

# Performance Study of PANA Pre-authentication for Interdomain Handover

Patryk Chamuczynski, Omar Alfandi, Constantin Werner, Henrik Brosene, Dieter Hogrefe

*Telematics Group, University of Göttingen  
Lotzestrasse 16-18, 37083 Göttingen, Germany*

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

**Abstract**—To provide seamless mobility to the wireless user, a continuous connection to the Internet is required while moving from one administration domain to another. To enable continuous connectivity, one prerequisite is the incorporation of seamless handover. The *make-before-break* approach facilitates seamless handover by means of executing an authentication to a new domain simultaneously while maintaining connection to current domain. The connection is only terminated after the handover to the new domain is successfully completed.

However, the duration of the authentication is critical for the handover process because if the mobile nodes move very fast the remaining amount of time of connection to the current domain can become very limited. Therefore, it is a vital issue for seamless mobility to study the authentication performance of a pre-authentication framework.

In this paper we model an authentication infrastructure and consider a scenario in which a high number of nodes handover to a new administration domain. The simulation of the authentication process shows the relation between authentication performance and traffic intensity. Furthermore we identify some critical points and potential bottlenecks of this pre-authentication approach.

## I. INTRODUCTION

Due to the increasing performance and dropping prices of wireless local area networks (WLAN), a tremendous availability of access points can be observed within urban and rural areas. This delivers a completely new experience of personal mobility, ubiquitous connectivity to users, and provides the means for pervasive services. Furthermore, it reveals new business concepts as mobile operators can group together to deploy access points over wide areas and thus, enable complete network access coverage over the land. On the other side of the coin, this also raises many security and performance issues. To be able to offer pervasive services throughout networks to users, one of them is the fast and reliable authentication process of a roaming user. A user who roams from one access provider to another, with both having agreed to grant access to each others users, need to be authenticated and authorized quickly in order to provide seamless mobility.

Such authentication schemes are currently developed by IETF Protocol for Carrying Authentication for Network Access (PANA) [1] and Handover Keying (HOKEY) [2] working groups (WG). The PANA WG is working on a transport protocol for authenticating IP hosts for network access. In

addition, the WG proposed a framework to pre-authenticate a user who is currently connected to a domain to a new, candidate domain and thus, enabling seamless connectivity for roaming between adjacent domains. However, for all kinds of mobility, the time needed to pre-authenticate a user to a new domain is a critical issue and has not been evaluated yet.

In this paper, we show the result of exhaustive network simulation of the PANA pre-authentication framework, provide insights into the time requirements and scalability and pinpoint potential bottlenecks. We have simulated the mobility aspect of authentication, i.e. user coming to a new domain from another domain. The paper is organized as follows: in Section II, the related and relevant work for this paper is briefly introduced. In Section III, the technical details of the protocols framework are presented. It provides an overview of the involved entities and the basic communication sequence that takes place. It details and provides rationales for the scenario architecture that have been considered for simulation. Section IV introduces to the background of the simulation, presents the results of the performance simulation, discusses the findings, and identifies potential bottlenecks of the protocol framework. The final Section V summarizes this paper and provides an outlook for future work.

## II. RELATED WORK

The main security mechanism used in this paper is the well known Transport Layer Security (TLS) Protocol [3]. It is used to protect communication through the Internet and is the basis of the applied authentication method.

An authentication framework which supports multiple authentication methods is the Extensible Authentication Protocol (EAP) [4]. The primary purpose is network access control. A peer and a server authenticate each other through a third party known as the authenticator. After successful authentication network access is granted to the peer by the authenticator or an entity controlled by the authenticator. Server and peer agree on one specific authentication method, there are currently about 40 different methods based on shared secrets, certificates or any other authentication fundamentals. Depending on the method different security features like mutual authentication or protection of the peer identity are supported. EAP runs

directly over layer 2 protocol, such as point-to-point protocol, without requiring IP.

EAP fits in the Authentication, Authorisation and Accounting (AAA) infrastructure where several authenticators are connected to one AAA server. The most recent AAA protocol is DIAMETER. It consists of a base protocol [5] and a set of extensions including the DIAMETER EAP Application [6] to exchange EAP messages.

The EAP Tunneled TLS (TTLS) [7] Authentication Protocol has high security claims by mutual authentication and protection of the peer identity. Furthermore it provides a TTLS authentication server in between the authenticator and the EAP authentication server. That matches our architecture with local and home authentication server.

A layer 3 transport protocol for EAP is the Protocol for Carrying Authentication for Network Access (PANA) [8]. PANA is independent of the layer 2 protocol used and the AAA infrastructure that may reside on the network. 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).

The PANA framework only considers a local authentication scenario and there is no consideration for (fast) re-authentication in the handover case. The PANA WG proposed PANA pre-authentication [9] to overcome this limitation. While still being connected to the current domain, the pre-authentication for the new domain is executed in the background. The HOKEY WG discusses the pre-authentication problem too [10]. In contrast to PANA pre-authentication that is mainly an adjustment of the standard PANA authentication, HOKEY pre-authentication is defined as the utilization of EAP to pre-establish authentication information on an authenticator prior to arrival of the mobile node.

### III. TECHNICAL DESCRIPTION

In this section, the scenario architecture is described. In the architecture, a mobile node (MN) performs access authentication procedures by taking advantage of the PANA pre-authentication mechanism. So that the MN movement is between two access routers and both access routers belong to different domains. While still being connected to the current domain, the MN can start with authentication to a new domain and thus, be able to complete many of the handover related operations.

Pre-authentication can be classified into direct and indirect methods. In case of direct pre-authentication, the MN can communicate with new authenticator directly. In case of indirect pre-authentication, the current authenticator acts as a proxy. This paper considers direct pre-authentication which is appropriate to the simulated scenario, because it is the only method supported by PANA.

The architecture considers the PANA protocol that carries EAP messages between a PaC and a PAA in the access network. PANA uses UDP as transport protocol. Since UDP does not handle the message acknowledgement, this feature

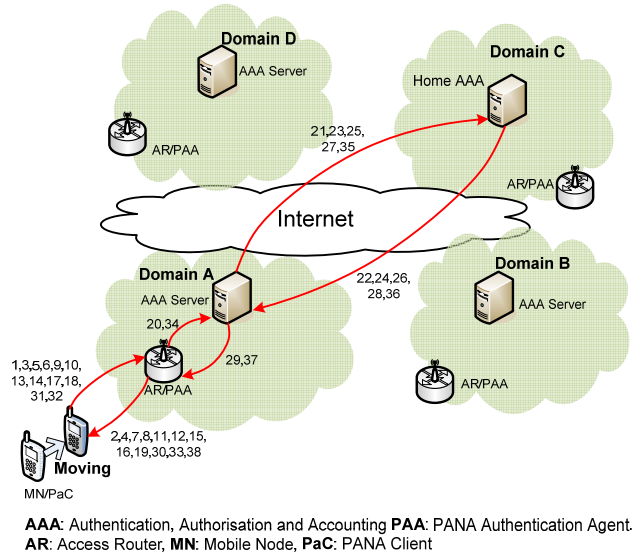


Fig. 1. Scenario Architecture

is provided by PANA. Each PANA Authentication Request message (PAR) is acknowledged by PANA Authentication Answer (PAA). PAA messages may be also used to carry EAP messages, however due to security reasons in our model we assume that this option is disabled. In this case Each PAR message transporting EAP message is acknowledged by empty PAA message.

The DIAMETER protocol is used to exchange EAP messages between PAA and local AAA server as well as between local AAA server and home AAA server. Not forgetting that across the Internet a TLS tunnel is established before transporting the EAP messages to secure the messages exchange.

Since the MN can move to any place, it is considered that the MN moves from any administration domain to any other domain. In this case, the problem is that the local AAA server in the new domain does not have the authentication information of the MN. For that reason the local AAA server has to contact the MNs home AAA server in order to receive the credentials to grant access to the MN in the new domain.

#### A. Scenario Architecture

For the simulation we have considered a scenario architecture comprising a number of administration domains which are connected to the Internet. The authentication components part of each domain is identical, that means each domain consist of an AAA server as a backend server and one or more than one PAA co-located with the access router (AR) as authenticator. The MN is also the client of the authentication process which is called PaC.

Fig. 1 shows the direct pre-authentication mechanism. Considered that, the MN discovers the basic information of the new domain. In particular it obtains the relevant information IP address of the new access router (nAR). Since the nPAA do co-exist with the nAR, the MN also obtains the address of nPAA as well.

The messages flow of the protocols used in this scenario is shown in Fig. 1. The numbers near the arrows represent messages. The pre-authentication is initiated by the mobile node by sending the PANA Client Initiation (PCI) message to the PAA in the new domain (message 1). After that, the EAP-TTLS process starts by exchanging messages between PaC and PAA (messages 2-19). The PAA contacts the local AAA server using DIAMETER EAP request (message 20). When the new domain is not home domain of the mobile node, local AAA server contacts its equivalent in the home domain of the mobile node. Otherwise this step may be skipped. To contact the home AAA, a TCP connection must be established between local AAA server and AAA server in the home domain of the mobile node (messages 21 and 22). This is necessary only when there is no existing TCP connection between these hosts (such a connection may be established, when authenticating other mobile node coming from the same domain). The security of the inter-AAA connection is guaranteed by the Transport Layer Security protocol (TLS). TLS requires 4-way handshake for establishing a secure connection (messages 23 to 26). However if such a connection already exists, or has been used recently TLS may be duplicated or re-established, respectively. In this case only two-way handshake is required. The DIAMETER message from local AAA to home AAA server is numbered as 27. The home AAA server sends a MD5 challenge to the mobile node, via the AAA server and PAA in the new domain (messages 28-30). The MD5 response is sent the same way, but in opposite direction (messages 32-35). Then the home AAA server sends the DIAMETER EAP Answer message to the PAA indicating whether the mobile node has been successfully authenticated (messages 36 and 37). This information is forwarded to the mobile node (message 38).

#### IV. SIMULATION

##### A. Framework

The PANA pre-authentication model was built using INET framework for OMNeT++ simulation environment. The INET framework for OMNeT++ contains definitions of many popular protocols (UDP, TCP, IPv4, IPv6, PPP) as well as models of basic network nodes (routers, hubs, access points etc.). That helped us focus on modelling authentication procedures without worrying about the underlying mechanisms.

##### B. Topology Assumptions

The simulated network has been modelled according to Fig. 1. The main elements that represent modelled infrastructure are domain and mobile node. Each domain contains one access router co-located with PANA agent (AR/PAA) and authentication server (AAA). We simulated network of 50 administration domains. All the domains have been indexed from 0 to 49. All mobile nodes try to authenticate to domain with index 0. They communicate with the same access router within this domain.

All data links are described by two parameters: data rate and propagation delay. For the mobile node access router link

we assumed data rate 10Mb per second. More accurate value was not possible, since there is no assumption regarding access technology. The propagation delay from mobile node to access router was assumed to be 5ms. The access router is directly connected with authentication server of the domain (AAA server). The propagation delay between these two nodes was chosen to be 10ms. This value was obtained after experiments with Ping application and a few servers in Germany. The data rate for AR/PAA AAA link was set to 100Mb/s.

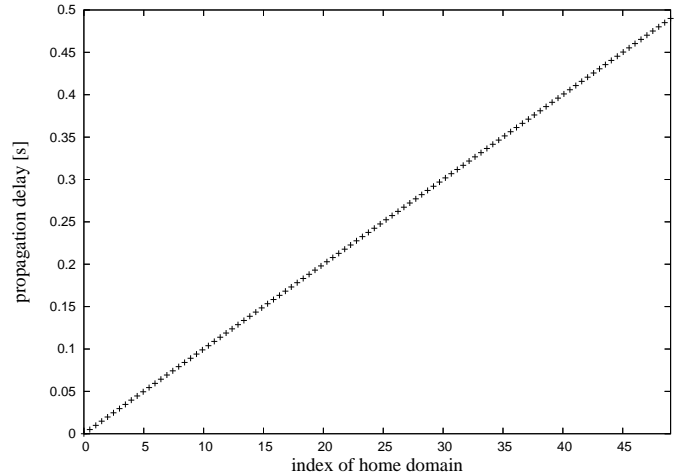


Fig. 2. Propagation delay to home domain

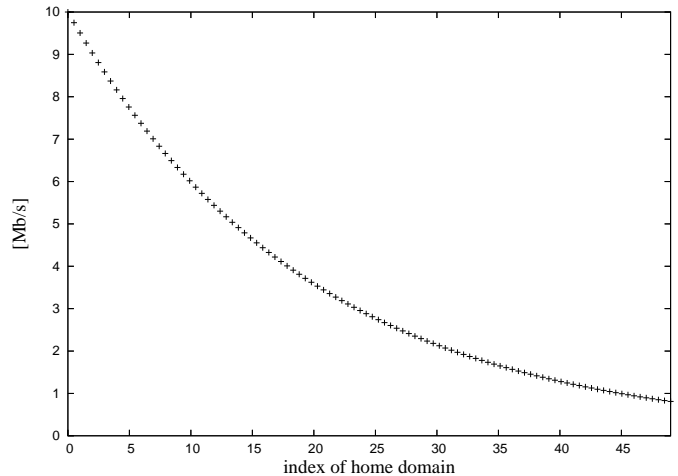


Fig. 3. Data rate of the link to home domain

The AAA server of domain 0 is directly connected with AAA servers in all domains. These links represent the Internet connection between domains. The propagation delay and data rate for the links are different for every connection. That is because domains are not in the same distance from each other and are connected with links of different quality. We assumed that the propagation delay between domains increases linearly according to formula:  $D_i = D_0 * i$ , where  $D_i$  is the propagation delay from domain 0 to domain  $i$ . For data rate

we assumed that it decreases exponentially with the distance. We considered that it is expressed by following formula:  $S_i = kS_{i-1} = kiS_1$ , where  $S_i$  is the data rate of the link from domain 0 to domain  $i$  and  $k$  is a constant between 0 and 1. We arbitrarily chose  $D_0 = 10ms$ ,  $S_1 = 10Mb/s$  and  $k = 0.95$ .

The parameters of inter-domain links that were used in the simulation are depicted in the Fig. 2 and Fig. 3.

We assumed no processing delay and unlimited output queues for the network interface in all network nodes.

### C. Mobility And Traffic Characteristics

Our simulation concerns mobile nodes that move into a single domain. The mobile nodes are assigned to different home domains and request authentication at different moment.

The home domain and the instant of initializing the authentication are randomly chosen for each mobile node. The distribution of nodes' home domains must reflect the fact that most of the authenticating nodes come from close domains, including nodes that home domain is the domain that they are trying to authenticate to (they are coming back to their home domain). We assume that the home domain of the nodes is distributed according to normal distribution with mean value 0. The probability density function of normal distribution is expressed by following formula:

$$PDF(x, \sigma, \mu) = \frac{1}{\sigma\sqrt{2\pi}} \cdot e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

The value of  $\sigma$  parameter should be chosen to get realistic coverage of home domains. If it is too small, then only the domains that are close to domain with index 0 will be covered. Big  $\sigma$  will cause that all domains will be covered with similar probability, which is not realistic scenario. The  $\sigma$  should depend on the number of domains that we simulated. The value of the  $\sigma$  parameter chosen for the simulation was 10. Mobile nodes pick random value according to this distribution and take the integral part of its absolute value as home domain. The probability of having by node the home domain with index  $i$  is expressed by following formula:

$$P(i) = 2 \int_i^{i+1} PDF(x, 0, 10)$$

The probability of choosing home domain by nodes can be seen in the Fig. 4.

The instant of pre-authentication process initialization for a mobile node is determined by a traffic intensity. According to [11] nodes arrivals form the Poisson process. In this case the probability density for instant of new request is described by the exponential function:

$$PDF(t - t_0, \lambda) = \lambda \cdot e^{-\lambda(t-t_0)}$$

where  $t$  is an instant of new incoming request and  $t_0$  the instant of the previous request. The expected value of interval between requests equals  $\lambda^{-1}$ , so the traffic intensity expressed in number of requests per second equals  $\lambda$ .

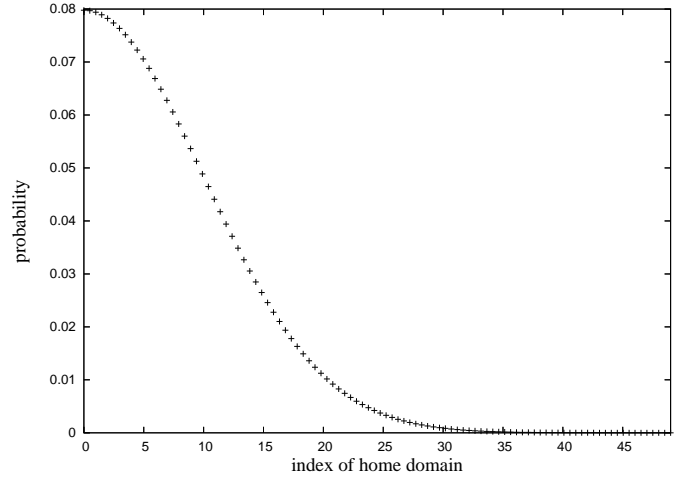


Fig. 4. Probability for mobile node to have home domain with given index

### D. Simulation Results and Discussions

We simulated the modelled network with authentication requests sent by mobile nodes coming with different intensity. Each simulation run was performed with  $\lambda$  incremented by one comparing to the previous run. We started from  $\lambda = 1$  and performed 100 simulation runs, so we tested the network with traffic intensity from 1 to 100 requests per second. For all runs we set the simulation time to 120 (simulated) seconds. The output that we were interested in was the duration of the authentication process and traffic that was generated on several links. Fig. 5 presents the results for duration of the pre-authentication in function of distance to nodes home domain. Picture shows average results and values obtained for an exemplary simulation run, with traffic intensity of 40 mobile nodes per second requesting pre-authentication.

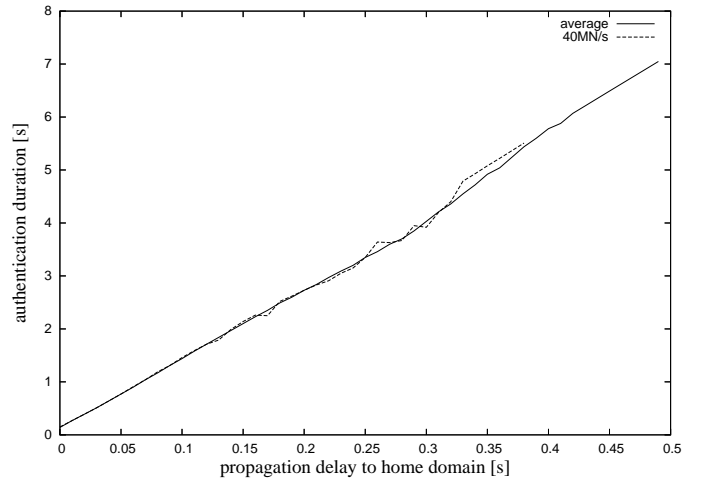


Fig. 5. Duration of authentication process

The simulation showed us that the busiest link is the link between the PANA agent and authentication server in the visited domain. The Fig. 6 shows the traffic generated on this

link in both directions for different intensity of authentication requests.

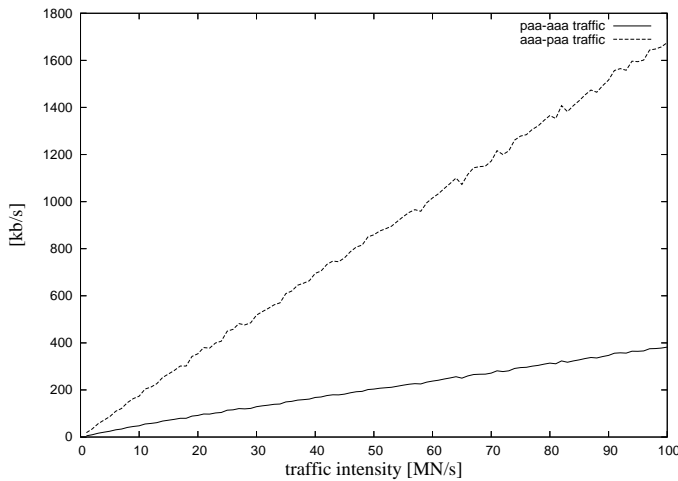


Fig. 6. Traffic generated by mobile nodes requesting authentication

The main results of our simulation concern the latency of the pre-authentication process and the scalability of the solution. The latency depends mostly on the distance between a new domain and home domain of the pre-authenticating user. The scalability is related to the level of signalling traffic generated for the purpose of pre-authentication of mobile node. The level of this traffic is low enough to allow implementing the solution in environment with any traffic characteristics.

## V. CONCLUSIONS AND FUTURE WORK

In this paper we studied the performance issue of the PANA pre-authentication as a step towards the solution for seamless mobility.

In this aspect we investigated the overall duration of the pre-authentication process and the scalability issue of the solution. The signalling traffic generated by pre-authenticating mobile nodes depends on the intensity of requests. Our simulation showed that this relation has a linear trend. The busiest link is the link between PANA authentication agent and authentication server in the visited domain. This link concentrates all the signalling traffic that is later split and forwarded by the AAA server to all domains. However, even on this link the level of generated traffic should not be difficult to handle. The traffic intensity necessary to generate signalling traffic of the 1Mb/s equals about 50 mobile nodes per second. This means daily traffic of over 4 millions mobile nodes coming to a single domain.

The duration of the pre-authentication phase of the handover depends mostly of the distance between the visited domain and the home domain of the pre-authenticating mobile node. As it has been showed by the simulation, the relation between the propagation delay to users home domain and the pre-authentication duration is linear. For users that have far home domain the pre-authentication process may last several seconds.

In the nearest future we plan to confirm our results by performing measurements in real environment, using existing implementation of PANA/DIAMETER framework. This implementation has been made by the Open Diameter project and is freely available under the GNU Public License.

The necessity of contacting users home domain for authentication seems to be the biggest threat for assuring seamless mobility between domains. Therefore our future plans concern also developing a method that allows pre-authenticating user without necessity of time-costly communication with its home domain.

## ACKNOWLEDGEMENTS

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] The PANA working group homepage. [Online]. Available: <http://www.ietf.org/html.charters/pana-charter.html>
- [2] The HOKEY working group homepage. [Online]. Available: <http://www.ietf.org/html.charters/hokey-charter.html>
- [3] T. Dierks and E. Rescorla, "The transport layer security (TLS) protocol," Internet RFC, 2006.
- [4] H. Levkowitz *et al.*, "Extensible authentication protocol (EAP)," Internet RFC, 2004.
- [5] P. Calhoun *et al.*, "Diameter base protocol," Internet RFC 3588, 2003.
- [6] P. Eronen *et al.*, "Diameter extensible authentication protocol (EAP) application," Internet RFC 4072, 2005.
- [7] P. Funk *et al.*, "EAP tunneled TLS authentication protocol version 0," IETF draft, 2007.
- [8] D. Forsberg *et al.*, "Protocol for carrying authentication for network access (PANA)," IETF draft, 2007.
- [9] Y. Ohba, "Pre-authentication support for PANA," IETF draft, 2006.
- [10] —, "EAP pre-authentication problem statement," IETF draft, 2007.
- [11] A. Erlang, "Solution of some problems in the theory of probabilities of significance in automatic telephone exchanges," in *The life and works of A.K. Erlang*, E. Brockmeyer, H. Halstrom, and A. Jensen, Eds., 1948.