

# Fast Re-Authentication for Inter-Domain Handover using Context Transfer

Omar Alfandi, Henrik Brosenne, Constantin Werner, Dieter Hogrefe

*Institute for Informatics, Telematics Group, University of Göttingen*

*Lotzestrasse 16-18, 37083 Göttingen, Germany*

{alfandi, brosenne, werner, hogrefe}@cs.uni-goettingen.de

**Abstract**— The exponential growth of wireless mobile systems in recent years has created strong demand to handover between different administration domains. Such movement suffers from limited resources such as limited bandwidth and high latency. Furthermore, authentication is the key factor when providing mobile roaming services, so fast re-authentication is one of the important issues to achieve a short overall handover delay. Therefore, it is important to develop techniques that utilize the available bandwidth efficiently. One way of utilizing the wireless resources efficiently is by transferring the required context that authenticates the user in new visited domain of the running session rather than establishing the connection from scratch. Current approaches only consider a repeated authentication process run for a new visited domain and therefore, can potentially introduce high latency by communicating with authorization services of a home domain. In this paper, we propose a novel way to authenticate a mobile node without the necessity to communicate with the home domain while maintaining a high level of security. We provide an overview of the method, show the improvement to related approaches in terms of message flows and discuss security aspects.

## I. INTRODUCTION

Nowadays wireless access networks can provide high data rate and ubiquitous access to network and services. One of the current research challenges which have to be dealt with is that these communication systems offer mobility to the user, even in the case when the networks are owned and managed by different operators. To support fast mobility, inter-domain handover should be performed with little delay. Inter-domain handover in this work means a Mobile Node (MN) running a communication session changes its attachment point from one network domain to another, in which the two domains are managed by different operators. To fulfil security requirements and financial aspects (e.g. billing), MN must be authenticated when it handovers to a new domain. When an inter-domain handover happens between visited domains, a full mutual authentication can hardly fulfil the requirement of short delay [7].

Existing approaches for authentication in mobile handover cover only the intra-domain case. Neither fast handover for Mobile IP nor for 3GPP-based networks are designed to work in an inter-domain scenario. Current developments in the IETF propose pre-authentication which can result in high latency and traffic overhead. Therefore, this paper proposes a new fast authentication method for inter-domain handover. To achieve this, an already established authentication context in the current visited domain is re-established in the new visited

domain. We combine a number of well-known protocols and approaches for intra-domain mobility and introduce extensions to enable inter-domain handover.

The remainder of this paper is organized as follows: the following Section 2 gives an overview of related work. Section 3 describes the proposed security framework of the used protocols with more detail and technical description. Section 4 summarises and discusses our new approach in comparison to the pre-authentication approach. Finally, the conclusions and the future work outlook are given in Section 5.

## II. RELATED WORK

Fast authentication for inter-domain handover is a topic of recent research in academia and industry. But besides few proprietary solutions fast handover is not supported in most mobile networks.

In 3GPP's latest technical specification of 3G mobile systems [1], inter-domain is called inter-PLMN (Public Land Mobile Network) [2]. Because only the basic requirements are identified, the inter-PLMN handover remains to be an optional feature.

IEEE 802.11F [4] standard defines the Inter-Access Point Protocol (IAPP) to support interoperability between WLAN access points (APs). The scope of 802.11F is limited to the intra-domain case, i.e. handover between WLANs of one network operator. Nevertheless approaches like proactive caching mechanism where an AP sends context parameters to neighbouring APs and the possibility that APs obtain information about one another are also valuable for inter-domain handover.

Inter-domain authentication as an extension to the standard IEEE 802.1x and Extensible Authentication Protocol (EAP) protocols [15] is analysed in [14]. The paper compares the performance of different authentication methods among multiple WLAN service providers.

IETF SEAMOBY Working Group [11] was focussing on mobility over IP wireless infrastructure within one network domain. It proposed a technique to smoothen network layer handover by transferring the context information for a session from the current access router (cAR) to the new access router (nAR) in order to avoid setting up the states from scratch. This Context Transfer Protocol (CXTTP) [3] is one of the proposals published by this working group and has been categorised as an experimental RFC.

The Protocol for Carrying Authentication for Network Access (PANA) [6] is proposed by the IETF PANA Working

Group [12]. PANA is a layer 3 transport protocol for EAP to enable network access authentication. PANA is independent of the layer 2 protocol used and irrespective of the Authentication, Authorisation and Accounting (AAA) infrastructure that may reside on the network. Clients do not have to understand the AAA protocols (e.g. DIAMETER, RADIUS) in local use. PANA will allow interaction with this infrastructure in a protocol-neutral way. The PANA protocol framework consists of a PANA Client (PaC) communicating with a PANA Authentication Agent (PAA). For each PANA message carrying an EAP message payload, a PANA confirmation message is returned. However, the PANA framework only considers a local authentication scenario and thus, there is no consideration for (fast) re-authentication in inter-domain handover case.

As a result, the PANA working group proposed the PANA pre-authentication [8] to overcome this limitation. While still being connected to the current domain, the pre-authentication for the new domain is executed in the background. In essence, the pre-authentication is only a slightly optimized version of the standard PANA authentication.

CXTP for PANA [5] based on PANA Mobility Optimizations [9] enhances intra-domain handover by recovering the already established PANA authentication context from the current PAA (cPAA) to the new PAA (nPAA). In [13] a similar idea is discussed, the new domain authenticates the MN based on the trust relation between the MN and the current domain

These ideas inspired our work and have been adapted to support inter-domain handover. Furthermore, security issues of context transfer are vital to be considered and the service level agreement (SLA) between the involved domains has to be considered.

### III. PROPOSED FRAMEWORK FOR INTER-DOMAIN HANDOVER

The authentication process triggered by movement to a new domain is a matter of keeping a connection alive to avoid the establishment of a service session from scratch every time the user reaches a new point of access the necessary credentials and information are re-establishment in advance. An automated mechanism that handles this process is a vital prerequisite for fast handover. Adequate authentication mechanisms are necessary to prevent unauthorised use of resources and information.

To authenticate a user moving through different domains the operators of the domains must have a mutual trust relationship among each other to exchange information and credentials of the user. These relationships are called service level agreement (SLA).

The general framework incorporates an Authentication, Authorisation and Accounting (AAA) infrastructure to authenticate the MN for access to network resources. In the proposed scenario depicted in Fig. 1, three domains are considered with each of them owning an AAA server: the current visited domain (cVD), the new visited domain (nVD) and the home domain (HD) of the user.

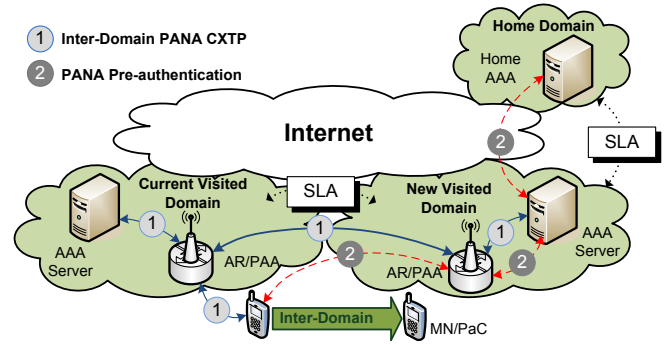


Fig. 1 Inter-Domain Scenario

For PANA pre-authentication, an SLA between the new visited and the home domain is required. After a handover has been triggered, the PANA pre-authentication runs a complete PANA-EAP authentication sequence with the AAA server of the new visited domain and in turn, with the home domain that is able to verify the given credentials ultimately. Not until the pre-authentication process has successfully completed, the connection to the current visited domain will be terminated.

In contrast, inter-domain PANA CXTP proposed in this paper transfers the PANA authentication contexts from the current visited domain to the new visited domain directly. This requires an SLA between the current and new visited domain so that both domains share a mutual trust relationship with each other and thus, accept context information to be received and actively instantiated on a PANA authentication agent (PAA). The approach allows receiving the user's context securely without the need to communicate with the home domain. This could potentially result in high latencies in the case that the home domain is located far away. In addition, our approach requires fewer messages to be exchanged than in PANA pre-authentication.

The following section details the enhancement and improvements of PANA by using the CXTP for inter-domain handover.

#### A. Scenario

The scenario architecture in Fig. 1 considers that a MN is authenticated in the cVD. The cPAA is the authentication agent for the current session. After a mean of time, the MN is attending to perform a handover or even the cVD desires a handover to the nVD.

A MN is authenticated to the nVD using inter-domain PANA CXTP by transferring the necessary context from the cPAA to the nPAA. The process is based on PANA [6], the fast handover with CXTP and PANA [5] and PANA Mobility Optimizations (MobOpts) [9]. As these methods are currently only designed for the intra-domain case, some enhancements are necessary to enable the inter-domain case.

The first enhancement is the introduction of new signalling messages between PAA and AAA server that allows the PAA to determine whether an appropriate SLA exists between its own and another domain. Because the SLAs are negotiated offline and the number of neighbouring domains is

manageable, an operator can smoothly export this information to the AAA server.

The second enhancement is the protection of the transferred context by public key encryption. As an MN can possibly handover to numerous PAAs it is not expedient to store the public key of each candidate nPAA. To solve this problem for each domain for which an SLA agreement has been made, the public key of the corresponding AAA server is stored in addition to the SLA information. If the determination of an appropriate SLA succeeds, the public key is sent to the requesting PAA. This key can be used to check integrity and validity of a public key sent by a PAA from the other domain provided that this public key is digitally signed by the associated AAA server. This can be realised with certificates for instance.

The transferred context is an authentication key stored in the PAA. The cryptographic separation of the authentication key in the cPAA, the intermediate key transferred between cPAA and nPAA and the key belonging to the new session in the nPAA is the third enhancement. Different than the intra-domain approach, the PANA based values taken into computation for the intermediate key are not exported to the nPAA. Following PANA MobOpts, the new authentication key is calculated using nonce values the cPAA is not aware of.

A security vulnerability of this approach is that a compromised cPAA could potentially pretend an unauthorized MN to the nPAA as being legally authorized. But compromised ARs/PAAs are a common risk. Only operators that can guarantee the same (high) level of AR/PAA intrusion or compromise protection will agree on an SLA that allows context transfer. Nevertheless further research is necessary to weaken this vulnerability.

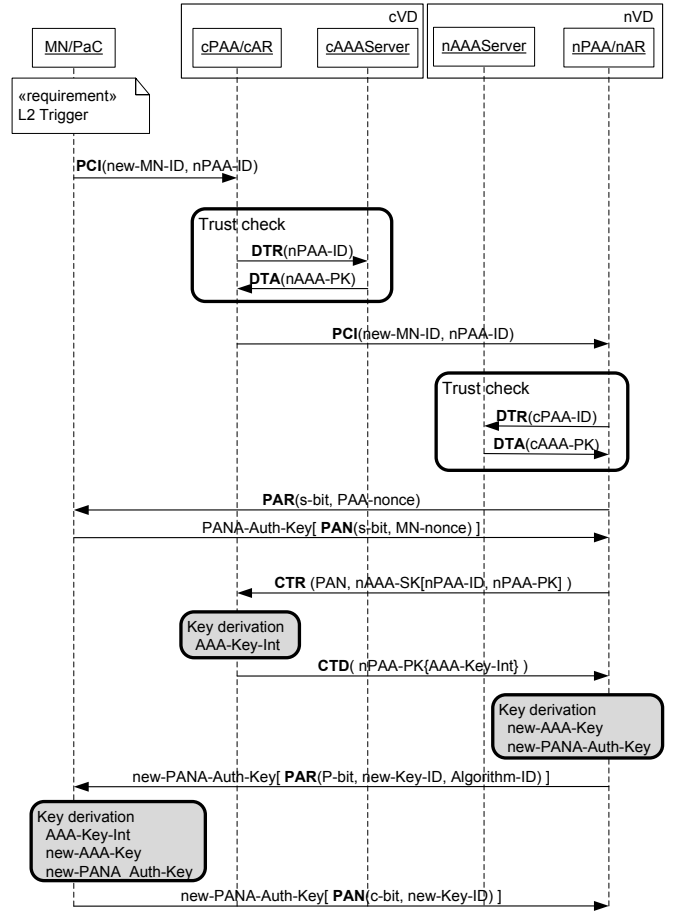
The different domains are connected by the Internet. To increase the level of security the domains may provide an additional solution to protect data exchanges over the Internet. These mechanisms are not taken into account in this paper. Even in the case that there is no appropriate SLA agreed between domains, the transfer can be activated based on dynamically established trust. However, this paper will not consider this case at the moment.

### B. Technical Description

In order to facilitate the authentication in the new visited domain, the PANA and CXTP in the AAA architecture is combined as shown in Fig. 1. The same issues that are involved in handover between access networks in the same administrative domain are relevant. A sequence diagram illustrating the message flow can be found in Fig. 2.

For sake of simplicity, it is assumed that the following prerequisites are satisfied.

- PaC is part of the MN.
- AR and PAA are co-located.
- Each domain has only one single AAA server deployed.
- PAA-ID contains information of the belonged domain.
- Each AAA server can access a database (or similar) containing predefined SLA with each domain (in case an SLA is agreed with that domain) and the public key of the corresponding AAA servers.



DTT: Domain-Trust-Request, DTA: Domain-Trust-Answer, PCI: PANA-Client-Initiation, PAR: PANA-Authentication-Request, PAN: PANA-Authentication-Answer, CTR: Context-Transfer-Request, CTD: Context-Transfer-Data, PK[payload]: payload encrypted under public key PK, SK[payload / message]: payload / message signed with private key SK.

Fig. 2 Inter-domain PANA CXTP Message Flow

In the considered scenario, the MN is authenticated to the current PANA authentication agent (cPAA) in the current visited domain (cVD) using an EAP method exporting a master session key addressed as AAA-Key in the PANA framework. MN and cPAA has derived a PANA authentication key (PANA-Auth-Key) from the AAA-Key and agreed on a distinct key id (Key-ID) for this key.

The MN receives a layer 2 handover trigger containing the ID of the new PAA (nPAA-ID) in the new visited domain (nVD). Based on the nPAA-ID the MN computes a new id (new-MN-ID) for the communication with the nPAA, e.g. if IPv6 is used a link-local IP address of the MN.

The MN initiates the negotiation by sending a Pana-Client-Initiation (PCI) message to the cPAA containing the nPAA-ID and the new-MN-ID. Originally the PCI initiates an authentication of the MN to the cPAA. The cPAA deduces inter-domain PANA CXTP because the PCI is not empty and contains the id of an authenticated MN as well as the id of an entity in a different domain.

The cPAA will only transfer context if a service level agreement (SLA) between the cVD and the nVD exists. This

is checked by sending a Domain-Trust-Request (DTR) containing the nPAA-ID to the cAAA. As confirmation the cAAA sends the nAAAs public key (PK-nAAA) in a Domain-Trust-Answer (DTA). The PK-nAAA will later be used to check the integrity of messages from the nPAA. After checking the SLA the cPAA forwards the PCI to the nPAA. Again the nPAA notices non standard PANA because the PCI is not empty. It includes the nPAA's own id so the nPAA interprets the other id as the id of a MN requesting inter-domain PANA CXTTP from the sender of the PCI (the cPAA) to the nPAA.

The nPAA will only accept transferred context if an adequate SLA exists. It sends a DTR to the nAAA and gets as confirmation a DTA containing the cAAA's public key (PK-cAAA). Currently we make no use of the PK-cAAA. The nPAA chooses a nonce (nPAA-nonce) and starts the PANA authentication by sending this nonce to the MN in a PANA authentication request (PAR) with start bit set (s-bit). The MN chooses a nonce (MN-nonce) too and reacts with a PANA authentication answer (PAN) signed by the PANA-Auth-Key with s-bit containing MN-nonce. In the original CXTTP for PANA approach [5] the PAN contains the id of the cPAA as part of a session id attribute value pair (AVP) and the presence of the session id AVP indicates the request for context transfer. In the current PANA specification [6] the session id AVP is replaced by a numerical session identifier but this is no problem, in our approach the id of the cPAA is already known by the nPAA and the request for context transfer is indicated by the PCI message.

The nPAA starts the context transfer by sending a Context-Transfer-Request (CTR) to the cPAA containing the last PAR message as well as the nPAA's identity and public key (nPAA\_PK) both signed by the nAAA. This can be a certificate for example.

The cPAA checks the integrity of the PAR message with the PANA-Auth-Key and validates identity and public key of the nPAA with the PK-nAAA. If all checks pass the cPAA computes an intermediate AAA-Key (AAA-Key-Int) cryptographically separated from the AAA-Key by taking the numerical session identifier, the Key-ID and the current id of the MN into computation.

The AAA-Key-Int is the PANA context used by the nPAA to authenticate the MN in the nVD. Originally the remaining lifetime of the PANA session is part of the context too. To enhance security in our approach the nPAA sets the session lifetime to a self-determined small value.

The cPAA transfers the PANA context encrypted under the nPAA's public key to the nPAA in a Context-Transfer-Data message (CTD). This is the sensitive part of the protocol. Because the prospective security associations between the MN and nPAA base on keys derived from AAA-Key-Int. In the intra-domain case no protection of the CTD payload is intended.

The nPAA derives a new AAA-Key from the AAA-Key-Int taking then prior exchanged PAA-nonce and MN-nonce into computation. An integrity algorithm (Algorithm-ID) is determined by the nPAA that specifies a pseudo-random

function to be used for the derivation of the new-PANA-Auth-Key.

The nPAA sends a PAR to the MN signed by the new-PANA-Auth-Key with the complete bit set (c-bit) containing the new key id (new-Key-ID) and Algorithm-ID.

The MN computes AAA-Key-Int, new-AAA-Key and depending on Algorithm-ID new-PANA-Auth-Key which is used to check the integrity of the PAR. The MN completes the protocol run by sending a PAN signed by the new-PANA-Auth-Key with the complete bit set (c-bit) containing new-Key-ID.

#### IV. COMPARATIVE ANALYSIS

During the PANA pre-authentication phases, the AAA server in the new domain will contact the home AAA (hAAA) in the home domain. Generally, these interactions will generate a higher amount of required signalling (see Table 2). Furthermore if the signalling from the nVD to the HD of the MN has high latency, e.g. if the MN comes from foreign country or continent, the handover latency will considerably increase.

TABLE I  
COMPARISON BETWEEN PANA PRE-AUTHENTICATION AND PANA CXTTP

Principles	PANA Pre-Authentication	Inter-domain PANA CXTTP
make-before-break	Yes	Yes
cryptographic separation of current and new PANA session	Yes	Yes
signalling overhead to the home domain	Yes	No
SLA requirements between	nVD and HD	cVD and nVD

Table 1 compares principles in PANA pre-authentication and inter-domain PANA CXTTP. In both mechanisms use the make-before-break handover principle. Cryptographic separation of the PANA sessions in PANA CXTTP is explained in the technical description. In PANA pre-authentication the old PANA session key is dropped and a new key is negotiated. To determine that the MN is allowed to transfer the authentication context to nVD, the SLA between cVD and nVD is required. The idea is to get benefits of existing agreements between domains to enhance the inter-domain mobility of the users accessing these domains.

Table 2 presents the number of messages exchanged in both cases. As an example, in order to compare these mechanisms the EAP-TTLS method with EAP-MD5-Challenge [10] to authenticate the user in the nVD is considered. The benefit of using this method compared to other EAP methods is to have high security by identity protection and key derivation and minimum signalling overhead to home domain.

The links in Table 2 are categorised in low, medium and high latency. Low latency is expected between the MN and a PAA communicating direct over the radio interface. Medium latency is expected where the communication partners are

PAAAs in neighbouring domains. And we expect high latency in case of communication with the home domain.

TABLE 2  
MESSAGES EXCHANGES OF EAP-TTLS WITH EAP-MD5 CHALLENGE VS.  
INTER-DOMAIN PANA CXTP

expected latency	Link	PANA Pre-Authentication	Inter-domain PANA CXTP
low	PaC ↔ cPAA	-	1
	PaC ↔ nPAA	26	4
	cPAA ↔ cAAA	-	2
	nPAA ↔ nAAA	4	2
medium	cPAA ↔ nPAA	-	3
high	nAAA ↔ hAAA	4	-
<b>Overall messages</b>		<b>34</b>	<b>12</b>

Inter-domain PANA CXTP requires 12 messages as shown in Fig. 2. PANA re-authentication starts with 3 and completes with one message between PaC and nPAA. The common EAP-TTLS needs 7 messages for the TLS handshake and the EAP-MD5-Challenge needs two EAP-Identity and two EAP-MD5 messages transported in two PANA messages between PaC and nPAA respectively. EAP-Identity as well as EAP-MD5 forwards a message to the nAAA which forwards it to the hAAA server from where a response message is sent along the same way back. That adds up to 34 messages in total.

## V. CONCLUSIONS AND FUTURE WORK

This paper presented a new approach of fast re-authentication for inter-domain handover using context transfer. To achieve this, an extension of PANA with CXTP is embedded into an AAA infrastructure.

The trust check that is the determination of the SLA between adjacent domains is the base for transferring authentication context between domains. Context is only allowed to be transferred or received respectively if an adequate SLA exists.

The transferred context is secured by asymmetric encryption. The integrity and validity of the used public key is guaranteed by an AAA public key digital signature.

The PANA authentication context is an authentication key. The key of the current PANA session is cryptographically separated from the transferred key by taking PANA based values into computation. The key of the new PANA session is calculated using nonce values and therefore separated from the transferred key and the key of the current PANA session.

A successful inter-domain PANA CXTP authentication requires a fixed amount of messages, whereas the number of messages for PANA pre-authentication depends on the respective EAP method. In this paper EAP-TTLS is considered as it provides high level of security by means of mutual authentication and key derivation. As shown PANA pre-authentication requires a considerable higher number of messages compared to the proposed inter-domain PANA CXTP.

Next step is to evaluate inter-domain PANA CXTP performance compared with PANA pre-authentication. This evaluation will introduce a numerical simulation for both approaches. Other issues can be studied concerning context transfer time, robustness and overall performance in different scenarios.

The current approach is not considering dynamic established agreements between adjacent domains. Therefore one interesting alternative may be to adopt a mechanism to negotiate this issue. Furthermore, the trust check extension can be used to select an authentication procedure depending on the SLA level between domains. To increase the trustworthiness of inter-domain PANA CXTP the protocol must take compromised PAAAs into consideration.

## ACKNOWLEDGMENT

The work described in this paper is based on results of IST FP6 Integrated Project DAIDALOS. DAIDALOS receives research funding from the European Community's Sixth Framework Programme. Apart from this, the European Commission has no responsibility for the content of this paper. The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

## REFERENCES

- [1] 3GPP, "Handover Requirements between UTRAN and GERAN or other Radio Systems", Tech. spec., 3GPP TS 22.129 v.8.0.0, March 2006.
- [2] 3GPP, "Vocabulary for 3GPP Specifications", Tech. spec., 3GPP TS 21.905 v.8.0.0, March 2006.
- [3] J. Loughney, M. Nakhjiri, C. Perkins, and R. Koodli, "Context Transfer Protocol", Internet RFC 4067, July 2005.
- [4] IEEE, "IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation", IEEE standard 802.11F-2003, July 2003.
- [5] J. Boumelle et al., "Use of Context Transfer Protocol (CXTP) for PANA", Internet Draft, expired, draft-ietf-pana-cxtp-01, March 2006.
- [6] D. Forsberg et al., "Protocol for Carrying Authentication for Network Access (PANA)", Internet Draft, work in progress, draft-ietf-pana-pana-14, March 2007.
- [7] H. Wang, A. R. Prasad, and P. Schoo, "Research Issues for Fast Authentication in Inter-Domain Handover", in Proceedings of the 8th Wireless World Research Forum (WWRF), February 2004.
- [8] Y. Ohba, "Pre-authentication Support for PANA", IETF draft-ietf-pana-preauth-01, expired, March 2006.
- [9] D. Forsberg et al., "PANA Mobility Optimizations", IETF draft-ietf-pana-mobopt-01, expired, October 2005.
- [10] P. Funk et al., "EAP Tunneled TLS Authentication Protocol Version 0", IETF draft-funk-eap-ttls-v0-01, work in progress, April 2007.
- [11] <http://www.ietf.org/html.charters/OLD/seamoby-charter.html>
- [12] <http://www.ietf.org/html.charters/pana-charter.html>
- [13] H. Wang and A.R. Prasad, "Fast Authentication for Inter-domain Handover", Lecture Notes in Computer Science, Volume 3124, pages 973-982, Springer, 2004.
- [14] W. Y. Lee, H. Lee, "Evaluation of authentication interworking methods among multiple WLAN service providers", International Journal of Communication Systems, 20(5):515-531, 2007.
- [15] H. Levkowitz et al., "Extensible Authentication Protocol (EAP)", Internet RFC 3748, June 2004.