in section IV.

C. HA Fault Tolerance in HLRM-IP

For a Non HLRM-IP, the HA needs to be continuously updated with the MNs' current location information, which will be reflected as more activity in the MN-FA binding table. On the other hand, consider a HA which provides the HA service for a number of MNs using HLRM-IP.

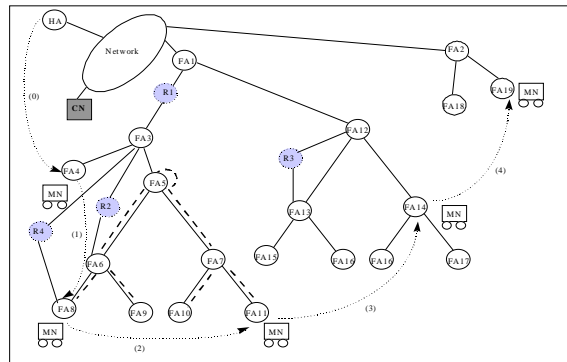


Fig. 1. Hierarchical Local Registration M-IP System

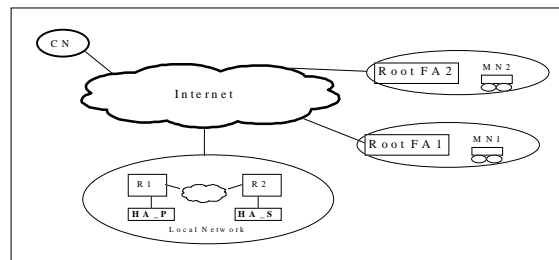


Fig. 2. Providing HA redundancy

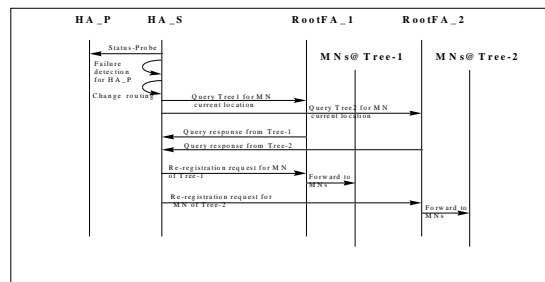


Fig. 3. Flow of control messages in HLRM-IP

Accordingly the HA will have entries in its MN-FA binding table pointing to root FAs. If the mobility of each of the MNs is confined to one tree (or one root FA), which is a reasonable assumption at least for a limited period of time, then this binding table will not experience significant maintenance activities. This is a direct result of the fact that the effect of the local mobility of the MNs has been isolated from the HA.

From the above discussion, we suggest providing HA redundancy to such system by the mean of a secondary redundant HA (HA_S) that can be located on a partitioned or a non-partitioned home subnet along with the primary HA (HA_P). Although a hot standby HA redundancy system as described in [6] can be applied in the case of HLRM-IP, the inherent features of the HLRM-IP suggests the use of less demanding HA redundant system. As a matter of fact, our proposed HA redundant system does not require the secondary system to be dedicated all the time. As shown in figures 2 and 3, redundancy can be provided to the dedicated primary HA by considering a non-dedicated secondary HA. HA_P is a regular HA, while the HA_S is a host capable of implementing the HA functionality when needed and have a

mechanism to monitor the health of the primary HA. HA_S is configured with the list of MNs supported by the HA_P and with a list of the supported root FAs, which is expected to be a short list. The detection of the HA_P failure by the HA_S will cause an update to the internal routing mechanism such that traffic will be directed to the HA_S instead of HA_P.

Under normal operation conditions, the HA_P will be responsible for the HA functionality. Upon the HA_P failure detection, the HA_S will send a request to the root FAs asking for the current location of the supported MNs. On receiving the root FAs responses, the HA will be able to build its binding table and the HA_S can restore communications with its MNs and ask them to re-register. The intention behind this mechanism is not to provide a hot standby system but is to provide a minimally demanding redundant system that takes advantage of the HLRM-IP features.

IV. FA FAULT TOLERANCE IN HLRM-IP

A characteristic that distinguishes HLRM-IP from the regular M-IP is that if any of the FAs along the path between the root FA and the leaf FA fails, this will cause the MNs located at the leaf FA to lose its network connectivity. Considering Fig 1. and a MN located with FA8 and no faulty FA, the data packets generated from the CN and destined to the MN will be forwarded to the HA. The HA will tunnel the packet to the root FA (FA1) and FA1 will tunnel the packet to FA3 to be tunneled to FA5. The process will continue until the packet reaches FA8. The failure of any of those FAs will break the path between the root and the leaf FAs. We should notice that this situation occurs even if a route bypassing the faulty FA exists.

In this paper, we will introduce two possible solutions to overcome the problem of loss of service resulting from a FA failure in HLRM-IP environment. The first possible solution will consider the MNs affected by the failure of the FA and instruct them to revert to Non HLRM-IP mode. The other approach considers healing the break in the encapsulation-decapsulation chain caused by the failure of the FA on the hierarchy.

A. Revert to Non HLRM-IP Mode

In the case of a FA failure, all MNs serviced directly by this FA or by a FA located in a lower level in the hierarchy and on a path on which the faulty FA is an intermediate point will suffer from loss of service. In this approach, all MNs affected by the FA failure will be notified and are instructed to send Home Registration to the HA. This message may be called Non-local Registration Request Solicitation. Considering a system as the one shown in Fig 3, the mechanism can be illustrated as follows:

- a) Consider the faulty FA (FA_F) and the FA in the higher hierarchical level (FA_H). FA_H will detect the failure of FA_F. (FA_F=FA4, FA_H=FA3)
- b) FA_H will construct a list (MN_list) of those MNs affected by this failure. (MN_List=MN1, MN2, MN3, MN4 and MN5)

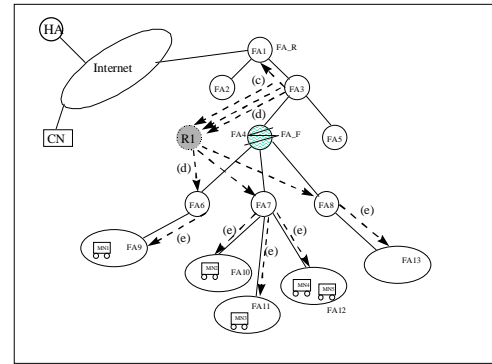


Fig. 4. Revert to Non HLRM-IP mechanism

- c) FA_H will contact the Hierarchy Registry to get a list (FA_list) of the FAs directly connected to the faulty FA. FA_List (FA_List=FA6, FA7 and FA8)
- d) For each FA in FA_list, the FA_H will send the MN_list.
- e) Upon receiving the MN_list, each FA will perform one of two possible actions. If none of the entry in the MN_list exists in the visitor list of the FA, no further processing is needed and the MN_list is disregarded. If one or more of the MNs included in the MN_list is found in the visitor list of the FA, the list will be forwarded to the next lower FAs in the hierarchy (as indicated in the visitor list).
- f) On receiving the Non-local Registration Request Solicitation, each of the affected MNs will send a non regional Registration Request to its HA. When this request is received by the HA, the HA will update its table to register the serving FA as the current FA in place of the root FA.
- g) The MN will need to send a Registration Request with the Previous Foreign Agent Notification option. This will have the effect of removing the binding information for the affected MN on the root FA. When route optimization is implemented the CN will have a binding information pointing to the root FA as the current FA serving the MN. On receiving packets from the CNs, the root FA will generate a Binding Warning to the HA.
- h) It is expected that the faulty FA will come back in service after the time needed for repair and for failure recovery. The FA_H may regularly examine the status of the FA_F. When FA_F recovery is detected, the FA_H may send a message of the type "Local Registration Solicitation" directed towards the affected MNs announcing that those MNs can start using local registration. The issuance of this message can be delayed using a timer if it is required to keep the MNs for extra time in the Non HLRM-IP mode.

B. Self-Healing Mode

This approach may be used when reverting back to Non HLRM-IP is not preferred, which may be the case if the relatively higher delay associated with non-local registration can not be tolerated. The basic idea of this solution is to heal the breakage in the hierarchy tree caused by the faulty FA. This can be accomplished by bypassing this faulty FA such that the FA in the hierarchical level just above the faulty FA

will remove the faulty FA from his copy of the hierarchy, and consider the FA in the level just below the faulty FA as its tunnel end. The same steps will be repeated for each FA connected to the faulty FA.

In an environment as the battlefield, where the probability of FAs failure is relatively high and location dependent, it is expected that other surrounding FA in the hierarchy will be subjected to similar attack. The higher FA may point to further lower FA and not necessarily a FA in the level just below the faulty FA. Steps involved in supporting this mechanism are as follows considering Fig. 5:

- a) The FA_H detects the failure of the FA below (FA_H=FA3, FA_F=FA4)
- b) FA_H will construct the MN_list of those MNs affected by this failure. (MN_List=MN1, MN2, MN3 and MN4)
- c) FA_H will contact the Hierarchy Registry to get a list (FA_list) of the FAs directly connected to the faulty FA (FA_List=FA6, FA7 and FA8)
- d) FA_H will send the message FA_Change_HIR to members of the FA_List. This message carry the list of MNs that FA_H has binding for. On receiving this message, each member of the FA_List will change its hierarchy information such that FA_H will become the FA in place of the faulty FA. In addition, a FA_Change_Hir_Confirm message will be sent from each member of the FA_List containing information about which MNs it has binding for such that the FA_H can update its binding and forward packets to the correct FA.
- e) FA_Ls propagate the message downwards. FAs will need to know the new hierarchy to be used when announcing their local registration support.
- f) The same information is sent to the Hierarchy Registry.

In some situation, or if desired, only one FA from the FA_List can be used to heal the hierarchy. For example, if connectivity exists between FA6 and FA7 and between FA6 and FA8 then FA7 and FA8 can be attached to the hierarchy through FA6.

C. Comparison between the two schemes

In the previous subsections we have demonstrated two approaches to tolerate the FA failure in Hierarchical Local Registration M-IP systems. In the following we will highlight the features associated with each mechanism. Consider the Revert to Non HLRM-IP mode as approach A and the Self-Healing as approach B:

1. Time needed to recover from a single FA failure

Approach A: Each affected MN is required to send a HA Registration Request and to wait until receiving the HA Registration Reply to be able to compensate for the effect of the FA failure. For the case when enhanced CHs exist in the network, the time to recover from FA failure is defined as the time starting from the failure detection till the time when all enhanced CNs receive Binding Updates from the HA informing about the current FA for all the affected MNs. For the non-enhanced CHs case, the time to recover is defined as the time starting from the failure detection till the time when the HA receives all Registration Requests from the MNs and

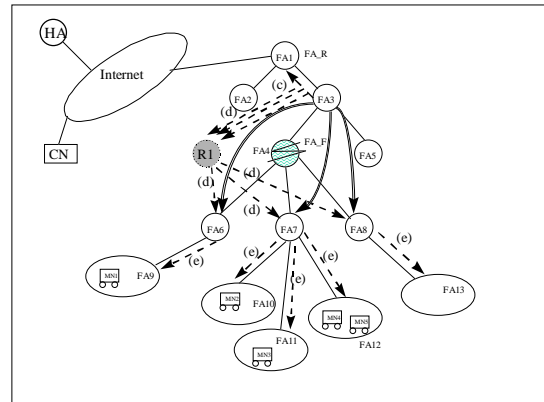


Fig. 5. Self healing mechanism

the MNs receive the corresponding registration replies. **Approach B:** Time to recover from failure is defined as the time starting from the failure detection till the time when the FA_H receives the FA_Change_Hir_Confirm. Since the distance between the MNs and FA_H is expected to be less than the distance between the MNs and the HA, the delay in this approach is accordingly expected to be less than that of approach A.

2. Performance under high probability of failure of multiple FAs on adjacent levels

It is expected that the FAs failure will be location dependent in a battlefield environment. For example, if a FA housed in a mobility support station was hit in an attack, it is expected that FAs on higher and lower adjacent levels will be subjected to similar attacks. Approaches A and B behave differently under such conditions.

Approach A: When in the Non HLRM-IP mode, MNs will not be affected by the failure of FAs on adjacent hierarchical levels as long as another route exists to forward packets from the HA to the current FA. When such multiple failure is expected, it is more efficient for the MNs to stay in Non HLRM-IP mode until the multiple failure status is not existing. This can be implemented using a timer function. **Approach B:** This approach is sensitive to multiple level failure. Each failure event will cause the control messages associated with the recovery mechanism to be generated and processed such that multiple failure will be associated with more control messages and more service loss time intervals.

3. Transparency of the recovery mechanism to the MNs

Approach A: Not transparent since MNs will need to receive and process the Non-local Registration Request Solicitation. **Approach B:** Transparent to MNs since the FA_Change_Hir messages are destined to the FAs and not the MNs.

V. SIMULATION

In this section we will show simulation results that describe the behavior of the two proposed techniques to support the FA fault tolerance in hierarchical environment. The environment simulation is composed of twenty MNs moving between the FAs at the leaf of a local registration

hierarchical tree. Any MN can roam between the cells determined by a mobility range. The hierarchy has eight levels, where the root FA is located at the top and the FAs where the MNs are roaming are at the bottom. The delay over a link between two FA on the hierarchy is set to one msec. The delay between any FA and a routing element is set to 2 msec, and the delay over wireless link is set to 2.5 msec. The delay between the HA and the root FA is set to 4 msec. A unidirectional uniform traffic is generated from two correspondent nodes to the different MNs. For each mobility range, a pool of FAs subjected to failure is created, where the failure rate is randomly distributed between 0.02 and 0.2 failures per minutes. The simulation time was divided to segments, where during each segment the failure of one FA will trigger the failure of another adjacent FA (from the pool) emulating multiple failures caused by the same attack. Simulation time of 100 minutes was considered, with randomly distributed mobility rate between 1 and 5 move/minute. The case of the Base Mobile-IP is considered.

The ratio of the average number of packets dropped is evaluated over different mobility ranges. Mobility range of a value two means that the Mobile Nodes are allowed to roam between cells served by FA located in an area limited by two hierarchical levels above the current level. A mobility range of two on a hierarchy as the one shown in Fig. 1 allows a MN currently located in FA8 to move between FA8, FA9, FA10 and FA11 (those are the FAs served by the FAs in the upper two levels on the hierarchy: FA5, FA6 and FA7). Two possible failure patterns were considered. The first one assumes that the FAs to fail will be located on the same level of the hierarchy. The other pattern corresponds to the case where the FAs subjected to failure will be located on adjacent level on the hierarchy and on the same branch. As mentioned before, the revert to Base M-IP approach is generally characterized by larger value for the time needed to recover from failure due to the time consumed in the HA registration process. Although this is true as shown in the results of Fig. 6 for the case of failures on the same hierarchy level, the Revert approach outperforms the Self-Healing mode when considering the case of failure on adjacent levels since one corrective action will allow the system to survive multiple failures when using the Revert to Non HLRM-IP approach. This can be illustrated in Fig. 6, where around mobility range of 3 and up, the Revert approach starts providing less packets drop than the other approach.

Fig. 7 represents the effect of the number of MNs considered on the number of control messages needed to perform the two FA fault tolerance mechanisms. As expected, the revert to Base M-IP provides more control messages mainly due to the HA registration requests and replies needed for each MNs affected by the failure. A deviation from this characteristic may happen if only few MNs exists in the area subjected to failure. In this case the HA registration messages will not represents the majority of those control messages, but as shown in the figure, the point where the Revert approach outperforms the Self-Healing approach occurs for number of

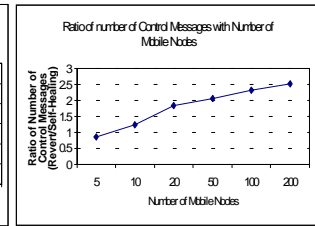
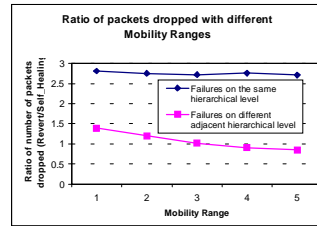


Fig. 6. Number of packets dropped Fig. 7. Number of control messages

MNs less than 8 in this simulated environment. Whenever the number of MNs increases, the probability of larger number of affected MNs increases also and hence more control messages. On the other hand, the number of control messages associated with the Self-Healing mechanism will not be tied up all the way with the number of MNs since the control messages are associated with the FAs directly serving the Mobile Nodes and not with the total number of MNs.

VI. CONCLUSION

Fault tolerance in mobile systems is of great importance for mission critical application. In this work, we presented a robust platform that tolerate both HA and FA failure in Hierarchical Local Registration Mobile-IP systems. The HA redundancy proposed in this work is characterized by minimal requirements on the redundant HA taking advantage of the hierarchical architecture features. Two possible alternatives to tolerate FAs failure were described and the corresponding features were demonstrated. Simulation results were demonstrated pointing to possible situations where one approach may outperform the other.

REFERENCES

- [1] Charles Perkins, "IP Mobility Support", IETF Proposed Standard, RFC-2002, Network Working Group, October 1996.
- [2] Charles Perkins and David Johnson, "Route Optimization in Mobile IP", IETF Draft, 'draft-ietf-mobileip-optim-07.txt', November 20, 1997.
- [3] Charles Perkins, "Mobile-IP Local Registration with Hierarchical Foreign Agents Approach", IETF Draft, February 1996.
- [4] Weidong Chen, Eric Lin and Hua Wei, "Dynamic Location Control for Mobile Nodes", July 1997.
- [5] Perkins, Charles, "Mobile IP Design Principles and Practices," Wireless Communications Series. Reading, MA: Addison Wesley Longman, 1997
- [6] HARP - "Home Agent Redundancy Protocol" <draft-chambless-mobileip-harp-00.txt>- Bjorn Chambless Portland State University, Jim Binkley Oregon Graduate Institute October 27,1997
- [7] S. Biaz and N. H. Vaidya, "Tolerating Location Register Failures in Mobile Environments", Texas A&M University, Technical Report 97-015
- [8] Sridhar Alagar, Ramki Rajagopalan, S. Venkatesan, Computer Science Program, University of Texas at Dallas, Tolerating Mobile Support Station Failures

* The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied of the Army Research Laboratory or the U.S. Government