AAA Context Transfer for Seamless and Secure Multimedia Services over All-IP Infrastructures

M. Georgiades, N. Akhtar, C. Politis, R. Tafazolli
University of Surrey
Centre for Communication Systems Research
Guildford, GU2 7XH, Surrey, UK
{m.georgiades, n.akhtar}@eim.surrey.ac.uk

***Abstract*: The all-IP based architecture for 3G networks and beyond will rely on a number of different access technologies, working seamlessly to support numerous services and applications. Security provisioning is an essential requirement in any such all-embracing network but this introduces an additional delay component to the total handoff delay crucially affecting the prime objective towards seamless mobility. In this paper we present a context transfer solution for seamless and secure multimedia services over all-IP infrastructures. The solution will act as an adhesive between the AAA and mobility management message exchanges by using the latter to forward AAA state information locally. For such a solution existing messages cellular IP were used as triggers and additional messages were introduced to carry the desired AAA context information. The results have shown that the overall handoff delay is reduced by approximately a factor of twenty. Additional results demonstrate the effect of AAA Context Transfer on multimedia services when integrated with the interworking mobility solution of SIP/Cellular IP [1].**

1 Introduction

Offering seamless multimedia services to mobile users across heterogeneous wireless environments is the main objective of next generation all-IP based network infrastructures. It is important to note that this work acts as a complement to the work presented in [1][2][3][4][5][6] and [7], and that it is an important component on the IST EVOLUTE project [8]. Two of the features in the EVOLUTE architecture are: (1) the development of a multilayer mobility management scheme which utilizes salient features and capabilities of existing and emerging protocols (e.g. Mobile IP, SIP, IP-based micro-mobility), in order to support multimedia services (either real-time or non-real-time) efficiently and (2) the provisioning of fast and secure access to mobile multimedia services using a scalable and robust AAA architecture. Authentication, Authorization, and Accounting (AAA) is a framework used in the EVOLUTE architecture for controlling the access of the mobile host to the network resources. From a handoff performance perspective, one of the key issues in the development of the multilayer mobility management scheme [8] is minimizing the handoff delay while a mobile host is roaming across the homogeneous/heterogeneous networks. On the contrary the introduction of AAA security provisioning adds an undesired delay component. The time consumed by AAA transaction may affect the handoff latency and consequently affect the ongoing sessions. During the handoff, the interactions between mobile host and AAA servers need to be avoided. The main objective of this work is to minimize and if possible eliminate the additional delay introduced due to AAA security provisioning. Context transfer could facilitate this by forwarding the AAA pre-established information to the new Access Router (nAR). In this paper, we propose a AAA context transfer solution for transferring AAA state information to the nAR. The motivation for this stems from the benefits of avoiding re-establishment of AAA and providing an interoperable solution that works for any Layer 2 radio access technology. This solution contributes to the seamless operation of application streams, minimize packet loss, reduce delay, save on bandwidth over radio link and reduce errors.

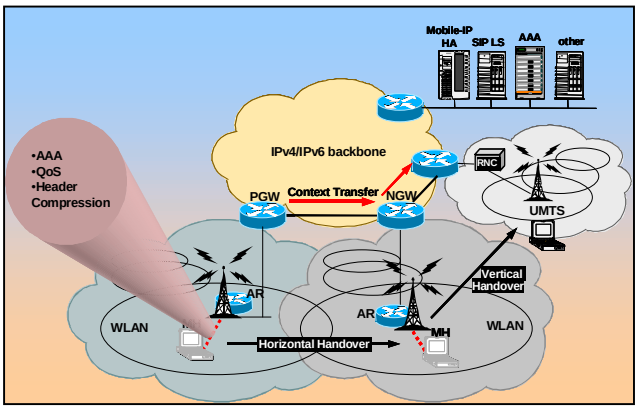


Figure 1 Context Transfer in all-IP infrastructures

What follows is an overview of the relevant components of the EVOLUTE Architecture, a description of the proposed AAA Context Transfer solution, followed by a performance analysis and discussion.

2 EVOLUTE Architecture

2.1 MMM- Multilayer Mobility Management

The solution proposed in this paper is centred on the domain-based approach to mobility management as envisaged in the IST EVOLUTE project [8]. The idea is to have a multilayer and hierarchical mobility management architecture for supporting and managing mobility between networks of the same/different access technologies. In the EVOLUTE architecture, a distinction is made between inter- and intra-domain mobility. Mobile IP [9] and SIP [10] serve as inter-domain mobility management protocols (mobility across administrative domains) what is also referred to

as macromobility. As these are not suitable for a small-scale mobility (micromobility, or mobility within an administrative domain) protocols like Cellular IP [11] and Hierarchical Mobile IP [12] are the preferred choices for intra-domain mobility. Hence EVOLUTE [8] follows a twofold mobility management approach by introducing hierarchies (isolating the wireless access from the core of the Internet), as well as, by using salient features of multiple protocols (multilayer approach addressing mobility awareness in the appropriate layer of the protocol stack). Therefore, the EVOLUTE mobility management architecture addresses mobility support at several layers; application layer based on SIP (when real traffic-time traffic is involved), network layer based on Mobile IP [9] (when non-real-time multimedia traffic is involved), and local area mobility based on an IP micro-mobility solution (e.g., Cellular IP, Hierarchical Mobile IP, etc.) for intra-domain mobility. These three mobility management schemes can work together to provide a reliable operation.

2.2 Cellular IP protocol overview

Cellular IP [11] is a protocol that provides mobility and handoff support for frequently moving hosts. It is designed for local mobility, for instance in a campus or metropolitan area network. Cellular IP will interwork with Mobile IP and SIP in the EVOLUTE architecture to support wide area mobility, that is, mobility between Cellular IP Networks.

In cellular IP the base stations periodically emit beacon signals. These are used by the mobile hosts to locate the nearest base station. Once this is done the mobile host can forward packets to this base station. Any IP packet transmitted by the mobile host towards the corresponding host (CH) will be forwarded on a hop-by-hop shortest path routing towards the Gateway. Each cellular IP node maintains a route cache containing entries on where to forward each IP packet destined for the mobile host. Packets transmitted from the mobile host are used to create and update these entries so that the cellular IP domain knows the current location of the mobile host.

When a base station receives a packet transmitted by the mobile host, it updates the route cache entry, mapping the mobile host's IP address to the neighbour from which the packet arrived to the node. The chain of cached mappings referring to a single mobile host constitutes a reverse path for downlink packets addressed to the same mobile host. As the mobile host handoffs, the chain always points to its current location because its uplink packets update the mappings. IP packets addressed to a mobile host are routed by the chain of cached mappings, which refer to the corresponding mobile host.

Within a cellular-IP domain, during a handover from one BS to another, cellular-IP control packets could be used to initiate and transfer authorised context from the Cellular IP (CIP-GW) to the new base station (NBS). The context information will be stored at the CIP-GW and a copy of this context (state information) will be forwarded to the NBS.

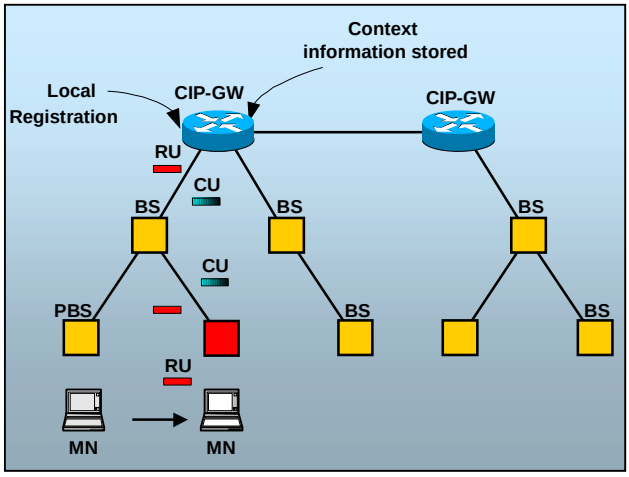


Figure 2 Context transfer enhancement to Cellular IP

One of the main advantages of using cellular-IP is the distinction it makes between idle and active users. This separation allows the network to follow a mobile node in active state from BS to BS and deliver packets without searching for the mobile host. By separating the caches for active and idle mobile hosts only a smaller cache needs to be searched for most of the packets, which results in faster lookups and better scalability. This CIP advantage of separating active hosts from idle mobile hosts is also a benefit to the context transfer mechanism since it also targets active mobile hosts.

2.3 EAP-TLS Authentication protocol overview

In the EVOLUTE architecture a scalable and robust AAA architecture is used to provide secure access to mobile multimedia services. For this the EAP-TLS [13] authentication protocol is used. Central to the EAP-TLS protocol are two main elements:

- EAP allows wireless client adapters to communicate with different back-end servers, in the EVOLUTE case, RADIUS (Remote Access Dial-In User Service).
- IEEE 802.1x, a standard for port-based network access control. EAP-TLS was the chosen protocol as it is 802.1x/EAP compliant, it supports mutual authentication and dynamic Wired Equivalent Privacy (WEP) support, which are essential for WLAN networks.

EAP provides a mechanism for supporting various authentication methods over wired and wireless networks. An access point that supports EAP authentication, authorization, and accounting (AAA) client is not required to have an understanding of the specific EAP type used in the EAP authentication process. The AAA client is aware only of when the EAP authentication process starts and ends.

In brief the following steps take place in the EAP-TLS protocol:

- The certificate-authority-server infrastructure issues certificates to the AAA server(s) and the clients
- A mobile client requires a valid certificate to authenticate to the network.
- The AAA server requires a "server" certificate to validate its identity to the clients.

The components involved in the 802.1x/EAP authentication process are:

- Supplicant (Mobile User)
- Authenticator (Access Point)
- Authentication Server (RADIUS Server)

The authenticator must support 802.1x/EAP authentication and the supplicant and authentication server must support EAP/TLS authentication.

3 AAA Context transfer solution

As mentioned earlier, in this paper, we propose a context transfer solution for transferring AAA state information stored at the micromobility domain gateway to the mobile host's new base station once handoff takes place. The new base station maybe within the same domain or a new domain, depending on whether the handoff was inter-domain or intra-domain. Figure 3 shows a signaling flow diagram of the EAP-TLS message exchanges between the mobile host, the new base station and the RADIUS server before introducing the context transfer solution in the EVOLUTE architecture. The CIP Route Update (CIP-RU) packet indicates the onset of handoff, which is then followed by the EAP-TLS exchange. As can be seen, multiple message exchanges are required between these entities before the network authenticates the mobile host. This delay could be very large especially if the RADIUS server resides far away from the new base station. Hence, it would be desirable to avoid this message exchange and find a faster to re-authenticate the mobile host.

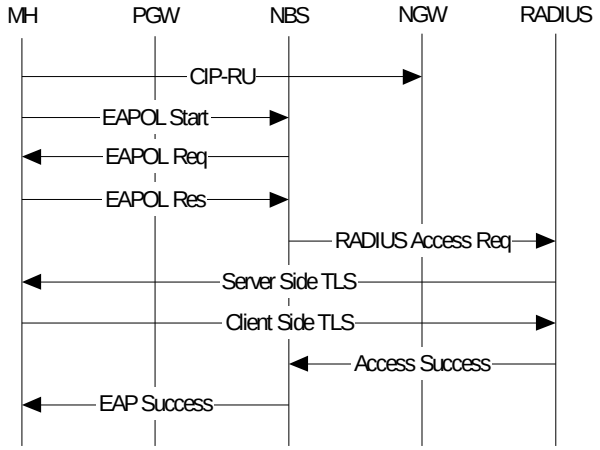


Figure 3 Signaling flow for AAA security in the EVOLUTE architecture

Figure 4 shows the resulting message flow when the AAA context transfer solution is used. It clearly demonstrates how the number of messages exchanged is reduced, thus avoiding communication with the RADIUS server but at the same time the client is authenticated by the network on the basis of the received context information. In this case, once the MH signals the handoff, the new base station requests for AAA context from the previous gateway. Upon receiving the desired context, the new BS is able to authenticate the mobile host straightaway on the basis of the context information.

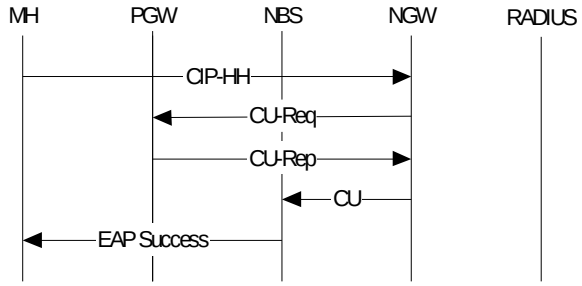


Figure 4 Signaling flow for AAA in the EVOLUTE architecture with context transfer

In order to incorporate this context transfer mechanism in the cellular-IP protocol the following enhancements are required:

- Introduction of a Context-Update (CU) packet
- Introduction of Context cache at each cellular-IP leaf node.
- Re-configure the cellular-IP Route-Update packet to indicate handoff when it occurs and in such a case, to inform the new base station/gateway about the previous gateway.
- Introduction of a Context-Update request (CU-Req) packet
- Introduction of a Context-Update reply (CU-Rep) packet

3.2 Intradomain Context Transfer

The performance of the proposed context transfer scheme was evaluated in the Wireless Networking Testbed (WNT) at the University of Surrey. Figure 5 below shows the hardware configuration for the intra-domain setup in the testbed. The Cellular IP Gateway is running on a Linux PC. We use the open source Cellular IP implementation from the University of Columbia [17]. There are two Cellular IP nodes running on Linux laptops in the setup. They have two network interfaces, one wired and one wireless. The wired interface is used to connect to the gateway while the wireless interface serves as the Access Point. The AP consists of a Linksys WPC11 wireless card with the open source hostAP driver (hostap-0.0.3). The mobile host is a Linux laptop equipped with a wireless network interface card..

In this scenario, when an active node connects to a new BS, it transmits a route-update packet to CIP-GW

(Figure 5). The route-update packet will update Route Caches in nodes along the way from the NBS to the CIP-GW. We introduce a new flag, called the 'H' (handoff) flag, in the route-update

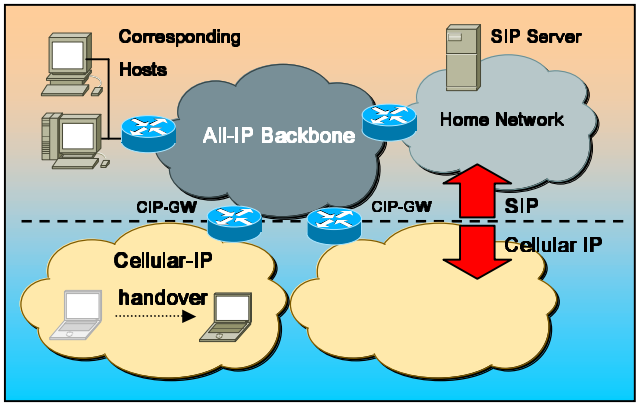


Figure 5 Intra-domain setup

Packet to indicate handoff. This helps the new BS/GW to differentiate between normal updates that refresh the existing caches and the route update that creates new entries in the caches after handoff. When the route-update packet reaches the CIP-GW, if the H flag is enabled, the CIP-GW will send a context-update packet towards the mobile node. The context-update packet, carrying the feature contexts (AAA information in our case), will be routed along the reverse path on a hop-by-hop basis towards the mobile node. When the context-update arrives at the NBS, the NBS stores the context data in its context cache and it discards the packet. Using the AAA context received, the NBS then authenticates the mobile host and informs it by sending an EAP Success message. It must be noted here that the last step is carried out by the authenticating entity in the NBS and not the Cellular IP. Hence, in the proposed scheme Cellular IP acts as a facilitator of fast re-authentication after handoff.

3.3 Interdomain Context Transfer

The setup for the interdomain context transfer scheme evaluation is shown in Figure 6. In this case we have two mobility gateways, running on Linux PCs. Further, each gateway is connected to a Cellular IP node on the downlink. Furthermore, the gateways are connected to the IP backbone. The leaf nodes are the same as the ones used for the intradomain case.

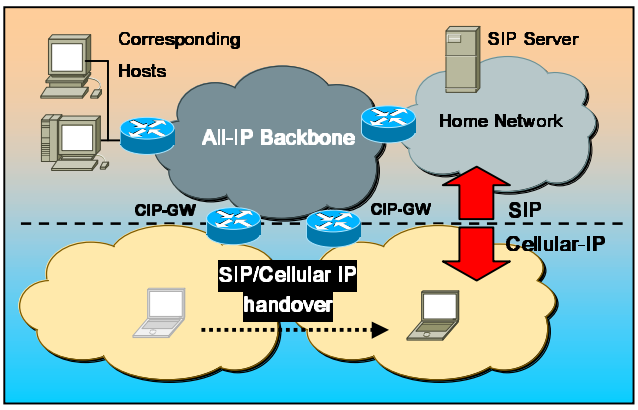
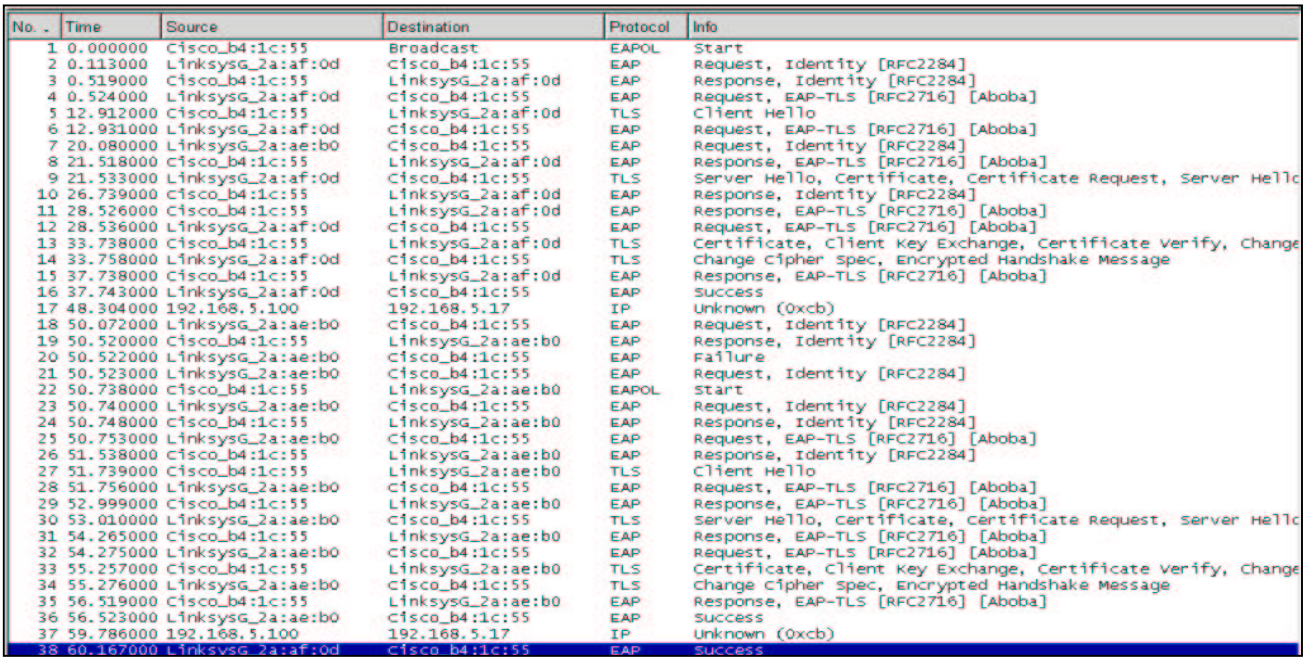


Figure 6 Inter-domain Setup

The signaling exchange is quite similar to the Intra-domain process (2.1) with additional messages to request and forward the desired context information from the previous CIP-GW to the new CIP-GW (Figure 6). When an active node connects to a new BS, it transmits a route-update packet (with the handoff flag set) to new CIP-GW. When the route-update packet reaches the new CIP-GW, it finds out that the H flag is enabled and identifies the MH as a newcomer to its domain. The new GW extracts the address of the previous GW from the CIP-RU and then, requests context information from the previous CIP-GW by sending a CT-Req packet. On reception of the CT-Req, the previous CIP-GW forwards the context information to the new CIP-GW using the CT-Rep message. The new CIP-GW in turn stores the context in the context cache and creates a CU packet containing the context. The CU packet, carrying the feature contexts, will be routed along the reverse path on a hop-by-hop basis towards the mobile node. When the context-update arrives at the NBS, the NBS stores the context data in its context cache and it discards the packet. As in the intradomain case, the new BS then proceeds to authenticate the mobile host and informs it about this.

4 Performance Evaluation & Discussion

Table 1 shows the EAP/TLS packets captured at the mobile host during the authentication procedure when an interdomain handoff takes place. For this set of observations, the context transfer has been disabled and therefore a full re-authentication is required. The handoff is initiated by the Cellular IP Route Update packet with the 'H' flag set (packet 1 in the figure. The re-authentication process is initiated with an EAPOL Start message sent by the MH to the new access point (AP2) while successful authentication is indicated by the EAPOL Success message. Using the timestamps associated with these two messages, we can find out the time taken for a successful authentication. The time difference between the Cellular IP Route Update packet and the EAP Success packet is used to determine the time taken for the handoff from one BS to another and the subsequent re-authentication.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco_b4:1c:55	Broadcast	EAPOL	Start
2	0.113000	LinksysG_2a:af:0d	Cisco_b4:1c:55	EAP	Request, Identity [RFC2284]
3	0.519000	Cisco_b4:1c:55	LinksysG_2a:af:0d	EAP	Response, Identity [RFC2284]
4	0.524000	LinksysG_2a:af:0d	Cisco_b4:1c:55	EAP	Request, EAP-TLS [RFC2716] [Aboba]
5	12.912000	Cisco_b4:1c:55	LinksysG_2a:af:0d	TLS	Client Hello
6	12.931000	LinksysG_2a:af:0d	Cisco_b4:1c:55	EAP	Request, EAP-TLS [RFC2716] [Aboba]
7	20.080000	LinksysG_2a:ae:b0	Cisco_b4:1c:55	EAP	Request, Identity [RFC2284]
8	21.518000	Cisco_b4:1c:55	LinksysG_2a:af:0d	EAP	Response, EAP-TLS [RFC2716] [Aboba]
9	21.533000	LinksysG_2a:af:0d	Cisco_b4:1c:55	TLS	Server Hello, Certificate, Certificate Request, Server Hello
10	26.739000	Cisco_b4:1c:55	LinksysG_2a:af:0d	EAP	Response, Identity [RFC2284]
11	28.526000	Cisco_b4:1c:55	LinksysG_2a:af:0d	EAP	Response, EAP-TLS [RFC2716] [Aboba]
12	28.536000	LinksysG_2a:af:0d	Cisco_b4:1c:55	EAP	Request, EAP-TLS [RFC2716] [Aboba]
13	33.738000	Cisco_b4:1c:55	LinksysG_2a:af:0d	TLS	Certificate, Client Key Exchange, Certificate Verify, Change
14	33.758000	LinksysG_2a:af:0d	Cisco_b4:1c:55	TLS	Change Cipher Spec, Encrypted Handshake Message
15	37.738000	Cisco_b4:1c:55	LinksysG_2a:af:0d	EAP	Response, EAP-TLS [RFC2716] [Aboba]
16	37.743000	LinksysG_2a:af:0d	Cisco_b4:1c:55	EAP	Success
17	48.304000	192.168.5.100	192.168.5.17	IP	Unknown (0xcb)
18	50.072000	LinksysG_2a:ae:b0	Cisco_b4:1c:55	EAP	Request, Identity [RFC2284]
19	50.520000	Cisco_b4:1c:55	LinksysG_2a:ae:b0	EAP	Response, Identity [RFC2284]
20	50.522000	LinksysG_2a:ae:b0	Cisco_b4:1c:55	EAP	Failure
21	50.523000	LinksysG_2a:ae:b0	Cisco_b4:1c:55	EAP	Request, Identity [RFC2284]
22	50.738000	Cisco_b4:1c:55	LinksysG_2a:ae:b0	EAPOL	Start
23	50.740000	LinksysG_2a:ae:b0	Cisco_b4:1c:55	EAP	Request, Identity [RFC2284]
24	50.748000	Cisco_b4:1c:55	LinksysG_2a:ae:b0	EAP	Response, Identity [RFC2284]
25	50.753000	LinksysG_2a:ae:b0	Cisco_b4:1c:55	EAP	Request, EAP-TLS [RFC2716] [Aboba]
26	51.538000	Cisco_b4:1c:55	LinksysG_2a:ae:b0	EAP	Response, Identity [RFC2284]
27	51.739000	Cisco_b4:1c:55	LinksysG_2a:ae:b0	TLS	Client Hello
28	51.756000	LinksysG_2a:ae:b0	Cisco_b4:1c:55	EAP	Request, EAP-TLS [RFC2716] [Aboba]
29	52.999000	Cisco_b4:1c:55	LinksysG_2a:ae:b0	EAP	Response, EAP-TLS [RFC2716] [Aboba]
30	53.010000	LinksysG_2a:ae:b0	Cisco_b4:1c:55	TLS	Server Hello, Certificate, Certificate Request, Server Hello
31	54.265000	Cisco_b4:1c:55	LinksysG_2a:ae:b0	EAP	Response, EAP-TLS [RFC2716] [Aboba]
32	54.275000	LinksysG_2a:ae:b0	Cisco_b4:1c:55	EAP	Request, EAP-TLS [RFC2716] [Aboba]
33	55.257000	Cisco_b4:1c:55	LinksysG_2a:ae:b0	TLS	Certificate, Client Key Exchange, Certificate Verify, Change
34	55.276000	LinksysG_2a:ae:b0	Cisco_b4:1c:55	TLS	Change Cipher Spec, Encrypted Handshake Message
35	56.519000	Cisco_b4:1c:55	LinksysG_2a:ae:b0	EAP	Response, EAP-TLS [RFC2716] [Aboba]
36	56.523000	LinksysG_2a:ae:b0	Cisco_b4:1c:55	EAP	Success
37	59.786000	192.168.5.100	192.168.5.17	IP	Unknown (0xcb)
38	60.167000	LinksysG_2a:af:0d	Cisco_b4:1c:55	EAP	Success

Figure 7 Cellular IP and EAP/TLS packet capture using Ethereal

Table 1 EAP/TLS signaling exchange (AAA Context Transfer Disabled)

Msg	Time	Source	Destination	Protocol	Info
1	48.304	MH	CIP-GW	CIP	Route Update
2	50.738	MH	AP2	EAPOL	Start
3	50.74	AP2	MH	EAP	Request
4	50.748	MH	AP2	EAP	Response
5	50.753	AP2	MH	EAP	Request
6	51.538	MH	AP2	EAP	Response
7	51.739	MH	RADIUS	TLS	Client Hello
8	51.756	AP2	MH	EAP	Request
9	52.999	MH	AP2	EAP	Response
10	53.01	RADIUS	MH	TLS	Server Hello
11	54.265	MH	AP2	EAP	Response
12	54.275	AP2	MH	EAP	Request
13	55.257	MH	RADIUS	TLS	Handshake
14	55.276	RADIUS	MH	TLS	Handshake
15	56.519	MH	AP2	EAP	Response
16	56.523	AP2	MH	EAP	Success

Handoff delay = 56.523-48.304 = 8.219 sec

All together the handoff delay is about 8 seconds and this demonstrates that the EAP/TLS exchange is a significant delay component in this scenario. In contrast Table 2 shows the handoff delay resulting when the Context Transfer mechanism is enabled. For this scenario the mobile host moves from AP2 back to AP1. As can be seen from the table, the handoff delay has been significantly reduced to only approximately 0.4 seconds. In this case, again the Route Update (with handoff flag set) indicates the handoff and then the context transfer takes place on between the new and previous gateways, followed by the 'reduced' re-authentication procedure based on the received context. Finally, the new BS (AP1) informs the mobile host that it has been successfully authenticated by sending the EAP Success message as indicated in Table 2. It is important to note that the improvement is almost 10 times. We have repeated this test a number of times and it has been observed that though the actual times vary the context transfer enabled handoff is much faster than the one without context transfer scheme.

Table 2 EAP/TLS Signaling exchange (AAA Context Transfer Enabled)

Msg	Time	Source	Destination	Protocol	Info
1	59.786	MH	CIP-GW	CIP	Route Update
2	60.167	AP1	MH	EAP	Success

Handoff delay = 60.167-59.786 = 0.381 sec

3.3 Effect on Real-Time Services

We have tested the above two scenarios, Cellular-IP with Context Transfer (1) enabled and (2) disabled, for the case where SIP/Cellular IP scheme is deployed for mobility management as a possible solution for handling mobility for real time services in all IP networks [8]. For this test, the network is configured as shown in Figure 4 with the addition of SIP clients on the mobile host and the corresponding host. We used a modified version of Linphone [18] as the SIP-based test application for evaluating the impact of the proposed context transfer solution on real time multi media services. A multimedia session is set up between the MH and the CH using the application. While the session is underway, the mobile host handoffs to a new base station and the session is disrupted. To re-establish the session, the application on the MH sends a new session set up request (a SIP re-INVITE message) to the CH. The resulting SIP signaling exchanges between the mobile host (MH) and corresponding host (CH) are

shown in Table 3 and Table 4 respectively. We also give the handoff delay, which in this case represents the time taken to re-establish the session after handoff.

Table 3 SIP Signaling exchange (AAA Context Transfer Disabled)

Msg	Time	Source	Destination	Protocol	Info
1	34.177	MH	CH	SIP/SDP	INVITE
2	34.178	MH	SIP LS	SIP	REGISTER
3	34.178	MH	SIP LS	SIP	REGISTER
4	36.177	MH	CH	SIP/SDP	INVITE
5	36.178	MH	SIP LS	SIP	REGISTER
6	36.178	MH	SIP LS	SIP	REGISTER
7	38.977	MH	CH	SIP/SDP	INVITE
8	38.978	MH	SIP LS	SIP	REGISTER
9	38.978	MH	SIP LS	SIP	REGISTER
10	38.984	CH	MH	SIP	100 Trying
11	38.999	CH	MH	SIP	200 OK
12	39.001	CH	MH	SIP	200 OK
13	41.516	CH	MH	SIP	180 Ringing
14	42.407	CH	MH	SIP/SDP	200 OK
15	42.412	MH	CH	SIP	ACK

Handoff delay = 42.412-34.177 = 8.235 sec

The results in Table 3 depict that the SIP client (MH) attempts to send a re-INVITE message towards the corresponding host (CH) and a REGISTER message towards the SIP location server (SIP LS) several times before reaching them successfully. This was due to the fact that the MH was not authenticated during the initial two attempts and so the packets could not go through to the CH via the new BS. We observe from the table that it takes more than 8 seconds to re-establish the session. Hence, the multimedia session remains disrupted for this period of time.

Table 4 SIP Signaling exchange (AAA Context Transfer Enabled)

Msg	Time	Source	Destination	Protocol	Info
1	65.240	MH	CH	SIP/SDP	INVITE
2	65.241	MH	SIP LS	SIP	REGISTER
3	65.242	MH	SIP LS	SIP	REGISTER
4	65.589	CH	MH	SIP	100 Trying
5	65.593	CH	MH	SIP	200 OK
6	65.594	CH	MH	SIP	200 OK
7	67.614	CH	MH	SIP	180 Ringing
8	68.403	CH	MH	SIP/SDP	200 OK
9	68.404	MH	CH	SIP	ACK

Handoff delay = 68.404-65.240 = 3.164 sec

In contrast Table 4 shows the SIP signalling exchange when AAA context transfer is enabled. For this case the MH is authenticated significantly faster allowing the first re-INVITE and REGISTER messages to reach the CH and SIP Location Server respectively. This minimises the delay in re-establishing the session to about 3 seconds, which is mainly caused by the SIP signaling exchange and not by the authentication signaling exchange as in Table 3.

For both scenarios the interdomain handoff was repeated several time and the results are shown in Figure 8.

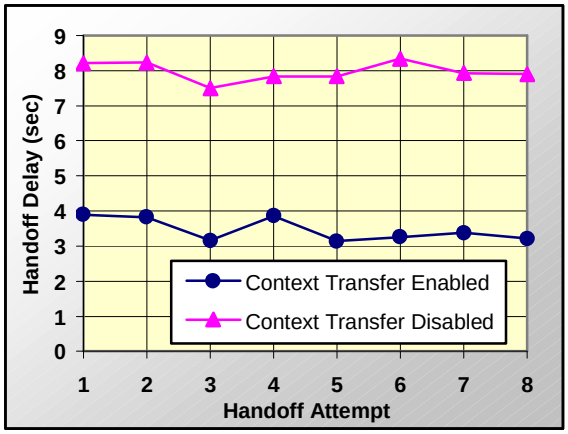


Figure 8 SIP signaling exchange: CT Enabled v CT Disabled

These results clearly indicate the improvement caused by the addition of a Context Transfer mechanism to Cellular IP. It is clear from the graph that the handoff delay when context transfer option was disabled was 8 seconds on the average. On the contrary when the context transfer option was enabled the handoff delay was significantly reduced to about 3.5 seconds on average. Figure 9 shows a breakdown of the handoff delay into the major components. The total handoff delay is mainly due to the Cellular IP (CIP), EAP/TLS and SIP message exchanges. Notice how when context transfer is disabled the full authentication procedure takes place introducing an undesired delay of about 5 seconds. The delay component caused by EAP/TLS is minimised to a couple of milliseconds when context transfer is introduced, reducing the overall delay from 8 to about 3.5 seconds (see Figure 9).

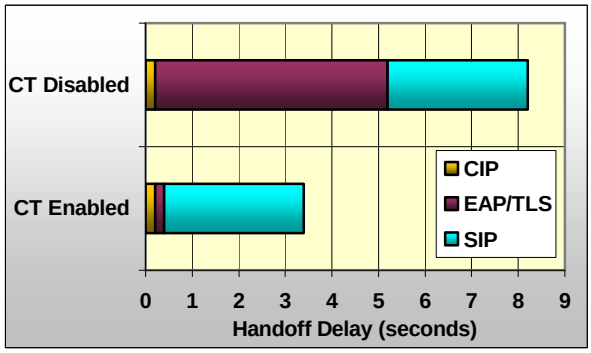


Figure 9 Handoff delay reduction with Context Transfer

The results presented here demonstrate the tremendous effect of deploying context transfer mechanism and how it aids in realizing a seamless and secure handoff.

5 Summary and Conclusions

In this paper we have proposed a context transfer solution to complement the multilayer mobility management with the objective of avoiding the additional delay introduced by the AAA operation. For this solution existing messages of cellular IP were used as triggers and additional messages where introduced to carry the AAA context information to the appropriate base station. Based on the results shown here, the proposed AAA context transfer solution reduces the overall handoff delay by a factor of twenty. This is because the full EAP/TLS procedure is avoided by transferring the AAA context to the new BS, thus enabling it to re-authenticate the mobile host without contacting the AAA server. Furthermore additional results presented here demonstrate the effect of AAA Context Transfer on SIP [10] multimedia services when the scheme was integrated in the interworking mobility solution of SIP/Cellular IP [1]. Due to the fast re-authentication process, the handoff performance of the multimedia application was greatly enhanced and the SIP session was re-established with much reduced delay. This work demonstrates how the context transfer mechanism improves the overall handoff performance and hence aids in realizing seamless and secure mobility management in all IP infrastructures.

Acknowledgements

This work has been performed in the framework of the IST-2001-32449 project EVOLUTE, which is partly funded by the European Union. The authors would like to acknowledge the contribution of their colleagues from Intracom, FhG Fokus, Alcatel-SEL, Motorola UK, University of Surrey, Cerfriel, and Telia.

References

[1] N. Akhtar, M. Georgiades, C. Politis, R. Tafazolli, "SIP-based End System Mobility Solution for All-IP Infrastructures", IST Mobile & Wireless Communications Summit 2003, 15-18th June 2003, Aveiro, Portugal.

[2] M. Georgiades, K. Chew, C. Politis, R. Tafazolli, "Context Transfer Extension to Mobility Protocols for All-IP Based Infrastructures", Wireless World Research Forum (WWRF), 9th meeting, Zürich, Switzerland, 1-2 July 2003.

[3] M. Georgiades, C. Politis, N.Akhtar, R. Tafazolli, "Context Transfer Extension to Cellular-IP" draft-georgiades-seamoby-ctecip-01.txt, expires December 2003.

[4] M. Georgiades, N. Akhtar, C. Politis, R. Tafazolli, "Hybrid SIP/Mobile IP End System Mobility Solution for All-IP Infrastructures", submitted to the 3rd IFIP-TC6 Networking Conference, Athens, Greece, May 9-14, 2004.

[5] N. Akhtar, M. Georgiades, C. Politis, R. Tafazolli, "Real-time Evaluation of Mobility Management Schemes for IP-based WLAN Infrastructures", International Evolute Workshop, 10th November, 2003, Surrey, UK.

[6] Kar Ann Chew, Christos Politis, Rahim Tafazolli, "Performance Evaluation of Micro-mobility Protocols for All-IP based Infrastructures", Wireless World Research Forum, 7th Meeting, December 2002.

[7] T.Dagiuklas, D.Theofilatos, D.Gatzounas, "Supporting Multimedia Services for Mobile Users in All-IP Based Networks: Requirements, Functions and Issues", Wireless World Research Forum (WWRF), 6th Meeting, June 2002.

[8] IST EVOLUTE project, http://evolute.intranet.gr/

[9] C.Perkins, Ed., “IP Mobility Support for Ipv4” RFC 344, August 2002.

[10] J.Rosenberg, H.Schulzrinne, G.Camarillo, A.Jonston, J.Peterson, R.Sparks, M.Handley, E.Schooler, “SIP: Sesion Initiation Protocol,” RFC 3261.

[11] A. Campbell et al., "Cellular IP", Internet Draft, Internet Engineering Task Force, October 1999.

[12] C.Castelluccia, “Hierarchical MIPv6 mobility management (HMIPv6), Internet Draft, Internet Engineering Force, draft-ietf-mobileip-hmipv6-06.txt.

[13] B. Aboba, D. Simon, PPP EAP TLS Authentication Protocols, RFC 2716, IETF, October 1999.

[14] IETF Seamoby Working Group, http://www.ietf.org/mail-archive/working-groups/seamoby/current/

[15] J.Kempf, “Problem Description: Reasons For Performing Context Transfers Between Nodes in an IP Access Network”, RFC 3374, Internet Engineering Task Force.

[16] http://www.gnu.org/software/osip

[17] http://www.comet.columbia.edu/cellularip/linux_src_code.htm

[18] http://www.linphone.org