Modelling the Impact of Virtual Identities on Communication Infrastructures

Marc Barisch
Institute of Communication Networks and Computer Engineering
Universität Stuttgart
Pfaffenwaldring 47
70569 Stuttgart, Germany
marc.barisch@ikr.uni-stuttgart.de

ABSTRACT

The virtual identity concept has been introduced to protect the user's privacy towards service providers as well as towards access network providers on a service session basis. So far the concept has been only considered from the security and privacy perspective. However, performance analysis is necessary as well to gain insights into the additional costs and their scaling behavior with respect to signaling load and state management. In this paper we propose an analytical model to evaluate the cost introduced by virtual identities. The model allows to quantify the additional signaling overhead and the additional states created by distributing service sessions of users across several virtual identities. We exemplify the use of the model for an authentication, authorization and accounting (AAA) infrastructure based on EAP-TLS [22] and derive figures on the required signaling bandwidth and state overhead to support the virtual identity concept in various service usage scenarios.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection; C.4 [**Computer Systems Organization**]: Performance of Systems—*Modeling techniques, Design studies*

General Terms

Performance, Security

Keywords

Identity management, virtual identities, authentication load, AAA performance

1. INTRODUCTION

Users rely more and more on information and communication technology (ICT) to accomplish their daily life. A multitude of services and applications offered by various service providers (SP) are used for business as well as for private purposes. Normally, SPs require users to create an account for each offered service implying the provision of personal data, like name or email address, to the SP. This results in more and more personal data that is processed and stored by ICT systems and imposes several privacy threats towards the user.

SPs can create detailed user profiles based on the released personal data and based on information that is inherent to today's Internet-based communication, like the IP address. The IP address can be used to get information about the user's access network provider and about the location of the user [17]. As long as the same IP address is used for different accounts at the same time, a SP is in the position to link them. In addition it is possible that two SPs collaborate and merge their user profiles in order to derive additional information.

Additionally, access network providers can create very detailed user profiles based on the transported traffic. They are in the position to trace which SPs have been used and can gain additional insights inspecting unencrypted traffic itself. This imposes a severe privacy threat to users, since it requires that access network providers are trustworthy.

The virtual identity (VID) concept [21] is one approach that mitigates the above introduced threats. A user has several VIDs, which can be used for service consumption. Each VID consists only of a subset of all user attributes. In addition, each VID has its own IP address, which prevents that VIDs can be linked based on network layer identifiers. That means, an untrusted access network provider perceives several virtual identities instead of one user with one IP address , which makes the creation of user profiles more difficult. Further improvements towards unlinkability require that the physical layer does not reveal more information, e.g. that the signal strength cannot be used to link different identities.

So far, research on the VID concept focussed mainly on improving the user privacy and security on the network and application layer. However, if the concept is applied in networks and service platformsm the performance impact and thus the costs of the VID concept have to be evaluated. In particular the approach to split the user identity into different VIDs is not for free, because it has to be maintained across all layers and across all protocols. For example, each virtual identity must be authenticated and periodically reauthenticated towards the access network provider independent of the others. The same holds with respect to mobility

DIM'09, November 13, 2009, Chicago, Illinois, USA.

management, i.e. mobility updates and handovers have to take place for each VID. Therefore, it is obvious that such an approach creates additional signaling and state management overhead.

This paper examines analytically the additional overhead introduced by the VID concept based on a theoretical model and exemplifies the implications for a federated authentication, authorization, and accounting (AAA) infrastructure using EAP-TLS authentication.

The remainder of this paper is structured as follows. Section 2 introduces related work in the areas of virtual identities and traffic models. Next, Section 3 elaborates the model that is used for the performance evaluation in Section 4. Finally, Section 5 concludes this paper.

2. RELATED WORK

Since this paper examines the performance impact of the virtual identity concept, we first introduce related work on virtual identities in Section 2.1. Afterwards, we present in Section 2.2 an overview on traffic models that characterize the service consumption behavior of individual users.

2.1 Virtual Identities

With the VID concept a user can split his digital identity into several virtual identites. The concept of VIDs is in literature also known as partial identities. [18] defines a partial identity as an identity that reflects a user in a specific role by means of pseudonyms and user attributeds linked to it. A partial identity contains only a subset of all user attributes. Thus, partial identities can be designed in way for data minimization and privacy protection on the application layer. To provide unlinkability on the network layer, network anonymization techniques are applied [8].

Our model follows closely the VID concept followed by the EU project Daidalos [21]. In this model the user identity is not only partitioned on the application layer, but also on the network layer. Each VID has its own IP address within a separated network stack [15] running on the user terminal to preserve the privacy of a user on the application layer as well as on the network layer. As a consequence each virtual identity has to be authenticated against the network provider independent of the other VIDs a user has. Therefore, additional signaling load is created on various networking subsystems.

To the best of our knowledge, partial and virtual identity concepts have been solely considered from the security and privacy perspective [13, 9]. The implications on existing communication infrastructures with respect to the additional overhead have not been explored so far.

2.2 Traffic Models

In order to analyze the additional overhead imposed by the VID concept, a user and his service consumption behavior needs to be statistically characterized. In literature various proposals for traffic models, which are also known as work load models, exist that describe the load exposed to systems [10, 19, 16, 6].

From telecommunication research it is known that in simple cases the number of calls per time interval can be described by a Poisson process [11], i.e. the time between two successive calls is negative exponentially distributed. The corresponding call holding time can also be described by a negative exponential distribution [12].

With the advent of the Internet, new services like telnet, electronic mail and file transfer had to be characterized. [7] shows that the interarrival of such service sessions can be modelled by means of negative exponential distributions, whereas the holding time can be modelled by a log-normal distribution.

A lot of research focused on the characterization of HTTP traffic [19, 6]. In [19] it is shown that HTTP sessions can be characterized by means of negative exponential distributions. A generalized approach are hierarchical workload models as proposed in [16]. They differentiate between session layer, function layer, and request layer. In scope of the paper only the session layer is relevant, because it models the different service sessions of users.

The above presented traffic models focus on the traffic observed by system components and cumulate several users. To the best of our knowledge no work exists that provides more details about the individual service consumption behavior of users. In particular for future pervasive systems the users' behavior cannot be foreseen and gets influenced by the introduction of the VID concept. Therefore, we model in Section 3.3 the interarrival time and the service holding time by means of negative exponential distributions as a first approximation.

3. IDM SYSTEM MODEL

We first provide an overview on the assumed identity management (IdM) system model. Afterwards, the work flow to consume a service is presented in Section 3.2. Finally, we describe in Section 3.3 the service consumption model based on the results from Section 2.2.

3.1 Overview

Figure 1 provides an overview on the assumed identity management system model. A user has a number of VIDs that are provided by an identity provider (IdP) based on a contract. Each virtual identity is represented on the network layer by means of an IP address and a corresponding L2 identifier, e.g. a VID specific MAC address [15]. The access network provider assigns IP addresses to the VIDs based on successful authentication against the IdP. That means for every VID that is in use, a separate authentication procedure has to take place. This is typically achieved by a set of protocols like EAP [3], 802.1X [1] and RADIUS [20] and a federated identity management infrastructure. Figure 1 exemplifies a representative configuration for such an infrastructure that consists of the supplicant in the user terminal, the authenticator residing in the access point or access router and set of interconnected authentication, authentication and authorization (AAA) servers. In the following we refer to all these components as AAA infrastructure.

A user can select each of his VIDs for consuming services provided by various service provider (SP). The SP trusts the IdP regarding successful authentication (Single Sign-On). In consequence, an access network provider as well as a service provider cannot easily link different virtual identities belonging to the same user neither based on network identifiers nor on application layer identifiers and attributes.

The number of VIDs that a user should have is governed by two conflicting factors: privacy versus cost and performance. From a privacy point of view the number of virtual identities should be large in order to have an optimized identity for the given context. This allows for data minimization

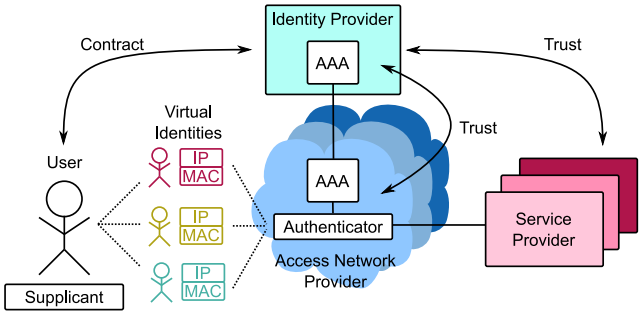

Figure 1: System model overview

and reduces the probability of linking two different VIDs. In the extreme case a VID is used exactly once for service consumption.

On the other hand the number of VIDs per user has a direct impact on the capital and operational expenditures of the access network provider and of the IdP. If a user can have several identities active in parallel, the authentication and periodic reauthentication signaling load as well as the amount of state information within network components are increased. Therefore, additional infrastructure is needed to support the virtual identity concept.

3.2 Work Flow

Given the user's intention to use a selected service we can divide the workflow into two phases [4]: the service preparation phase and the service consumption phase. The service preparation phase consists of at least two steps.

First, the user has to select one out of his N_{VID} VIDs to consume the service. The selection of VIDs should adhere to privacy considerations based on privacy policies.

Second, the selected VID needs to be potentially activated depending on the current state. Either the VID is already used in other service sessions, i.e. the VID is active and no activation is required, or the VID is not active and needs to be activated. Activation entails to authenticate against the access network and the IdP through additional signaling messages.

If the last service session that is using a specific VID terminates, the VID is deactivated. That means the VID is disassociated from the access network and from the IdP. For future use it needs to be reactivated. Basically, it is possible to keep VIDs active without service sessions. However, this affects among others the interaction with mobility protocols and is subject for future studies.

3.3 Service Consumption Model

The service consumption model shown in Figure 2 details the first phase of the work flow introduced in Section 3.2 for an individual user. The model supports m different service classes. Each service class i models a set of services that have independent identical service holding time distributions and their interarrival behaviour follow the same independent interarrival time distribution.

The interarrival time distribution characterizes the time between two service session requests (mean: d_i), whereas the service holding time distribution describes how long the service is consumed (mean: h_i). With the assumption from Section 2.2 that interarrival times and service holding times

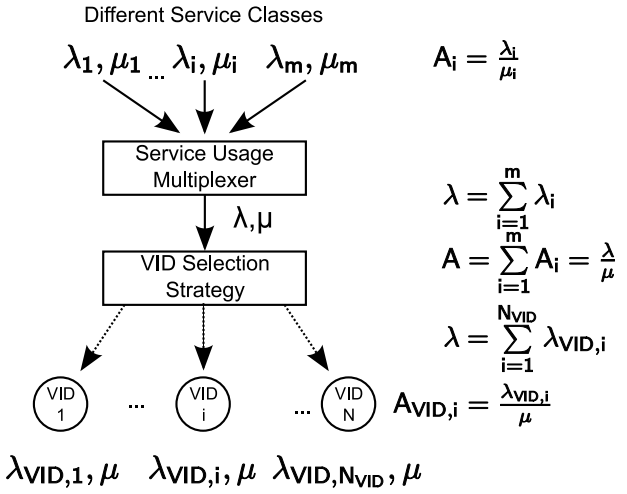

Figure 2: Service Consumption Model

are negative-exponentially distributed, we can characterize the distributions by the mean interarrival rate $\lambda_i = 1/d_i$ and the mean termination rate $\mu_i = 1/h_i$.

With the "Law of the Conservation of Flow" [14] the superposition of all service sessions in the service usage multiplexer leads to a negative exponential distributed interarrival time with with a mean interarrival rate of $\lambda = \sum_{i=0}^{m} \lambda_i$. In contrast, the superposition of all termination rates results in a more complex distribution. For simplicity we assume as an approximation that $\mu = 1/\sum_{i=1}^{m} \frac{\lambda_i}{\lambda} h_i$ is negative exponential distributed.

Finally, service session requests have to be splitted on one of the user's N_{VID} VIDs. Due to the lack of statistical data on VID selection and for simplicity, we assume a discrete uniform distribution across all N_{VID}. Based on [14] we obtain that $\lambda_{VID_i} = \frac{\lambda}{N_{VID}}$.

Further, we assume that the VID concept has no influence on the service consumption behavior of users. That means the load $A = \lambda/\mu$ resulting from the superposition of all service classes does not depend on N_{VID}. The load characterizes the mean number of service session that a user simultaneously has.

4. PERFORMANCE EVALUATION

Based on the in Section 3.3 introduced service consumption model, we are in the position to quantify the overhead introduced by the VID concept. We introduce the used key metrics followed by a mathematical model based on Markov chains and apply the results on the in Section 3.1 introduced system model.

4.1 Metrics

We selected three key metrics for the quantification of the performance impact caused by the VID concept:

- *VID activation rate:* The mean VID activation rate AR quantifies how often VIDs are activated per time unit. It is used to determine the signaling overhead caused by the activation of VIDs. In accordance to AR we can define a VID deactivation rate. Since we

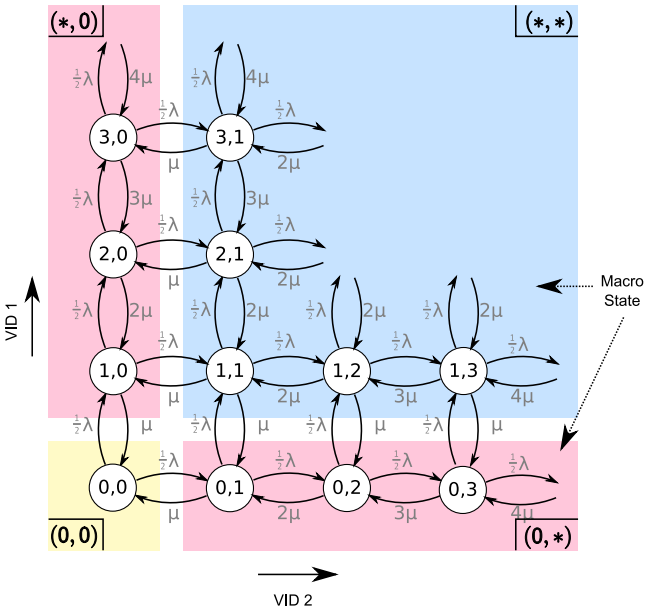

Figure 3: Mathematical Model for 2 VIDs

assume a stationary system, which means that the obtained results are independent of the particular instant of observation, the mean VID deactivation rate has to be the same as AR.

- *Authentication load:* The authentication components (authenticator, AAA server) are only involved during the VID activation. Therefore, the authentication load A_{Auth} is significantly lower than A and can be obtained by multiplying AR with a factor h_{Auth}.

- *Mean number of active VIDs:* The mean number of active VIDs $E[N_{act}]$ gives the average number of VIDs that are simultaneously active. $E[N_{act}]$ can be used to quantify the additional state that has to be managed by network components and the signaling for reauthentication.

4.2 Mathematical Model

4.2.1 Overview

The above introduced user model can be described in an analytical way by means of infinite n-dimensional Markov chains. The number of required dimensions is N_{VID}. Figure 3 illustrates the necessary states and the corresponding transitions for the case of $N_{VID} = 2$.

Each state $X(t) = (x_1, \ldots, x_i, \ldots, x_{N_{VID}})$ describes the number of active service sessions x_i per VID i at time t. The system state transits during an infinitesimal small time interval dt into a state $X(t+dt) = (x_1, \ldots, x_i+1, \ldots, x_{N_{VID}})$ with a rate $\lambda_{VID,i} = \lambda/N_{VID}$, i.e. a newly initiated service session uses VID i. A transition into state $X(t+dt) = (x_1, \ldots, x_i - 1, \ldots, x_{N_{VID}})$ takes place with rate $x_i \cdot \mu$, if one of the x_i service sessions using VID i terminates.

From the Markov chain model and based on the BCMP theorem [5], we obtain the probability to be in state:

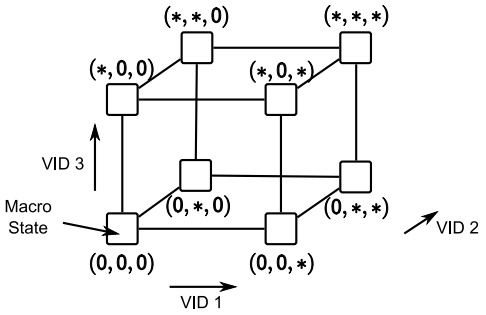

Figure 4: Macro States for $N_{VID} = 3$

$$p(x_1, x_2, \ldots, x_{N_{VID}}) = p(0, \ldots, 0) \frac{(\frac{A}{N_{VID}})^{x_1+x_2+\ldots+x_{N_{VID}}}}{x_1! \cdot x_2! \cdot \ldots \cdot x_{N_{VID}}!} \quad (1)$$

$$p(0, \ldots, 0) = \frac{1}{e^A} \quad (2)$$

4.2.2 VID Activation Rate

A VID is only activated if it is not used in a prior service session. That means only transitions from $X(t) = (x_1, \ldots, 0, \ldots, x_{N_{VID}})$ to $X(t+dt) = (x_1, \ldots, 1, \ldots, x_{N_{VID}})$ are of interest. In consequence we can group all states in one of $2^{N_{VID}}$ different macro states, in which the same VIDs are active or inactive independent of the number of service sessions per VID. Whether a VID is active is illustrated in Figure 4 by the $*$ symbol for the case of $N_{VID} = 3$, i.e. $x_i > 0$. The edges between the macro states represent VID activation events that are used to calculate AR in combination with the probability to be in one of the macro states.

Due to the symmetry of the macro states, only the number of active VIDs N_{act} per macro state matters for the propability calculation. The probability $p_{1,VID}$ to be in one macro state in which exactly one VID is active can be calculated as:

$$\begin{aligned} p_{1,VID} &= p(*, 0, \ldots, 0) = p(0, \ldots, *, \ldots, 0) \\ &= \frac{1}{e^A} \sum_{i=1}^{\infty} \frac{\frac{A}{N_{VID}}^i}{i!} \\ &= \frac{1}{e^A} \left(e^{\frac{A}{N_{VID}}} - 1 \right) \end{aligned} \quad (3)$$

For the following calculations we have to take into account all macro states in which one VID is active.

$$P(N_{act} = 1) = \binom{N_{VID}}{1} p_{1,VID} \quad (4)$$

This can be generalized for k VIDs:

$$p_{k,VID} = p(\underbrace{*, \ldots, *}_{k}, 0, \ldots, 0) = \frac{1}{e^A} \cdot (e^{\frac{A}{N_{VID}}} - 1)^k \quad (5)$$

$$\begin{aligned} P(N_{act} = k) &= \binom{N_{VID}}{k} p_{k,VID} \\ &= \binom{N_{VID}}{k} \frac{1}{e^A} (e^{\frac{A}{N_{VID}}} - 1)^k \end{aligned} \quad (6)$$

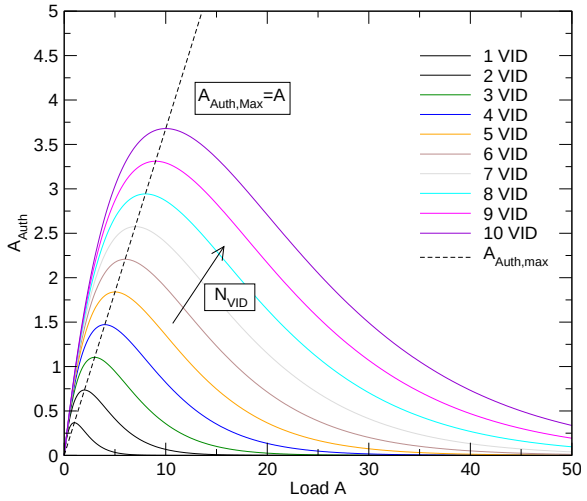

Figure 5: Authentication Load

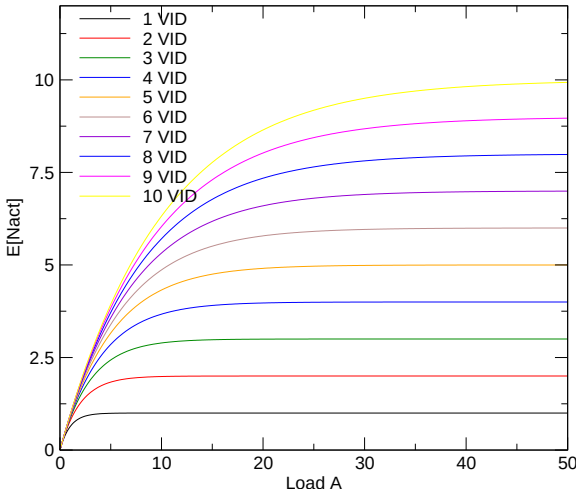

Figure 6: Mean number of active VIDs

With (7), we can calculate AR by taking all transitions between the macro states into account. The transition rate from a state with k active VIDs to a state with $k+1$ VIDs is $\frac{N_{VID}-k}{N_{VID}}\lambda$.

$$AR = \sum_{i=0}^{N_{VID}-1} \frac{N_{VID}-i}{N_{VID}}\lambda \cdot P(N_{act}=i) \quad (7)$$
$$= \frac{A \cdot \mu}{e^{\frac{A}{N_{VID}}}}$$

4.2.3 Authentication Load

(8) indicates that the VID activation rate AR depends on the load and the mean service termination rate, i.e. the longer the service holding time, the smaller the activation rate. To reflect the actual authentication load A_{Auth} we introduce $h_{Auth} = \mu$ and obtain

$$A_{Auth} = AR \cdot h_{Auth} = \frac{AR}{\mu} = \frac{A}{e^{\frac{A}{N_{VID}}}} \quad (8)$$

Figure 5 shows the effect of the number of VIDs on A_{Auth} in dependence of the load A. We can distinguish two different effects. For low load situations, the probability is high that a new service session triggers the activation of a VID, i.e. A_{Auth} is high. On the other hand, the higher the load A the higher the probability that the selected VID is already active, which means that no VID activation takes place.

We obtain a maximum authentication load $A_{Auth,max}$ on the authentication components for $A = N_{VID}$

$$A_{Auth,max} = N_{VID} \cdot e^{-1} \quad (9)$$

4.2.4 Mean number of active VIDs

From (5) we can derive the the mean number of active VIDs in dependence of the offered load A.

$$E[N_{act}] = \sum_{k=0}^{N_{VID}} k \cdot P(N_{act}=k) \quad (10)$$
$$= N_{VID}\left(1 - e^{-\frac{A}{N_{VID}}}\right)$$

Figure 6 presents the mean number of active VIDs $E[N_{act}]$ in dependence of the load A. We perceive that for low load values the number of VIDs N_{VID} has not a tremendous effect, i.e. it does not matter whether a user 3 or 10 VIDs. Low load values mean that the number of simultaneous service sessions is lower than the number of available VIDs.

In contrast, for high load situations (11) converges to N_{VID}, i.e. all VIDs are active. Therefore, the overhead caused by the VID concept is the same as if the number of user is multiplied by N_{VID}.

4.3 Impact on AAA infrastructure

In the following we illustrate the application of this model for the initial architecture depicted in Figure 1 and will focus on the signaling bandwidth needed at the AAA servers. We assume that the processing capacity of the AAA server does not limit the performance. As stated in [2], a RADIUS-based AAA server is capable of several 1000 requests per second.

At first, we introduce the used protocols for the given scenario in Section 4.3.1. Afterwards, more details on the assumed scenario are provided in Section 4.3.2 followed by the presentation of the results in Section 4.3.3.

4.3.1 Used Protocols

We assume that each VID is authenticated against the access network provider by means of EAP-TLS [22], i.e. every VID has an associated certificate. The authenticator exchanges the EAP messages with the AAA server of the access network provider, which in turn forwards the messages to the identity provider as shown in Figure 7. The EAP messages between the authenticator and the AAA server and between the AAA servers are encapsulated in RADIUS [20] messages. Table 1 gives the correspondig message sizes that have been measured in an example scenario. The given values reflect the size of the exchanged IP packets if not stated otherwise.

Given the assumption that the maximum transmission unit of the underlying communication channel is limited (e.g. 1500), larger messages will be fragmented. Message number 4 will be fragmented into three EAP messages, because it contains a certificate chain consisting of three certificates

Table 1: Assumed message sizes

No	Message Type	Length
0	EAP Request Identity	5 Byte[1]
1	EAP Response Identity	62 Byte[2]
2	EAP Request Start TLS	58 Byte[2]
3	Client Hello	155 Byte[2]
4	Server Hello	3938 Byte ($3 \cdot 1312$ Byte[2])
5	Client Finish	1022 Byte[2]
6	Server Finish	79 Byte[2]
7	EAP Response	58 Byte[2]
8	EAP Success	52 Bytes[2]

Table 2: Different User types

User type	N_{VID}	A per user	$1/\mu$
Ordinary User	1	1	1h
Privacy Aware User	10	1	1h
Pervasive User	1	10	360s
Privacy Aware Pervasive User	10	10	360s

that allow to authenticate the A4C server. Each of the EAP messages will be acknowledged, which is not shown in Figure 7, to cope with unreliable transmission channels.

4.3.2 Scenario

In order to get additional knowledge on the consequences caused by the VID concept, we compare four different user behaviors and calculate the imposed bandwidth requirements and the state overhead on the AAA servers.

- **Ordinary User:** An ordinary user has only one VID and uses this VID for all of his service sessions. We assume that the he activates his VID once a hour.
- **Privacy Aware User:** A privacy aware user has the same service consumption behavior as an ordinary user, but distributes his service sessions across 10 VIDs.
- **Pervasive User:** The pervasive user consumes much more services, i.e. higher load, than the ordinary user. He is not privacy aware and has only one VID.
- **Privacy Aware Pervasive User:** The privacy aware pervasive user is the most powerful user. He makes use of all of his 10 VIDs to protect his privacy and consumes a lot of services.

Table 2 provides an overview on the four different user behaviors.

4.3.3 Results

From Table 1 we can derive that one VID activation requires 1297 bytes in downstream direction and 4087 bytes in upstream direction. Since the upstream direction is dominating, we focus on it and use (11) to estimate the imposed bandwidth requirements on the AAA servers for N_{User} users connected to the platform.

$$BW_{up} = AR \cdot N_{User} \cdot 4087byte \tag{11}$$

Regarding the additional state overhead, we introduce the total amount of active users $N_{tot,act}$ in (12).

$$E_{N_{tot,act}} = N_{User} \cdot E[N_{act}] \tag{12}$$

Table 3 contains the results for $N_{User} = 1,000,000$. If an operator supports 10 virtual identities for ordinary users the bandwidth requirements on his AAA servers are increased by a factor of approximately 2.5. The total amount of active users is increased 1.5 times.

In case of pervasive users the requirements on the AAA infrastructure are decreased. Since, the user is almost always authenticated to the platform, the bandwidth requirements are very low. This is also reflected in the total amount of active users.

In particular interesting is the impact of virtual identities for pervasive users, i.e. privacy aware pervasive users. Due to the fact that the service sessions are now distributed on 10 different identities, the bandwidth requirements are increased by several orders of magnitude.

In consequence an identity provider has to know the user traffic models to quantify the impact of virtual identites on his infrastructure as well as on the infrastructure of access network operators.

Regarding the number of states that have to be maintained by network components, we have to cope with 10-times the number of states compared between pervasive users and ordinary users. The privacy-aware user causes only 2.6-times the number of states compared to the ordinary user.

Table 3: Overview on required bandwidth and total active users for $N_{User} = 1,000,000$

User-type	BW_{up} $[MByte/s]$	$E[N_{tot,act}]$
Ordinary User	0.4176	632121
Privacy Aware User	1.0272	951626
Pervasive User	0.0005	999955
Privacy Aware Pervasive User	41.7645	6321206

5. CONCLUSION AND OUTLOOK

The introduced mathematical model based on Markov chains allows the quantification of the performance impact caused by the virtual identity concept, which has been targeted to increase the security and privacy of users. We are in the position to determine how often VIDs are activated and how many VIDs are active at the same time. This allows the quantification of the created signaling traffic and supports the dimensioning of network components to cope with additional state caused by the identity partitioning approach. We exemplified the use of the proposed model for an AAA infrastructure and perceived a significant increase of signaling traffic compared to the model without virtual identities.

Even if we are not in the position to forecast the user behavior in the future, we have a measure that allows us to evaluate various scenarios in order to support the dimensioning of the infrastructure. Moreover, the model can serve

[1]Only EAP message size considered

[2]Measured at the AAA server, including RADIUS header, UDP header and IP header

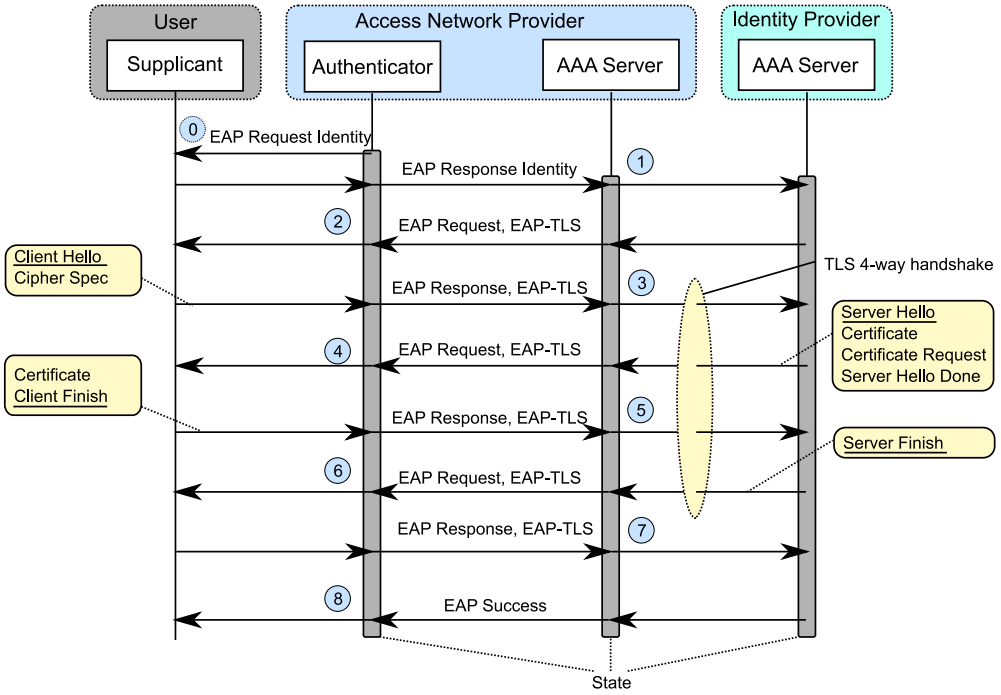

Figure 7: Authentication based on EAP-TLS

as a foundation to answer exceeding questions. For example, the impact of the user mobility on the VID concept is not yet explored and will subject of future work to estimate the consequences on the signaling infrastructure as well as on user's privacy.

6. ACKNOWLEDGEMENTS

This work was supported in part by the Daidalos project and in part by the SWIFT project. Both projects are funded by the European Union Framework Programme 6 and 7, respectively. The authors thank Andreas Reifert for valuable comments and stimulating discussions.

7. REFERENCES

[1] 802.1x Port-Based Network Access Ccontrol, 2004, IEEE Standard.

[2] Freeradius Performance Indications. http://freeradius.org/features/fast.html, 2009.

[3] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz. Extensible Authentication Protocol (EAP). RFC 3748 (Proposed Standard), June 2004.

[4] M. Barisch, M. Neubauer, J. Pagaime, J. Girao, and R. L. Aguiar. Privacy and Identity Management in a Layered Pervasive Service Platform. In *Proceedings of ICT Mobile Summit*, 2008.

[5] F. Baskett, K. M. Chandy, R. R. Muntz, and F. G. Palacios. Open, Closed, and Mixed Networks of Queues with Different Classes of Customers. *J. ACM*, 22(2):248–260, 1975.

[6] E. Casilari, F. Gonzblez, and F. Sandoval. Modeling of HTTP Traffic. *Communications Letters, IEEE*, 5(6):272–274, Jun 2001.

[7] R. Chinchilla, J. Hoag, D. Koonce, H. Kruse, S. Ostermann, and Y. Wang. Characterization of Internet Traffic and User Classification: Foundations for the Next Generation of Network Emulation. In *Proceedings of the 10th International Conference on Telecommunication Systems, Modeling and Analysis (ICTSM10)*, 2002.

[8] S. Clauß, D. Kesdogan, and T. Kölsch. Privacy Enhancing Identity Management: Protection Against Re-identification and Profiling. In *DIM '05: Proceedings of the 2005 workshop on Digital identity management*, pages 84–93, New York, NY, USA, 2005. ACM.

[9] S. Clauß and M. Köhntopp. Identity Management and its Support of Multilateral Security. *Computer Networks*, 37(2):205 – 219, 2001. Electronic Business Systems.

[10] A. Dwivedi and R. E. Wagner. Traffic Model for USA Long-distance Optical Network. In *Proc. Optical Fiber Communication Conference*, volume 1, pages 156–158, 7–10 March 2000.

[11] V. S. Frost and B. Melamed. Traffic Modeling for Telecommunications Networks. 32(3):70–81, March 1994.

[12] R. A. Guerin. Channel Occupancy Time Distribution in a Cellular Radio System. 36(3):89–99, Aug 1987.

[13] C. Hauser. *Protecting Virtual Identities in Mobile IP-based Communication*. PhD thesis, Universität Stuttgart, Institut für Kommunikationsnetze und Rechnersysteme, 2007.

[14] P. Kühn. Approximate Analysis of General Queuing Networks by Decomposition. *IEEE Transactions on Communications*, 27(1):113–126, 1979.

[15] A. Matos, J. Girao, S. Sargento, and R. L. Aguiar. Preserving Privacy in Mobile Environments with Virtual Network stacks. In *50th Annual IEEE Global*

Telecommunications Conference, Washington, DC, USA, November 2007. GLOBECOM 2007.

[16] D. Menascé and V. Almeida. *Capacity Planning for Web Services – Metrics, Models, and Methods*. Prentice Hall, 2002.

[17] V. N. Padmanabhan and L. Subramanian. An Investigation of Geographic Mapping Techniques for Internet Hosts. In *SIGCOMM '01: Proceedings of the 2001 conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, pages 173–185, New York, NY, USA, 2001. ACM.

[18] A. Pfitzmann and M. Hansen. Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology, version 0.31, February 15th 2008.

[19] A. Reyes-Lecuona, E. Gonzalez-Parada, E. Casilari, J. C. Casasola, and A. Diaz-Estrella. A Page-oriented WWW Traffic Model for Wireless System Simulations. In *Proceedings of 16th International Teletraffic Congress (ITC), Edinburgh*, 1999.

[20] C. Rigney, S. Willens, A. Rubens, and W. Simpson. Remote Authentication Dial In User Service (RADIUS). RFC 2865 (Draft Standard), June 2000. Updated by RFCs 2868, 3575, 5080.

[21] A. Sarma et al. Virtual Identity Framework for Telecom Infrastructures. In *Wireless Personal Communications*, Netherlands, February 2008. Springer. ISSN 0929-6212.

[22] D. Simon, B. Aboba, and R. Hurst. The EAP-TLS Authentication Protocol. RFC 5216 (Proposed Standard), Mar. 2008.