An MPLS-Based Micro-mobility Solution
IEEE-802.21-Based Control Plane

Rajendra Persaud[1], Ralf Wienzek[1], Gerald Berghoff[2], and Ralf Schanko[2]

[1] Chair of Computer Science 4, RWTH Aachen University, Germany
[2] Nokia Networks GmbH, Germany

Abstract. Core network micro-mobility solutions resolve L3 handovers and may be based on the Internet Protocol (IP) or on Multi-Protocol Label Switching (MPLS). When a micro-mobility solution triggers the L3 handover before the L2 handover, it is called predictive, otherwise reactive. The outage period due to the handover is smaller for predictive solutions. However, in order to be predictive, a L3 mobility solution needs support from the underlying link-layer. This support may be provided with the help of IEEE 802.21 that is exploited for intra-technology handovers in WLANs in this paper.

1 Introduction

Each wireless network may be subdivided into an access network and a core network. A mobile device is generally attached with a link-layer (L2) Point of Attachment (PoA) in the access network and a network-layer (L3) PoA in the core network. A handover between two L2 PoAs belonging to the same access network is generally resolved by a L2 mobility solution and called L2 handover. A handover between two L2 PoAs belonging to different access networks is generally resolved by a L3 mobility solution and called L3 handover. Note that a L3 handover includes a L2 handover. The focus of this paper is on L3 handovers.

Such a L3 handover is implemented by a L3 mobility solution which may either be based on the Internet Protocol (IP) or on Multi-Protocol Label Switching (MPLS). The focus of this paper is on MPLS-based intra-domain (i.e. micro-mobility) solutions. Any L3 mobility solution can be viewed as either predictive or reactive. A predictive solution starts the L3 handover before the L2 handover, a reactive solution starts the L3 handover after the L2 handover. The great advantage of a predictive solution is that L2 and L3 handovers can be executed in parallel and not in sequence as in reactive solutions. The outage period in predictive solutions is thus generally lower than in reactive solutions.

In order to help with the decision when to start the L3 handover, the mechanisms of IEEE 802.21 can be used. IEEE 802.21 has been conceived as L2/L3 management layer in order to support L3 mobility solutions for inter-technology handovers. Whenever a technology does not incorporate a mechanism for higher-layer mobility, which is the case for WLANs, IEEE 802.21 can be exploited for intra-technology handovers as well.

IEEE 802.21 provides an Event Service, a Command Service and an Information Service by a Media Independent Handover Function (MIHF). The MIHF

F. Boavida et al. (Eds.): NETWORKING 2006, LNCS 3976, pp. 1119–1124, 2006.

transfers higher-layer commands into corresponding L2 commands and L2 events into corresponding higher-layer events. Although IEEE 802.21 is still in draft status, the basic idea and the basic events, commands and messages are already specified and shall be exploited in this paper.

Note that a handover is primarily an issue for downstream data packets. For upstream data packets, no location updates or redirections of data packets are necessary in the core network.

2 Previous Work

Most IP-based micro-mobility solutions such as Hierarchical Handovers for Mobile IPv6 (HMIPv6) are reactive solutions. The reason is that the mobile device needs to have a new IP address at the new L3 PoA, which it can, in general, only acquire at the new L3 PoA belonging to the new subnet. With IPv6 Stateless Address Autoconfiguration this restriction is removed for IPv6 and exploited by the predictive mode of Fast Handovers for Mobile IPv6 (FMIPv6).

Many MPLS-based mobility management solutions such as [1, 2, 3] propose a combination of MPLS and Mobile IPv4 or of MPLS and HMIPv6. While MIPv4 and HMIPv6 are exploited to provide the signalling necessary for mobility management, MPLS is exploited instead of IP encapsulation for data delivery on the user plane. The main objective is thus to reduce the overhead of IP encapsulation. Since the cited mobility solutions are based on the signalling of MIPv4 and HMIPv6, they are all reactive solutions.

A purely MPLS-based approach introducing the concept of Label Edge Mobility Agents (LEMAs) is presented by [4]. A LEMA is an LER enhanced by a function for mobility management. The objective of deploying LEMAs is to reduce the time needed for the location update at the domain ingress router. The LEMA approach is a reactive MPLS-based micro-mobility solution.

In [5], another purely MPLS-based handover solution is proposed. Before a handover, the traffic of a particular user is sent as part of an aggregated traffic flow over a primary Label Switched Path (LSP) to the previous L3 PoA. During the handover, the user traffic is separated from the aggregated traffic flow and successively placed on handover LSPs leading towards the new L3 PoA. After the handover, the user traffic is re-inserted into an aggregated traffic flow, this time towards the new L3 PoA.

3 Start-Up

The main objective of the start-up procedure is to enable the mobile device to send and receive IP packets. Therefore, the mobile device has to be registered in the core network. If IEEE 802.11 is the underlying L2 technology, the mobile device authenticates and associates with an Access Point (AP) (cf. Fig. 1 (a)). If IEEE 802.11i is used, the AP has to be capable of using an Authentication, Authorization and Accounting (AAA) protocol such as Remote Dial-In User Service (RADIUS). Since the AP located in the access network would have to

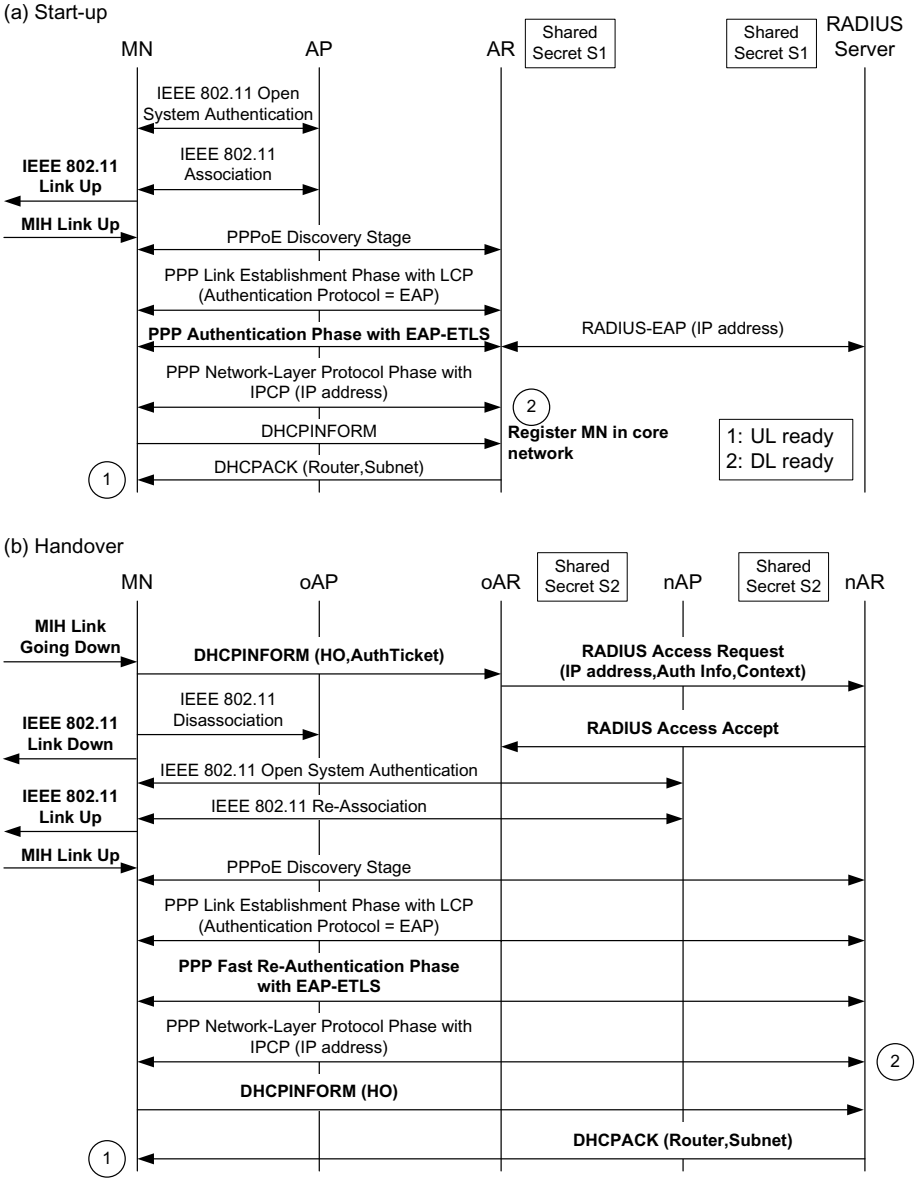

Fig. 1. Start-up and handover for IEEE-802.11-based access networks using PPP (extensions/adaptations in bold)

communicate with the RADIUS server located in the core network, which might be undesirable if the access and core networks are administered by different providers, we propose to use the Point to Point Protocol (PPP) and PPP over Ethernet (PPPoE) so that the actual authentication can be done between the

mobile device and the Access Router (AR) in the core network. In that case, Open System Authentication is used as IEEE 802.11 authentication.

The MIH Link Up event can be used as trigger to establish a PPP connection between mobile device and AR. In the PPP Link Establishment phase based on the Link Control Protocol (LCP), the AR makes use of the Authentication-Protocol Configuration Option set to Extensible Authentication Protocol (EAP).

In the subsequent Authentication phase that is initiated by the AR as EAP Authenticator in pass-through mode, the mobile device authenticates to a back-end RADIUS server. We propose to use Transport Layer Security (TLS) and an extension to EAP-TLS (EAP-ETLS) to support Fast Re-Authentication for handovers. EAP-ETLS is designed to be downwards compatible to EAP-TLS. In EAP-ETLS, the type-data field of the EAP-Request/Identity contains the public key $Publ_{AR}$ of the AR. For the start-up procedure, $Publ_{AR}$ is not needed and can be ignored. At the end of the EAP exchange, the mobile device (also called Mobile Node (MN)) and the AR share a master key from which a session key (S_{MN-AR}) can be derived. The session key is used for securing control plane and optionally also user plane messages between MN and AR.

If the authentication is successful, the MN is allowed to proceed to PPP Network-Layer Protocol phase where it uses IP Control Protocol (IPCP) to obtain an IP address. The IP address has been handed to the AR by the RADIUS server during the PPP Authentication phase. Finally, the MN needs to obtain further L3 configuration information that may be obtained through DHCP. We propose to exploit the DHCPINFORM message as trigger to register the MN in the MPLS-based core network.

4 Handover

In order to reduce the outage period for the mobile device, the L3 handover is triggered before the L2 handover. In principle, two issues have to be solved. One is to redirect the data packets to the new L3 PoA as fast as possible, which has been solved by [5]. If data packets are redirected to the new L3 PoA and arrive there before the mobile device attaches with it, the new L3 PoA may buffer these data packets. However, it may not start delivering the buffered data packets as soon as the mobile device attaches with it since the mobile device has to be authenticated before. If authentication is done with a distant AAA server, the outage period is certainly not reduced. Therefore, the other issue is to re-authenticate the mobile device at the new L3 PoA as fast as possible, which is shown in the following.

We propose a (new) Handover (HO) Option for the DHCPINFORM message. The HO Option shall contain the IP address of the previous AR and, if broadcast by the previous AP or AR or obtained by some other means, the IP address of the new AR, otherwise the Basic Service Set ID (BSSID) of the new AP. It shall further contain an authentication ticket to provide fast re-authentication with the new AR. The authentication ticket (cf. (1)) consists of a handover sequence number (HOSeqNo), a new master key nMK (a random number chosen by the

MN), and a unique identifier MNID of the MN (e.g. L2 address, L3 address, etc.). The new master key nMK and the MNID are encrypted with a randomly chosen secret key SK so that the receiving old AR cannot decrypt them. The handover sequence number is used to prevent replay attacks and to avoid misconfigurations in the core network. The authentication ticket is itself protected with the secret key S_{MN-oAR} (cf. Section 3 where it is denoted as S_{MN-AR}) used between MN and old AR.

$$AuthTicket := \{HOSeqNo, (nMK, \text{MNID})_{SK}\}_{S_{MN-oAR}} \quad (1)$$

When IEEE 802.21 is used, the Link Going Down event issued at the MN on L2 can be used as trigger for the DHCPINFORM message.

On receipt of the DHCPINFORM message (cf. Fig. 1 (b)), the old AR evaluates the HO Option enabling it to contact the new AR for context transfer. We propose to exploit RADIUS that is subject to continuous extensions for different purposes. The RADIUS message shall contain $(nMK, \text{MNID})_{SK}$ decrypted from (1), and the context of the MN, i.e. the MNID and all further information that is necessary to receive and send IP packets from and to the MN at the new AR.

Note that the context transfer can be performed in parallel to the L2 handover, which is done by disassociating from the previous AP and re-associating with the new AP. After PPPoE Discovery and the PPP Link Establishment phase, the PPP Authentication phase can be kept short due to the context transfer. This phase is thus called Fast PPP Re-Authentication phase.

On receipt of the EAP-Request/Identity containing the public key $Publ_{nAR}$ of the new AR, the MN sends an EAP-Response/Identity to the new AR where the type-data field contains both the $AuthTicket$ and the following $ReAuthTicket$.

$$ReAuthTicket := \{\text{MNID}, oAR, (SK)_{Publ_{nAR}}, HMAC_{nMK}(Publ_{nAR})\} \quad (2)$$

$HMAC_{nMK}(Publ_{nAR})$ is a Hashed Message Authentication Code (HMAC) computed over $Publ_{nAR}$ and seeded with nMK, the same random number that the MN used in the authentication ticket sent to the old AR (cf. (1)). On receipt of $ReAuthTicket$, the new AR uses the MNID to retrieve $(nMK, \text{MNID})_{SK}$. If the new AR has not yet received the RADIUS message containing $(nMK, \text{MNID})_{SK}$, it sends a RADIUS message including $AuthTicket$ to the previous AR in order to trigger the fast re-authentication. Once in possession of $(nMK, \text{MNID})_{SK}$, it decrypts SK from (2) with its private key and is then able to decrypt nMK and MNID. The decrypted MNID serves to verify that the context the new AR received from the old AR indeed belongs to the MN having sent the $AuthTicket$. The HMAC serves to verify that $ReAuthTicket$ has been sent by the same MN as $AuthTicket$. As the new AR receives the authentication ticket from a trustworthy partner, i.e. from the old AR, over a secure channel, the MN is authenticated and the new master key nMK is established. With only three messages and without the necessity of contacting a RADIUS server the procedure is fast and, with the exception of two public-key operations, the computational overhead is low.

In the subsequent PPP Network-Layer Protocol phase, the MN asks to be assigned the same IP address as before. In order to notify the new AR on its

arrival, the MN sends a DHCPINFORM containing the HO Option, yet without *AuthTicket* that is not necessary there. If the new AR has not yet received a handover notification message from the previous AR, it sends a handover indication message to the previous AR in order to trigger the handover procedure. The new AR finally acknowledges the DHCPINFORM with a DHCPACK containing all necessary configuration information such as gateway address and subnet mask. The DHCPACK completes the handover.

5 Conclusion

This paper has shown that MPLS-based micro-mobility solutions may be triggered before the corresponding L2 handover by exploiting IEEE 802.21. The outage period is, however, only reduced for the mobile device when both packet redirection at the previous L3 PoA and the re-authentication at the new L3 PoA are done in a fast and efficient way. Both issues can be solved as shown in this paper. DHCP is exploited for handover indication. A new HO Option is introduced in order to distinguish a handover trigger from a conventional DHCP message. Security has been addressed by EAP-TLS. In order to allow for fast re-authentication during handover, EAP-ETLS has been introduced as extension. Inter-technology handovers have not been covered in this paper. For inter-technology handovers, a mobile device has to be equipped with at least two L2 interfaces of different technologies. Furthermore, a L2 interface change requires a mobility management entity in the mobile device. The issue of inter-technology handovers thus remains for further study.

References

1. Ren et al., Z.: Integration of mobile ip and multi-protocol label switching. In: IEEE International Conference on Communications. (2001)
2. Vassiliou et al., V.: A radio access network for next generation wireless networks based on multi-protocol label switching and hierarchical mobile ip. In: Proceedings of the 56th IEEE Vehicular Technology Conference. (2002)
3. Vassiliou et al., V.: M-mpls: Micromobility-enabled multiprotocol label switching. In: IEEE International Conference on Communications. (2003)
4. Chiussi et al., F.: A network architecture for mpls-based micro-mobility. In: IEEE Wireless Communications and Networking Conference. (2002)
5. Persaud et al., R.: An mpls-based handover solution for cellular networks. In: 19th International Teletraffic Congress (ITC). (2005)