A Privacy Preserving Range Extension for Commercial WLANs with User Incentives

Johannes Barnickel
IT Security Group
RWTH Aachen University
barnickel@umic.rwth-aachen.de

Ulrike Meyer
IT Security Group
RWTH Aachen University
meyer@umic.rwth-aachen.de

***Abstract*—Worldwide service availability via international roaming is one of the success factors of mobile telecommunications and hopefully also for WLAN access in the near future. Recently, a promising protocol suite for inter-operator roaming in commercial WLAN has been proposed. This protocol suite offers several advantages over other roaming protocols such as secure payment, short time tariff shaping, and strong privacy guarantees. In this paper, we propose an extension to this protocol suite, which allows any WLAN customer with a mobile device that supports virtual interfaces on its WLAN card to act as a paid relay station, or as we call them, Hops. The WLAN provider profits from these relaying stations at they increase the coverage area of his access points even beyond his domain. The owner of the Hop will receive monetary compensation over an integrated tick payment scheme. Like the original protocol suite, our protocol extension offers secure payment, tariff shaping, and strong privacy guarantees.**

keywords – WLAN roaming; micropayment; Internet access; mobile Internet; wireless hops.

I. INTRODUCTION

Worldwide roaming is one of the most valuable services provided by modern mobile operators. It is based on the fact that each mobile device (**MD**) has a contract with one of several home networks (**HN**s), which has MD's billing information. The HN has a roaming agreement with various foreign networks (**FN**s) via which they agree to provide access services to each other's customers. MDs are billed for the use of FN's service via HN, and roaming tariffs are negotiated between the two providers. Unfortunately, the latter has led to very high roaming prices and users ending up with unexpectedly high bills due to a missing transparency of the tariffs being charged. In addition, tariffs are quite inflexible and need to be fixed based on legal agreements between the operator rather than being based on the current demands. Finally, current roaming practices do not preserve the privacy of customers as HN learns everything about MD's service use via FN, and FN learns the identity of MD. Some mobile operators have started to use SIM-based access to WLANs and are thereby able to reuse the roaming infrastructure of their telephony networks in the WLAN context – including its shortcomings.

In many commercial WLANs, however, user are still directed to a webpage where they have to provide their credit card information to the operator of the access point, which is cumbersome for short term use and requires the user to disclose his personal data. Also, the credit card transaction fees make paying small amounts for Internet access not efficient. Often, long term contracts are offered by operators of multiple access points, e.g., mobile phone operators, or dedicated providers. For the user, this means having to sign an (often long running) contract with an unknown provider, without being able to judge how often he will be close to an access point of this provider.

The roaming solution proposed in [1] addresses these shortcomings of current roaming solutions. It combines secure and convenient access to paid WLANs with tariff transparency, tariff flexibility, integrated micropayment, and privacy protection. Unlike in mobile telephony networks, the FNs are able to change the tariffs they offer at any time without even notifying HN, as they are not part of the roaming agreements. As MDs can choose any tariff offered by any FN, tariff negotiation between MDs and FNs is enabled. To retain customer privacy, the HN does not receive any details about its clients' sessions, and the FN will not be able to identify or track HN's clients.

In this paper, we propose a new Hop extension to the roaming solution proposed in [1]. This proposed extension allows any MD connected to a participating WLAN to act as access point itself. We refer to such an MD as "Hop". These Hops increase the area covered by WLAN, increase the operator's number of potential clients, and can help to create ubiquitous access. The owner of a Hop is reimbursed for acting as a Hop such that our approach does not suffer from missing incentives to share connectivity like many free WLAN initiatives [2] do. A client using a Hop will still receive a single bill from his home network. Note that acting as a Hop is perfectly feasible with off the shelf laptops and smartphones. Many mobile devices today support virtual interfaces in their WLAN module or can use multiple different network interfaces at the same time. This means that these devices are able to act as client and access point in different networks at the same time.

The rest of the paper is structured as follows: In Section II, we reconsider the approach to WLAN roaming described in [1]. In Section III, we extend the protocol to cover mobile devices acting as Hops. We review related work in Section IV.

 ISBN: 978-1-61208-229-5

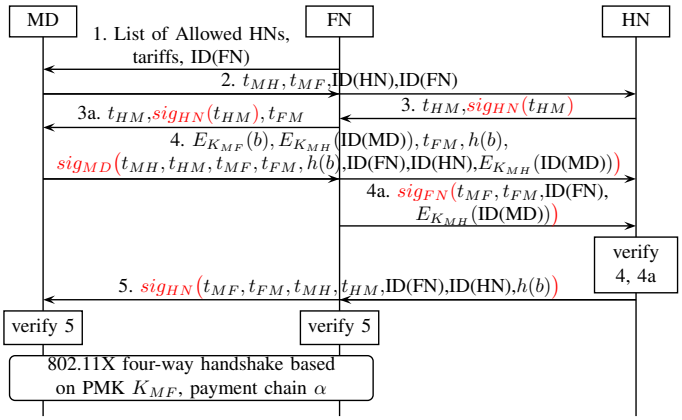

Fig. 1. Basic Connection Setup Protocol

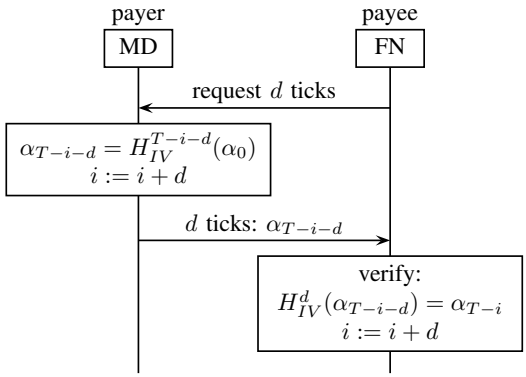

Fig. 2. Basic Tick Payment Protocol

II. The Basic Roaming Protocol

In this section, we briefly resume the roaming protocol suite proposed in [1]. We will then extend it to include Hops in Section III.

It is assumed that HN and MD, and HN and FN are in possession of each other's public key. The protocol suite consists of three protocols: a connection setup protocol, a tick payment protocol, and a clearing protocol. The connection setup protocol involves MD, HN, and FN and is used for authentication, key agreement, and payment initialization when MD requests access to an access point operated by FN. The tick payment protocol is used between MD and FN. It keeps the connection alive with regular tick payments created by MD to pay for the service it uses. When the connection ends, the clearing protocol is executed between FN and HN, and optionally MD.

A. Basic Connection Setup Protocol

The connection setup protocol assures FN that MD is owned by a client of HN, and that HN will pay FN for the services MD used. It allows FN to advertise his current tariffs and these tariffs are authenticated as part of the setup protocol such that MD is assured of the tariffs offered by FN and that FN is a roaming partner of HN. HN is assured of MD's identity and that MD has agreed on the tariff used. At the same time, MD's privacy is protected, such that HN does not learn payment details from the connection setup protocol. FN cannot learn MD's identity, cannot recognize if MD has been a client before, and therefore cannot track MD using access points in multiple locations. Obviously, MD would also have to change its MAC address for every new connection to a FN it used before.

The protocol is described in Fig. 1, and the notations are given in Table I.

Message 1 is a broadcast that is continuously sent by FN's access point. It contains a list of tariffs and HNs with which FN has a roaming agreement, i.e., whose clients may connect. Tariffs can be offered in cost per minute or cost per data volume. The broadcast mechanism allows FN to change its tariffs at any time and it allows MDs to discover the network and to review the tariffs offered by FN. We include the ID of FN in message 1 as well, although it was not mentioned explicitly in [1]. The client software on the MD is able to decode this broadcast, and enables the user to select one of the tariffs offered by FN. When multiple FNs offer wireless networks in the same location, the user can choose freely among the FNs.

We have implemented the broadcast on commodity hardware using a special encoding in the SSID. The SSID may contain up to 256 bits. The SSID must contain the FN's name, which could be at most 10 characters = 80 bits. With four different interval sizes and 32 different per unit prices (e.g., from 0.1 to 28.5ct in steps of 20%), 8 bits per tariff offered are required. With two types of tariffs (data volume and time based), up to 8 tariffs are possible for each network, requiring $8 \cdot 8 = 64$ bits of the SSID. Allowed HNs can be encoded as a bit string (assigned by some authority), the length of which could be 10 bit, allowing for a total of $2^{10} = 1024$ HNs. With an operator name length of 10 bytes in clear text, at most $\lfloor (256 - 80 - 64) : 10 \rfloor = 11$ allowed HNs fit in the SSID.

Messages 2.–5. contain a key establishment protocol based on Diffie-Hellman with authentication via signatures. As MD and FN do not share public keys, HN verifies the signatures and confirms their correctness in message 5. MD and FN establish the key K_{MF}, of which one derivation will be used in a subsequent 802.11X four-way handshake, and another derivation is used to hide details about the payment information from HN. MD and HN establish the key K_{MH} to hide MD's identity ID(MD) from FN. Message 3. and 3a. are modified over [1] to include HN's signature to prevent an attacker acting as FN from executing a man-in-the-middle-attack on K_{MH} to extract ID(MD).

Messages 4. and 5. also contain the list of offered tariffs, the tariff selected by MD, payment initialization values IV and α_T, and the first tick payment, which are summarized as b in Fig. I. Further service intervals and clearing of payments are discussed in Sections II-B and II-C.

B. Tick Payment Protocol

The tick payment protocol has been proposed by Horn and Preneel [3] and Pedersen [4]. In [1], the first tick payment has been integrated into the setup phase to speed up service provision.

 ISBN: 978-1-61208-229-5

Diffie-Hellman related:	
g	Publicly known generating element of a finite group G where the discrete logarithm problem is hard
p	Publicly known large prime
r_{XY}	Private DH key chosen by party X for key setup with party Y
t_{XY}	Public DH key calculated by X for setup with Y: $g^{r_{xy}} \bmod p = t_{xy}$
General Cryptographic Operations:	
$H_{IV}(m)$	Preimage resistant hash function with input m and initialization vector IV
K_{XY}	Symmetric key established between parties X and Y during the protocol run
$sig_X(m)$	Signature of m by party X, does not include the message m. Signatures are unlinkable with regard to the signer.
$E_K(m)$	Symmetric encryption of plaintext m with key K, e.g., AES
ID(FN)	Identifier of FN, i.e., its unique brand name
Payment Related:	
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
d	Amount of ticks per unit as requested per tariff
α	payment chain used between MD and FN
α_0	Root of the payment hash chain chosen by the payer
α_T	Last element in the chain in generation order, $\alpha_T = H_{IV}^T(\alpha_0)$
α_{T-d}	First tick payment. $\alpha_{T-d} = H_{IV}^{T-d}(\alpha_0)$
IV	Initialization vector chosen by the payer
b	Payment info vector. $b = (IV, \alpha_T, \alpha_{T-d},$ selected tariff, offered tariffs)
pay_α	graceful payment string $pay_\alpha = \alpha_T, IV, T, sum, \alpha_{end}$
Hop Related (Section III):	
htariffs	tariffs offered by FN which are supported by Hop
PID(Hop)	pseudonym ID of Hop, i.e., a permanently fixed random string shared with HN
α	payment chain used between Hop and FN
β	payment chain used between MD and FN
γ	payment chain used between MD and Hop
c	Payment info vector. $c = (IV_\beta, \beta_T, \beta_{T-d}, IV_\gamma, \gamma_T, \gamma_{T-d},$ selected tariff, offered tariffs)
t_*	All public DH keys $t_* = (t_{GM}, t_{MG}, t_{FM}, t_{MF}, t_{HopM}, t_{MHop})$

TABLE I
NOTATIONS

Initialization of Tick payment: MD generates payment data by randomly choosing α_0, IV, and then calculating a payment chain α, where $\alpha_i = H_{IV}(\alpha_{i-1}), i \in \{1, \ldots, T\}$, where T is given by the tariff, and IV and α_0 are randomly chosen by the MD. MD commits to the payment by calculating a signature on α_T, IV, the ID(FN), and the selected tariff in message 4 of the setup protocol, so that FN can later prove to HN that it was MD who created the payment for FN. FN verifies the first tick α_{T-d} by testing $H_{IV}^d(\alpha_{T-d}) = \alpha_T$. If successful, FN provides service to MD until the first service interval is used.

For **Later Service Intervals**, e.g., after i ticks, FN will request d new tick payments as illustrated in Figure 2. After MD has sent the last tick α_{T-i-d}, FN verifies that $H_{IV}^d(\alpha_{T-i-d}) = \alpha_{T-i}$. Both parties increase i by d and store i. This can be repeated until $i > T$. After $\frac{T}{d}$ service intervals, all ticks have been used and the connection aborts. Therefore, T limits the amount of service used in a session. Note that T is chosen by FN.

d ticks correspond to a small amount of money called unit, which should be chosen so small that losing it is not a problem, because at most one unit will be lost when the connection aborts unexpectedly, or when FN provides no service, e.g., d ticks could be worth 0.05 EUR or less. We use $d = 1$ in our implementation.

C. Basic Clearing Protocol

There are two separate clearing protocols that differ in the information that is kept private from HN.

The **abort protocol**, as shown in Figure 3 is started by FN when MD does not actively terminate the connection, or in general when MD fails to initiate the graceful ending protocol (discussed later). FN has obtained the signature from MD in message 5 during the connection setup protocol described in Section II-A, and the last tick payment α_{T-i} during the tick payment phase described above. By sending the setup messages 3, 4, 5, b, and α_{T-i}, FN can prove to HN that MD is a customer of HN, the amount of provided service, and the selected tariff, which results in the amount to be paid. HN will reimburse FN and charge MD. Regarding privacy, 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.

The **graceful ending protocol**, as shown in Figure 4 is started by MD when it does not want to use further service. At the end of a connection with an amount of service used worth sum, MD creates a payment string for FN,

 ISBN: 978-1-61208-229-5

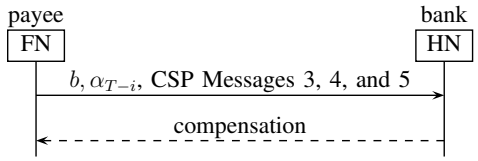

Fig. 3. Basic Clearing Phase after Abort. CSP = Connection Setup Protocol

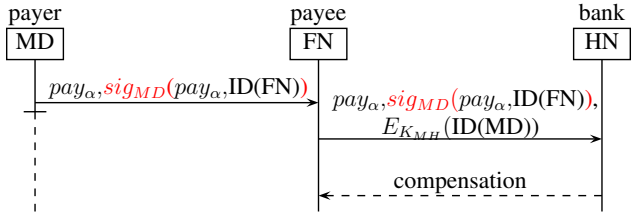

Fig. 4. Basic Clearing Phase with Graceful End

$$pay_\alpha = \alpha_T, IV, T, sum, \alpha_{end},$$

which is used in the ending message pay_α, $sig_{MD}(pay_\alpha$, ID(FN)) for FN. FN will forward this signature to HN. The information contained in this message is sufficient for FN to prove to HN that MD owes FN the amount in question. In the interest of MD's privacy, HN will not obtain knowledge of any tariff or service use details MD and FN have agreed on. As FN cannot verify the signature on pay_α, ID(FN), it keeps the data required to run the abort protocol, so that it can be executed when HN refuses the graceful ending message. E.g., when MD tries to cheat by sending an invalid signature, FN will behave as if MD aborted the connection. Note that given α_i, no one can calculate α_{i-j} for any $j > 0$ because H_{IV} is a preimage resistant hash function. Therefore, new ticks to an existing chain cannot be forged. Due to the nature of tick payment, MD only loses the value of a single (small) service unit when FN stops providing service after MD has paid for it. To avoid HN reconstructing service use from the amount of ticks and the total sum, FN can vary his service interval size, and adjust the price per unit so that the effective price stays constant.

III. Extension to Hops

In this section, we describe our new Hop extension of the protocol suite described in the last section. It allows MDs to act as Hops, i.e., access points for other MDs. Hops will receive a small payment from MD for providing service, and FN will receive the regular payment as if MD was connected without a Hop. Note that the extension is not straight forward, as Hops — as opposed to FNs — do not have a trust relationship with the HNs of other MDs. Also, there is a higher risk that Hops act maliciously than that FNs act maliciously as the later can be considered to care about their reputation as they want to stay in business.

A. Scenario and Requirements

In the following, the term MD is always used for a device that uses a Hop and has no direct wireless connection to FN. The Hop is a regular MD currently connected to FN, and is owned and operated by an end user. MD's home network will be called **GN** (guest network) in the following, and the home network of Hop will be called **HN**. No roaming agreement is required between HN and GN, but both need a roaming agreement with FN.

As a Hop is using resources to provide service to a MD (battery life, system load), an incentive is required for MDs to become Hops. This is achieved by the MD paying a small fee to the Hop with each tick payment. MD also pays the regular fees for the services it uses to FN.

The amount paid by MD to Hop is chosen by FN and advertised in FN's tariff broadcast. Not allowing the Hops to freely choose the amount they earn prevents them from charging disproportionate tariffs from careless MDs, which may ruin FN's reputation as well. Note that a Hop can choose to accept or reject individual tariff options advertised by FN before forwarding them to MD. Depending on the tariffs offered by FN, acting as a Hop might even be a business model, i.e., other providers might deploy fixed devices to act as Hops in highly frequented places along the borders of FN's network coverage.

MDs have to pay more for service used over a Hop compared to a direct connection. If the incentive for Hop would be paid by FN, it would be subtracted from FN's profit, and enable attackers running an MD to pose as both a Hop and an MD at the same time, e.g., by using two devices, and pocketing the Hop incentive themselves. Theoretically, FN could also setup Hops and try to charge MDs more, however, we neither consider this realistic nor an attack per se, as FN can freely set its tariffs anyway.

Our extended roaming protocol suite aims at meeting the following goals:

Sec-1: Authentication and key establishment between MD, Hop, FN, and GN.
Sec-2: MD can avoid a Hop that acted dissatisfactory in the past.
Sec-3: Hop cannot read or modify MD's traffic.
Pri-1: MD must stay anonymous and untrackable to anybody.
Pri-2: Hop must stay anonymous to anybody.
Pri-3: GN must not learn details about MD's and Hop's session with FN.
Pri-4: HN must not learn details about MD's and Hop's session with FN.
Pay-1: Hop will never have to pay for the services MD uses with FN.
Pay-2: FN and Hop will be paid by MD for the services MD uses.
Pay-3: FN and Hop cannot charge more than negotiated with MD.

B. Extended Connection Setup Protocol

The Hop Protocol is illustrated in Figure 5 using the notations from Table I.

 ISBN: 978-1-61208-229-5

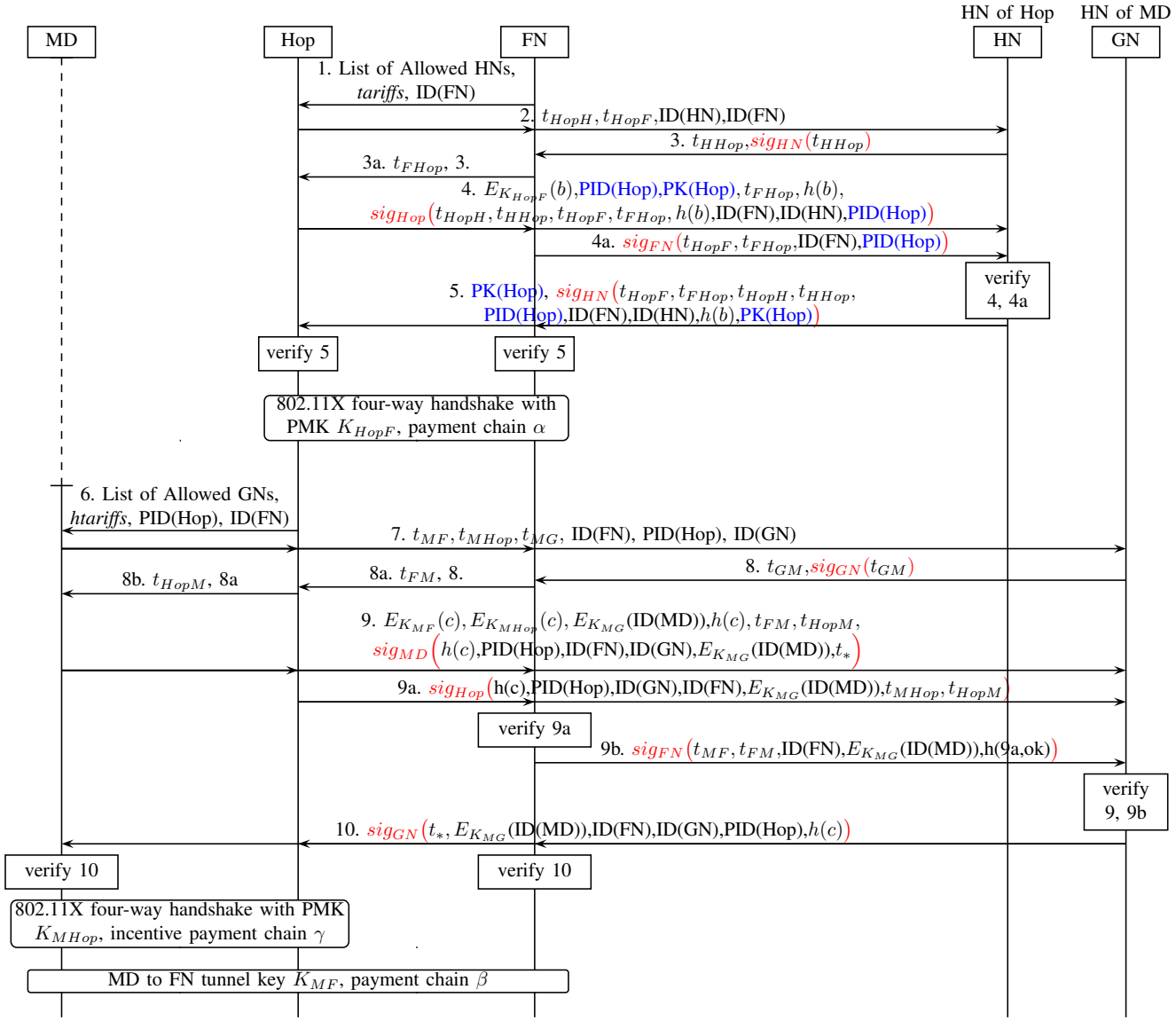

Fig. 5. Extended Connection Setup Protocol. red: signatures; blue: changes to 1 in 1.–5.

1.–5. These messages are similar to the Basic Connection Setup Protocol as discussed in Section II-A, except for the added pseudonym ID of Hop PID(Hop), and its public key PK(Hop). The tariff list now also includes rates indicating how much Hops must be paid. HN confirms that Hop is entitled to act as a Hop by confirming its PID(Hop).

5.–11. These messages contain two entwined runs of the roaming mechanism discussed in Section II-A between the pairs MD, Hop and MD, FN. These are similar to the two-party protocol, but now the Hop uses the static identifier PID(Hop) issued by HN instead of the encrypted identifier $E_{K_{MH}}$(ID(MD)) that MD used in the basic protocol. This enables MD to recognize and avoid certain Hops. Two new tick payment chains β between MD and FN, and γ between MD and Hop are initialized. The mechanism is straightforward and works as in the two-party case. Payment information during the setup protocol is shortened to c in Figure 5.

6. Like FN, the Hop continuously sends a broadcast message, e.g., using a special encoding in the SSID. It contains the pseudonym ID of Hop PID(Hop) issued by HN of Hop, a (possibly) reduced set of tariffs from FN's broadcast called *htariff*, the ID of FN, and a list of allowed GNs (HNs of MDs), which are taken from FN's broadcast (1.).

7. The user of MD selects a suitable tariff. MD chooses DH private values $r_{MHop}, r_{MF}, r_{MG} \in_R \mathbb{Z}_p$, and calculates public $t_{MHop} = g^{r_{MHop}}, t_{MF} = g^{r_{MF}}, t_{MG} = g^{r_{MG}} \mod p$. t_{MHop} is meant for key establishment with Hop, t_{MF} for FN, and t_{MG} for GN. MD sends the IDs of Hop and FN, the public DH values to Hop, and the identifier ID(GN) of its HN so that FN will know where to forward messages 7 to. Hop forwards the message to FN when PID(Hop) is correct. FN verifies that it has a roaming agreement with GN, and forwards the message if it does.

 ISBN: 978-1-61208-229-5

8. GN verifies that it has a valid roaming agreement with FN. GN creates private $r_{GM} \in_R \mathbb{Z}_p$ and public $t_{GM} = g^{r_{GM}} \mod p$ and calculates $K_{MG} = {t_{MG}}^{r_{GM}} \mod p$ for use with MD. t_{GM} is sent to FN.

8a. FN creates private $r_{FM} \in_R \mathbb{Z}_p$ and public $t_{FM} = g^{r_{FM}} \mod p$ and calculates $K_{MF} = {t_{MF}}^{r_{FM}} \mod p$ for use with MD. t_{GM}, t_{FM} are sent to Hop.

8b. Hop creates private $r_{HopM} \in_R \mathbb{Z}_p$ and public $t_{HopM} = g^{r_{HopM}} \mod p$ and calculates $K_{MHop} = {t_{MHop}}^{r_{HopM}} \mod p$ for use with MD. t_{GM}, t_{FM}, t_{HopM} are sent to MD.

9. MD calculates K_{MF}, K_{MHop}, K_{MG}. MD generates the payment data c according to the tariff selected, which contains the payment chains β for FN and γ as incentive for Hop. c also contains the tariffs offered by Hop and an identifier of the tariff selected by MD. MD creates a signature on its encrypted identifier, a hash of c, all the ephemeral DH public parameters t_*, the ID of FN and GN, and PID(Hop). MD sends this signature, its identifier encrypted for GN, the payment data c encrypted for Hop and FN, a hash of c, and the two ephemeral DH public parameters not seen by HN so far t_{FM}, t_{HopM} to GN. This data is required by GN to verify the signature.

9a. Hop verifies $h(c)$. Hop creates a signature on MD's encrypted identifier, the ephemeral DH public parameters Hop used t_{MHop}, t_{HopM}, the ID of FN and GN, and PID(Hop). Hop sends this signature and message 9 to FN.

9b. FN verifies $h(c)$ and the signature of Hop from message 9a using the public key from message 4, which was confirmed by HN in message 5. FN creates a signature on MD's encrypted identifier, the ephemeral DH public parameters FN used t_{MF}, t_{FM}, the ID of FN and GN, and PID(Hop). FN sends this signature, message 9, and 9a to GN.

10. After GN verifies the signature by MD and FN from message 9 and 9b, GN creates a signature on all ephemeral DH values, the identifiers of GN, FN, Hop, and the encrypted identifier of MD, and the hashed payment information $h(c)$, which is sent to FN. FN verifies the signature by GN and forwards it to Hop when the verification succeeds. Hop forwards the message to MD, who verifies GN's signature.

Now that the parties have authenticated, established keys and initialized payment, MD and Hop execute an 802.11X handshake using a derivation of K_{MHop} and the payment chain γ, and MD and FN set up an IPsec tunnel using a derivation of K_{MF} and the payment chain β.

C. Discussion of the Extended Connection Setup Protocol

The Hop connection setup protocol is built on similar goals as to the basic roaming mechanism described in [1], on which we gave a summary in Section II-A. We will now discuss how the security and privacy goals for the extended protocol described in Section III-A are achieved.

Sec-1: Secure authentication and key establishment between MD, Hop, FN, and GN is achieved as all parties include ephemeral public keys from messages 2–3, 7–8 within the signed parts of messages 4–5, 9–10. The signature that cannot be verified directly due to lacking public keys are verified by parties that are trusted by MD (GN verifies FN's signature), Hop (FN is trusted via HN's roaming agreement, FN verifies GN's signature), and GN (FN verifies Hop's signature). FN verifies Hop's signature using the PK(Hop) supplied in message 4 and confirmed by HN in message 5. Therefore, all parties are aware that the other parties are actively participating in the current protocol run. The keys K_{MHop}, K_{MF}, and K_{MG} established during the protocol run are fresh, as the ephemeral public DH parameters are chosen by all parties for only this session. Also, the keys are **exclusive** as they can only be calculated by a party that knows the corresponding private ephemeral DH parameter r corresponding to the public parameter t it sent. Explicit key confirmation is achieved by the encryption of c between MD and Hop, and MD and FN, and by the encryption of ID(MD) between MD and GN. Thus, mutual belief in the keys K_{MHop}, K_{MF}, and K_{MG} is achieved. Note that there is always input from at least one self chosen ephemeral DH value in every signature in the protocol to prevent **reuse of old signatures** by an attacker.

Sec-2: PID(Hop) is sent to MD to achieve **linkability** of Hop to MD. This way, MD is able to avoid using Hop when service has been poor before.

Sec-3: The Hop cannot read or modify traffic between MD and the Internet, because the traffic between MD and FN is encrypted and integrity protected using an IPsec tunnel based on a derivation of the key K_{MF}.

Pri-1: The MD stays anonymous and untrackable to both Hop and FN, as ID(MD) is only sent encrypted with K_{MG}, which is only known to GN.

Pri-2: PID(Hop) is issued by Hop's HN and does not contain a real name, so that Hop stays anonymous, but linkable.

The **verification of MD's signature** on $h(c)$ sent in message 9 is interesting. Only GN is able to verify MD's signature directly. GN signs the $h(c)$ sent by MD in message 10, which can be verified by FN, but not by Hop. Therefore, another mechanism is needed. Hop includes $h(c)$ in its signature in message 9a, which FN verifies. After verifying message 9a and 10, FN knows that MD has encrypted the same c for Hop, FN, and GN.

D. Payment for Hops

The tick payment protocol uses two payment chains β from MD to FN and γ from MD to Hop. The payment chains are bound to the authenticated payer and the intended receiver by MD's signature in message 9 of the Extended Connection Setup Protocol (Figure 5). As shown in Figure 6, FN requests d new ticks after a service interval has been used up by MD. MD is paying to FN and Hop by sending ticks β_i and γ_i.

MD keeps track of its service use so that it cannot be overcharged by FN. Hop keeps track of MD's service use and verifies that payment ticks γ_i arrive in a timely fashion. Hop

 ISBN: 978-1-61208-229-5

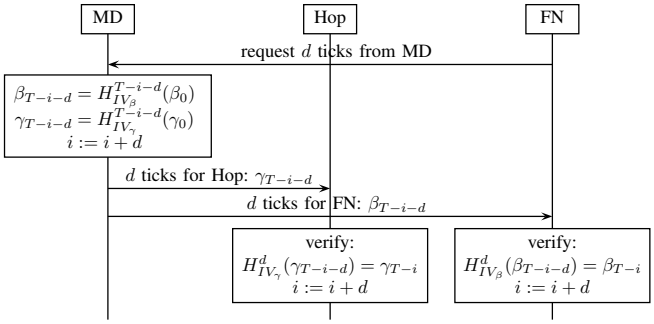

Fig. 6. Extended Tick Payment Protocol

and FN verify the received ticks in the same way using H_{IV}. The Hop does not have to request payment itself, as the tariff chosen by MD includes the incentive paid to Hop, which uses the same unit size (time or data volume) and maximum number of service intervals T.

E. Extended Clearing Protocols

FN is clearing the payments α from Hop to FN as described in Section II-C. Only the payments from MD to FN β and from MD to Hop γ are cleared using the extended clearing protocols. As for the basic protocol, there are two variants, depending on whether or not MD sent a graceful ending message.

The Extended Abort Protocol is executed when MD aborts the connection as shown in Figure 7. The messages from the extended connection setup protocol are used to prove to GN that MD has committed on the payment chains to pay FN and Hop, as they contain MD's signature on c and GN's signature of $h(c)$. Hop and FN disclose c to GN, who can verify it using $h(c)$. The last tick payments β_{end} and γ_{end} and the tariff data from c allow FN and Hop to prove the amount to be paid.

By disclosing c and the last tick payment, the GN will obtain knowledge of the tariffs offered by FN, the tariff MD has agreed on, and the amount of service used by MD, which can be avoided by MD sending an ending message.

As the Hop can lose its wireless link at any time, e.g., when the user forgets to log off and leaves the range of FN's wireless network, the abort clearing protocol can be executed in regular intervals with a delay flag so that FN will not contact GN immediately.

The Extended Graceful Ending Protocol is shown in Figure 8. When MD does not want to use further service, it sends an ending message for Hop, which is relayed to FN. The message is based on two signed payment strings,

$$pay_\beta = \beta_T, IV_\beta, sum_\beta,$$
$$pay_\gamma = \gamma_T, IV_\gamma, sum_\gamma,$$

to pay for services MD used itself. $\beta_T, \gamma_T, IV_\beta, IV_\gamma$ are random values that the payment chain is based on. They are sent to prevent double spending so that Hop and FN cannot clear the same payment chain twice. sum_β and sum_γ is the amount to be paid to FN and Hop in a real world currency. Hop forwards message 1, but also the last tick payment Hop received γ_{end} to FN. FN is forwarding message 1 to GN along with MD's encrypted identifier used in the extended connection setup protocol. GN verifies the signature of MD and acknowledges the claim. GN will credit FN, possibly later at the end of a billing period. GN cannot credit Hop, because GN might not have a roaming agreement with HN. Therefore, GN sends payment for Hop to FN, and in message 4 FN forwards it to HN, who credits Hop in message 5.

The Hop has included γ_{end} in message 1a. to FN so that FN can execute the Abort Clearing Protocol without contacting the Hop again, should GN reject MD's signature from message 1. The other information c, β_{end} and the Setup Message 7, 8, 9, 10 are already known to FN from the Extended Setup Protocol. Hop includes c again to identify the connection with MD.

F. Discussion of the Extended Payment Protocol

The tick payment chains for MD to Hop and MD to FN payments are both securely initialized in the Extended Connection Setup Protocol. Each of the payment chains provides the properties discussed in Section II-B such that the chains cannot be forged, payments cannot be stolen and cleared by someone else, and payments cannot be used or cashed more than once. We will now discuss how the payment security and privacy goals described in Section III-A are achieved.

Pri-3: GN does not learn any details about MD's and Hop's session with Hop and FN when the extended graceful end protocol is executed correctly, as the payment strings pay_β and pay_γ only contain the amount to be paid and the party to be paid. However, if GN would wrongfully reject MD's signature, it can force FN to reveal the details. FN would detect this attack if it happens often and could cancel the roaming agreement with GN.

Pri-4: HN does not learn any details about MD's and Hop's session with Hop and FN, because HN only receives ID(GN) and the payment strings, which only contain the sum to be paid, Hop's PID, and ID(GN).

Pay-1: The Hop is assured that it will not have to pay for the services MD uses with FN, because MD is using its own payment chain β with MD, and FN counts the service used by MD separately from those used by Hop. When FN tries to overcharge Hop, Hop can abort the connection upon receiving a wrongful tick payment request. The maximum risk for Hop is the value of a single tick payment.

Pay-2: FN and Hop are convinced that they will be paid by MD for the services MD uses, because MD has committed on one payment chain each for Hop and HN in message 9, which was confirmed by GN in message 10, which was confirmed to Hop by FN forwarding message 10 and providing subsequent service to MD. Every single tick payment sent by MD can be verified by Hop and FN immediately, and clearing does not rely on MD's cooperation.

Pay-3: FN and Hop cannot charge more than negotiated with MD. They cannot calculate additional tick payments in pay_β and pay_γ, because H_{IV} is a one-way function. FN and Hop cannot clear the same connection twice, as β_T, IV_β and/or γ_T, IV_γ will be the same as those cleared before, which will be detected and rejected by GN.

 ISBN: 978-1-61208-229-5

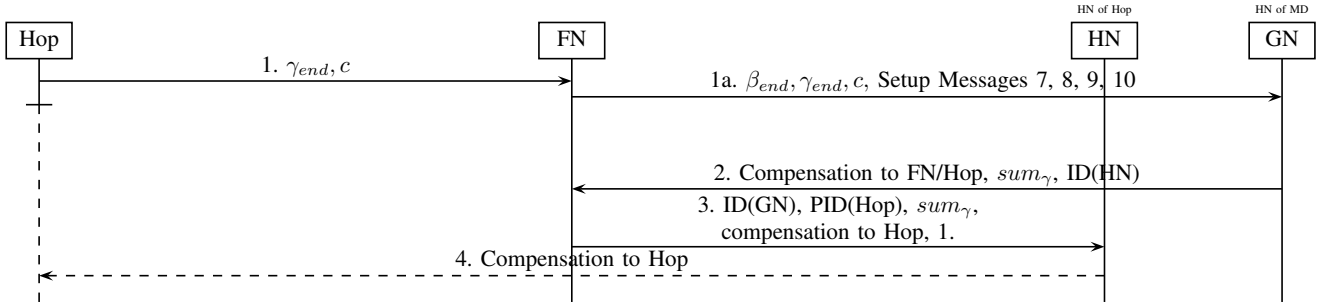

Fig. 7. Extended Abort Clearing Protocol

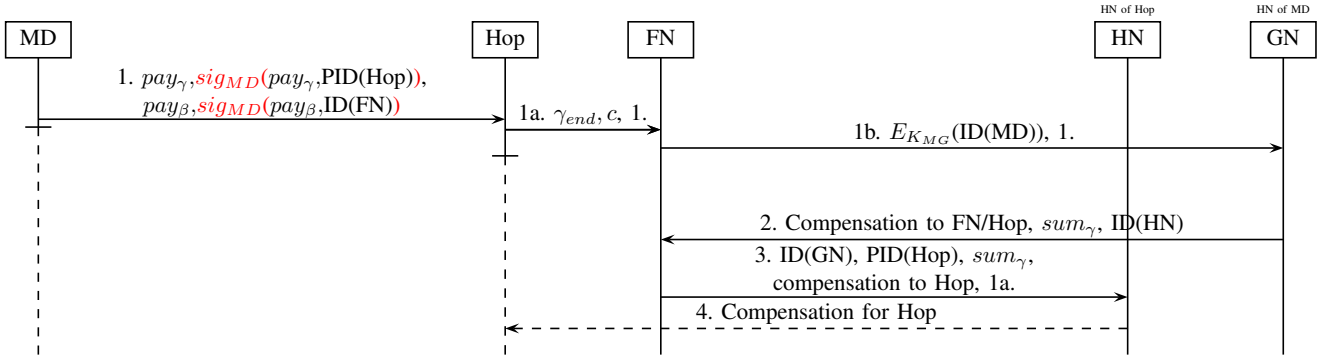

Fig. 8. Extended Clearing with Graceful End

IV. Related Work

In this section, we will compare the proposed extended solution to existing academic and non-academic roaming approaches and show that none of these approaches simultaneously meets all the features our solution offers.

A. Roaming Solutions without Hops

3GPP [5] 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 by dialing special codes on the MDs, but no on-demand tariff shaping for operators. Despite the TMSI mechanism, active attackers are able to track mobile devices, HN always obtains all connection details, and FN always obtains the subscriber's longterm identifier.

A variety of roaming protocols exist that do not support payment initialization and tariff negotiation. These include for example the protocol suggested in [6], [7], [8], [9], [10], [11], [12], [13], existing solutions like the Extensible Authentication Protocol [14] in 802.11i WLANs, and the recently launched PassPoint by the Wi-Fi Alliance and Wireless Broadband Alliance [15]. We will only discuss protocols in more detail that include secure payment as well.

In Buttyán-Hubaux [16], a customer care agency provides tickets to mobile devices. These tickets can be used by the mobile device to roam to different networks. The protocol is preserving the privacy of the user to the visited network, but not to the customer care agency. 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.

EAP-TLS-KS [17] uses a key splitting unique for each FN, distributed decryption, and distributed signatures for mutual authentication of MD and FN, which trades network round trips for additional cryptographic operations. EAP-TLS-KS can include any accounting method based on the Buttyán-Hubaux-Protocol.

B. Roaming Solutions with Hops

The solutions discussed so far did not discuss connections established over other parties (Hops). This research area is generally covered by wireless mesh networks (WMNs), where independent stations are also routers, even when they have no other network interface. Our work is not part of a WMN architecture, as it is limited to a single Hop.

ARSA [18] is a roaming solution based on identity based cryptography, which is not widely available for implementation. Brokers, connected to each other and to the operators, are used so that no agreements between operators are needed. 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. Tariffs are announced, but only a single tariff priced per data volume is available per operator. Our approach avoids brokers, as all the participants would have to settle on the same one and would have to pay them a share, and rather uses the HN with a connection to the FN and a bilateral agreement, which are easier to set up.

The solution by Pierce-O'Mahony [19] combines roaming in GSM multi-mop networks with multiparty micropayment. Two MDs are connected to each other over a number of hops, and the initiator pays a large amount to the first hop, which keeps some of it, and forwards the rest to the next

 ISBN: 978-1-61208-229-5

hops, who repeat this process. The system is prepaid. MD's demand regarding QoS influences the tariff, but MD cannot directly choose a tariff, as the tariffs are chosen by the hops. The system is single-operator, which is hard to establish for a large audience in the real world. There is no protection against tracking of MD.

Jakobsson et al. [20] encourage collaboration in multi-hop networks using probabilistic micropayment, where the operator is capable of detecting and punishing misbehaving stations. Hops between MD and base station are paid for a random fraction of the packets they forward. The solution does not address tariffs, authentication, and privacy.

V. Conclusion and Future Work

We have presented an extension to the protocol suite in [1] for secure and privacy preserving roaming and payment in WLAN to include regular user devices acting as Hops, i.e., as relay stations to enhance the area where service is available. The privacy and security goals of the basic protocol suite are retained except for tracking of the Hop, which is a design choice to enable MDs to avoid certain Hops. The proposed solution retains tariff flexibility for users, Hops, and operators, as users can select a tariff that fits their demands. There is an incentive for Hops to provide service to MDs, and Hops only have to support tariffs they deem worthy. Operators are still free to modify their offered tariffs at any time. The clearing protocols ensure that all stations can be billed and credited correctly even when they disappear without advance notice or when they try to cheat.

We currently create a new EAP method for *hostapd* access points on Laptops, and a client for Linux and Android smartphones to implement the original protocol, and aim to implement the extension described in this paper as well. The client will be user friendly and recommend tariffs based on different Internet usage profiles, e.g., e-mail, chatting, surfing, and video chat.

We hope that our solution creates better WLAN coverage, fosters competition between paid WLANs operators, and ends insecure and cumbersome setup procedures.

VI. Acknowledgments

This work has been supported by the UMIC Research Centre, RWTH Aachen University. We want to thank the reviewers of Information Security Conference 2012 for providing insightful comments and discovering an attack on MD's anonymity in the original protocol.

References

[1] J. Barnickel and U. Meyer, "Security and privacy for wlan roaming with per-connection tariff negotiation," IEEE Conference on Local Computer Networks, 2011, pp. 338–353.

[2] WeFi, http://www.wefi.com/, retrieved August 1st, 2012, archived at http://www.webcitation.org/69Q5bO0zg.

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

[4] T. Pedersen, "Electronic Payments of Small Amounts," Security Protocols, LNCS 1361, pp. 59–68, 1997.

[5] *3GPP TS 32.240 (Release 9): Telecommunication management; Charging management; Charging architecture and principles*, 3GPP Std., 2009.

[6] P. Bahl, S. Venkatachary, and A. Balachandran, "Secure wireless internet access in public places," IEEE International Conference on Communications, 2001.

[7] L. Buttyán, L. Dóra, F. Martinelli, and M. Petrocchi, "Fast certificate-based authentication scheme in multi-operator maintained wireless mesh networks," Journal of Computer Communications, Volume 33 Issue 8, pp. 907-922, May 2010.

[8] K. Bayarou, M. Enzmann, E. Giessler, M. Haisch, B. Hunter, M. Ilyas, S. Rohr, and M. Schneider, "Towards certificate-based authentication for future mobile communications," Wireless Personal Communications 29, pp. 283–301, 2004.

[9] J. Gu, S. Park, O. Song, J. Lee, J. Nah, and S. Sohn, "Mobile PKI: A PKI-Based Authentication Framework for the Next Generation Mobile Communications," Proceedings of ACISP'03, volume 2727 of LNCS, 180–191, 2003.

[10] T. Heer, S. Li, and K. Wehrle, "PISA: P2P Wi-Fi Internet Sharing Architecture," Seventh IEEE International Conference on Peer-to-Peer Computing, P2P2007, pp. 251–252, 2007.

[11] D. Leroy, G. Detal, J. Cathalo, M. Manulis, F. Koeune, and O. Bonaventure, "SWISH: Secure WiFi sharing," Computer Networks, Volume 55, Issue 7, 16 May 2011, pp. 1614–1630.

[12] M. Long, C.-H. Wu, and J. D. Irwin, "Localized authentication for wireless lan internetwork roaming," IEEE Conference on Wireless Communications and Networking, WCNC, pp. 496–500, 2004.

[13] L. Salgarelli, M. Buddhikot, J. Garay, S. Patel, and S. Miller, "Efficient authentication and key distribution in wireless IP networks," IEEE Wireless Communications Magazine Volume 10, Issue 6, pp. 52–61, December 2003.

[14] B. Aboda, D. Simon, and P. Eronen, "Extensible Authentication Protocol (EAP) Key Management Framework," IETF RFC 5247, 2008.

[15] WiFi Alliance, "Frequently Asked Questions on Wi-Fi CERTIFIED Passpoint," http://www.wi-fi.org/sites/default/files/uploads/20120626_Passpoint_FAQ.pdf, retrieved August] 2nd, 2012, archived at http://www.webcitation.org/69IOmvHOm.

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

[17] U. Meyer, J. Cordasco, and S. Wetzel, "An approach to enhance inter-provider roaming through secret sharing and its application to WLANs," Proceedings of the 3rd ACM international workshop on Wireless mobile applications and services on WLAN hotspots (WMASH), pp. 1–13, pp. 1–13, 2005.

[18] Y. Zhang and Y. Fang, "A secure authentication and billing architecture for wireless mesh networks," Wireless Networks, Volume 13, Number 5, pp. 663–678, 2007.

[19] M. Pierce and D. O'Mahony, "Flexible real-time payment methods for mobile communications," IEEE Personal Communications, Volume 6 , Issue 6, pp. 44–55, 1999.

[20] M. Jakobsson, J. Hubaux, and L. Buttyán, "A Micro-Payment Scheme Encouraging Collaboration in Multi-hop Cellular Networks," Financial Cryptography, 7th International Conference, FC 2003, pp. 15–33, 2003.

 ISBN: 978-1-61208-229-5