WIRELESS COMMUNICATIONS AND MOBILE COMPUTING
Wirel. Commun. Mob. Comput. (2010)
Published online in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/wcm.1019

SPECIAL ISSUE PAPER

Privacy preserving context transfer schemes for 4G networks

Iosif Terzis[1], Georgios Kambourakis[1]*, Giorgos Karopoulos[1] and Costas Lambrinoudakis[2]

[1] Laboratory of Information and Communication Systems Security, Department of Information and Communication Systems Engineering, University of the Aegean, Karlovassi, Samos GR-83200, Greece
[2] Department of Digital Systems, University of Piraeus, GR-18534, Greece

ABSTRACT

In the near future, wireless heterogeneous networks are expected to interconnect in an all-IP architecture. An open issue towards this direction is the uninterrupted continuation of the received services during handover between networks employing different access technologies. In this context, Mobile IP (MIP) is a protocol that allows fast and secure handovers. However, MIP per se cannot handle all the issues that surface during handovers in certain services, and more specifically, when the information of the current state of a service requires re-establishment on the new subnet without having to repeat the entire protocol exchange with the mobile host from the outset. A number of methods have been proposed to solve the aforementioned problem, commonly referred to as secure context transfer. However, while such methods do succeed in minimising the disruption caused by security-related delays, it seems that little has been done to protect the end-users' privacy as well. In this paper, a number of privacy enhanced (PE) context transfer schemes are presented. The first two of them have been introduced in a previous work of ours while the other two are novel. All schemes are analysed in terms of message exchange and evaluated through simulations. The performance of our schemes is compared with the standard ones proposed by the Seamoby work group (WG). The results demonstrate that the proposed schemes are very efficient in terms of application handover times, while at the same time guarantee the privacy of the end-user. Copyright © 2010 John Wiley & Sons, Ltd.

KEYWORDS
privacy; CXTP; secure context transfer; 4G; NGN; secure handover

***Correspondence**
Georgios Kambourakis, Laboratory of Information and Communication Systems Security, Department of Information and Communication Systems Engineering, University of the Aegean, Karlovassi, Samos GR-83200, Greece.
E-mail: gkamb@aegean.gr

1. INTRODUCTION

The advances in wireless communication technologies towards 4G networks and the wide use of mobile devices have enabled users to communicate with each other and receive a wide range of mobile wireless services through various types of access networks and systems everywhere, anytime. However, a major step forward towards 4G systems is the smooth integration of all these heterogeneous wireless access technologies. An open issue that concerns this evolution is the uninterrupted continuation of the received services during a user handover. A handover may occur between networks with different access technologies (vertical handover) or between different wireless access points (AP) that use the same technology (horizontal handover) [1]. Also, a handover occurrence may only involve the same administrative domain or happen between different administrative domains. Thus, making handover seamless and secure for the end-users is one of the key issues in mobility management for next generation all-IP networks.

The Mobile IP (MIP) protocol [2,3] provides certain solutions for mobile users because it allows fast and secure handovers. However, MIP cannot handle all the issues that result during handovers in certain services, and more specifically, when the information of current state of a service requires re-establishment on the new subnet without having to perform the entire protocol exchange with the mobile node (MN) from the scratch. Examples of such services are the authentication authorisation accounting (AAA) framework, QoS Policy, IPsec State and Header Compression to mention just a few. So far, a number of methods have been proposed to solve the aforementioned problem like the optimised integrated registration procedure of mobile IP and session initiation protocol (SIP) [4] with AAA operations (OIRPMSA) [5], media-independent pre-authentication (MPA) [6] and context transfer protocol (CXTP) [7]. However, while these methods do succeed in minimising the disruption caused by security related delays, it seems that little has been done for protecting the end-users' privacy as well [8].

In this paper, we present and analyse four privacy enhanced (PE) context transfer schemes. Two of these schemes were initially proposed and theoretically discussed in Reference [9], while the rest are novel. Here, all four schemes are analysed in terms of message exchange, evaluated through simulations and compared with the ones been proposed by the Seamoby work group (WG) in CXTP RFC 4067 [7]. It has to be mentioned that this work mainly focuses on user's roaming between different administrative domains location privacy. Note that, to the best of our knowledge, no other work on the privacy of CXTP exists so far; therefore, we only compare our schemes with the ones proposed by the Seamoby WG. The network simulator 2 (NS-2) [10] and Crypto++ [11] are used to evaluate all schemes in terms of application handoff service time. To do so, CXTP has been partially implemented on NS-2 and configured properly in order to cooperate with the already implemented MIP protocol extension. Finally, the cryptographic operations have been separately implemented in Crypto ++ to measure cryptographic workload in each scenario as the case may be.

The rest of the paper is organised as follows. The next section summarises relevant work and elaborates on privacy issues stemming from CXTP, highlighting their importance for next generation networks (NGN). Section 3 analyses the proposed privacy preserving context transfer methods, while Section 4 gives the internal mechanics of our schemes in terms of message exchanges. The evaluation of PE schemes together with the standard ones described in Reference [7] takes place in Section 5. Last section offers concluding thoughts and future directions for this work.

2. PREVIOUS WORK AND PROBLEM STATEMENT

Considering previous relevant work on CXTP evaluation performance and security, little has been done until now. Works in Reference [12,13] present theoretical evaluations for QoS support in CXTP. The authors propose a performance model to compare different CXTP scenarios when CXTP runs on top of IPv6 with fast handover mechanisms. An analysis and performance evaluation of CXTP in MIP environment is given in Reference [14]. The authors propose mechanisms that enable context transfer between access routers offering Internet connectivity for MNs. They use a properly designed test bed to test the performance of context transfer for different services and analyse the benefits that can be obtained using such mechanisms. A similar work that evaluates CXTP over IPsec in MIP v6 realms is presented in Reference [15]. The authors describe a CXTP-based solution to transfer context data between two access routers in an IPv6 mobility environment under the protection of IPsec tunnel. The authors in Reference [16] provide a number of test scenarios to demonstrate how middleboxes could intervene with multimedia sessions during mobility. Also, they show how context transfer can provide a solution for improving the performance in the multimedia session re-establishment as well as enhancing middlebox security. Moreover, some issues that stem from context transfer for seamless micromobility are discussed in Reference [17]. The authors identify the problems related to seamless mobility, highlight design issues to be observed when designing seamless mobility solutions and propose an architecture that can be used as a framework for the implementation of such solutions. Very recently, the work in Reference [18] focuses on CXTP security and provides a number of solutions regarding its flaws.

Privacy is a serious concern for both emerging applications and mobile users in future wireless networks. In fact, the protection of user's privacy may become a *sine qua non* for the so-called NGN, since without privacy-preserving mechanisms in place, the end-user can be easily tracked and profiled in the mid- or long term. That is, network or service operators–especially colluding ones–may collect user information and keep them for long time in order to profile their users and eventually sell these profiles to say advertising companies for profit. After that, the user is left defenceless to spamming and/or other related threats that violate his private sphere. Generally, privacy is a complex concept that affects aspects such as location, identification and authentication [19]. While location privacy requires that the location of a mobile user is untraceable to unauthorised parties (including the network), identification privacy mandates user's anonymity except for authorised parties. As we can perceive, these types of privacy are interrelated. If user's identity remains confidential, then location data are worthless. At the same time, both types of privacy strongly depend on the authentication process where user's permanent identity must be exchanged. If the authentication mechanism does not afford an adequate level of privacy to protect identification-related data, the location can be revealed to unauthorised third parties. Therefore, every underlying mechanism should have the ability to prevent other parties from arbitrarily learning one's current position. Location privacy is about controlling access to this information, which is granted by the user who must be the only one responsible to decide if someone is going to have access to his location data or not.

As noted in the introduction, no work except Reference [9] addresses the privacy of the end-user when CXTP is in use. This work has also presented a number of privacy issues related to user location and movement which do arise from the way CXTP operates. According to this study, end-user location and movement when roaming between different administrative domains can be tracked. Taking a closer look in CXTP inner function [7], we conclude that when a horizontal or vertical handoff occurs, the context data are transferred from the previous access router (pAR) to the new one, namely nAR. It is, thus, obvious that the ARs are able to perceive the source network of the user (pAR) as well as his destination (nAR). In case the two ARs belong to the same administrative domain, there are no issues concerning end-user privacy and particularly his location privacy. However, when the two ARs belong to different administrative domains, end-user privacy is not protected at all. That is, every administrative domain is aware of the previous and next administrative domain of the MN. This means that every domain can successfully track a part of the user's movement. Even worse, the user's movement can be entirely tracked, in case that some administrative domains collude. This does not imply that all administrative domains in the path of the user movement are required to collude for such an attack, but every second domain in that path.

3. PRIVACY ENHANCED CONTEXT TRANSFER SCHEMES

In this section, we present four PE context transfer schemes to deal with the above problem. In the following, we refer to our schemes as PE Schemes I to IV. Our goal is to protect the location privacy of users roaming between different administrative domains. As already mentioned, the first two PE context transfer schemes presented here have been theoretically discussed in Reference [9], while the rest are novel.

The PE Scheme I is based on the fact that the MN is solely responsible for the context transfer. The MN detects that it is about to handover to a new AR that belongs to a different administrative domain. The pAR sends the context of the user to the MN and after the handoff, the MN forwards the context to the nAR. There are two major issues concerning the internal workings of this scheme. The first one is the trust relationship that somehow has to pre-exist between the user's home network and the corresponding nAR. The other issue concerns the integrity of the context data message during the time that is being held by the MN. A graphical representation of the first scheme is given in Figure 1.

The PE Scheme II depicted in Figure 2 depends on the user's home network. In this paper, we use the general term home domain agent (HDA) to refer to a network entity, which is placed inside the user's home domain. For a Third Generation Partnership Project (3GPP) realm, this entity could be a home subscriber server (HSS) or another machine or module connected or embedded to a gateway GPRS support node (GGSN) (the latter is linked to the HSS). The HDA is responsible for the context transfer acting as a proxy between the pAR and nAR. As with the first scheme, the MN detects that it is about to handover to a new AR that belongs to a different administrative domain. This time, however, the pAR sends the user's context to the HDA, and after the handover, the HDA forwards the context to the nAR. It is also assumed that a trust relationship exists between the HDA and the MN (user). More details about the aforementioned schemes are provided in Reference [9].

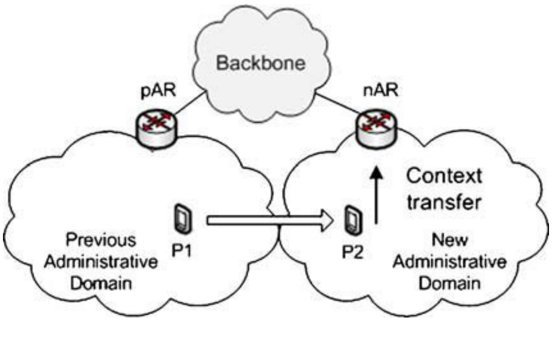


Fig. 1. Network scenario for PE Scheme I.

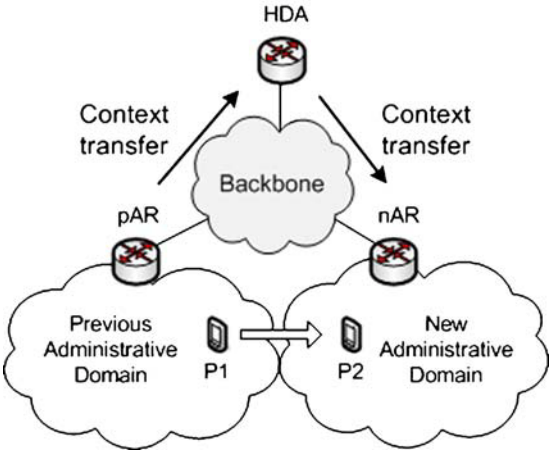


Fig. 2. Network scenario for PE Scheme II.

As already mentioned, the PE Schemes III and IV are novel. In fact, they comprise variations of our second scheme discussed previously. In the near future, it is expected that a variety of different administrative domains will provide similar or dissimilar wireless network services to potential users simultaneously. Moreover, users may have to choose between a range of similar or competitive services provided by a great number of providers at the same time and at the same routing area. Also, the quality of each service offered may depend on the employed network access technology. In such an environment, the key question is when, how and why a given user will decide to handoff from a wireless network to another in order to acquire the desired service. Of course, 4G networks are expected to utilise such a decision mechanism transparently in order for the users to always acquire the best service available [20]. Our last two schemes move towards this direction. They have been designed having in mind that different administrative domains are able to serve the user in a given area by providing similar and competitive services. It is worth noting here that the HDA is responsible for the context transfer in both last two schemes.

The PE Scheme III works as follows: The MN is moving out of range of the pAR and is about to handover to a nAR. In addition, the MN has the opportunity to choose between a number of different nARs that may belong to different network operators. Thus, the MN has not yet decided to which nAR will eventually connect and associate with. In any case, the MN sends a message to the pAR requesting context transfer. Upon reception, the pAR sends the user's context data towards the HDA. Sometime later on, the MN finally decides to handover to one of the candidate nARs. So, it sends a message to the corresponding nAR triggering the context transfer procedure. In response, the nAR requests the context data from the HDA and establishes the services based on the acquired context. This scheme has the following advantages:

- The MN is able to initiate a context transfer and send the appropriate data to the HDA, even before it is able to decide to which nAR will eventually connect and associate with. The MN only needs to know that a handover is about to occur. In this way privacy is guaranteed because context transfer messages do not include any information about the nAR to which the MN will eventually connect and associate with.
- After initiating a context transfer, the context data can remain active in the HDA for a short period of time even if the context transfer delays for some reason. The MN can keep alive the context data by simply sending occasionally a context transfer (*CT*)-*Refresh* message directly to the HDA (see also subsection 4.3).

The last scheme, namely PE Scheme IV, is more dynamic and time efficient but is more complex to implement. The idea behind this scheme is that the HDA and MN already share a symmetric secret key (e.g. a session key derived from a master key after authentication). For instance, considering universal mobile telecommunications system (UMTS) networks the user and his home network share two keys after mutual authentication. The first one, namely ciphering key (CK), is used for confidentiality and the other, namely integrity key (IK), for protecting the integrity of signalling. The symmetric key is used by the MN to encrypt the IP address of every candidate to handoff and associate with nAR. By doing so, the MN sends a message to the pAR for each possible nAR requesting context transfer. Every message contains the IP address of each candidate nAR encrypted with the secret key. Bear in mind that this key is known to the MN and its HDA only. After that, and for every nAR, the pAR forwards the context(s) to the HDA including the encrypted nARs IP addresses. The HDA decrypts the IP addresses of all the nARs using the same symmetric key. Finally, the HDA forwards the context(s) to the corresponding nAR. After receiving the context(s), every candidate nAR is ready and waits for possible handoff to occur. When the MN eventually handoffs to the chosen nAR, the nAR instantly establishes the services based on the context(s) received. This scheme has the following advantages:

- The overall context transfer time from the HDA to a given nAR may differ significantly from one nAR to another. This time actually depends on the quality of the network link between the HDA and the nAR. However, the MN may be aware of which nAR has already received the context data through the HDA. This can be achieved by (optionally) adding one extra message sent by the HDA to the MN after the nAR has sent a *context transfer data reply* (CTDR) message to the HDA (see next section). The calculation of round-trip-time (RTT) between a given nAR and the HDA is also possible through context transfer packets. Therefore, the MN is able to estimate the total time for the overall procedure to complete. When the estimated time for each nAR is available, the final handover decision, i.e. to which nAR the MN will eventually handover, can be taken more efficiently.
- Context data may contain information for transferring one or more (context data) candidate services. The current scheme serves best for this purpose by allowing different contexts to be transferred for each candidate nAR. So, the MN is able to choose which services are more network-sensitive and send the corresponding contexts to the nARs. For other services it may choose not to do so, i.e. when it handoffs to a new AR, it re-establishes a service from the outset.

4. ANALYSIS OF MESSAGE EXCHANGES

In this section, we further analyse our schemes in terms of CXTP message exchanges. It is stressed that in several occasions, CXTP's current functionality and standard message format [7] is inadequate to supply every requirement of each of the proposed schemes. Hence, we were forced to make several changes in the core CXTP protocol. All the changes we made are described in the following. It has to be mentioned that we strictly followed the security logic behind RFC4067 CXTP's inner function. The same cryptographic mechanisms and security logic was adopted by our schemes and have been modulated accordingly. For more information about cryptographic mechanisms of CXTP, the reader should refer to Reference [7]. Note that cryptographic operations needed in each PE Scheme are shown in italics in the corresponding figures and analysed later in subsection 5.1. Each scheme has both a proactive and a reactive phase. Without doubt, the most important phase is the reactive one. This stands because the proactive phase can be accomplished in parallel with the reception of services. The services during the network handover are interrupted and continued after the context transfer reactive session completion (application handoff). So, the faster the reactive phase is the sooner a sensitive service will continue its provision. However, the proactive phase is also equally critical when the time that the MN is able to maintain connection with a given pAR is limited and hence it has to handover quickly to another AR (nAR).

It is to be noted that the internal working of the two Seamoby's WG schemes is not provided in the paper. The reader should refer to the corresponding RFC [7].

4.1. PE Scheme I

The MN sends a *context transfer active request* (CTAR) message towards the pAR, requesting context transfer. This

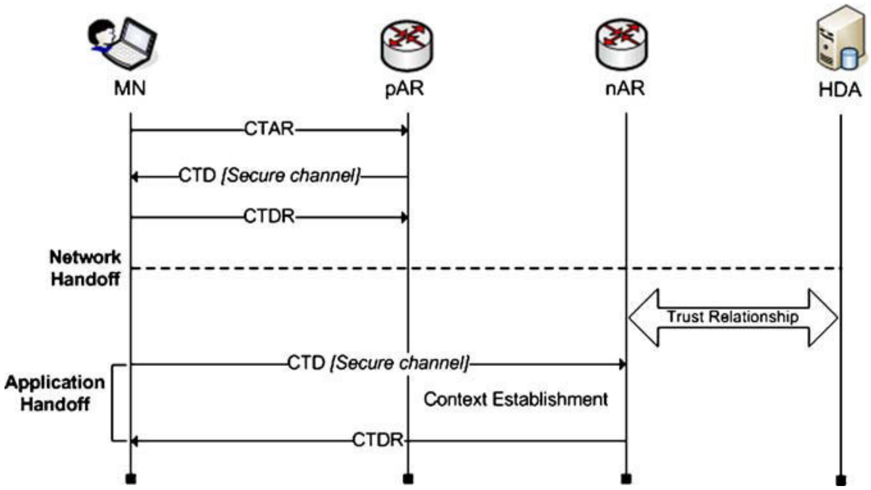


Fig. 3. Message flow for PE Scheme I.

message contains the MN's previous IP address and the context data blocks (CDB) that are going to be transferred. The pAR's/nAR's IP address may not be present in the message. Therefore, the corresponding field remains null declaring that the recipient of the context transfer is the MN itself. The authorisation token field takes the null value as well (see the last paragraph of this section for more information about the authorisation token). Responding to a CTAR message, the pAR sends a *context transfer data* (CTD) message to the MN. No cryptographic material is contained in the message. The MN is now responsible for the context transfer. The MN performs a network handover and eventually acquires a new IP address. After that, the application handoff (from the pAR to the nAR) initiates and the MN forwards the CTD message to the nAR. Upon that, the nAR re-establishes the services based on the context data received. Figure 3 depicts the message exchange between all the involved entities. Note that the security of this scheme is based on a pre-existing trust relationship between the MN, the nAR and the user's home domain. However, the establishment of such a relationship remains out of the scope of this paper.

The current scheme requires minor modifications to the CXTP message format. Actually, the only change involves the possible values of the pAR/nAR IP Address field contained in a CTAR message. Except from the pAR/nAR IP address value, null must be included as a possible value, so that the pAR sends properly the CTD message to the MN, according to the architecture. Moreover, the *Algorithm*, *Key Length* and *Key fields* of the CTD message should be able to carry the null value as well. Last, the authorisation token according to RFC 4067 is calculated as: *First (32, HMAC_SHA1 (Key, Previous IP Address|Sequence Number|CDB's)*, where '|' means concatenation and 'Key' is a shared secret known only to the MN and pAR. Also note that the CTDR message is a reply to a CTD message and a *context transfer active acknowledgement* (CTAA) message a reply to a CTAR message. This stands for all the PE-schemes.

4.2. PE Scheme II

According to this scheme, the MN sends a CTAR message directly to the HDA. This means that a secure session between them has to be established beforehand. The CTAR message contains not only the pAR's IP address but nAR's IP address as well. Thus, CTAR message format modification is necessary here. The CTAR message provides also an authorisation token and a sequence number. The token is used by the HDA to authenticate the message. The HDA is now aware of nAR's and pAR's IP addresses. Therefore, HDA communicates with the pAR requesting the user's context by sending a *Context Transfer Request* (CTReq) message. When the HDA receives the context, verifies the token and forwards it to the nAR. After network handoff, the MN sends a CTAR message to the nAR requesting context establishment. The nAR authenticates the MN and then establishes the services based on the context. If the nAR receives the CTAR message before the context data arrives, the nAR can request the context from the HDA anytime by transmitting a CTReq message. All message exchanges for the current scheme are depicted in Figure 4.

For this second scheme the CTAR message sent by the MN to the HDA must include both the nAR and pAR IP addresses. Hence, modifications must be made to the current CTAR message format, i.e. an extra field must be added. The first field will contain the pAR's IP address, thus notifying the HDA where to request the context from. The other field will carry the nAR's IP address, so that the HDA knows where to forward the context data. The CTAR message, which the MN sends to the nAR, includes the HDA's IP address in the pAR/nAR IP address field and specifies no contexts. By doing so, if the CTD has delayed to respond

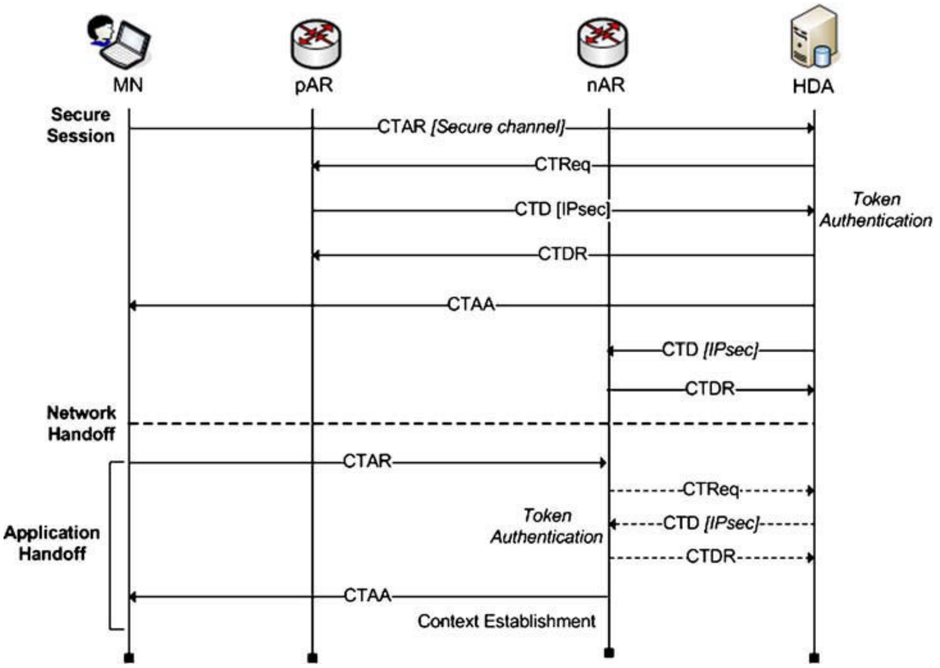


Fig. 4. Message flow for PE Scheme II.

for some reason and the nAR has not received the context(s) yet, the nAR is possible to request the contexts directly from the HDA.

4.3. PE Scheme III

The third scheme depicted in Figure 5 unfolds as follows. The MN sends a CTAR message to the pAR. Instead of the nAR's IP address, the CTAR message contains the IP address of the HDA. Also, this message provides a sequence number and the MN's previous IP address. The token authorisation field is not necessary and thus it can be left blank (null). The pAR receives a CTAR message and sends a CTD message to the HDA. The latter contains a sequence number included in the CTAR and all the cryptographic material needed by the nAR to authenticate the MN. After the

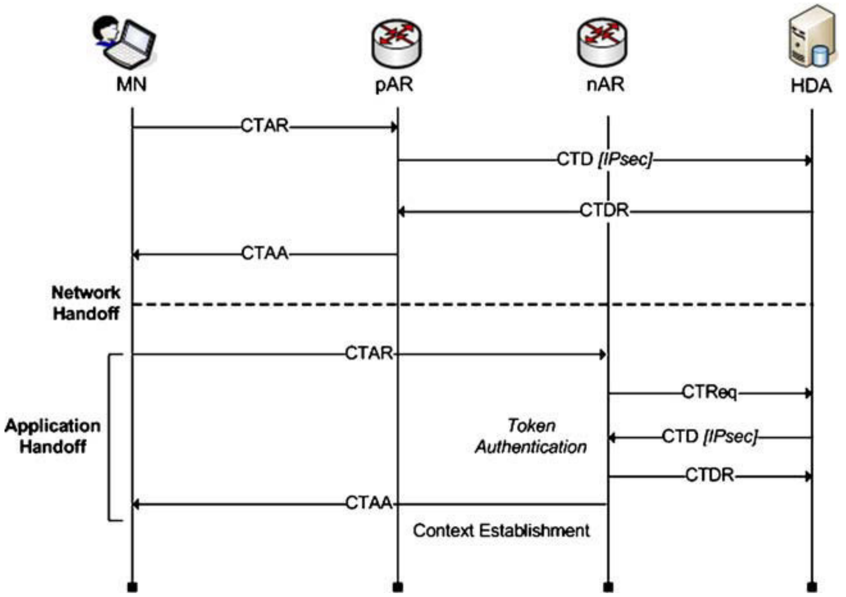
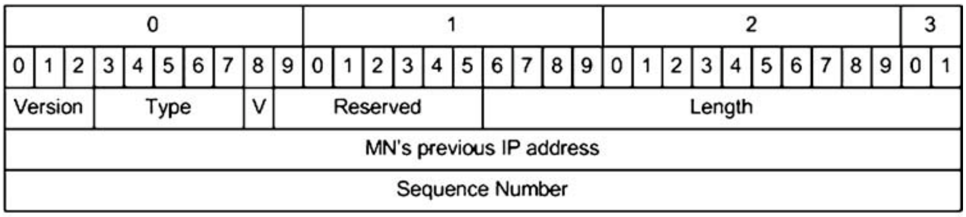


Fig. 5. Message flow for PE Scheme III.



<table>
<tr><td colspan="10">0</td><td colspan="10">1</td><td colspan="10">2</td><td colspan="2">3</td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td></tr>
<tr><td colspan="3">Version</td><td colspan="5">Type</td><td colspan="1">V</td><td colspan="7">Reserved</td><td colspan="16">Length</td></tr>
<tr><td colspan="32">MN's previous IP address</td></tr>
<tr><td colspan="32">Sequence Number</td></tr>
</table>

Version: Version of CXTP = 0x1
Type: CT-Ref = 0x8 (Context Transfer Refresh)
'V' flag: When set to '0', using IPv6 addresses. When set to '1', using IPv4 addresses
Reserved: Set to '0' be the sender. Ignored be the receiver
Length: Message length in units of octets
MN's Previous IP Address Field: IPv4 address (4 octets) or IPv6 address (16 octets)
Sequence Number: Request identification number

Fig. 6. Format of CT-Refresh (custom) message.

network handoff, the MN sends to the nAR a CTAR message containing: (a) the same sequence number as in the first CTAR message, (b) the authentication token and (c) the IP address of the HDA. After that, the nAR requests the context data from the HDA by presenting the corresponding sequence number and the MN's previous IP address. The HDA sends the CTD message to the nAR. Finally, the nAR authenticates the MN and establishes the required services based on the context(s) received.

The message modifications in this third scheme affect mainly the CTAR message format. When the MN sends a CTAR message to the pAR, it places in the 'pAR/ nAR IP address' field, the HDA IP address. The same applies in case the MN sends a CTAR message to the nAR. However, this time no context is specified and the nAR requests the context(s) from the HDA. Finally, the CTD message must include a sequence number field.

Another possible variation of PE Scheme III considers an additional message, namely context transfer (*CT*)*-Refresh*. The HDA may cache CTD messages and keep them alive when receiving CT-Refresh messages by the corresponding MN. In this case, re-negotiation for context transfer is avoided. In order for this method to work properly, the CT-Refresh message must contain the previous IP address of the MN and a sequence number which has the same value with the corresponding CTD message that the MN wants not to expire. The structure of a CT-Refresh message is depicted in Figure 6. An HMAC field could also be added above the 'Sequence Number'. Based on this field, the recipient (HDA) is able to verify the integrity and authenticity of the message.

4.4. PE Scheme IV

According to this last scheme, the MN sends a CTAR message to the pAR. This is done for every nAR that the MN is possible to handover and associate with. The CTAR message contains the IP address of the nAR encrypted with a symmetric key. Also, the CTAR message contains the IP address of the HDA, an authentication token and a sequence number. As mentioned in Section 3, the symmetric key is known only to the MN and the HDA. For every nAR (corresponding to a CTAR message), the pAR encapsulates the encrypted nAR's IP address into a CTD message and forwards it towards the HDA. The HDA reveals the recipient of every CTD message by decrypting the corresponding IP address field. After that, every nAR receives a CTD message from the HDA and waits for a CTAR message from the MN to initiate an application handoff. Only one of the candidate nARs will finally receive a CTAR message and will proceed to re-establish user's service(s) according to the acquired context data. Message flow for the current scheme is described in Figure 7.

This scheme requires the following modifications to CXTP message format. The IP address of the HDA is to be contained in the 'pAR/nAR IP address' field of the MN-to-pAR CTAR message. Moreover, the CTAR message requires an additional field which stores the encrypted IP address of the nAR. For the same reason the pAR-to-HDA CTD message requires an additional field. Also, the CTAR message that the MN sends to the nAR contains the IP address of the HDA in the 'pAR/nAR IP address' field.

5. IMPLEMENTATION

In order to examine the behaviour and evaluate in terms of application handoff service time the above context transfer schemes, we construct several prototype simulation scenarios based on NS-2. For cryptographic operations, where needed, we use the Crypto ++ library in version 5.6.0. All the discussed scenarios are simulated and compared with the two core context transfer schemes proposed in Reference [7]. The performance evaluation is performed at the level of context transfer packet exchange. This means that we measure the round trip time of the context transfer

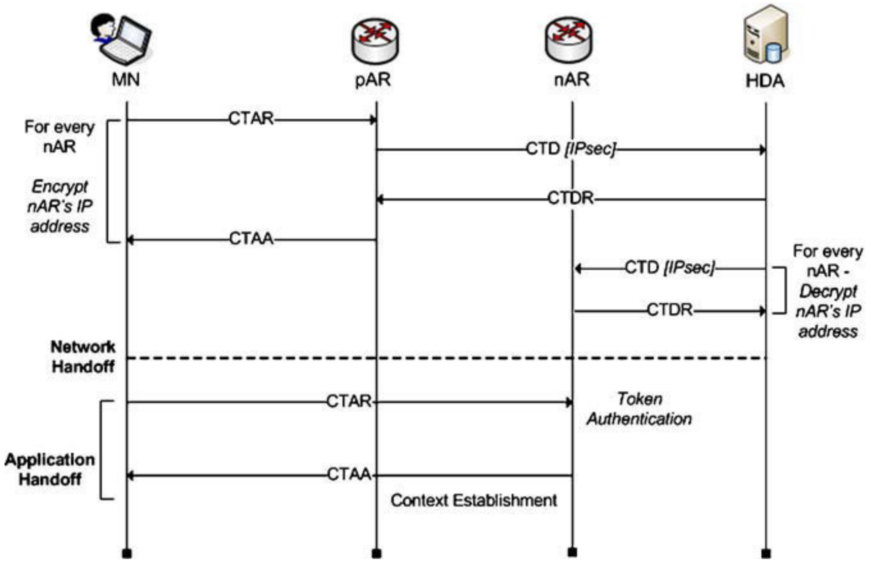


Fig. 7. Message flow for PE Scheme IV.

packet exchange in every scenario as the case may be. In a nutshell the main objectives of the simulations are the following:

- Application handoff time comparison between the proposed PE context transfer schemes.
- Comparison between PE context transfer schemes and the default RFC 4067 schemes [7], namely SeaMoby ProActive (SM PA) and ReActive (SM RA).

5.1. Cryptographic mechanisms

As already pointed out in Section 4 our scenarios include several cryptographic operations. Therefore, the latency induced by such operations has to be taken into account for the simulations. Here, we choose to separately implement all cryptographic functions involved in each scheme and embed them into the simulation scenario as the case may be. This is justified by the fact that the cryptographic functions involved in all scenarios heavily rely on the device employed, not the network. Also, this gives us the ability to easily recalculate total times when changing the hardware characteristics of a device or the security algorithm employed.

A considerable number of cryptographic libraries exist for the above purpose. We used Crypto ++ in an AMD Athlon 2 GHz system running Linux. We only measure cryptographic operations workload induced in every fixed (wired) node. On the other hand, in PE Scheme II the MN has to establish a secure channel between itself and the HDA. PE Scheme I also requires the establishment of a secure channel between the MN and the pAR. Such a secure channel however is assumed to already exist between the MN and the home/visited network, according to the access technology used (e.g. UMTS, IEEE 802.16, 802.11). For instance, in case of a UMTS 3G user the link is protected by means of CK, IK. IEEE 802.16 sessions are protected by means of cryptographic keys generated by Privacy Key Management (PKM)/PKMv2 protocol. Also, considering vertical handovers, e.g. a UMTS user handovers to an 802.11 network, EAP-AKA [21] or other EAP methods should be used for session key derivation. Table I summarises the average cryptographic times for basic cryptographic operations used by our schemes. Figure 8 depicts the total cryptographic operations workload per scheme for both the proactive and reactive phase.

Table I. Average times for cryptographic operations (fixed nodes).

Operation	Algorithm	Time (milliseconds)
Token Authentication	HMAC_SHA1	0.021
IPSec Authentication	SHA1	0.009
Encryption (IPSec / nAR Address)	ENCRYPT_3DES	0.064
Decryption (IPSec / nAR Address)	DECRYPT_3DES	0.050

5.2. Simulations

The MIP implementation of SUN Microsystems [2,3] have already been included in the latest versions of NS-2. So, we use this implementation for performing network handoff during our experiments. However, the MIP module does not support CXTP. So, we extend it to include context transfer capabilities. As already pointed out, in each context transfer scenario a proactive and a reactive phase

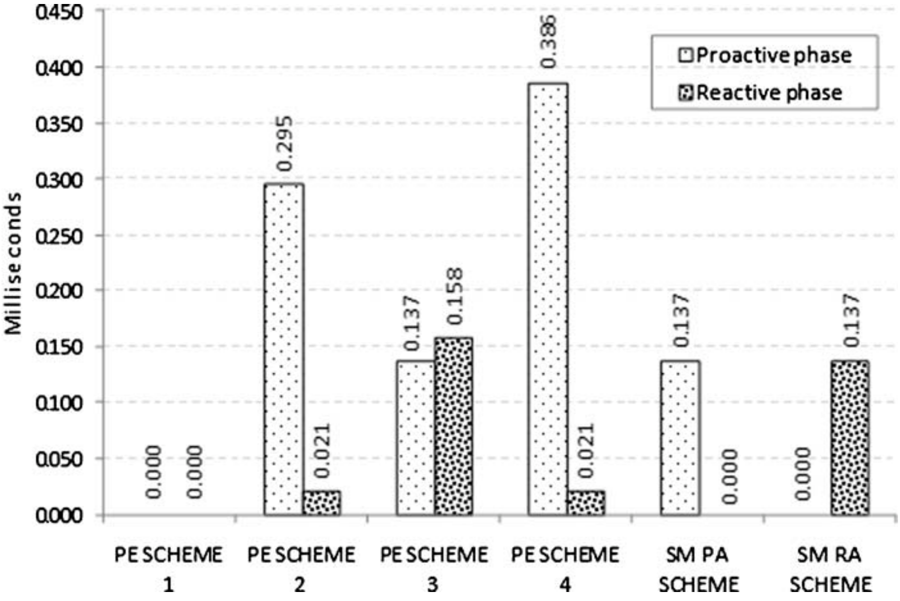


Fig. 8. Cryptographic operations workload per scheme: proactive and reactive phase.

Table II. Total application handoff times per scheme (seconds).

Scheme	Type (P = Proactive, R = Reactive)	Scenario I	Scenario II	Scenario III	Scenario III_b
SM RA	R only	0.0211	0.0637	0.0294	0.2114
SM PA	P + R	0.0256	0.1779	0.0338	0.4345
PE Scheme I	P + R	0.0195	0.0363	0.0236	0.1078
PE Scheme II	P + R	0.0256	0.2101	0.0648	0.7506
PE Scheme III	P + R	0.0267	0.1768	0.0583	0.4347
PE Scheme IV	P + R	0.0227	0.1722	0.0484	0.4346

exist except SM RA that is purely reactive. Between these two phases, a network handoff is executed. We do not measure the duration of the MIP handoff at all. We only measure the application handoff time, i.e. the duration of both the proactive and the reactive phase in each scenario. Therefore, the total CXTP time for every scheme is calculated as: *Total time = proactive phase time + reactive phase time + cryptographic operations time*. This time for each scheme is given in Table II. Every phase in each scenario may start in different point of time. Hence, we measure every proactive phase starting from hypothetical point of time 0.

5.2.1. Scenario I.

Figure 9 depicts the simulation architecture for our first scenario consisting of five nodes. Each node has its own name (n0 to n4) and address (0.0.0 to 1.0.1). Nodes n0 and n1 are wired, while n2 and n3 support both wired and wireless technology. The last node is a wireless one. The MN (n4) is moving from AR1 (pAR) towards AR2 (nAR) and eventually handovers to AR2. There is a TCP connection between the corresponding node (CN) (used by MIP) and the MN. All nodes are configured to the default NS-2 values. Also, the wired links are set to 5 Mbps bandwidth with 2 ms delay. Assuming a 3 G connection the bandwidth of the wireless link is set to 1 Mbps, while the wireless node has a 250 m radius (picocel). We simulated every scheme using three different variations (scenarios) and we present the results for the proactive and the reactive phase separately. The total simulation time is 30 s.

The simulations results for all six schemes are depicted in Figure 10. Obviously, the SM PA and PE Scheme II present far more workload (packet exchanges) than the rest and so the proactive phase takes considerably longer time to

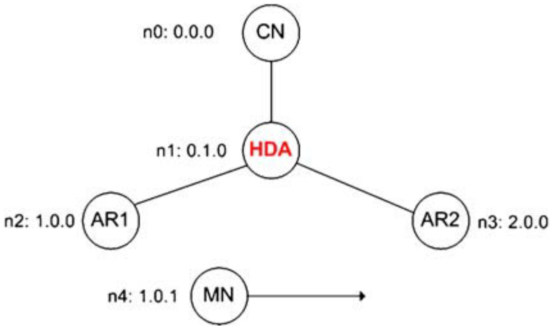


Fig. 9. Simulation topology for Scenarios I and II.

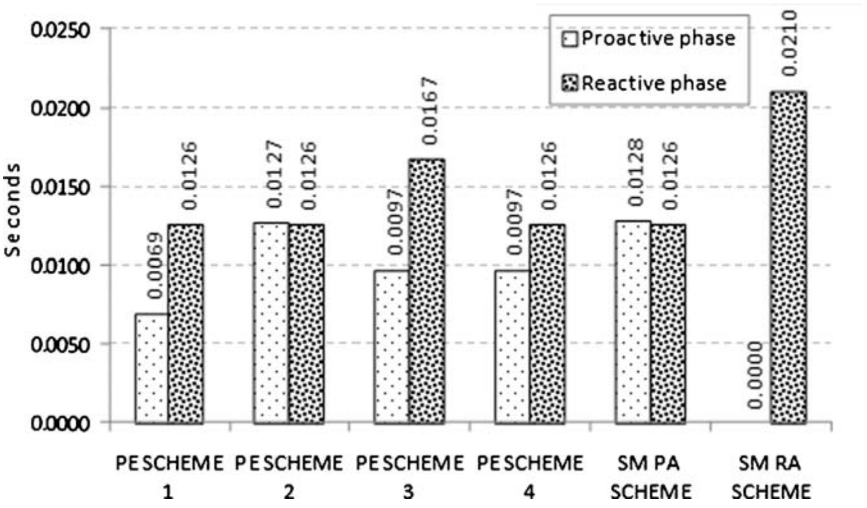


Fig. 10. Overall application handoff time per scheme (Scenario I).

complete. The time difference between the schemes having a proactive phase is very small, spanning from 0.0001 to 0.0060 s. All the proposed PE schemes are more, or at least, equal efficient to the SM PA scheme. The SM RA scheme has no proactive phase. On the other hand, considering the reactive phase the SM RA scheme has the greatest delay as expected, followed by the PE Scheme III. All other schemes have reactive phases that finish almost simultaneously.

5.2.2. Scenario II.

For this second scenario we modify the simulation environment. The wired link between n3 and n2 has 0.5 Mbps bandwidth. Also, there is FTP traffic between n0 and n4. Thus, we expect a greater delay in the handover process than in the previous case. As depicted in Figure 11, the time required for the completion of the proactive phase take much longer. This applies to the majority of the schemes. The PE Scheme II has as always the maximum delay followed by all others. The changes we made to the simulation environment do not affect the performance of the PE Scheme I. Actually, it has about the same completion time as in the previous scenario. The overall time for the reactive phase of each scheme (see Figure 11) is straightforwardly comparable to those of the reactive phase of scenario I. However, the completion time for all the schemes is greater because of the changes we made to the simulation configuration parameters of the current scenario. The proactive phase of PE Scheme II is slower by 0.16 s compared to the corresponding time of scenario I. The same applies for the rest

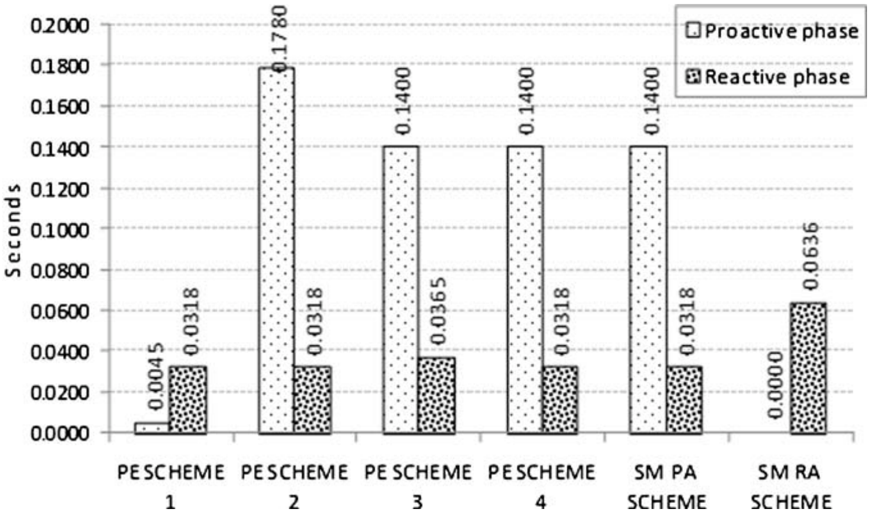


Fig. 11. Overall application handoff time per scheme (Scenario II).

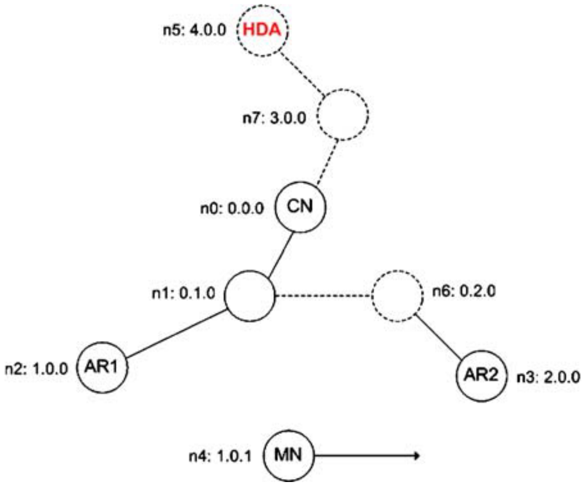


Fig. 12. Simulation topology for Scenario III.

of the schemes except the PE Scheme I which is not affected by network link conditions. On the other hand, we witness a slight increment to the times of the reactive phase of all schemes. This is because, after the network handoff, the TCP traffic has not reached its maximum performance. We also notice that the SM RA and PE Scheme III present the maximum delay due to the greater number of exchanges during the reactive phase in comparison to the rest of the schemes.

5.2.3. Scenario III.

In the third scenario, we further expand the simulation topology. The new architecture is depicted in Figure 12. We move the HDA node further away from the other nodes in order to examine if there is a significant impact to the performance of the HDA-oriented schemes. The simulation parameters are identical to those used in scenario I. The overall time for each scenario for the proactive and reactive phase is given in Figure 13. We can easily infer that moving the HDA deeper into the network generates an additional time penalty only to the HDA-oriented schemes. This stands for both the proactive, e.g. PE Schemes II, IV and the reactive phase (PE Scheme III). Hence, we can infer that the actual distance between the nodes plays a significant role in the overall performance of CXTP.

Also, we modified the current scenario (referred to as scenario III_b) by using the same simulation parameters as in Scenario II. That is, the wired link between n3 and n2 has 0.5 Mbps bandwidth and there is FTP traffic between n5 and n4. The results show a severe degradation to the completion of both the reactive and proactive phase. This is especially true for the schemes that employ the HDA. For instance, the proactive phase of PE Scheme II increased by 1200%, while the reactive phase of SM RA increased by 800%.

5.2.4. Discussion.

Summarising all the above, the SM RA scheme, proposed by the Seamoby group [7], is clearly a reactive one. Compared to all the others, this scheme presents the worst performance. It may be used only in need of emergency. That is, when for some reason, the proactive phase cannot be executed. However, even in this case it should be wise to calculate the benefits from using it against the re-establishment of the services in the new administrative domain from the outset. The SM PA scheme is more efficient than the first one but it has a relatively slow proactive phase. As already pointed out, the problem with the two aforementioned schemes is that they do not preserve the privacy of the end-user.

On the other hand, our schemes do preserve location privacy but the main question is how efficient they are in comparison to the Seamoby ones. The best scheme in terms

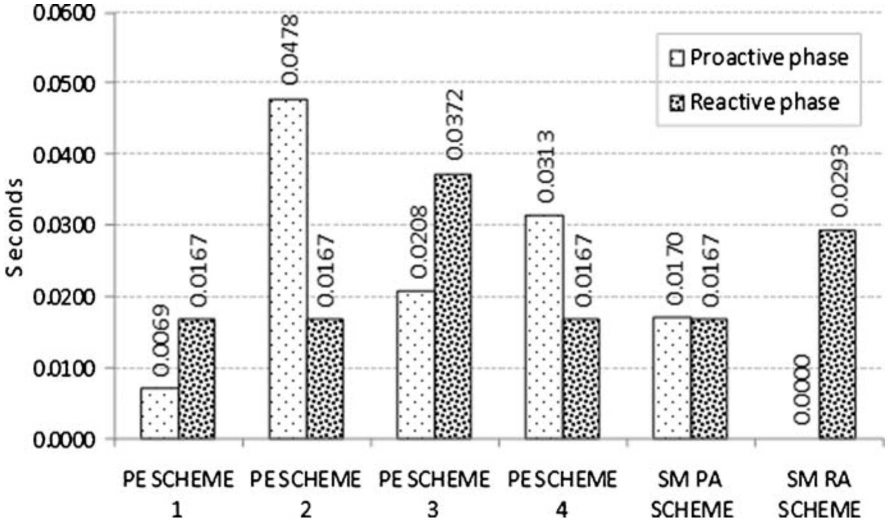


Fig. 13. Overall application handoff time per scheme (Scenario III).

of performance is the PE Scheme I. It is fast because the node distances and traffic conditions have little impact on this scheme. However, as discussed previously in Section 3, there are two drawbacks concerning the internal workings of this scheme. The first one is the trust relationship that has to somehow pre-exist between the user's home network and the corresponding nAR. The other one concerns the integrity of the context data message during the time that is being held by the MN. The PE Scheme II has a very efficient reactive phase but also presents a very inefficient proactive phase. Its performance is affected by node distances and network conditions (speed, link capacity, congestion etc). If the HDA is not placed too far away from the MN, this scheme can equally substitute the SM PA one.

The last two PE schemes are more demanding and complex than the others but they serve a different purpose focusing on future NGN services. Nevertheless, the results demonstrate that they are quite efficient for 4G environments. The PE Scheme IV has some extra features like selecting many potential visiting domains while other schemes do not follow the same logic. Therefore, it was not our intention to simulate sub-scenarios suitable only for PE Scheme IV. This is actually a concern for future work. Though, it should be mentioned that the cost of selecting a nAR amongst many potential visiting domains depends on the number and the distance of potential nAR as well as the network conditions. In any case, however, only the proactive phase performance is affected; that means that there is no perceived delay during the handover. Overall, PE Scheme IV is proved to be more efficient than PE Scheme III because it has a fast reactive phase. On the other hand, PE Scheme III is simpler, has faster proactive phase and is more secure than PE Scheme IV. This stands because the former does not transmits any sensitive data while the latter transmits encoded sensitive data. Specifically, recall from subsection 4.4 that in PE Scheme IV, every nAR receives context information from the pAR (i.e. CTD message). This is triggered by the MN, and the CTD message is delivered to every nAR *via* the HDA which acts as a proxy. Thus, the nAR candidates are unaware of the MN's current pAR and *vice versa*. Consequently, by putting the HD to act as an intermediary, we succeed in securing end-user location privacy in CXTP. However, several domains receive the CTD message before the MN finally handovers to one of them and this may result to a privacy breach. If we examine a CTD message, the most important values exposed, that may affect CXTP security are the context data, the pre-shared key the pAR and MN share, and the MN's previous IP address. Any privacy issue arises from the content of the context data remains out of the scope of this paper because it is not a problem of the CTXP *per se*. Also, it is obvious that the pre-shared key does not provoke any privacy issues. Finally, it seems that the MN's previous IP address could affect user's location privacy; however, in practice, it can barely cause location privacy issues and only if different domains collude including the chosen nAR. This is actually a general issue and of course applies to every scheme described in this paper. Moreover, while an IP address can reveal some information about the network domain a user is connected to, this information is well known not to be always accurate. Specifically, the only thing an IP address reveals reliably is the name of the service provider or anonymising proxy (if used). The rest depends on the way the service provider's systems are configured. In fact, there are solutions for the protection of this information like those reviewed in Reference [22].

6. CONCLUSION AND FUTURE WORK

It is envisioned that future wireless networks will converge to an all-IP platform offering more bandwidth consuming services at higher speeds. In such an environment, the confidentiality of the service without perceived degradation by the end-user is a very challenging issue. The realisation of this objective includes the cooperation of mobility management schemes with AAA protocols for the secure and uninterrupted multimedia services provision. In this paper, we propose four privacy preserving schemes for CXTP. Our schemes are compared with those proposed by the Seamoby Group in RFC 4067. By employing three different simulation scenarios, we study the performance of all six schemes in terms of application handoff service time. Simulations are analytical including separate measurements for the proactive and reactive phase of each scheme. Also, where required, cryptographic penalties are calculated for fixed nodes and added to the overall simulation time according to the scenario. The results show that all the proposed schemes are promising and in several cases perform better or at least equal to those of the Seamoby WG.

As future work, we would like to expand this proposal by refining our schemes and conducting real experiments to better approximate their behaviour. Another direction is to formalise the attack model employed by the adversary and use it to show how privacy is breached/preserved.

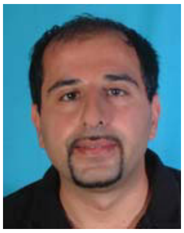
REFERENCES

1. Nasser N, Hasswa A, Hassanein H. Handoffs in fourth generation heterogeneous networks. *IEEE Communications Magazine* 2006; **44**: 96–103.
2. Perkins C (ed.), *IP Mobility Support for IPv4, IETF RFC 3344*, August 2002.
3. Johnson D, Perkins C, Arkko J. *Mobility Support in IPv6, IETF RFC 3775*, June 2004.
4. Rosenberg J, Schulzrinne H, Camarillo G, *et al. SIP: session initiation protocol. RFC 3261, IETF*, June 2002.
5. Xu P, Liao J, Wen X, Zhu X. Optimized integrated registration procedure of mobile IP and SIP with AAA operations, 20th International Conference on Advanced Information Networking and Applications (AINA'06), IEEE CS Press, Vol. 1, 2006; 926–931.
6. Dutta A, (ed.) Fajardo V, Ohba Y, Taniuchi L, Schulzrinne H. A framework of media-independent

pre-authentication (MPA) for Inter-domain Handover Optimization. IETF Internet Draft, draft-irtf-mobopts-mpa-framework-07, work in progress, April 2010.

7. Loughney J, Nahkjiri M, Perkins C, Koodli R. *Context Transfer Protocol*, *IETF RFC 4067*, July 2005.
8. Karopoulos G, Kambourakis G, Gritzalis S. Survey of secure hand-off optimization schemes for multimedia services over all-IP wireless heterogenous networks. *IEEE Communications Surveys and Tutorials* 2007; **9**(3): 18–28.
9. Karopoulos G, Kambourakis G, Gritzalis S. Two Privacy Enhanced Context Transfer Schemes, Q2SWinet'07. ACM Press. Chania, Greece, 2007.
10. NS-2, Network Simulator 2. Available at: www.isi.edu/nsnam/ns
11. Wei D. The Crypto++ Library. Available at: www.eskimo.com/weidai/cryptlib.html
12. Bartolini N, Campegiani P, Casalicchio E, Tucci S. A performance study of context transfer protocol for QoS support, *Proceedings of 19th Inernational Symposium on Computer and Information Sciences*, Turkey, LNCS 3280, Springer, 2004; 594–603.
13. Bartolini N, Casalicchio E. A performance analysis of context transfer protocols for QoS enabled Internet services. *Computer Networks* 2006; **50**(1): 128–144
14. Garcia-Martinez CP, Garcia-Macias JA. Analysis of context transfer in seamless IP mobility, *5th International School and Symposium (ISSADS 2005), PL Mexico*, LNCS 3563, Springer. 2005.
15. Allard F, Bonnin JM. An application of the context transfer protocol: IPsec in Ipv6 mobility environment. *International Journal of Communication Networks and Distributed Systems* 2008; **1**(1): 110-126.
16. Georgiades M, Dagiuklas T, Tafazolli R. Middlebox context transfer for multimedia session support in all-IP networks, *Proceedings of international Conference On Communications And Mobile Computing*, Vancouver, Canada, ACM Press, 2006; 389–394.
17. Oyoqui JM, Garcia-Macias JA. Context transfer for seamless micro-mobility, *Proceedings of the International IEEE Conference on Computer Science (ENC)*, IEEE Press, 2003; 291–297.
18. Allard F, Combes J-M, Marin R, Gomez AF. Security analysis and security optimization for the context transfer protocol, *Proceedings of New Technologies, Mobility and Security (NTMS '08)*, IEEE Press; 1–5.
19. Askwith B, Merabti M, Shi Q, Whiteley K. Achieving user privacy in mobile networks, *Proceedings of 13th Annual Computer Security Applications Conference, ACSAC*, IEEE Computer Society, San Diego, CA, USA, December 1997; 108–116.
20. Kassar M, Kervellaa B, Pujollea G. An overview of vertical handover decision strategies in heterogeneous wireless networks. *Computer Communications* 2008; **31**(10): 2607–2620.
21. Arkko J, Haverinen H. Extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA), *IETF RFC 4187*, January 2006.
22. Gritzalis S. Enhancing web privacy and anonymity in the digital era. *Information Management and Computer Security* 2004; **12**(3): 255–288

Authors' Biographies



Iosif Terzis was born in Thessaloniki, Greece in 1979. He holds a diploma in Computer Science and Telecommunications from Technological Educational Institute of Epirus, Greece and a MSc in Information and Communication System Security. He is currently a Ph.D. candidate at the Department of Information and Communication Systems Engineering, University of the Aegean, Greece. His primary research interests lie in the field of wireless network security and privacy protection.

Georgios Kambourakis received the Diploma in Applied Informatics from the Athens University of Economics and Business and the Ph.D. in Information and Communication Systems Engineering from the Department of Information and Communications Systems Engineering of the University of Aegean. He also holds a M.Ed. from the Hellenic Open University. Currently, Dr. Kambourakis is a Lecturer at the Department of Information and Communication Systems Engineering of the University of the Aegean, Greece. His main research interests are in the fields of mobile and wireless networks security and privacy, VoIP security and mLearning. He has been involved in several national and EU funded R&D projects in the areas of Information and Communication Systems Security. He is a reviewer of several IEEE and other international journals and has served as a technical program committee member in numerous conferences.

Giorgos Karopoulos (gkar@aegean.gr) is currently a Postdoctoral research fellow at the Info-Sec-Lab of the Department of Information and Communication Systems Engineering, University of the Aegean. He holds a diploma in Information and Communication Systems Engineering, a MSc in Information and Communication Systems Security, and a PhD in Computer Network Security from the University of the Aegean. His current research focus is in mobile multimedia security in all-IP heterogeneous networks.

Dr. Costas Lambrinoudakis holds a B.Sc. (Electrical and Electronic Engineering) from the University of Salford (1985), an M.Sc. (Control Systems) from the University of London (Imperial College -1986), and a Ph.D. (Computer Science) from the University of London (Queen Mary and Westfield College - 1991). Currently he is an Assistant Professor at the Department of Digital Systems, University of Piraeus, Greece. From 1998 until 2009 he has held teaching position with the University of the Aegean, Department of Information and Communication Systems Engineering, Greece. His current research interests are in the areas of Information and Communication Systems Security and of Privacy Enhancing Technologies. He is an author of more than 85 scientific publications in refereed international journals, books and conferences, most of them on ICT security and privacy protection issues. He has served as program committee chair of two international scientific conferences and as a member on the program and organizing committees of many others. Also he participates in the editorial board of two international scientific journals and he acts as a reviewer for more than 20 journals. He has been involved in many national and EU funded R&D projects in the area of Information and Communication Systems Security. He is a member of the ACM and the IEEE.

DOI: 10.1002/wcm