2009 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications

A Connection Stability Aware Handoff Management Scheme

Tarik Taleb[1,*], Zubair Md. Fadlullah[2,†], Marcus Schöller[1,‡], and Khaled Ben Letaief[3,§]
[1] NEC Europe LTD.
[2]Graduate School of Information Sciences, Tohoku University, Japan
[3]The Hong Kong University of Science and Technology
*Tarik.Taleb@nw.neclab.eu, †zmfadlullah@gmail.com, ‡schoeller@nw.neclab.eu, §eekhaled@ece.ust.hk

***Abstract*— Fast handover management in mobile IPv6 environments has been a research subject for a long time. Exploiting the cooperative diversity paradigm in Partner-based Hierarchical MIPv6 (PHMIPv6) promises an acceleration of the handoff management operation by relaying some signaling over a selected partner node prior to the actual handover to the new access point. For this purpose, a suitable partner node, that stays in communication range for sufficient time until the signaling in the pre-handoff phase is finalized, should be selected. PHMIPv6 proposes to select the node with the highest signal strength as the partner node. In this paper, we show that using the Link Expiration Time (LET) metric to select the partner node can significantly improve handovers in Mobile IP (MIP) networks. The basis of this new metric is the relative position and the relative speed of the mobile node to the potential partner nodes. A set of simulations is conducted to evaluate the performance of the proposed scheme and encouraging results are obtained.**

I. Introduction

The Internet is the dominant network of today which faces a rapid convergence of wired and wireless access. The Internet-based applications and the data traffic load generated have transformed the mobile network into an all-Internet Protocol (IP) configuration framework. From these rapid transformations, one can foresee the inevitable fact whereby the next-generation mobile systems will be based on IP to a large extent (if not solely). But the IP suite, as originally specified, does not support mobility for a number of reasons related to the protocol syntax and semantics. Therefore, finding efficient and optimum solutions for handling the IP mobility has become an imperative topic of research.

Within the Internet Engineering Task Force (IETF), the Mobile IP Working Group has been established. There, a packet-based mobility management protocol called Mobile Internet Protocol (MIP) [1] and its extension for IPv6 networks called MIPv6 [2] have been proposed.

Many extensions have been proposed to these initial documents to improve mobility, reduce signaling overhead or to overcome shortcomings. In case of mobile users roaming far away from their respective home networks, MIP performance degrades severely and the signaling delays for Binding Updates (BUs) increase remarkably. This can result in the loss of a significant amount of in-flight packets. In order to make MIP scalable for such scenarios, Hierarchical Mobile IPv6 (HMIPv6) protocol [3], [4] was proposed. There, local mobility is treated differently than global mobility. Mobility Anchor Points (MAPs) are introduced where each MAP is responsible for a set of Access Routers (ARs) forming the actual access network. Mobility of a Mobile Node (MN) between ARs of one MAP is treated locally and only handovers between different access networks, i.e. different MAPs, require a binding update. In order to improve the handover between two MAPs, Chen *et al.* [5] introduced the Partner-based HMIPv6 (PHMIPv6) protocol. There, the handoff process is accelerated by initializing it prior to the entrance of a mobile node into the overlapping zone. A Partner Node (PN) is selected which performs signaling with the new AR and the new MAP *a priori*.

Selection of a suitable PN is critical to make PHMIPv6 work and manage the handover. The original work proposes a rather naive strategy by choosing the mobile node with the highest signal strength (in its ad hoc mode) as PN. But as an in depth analysis of PHMIPv6 reveals, the PN has to remain in communication range with the MN and the new Access Point (AP) until the pre-handover signaling is finalized. Moving out of range from any of these two entities means that the pre-handover scheme has to be aborted. The MN either restarts the hand-over process by selecting a different PN or uses the HMIPv6 mechanism doing the signaling itself. To address this issue, we propose the use of Link Expiration Time (LET) [6] as a parameter in the selection of the best possible PN, which will be able to communicate with the new AP for a sufficiently long time. To achieve this, the metric takes the relative movement of the potential PNs towards the MN and AP into account. Conducting and evaluating the results of extensive simulations show that the usage of LET improves PHMIPv6 handover performance.

This paper is organized as follows. First, the relevance of this work to the state-of-art in the field of cooperative diversity is presented in Section II. The proposed enhancements to PHMIPv6 are described in Section III followed by their evaluation. The simulation results are summarized in Section IV. Concluding remarks are presented in Section V.

II. Related Work

Macro-mobility is a dominant technique for managing network-infrastructure based mobility. In macro-mobility, a mobile node, when moving into a different network zone, requests for a new Care-of-Address (CoA). Then, a BU

978-0-7695-3841-9/09 $26.00 © 2009 IEEE
DOI 10.1109/WiMob.2009.41

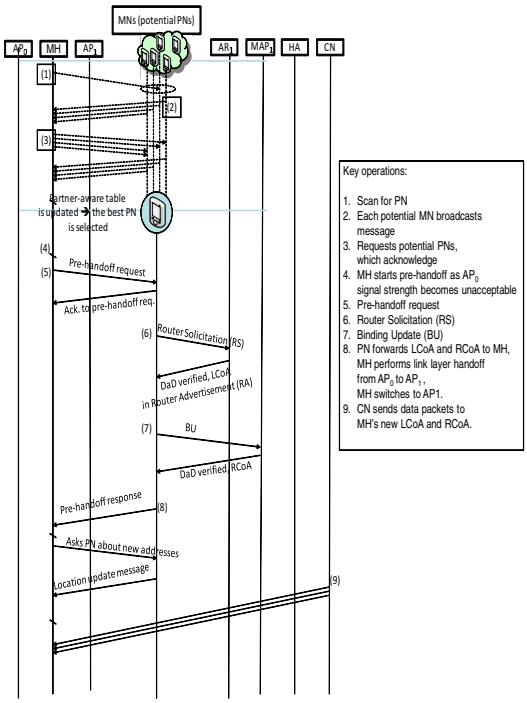


Fig. 1. Inter-MAP handoff messages in PHMIPv6.

message is dispatched to the HA. However, users that roam far away from their respective home networks experience substantial handoff signaling latencies under macro-mobility. This leads to disruption of active network connections when handoff events occur. To handle this issue and also to effectively perform Macro Diversity HandOver (MDHO) events in Mobile Multihop Relay (MMR) environments, a standard [7] was formulated. In this standard, concurrent connections to different APs are maintained by the subscribing Mobile Host (MH) so that it can seamlessly bind with the AP, which provides the best connection quality. In order to facilitate this, the same MAC/PHY message is transmitted to the MH's downlink by each access point (i.e., by each of the new APs and also the old one). In response, the MH transmits, via its uplink, the same message to each of these APs. This particular standard takes into account nine different network topologies whereby handoff events within the same MMR cell and also between various MMR cell-pairs are considered. In addition, the MDHO handover schemes and their corresponding MAC management messages via the relay stations are implemented to enable IEEE 802.16e-based MHs to perform smooth handoffs both within a MMR network and within an IEEE 802.16j environment.

In recent time, researchers have also focused on fast and smart handoff techniques due to the advent of the Fourth Generation (4G) wireless technologies. The Transport and Application Layer Architecture for Vertical Mobility with Context-awareness (Tramcar) [9] is worth noting in this regard. Tramcar is capable of meeting user preferences and reducing handoff latencies through its cross-layer application and transport services, respectively. Tramcar also demonstrates the importance of considering multiple handoff decision attributes (e.g., power consumption, services cost, network performance, network conditions, and security) rather than solely relying on the best signal strength to choose a new access point. The shortcoming of Tramcar is, however, in its lack of support for utilizing relay nodes to facilitate cooperative diversity, which may lead to lower handoff delays.

In order to reduce handoff-signaling latencies in macro-mobility, various research work were carried out by adopting hierarchical management strategies using local agents. A notable example is Hierarchical MIPv6 (HMIPv6) [4] which considers the overall handoff delay in two layers, namely in link and network layers. The link layer handoff delay comprises two sequences, namely the discovery and re-authentication phases. The discovery phase experiences delay due to "probing" while the re-authentication step is associated with authentication and re-association delays. The most dominant latency is, however, the probe delay. The handoff schemes proposed in [10]–[14] focus on reducing the delays associated with the discovery and re-authentication phases, respectively. On the other hand, the network layer handoff delay consists of three elements, namely the rendezvous time, the Duplicate Address Detection (DAD) delay, and the binding update time. In case of HMIPv6, the most dominant delay is attributed by the DAD operation. By starting the handoff operation before its actual time, the work in [5], [15] attempt to reduce the DAD delay. In particular, in [5], when a MH roams inside the same MAP, mobility management issue is considered to be the same as that in HMIPv6. On the other hand, as the MH switches from access point AP_0 to AP_1 (the old and new access points belong to MAP_0 and MAP_1, respectively), the handoff operation consists of the following three phases. The overall handoff procedure is illustrated in Fig. 1.

Partner node selection: A MH that approaches the edge of AP_0 initiates a scan for an adequate PN by transmitting periodic broadcast messages. MNs that may serve as potential PNs periodically broadcast messages containing information of the serving AR. To these PNs, the MH sends a request, which the PNs acknowledge. The MH updates the partner-aware table based on the responses from the potential PNs and attempts to select the best possible PN.

Pre-hand signaling: Once the signal strength of the currently attached access point (i.e., AP_0) falls below a pre-defined threshold, the MH initiates the pre-handoff operation by scanning for an alternate AP [10]. Having detected the new AP, the MH sends a pre-handoff request message to the PN with the strongest signal. The PN acknowledges the pre-handoff request message. Then, the PN requests a new on-Link Care-of Address (LCoA) from the new access router, AR_1 and a new Regional Care-of Address (RCoA) from MAP_1. In addition, a BU is performed with the new MAP_1. The PN signals the finalization of the pre-handoff by issuing a pre-handoff response message to the MH.

Macro-mobility handoff: The MH then performs the link layer handoff from AP_0 to AP_1. Simultaneously, the MH inquires its new LCoA and RCoA addresses from

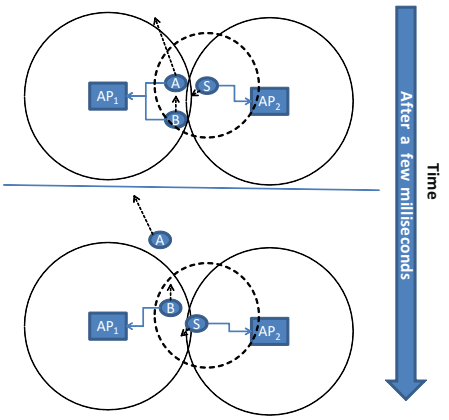


Fig. 2. Erroneous partner selection in PHMIPv6.

the PN. The CN already sends data packets to this new LCoA and RCoA of the MH which are now received via the new AP_1.

By thus cooperating with a partner entity, it is possible for a mobile node to substantially decrease the handoff latency (associated with the network layer). However, the PHMIPv6 mechanism naively selects the partner nodes based on only signal strength. As per the work in [16], the nodes' relative moving directions also need to be taken into account. Parameters other than the signal strength (e.g., the ones considered by the aforementioned Tramcar framework [9]) may also be considered so that PHMIPv6 can be endowed with a more suitable decision parameter (or a set of parameters) for making a handoff decision. In addition, the fact that the MH and PN may move out of communication range should also be considered. Fig. 2 illustrates this possibility whereby the pitfall of using only signal strength for making the handoff decision becomes even more apparent. Fig. 2 depicts a wireless network with three nodes, namely A, B, and S. The figure on the top shows the initial locations of the nodes and the figure on the bottom shows their new positions after a few milliseconds. The dashed circle shows the ad hoc range of node S, which is assumed not to be moving. By applying a naive partner selection scheme as in PHMIPv6, node S will be selecting node A as its partner given its geographical proximity and thus its stronger signal. This selection is obviously not appropriate as node A will be soon outside the ad hoc range of node S. Indeed, from this example, it becomes clear that a partner selection mechanism is required that considers, in addition to the signal strength, the duration over which the nodes can communicate with one another.

III. Envisioned Enhancement to PHMIPv6

In this section, we first delineate some security concerns evolving from the original PHMIPv6 scheme. We then introduce an enhanced edition of PHMIPv6 based on the Link Expiration Time (LET) parameter. This enhanced version deals with the security concerns of the original PHMIPv6, and also reflects, in the partner node's selection mechanism, the stability of the connection between a given MH and its PN.

A. Incorporating security in PHMIPv6

Since the original PHMIPv6 selects unknown PNs for performing handoff operations, it is vulnerable to the following security threats. Adequate security measures should be incorporated in the enhanced version of PHMIPv6 so that these security risks are carefully addressed and dealt with.

Malicious PN: First, a MH provides its corresponding PN with its security key for Authentication, Authorization, and Accounting (AAA) purposes in the original PHMIPv6 scheme. This security key can be reused at a later time by a malicious PN, to bind with the access point posing itself as the MH. This may be of particular benefit to the PN in case that this security key provides the PN with a higher service level than what it is originally entitled for. We take this security flaw into account in our enhancements to the PHMIPv6 scheme by allotting two different security keys to the PN and the MH for pre-handoff request and authentication with the wireless network operator/service provider, respectively.

Malicious MH: The second security risk is pertaining to a malicious MH, which aims at flooding the access point/router with multiple pre-handoff requests and eventually cause a Denial of Service (DoS). To this end, the malicious MH may send pre-handoff requests to a large number of PNs concurrently. In our envisioned enhancement to the original PHMIPv6 scheme, this threat can be addressed by permitting only one pre-handoff request for every MH, which can be easily identified by its unique security key.

Network layer attacks: During the PNs discovery phase, a malicious MN may appear itself to the subscribing MH as a potentially suitable PN. Upon being selected, this rogue PN may not forward the requests, responses, and other messages between the MH and the new access point. The malicious PN can also willingly delay forwarding these messages, thereby contributing to further handoff latency. Our enhancement to the PHMIPv6 circumvents such scenarios by employing a considerably small time-out parameter at the MH. If the MH does not receive the response within the time-out period, it considers either of the following options: (i) it may select another PN, or (ii) carry on performing handoff to the new AP on its own. In addition, to prevent the scenario in which a malicious PN forges the new LoCA and/or RoCA, we may delegate more responsibility to the new access point (i.e., similar in spirit to the Proxy MIP-PMIP approach (RFC5215)) rather than to the PN as the cooperative partner of the MH. The evaluation of such scheme formulates some of our future research work in this domain.

B. Connection Stability Aware (CSA) PHMIPv6

Fig. 3 depicts the Connection Stability Aware (CSA) PHMIPv6 mechanism, which we envision by making adequate enhancements to the original PHMIPv6 scheme. The duration for which PN may access AP_1 is indicated by t_{dur}. t_{pre} denotes the pre-handoff time. By applying the Exponential

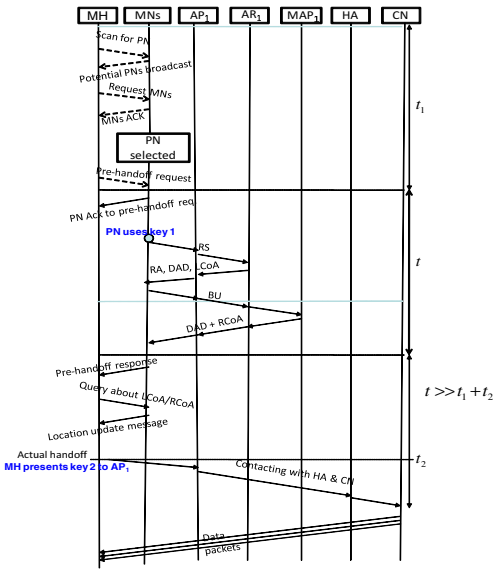


Fig. 3. Connection stability aware PHMIPv6.

Moving Average (EMA) method, CSA-PHMIPv6 estimates the average values of t_{pre} and t_{dur} from their history. The most appropriate PN is then selected based on these estimated values as follows.

i. Two groups of MNs denoted by N_a and N_b are formulated. N_a is constructed by sorting the MNs, LET values of which exceed t_{pre}. N_b is formed including the sorted MNs in N_a that have LET with AP_1 exceeding t_{dur}.
ii. CSA-PHMIPv6 scheme reduces to original PHMIPv6 if $(N_a = \emptyset)$.
iii. On the other hand, if $(N_b = \emptyset)$, the MN, LET value of which with the MH is the maximum, is selected from N_a as the PN.
iv. Otherwise, the MN, LET value of which with the MH is the maximum, is chosen from N_b as the appropriate PN.

As shown in Fig. 3, t_1, t, and t_2 denote the time required for selecting an adequate PN and sending a pre-handoff request, the time required by PN to perform handoff, and the time required so that PN notifies MH of a successful pre-handoff operation, respectively. t_{pre}, evaluated as the sum of these three parameters, can then be used to evaluate t_{dur} as follows.

$$t_{pre} = (t_1 + t + t_2) \quad (1)$$

$$t_{dur} \simeq t_{pre} + \Delta(MH, PN) + \Delta(PN, AP_1) \quad (2)$$

It is worth stressing that the values of t_1, t, and t_2 can be estimated from the propagation delays of the links involved in the communication (e.g., PN to AP_1, AP_1 to AR_1) averaged over a certain period of time by employing the EMA method. $\Delta(m, n)$ indicates the propagation delay between nodes m and n.

IV. Performance Evaluation

A. Simulation Set-up

The performance of the envisioned CSA-PHMIPv6 scheme is evaluated in this section based on computer simulations by employing the Network Simulator (NS2) [17]. The considerations behind designing a realistic simulation set-up are described and justified below. The parameters stated in the remainder of this section are used in all the conducted simulations unless otherwise specified. The original PHMIPv6 and HMIPv6 schemes are used to compare the performance of the proposed CSA-PHMIPv6 approach.

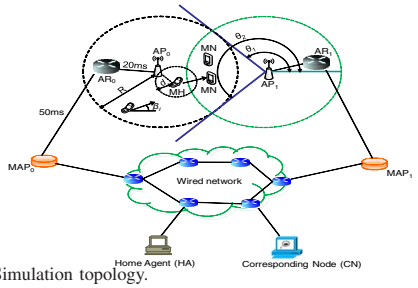


Fig. 4. Simulation topology.

Fig. 4 depicts the considered network topology in the conducted simulations. Broadly speaking, the network configuration comprises two parts, namely the wireless and wired parts. The former consists of two adjacent wireless cells, each with a coverage radius of 400 meters. The two neighboring APs are set 800 meters apart. As a consequence, the maximum overlapping distance equals 50 meters. It should be noted that these parameters are selected with no specific purpose in mind and do not inflict any change in the rudimentary observations pertaining to the simulation results. In case of the wired network, a general scenario is chosen whereby the two APs are connected via a two-layered network comprising two ARs and two MAPs. AR_i and AP_i are served by MAP_i, where $i \in \{0, 1\}$. The MAPs are connected to a HA and a CN via a wired network (e.g., the Internet). The one-way propagation delays of AP-AR, AR-MAP, and wired network to MAPs are set to 20ms, 50ms, and 100ms, respectively. In case of bandwidth of the considered links, the wireless links have smaller bandwidth in contrast with the wired ones. For the sake of generality, however, the capacity of each link is set to 100Mbps, and this should not influence the fundamental observations about the proposed CSA-PHMIPv6 scheme.

The duration for each simulation is set to a long enough value of 600s, within which the system is allowed to attain a consistent behavior. The initial 60s and the final 60s are used to initialize the simulations and to ensure that the results have stabilized, respectively. The average values of multiple simulation runs are used as results.

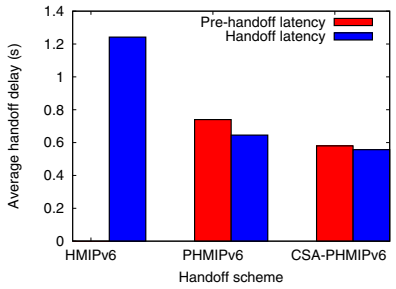
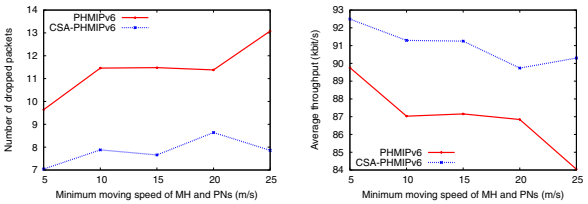


Fig. 5. Handoff delay for the three considered schemes.



(a) Packet drops vs. moving speeds of the mobile nodes for PHMIPv6 and CSA-PHMIPv6 schemes.

(b) Average throughput vs. moving speeds of the mobile nodes for PHMIPv6 and CSA-PHMIPv6 schemes.

Fig. 6. Comparison between the original PHMIPv6 and the proposed CSA-PHMIPv6 schemes in terms of packet drops and throughput.

In order to model mobility, a population comprising one hundred MNs is randomly scattered over the regions covered by the two access points AP_0 and AP_1 (as shown in Fig. 4). The coverage areas of AP_0 and AP_1 are restricted by the angels θ_1 and θ_2, respectively. The MNs' velocities are obtained from a uniform distribution. The moving directions of the considered MNs are simulated in such a manner that their handoffs occur between AP_0 and AP_1 at different time instances. The mobility model considers users in two scenarios, namely a highway and an urban area. Based on this consideration, the minimum and maximum values of the uniform distribution are set to a high node moving speed of 120km/h and a slow node moving speed of 4km/h, respectively. When a simulation starts, all nodes remain stationary for a short duration. This is done in order to make sure that the results achieve a certain level of stability. The radius of the ad hoc transmission range of the MNs denoted by d is varied, from 30 to 70 meters, during the simulations.

For evaluating the performance of the proposed CSA-PHMIPv6 scheme, we consider a number of quantifying parameters. First, the average handoff delays experienced in case of the three schemes are taken into account. Then, the number of dropped packets and throughput for the considered schemes are compared. The pre-handoff success ratio and pre-handoff failure ratio of the different methods are also compared. Finally, the influence of the LET value between a MH and its selected PN on each scheme is also investigated.

We consider a pre-handoff to an access point AP_i to fail in two cases, namely (i) if a MH loses communication with its selected PN, or (ii) the selected PN moves out of AP_i's coverage area prior to the finalization of the handoff operation. However, if a MH cannot find an adequate PN for performing handoff, we do not consider that pre-handoff attempt as a failure. Therefore, the pre-handoff success ratio and the pre-handoff failure ratio do not necessarily add up to one.

B. Simulation Results

The average handoff latencies experienced in case of the three considered schemes are plotted in Fig. 5. The red rectangle's value implies the time taken by the chosen PN to inform a MH regarding the successful pre-handoff operation since the reception of the pre-handoff request message from that MH. We consider the pre-handoff to fail in case that the PN is able to maintain connection with the corresponding MH/AP for a smaller duration than this value. In HMIPv6, no pre-handoff operation takes place and therefore, the pre-handoff delay is considered to be zero. The average handoff latency experienced in PHMIPv6 is a bit longer in contrast with that experienced in CSA-PHMIPv6. The reason behind this is the fact that the number of pre-handoff failures is higher in PHMIPv6 which prompts the nodes to adopt the basic HMIPv6 strategy. As a consequence, the original PHMIPv6 approach suffers from an increase in the average handoff latency.

Fig. 6(a) compares the number of dropped packets for PHMIPv6 and CSA-PHMIPv6 approaches. The former experiences a high number of dropped packets. Indeed, it becomes even worse along with the increase in moving speeds of the considered MH and its corresponding PN(s). On the other hand, CSA-PHMIPv6 achieves significantly lower packet drops. As a consequence, the throughput achieved by the enhanced CSA-PHMIPv6 scheme is much higher compared to that by its original counterpart (i.e., PHMIPv6) as demonstrated in Fig. 6(b). Indeed, CSA-PHMIPv6 attains throughputs over 90Kbps even when the mobile nodes roam at a substantially high speed of 25m/s. In contrast, the original PHMIPv6 shows poor performance in terms of throughput and achieves, at best, a throughput of 90Kbps when the moving speed of each considered node is set to a meager 5m/s. When the mobile nodes roam much faster, PHMIPv6 results in a gradual degradation in the throughput. As the nodes travel much quicker (i.e., at 25m/s), the throughput of PHMIPv6 drops to 84Kbps.

In Fig. 7, the values of the pre-handoff success ratio for different values of the radius of the nodes' ad hoc transmission range, d, are plotted. When d has a relatively larger value, a MH can choose a PN from a larger population of MNs. Then, the communication time between these two nodes increases appreciably. As a consequence, the pre-handoff success rates are higher for the larger values of d. However, the original PHMIPv6 approach chooses the PN based on only the signal strength of the nodes, and this causes the subscribing MH to, at times, select a partner, which may move out of communication range during the pre-handoff operation. This is why the basic PHMIPv6 scheme achieves lower pre-handoff success rates. In contrast, the higher success ratio of the proposed CSA-PHMIPv6 strategy can be attributed to its partner selection based on the LET parameter. Indeed, the pre-handoff success ratio reaches nearly 100% as the ad hoc transmission range exceeds 60 meters.

Fig. 8 demonstrates the pre-handoff failure ratio experienced

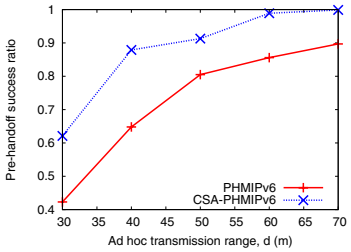


Fig. 7. Pre-handoff success ratio.

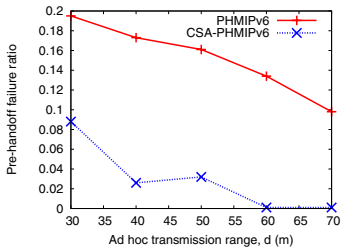


Fig. 8. Pre-handoff failure ratio.

by the PHMIPv6 and CSA-PHMIPv6 schemes. As evident from these results, PHMIPv6 suffers from many pre-handoff failures. The reason behind most of these failed pre-handoff operations is the fact that the chosen PNs and their corresponding MNs moved out of communication range. Fig. 9 demonstrates this idea more clearly by plotting the average and minimum values of LET between a MH and its respective PN for different ad hoc transmission ranges in case of both PHMIPv6 and CSA-PHMIPv6 schemes. The results in this figure reveal that the minimum LET experienced in PHMIPv6 is smaller than the average pre-handoff delay (Fig. 5) as long as d is less than 70 meters. This explains the high pre-handoff failure ratio experienced in case of PHMIPv6. On the other hand, when d equals 70 meters, the minimum LET experienced in PHMIPv6 exceeds the average pre-handoff delay, yet some pre-handoff operations failed. This is most probably because the selected PNs roamed out from the coverage area of the respective APs prior to the completion of the pre-handoff operation. In contrast, in CSA-PHMIPv6, such situations are not encountered as often due to the fact that its partner selection mechanism considers the LETs between PNs and their respective MHs/APs.

V. Conclusion

To overcome its shortcomings, an enhanced version of the original PHMIPv6 protocol called CSA-PHMIPv6 is envisioned in this paper. The proposed scheme permits the handoff mechanisms to effectively exploit cooperative diversity by using the Link Expiration Time parameter. This also ensures the stability of the connection between a subscribing mobile host, its respective partner node, and other involved entities. Furthermore, adequate security features are incorporated within the enhanced design of PHMIPv6 for circumventing malicious threats against the mobile hosts and/or the partner nodes. We have verified the performance of the proposed CSA-PHMIPv6 scheme via simulations. Efficient adoption of cooperative diversity based communications through the proposed approach may indeed prove quite useful to roaming nodes in ad hoc wireless networks and ensure high quality of experience as validated by the simulation results.

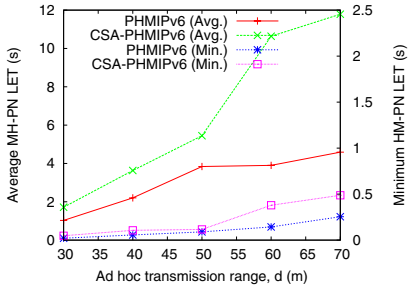


Fig. 9. PN's LET values over different transmission ranges.

Being based on hierarchical centralized mobility management schemes, our approach is also suitable for decentralized schemes like DMA and GPRS Tunnelling Protocol [18]. In DMA short living tunnels between Access Nodes (ANs) are established when a MN roams from one AN to the other. All active connections are forwarded via this tunnel to the MN. As soon as the last of this connection is terminated, the tunnel is teared down. A partner-based pre-handoff procedure, which establishes the tunnel and prepares the new address for the MN, can quicken the handover procedure significantly. Evaluation of this application in our scheme is currently conducted and results should be available shortly.

References

[1] C. Perkins, *"IP mobility support"*, Network Working Group, RFC 2002, Oct. 1996.
[2] D. Johnson, C. Perkins, and J. Arkko, *"Mobility support in IPv6"*, Network Working Group, RFC 3775, Jun. 2004.
[3] H. Soliman, *"Mobile IPv6: Mobility in a wireless Internet"*, Addison-Wesley Professional, 2004.
[4] H. Soliman, C. Catelluccia, K. El Malki, and L. Bellier, *"Hierarchical mobile IPv6 mobility management (HMIPv6)"*, Network Working Group, RFC 4140, Aug. 2005.
[5] Y. S. Chen, W. H. Hsiao, and K. L. Chiu, *"Cross-Layer Partner-Based Fast Handoff Mechanism for IEEE 802.11 Wireless Networks"*, in Proc. IEEE VTC, Baltimore, USA, Sep. 2007.
[6] E. Sakhaee, T. Taleb, A. Jamalipour, N. Kato, and Y. Nemoto, *"A Novel Scheme to Reduce Control Overhead and Increase Link Duration in Highly Mobile Ad Hoc Networks"*, in Proc. IEEE WCNC, Hong Kong, China, Mar. 2007.
[7] Patent: *"Macro diversity handover and fast access station switching in wireless multi-user multi-hop relay networks"*, available at, http://www.freshpatents.com
[8] G. Kirby, *"Locating the user"*, Commun. Int. Mag., Oct. 1995.
[9] A. Hasswa, N. Nasser, and H. Hassanein, *"A Seamless Context-aware Architecture for Fourth Generation Wireless Networks"*, in J. Wireless Personal Communications, Vol. 43, No. 3, Nov. 2007, pp. 1035-1049.
[10] Y. S. Chen, W. H. Chuang and C. K. Chen, *"DeuceScan: Deuce-Based Fast Handoff Scheme in IEEE 802.11 Wireless Networks"*, in IEEE TVT, Vol. 57, No. 2, Mar. 2008, pp. 1126-1141.
[11] I. Ramani and S. Savage, *"SyncScan: Practical Fast Handoff for 802.11 Infrastructure Networks"*, in Proc. IEEE Infocom, Miami, Florida, USA, Mar. 2005.
[12] H. H. Duong, A. Dadej, and S. Gordon, *"Proactive Context Transfer in WLAN-based Access Networks"*, in Proc. Int'l WMASH, Philadelphia, PA, USA, Oct. 2004.
[13] A. Mishra, M. H. Shin, N. L. Petroni, T. C. Clancy, and W. A. Arbaugh, *"Proactive Key Distribution Using Neighbor Graphs"*, in Wireless Commun., Vol. 11, No. 1, Feb. 2004. pp. 26-36.
[14] S. Pack, H. Jung, T. Kwon, and Y. Choi, *"A Selective Neighbor Cashing Scheme for Fast Handoff in IEEE 802.11 Wireless Networks"*, in Proc. IEEE ICC, Seoul, South Korea, May 2005.
[15] W. K. Lai and J. C. Chiu, *"Improving Handoff Performance in Wireless Overlay Networks by Switching Between Two-Layer IPv6 and One-Layer IPv6 Addressing"*, IEEE JSAC, Vol. 23, No. 1, Nov. 2005. pp. 621-628.
[16] T. Kanai and Y. Furuya, *"A handoff control process for microcellular systems"*, in Proc. IEEE VTC, Philadelphia, PA, USA, Jun. 1988.
[17] Network Simulator - NS-2, available at http://www.isi.edu/nsnam/ns/
[18] P. Bertin, Servane Bonjour, and J.-M. Bonnin, *"A Distributed Dynamic Mobility Management Scheme Designed for Flat IP Architectures"*, in Proc. New Technologies, Mobility and Security (NTMS), Tangiers, Morocco, Nov. 2008.