ISP Offload Infrastructure to minimize cost and time deployment

Daniel Migault*, Daniel Palomares*, Emmanuel Herbert*, Wei You*, Gabriel Ganne*, Ghada Arfaoui†, Maryline Laurent†
*France Telecom, †Institut Télécom, Télécom SudParis, CNRS Samovar UMR 5157

***Abstract*—To face the huge demand on mobile traffic, ISPs are looking to offload traffic of their Radio Access Network to WLAN. Currently I-WLAN is the proposed offload architecture by 3GPP which tunnels the traffic to a Security Gateway. This paper proposes for ISPs an *ISP Offload Infrastructure* which minimizes the infrastructure cost deployment, and which can be deployed in a very short term. The *ISP Offload Infrastructure* classifies the EU traffic into 3 distinct classes and assigns each class a specific and adapted offload architecture: *ForWarD Architecture* (FWDA), *Offload Service Architecture* (OSA) and *Offload Access Architecture* (OAA). This paper shows how to deploy each Offload Architecture by using SCTP in conjunction to MOBIKE(-X) or only MOBIKE(-X). Then we measure how each Offload Architecture may affect the EU experience, and provide recommendations on how to deploy and implement the *ISP Offload Infrastructure*.**

***Index Terms*—IPsec, IKEv2, MOBIKE, MOBIKE-X, Mobility, Multihoming, Offload**

I. Introduction

One of today's ISPs challenge is to deal with an increasing demand for Mobile traffic. By the end of 2012, mobile-connected devices are expected to exceed the number of people on earth to reach 1.4 mobile per capita in 2016. Moreover by 2016 the global mobile traffic is expected to be 18 times larger than in 2011 [5]. Not being able to handle this traffic represents a loss of revenues for ISPs as a large part of their revenues are provided by Services. To overcome this traffic growth, [7], [12], [19], [24] agree that upgrading current 3G technology to 4G technology and scaling current Radio Access Network (RAN) costs about 5 times more than offloading the traffic to Wireless LAN (WLAN).

Offload Architectures must be designed to move the End User (EU) from RAN to WLAN, to move between WLAN Access Points and to move back from WLAN to RAN. Because RAN and WLAN have different levels of trust Mobility protocols are associated to Security Protocol. 3GPP specifies Interworking Wireless LAN (I-WLAN) [1] an offload architecture which overcomes the different levels of trust between WLAN and RAN, by tunneling the traffic into an encrypted IPsec tunnel to a Security Gateway. To move between WLAN Access Points, I-WLAN uses MOBIKE [6], the Mobility and Multihoming IPsec extension. To move between RAN and WLAN, I-WLAN uses Mobile IP [20]. Most ISPs have neither deployed I-WLAN, nor a MIP infrastructure. In fact, Upgrading the 3G infrastructure to 4G is costly. Moreover MIP concentrates all the EU in the ISP Network, which represents a non trivial evolution and requires Network provisioning. Hence, ISPs are looking for alternative offload architectures that reduce the deployment costs and that can rapidly be deployed.

To reach these goals, this paper proposes *ISP Offload Infrastructure* considers the EU traffic and defines 3 different classes associated to a specific and adapted Offload Architecture. Traffic with no need for Security is associated to the ForWarD Architecture **FWDA**. FWDA forwards the traffic directly from the WLAN Access Point to the Internet. Traffic for specific ISP Services with End-to-End security is associated to the Offload Service Architecture **OSA**. The remaining traffic that needs to be protected but that cannot be protected via End-to-End security is tunneled to a Security Gateway with the Offload Access Architecture **OAA** —cf. figure 1.

We use IPsec for the Security protocol. For Mobility and Multihoming protocols, we consider in this paper SCTP [27] and MOBIKE [6] / MOBIKE-X [15] IKEv2 Mobility Multihoming extensions. SCTP provides End-to-End Mobility, and does not require the ISPs to deploy any infrastructure. Furthermore it makes Mobility independent of Security, and thus makes Mobility between RAN and WLAN possible. On the other hand it requires that applications or EU terminals to be SCTP enabled. Although we believe, making terminals or applications SCTP enable does not represent a major cost, we also show how MOBIKE(-X) makes Mobility between RAN and WLAN possible. For Mobility within the WLAN both OAA and OSA use MOBIKE(-X).

This paper is organized as follows: Section II positions our work. Section III describes the FWDA, OSA and OAA architectures and the involved protocols, i.e. SCTP [27] and MOBIKE(-X) [6], [15]. Section IV provides different ways to deploy FWDA, OSA and OAA for SCTP and non SCTP traffic and section V measures how Mobility with the various configurations interrupts the communication and thus impacts the EU experience. Then, we provide recommendations for deploying the *ISP Offload Infrastructure* and section VI proposes a deploying plan as well as future work.

II. Related Work & Position of Our Work

Our paper proposes an Offload Architecture that minimizes the deployment costs for the ISPs, and improves the current I-WLAN. [2] describes how IKEv1 establishes an IPsec SA with the multiple IP addresses of the SCTP association. MOBIKE(-X) is based on IKEv2 and [2] does not consider dynamic IP address management. Other pieces of work [3], [4], [8], [13],

[30] evaluate different ways to secure SCTP communications and design TLS based protocol specific to SCTP: *Secure - SCTP* and *Secure Socket SCTP*. One of the reason the papers rejected IPsec is the lack of Dynamic Address Configuration flexibility. However, none of them considers performance measurements for Multihoming and Mobility operations. Our work considers MOBIKE-X which is not SCTP specific and measures performances over Mobility and Multihoming.

[18] analyses a Home Node B in a I-WLAN/3GPP architecture, with multiple WLAN/WIMAX/UMTS interfaces that use SCTP over MOBIKE so to select the best interface. This work differs from ours since Multiple Interfaces are never used for Soft Handover which is reported as a missing feature. Note that MOBIKE-X addresses that problem.

We give a special attention to HIP [16], [17] that provides both IPsec security and Mobility Multihoming facilities. However, HIP suffers from two drawbacks: 1) HIP breaks current IP oriented communications and 2) does not provide non IPsec secured communications, which on RAN adds an unnecessary security and bandwidth overhead.

As mentioned earlier Mobility and Multihoming can be performed at different layers [21]. IPsec does it at Layer 2 with the TUNNEL mode, SCTP does it at Layer 4.

III. Offload: Architectures & Protocols

Mobility and Multihoming operations are closely linked to security in the case of offload because the EU interacts between networks with different levels of trust, and thus, different security requirements. Mobility and Multihoming Security Requirements are fulfilled if the EU is able to:

1) Move a communication from RAN to WLAN.
2) Move a communication between WLAN Access Points.
3) Move a communication from WLAN to RAN.
4) Provide Alternate IP addresses to recover from a connection fail over.

These Requirements are fulfilled for each type of traffic and each FWDA, OSA and OAA architectures. Furthermore for a given architecture Mobility may be handled by various protocols (SCTP, MOBIKE(-X), Application) in various ways (Soft Handover, Hard Handover). For each case, we measure how it impacts the EU experience so that ISPs can choose the appropriate way to offload the EU traffic.

Section III-A presents FWDA, OSA and OAA. Then section III-B presents SCTP which provides Multihoming and Mobility features at the transport layer. Section III-C presents the different IPsec Multihoming and Mobility extensions: MOBIKE [6] and MOBIKE-X [15]. Then we compare and position SCTP, MOBIKE and MOBIKE-X for Mobility and Multihoming handling.

A. *Offload Architectures: FWDA, OSA and OAA*

FWDA: Public Traffic that does not require any protection, or traffic that is already protected at upper layers is directly forwarded by the WLAN Access Point to the Internet, and is not redirected on the ISP Network (cf. figure 1).

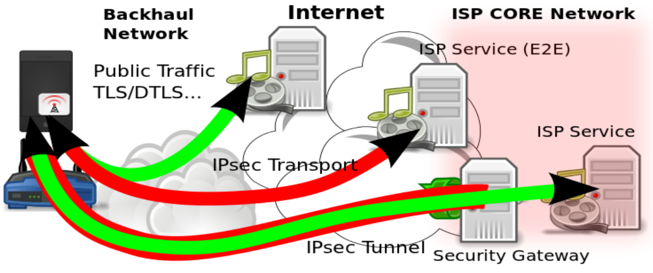
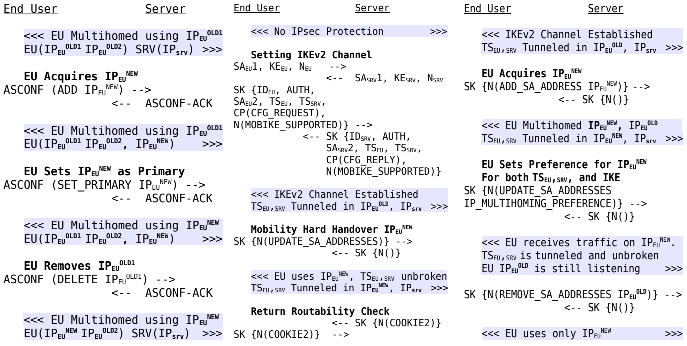


Fig. 1. ISP Offload Infrastructure

OSA: provides End-to-End connectivity between the EU and the Service and uses the IPsec TRANSPORT mode (cf. figure 1). To the difference with OAA where all the EU traffic is offloaded, in OSA, each Service offloads its own traffic. Advantages of OSA are 1) Offload is adapted to the Service and avoids multiple layer encryptions. 2) OSA provides End-to-End Security which reduces the load especially on ISP CORE and backhaul network. At last 3) OSA reduces the Security Overhead by not only reducing the traffic that needs to be IPsec secured, but also by using TRANSPORT mode rather than the TUNNEL mode. OSA uses IPsec TRANSPORT mode which reduces the number of bytes to be encrypted, as well as the networking overhead required by encapsulation.

OAA: tunnels the EU traffic on the WLAN to a Security Gateway using IPsec TUNNEL mode as presented in figure 1. A Mobility protocol other than MOBIKE(-X) is required because MOBIKE(-X) only works for IPsec protected communication. To the difference with I-WLAN [1], OAA uses SCTP as the Mobility protocol to move from RAN to WLAN instead of MIP. Thus ISPs don't have to deploy any infrastructure.

B. *SCTP*


End User
Server
<<< EU Multihomed using IP_{EU}^{OLD1} EU(IP_{EU}^{OLD1} IP_{EU}^{OLD2}) SRV(IP_{srv}) >>>
EU Acquires IP_{EU}^{NEW}
ASCONF (ADD IP_{EU}^{NEW}) -->
<-- ASCONF-ACK
<<< EU Multihomed using IP_{EU}^{OLD1} EU(IP_{EU}^{OLD1} IP_{EU}^{OLD2}, IP_{EU}^{NEW}) >>>
EU Sets IP_{EU}^{NEW} as Primary
ASCONF (SET_PRIMARY IP_{EU}^{NEW}) -->
<-- ASCONF-ACK
<<< EU Multihomed using IP_{EU}^{NEW} EU(IP_{EU}^{OLD1} IP_{EU}^{OLD2}, IP_{EU}^{NEW}) >>>
EU Removes IP_{EU}^{OLD1}
ASCONF (DELETE IP_{EU}^{OLD1}) -->
<-- ASCONF-ACK
<<< EU Multihomed using IP_{EU}^{NEW} EU(IP_{EU}^{NEW} IP_{EU}^{OLD2}) SRV(IP_{srv}) >>>
End User
Server
<<< No IPsec Protection >>>
Setting IKEv2 Channel
$SA_{EU}1$, KE_{EU}, N_{EU} -->
<-- $SA_{SRV}1$, KE_{SRV}, N_{SRV}
SK {ID_{EU}, AUTH, $SA_{EU}2$, TS_{EU}, TS_{SRV}, CP(CFG_REQUEST), N(MOBIKE_SUPPORTED)} -->
<-- SK {ID_{SRV}, AUTH, $SA_{SRV}2$, TS_{EU}, TS_{SRV}, CP(CFG_REPLY), N(MOBIKE_SUPPORTED)}
<<< IKEv2 Channel Established $TS_{EU,SRV}$ Tunneled in IP_{EU}^{OLD}, IP_{srv} >>>
Mobility Hard Handover IP_{EU}^{NEW}
SK {N(UPDATE_SA_ADDRESSES)} -->
<-- SK {N()}
<<< EU uses IP_{EU}^{NEW}, $TS_{EU,SRV}$ unbroken $TS_{EU,SRV}$ Tunneled in IP_{EU}^{NEW}, IP_{srv} >>>
Return Routability Check
<-- SK {N(COOKIE2)}
SK {N(COOKIE2)} -->
End User
Server
<<< IKEv2 Channel Established $TS_{EU,SRV}$ Tunneled in IP_{EU}^{OLD}, IP_{srv} >>>
EU Acquires IP_{EU}^{NEW}
SK {N(ADD_SA_ADDRESS IP_{EU}^{NEW})} -->
<-- SK {N()}
<<< EU Multihomed IP_{EU}^{NEW}, IP_{EU}^{OLD} $TS_{EU,SRV}$ Tunneled in IP_{EU}^{NEW}, IP_{srv} >>>
EU Sets Preference for IP_{EU}^{NEW}
For both $TS_{EU,SRV}$, and IKE
SK {N(UPDATE_SA_ADDRESSES IP_MULTIHOMING_PREFERENCE)} -->
<-- SK {N()}
<<< EU receives traffic on IP_{EU}^{NEW}. $TS_{EU,SRV}$ is tunneled and unbroken EU IP_{EU}^{OLD} is still listening >>>
SK {N(REMOVE_SA_ADDRESSES IP_{EU}^{OLD})} -->
<-- SK {N()}
<<< EU uses only IP_{EU}^{NEW} >>>

(a) SCTP Soft Hand-Over (b) MOBIKE(-X) Hard Hand-Over (c) MOBIKE-X Soft Hand-Over

Fig. 2. SCTP / MOBIKE(-X) Mobility

The main advantages of SCTP [27] are that 1) it provides Mobility and Multihoming features for the EU without requiring the ISPs to deploy any infrastructure. Furthermore 2) SCTP is the most mature Mobility and Multihoming with Kernel and User Land implementations, which eases the deployment of SCTP either within the terminal Operating System or within the applications.

With Multihoming, SCTP can initiate a communication with multiple IP addresses - one Primary, one or multiple Alternate. In case the Primary IP address is not reachable, the communication switches to the Alternate. SCTP Mobility features are based on Multihoming and Dynamic Address Reconfiguration [28] and makes Soft Handover possible, as shown in figure 2a. Soft Handover [23] consists in changing an Alternate IP address that is expected to receive the traffic to a Primary IP address. On the other hand, SCTP cannot perform Hard Handover, and Mobility with SCTP requires at least two Interfaces.

With SCTP Kernel-based *LKSCTP* [14] and user land (*sctplib* [26]) implementations, ISPs can provide terminals with SCTP enable kernels, and for terminals that are non SCTP enable —either old terminal, or terminal provided by other ISPs —ISPs can provide applications that are SCTP enable. Note that porting TCP applications to SCTP is quite easy with tools such as *withsctp* from *lksctp-tools*.

Although SCTP does not present major deployment issues, there are still a few complications to overcome. First ISPs must maintain different TCP and SCTP application versions, then some applications like FTP interacts closely with IP address, and so cannot easily rely on the SCTP Mobility and Multihoming facilities. At last NAT, firewalls proxies have not yet been configured for SCTP.

For the Mobility and Multihoming protocol we take advantage of MOBIKE designed for OAA only. MOBIKE-X is the MOBIKE extension designed to enhance and extend Mobility and Multihoming features for both OAA and OSA. However, MOBIKE and MOBIKE-X only provide Mobility and Multihoming for EU with IPsec protected links, which may not be sufficient, for example, when the EU moves from RAN to WLAN. In that case, SCTP may be considered.

C. IPsec, MOBIKE and MOBIKE-X

IPsec architecture [10] defines at least two databases: the Security Policy Database (SPD) and the Security Association Database (SAD). The SPD defines which Traffic Selectors (TS) must be BYPASSed, DISCARDed or PROTECTed and how the protection must be applied: encryption algorithms, IPsec mode (TUNNEL / TRANSPORT) and in the case of TUNNEL mode what is the Security Gateway. IKEv2 [9] is the protocol that negotiates the Security material and registers it in the SAD. Because IPsec designates multiple protocols, and because changing the outer IP address in the TUNNEL mode results as a side effect in moving an IPsec protected communication, IPsec Mobility and Multihoming are often confusing. MOBIKE [6] defines Mobility and Multihoming for IKEv2 and for updating the SPD and SAD of an IPsec communication protected with the TUNNEL mode with a single Interface. MOBIKE-X [15] extends MOBIKE for the TRANSPORT mode, and for Multiple Interfaces.

Let an EU with a single Interface, protecting a communication using the TUNNEL mode. As presented in figure 2b, when the EU changes its IP address, it sends an UPDATE_SA_ADDRESSES message to the Security Gateway to updates the IKE_SA, as well as to change the outer IP addresses of the EU Tunnel. Note that TS are not modified, and thus SPD as well as SAD indexes are not modified. MOBIKE Mobility results in a Hard Handover, which may result in larger packet loss compared to Soft Handover. Multihoming with MOBIKE consists in providing Alternate IP addresses, and if one peer detects the other is not reachable on its Primary IP address, then it sends an UPDATE_SA_ADDRESSES message to proceed to a Mobility operation.

MOBIKE-X [15] extends MOBIKE Mobility features to TRANSPORT mode, and Multihoming with Multiple Interfaces so to make possible Soft Handover as illustrated in figure 2c. Unlike TUNNEL mode, TRANSPORT mode updates the TS, which modifies both the SPD as well as the SAD indexes. Then, with the TRANSPORT mode, updating the database does not move the communication. Only the IPsec rules are updated and Mobility MUST be performed by Mobility protocol like SCTP. MOBIKE-X also considers Multiple Interfaces and makes possible to ADD or REMOVE an IP address for a given SP/SA. With the TUNNEL mode, ADDing and outer IP address means that IPsec is configured for receiving and sending traffic on both IP addresses. Similarly, with the TRANSPORT mode, ADDing an IP address means that the applications can send datagram on two distinct Interfaces.

IV. Deploying FWDA, OSA and OAA

The *ISP Offload Infrastructure* defines 3 different classes of traffic and associates each class to an offload architecture. FWDA is associated to traffic without any security requirements, OSA for traffic that provides End-to-End security, and OAA that tunnels all remaining traffic that needs to be protected (cf. figure 1). When possible, Mobility is handled with MOBIKE(-X). However MOBIKE(-X) provides Mobility only for IPsec with TUNNEL mode protected links, and so cannot deal with FWD and OSA. SCTP can deal with Mobility, and section IV-A shows how FWDA, OSA and OAA can be deployed by combining SCTP and MOBIKE(-X). On the other hand, there may be multiple reasons an ISP does not want to deploy SCTP on its EU terminal or on its application. In that latter case, we detail in section IV-B, how ISPs can still provide an infrastructure based on MOBIKE(-X), and/or applications ability to deal with Mobility. The performance measurements of the two alternatives in section V will provide inputs for ISPs to decide whether SCTP worth to be deployed or not. In both sections IV-A and IV-B, we define for FWDA, OSA and OAA how the EU moves between RAN and WLAN as well as between WLAN Access Points.

A. Deploying FWDA, OSA and OAA with SCTP/MOBIKE(-X)

This section supposes the ISP has deployed SCTP and MOBIKE(-X), and details how FWDA, OSA and OAA can

be deployed.
While connected on the RAN, SCTP Mobility and Multihoming features are not used. SCTP Multiple Interfaces ability is used to associate the IP address acquired on the RAN and the WLAN to a given connection. As represented in figure 2a, the EU configures the new Interfaces (authentication, eventually IPsec IKE negotiation...) before sending an ASCONF ADD IP Payload. When the EU is connected through both IP_{RAN} and IP_{WLAN}, it defines its Primary Address to perform a Soft Handover. The EU may choose to REMOVE the old IP address, however, we recommend to keep IP_{RAN} when being offloaded and eventually REMOVEs IP_{WLAN} when it is not reachable any more. SCTP Multihoming feature is used when the EU is connected on both IP_{RAN}, and one or multiple IP^{i}_{WLAN}. When none of IP^{i}_{WLAN} are reachable anymore, then SCTP is used to switch on IP_{RAN}

The way Mobility is handled between various WLAN Access Points varies according to the Offload Architecture
FWDA: Forwards traffic on the Internet. SCTP is used to move the traffic from IP^{OLD}_{WLAN} to IP^{NEW}_{WLAN} with Soft Handover. SCTP Multihoming is also used to prevent breaking the communication if a WLAN Access Point fails. If the EU has only one WLAN Interface, to avoid breaking the SCTP connection, it may performs two Soft Handover from IP^{OLD}_{WLAN} to IP_{RAN}, then ADD IP^{NEW}_{WLAN} with an ASCONF before moving again from IP_{RAN} to IP^{NEW}_{WLAN}.
OSA: provides End-to-End IPsec Security using TRANSPORT mode. With the TRANSPORT mode, MOBIKE-X Mobility features must be used in conjunction of SCTP. More specifically, MOBIKE-X is not used to move the communication, but only to configure IPsec so that IP^{NEW}_{WLAN} is IPsec ready to protect the communication on IP^{NEW}_{WLAN}. Moving the communication from IP^{OLD}_{WLAN} to IP^{NEW}_{WLAN} is performed by SCTP Soft Handover. MOBIKE-X Multiple Interfaces feature is used to prepare the Soft Handover and avoid blocking the communication (cf. figure 2c), and Multihoming is used in case the Primary Address does not work, and Alternate IP address is used. Multihoming works for the IKEv2 application, otherwise, with TRANSPORT, SCTP Multihoming must be used to move the communication from Primary to the Alternate Address.
OAA: The communication is TUNNELed to the Security Gateway, and MOBIKE is used to move within the WLAN with Hard Handover. MOBIKE-X makes Soft Handover possible as presented in figure 2c, which improves the EU experience, by reducing the number of lost packets. MOBIKE(-X) Multihoming works as with OSA, but with the TUNNEL mode, both IKEv2 and the communication are moved to the Alternate Address. MOBIKE(-X) Multihoming is only used with the WLAN, the Alternate IP address is on the RAN, then SCTP Multihoming is used to switch from WLAN to RAN.

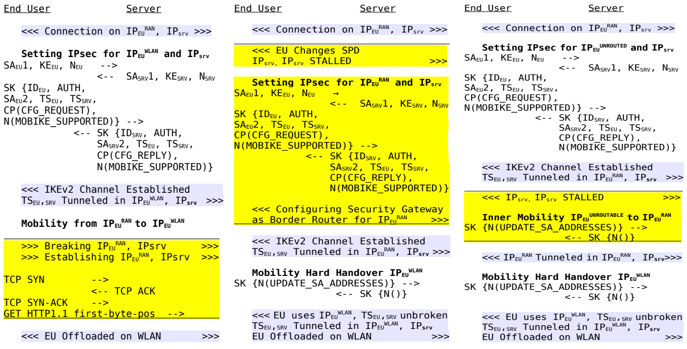
B. Deploying FWDA, OSA and OAA with only MOBIKE(-X)

This section defines how FWDA, OSA and OAA can be deployed without SCTP. In section IV-A SCTP is used to switch from RAN to WLAN. Without SCTP, RAN to WLAN and WLAN to RAN Mobility relies on other mechanisms. Most applications like FTP/HTTP, have session resumption mechanisms that avoids re-downloading a whole file when a connection is restarted —*first-byte-pos* option. Similarly TLS provides also session resumption [11], [22], [25] mechanisms. The main difference with SCTP is that applications perform Hard Handover, whereas SCTP performs Soft Handover. Hard Handover results in longer interruptions and more lost packets. Then, SCTP provides the Mobility and Multihoming framework for all applications whereas without SCTP each application has to deal with its own session resumption mechanism. However, most EU applications have been designed to be robust to network failures, and interrupted sessions: HTTP, HTTPS, FTP have session resumption mechanisms, Peer-to-Peer Files download don't stall when a peer is not reachable, downloading time during Web Browsing is very short, Video Streaming buffers up to a few seconds of videos. As a result, only few real time applications like games, chat, VoIP may be impacted by small interruptions.

FWDA: Mobility and Multihoming is completely handled by applications. If an application cannot handle them, then it should be offloaded with OAA or OSA with TUNNEL mode.
OSA: With TRANSPORT mode, Mobility must be handled by the applications. Thus, moving from RAN to WLAN is performed as in figure 3a, except that TRANSPORT mode is used instead of TUNNEL. However, if the applications cannot provide Mobility features, the ISP may use OSA with TUNNEL mode. This adds a Security overhead, but still provides End-to-End connectivity as well as Mobility and Multihoming features on WLAN. In that case, it is recommended that IP_{RAN} may be globally routable, as detailed for OAA.
OAA: OAA tunnels traffic to a Security Gateway. There are three types of traffic: 1) traffic addressed to mobility aware applications that requires to be encrypted 2) traffic addressed to applications that are not mobility aware applications that requires to be encrypted and 3) traffic of FWDA of applications that are not mobility aware. Figure 3 presents the RAN to WLAN Mobility with OAA, indicating between horizontal lines and with a yellow background the time the communication is stalled. With 1) applications move from RAN to WLAN and from WLAN to RAN (cf. figure 3a). On WLAN Mobility is handled with MOBIKE(-X) as in section IV-A (cf. figure 2b and 2c).
For 2) and 3) MOBIKE-X must be used to move the communication between RAN and WLAN. With 3), the TUNNEL may not be encrypted, IPsec is only used to provide Mobility and Multihoming. To move from RAN to WLAN, the main idea is to establish an IPsec TUNNEL and then use MOBIKE-X to move to the WLAN. The EU modifies its SPD from BYPASS to PROTECT for the given traffic,

and initiates an IKE negotiation. The Security Gateway may be configured with a light authentication, since the EU has been authenticated by the RAN. Then the Security Gateway must configure the ISP CORE network to become a border router for the IP_{RAN}. In fact, the EU encapsulates between IP_{RAN} and $IP_{SECURITY\,GATEWAY}$ the traffic from IP_{RAN} to IP_{SERVER}. IP_{RAN} and IP_{SERVER} are designated as Traffic Selectors (TS). The Security Gateway decapsulates the traffic and sends it to IP_{SERVER} on the Internet. In return, when the Server responds to IP_{RAN}, the IP datagram must be routed to the Security Gateway so that it can encapsulate it back to the EU. Once the IKEv2 negotiation is finished and the SA configured, the EU can use MOBIKE(-X) Multihoming / Mobility mechanisms to move on WLAN. On WLAN, Traffic Selectors are not modified, only the Tunnel outer IP addresses are modified. This scenario is presented in figure 3b. Note that IP_{RAN} must be routable and that the connection is stalled during the whole IKEv2 negotiation. On the other hand MOBIKE can be used for that scenario, even though MOBIKE-X may be preferred for Multiple Interfaces and Soft Handover. Figure 3c shows how to take advantage of MOBIKE-X to avoid stalling the communication during the IKEv2 negotiation. MOBIKE-X does not require any Routing configuration in the ISP Network, nor IP_{RAN} to be globally routable. However, using non globally routable IP_{RAN} results in breaking the connection and rely on application Mobility or recovery mechanisms. The main idea is to use MOBIKE-X to negotiate the tunnel with a non routable IP address as the inner IP address, then, to change the inner IP addresses —TS. Once the tunnel is configured with the proper inner IP addresses, the EU proceeds to the regular MOBIKE(-X) Mobility by changing the outer IP addresses.

WLAN to RAN Mobility is performed using MOBIKE(-X) as if RAN required to be secured. The EU can either re-negotiate the SA, and remove the encryption in case of another offload. The EU can also choose to DELETE the SA and provide direct connectivity between the inner IP address and IP_{SERVER}. MOBIKE-X Inner mobility may be required to change the IP_{WLAN} inner IP address to IP_{RAN}.



```
End User                Server

   <<< Connection on IP_EU^RAN, IP_srv >>>

   Setting IPsec for IP_EU^WLAN and IP_srv
SA_EU1, KE_EU, N_EU    -->
                   <--  SA_SRV1, KE_SRV, N_SRV
SK {ID_EU, AUTH,
SA_EU2, TS_EU, TS_SRV,
CP(CFG_REQUEST),
N(MOBIKE_SUPPORTED)} -->
              <-- SK {ID_SRV, AUTH,
                  SA_SRV2, TS_EU, TS_SRV,
                  CP(CFG_REPLY),
                  N(MOBIKE_SUPPORTED)}

   <<< IKEv2 Channel Established
   TS_EU,SRV Tunneled in IP_EU^WLAN, IP_srv  >>>

   Mobility from IP_EU^RAN to IP_EU^WLAN

   >>> Breaking IP_EU^RAN, IPsrv       >>>
   >>> Establishing IP_EU^RAN, IPsrv   >>>

TCP SYN          -->
                <-- TCP ACK
TCP SYN-ACK      -->
GET HTTP1.1 first-byte-pos  -->

   <<< EU Offloaded on WLAN        >>>
```

(a) Application Mobility

```
End User                Server

   <<< Connection on IP_EU^RAN, IP_srv >>>

   <<< EU Changes SPD
   IP_srv, IP_srv STALLED              >>>

   Setting IPsec for IP_EU^RAN and IP_srv
SA_EU1, KE_EU, N_EU    →
                   <--  SA_SRV1, KE_SRV, N_SRV
SK {ID_EU, AUTH,
SA_EU2, TS_EU, TS_SRV,
CP(CFG_REQUEST),
N(MOBIKE_SUPPORTED)} -->
              <-- SK {ID_SRV, AUTH,
                  SA_SRV2, TS_EU, TS_SRV,
                  CP(CFG_REPLY),
                  N(MOBIKE_SUPPORTED)}

   <<< Configuring Security Gateway
   as Border Router for IP_EU^RAN      >>>

   <<< IKEv2 Channel Established
   TS_EU,SRV Tunneled in IP_EU^RAN, IP_srv >>>

   Mobility Hard Handover IP_EU^WLAN
SK {N(UPDATE_SA_ADDRESSES)} -->
                    <-- SK {N()}

   <<< EU uses IP_EU^WLAN, TS_EU,SRV unbroken
   TS_EU,SRV Tunneled in IP_EU^WLAN, IP_srv
   EU Offloaded on WLAN                >>>
```

(b) MOBIKE

```
End User                Server

   <<< Connection on IP_EU^RAN, IP_srv >>>

   Setting IPsec for IP_EU^UNROUTED and IP_srv
SA_EU1, KE_EU, N_EU    -->
                   <--  SA_SRV1, KE_SRV, N_SRV
SK {ID_EU, AUTH,
SA_EU2, TS_EU, TS_SRV,
CP(CFG_REQUEST),
N(MOBIKE_SUPPORTED)} -->
              <-- SK {ID_SRV, AUTH,
                  SA_SRV2, TS_EU, TS_SRV,
                  CP(CFG_REPLY),
                  N(MOBIKE_SUPPORTED)}

   <<< IKEv2 Channel Established
   TS_EU,SRV Tunneled in IP_EU^RAN, IP_srv  >>>

   <<< IP_srv, IP_srv STALLED              >>>

   Inner Mobility IP_EU^UNROUTABLE to IP_EU^RAN
SK {N(UPDATE_SA_ADDRESSES)} -->
                    <-- SK {N()}

   <<< IP_EU^RAN Tunneled in IP_EU^RAN, IP_srv>>>

   Mobility Hard Handover IP_EU^WLAN
SK {N(UPDATE_SA_ADDRESSES)} -->
                    <-- SK {N()}

   <<< EU uses IP_EU^WLAN, TS_EU,SRV unbroken
   TS_EU,SRV Tunneled in IP_EU^WLAN, IP_srv
   EU Offloaded on WLAN                >>>
```

(c) MOBIKE-X

Fig. 3. OAA RAN to WLAN Mobility

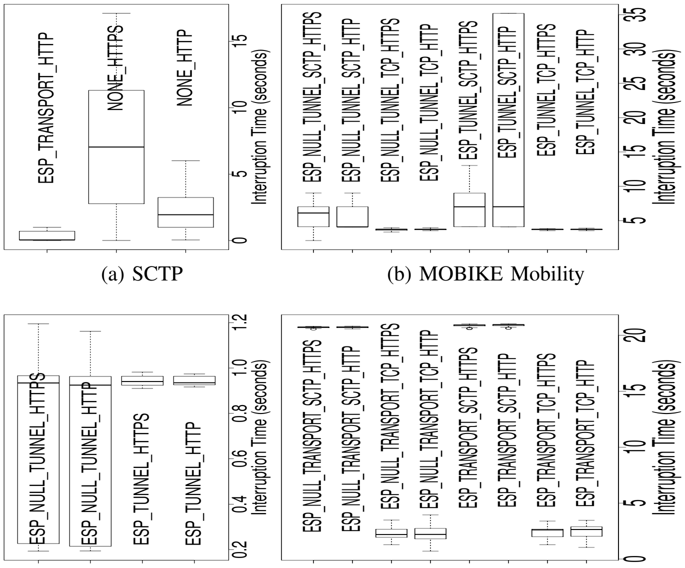
V. Performance Measurements

Section IV describes various ways to deploy FWDA, OSA and OAA by considering either SCTP traffic or non SCTP traffic. On the WLAN, when the connection is IPsec protected with the TUNNEL mode, OAA uses the standard MOBIKE(-X) for Mobility. OSA with TRANSPORT mode combines MOBIKE(-X) with SCTP, or with application Mobility or Session Resumption mechanisms. The main issue comes with connections that are not IPsec protected. In that case, standard MOBIKE(-X) is not supposed to be used. Section IV-A describes how to deploy FWDA, OSA and OAA with SCTP and section IV-B describes how FWDA, OSA and OAA can be deployed without SCTP, with only MOBIKE(-X). This section presents the platform we use to measure how the various Mobility mechanisms affect the connectivity. Then, given how the EU experience is affected by the various WLAN Mobility, we provide recommendations for deploying progressively the *ISP Offload infrastructure* in section V-C. This is followed in section V-D by recommendations on the protocols to use to move between RAN and WLAN, and whether Mobility should be performed by the applications or by SCTP.

A. Experimental Platform

Our experimental platform is composed of a EU with Multiple Interfaces running on *Fedora 17 Linux OS 2.6.38-rc7*. SCTP implementation is *LKSCTP-2.6.28-1.0.10* [14] patched with *fastmsctp-2.6.34-rc5.patch* to enable ASCONF. IKEv2 implementation uses *strongSwan 4.3* [29] and implemented MOBIKE-X [15] on this version. All tests are performed with HTTP(S) traffic over Ethernet. Measurements show statistical results, and present median as well as quartiles.

B. Experimental Mobility Measurements



(a) SCTP

(b) MOBIKE Mobility

(c) MOBIKE Multihoming

(d) MOBIKE-X Mobility

Fig. 4. Experimental WLAN Mobility

FWD: is associated to HTTPS traffic as well as HTTP traffic with no security requirements. SCTP Mobility is performed with a Multihomed EU by putting down the Primary Interface. The EU discovers the Primary Interface is down, and switches to the Alternate Interface. Figure 4a sums up the results, and shows that SCTP interrupts the HTTP communication for $1.94\,s$. SCTP Multihoming does not require extra messages, thus this time is more or less the same on *Public HotSpot*. Figure 4a also shows that TLS interacts with SCTP, which results in an $7.01\,s$ interruption. Finally, Mobility handled with SCTP impacts the EU experience for Real Time Applications. Then, LKSCTP and TLS interactions shows that porting applications to SCTP is not straight forward and that resources must be dedicated for that task.

OSA: Figure 4d shows that Mobility with MOBIKE-X and TRANSPORT mode is independent from TLS or the use of non encrypted IPsec. On the other hand SCTP and IPsec results in a $20\,s$ interruption compared to a $2.57\,s$ with TCP. With the TRANSPORT mode, HTTP and HTTPS re-initiates the TCP connection. Comparing the HTTP/HTTPS connection re-establishment to SCTP Mobility shows a difference of $2.57 - 1.94 = 0.63\,s$ in favor of SCTP.

OAA: Figures 4b (resp. 4c) measures MOBIKE Mobility (resp. Multihoming) impact on the communication. Mobility is performed by changing the IP address of the running Interface, as if the EU had a single Interface. Multihoming requires Interface down detection before switching to the Alternate Address. Figures 4b and 4c show that Mobility is neither impacted by the use of TLS nor the use of null encryption Tunnel. However, SCTP interrupts the communication around $7.02\,s$ compared to $3.72\,s$ with TCP. In fact SCTP and TUNNEL interact with the Kernel routing policies. Figure 4c shows that Multihoming performs better than Mobility, probably because Multihoming orders Kernel events to prepare the Mobility.

C. Recommendation for Offload Deployment

This section compares the EU experience on WLAN Mobility over FWDA, OSA or OAA, and provides deployment strategies for the *ISP Offload Infrastructure*.

FWDA: From figure 4d and figure 4a SCTP Mobility takes $\approx 1.94\,s$ for non TLS traffic. For TLS traffic, session resumption would add 3 RTT, and with a measured $RTT = 0.015\,s$ on *Public HotSpot*, SCTP Mobility for TLS is $\approx 2\,s$.

OSA: MOBIKE-X and TRANSPORT Mobility takes $\approx 2.7\,s$. For MOBIKE(-X) one can eventually add 1 or 2 RTT depending whether Return Routability Check is performed or not. This adds a 40% increase over FWDA, but MOBIKE-X Multiple Interfaces ability may reduce even further this delay.

OAA: MOBIKE(-X) and TUNNEL Mobility takes $\approx 3.8\,s$, adding 100% over FWDA which affects the EU experience. This considers neither routing indirection nor latency introduced by the Security Gateway.

Given how the EU is affected by the various Offload Architectures, we recommend ISPs to firstly deploy FWDA for all TLS and traffic with no protection requirements. Secondly to deploy OSA for service with Real Time requirements, and OAA for the remaining traffic. Note those recommendations match those to optimize costs deployment of the architecture. In the second phase, ISPs may improve the EU experience by taking advantage of MOBIKE-X Multiple Interfaces and deploy Soft Handover. In fact measurements indicate that interruption mostly results from OS Network Layers configuration rather than Network latencies.

D. Recommendation on Mobility between RAN and WLAN

This section compares the various ways to move between RAN and WLAN. Then it provides recommendations on whether Mobility may use SCTP, MOBIKE or MOBIKE(-X) only architecture.

FWDA: SCTP interrupts the communication around $2\,s$ for both non-TLS and TLS traffic.

OSA: MOBIKE-X and TRANSPORT mode interrupts the communication for $1\,s$ with SCTP and 2.74 when the application handles the Mobility.

OAA: SCTP presents similar performances in OAA and FWDA. With MOBIKE we estimate IKE negotiation $T_{IKE} \approx 60\,ms$ with the PSK authentication. PSK authentication is very fast and including T_{IKE} does not affect MOBIKE Mobility which is $\approx 3.8\,s$. To avoid T_{IKE}, MOBIKE-X must modify inner IP address first. This does not affect the Network Layers of the OS as the outer IP address are not modified. In fact only IPsec databases are updated, which should add a $1 - 2\,s$ delay, leading to a $5.5\,s$ interruption. MOBIKE, even though it includes an IKE negotiation, provides faster Mobility.

Thus, the first recommendation is to keep the architecture as simple as possible by using dedicated protocols or limiting Network Layer modifications. If SCTP is available then using SCTP is recommended, otherwise MOBIKE with fast authentication is recommended (like PSK). If there are specific needs for the applications, or the authentication cannot use PSK, then MOBIKE-X should be used. In a second phase, ISPs may take advantage of MOBIKE-X Soft Handover, and inner mobility.

E. Recommendations on Mobility with SCTP vs Application

This section discusses whether Mobility should be handled by SCTP or by the applications themselves.

SCTP Mobility is around $2\,s$ for HTTP connection, and around $2.73\,s$ for HTTP with MOBIKE-X TRANSPORT. SCTP provides a 30% advantage over applications. However, SCTP advantage must be balanced with the fact that HTTP(S)/FTP clients are very easily configured, and that slight modifications can generate long delays with SCTP ($7\,s$ with TLS, $20\,s$ and TRANSPORT, routing interactions with TUNNEL).

Thus, recommendations are to configure Mobility at the application layer for most ISPs applications, and consider SCTP when the EU experience is impacted by Mobility.

VI. Conclusion

This paper describes the *ISP Offload Infrastructure*. To the difference with I-WLAN [1] where ALL EU traffic is tunneled to a Security Gateway, the *ISP Offload Infrastructure* defines 3 types of traffic it associates a specific and dedicated Offload Architecture. Traffic that does not require any security, or that is already protected by other layers like TLS is associated to FWDA that forwards it directly on the Internet. Traffic for specific ISP hosted services is associated to OSA that provides End-to-End security with TRANSPORT mode. The remaining traffic is tunneled to the Security Gateway with IPsec TUNNEL mode.

By providing an adapted Offload Architecture to each type of traffic, we expect to reduce drastically the infrastructure ISPs have to deploy, as well as to improve the EU experience. OSA and OAA are IPsec based architectures and so require the ISPs to deploy an IPsec infrastructure. The IPsec infrastructure can handle Mobility with MOBIKE(-X), but other Mobility protocols are required when the communication is not protected with the TUNNEL mode. This paper considers deploying OSA, OAA and FWDA by either using SCTP or by relying on the application session resumption mechanisms. For all possible scenarios we measure how Mobility interrupts the communication and may affect this EU experience. Then, we balance these disadvantages with the cost of porting applications to SCTP. We find out that ISPs may deploy in a first phase FWDA. Then ISPs should deploy OAA and OSA. To ease OSA deployment, ISPs may start by deploying OSA with the TUNNEL mode which makes MOBIKE(-X) deals with Mobility on the WLAN. To move from RAN to WLAN, MOBIKE may also be used at first. This would correspond to a first deployment version of the *ISP Offload Infrastructure*. For version 2, we recommend ISPs decide to port applications to SCTP or to configure properly the session resumption mechanisms so that OSA can migrate from TUNNEL to TRANSPORT mode and do not rely on MOBIKE for Mobility between RAN and WLAN. For version 3, we recommend to optimize MOBIKE(-X) so perform Soft Handover. For version 4, we recommend ISPs to focus on the RAN to WLAN optimization with MOBIKE-X for applications that are not ported to SCTP.

Future work includes interactions between IPsec and SCTP, especially for the OSA architecture, SCTP and MOBIKE-(X) performs Mobility simultaneously for IPsec and SCTP. We believe SCTP may take advantage of IPsec signalization, using a cross layer communication. This would require the definition of an IPsec API.

References

[1] 3GPP-LTE. 3gpp system to wireless local area network (wlan) interworking; system description, ts 23.234, release 10. Standard, Mar. 2011.

[2] S. Bellovin, J. Ioannidis, A. Keromytis, and R. Stewart. On the Use of Stream Control Transmission Protocol (SCTP) with IPsec. RFC 3554 (Proposed Standard), July 2003.

[3] J. Cao, M. Li, C. Weng, Y. Xiang, X. Wang, H. Tang, F. Hong, H. Liu, and Y. Wang, editors. *IFIP International Conference on Network and Parallel Computing, NPC 2008, Shanghai, China, October 18-21, 2008, Workshop Proceedings*. IEEE Computer Society, 2008.

[4] E.-C. Cha, H.-K. Choi, and S.-J. Cho. Evaluation of security protocols for the session initiation protocol. In *ICCCN'07*, pages 611–616, 2007.

[5] Cisco. Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2010-2015, Feb. 2011.

[6] P. Eronen. IKEv2 Mobility and Multihoming Protocol (MOBIKE). RFC 4555 (Proposed Standard), June 2006.

[7] A. Handa. Mobile Data Offload for 3G Networks, http://www.intellinet-tech.com. (Work in Progress), Oct. 2009.

[8] C. Hohendorf, E. P. Rathgeb, E. Unurkhaan, and M. Txen. Secure end-to-end transport over sctp. In G. Mller, editor, *Emerging Trends in Information and Communication Security, International Conference, ETRICS 2006, Freiburg, Germany, June 6-9, 2006, Proceedings*, volume 3995 of *Lecture Notes in Computer Science*, pages 381–395. Springer, 2006.

[9] C. Kaufman, P. Hoffman, Y. Nir, and P. Eronen. Internet Key Exchange Protocol Version 2 (IKEv2). RFC 5996 (Proposed Standard), Sept. 2010. Updated by RFC 5998.

[10] S. Kent and K. Seo. Security Architecture for the Internet Protocol. RFC 4301 (Proposed Standard), Dec. 2005. Updated by RFC 6040.

[11] T. Koponen, P. Eronen, and M. Särelä. Resilient connections for ssh and tls. In *Proceedings of the annual conference on USENIX '06 Annual Technical Conference*, pages 30–30, Berkeley, CA, USA, 2006. USENIX Association.

[12] W. Lehr and L. W. Mcknight. Wireless Internet access: 3G vs. WiFi? *Telecommunications Policy*, 27(5-6):351–370, 2003.

[13] S. Lindskog and A. Brunstrom. A comparison of end-to-end security solutions for sctp. Technical report, Proceedings of the 5th Swedish National Computer Networking Workshop (SNCNW 2008). Karlskrona, Sweden, apr 2008.

[14] LKSCTP. Linux Kernel SCTP, http://sourceforge.net/projects/lksctp/.

[15] D. Migault. MOBIKE eXtension (MOBIKE-X) for Transport Mobility and Multihomed IKE_SA. (Work in Progress), Sept. 2009.

[16] R. Moskowitz and P. Nikander. Host Identity Protocol (HIP) Architecture. RFC 4423 (Informational), May 2006.

[17] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson. Host Identity Protocol. RFC 5201 (Experimental), Apr. 2008.

[18] P. Noriega-Vivas, C. Campo, C. Garcia-Rubio, and E. Garcia-Lozano. Supporting l3 femtocell mobility using the mobike protocol. Technical report, ACCESS 2011 : The Second International Conference on Access Networks, apr 2011.

[19] T. Norman and R. Linton. The case for wi-fi offload: the costs and benefits of wi-fi as a capacity overlay in mobile networks. Technical report, Analysys Masson, dec 2011.

[20] C. Perkins. IP Mobility Support for IPv4, Revised. RFC 5944 (Proposed Standard), Nov. 2010.

[21] M. Ratola. Which layer for mobility? - comparing mobile ipv6, hip and sctp. *HUT T-110.551 Seminar on Internetworking*, 2004.

[22] E. Rescorla, M. Ray, S. Dispensa, and N. Oskov. Transport Layer Security (TLS) Renegotiation Indication Extension. RFC 5746 (Proposed Standard), Feb. 2010.

[23] M. Riegel and M. Tuexen. Mobile SCTP. Internet-Draft (Work in progress), Nov. 2007.

[24] S. Risto and L. Antti. Operator's Dilemma : How to take advantage of the growing mobile Internet, May 2010.

[25] J. Schönwälder, G. Chulkov, E. Asgarov, and M. Cretu. Session resumption for the secure shell protocol. In *Proceedings of the 11th IFIP/IEEE international conference on Symposium on Integrated Network Management*, IM'09, pages 157–163, Piscataway, NJ, USA, 2009. IEEE Press.

[26] sctplib. The SCTP library, http://www.sctp.de/sctp-download.html.

[27] R. Stewart. Stream Control Transmission Protocol. RFC 4960 (Proposed Standard), Sept. 2007. Updated by RFC 6096.

[28] R. Stewart, Q. Xie, M. Tuexen, S. Maruyama, and M. Kozuka. Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration. RFC 5061 (Proposed Standard), Sept. 2007.

[29] StrongSwan. the OpenSource IPsec-based VPN Solution, http://www.strongswan.org.

[30] E. Unurkhaan, E. P. Rathgeb, and A. Jungmaier. Secure sctp - a versatile secure transport protocol. *Telecommunication Systems*, 27(2-4):273–296, 2004.