Security and Privacy for WLAN Roaming with per-connection Tariff Negotiation (Revised)

Johannes Barnickel, Ulrike Meyer
IT Security Research Group
RWTH Aachen University
barnickel,meyer@umic.rwth-aachen.de

July 11, 2012

Abstract

In this draft, we propose a novel protocol suite for roaming WLAN devices. It supports authentication, key agreement, and secure payment between roaming devices and network operators. This is achieved with the help of an integrated tick payment scheme. Our protocol suite allows operators to quickly change tariffs depending on current demand and allows users to choose between different operators and select from different tariff options on a per-connection basis. In addition, our protocol suite offers a very high degree of privacy protection by revealing only strictly required information to the participating parties.

1 Introduction

Mobile telecommunication networks such as GSM or UMTS enable international roaming in a way that is convenient for users and just works out of the box without any cumbersome configuration. It requires no user interaction, and users receive a single monthly bill through which they pay for the services of the operator they subscribed to as well as services offered by foreign networks. Nevertheless, the roaming approach used in current mobile telecommunication networks has several disadvantages. For one, tariffs are always negotiated between operators, and not between users and operators. As a consequence, users cannot directly influence the tariffs they need to pay when using the services of a foreign network. Also, roaming tariffs remain very high to this day. Although SMS price indication is required in some jurisdictions, in general it is still hard for users to tell how much they have to pay. Often, users cannot choose between different foreign operators but are instead forced to use the single foreign operator with whom their home operator has made an agreement, regardless of the

users' current network coverage and tariff preferences. For operators, there is no flexibility in tariff shaping and the life time of tariffs, as roaming agreements negotiated between operators are rather long-term agreements.

In WLAN roaming, wide area roaming is possible e.g. via eduroam [1], but this is not paid, or via Hotspots offered by (mobile) phone operators, e.g., [2, 3]. There are some islands of free WLAN networks in some coffeehouses etc [4], and some free WLAN initiatives, such as [5, 6], with a wider coverage area. However, free WLAN initiatives often run into problems with respect to overuse, abuse, and sometimes lawful interception requirements. Paid WLAN services are mostly pre-paid or credit card based, and often insecure [25]. Many paid WLAN services are cumbersome to set up, and usually very few tariffs are offered [7].

Our solution is targeted for convenient global roaming in WLAN networks and offers (1) secure payment, (2) short-term, on-demand tariff shaping for operators, (3) direct tariff selection on a per connection basis for users, (4) operator selection by users based on tariffs offered, (5) advanced privacy protection. In particular, no personal information about the user is revealed to the foreign operator and no information about the tariffs and the services used is provided to the user's home operator unless an user abruptly aborts a connection to the foreign operator. Still, law enforcement requirements can be met on a case-by-case basis.

Our solution consists of a protocol suite for mobile devices connecting to a foreign network and clearing protocols that offer the aforementioned features. We discuss the security and privacy features of the proposed protocols.

The rest of the paper is structured as follows: In Section 2, we explain our approach to WLAN roaming. In Section 3, details on the protocol between a mobile device and foreign network are provided and achievement of the goals is discussed. We compare our approach to existing solutions in Section 4. The conclusion is drawn and we provide an outlook on future work in Section 5.

2 Our Approach

2.1 Terms and Scenario

In our scenario users operate Mobile Devices (**MDs**) such as laptops or smart phones with a wireless interface. Each user has a trust relationship with one operator, referred to as the Home Network (**HN**) of that user's mobile device. In particular, HN has issued initial credentials for MD, knows the user's personal data and is able to (legally) enforce billing against MD. (Note that the home operator does not necessarily have to operate a wireless access network itself.) Any wireless access network operated by an operator other than MD's home operator is called Foreign Network (**FN**). In the following we will focus on a WLAN consisting of one or more Access Points (APs) as access network.

Users use their MDs to obtain Internet service via the APs of some network operator. Our goal is to enable MDs to obtain service not only from their home

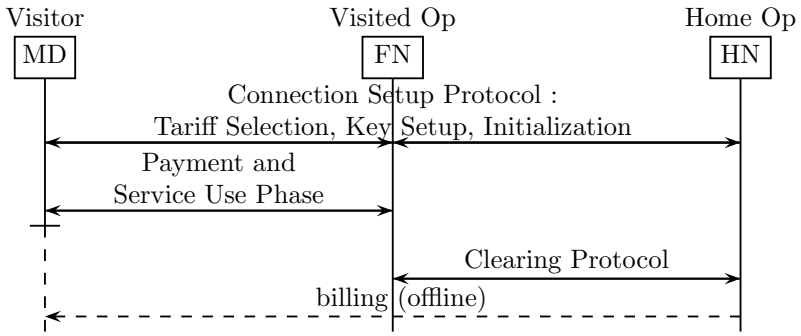

Figure 1: Phases of the Roaming Protocol

operator but also from those foreign operators that have established a roaming agreement with MD's home operator. The roaming agreement establishes a trust relationship between FN and HN: FNs trusts HN to reimburse FN for the service FN provides to HN's MDs. HN in turn bills MD for its service use at FN. Naturally, FN must be able to verify that an MD is entitled to use its services, i.e. that it is registered with an operator with which FN has a roaming agreement. Vice versa, MD has to be assured that FN is indeed a network operator with which MD's HN has a roaming agreement. A roaming agreement includes a clearing interface between operators.

So far the roaming scenario described is the same as in all common mobile telephony networks. However, our goal is to incorporate two novel requirements into this scenario.

First, in our scenario, MDs and FNs will be able to negotiate directly on the tariff to use for the next connection. In current mobile telephony networks, the tariffs are negotiated between FN and HN instead. Enabling negotiation between MDs and FNs directly allows for much more flexibility in traffic shaping. The idea here is that FNs broadcast their current tariff options in cost per minute or data volume and quality of service details such as provided bandwidth or maximum latency to the public. MDs select a suitable tariff from the list of tariffs currently offered by the FNs within its range depending on the user's choice or preferences.

Second, in current mobile telephony networks HN will receive all information on MD's service use in foreign networks. In addition, FN receives the correct long term subscriber identifier of MD and is able to track MD's service use over several connections. These disclosures are unnecessary. We therefore aim at a comprehensive roaming and accounting solution that incorporates the following privacy requirements: HN can neither find out where, when, and what specific services a user used at a specific FN nor what tariff was negotiated between the user and MD. FN cannot identify the user of an MD but only the correct HN of that user. In addition, FN cannot link different service uses of the same MD.

2.2 Basic Assumptions on Prerequisites

Our approach is based partly on public key primitives, but does not require a full public key infrastructure to be in place. In particular, we assume that each operator runs its own certification authority service. All certificates issued by these authorities are issued on signature creation keys and contain signature verification keys. Each MD stores the public key of its own HN. Each operator runs its own authentication server AuS that has access to the private key of the operator. Each AP is connected to the AuS of its respective operator.

MDs are not required to obtain certificates of FNs and vice versa. No public keys of FN have to be known to MD, and no public keys of MD have to be known to FN. No secret keys need to be preinstalled between MD and FN.

MDs carry a list of identifiers which are known to HN, i.e. serial numbers given by HN. Each MD carries a signature creation key, with the corresponding signature verification key known to HN. MD knows HN's signature verification key. These can be set up from HN to MD using a SIM card or a similar mechanisms and can be kept up to date using existing mechanisms.

To enable roaming among their users, operators have to exchange public keys among each other and keep them up to date using suitable mechanisms.

For the integrated micropayment system, HN has to vouch for MD to FN. Therefore, HN can verify that MD is solvent (post-paid contract) or that MD has made a deposit at HN beforehand (pre-paid contract).

We assume that access points are able to broadcast messages. For WLAN, this can be achieved using an efficient encoding scheme in the ssid or using a two-tier approach, where any device is able to associate on a separate broadcast network to receive the broadcast.

3 Roaming Protocol Suite

The roaming protocol suite consists of a connection setup protocol, a payment protocol, and a clearing protocol.

The connection setup protocol (CSP) provides mutual authentication and key establishment between MD, HN's AuS, and FN's AuS to establish a secure connection between MD and FN. When used for WLAN, the CSP could be implemented as a new key-generating EAP-method. Then, the key established during the protocol could be used as pair-wise master key in the 802.1X four-way handshake to establish a confidential and integrity protected connection between MD and AP. Beyond authentication and key establishment, the connection setup protocol includes secure tariff negotiation between MD and FN as well as the secure initialization of a tick payment scheme while protecting MD's privacy.

The payment protocol is based on a secure tick payment scheme. It consists of a payment and a clearing phase. In the payment phase MD uses the ticks to pay for the next unit of service and FN provides the service only if it received the corresponding ticks. In the clearing phase FN presents the ticks received from MD to MD's HN and is reimbursed. The clearing phase may take place

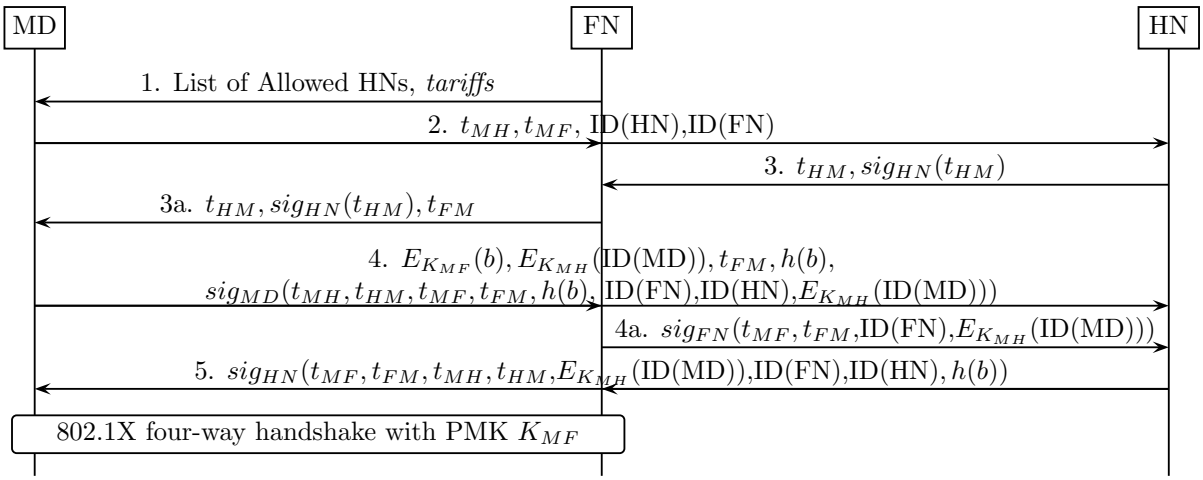

Figure 2: Connection Setup Protocol CSP

immediately after service use or periodically. MD in turn reimburses HN using an existing billing relationship between MD and HN.

Figure 1 provides a high level overview on the protocol suite and the entities involved in the different protocol phases.

3.1 Connection Setup Protocol CSP

The connection setup protocol is executed over a publicly visible, unencrypted, and unauthenticated channel. It includes discovery of tariffs, authentication, key establishment, tariff selection, payment initialization, and the first tick payment. Immediately after CSP is executed, MD can send the first data request. Remember that we assume HN is required to have an authentic copy of FN's and MD's current public signature verification keys. Furthermore we assume MD and FN to have an authentic copy of HN's current public signature verification key. The connection setup protocol is illustrated in Figure 2. The message exchange is described in detail in the following using the notations summarized in Table 1.

1. FN continuously broadcasts HNs whose MDs are allowed to use its services and its tariffs for these services. MD downloads these broadcasts from all APs within its radio reception range.

2. MD selects an FN AP which allows clients of MD's HN and which offers a suitable tariff. MD chooses $r_{MH}, r_{MF} \in_R \mathbb{Z}_p$ and calculates $t_{MH} = g^{r_{MH}} \mod p$, $t_{MF} = g^{r_{MF}} \mod p$ for HN and FN, which are sent to FN and relayed by FN to HN. ID(HN) is included in the message so that FN can verify that has it as a roaming agreement, that it knows where to forward the message to, and where to do the clearing after the connection ends.

ID(FN) is also included. (A TCP connection is assumed, so that following messages will not need routing information.)

3. HN chooses $r_{HM} \in_R \mathbb{Z}_p$ and calculates $t_{HM} = g^{r_{HM}} \mod p$. HN calculates $K_{MH} = {t_{MH}}^{r_{HM}} \mod p$. t_{HM} signed[1], and is sent to FN.

3a) FN chooses $r_{FM} \in_R \mathbb{Z}_p$, calculates $t_{FM} = g^{r_{FM}} \mod p$, and sends t_{HM} and t_{FM} to MD. FN calculates $K_{MF} = {t_{MF}}^{r_{FM}} \mod p$.

4. MD verifies the signature on t_{HM}. MD calculates $K_{MH} = {t_{HM}}^{r_{MH}} \mod p$ and encrypts its identifier ID(MD) for HN using K_{MH} to hide it from FN and eavesdroppers. MD also calculates $K_{MF} = {t_{FM}}^{r_{MF}} \mod p$ and encrypts b for FN using K_{MF}, thus hiding it from HN. After receiving message 4, FN decrypts b and verifies that MD's payment chain is correct for the selected tariff and that the tariff offers MD received really were offered by FN.

   MD creates payment data b by choosing random IV and α_0, to create a payment chain α, starting with $\alpha_1 = H(\alpha_0), \alpha_2 = H(\alpha_1), ...$, ending with $\alpha_T = H^T(\alpha_0)$, where T refers to the total ticks indicated by the selected tariff. MD also generates the first tick payment $\alpha_{T-d} = H^{T-d}(\alpha_0)$ as requested by the tariff. In the following, payment and tariff information is noted as $b =$ (ID(FN), chosen tariff, offered tariffs, IV, α_T, α_{T-d}).

   For message 4, MD creates a signature of the hash of b, the public DH parameters $t_{MH}, t_{HM}, t_{MF}, t_{FM}$, ID(FN), and ID(HN) as well as MD's hidden identifier $E_{K_{MH}}$(ID(MD)) known to HN.

   Note that our notation, $sig_X(m)$ does not contain m, but only the hash of m and the signature of the hash of m. Therefore, the message must also contain t_{FM} and $h(b)$, so that HN can verify the signature.

   After receiving message 4, HN uses ID(MD) to look up the real identifier of MD and its public signature verification key, which is used to verify the signature. t_{MH} and t_{HM} must match the values received in message 2 and sent in message 3. The received ID(HN) must match its own ID and ID(FN) must match the FN which delivered the message. $H^d(\alpha_{T-d})$ must match α_T.

4a) FN generates a signature on t_{MF}, t_{FM} and the identifiers ID(FN) and $E_{K_{MH}}$(ID(MD)). The signature is sent to HN because MD does not know FN's signature verification key.

5. After successfully verifying the signatures sent by MD and FN, HN creates a signature to authenticate the key agreements MD-FN and MD-HN, and to confirm to FN that MD's signature is correct and that MD is credit worthy. To enable FN to validate the signature without knowledge of ID(MD), instead $E_{K_{MH}}$(ID(MD)) is signed. Both FN and MD verify HN's signature.

[1] Update: to prevent a man-in-the-middle-attack executed by FN to obtain ID(MD)

tariffs	list of: type of tariff (per data volume, time, packets, etc), price (amount, currency, unit), total ticks T (connection limit), ticks per unit d, e.g.: charged per time, 0.01 EUR per 30 seconds, 14400 ticks total, 5 ticks per unit
r_{xy}	private Diffie-Hellman key chosen by party x for setting up a key with party y
t_{xy}	the public Diffie-Hellman key of party x corresponding to r_{xy} shared with party y
p	publicly known large prime
g	publicly known generating element of a finite group G where the discrete logarithm problem is hard
b	payment data and tariff chosen by MD
α_0	root of the payment hash chain chosen by the payer, α_T last element in the chain in generation order
IV	initialization vector chosen by the payer
$H(m)$	preimage resistant hash function with input m and initialization vector IV
$h(x)$	cryptographic hash of input x
$E_K(m)$	symmetric encryption of plaintext m with key K, e.g. AES
$sig_X(m)$	signature of message m by party X, does not include the unhashed message m
K_{MF}	symmetric key which is being established between MD and FN during the protocol run
K_{MH}	symmetric key which is being established between MD and HN during the protocol run
ID(MD)	identifier of MD, i.e. serial numbers known only to MD and HN
ID(FN)	identifier of FN, i.e. its unique brand name
ID(HN)	identifier of HN, i.e. its unique brand name

Table 1: Notations

Now, MD and FN use K_{MF} as MSK in an 802.1X four-way handshake and FN provides the first service interval to MD at the tariff selected by MD. Further service intervals and redemption are discussed later in Section 3.2.

Discussion of the Connection Setup Protocol: The connection setup protocol illustrated in Figure 2 offers the following security and privacy features:

Entity authentication is achieved as MD, FN, and HN include ephemeral public keys from messages 2, 3, and 3a and identifiers of the participating parties within the signed parts of messages 4, 4a, and 5. Therefore, all parties are aware that the other parties they established keys with are actively participating in the current protocol run. This is similar to two runs of the BCK protocol [13].

The keys K_{MH} and K_{MF} established during each protocol run are **fresh** as the ephemeral DH parameters are chosen by MD, FN, and HN for only this session. Also, K_{MF} is **exclusive** to MD and FN as it can only be calculated

by a party that knows the corresponding private DH parameter to the public ephemeral key a party sent. The same holds for K_{MH}, which is exclusive to MD and HN.

Because HN verifies FN's signature for MD, HN is able to impersonate FN. But as they have a roaming agreement, HN and FN already trust each other. Also, there is no financial gain in this attack.

Impersonation of MD is impossible, as MD is required to create a signature matching a public key known to HN. An attacker impersonating HN (and possibly MD at the same time) to FN will be detected because he cannot create the signature in message 5.

Explicit key confirmation is achieved by the encryptions with K_{MH} in messages 4 and 5 and with K_{MF} in message 4. As entity authentication of MD, FN, and HN is given, mutual belief in the keys is achieved.

Privacy: In our protocol, FN does not learn MD's ID or a constant pseudonym of MD. It is only disclosed to HN. Passive eavesdroppers will only learn the MAC address of MD but not its ID/pseudonym. This decouples the problem of staying unlinkable with respect to passive eavesdroppers from the problem of staying untraceable with respect to FN. For MD to stay unlinkable from passive eavesdroppers it is sufficient to change the MAC address between two connection setups. MD stays unlinkable to FN because $E_{K_{MH}}(\mathrm{ID(MD)})$ is different each time as it depends on DH parameters freshly chosen by MD and HN.

Tariff negotiation is done by FN sending a numbered list of supported tariffs and MD returning a signature on the hash of the complete numbered list as well as the number of its selected tariff to HN. HN creates a signature on this for FN. Therefore, FN is able to not only verify the authenticity of MD's choice of tariff but also to verify that MD has received the full unmodified tariff list as originally broadcasted to MD. This prevents attacks where an attacker modifies FN's tariff announcements. However, from the connection setup, HN does not learn anything about the tariffs offered by FN, the tariff chosen by MD, or the payment data generated by MD. This is meant to protect the privacy of MD.

3.2 Tick Payment Protocol

The payment protocol is similar to the one suggested by Horn and Preneel [20], but the first tick payment is integrated into the setup phase. The idea of micropayment in roaming is that MD pays d ticks to FN for each small service interval before it is provided. Each tick corresponds to a small amount of money. In the proposed protocol, the service unit (time, data volume), the size of the service interval, the number of ticks per service interval, and the monetary value of a single tick have all been agreed upon during tariff negotiation in the connection setup protocol.

Initialization of Tick Payment: MD generates a payment chain by randomly choosing α_0, IV, and calculating $\alpha_i = H(\alpha_{i-1}), i \in \{1, \ldots, T\}$. When pairs $\alpha_i = \alpha_j, i, j \in \{1, \ldots, T\}$ appear, MD selects new random values. In message 4 of CSP discussed in Section 3.1, MD commits to the payment data b by calculating a signature on its hash. b contains the initial values of the payment

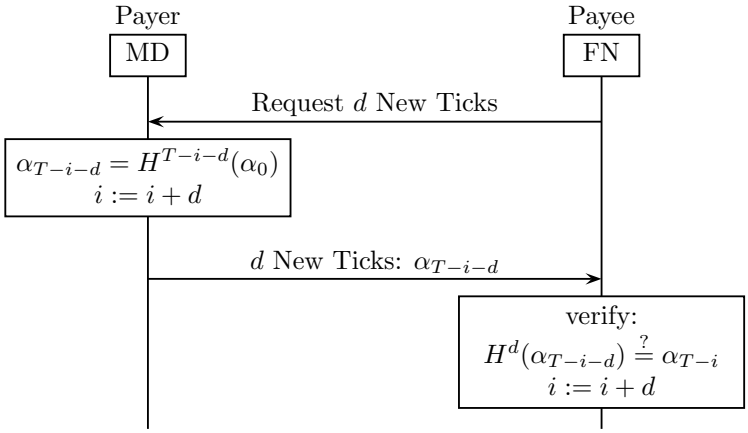

Figure 3: Tick Payment Protocol MD to FN

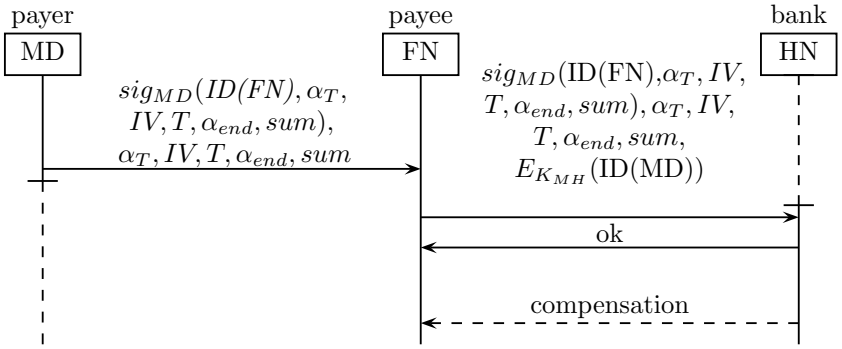

Figure 4: Clearing Phase with Graceful End

protocol α_T, IV, the ID(FN), the selected tariff, and the first payment of d ticks, α_{T-d}. HN verifies MD's signature and creates a new signature on $h(b)$ for FN. FN will now provide service to MD until the first service interval expires.

New Service Interval: When a service interval is used up, new tick payments are requested by FN as illustrated in Figure 3. After i ticks were used, MD provides d new tick payments to FN by calculating $\alpha_{T-i-d} = H^{T-i-d}(\alpha_0)$ and sending α_{T-i-d} it to FN. FN verifies that $H^d(\alpha_{T-i-d}) \stackrel{?}{=} \alpha_{T-i}$. Both parties increase i by d and store i. This can be repeated until $i > T$, when MD must commit to a new payment chain by MD creating a new message 4 as described in 3.1. This can be done earlier if MD wants to switch to a different tariff at the same FN. MD always has to keep track of the service it uses so that it cannot be overcharged by FN.

Clearing Phase: When MD closes the connection to FN gracefully, clearing is done at anytime after the end of MD's service use as shown in Figure 4. Here, MD sends an ending message $sig_{MD}(ID(FN), \alpha_T, IV, T, \alpha_{end}, sum)$, where sum is the total monetary amount of service used. This signature is sent to HN.

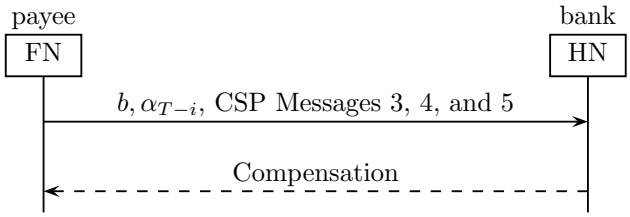

Figure 5: Clearing Phase after Abort

Note that HN will still not obtain knowledge of any details MD and FN have agreed on. In the interest of MD's privacy, HN will only receive information on whom to pay how much. When MD tries to cheat by choosing a lower amount in the ending message than it has to pay, or when HN does not accept MD's ending message, FN will behave as if MD aborted the connection.

When a connection aborts without MD sending an ending message, FN is able to collect compensation from the visitor's HN by the clearing protocol as shown in Figure 5. During the authentication phase as described in Section 3.1, FN has obtained the billing information b from message 4 and the signature sent from HN on $h(b)$ from message 5. The last tick payment α_{T-i} was obtained from MD during the tick payment phase described above. Together, this data allows FN to prove that HN has to pay for the services MD used. FN can prove to HN that MD is a customer of HN, the amount of service FN provided to MD, and the tariff MD selected, which results in the amount to be paid. In this case, HN obtains the details about the tariffs offered by FN, the tariff chosen by MD, and the service used by MD.

In both cases, HN will reimburse FN and charge MD. HN learns nothing about the time, date, and location of the service used by its MD during clearing and billing with FN. When MD aborts without sending an ending message, HN will obtain knowledge of the tariffs offered by FN, the tariff MD and FN have agreed on, and the amount of service MD used.

HN knows K_{MH} from the connection setup and has stored it together with α_T, so that it can decrypt $E_{K_{MH}}(\mathrm{ID(MD)})$. As HN has issued ID(MD), HN is able to resolve ID(MD) to the real identity MD, so HN is able to bill MD. To prevent FN from double charging by using both the graceful and the aborted redemption messages, α_T, IV, T, and α_{end} are included in the graceful ending message. This way, HN can detect that these describe the same session.

Discussion of the payment protocol: A fundamental property of micropayment schemes is the very low value of a single tick payment. Therefore, it is not a problem when MD provides the first tick payment during setup and FN does not provide service. The same holds when the connection aborts after a number of intervals, when MD might have paid for one more tick than it could use.

The security of micropayment schemes based on hash chains is well researched. Given α_i, no one can calculate α_{i-j} for any $j > 0$ because H is a preimage resistant hash function. Therefore, new ticks to an existing chain

Party	Messages Sent	Receive	Fwd	Signatures Create	Verify	Symmetric Enc	Dec
Connection Setup Protocol							
MD	2	2*	0	1	1	2	0
FN	2*	1	3	1	1	0	1
HN	2	3	0	1	2	0	1
Clearing Protocol With Graceful End							
MD	1	0	0	1	0	0	0
FN	1	2	0	0	0	0	0
HN	1	1	0	0	1	0	1
Clearing Protocol After Abort							
MD	0	0	0	0	0	0	0
FN	1	0	0	0	0	0	0
HN	0	1	0	0	3	0	1

*and one broadcast message

Table 2: Efficiency of the Protocols

cannot be forged.

The identity of the payer is bound to the payment chain because of MD's signature in message 4, which is validated by HN. The identity of the payee is also bound to the payment chain because the signature contains ID(FN), which is confirmed by HN. Therefore, payments cannot be stolen. Because all payment chains generated by MD are validated over the same HN, contain fresh values α_T, IV, and as HN keeps records of payments, a payment chain cannot be used more than once. FN cannot be tricked into accepting the same payment twice as the signature in message 4 contains t_{FN}, which is chosen by FN. FN does not learn the identity of MD during payment or clearing, as only $E_{K_{MH}}(\text{ID(MD)})$ is disclosed to FN, which is different for each session.

3.3 Efficiency of the protocols

A summary of the costly operations executed in all protocols is given in Table 2. The connection setup protocol is discussed in the following:

- MD has to send two messages, receive two messages (and a broadcast message), create one signature, verify one signature, and calculate two symmetric key encryptions.
- FN has to forward three messages, receive one message, send two messages (and a broadcast message), verify one signature, create one signature, and execute one symmetric key decryption.
- HN has to send two messages, receive three messages, create one signature, verify two signatures, and execute one symmetric key decryption.

We can see that the setup protocol requires only a single computationally expensive operation per party (on private keys). The tick payment protocol does not require any costly operations during use. Only for privacy preserving clearing using the graceful ending message, MD has to generate another signature, which HN has to verify. For the clearing of aborted messages, HN has to verify three signatures.

3.4 Lawful Data Retention

In many jurisdictions Internet access operators are required by law to keep records of who accesses the Internet during which period of time using which IPs. In this case, FNs need to keep lists of the IPs assigned during which time for each encrypted pseudonym $E_{K_{MH}}(\mathrm{ID(MD)})$ that was used. The HNs already need to keep track of ID(MD), K_{MH}, and real identities for billing purposes.

When a court order is given to FN to reveal the identity of the user behind a certain IP and time period, FN looks up the $E_{K_{MH}}(\mathrm{ID(MD)})$ that used the IP during that time and returns it to law enforcement. Law enforcement forwards the request and $E_{K_{MH}}(\mathrm{ID(MD)})$ to HN. HN discloses the real ID behind ID(MD) and the original query to the requesting agency.

When a court order is given to HN to reveal the IPs used at a certain time by a certain user whose identity is known, HN creates a list of $E_{K_{MH}}(\mathrm{ID(MD)})$ used by the user and a list of FNs with which it had roaming agreements during the period in question. These lists are sent back to law enforcement. Law enforcement forwards the list and the court order to all FNs listed by HN. The FNs respond by sending time periods and IPs for connections using matching values of $E_{K_{MH}}(\mathrm{ID(MD)})$ to the requesting agency.

4 Related Work

Our solution offers (1) secure payment, (2) short-term, on-demand tariff shaping for operators, (3) direct tariff selection on a per connection basis for users, (4) operator selection by users based on tariffs offered, and (5) advanced privacy protection. In this section we will compare our solution to existing academic and non-academic roaming approaches and show that none of these approaches simultaneously meets all the features our solution offers. We also briefly review prior work on the building blocks we use in our protocol, namely the authenticated key establishment and tick payment schemes.

4.1 Operational Roaming Solutions

The use of the Extensible Authentication Protocol [12] in 802.11i WLANs allows for authentication and key agreement between a foreign network and a mobile device with the help of the home network of the user. In this case, the foreign network and the home network each operate an EAP server. Authentication requests from a roaming mobile device are proxied through the foreign network's

EAP server to the home EAP server, such that the EAP-method is carried out between the mobile device and its home EAP server. The home EAP server indicates a successful authentication to the foreign EAP server. Examples for operational networks using this approach are [1, 10, 8]. This EAP-based approach does not support tariff shaping or tariff selection and consequently does not support the advanced privacy protection in our approach.

3GPP [9] relies on stored customer profiles to facilitate billing and user authentication. Tariff selection on a per connection basis for users is possible with some operators, although rarely used. The users dial a special code on their MD to activate various options, e.g. to purchase an amount of data volume. However, this does not enable on-demand tariff shaping for operators. The TMSI mechanism provides some privacy protection against passive eavesdroppers tracking the device, but active attackers are able to track mobile devices. In addition, the HN always obtains all connection details and FN always obtains the subscriber's longterm identifier.

Wireless Roaming Intermediary Exchange by the Wireless Broadband Alliance [8] is a modularized standard service specification to allow global WLAN roaming between WBA members (operators) based on EAP with a foreign operator, e.g. iPass and Boingo. These operators typically offer flat rate accounts or a monthly allowance regarding time or traffic, but no dynamic pricing.

4.2 Proposed Academic Roaming Solutions

A variety of roaming protocols do not support payment initialization and tariff negotiation. These include for example the protocols suggested in [19, 28, 18, 17, 23]. As the integration of payment is one of the most crucial features of our proposed roaming solution, we only discuss those protocols in more detail that also include secure payment.

In Buttyán-Hubaux [14], a (potentially offline) customer care agency provides tickets to mobile devices. These tickets can be used by the mobile device to roam to different networks. The customer care agencies also have the tasks of user identification and billing, like our HNs. The protocol is preserving the privacy of the user to the visited network, but not to the customer care agency, which will always receive information about the tariff. This is the most important difference to our solution. The protection of MD against tracking is based on so-called tickets, which are multiple identifiers used by MD. However, revocation of stolen unused tickets is not discussed. There is a single tariff chosen freely by the involved stations at each new connection, but no influence from the user on the selected tariff. A vulnerability in the signature and hash chain based payment system used in [14] was discovered in [24], which also proposed a solution.

EAP-TLS-KS [24] avoids certificate verification paths on the MD by using a key splitting method unique for each FN, distributed decryption, and distributed signatures for mutual authentication of MD and FN. During each authentication, HN is required to be online. The mechanisms trades network round trips for additional cryptographic operations. An implementation of the DHE-RSA

case showed superior performance to EAP-TLS [15]. EAP-TLS-KS can include any accounting method and proposes a more secure variant of the Buttyán-Hubaux-Protocol [14], which inherits the same properties regarding tariffs as Buttyán-Hubaux: A single tariff for each operator and no influence by the user besides selecting another operator.

Pierce-O'Mahony [27] integrates multiparty micropayment into roaming for GSM multi-mop networks: When an MD is connected to its communication partner over a number of stations, MD pays a large amount of ticks to the first station, which keeps some of it, and forwards the rest to the next station. The next station keeps some of the payment, and forwards the rest to the next station. The system is prepaid. No signatures by MD are required. Tariffs are chosen by the stations between MD and target regarding MD's demand on quality of service, but cannot be selected directly by the user. Users choosing between operators and protection of MDs against tracking are not discussed.

Huitema et al. [21] propose an architecture for automatic and dynamic negotiation of compensation agreements by integrating agreement negotiation, agreement realization, and an overall compensation process. Operators are flexible with respect to charging depending on demand, and users may choose tariffs freely. There is no integrated payment or authentication/key establishment, instead the solution is meant to operate on top of existing compensation systems.

Fu et al. [16] present a policy language to obtain inter-operator roaming agreements through policy based negotiation spontaneously when requested by an user. Negotiation between users and operators is not supported.

ARSA [30] is a solution based on identity based cryptography to facilitate roaming. Brokers are connected to each other and to the operators, so that no agreements between operators are needed. Revocation of stolen credentials and spending limits are addressed. User aliases are used to achieve unlinkability to the operator. A micropayment scheme is included. The hops are not paid by the mobile device, but by the FN, which is thought to be more efficient for a large number of hops and computationally weaker mobile devices as it is placing more load on the FN. Our approach avoids brokers, and rather uses the HN with a sporadic connection to the FN and bilateral agreements.

Jakobsson et al. [22] propose a probabilistic micropayment scheme to encourage collaboration in networks with a large number of hops. The operator is capable of detecting and punishing misbehaving participants in its payment scheme. Stations on the path between user and base station are paid for a fraction of the packets they forward. Tariffs, authentication, privacy, and revocation are not addressed.

Wan et al. [29] propose a hierarchical ID-based roaming protocol with a trusted party and an offline HN to protect the user's privacy. The protocol execution requires pairing operations and public key cryptography. A hash based payment scheme is included, but no tariff negotiation is performed.

4.3 Review of the Used Building Blocks

Authentication and Key Agreement: The authentication and key establishment between MD and HN as illustrated in Figure 2 is very similar the BCK protocol [13]. The security of the BCK two party authentication and key agreement protocol is well researched. It provides implicit key confirmation. Because in our protocol MD uses the key K_{MF} on b which is partially known and completely meaningful to FN, we achieve explicit key confirmation. The ISO/IEC 11770-3 Key Agreement Mechanism 7 [11] is also a variant of the BCK protocol with added explicit key confirmation using message authentication codes. We have extended our protocol to also authenticate FN to MD and HN.

The Tick Payment Protocol: Tick payment protocols combine some advantages of prepaid and postpaid payment systems and are well suited for telecommunications, as the payment amount is constantly growing. The tick payment protocol we use in our roaming solution is the protocol introduced by Pedersen in [26]. More formal proofs of the security properties of this tick payment protocol can be found briefly discussed in Section 3.2. We have integrated the initialization of the payment protocol into the authentication and key agreement protocol without requiring additional messages.

5 Conclusion and Future Work

We have presented a protocol suite for secure and privacy preserving roaming and payment in WLAN networks without an online connection to a home network or any other form of trusted third party. The proposed solution highlights tariff flexibility for both users and operators, as users can select a tariff that fits their demands and operators are free to modify their offered tariffs at any time.

In the future, we will implement the protocol as an EAP method that runs on off-the-shelf hardware. A client for mobile devices will be developed that is especially easy to use to underline the transparency of the roaming options. Performance tests and evaluation will be done. In addition, an extension of our protocol suite with all its properties to already connected mobile devices acting as hops for other devices while preserving all privacy and security goals of the existing protocol will be investigated.

Acknowledgments

This work has been supported by the UMIC Research Centre, RWTH Aachen University. We would like to thank the reviewers of the 2012 Information Security Conference for their insightful remarks and pointing out an attack described in the footnote of Section 3.1.

References

[1] eduroam (education roaming), http://www.eduroam.org/, retrieved 07-25-2011.

[2] AT&T hotspots http://www.wireless.att.com/learn/internet/wifi.jsp, retrieved 07-25-2011.

[3] Unitymedia Hotspots http://www.unitymedia.de/produkte/internet/hotspots.html, retrieved 07-25-2011.

[4] Starbucks Wireless Internet http://www.starbucks.com/coffeehouse/wireless-internet, retrieved 07-25-2011.

[5] About Wifi Foundation http://www.wififoundation.org/about-wififoundation/, retrieved 07-25-2011.

[6] WeFi, http://www.wefi.com/, retrieved 07-25-2011.

[7] T-Mobile Germany hotspot tariffs http://www.hotspot.de/content/tarife_2.html, retrieved 07-25-2011.

[8] Wireless Broadband Alliance, http://www.wballiance.net/, retrieved 07-25-2011.

[9] 3GPP TS 32.240 (Release 9): Telecommunication management; Charging management; Charging architecture and principles.

[10] IEEE 802.16-2009 standard for local and metropolitan area networks part 16: Air interface for broadband wireless access systems.

[11] ISO/IEC 11770-3: Information technology - Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques.

[12] Aboda, Simon, and Eronen. Extensible Authentication Protocol (EAP) Key Management Framework. IETF RFC 5247, 2008.

[13] Blake-Wilson and Menezes. Authenticated Diffie- Hellman Key Agreement Protocols. Proceedings of the 5th Annual Workshop on Selected Areas in Cryptionsgraphy (SAC '98), LNCS 1556, 1998.

[14] Buttyán and Hubaux. Accountable anonymous Service Usage in mobile communication systems. EPFL SSC Technical Report No. SSC/1999/016, 1999.

[15] Cordasco, Meyer, and Wetzel. Implementation and Performance Evaluation of EAP-TLS-KS. Proceedings of Security and Privacy in Communication Networks, 2006.

[16] Fu, Shin, Strassner, Jain, Ram, and Arbaugh. AAA for spontaneous roaming agreements in heterogeneous wireless networks. Proceedings of 4th International Conference of Autonomic and Trusted Computing, 2007.

[17] Giessler, Schneider, Bayarou, Haisch, Hunter, Rohr, Ilyas, and Enzmann. Towards Certificate-Based Authentication for Future Mobile Communications. Wireless Personal Communications 29, 2004.

[18] Jabeom Gu, Sehyun Park, Ohyoung Song, Jaeil Lee, Jaehoon Nah, and Sungwon Sohn. Mobile PKI: A PKI-Based Authentication Framework for the Next Generation Mobile Communications. Proceedings of ACISP'03, LNCS volume 2727, 2003.

[19] Heer, Li, and Wehrle. PISA: P2P Wi-Fi Internet Sharing Architecture. Seventh IEEE International Conference on Peer-to-Peer Computing, P2P, 2007.

[20] Horn and Preneel. Authentication and payment in future mobile systems. Journal of Computer Security 8(2/3), pp. 183-207, 1999.

[21] Huitema, Kühne, Meyer, Ensing, Alf, Bibas, Karasti, Rumph, and Siljee. Compensation: Architecture for Supporting Dynamicity and Negotiation in Accounting, Charging and Billing. Journal of Computer Communications, Elsevier, June 2010.

[22] Jakobsson, Hubaux, and Buttyan. A Micro-Payment Scheme Encouraging Collaboration in Multi-hop Cellular Networks. Financial Cryptography, 2003.

[23] M. Manulis, D. Leroy, F. Koeune, O. Bonaventure, and J.-J. Quisquater. Authenticated Wireless Roaming via Tunnels: Making Mobile Guests Feel at Home. 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS 2009.

[24] Ulrike Meyer, Jared Cordasco, and Susanne Wetzel. An approach to enhance inter-provider roaming through secret sharing and its application to WLANs. The ACM Workshop on Wireless Mobile Applications and Services on WLAN Hotspots, 2005.

[25] Ogle, Wagner, and Talbert. Hotel Network Security: A Study of Computer Networks in US Hotels. Cornell Hospitality Report 2008 Vol. 8 No. 15 pp. 4-20, 2008.

[26] Pedersen. Electronic Payments of Small Amounts. International Workshop on Security Protocols, 1997.

[27] Pierce and O'Mahony. Flexible real-time payment methods for mobile communications. IEEE Personal Communications, 1999.

[28] Salgarelli, Buddhikot, Garay, Patel, and Miller. Efficient authentication and key distribution in wireless IP networks. IEEE Wireless Communications Magazine, 2003.

[29] Wan, Ren, and Preneel. A Secure Privacy-Preserving Roaming Protocol Based on Hierarchical Identity-Based Encryption for Mobile Networks. Proceedings of the 1st ACM conference on Wireless network security, 2008.

[30] Zhang and Fang. A secure authentication and billing architecture for wireless mesh networks. Wireless Networks, Volume 13, Number 5, 663-678, Springer, 2007.