Secure Mobile IPv6 for Mobile Networks based on the 3GPP IP Multimedia Subsystem

Domenico Celentano, Antonio Fresa, Maurizio Longo,
Fabio Postiglione, Anton Luca Robustelli

***Abstract*—The rapid spread of new radio access technologies and the consequent service opportunities have stimulated the technical and scientific community to investigate future evolution scenarios for 3rd Generation networks (3G), generically referred to as Beyond-3G or 4G. They are going to be characterized by ever stronger requirements for security, as well as the capability for the final users to experience continuous connectivity and uninterrupted services of IP applications as they move about from one access network to another. Key issues are: i) security provision for applications exchanging data in diverse wireless networks; ii) seamless mobility (handoff) between different coverage domains and, in case, access technologies. Since many proposals are based on the use of the Mobile IPv6 protocol, in this paper we analyze the security threats emerging from some Mobile IPv6 mechanisms for mobility management, and we propose a solution against such threats, under the assumption that both end users (mobile or not) are attached to a Mobile IPv6-enabled 3GPP IP Multimedia Subsystem network.**

***Index Terms*—IP Multimedia Subsystem, Mobility management, Mobile IP version 6, Security, Inner Attacks.**

I. INTRODUCTION

THE rapid advancement of wireless technologies and the emergence of multimedia data services have determined a fast evolution of mobile cellular networks towards the third generation (3G) in just two decades. Recently, the studies about next generation mobile networks have come under the name of *Beyond-3G* (B3G). The vision of a B3G network is that of a user-centric network providing broadband mobile access using different technologies and seamless global roaming. A B3G network will be IP-based and will allow mobile users to use the most appropriate technology for each connection and service, according to the *Always-Best-Connected* (ABC) [1] concept. The organization specifically set up for standardization of 3G-and-beyond networks, called 3GPP, has defined a network infrastructure, named the *IP Multimedia Subsystem* (IMS) [2, 3], which adopts the *Session Initiation Protocol* (SIP) for signalling [4]. IMS will provide all real-time multimedia services (video conferencing, presence services, multi-party gaming, content sharing etc.) to mobile users through the IP technology.

Recent developments tend to converge towards the general adoption of *Mobile IPv6* (MIPv6) [5] as the unified mobility layer allowing to stitch together various and mutually incompatible radio access technologies (WCDMA, CDMA2000, EDGE, WiFi, WiMAX, etc.) in order to allow seamless vertical (inter-technology) roaming, service continuity and ABC provision to mobile users. In particular, MIPv6 permits an IPv6 user terminal to be reached and to reach other users while roaming across various subnets. Unfortunately, MIPv6 presents some security vulnerabilities when adopted in heterogeneous wireless networks. In particular, serious security threats are currently associated to the delivery of messages sent by a mobile terminal, during a roaming activity, towards other corresponding users when notifying its new MIPv6 contact address.

Our purpose is to propose an overall architecture, integrating the MIPv6 framework within the SIP-based IMS networks, which provides telephone- class security standards. More specifically, we improve the security level of MIPv6 signalling messages exchanged in order to allow seamless session continuity in case of mobility.

The present paper is structured as follows. After introducing the IMS scenario in Section 2, we describe in Section 3 the MIPv6 protocol, its security mechanisms and vulnerabilities. In Section 4 we propose our architectural solution to provide seamless secure mobility in a B3G IMS-based scenario. In Section 5 some mechanisms are described to provide secure MIPv6-based roaming to B3G mobile users, both in case of attacks from users not involved in the communication and of malicious behaviours by the communicating nodes themselves.

II. THE IMS SCENARIO

The IMS will play a central role in B3G all-IP networks as it offers telecom operators the opportunity to build a unified and open service infrastructure that will enable an easy deployment of new and rich real-time multimedia communication services, thus determining a merging of present telecommunication and data services.

3GPP adopted SIP as the signalling protocol for setup, modification and tear-down of the multimedia sessions and

Manuscript received April 02, 2007 and revised May 18, 2007. This paper was presented in part at the Conference on Software, Telecommunications and Computer Networks (SoftCOM) 2006.

D. Celentano, A. Fresa, and A.L. Robustelli are at Co.Ri.TeL - Via Ponte Don Melillo, I-84084 Fisciano (SA), Italy (e-mail: {celentano,fresa,robustelli}@coritel.it).

M. Longo and F. Postiglione are with Università degli Studi di Salerno - Via Ponte Don Melillo, I-84084 Fisciano (SA), Italy (e-mail: {longo,fpostiglione}@unisa.it).

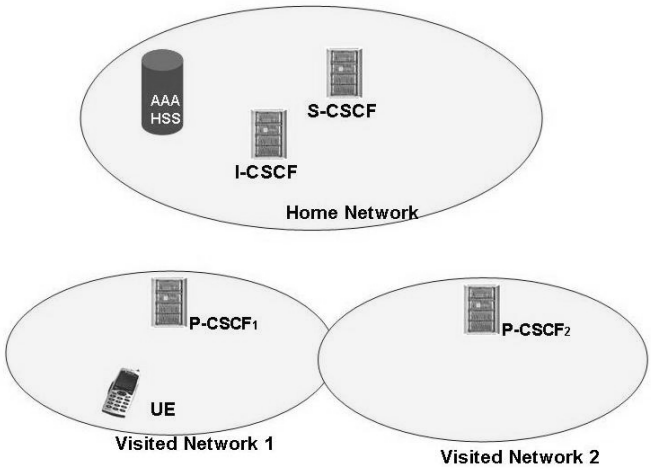

Fig. 1. IP Multimedia Subsystem

introduced the *Call Session Control Function* (CSCF) servers that represent the core elements, within the IMS, for the management of SIP signalling. The CSCFs perform several functions in relation to the received SIP messages, such as multimedia session control, user profile management and address translations.

The CSCF functionalities are distributed among three different types of SIP servers (see Fig. 1): a *Proxy CSCF* (P-CSCF), usually located in the *Visited Network*, that represents the first contact point for the user terminal towards the IMS network and takes care of forwarding the SIP signalling towards the subscriber's *Home Network*; an *Interrogating CSCF* (I-CSCF), located in the subscriber's Home Network and responsible for the selection of the appropriate *Serving CSCF* (S-CSCF) according to the capacity and current workload of the latter; an S-CSCF, located again in the subscriber's Home Network, which is the main node among the CSCFs and processes the SIP signalling, takes decisions and manages the multimedia sessions.

Another important function of the IMS architecture is the *Home Subscriber Server* (HSS), a database located within the Home Network that contains all the user-related subscription data required to handle a multimedia session: the S-CSCF serving the user, information on user location, security data and user profiles. The interaction among the three CSCF nodes and the HSS allows the complete management of the SIP signalling necessary for the establishment and support of the multimedia sessions.

In such a scenario, a top priority for both users and operators is to achieve secure communications. Our goal is to increase the security level of the mobility-related signalling exchanges, in order to provide a robust framework guaranteeing certainty about roaming users' identities, and to prevent session hijackings and attacks based on the mobility activity. The next section details a MIPv6-based approach to provide inter-technology seamless mobility by guaranteeing session continuity, and points out its specific vulnerabilities.

III. Security Vulnerabilities of Mobile IPv6 and Return Routability Procedure

The Mobile IPv6 (MIPv6) protocol represents a possible technique to provide both vertical (inter-technology) and horizontal (inter-domain) seamless mobility in a B3G context. It is a network-layer protocol. In principle, it is possible to provide mobility support at the Application or Transport layers as well, but one needs to cope with transport-layer *survivability* issues by costly adaptations to the applications or provide transport-layer-based solutions, which need very expensive modifications to the widely deployed transport protocols.

Instead, MIPv6 extends IPv6 in order to make the transport layer and hence applications completely unaware of the changes in address configurations. By means of MIPv6, application and transport layer protocols can always refer to a single IPv6 address that is permanently assigned to the MIPv6 node, and which does not change because of mobility: such address is called *Home Address* (HoA) and remains unchanged regardless of the *Mobile Node* (MN)'s current location. Henceforth, by the term of MN we refer to a *User Equipment* (UE) that roams from one network to another; and that is identified by a permanent HoA assigned by its *Home Network* (HN) and belonging to the HN's address space. The other components in the MIPv6 framework are the *Home Agent* (HA), which is a router located in the HN that maintains registrations of mobile nodes that are away from home, together with their current temporary *Care-of-Addresses* (CoAs), and the *Correspondent Node* (CN), which is a generic IPv6 node having a communication in progress with the MN. A correspondent node does not have to be necessarily MIPv6-compliant.

When the MN, while roaming away from its HN, detects a new access network (*Visited Network* – VN) through the *Neighbor Discovery* [6] mechanism or *Dynamic Host Configuration Protocol for IPv6* (DHCPv6) [7], it acquires a temporary CoA from the VN (belonging to the VN's address space) by means of either a stateless or stateful address configuration process. This mechanism ensures that the MN always has a temporary MIPv6 address consistent with the network segment (subnet) which it is currently attached to. Subsequently, it notifies its new current position to its HA by sending an appropriate *Binding Update* (BU) message. MIPv6-compliant Correspondent Nodes and Home Agents maintain information about MN bindings in a *Binding Cache*, whereas MNs maintain information about correspondent nodes in a *Binding Update List*.

MIPv6 adopts the *Routing Header Type 2* and the *Home Address Option* headers in order to be transparent to the upper layers and avoid session interruptions. As a consequence, every packet addressed to the MN (i.e. to its HoA) reaches the HA which then forwards it to the MN at its current CoA (*triangular routing*). However, MIPv6 contemplates an optimization of such costly mechanism: if the CN supports

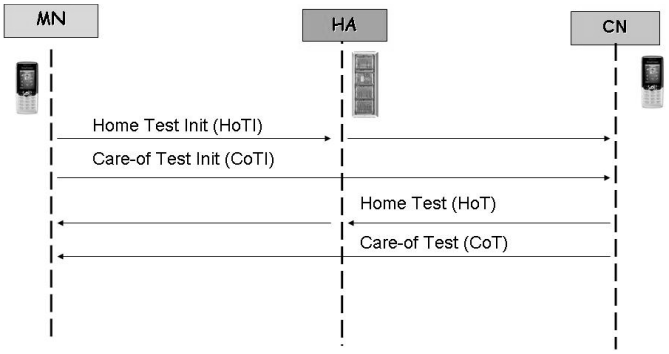

Fig. 2. The RRP mechanism

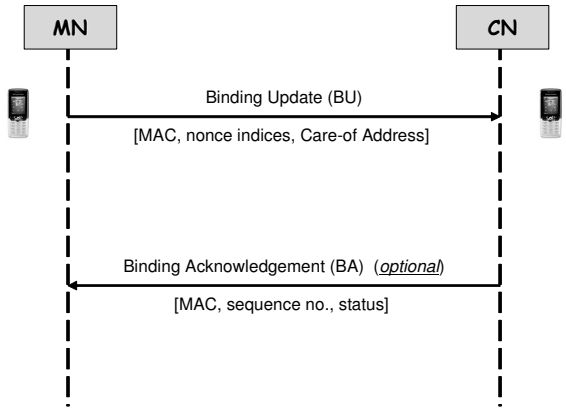

Fig. 3. BU and BA messages from MN to CN

MIPv6, the MN can choose to notify its current CoA to the CN, too, by sending an appropriate BU message to it; in this way the MN requests the CN to send further packets directly to its CoA. This mechanism, called *Route Optimization*, eliminates the triangular routing through the HA and hence reduces the end-to-end delays: this is typically necessary for real-time communications in order to avoid QoS degradations due to delay.

Unfortunately, MIPv6 presents some security vulnerabilities when adopted in heterogeneous wireless networks. In particular, possible security threats are associated to the BU messages sent by the MN to its CN(s), whereas security between MN and HA is guaranteed by the adoption of IPsec [8] together with the *Encapsulation Security Payload* (ESP) protocol [9]. Indeed, when the MN changes access network and therefore acquires a new CoA, the *IPSec Security Association* (SA) between HA and MN is not affected at all: the use of MIPv6 Routing Header Type 2 and Home Address Option assures that such address change happens in a totally transparent way to the existing IPsec SA. That is, such a SA does not need to be renegotiated nor re-created, thus avoiding any supplementary delay in the communication.

On the other hand, BU messages between MN and CN(s) can be protected by the recently proposed *Return Routability Procedure* (RRP), shown in Fig. 2. According to RRP, the MN sends two different messages to the CN along two different paths. The CN will answer with two messages following the same paths as the requests. In detail, after the acquisition of a CoA and the subsequent BU with the HA, the MN sends two packets to the CN carrying two different cookies: the first packet (*Home Test Init*, HoTI) is addressed to the HA and then routed to the CN, while the latter (*Care-of Test Init*, CoTI) is sent directly to the CN and will therefore follow a different route. The MN stores these cookie values in order to obtain some assurance that the subsequent corresponding answers (which will be carrying the same cookies) were generated by the authentic CN.

Consequently, the CN generates a *Home Keygen Token* and a *Care-of Keygen Token*, as shown in Fig. 3, and sends them (see Fig. 2) respectively to the MN's HoA through the HA (encapsulated in the *Home Test* – HoT answer) and directly to the MN's CoA (encapsulated in the *Care-of Test* – CoT answer).

These two tokens will then be used by the MN to generate a key necessary to authenticate the subsequent BU towards the CN. The use of two different paths and two different addresses (HoA and CoA) for the two test messages provides some proof to the CN that the MN is reachable at both its HoA (and then no *Impersonation Attack* by a third party should be under way) and its CoA (so as to avoid *Bombing Attacks* where a malicious MN provides a fake CoA redirecting all CN traffic towards a victim third party).

The CN holds a private secret key, K_{cn}, and random numbers (*nonces*), which it renews at regular intervals. The *Home Keygen Token* and the *Care-of Keygen Token* are formed from the first 64 bits of the HMAC_SHA1 hashing function [10,11], with key K_{cn}, of the concatenations ($HoA|nonce|0$) and ($CoA|nonce|1$), respectively:

$$\begin{aligned} &Home\ Keygen Token = \\ &\quad = First\left(64, HMAC\_SHA1\left(K_{cn}, (HoA \mid nonce \mid 0)\right)\right), \end{aligned} \tag{1}$$

$$\begin{aligned} &Care-of\ Keygen Token = \\ &\quad = First\left(64, HMAC\_SHA1\left(K_{cn}, (CoA \mid nonce \mid 1)\right)\right), \end{aligned} \tag{2}$$

where "|" is the concatenation operator between two binary strings.

The SHA1 hashing function [11] of the concatenation of the *Home Keygen Token* and the *Care-of Keygen Token* provides the MN with the key K_{bm} necessary to the CN for authentication of the subsequent BU:

$$K_{bm} = SHA1\left(Home\ Keygen Token \mid Care-of\ Keygen Token\right). \tag{3}$$

Fig. 3 shows the structure of the resulting BU message. The *Message Authentication Code* (MAC) value is formed as the first 96 bits of the HMAC_SHA1 hashing function, with key K_{bm} derived in (3), of the concatenation of *CoA*, *CN address*

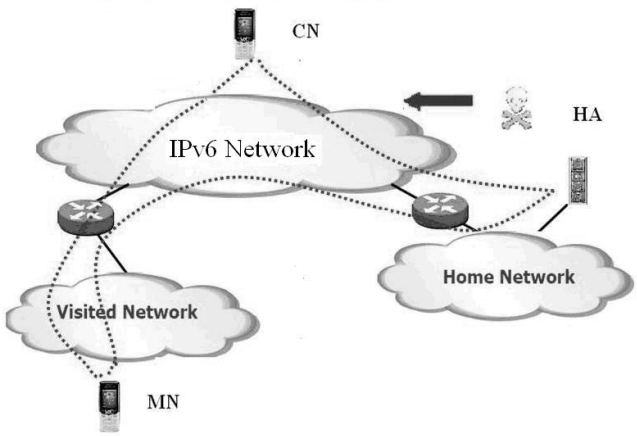

Fig. 4. An RRP vulnerability

and the other fields composing the standard BU message (BU_f):

$$MAC = \\ = First\left(96, HMAC\_SHA1\left(K_{bm}, \left(CoA \mid CN\ Address \mid BU_f\right)\right)\right) \quad (4)$$

Such MAC value is then encapsulated within the BU. If the authentication data of the BU is valid, the CN adds an entry in its *Binding Cache* for the particular MN and sends back a *Binding Acknowledgement* (BA) message. Upon receipt of the BA message, the MN adds an entry to its Binding Update List for the CN.

In this procedure we can notice that the link MN-HA is protected by IPsec [9], but when the message from the HA is forwarded to the CN, it lacks any type of protection, as depicted in Fig. 4. Then the risk arises that a malicious node, aware of a session between MN and CN, might simulate a handoff of the MN by sending fake HoTI and CoTI messages to the CN, so obtaining K_{bm}. Then it might send a fake BU to the CN in order to redirect the MN-CN communication towards itself (*Impersonation Attack*) or possibly also forward the traffic to the MN after analysing it (*Man-In-The-Middle* attack).

IV. Deploying MIPv6 In IMS Networks

This section analyses the addressing mechanism used for IMS SIP-based transactions, the architectural implications of the SIP signalling infrastructure and the advantages of the integration of MIPv6 within IMS for both mobility management and security.

The IMS defines a security mechanism which verifies that the IPv6 packet source address of SIP messages originating from the MN corresponds to the IPv6 address reported in the SIP headers, hence requiring that the MN use the same address (i.e., either the HoA or the CoA) for both the IPv6 packet source address and the IPv6 address used at SIP level (i.e. within SIP headers).

Therefore, several scenarios are possible for address management [12]. *(i)* The MN may use the CoA as source address and then provide it at SIP registration and for session establishment. In such a way, the MN needs to re-register the new CoA with the Serving-CSCF every time it changes its point of attachment to the network; this corresponds to using *SIP mobility*. In real-time communications this would cause loss of RTP packets while the re-INVITE procedure is completed while not guaranteeing TCP-based session continuity. *(ii)* The MN provides both the CoA and HoA within SIP signalling. This requires changes to current SIP standards and therefore it is neither easily feasible nor recommended. *(iii)* The MN provides the HoA at SIP registration, for session establishment and as IPv6 source address. In this way the MN does not need to re-register or re-invite other nodes when it changes CoA, but it updates the new CoA through MIPv6 signalling. If we suppose that the SIP proxy (P-CSCF), supports the MIPv6 stack, then the SIP application can be completely unaware of changes of the MN's CoA.

The third solution appears as the most promising by virtue of its efficiency and low impact on existing applications, protocols and nodes.

V. A Solution to MIPv6 Security Threats

A solution is now presented to address the security vulnerabilities reported in Sect. 3 in an MIPv6-enabled IMS network.

The P-CSCF, acting as a CN for all MNs registered to the IMS through it, stores a *Binding Update List* (BUL) containing all the HoA–CoA associations for those MNs. At SIP registration, a MN provides its HoA as its SIP contact entity, and its current CoA, through a specific BU (updated after every MN handoff), which does not require the RRP because the link MN–P-CSCF is protected by an IPsec ESP tunnel.

As in [13], we propose to create at call setup (INVITE message) the authentication key K_{bm} necessary for the subsequent MN-CN BU authentication procedures, and to distribute it to the MN and CN within the body of the SIP 200 OK and ACK messages, instead of using the RRP procedure. In this way, security management is entirely delegated to the IMS infrastructure. Indeed, the K_{bm} authentication key can be generated by the *Authentication, Authorization, Accounting* (AAA) Server and distributed as depicted in Fig. 5. The key distribution is secured by the already standardized adoption of IPsec with ESP between any SIP user (MN and CN) and its own P-CSCF. It is important to highlight that this procedure is performed only at the beginning of a communication session, while the standard MIPv6 RRP between MN and CN should be repeated, together with the BU, after *every* terminal handoff. Such improvement can appreciably reduce end-to-end delays during real-time communications. In fact, as shown in Fig. 6, in standard MIPv6 the total handoff time is the sum of T_d (movement detection time), T_c (configuration time), T_r (binding registration time) and T_o (route-optimization time),

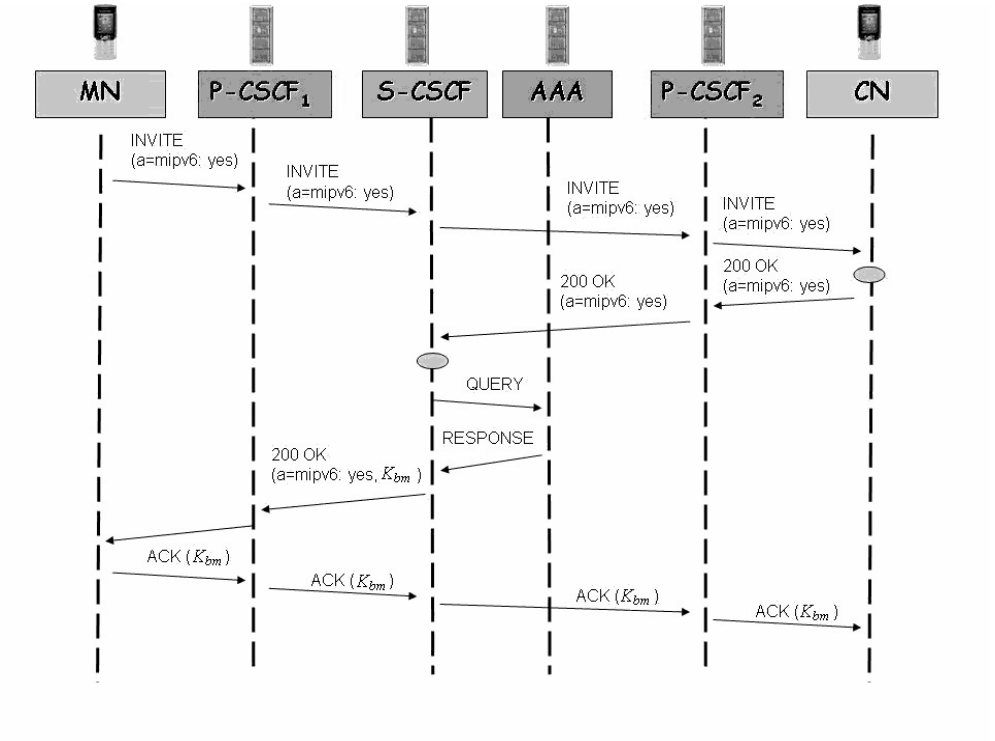

Fig. 5. Generation and distribution of the authentication key [13]

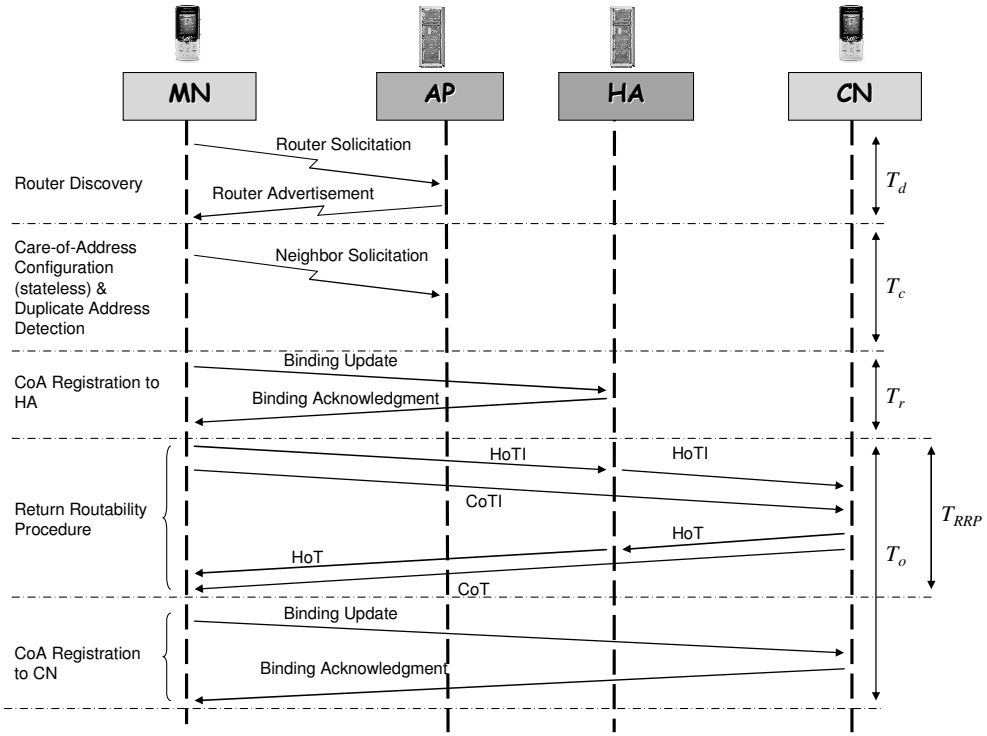

Fig. 6. Delays during a mid-session handoff procedure [13]

which includes T_{RRP} (RRP time). In our proposal the T_{RRP} delay is completely eliminated.

We refer to [13] for further details on this mechanism and quantitative estimations of delay reduction.

A. A Solution for Protection from Inner Attacks

Note, however, that using the K_{bm} key alone would protect from attacks by third parties, but not by the mobile nodes involved in the communications in case they behave

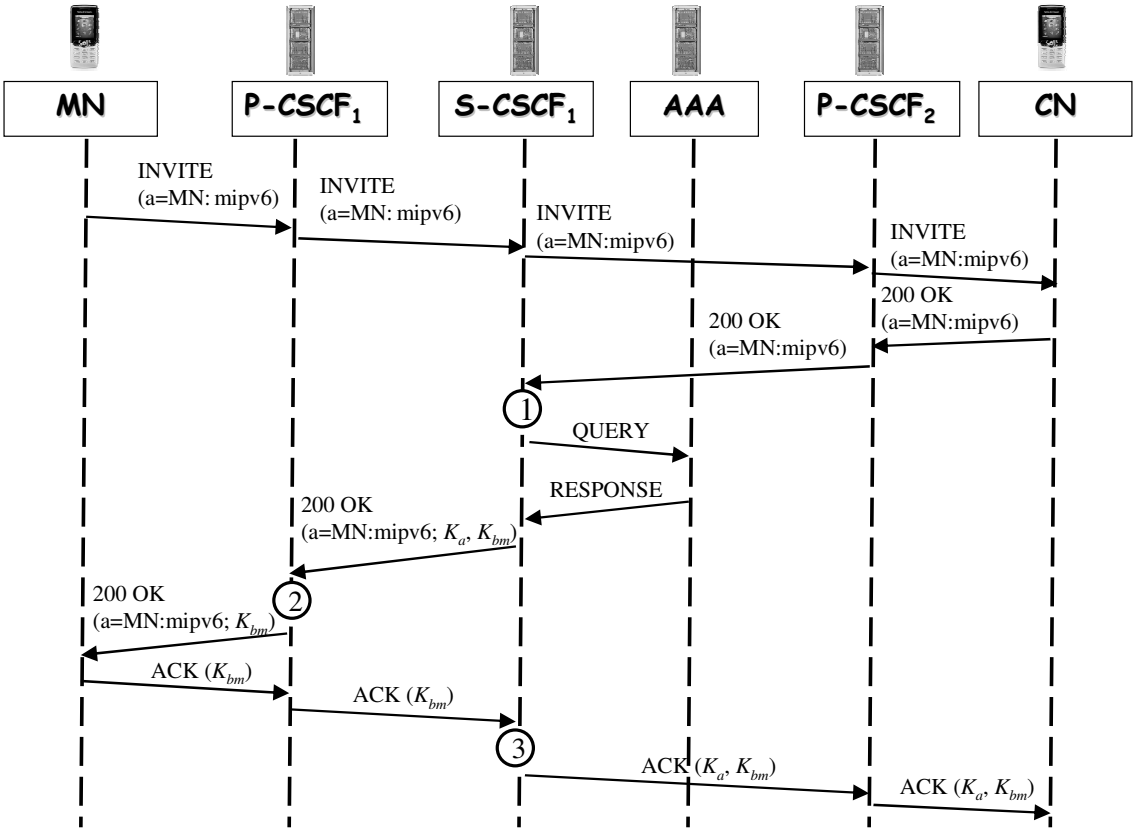

Fig. 7. Generation and distribution to P-CSCF$_1$ and CN of the authentication key K_{bm} and the additional key K_a

themselves maliciously. For instance, as already reported in [14], an ill-intentioned MN could send fake BUs to various CNs, so making them believe it has acquired a new CoA, which on the contrary corresponds to the address of a particular user it is willing to attack (*Bombing Attack*).

Obviously, if a sufficient number of different CNs is involved in such an attack, the resources of the victim node might be saturated.

Our proposal against this kind of threats is based on the use of the AAA server and is essentially a generalization of our previous proposals in [13] and [14]. Under the assumption that the caller (here, MN) is the only node to require handoff procedures (the CN is considered to be attached to one and the same base station throughout the session), the AAA server must generate an additional key, named K_a, which is then distributed during the INVITE phase to P-CSCF$_1$ and the CN, but not to the MN. Then, a new key distribution mechanism is necessary.

It can be derived by modifying the one reported in Fig. 5, as described in Fig. 7. The additional key K_a is distributed to P-CSCF$_1$ (the operation is marked by a tag 1 in Fig. 7) and the CN (the S-CSCF re-introduces K_a in the ACK generated by the MN and addressed to the CN – tag 3 in Fig. 7) but it is not forwarded to the MN (P-CSCF$_1$ removes K_a from the 200 OK message before sending it to the MN – tag 2 in Fig. 7).

The MN notifies its support of the MIPv6 protocol by means of a *Session Description Protocol* (SDP) [15] attribute, namely a=MN:mipv6, conveyed within the SIP INVITE message. If present, the S-CSCF asks the AAA server for both the authentication key K_{bm} and the additional key K_a.

B. Binding Update Procedure vs. the Proposed Security Key K_a

The MN, after roaming to a new subnet (not necessarily controlled by a different P-CSCF) and acquiring a new CoA, namely CoA_n, sends a BU message to its P-CSCF$_1$; in the subsequent BA answer message the MN is provided with a value *CoA–Auth* generated by P-CSCF$_1$ as a hash function *SHA1*( ) of K_a and CoA_n:

$$CoA - Auth = SHA1(K_a, CoA_n), \tag{5}$$

as shown in Fig. 8.

The subsequent BU from MN to CN will then include the value *CoA–Auth* instead of CoA: the former is used by the CN (together with K_a) to authenticate the new MN's CoA, as reported in Fig. 9. The MAC is computed through (4), in order to avoid fake BUs generated by malicious third parties, as previously explained.

It is worth noting that a new "*IMS Care-of-Address Authentication"* MIPv6 Mobility Option must be adopted, in order to include the *CoA–Auth* value in the BA and BU messages.

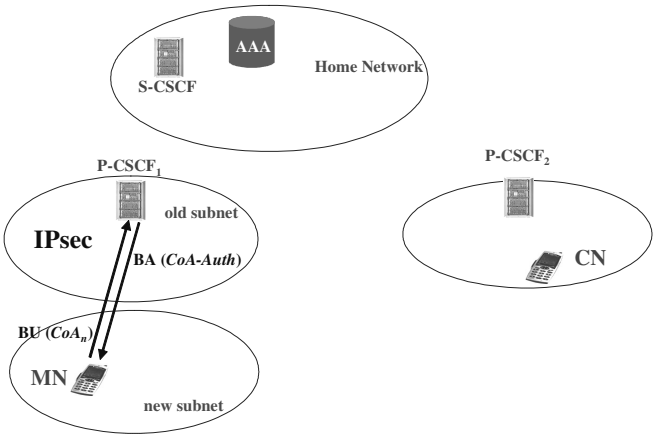

Fig. 8. A Binding Update from MN to P-CSCF$_1$, followed by a BA containing CoA-Auth

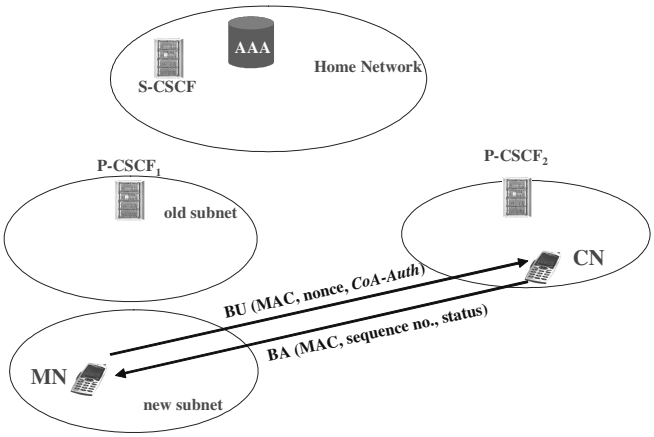

Fig. 9. Authentication of CoA$_n$ by means of CoA-Auth and K_a, during a Binding Update between MN and CN

C. A More General Solution for Inner Attacks Protection

The previous solution works under the assumption that the MN is the only node able to move and thus to initiate a handoff procedure. If the *called node* (previously named CN, now MN$_2$) is a mobile user as well, then an equivalent key named $K_a^{(2)}$ must be introduced to avoid malicious operations by the called party. This scenario is represented in Fig. 10, where we assume that MN$_1$ and MN$_2$ are subscribed to different mobile operators and thus refer to different S-CSCFs, namely S-CSCF$_1$ and S-CSCF$_2$.

Here, the AAA server, interrogated by S-CSCF$_1$ during session setup, plays the role of a AAA Proxy, which should contact the AAA server (connected to the HSS database) of MN$_2$'s Home Network, if it is required that $K_a^{(2)}$ be generated by the security infrastructure of the telecom operator responsible for MN$_2$.

In our proposal, only S-CSCF$_1$ uses the AAA infrastructure (by means of the Diameter protocol [16]), in order to obtain the keys K_{bm}, K_a (if the SDP attribute a=MN$_1$:mipv6 is present), and $K_a^{(2)}$ (if MN$_2$ supports MIPv6 and modifies the SDP attribute into a=MN$_1$,MN$_2$:mipv6 – tag 1 in Fig. 10). Afterwards, S-CSCF$_1$ encapsulates the keys (tag 2 in Fig. 10) into the SIP 200 OK message toward the P-CSCF$_1$, which removes K_a (tag 3). Then, S-CSCF$_1$ re-introduces all the keys (tag 4) in the ACK message from MN$_1$ to P-CSCF$_2$ and MN$_2$. Finally, P-CSCF$_2$ removes $K_a^{(2)}$ from the ACK message (tag 5) and forwards it toward MN$_2$.

In case of handoff of either MN$_1$ or MN$_2$, the BU mechanism follows, *mutatis mutandis*, the procedure described in Sect. 5.2.

VI. CONCLUSION

In this paper we propose a way to secure MIPv6-based mobility within the *IP Multimedia Subsystem* network domain for seamless session mobility purposes, where the IMS centralized AAA server generates, manages and distributes the MIPv6 authentication keys involved in the Binding Update procedures, thus increasing security and allowing telecom operators to have access to all the mobility-related information (mobility sessions, data records, etc.). Under the assumption that mobile nodes are attached to the IMS, the costly MIPv6 *Return Routability Procedure* is avoided, so considerably increasing the overall MIPv6 security level as a vulnerability in the Home Agent-Correspondent Node link is eliminated. Furthermore, the number of messages exchanged during handoffs between terminals and network is reduced with respect to standard MIPv6, and the handoff latency consequently minimized, as already shown in [13] and [14].

In particular, in this paper we address the problem of protecting users in case the malicious node is one of the mobile nodes involved in the communications and we present a general solution which meets such possible threats. However, in order to achieve this a new "*IMS Care-of-Address Authentication"* MIPv6 Mobility Option should be introduced.

REFERENCES

[1] E. Gustafsson, A. Jonsson: *Always best connected*, IEEE Wireless Communications, Vol.10, No. 1, pp. 49 –55, February 2003.

[2] 3GPP, Tech. Spec. 22.228 version 8.1.0, Service requirements for the Internet Protocol (IP) multimedia core network subsystem; Stage 1 (Release 8), September 2006.

[3] 3GPP, Tech. Spec. 23.228 version 8.0.0, IP multimedia subsystem (IMS); Stage 2 (Release 8), March 2007.

[4] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler (2002 June): "SIP: Session Initiation Protocol", IETF RFC 3261, Available: http://www.ietf.org/rfc/rfc3261.txt.

[5] D. Johnson, C. Perkins (2004, June): "Mobility Support in IPv6", IETF RFC 3775, Available: http://www.ietf.org/rfc/rfc3775.txt.

[6] T. Narten, E. Nordmark, W, Simpson (1998, December): "Neighbour Discovery for IP Version 6 (IPv6)", IETF RFC

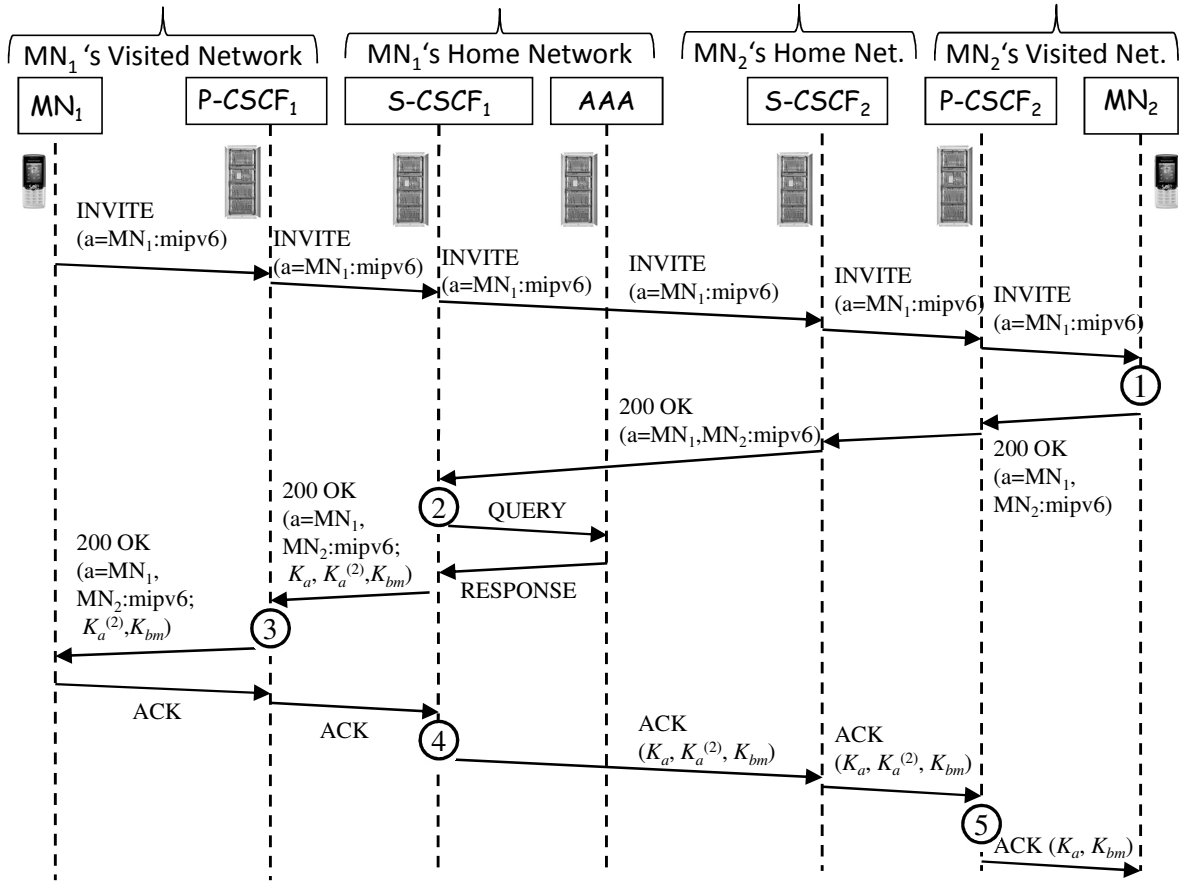

Fig. 10. Distribution of the keys K_a and $K_a^{(2)}$, together with the BU authentication key K_{bm}

2461, Available: http://www.ietf.org/rfc/rfc2104.txt.

[7] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney (2003, July): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", IETF RFC 3315, Available: http://www.ietf.org/rfc/rfc3315.txt.

[8] S. Kent, R. Atkinson (1998, November): "Security Architecture for the Internet Protocol", IETF RFC 2401, Available: http://www.ietf.org/rfc/rfc2401.txt.

[9] J. Arkko, V. Devarapalli, V. and F. Dupont (2004, June): "Using IPsec to Protect Mobile IPv6 Signaling between Mobile Node and Home Agents", IETF RFC 3776, Available: http://www.ietf.org/rfc/rfc3776.txt.

[10] H. Krawczyk, M. Bellare, R. Canetti (1997, February): "HMAC: Keyed-Hashing for Message Authentication", IETF RFC 2104, Available: http://www.ietf.org/rfc/rfc2104.txt.

[11] D. Eastlake, P. Jones (2001, September): "US Secure Hash Algorithm 1 (SHA1)", IETF RFC 3174, Available: http://www.ietf.org/rfc/rfc3174.txt.

[12] S. M. Faccin, P. Lalwaney, B. Patil: *IP Multimedia Services: Analysis of Mobile IP and SIP Interactions in 3G Networks*, IEEE Communication Magazine, Vol. 42, No. 1, pp. 113-120, January 2004.

[13] D. Celentano, A. Fresa, M. Longo, F. Postiglione, A. L. Robustelli: *MIPv6 Binding Authentication for B3G Networks*, Wireless Systems and Network Architectures, (Eds.) M. Cesana, L. Fratta, Lectures Notes in Computer Science, Springer-Verlag, Vol. 3883, pp. 170-183, May 2006.

[14] D. Celentano, A. Fresa, M. Longo, F. Postiglione, A. L. Robustelli: *Secure Mobile IPv6 for B3G Networks*, in Proc. of SoftCOM'06, Split – Dubrovnik (Croatia), September 29 - October 1, 2006.

[15] M. Handley, V. Jacobson (1998, April): "SDP: Session description protocol", IETF RFC 2327, Available: http://www.ietf.org/rfc/rfc2327.txt.

[16] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko (2003, September): "Diameter Base Protocol", IETF RFC 3588, Available: http://www.ietf.org/rfc/rfc3588.txt.

Domenico Celentano received the Laurea degree in electronic engineering (Laurea in Ingegneria elettronica) from the University of Salerno in 2004. He then joined Co.Ri.TeL.(Consortium of telecommunication research) whose main interests have covered the fields of a telecommunication architectures of third generation and beyond networks. In particular mobility and secure access issues; management of security inside IMS (IP Multimedia Subsystem); research in AAA (Authentication Authorization Accounting) architecture, including authentication in multi-access environment through the EAP (Extensible Authentication Protocol) protocol.

At present, he takes care of the security aspects in the Project "Functional Subsystem of intelligent networks for heterogeneous multi-services in IMS environment (SINSIMS)" supported by the Italian Ministry for Industry (Ministero delle Attività Produttive).

Antonio Fresa received a Master's degree in Electronic engineering, with honours, from the University of Naples (Italy) in 1987 after a thesis about Interception of Spread Spectrum Signals.

He had a long experience in software technologies and telecommunication networks working in various projects and organizations. Currently he is Manager for Innovation activities and for Core Networks products in Ericsson.

He has participated, jointly with Co.Ri.TeL., in research projects dealing with B3G architectures and security in next generation networks.

Antonio is author of many papers for conferences and magazines and has been reviewer in many international conferences. He has been lecturer of Telecommunication Networks at University of Salerno.

Maurizio Longo ("laurea" in Electronics Engineering, University of Napoli, 1972; MSEE, Stanford University, 1978), is Full Professor of Telecommunications, Chairman of the Graduate School of Information Engineering at the University of Salerno (Italy), and Director of the CoRiTel Lab. based at the University of Salerno (CoRiTel is a consortium having Marconi and ITS as industrial partners). Previously he held academic positions at the Universities of Napoli and Lecce, the Istituto Universitario Navale (Napoli) and the Accademia Aeronautica (Pozzuoli).

During 1986-87 and then in 1990 he was on leave at the Information Systems Lab., Stanford University (CA), as a Formez Fellow and then as a NATO-CNR Senior Fellow.

In 1988 he was awarded the Lord Brabazon Premium by IERE—IEE, London (UK). He is the author or co-author of over 120 papers in the fields of telecommunications and signal processing. His main current interests are in design and performance evaluation of telecommunication networks, with emphasis on wireless networks.

Fabio Postiglione received the Laurea degree (*summa cum laude*) in electronic engineering and the Ph.D. degree in information engineering from University of Salerno, Fisciano, Italy, in January 1999 and May 2005, respectively.

He is currently working with the University of Salerno. His main research interests include performance evaluation of telecommunications systems, network topology and gravitational waves data analysis (LIGO Project). He has also been involved in many research projects on next generation wireless networks in collaboration with many Academy and Industry partners. Previously he held research positions at the Tin.it R&D Dept. (Telecom Italia Group) and the University of Sannio.

Dr. Postiglione is a Member of the Italian National Inter-University Consortium for Telecommunications (CNIT), the LIGO Scientific Collaboration (LSC) and the Italian National Institute of Nuclear Physics (INFN). He has coauthored about 40 papers mainly on peer-reviewed international journals and conference proceedings.

Anton Luca Robustelli received a laurea degree in Electronic engineering with honours from the University of Salerno (Italy) in March 1999 after a thesis about Automatic video segmentation in the MPEG compressed domain. After a scholarship in software technologies for TLC systems, he joined Ericsson in 1999. He has then participated in several projects in the ISDN, Network Management, Lawful Interception and switching systems technical areas, at the same time strictly collaborating with the Research and Technology department.

Since 2002 he is involved with Co.Ri.TeL. (a research consortium including Ericsson R&D in Italy and several Italian universities) and currently coordinates a research group dealing with Beyond-3G architectures and applications, with particular focus on multi-access, 3G IP Multimedia Subsystem and security solutions. He has been lecturer at the University of Salerno.