E2E : an optimized IPsec architecture for secure and fast offload

Daniel Migault, Daniel Palomares, Emmanuel Herbert, Wei You, Gabriel Ganne, Ghada Arfaoui, Maryline Laurent

E2E: An Optimized IPsec Architecture for Secure And Fast Offload

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*—When mobile End Users are offloaded from a Radio Access Network (RAN) to a WLAN, current I-WLAN [1] offloaded architectures consider traffic converging to a common Security Gateway. In this paper, we propose an alternative End-to-End security (E2E) architecture based on the MOBIKE-X [2] protocol, which extends the MOBIKE [3] Mobility and Multihoming features to Multiple Interfaces and to the Transport mode of IPsec. The benefits of this E2E architecture are mostly load reduction and a better End User experience. First, E2E offloads the ISP CORE and backhaul networks, then E2E uses IPsec Transport mode instead of Tunnel mode, which removes networking and security overhead. This reduces CPU load by 20%, enhances Mobility and Multihoming operations by about 15%, and makes the system 2.9 times more reactive for detecting modifications of interfaces.**

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

I. Introduction

One of today's ISP challenge is to deal with an increasing demand for Mobile traffic. By the end of 2012 mobile-connected device is expect to exceed the number of people on earth to reach 1.4 mobile per capita in 2016, making the aggregate smartphone traffic in 2015 will be 47 times greater than it is today. In conjunction with the Machine-to-Machine mobile traffic, the global mobile traffic is expected to be 18 times larger than in 2011 [4]. Unability to handle this traffic represents a significant loss of revenues for ISPs as a large part of their revenues are provided by Services. To overcome this traffic growth, ISPs have to make their infrastructures ready to deal with that traffic growth, and have three alternatives [5]–[9]:

- **Upgrade their infrastructure** by increasing the number of cells;
- **Optimize their infrastructure** by improving the current technology and increasing each cell's capacity;
- **Offload** the traffic on Alternate Networks such as WLAN.

In [9], it was shown that the Radio Access Network (RAN) infrastructure does not require any upgrade nor optimization if 52% of the traffic growth is offloaded. Thus, the large deployment of indoor WLAN Access Points can promote the offload scenario and lead to a cost reduction by 4.8 over the *Optimize* and *Upgrade* scenario.

This paper proposes E2E as an alternative architecture to Interworking Wireless LAN (I-WLAN) [1] for offloading the traffic. E2E is an End-to-End Security architecture based on IPsec in Transport mode. This paper aims at measuring the Mobility and Multihoming performances of E2E over I-WLAN and Tunnel-based architectures, for Real Time Applications. Therefore, section III positions our work, with respect to related works. Section IV compares the I-WLAN and E2E architecture, and gives the ISP new business opportunities provided by E2E. Section V focuses on the interactions between Mobility, Multihoming and Security. It provides Mobility and Multihoming Security requirements, and positions E2E with Transport mode toward those requirements. We point out that E2E cannot fulfil those Requirements with the current MOBIKE [3] extension, and that MOBIKE-X [2] is required. A presentation of MOBIKE-X which extends MOBIKE for the Transport mode and Multiple Interfaces follows. Section VI presents our experimental measurements. We measure how SCTP Mobility with IPsec protected links differs from SCTP Mobility on non-IPsec protected links. We use SCTP because with Transport mode IPsec Mobility must be combined with a Mobility protocol to move the traffic. Then SCTP provides End-to-End Mobility, and the ISP does not require to deploy and Mobility Architecture like with Mobile IP [10]. After measuring SCTP Mobility performances, we measure Mobility with MOBIKE (Tunnel mode) and MOBIKE(-X) (Transport mode). Finally, section VII concludes this paper as well as provides future work.

II. Notations & Abreviations

This paper uses the following notations and abbreviations:

- **MM:** Mobility and Multihoming
- **MMN:** Mobile and Multihomed Node (e.g. smartphone with multiple interfaces)
- **E2E:** End-to-End Architecture
- **RAN:** Radio Access Network
- **TRANSPORT:** IPsec Transport mode
- **TUNNEL:** IPsec Tunnel Mode
- **SP:** IPsec Security Policy which specifies the rules for handling security over IP packets (either BYPASS IPsec, DISCARD packets, or PROTECT with a specific SA)
- **SPD**: Security Policy Database which contains all SPs
- **SA:** IPsec Security Association, i.e. the cryptographic elements for protecting IPsec packet
- **SAD:** Security Association Database with all SAs
- **RTA:** Real Time Application

III. Position of our Work & Related Work

Our paper measures how the E2E secured communication performs during MM operations on to offloading traffic. We test communications with SCTP over IPsec, so we position our work toward IPsec, SCTP & IPsec, HIP and MIP. Several works [11]–[15] analyse IPsec performances in several VPN configurations.

Bellovin and al. [16] describes how IKEv1 establishes an IPsec SA with the multiple IP addresses of the SCTP association. MOBIKE(-X) is based on IKEv2 and [16] does not consider dynamic IP addresses management. Other works [17]–[21] evaluate different ways to secure SCTP communications and design TLS based protocol specific to SCTP: *Secure - SCTP* and *Secure Socket SCTP*. IPsec was rejected because of its 4 bytes overhead over TLS, leading to less than 3% throughput performance loss and a lack of flexibility for (1) different chunks (specific to SCTP) and (2) with Multihoming and Dynamic Address Configuration [22]. None of the previous work considers performance measurements for MM operations. Our work provides a generic solution MOBIKE-X, not SCTP specific and measures performances over MM operations. Note that MOBIKE-X addresses MM IPsec limitations.

Noriega-Vivasand and al [23] analyses a Home Node B (HNB) 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 (1) the architecture is WLAN and TUNNEL based and (2) multihoming is never used for Soft Handover which is reported as a missing feature. Note that MOBIKE-X addresses that problem.

Other protocols than SCTP could have been selected. We give a special attention to HIP [24], [25] that provides both security with IPsec BEET mode [26] and MM facilities. HIP communications are established between crypto identifiers (Host Identity Tags or HIT). HIT are bound to an IP address. Since HITs remain fixed during the communication, IP addresses can be changed / added transparently to the application. Actually HIP takes advantage of the TUNNEL and TRANSPORT mode with the BEET mode. MM is transparent to the applications, and there is no tunnel header. However, HIP suffers from two drawbacks: (1) Communications are always IPsec protected and (2) HIP breaks the current IP oriented communications. Protecting all communications adds an extra overhead on RAN for example, even though it could be reduced by using ESP_NULL. HIP breaks the current IP-oriented communication model and the non-incremental characteristic imposes HIP to be deployed between the MMN and the server on the RAN. Thus MOBIKE-X provides the IPsec characteristics of HIP to the IP oriented communications. On the other hand MOBIKE-X only considers the IPsec layer, and the MM features of the communication must be provided by other protocol. SHIM6 and SCTP are very good candidates. We choose SCTP because our platform is IPv4 only, as most of over infrastructure has not been yet deployed in IPv6.

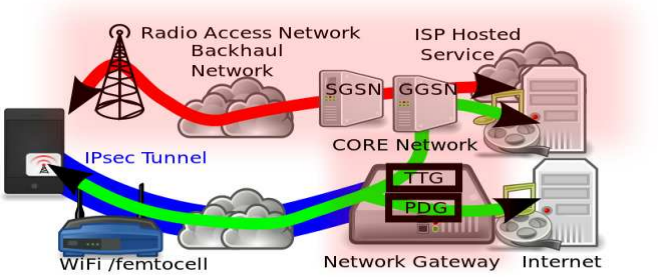
The E2E architecture differs from traditional Mobile IP based architectures [10], [27] as the MMN is managing the MM operation. This may add complexity at the terminal side, but experimentations have concluded that using MM aware terminal optimizes the MIP mobility operation [28]. Thus we do not consider it is a major constraint. Then, MIP and MOBIKE-X do not address the same issue. MIP makes the MMN reachable with its Home Address, whereas the E2E provides MM operation for a given communication. As a result simultaneous mobility of the nodes is not possible with E2E. [29] is quite close to E2E architecture, as specific applications benefit from an HIP end-to-end communication with security and MM features. The remaining communications are tunnelled to a Security Gateway located in the EU private network rather than in its ISP's core network.

As mentioned earlier MM can be performed at different layers [30]. Here IPsec MM is handled at the IPsec layer, independently to other Mobility / Multihoming protocols. Therefore, we hope MOBIKE-X can be compatible with most of the Mobile / Multihomed architectures.

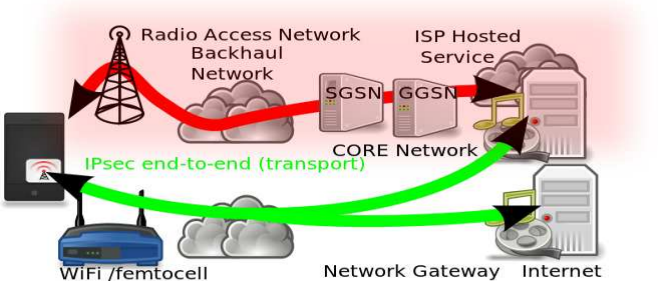
IV. E2E vs I-WLAN

This section compares our E2E End-to-End Security Offload Architecture to the 3GPP I-WLAN Offload Architecture [1], and explains how Offload and E2E represents new business opportunity for ISPs.

A. Description of the Architectures



(a) I-WLAN



(b) E2E

Fig. 1. Offload Architectures

I-WLAN illustrated in figure 1a is the proposed 3GPP offload architecture. A smartphone connected to a WLAN sets up an IPsec tunnel with the ISP Tunnel Terminating Gateway

(TTG) which decapsulates and forwards the traffic. That is, communications with an ISP service hosted application are forwarded to the Gateway GPRS Support Node (GGSN), otherwise Internet communications are forwarded to the Packet Data Gateway (PDG). MM is handled by the MOBIKE extension of IKEv2 [3].

E2E as illustrated in figure 1b, provides End-to-End security. That is, the communication is encrypted from the MMN to the server hosting the service. That is, there is no Security Gateway. Compared to the End-to-End, I-WLAN suffers from the following drawbacks:

- **Cost overhead for the ISP:** The main reason for encrypting and redirecting traffic to a Security Gateway is to protect this traffic. This traffic overloads the ISP CORE Network, and ISPs have to deploy VPN concentrators, platforms and licences. With current 3G RAN architecture, licence costs are derived from Packet Data Protocol (PDP) context activation. When an MMN is being offloaded, this requires a new PDP activation which adds unnecessary costs for the ISP. There are at least two types of traffic that are unnecessarily redirected to the Security Gateway: (1) Traffic that is not confidential and (2) traffic already protected like HTTPS for example. Note also that I-WLAN, in addition to the Security Gateway requires also a Mobile IP infrastructure [10] to move EU from RAN to WLAN.
- **Latency overhead:** The Security Gateway introduces extra latencies by doing extra processing over the packet (e.g. encapsulation, forwarding), and routing indirection. Traffic tunnelling adds network complexity as each packet is forwarded twice in the IP stack. Furthermore, an overhead by at least $20\,bytes$ in IPv4 and $40\,bytes$ in IPv6, is introduced and leads to extra network load and network latency. Tunnelling with IPsec requires extra encryption costs of the inner header. Of course, the smaller the application datagram is, the higher the cryptographic cost is. Section V-C evaluates the cost of encrypting the inner IP header.
- **Single point of failure:** The Security Gateway where all the traffic is going through is exposed to DoS or DDoS attacks.

On the other hand, the E2E security approach provides the following advantages:

- **Per service granularity:** The ISP secures only the services that need to be secured.
- **ISP Network load reduction:** End-to-End communications are not redirected to the CORE network of the ISP, and eventually not even on the Access Network nor the backhaul Network of the ISP. We use SCTP [31] in conjunction of IPsec so that Mobility is handled by the Terminal, and does not require the ISP to deploy any infrastructure like with Mobile IP [10]. Similarly to I-WLAN, E2E needs a Mobility protocol to move from RAN to WLAN. However, IPsec TRANSPORT mode cannot be used for moving the traffic on its own and E2E requires a Mobility protocol as SCTP.
- **Security overhead reduction:** Avoiding some useless traffic encryption, smaller clusters of VPN concentrators are necessary for deploying the Security Gateway. Using TRANSPORT mode rather then TUNNEL mode increases the capacity of each concentrator by reducing both the cryptographic and the network load.
- **Latency reduction:** Both in term of network latency and routing indirection.
- **Provision of new services:** Security can be considered as a service for third service providers (see section IV-B).

As a result, for a given traffic E2E requires a smaller infrastructure as I-WLAN, and provides a better EU experience, especially for RTA with small datagram. In this paper, we compare E2E and I-WLAN and measure how E2E provides a better EU experience. However, E2E is not expected to replace I-WLAN, we expect ISPs to deploy E2E for high value Services, and I-WLAN for the remaining traffic of the EU.

B. E2E New Business Opportunities

Recent works investigated different behaviours for offloading traffic. [32] and [33] consider social networking applications and offload over ad-hoc networks. [34] evaluates, based on live traffic, which download strategy saves battery. WLAN offers higher bandwidth than RAN which reduces download time and saves battery. With a 1 hour timer before switching to RAN, the offloaded MMN increases by 29% the traffic downloaded from WLAN. Because WLAN provides higher bandwidth, this reduces downloading time which results in reducing battery consumption by 20%.

Similarly to application specific download strategies, our paper optimizes the security according to the application security requirements and the network level of trust. More specifically, RAN is considered secured, and thus layer 2 security is enough. Switching on a WLAN may require layer 3 security depending on the level of trust of the network and application security requirements —i.e. what data are carried, is the communication secured at layer 4 by TLS for example. Our paper considers three ways to secure a communication: (1) An optimized security channel using IPsec TRANSPORT mode, (2) a secure network access (I-WLAN) and (3) no security at all. Since the network defines how security should be deployed, ISPs are good candidates for such services. Note that security also includes authentication of the MMN. With offload, the ISP may also be able to authenticate a MMN with RAN authentication method on behalf of some IP based services.

V. Mobility and Multihoming: IPsec & MOBIKE-X

This section presents MOBIKE-X [2] as well as its motivations for designing this MOBIKE extension. Section V-A presents security requirements for MM. Section V-B explains why we prefer IPsec [35], [36] over TLS [37]/DTLS [38] for E2E. A key difference between I-WLAN and E2E is that I-WLAN uses IPsec TUNNEL mode whereas E2E uses the TRANSPORT mode. In section V-C we estimate the

advantages provided by using TRANSPORT, especially in term of CPU consumption. The remainder sections V-D and V-E describe the IPsec MM extensions. Section V-D describes MOBIKE [3], [39], the IKEv2 [36] MM extension for the TUNNEL mode, and shows what MOBIKE misses to fulfil MM Security Requirements. Then in section V-E, we describe MOBIKE-X [2] and show how MOBIKE-X fulfils the MM Security Requirements.

A. Mobility and Multihoming Security Requirements

In order to choose properly the Security protocol, this section lists General requirements the protocol must fulfil, followed by specific MM requirements.

- **Granularity:** With E2E, the traffic that is secured depends on the Service, the level of trust of the Network, so we must be able to define SP using selectors as IP addresses, ports, application protocols.
- **Security Layer:** With E2E, a Service Provider must be able to request the ISP to secure its traffic over untrusted networks like WLAN. The way the ISP secures the Service should be transparent for the Service Provider. In that sense TLS, for example, requires to modify the source code of the application.
- **Architecture:** E2E and I-WLAN are complementary Architectures. E2E addresses traffic of a specific service whereas I-WLAN address other traffic. For a given service, an ISP may start to use I-WLAN, and then evolves to E2E. It is thus recommended to use the same Security Protocol for E2E as the one used for I-WLAN.
- **Authentication:** Offload Security should support similar authentication mechanisms from the WLAN and the RAN, for homogeneous network access. This would provide the opportunity for an EU to initiate a connection directly from WLAN, rather than from RAN before being offloaded.

This list can be enriched with the MM Security Requirements of [40]:

- **Mobility:** A MMN must be able to UPDATE the IP address of its interface.
- **Multihoming:** WLAN Access Point may not be maintained by the ISP, and so may be unreliable. The MMN must be able to provide alternate IP addresses that may be used if the running IP address is not reachable anymore.
- **Multiple Interfaces:** Similarly, the MMN may be attached to various WLAN Access Points simultaneously. The MMN should be able to ADD, REMOVE or UPDATE an interface to a given communication.

B. The Choice Of IPsec For Securing E2E

Comparing TLS [37] / DTLS [38] and IPsec shows that IPsec [35] is recommended to Offload Security. TLS/DTLS does not provide other granularity than a service granularity (port). In other words, DTLS/TLS provides a secure version of a given service. Moreover TLS/DTLS's main drawback is that it requires code modifications, and thus makes ISP Offload service of section IV-B hard to be deployed for third party. Furthermore, TLS/DTLS has been designed for End-to-End connectivity, and may not fit all requirements of a Security Gateway Architecture. At last, TLS/DTLS does not provide EAP [41] framework for authentication. On the other hand, IPsec defines Security Policies according to various Traffic Selectors that includes subnetworks, IP addresses, ports, and upper layer protocols. Furthermore it secures the IP layer in the kernel, which does not impact the service, and thus makes possible an ISP to provide a Secured Offload for a third party service. IPsec has two modes: the TRANSPORT mode for End-to-End connectivity and the TUNNEL mode to secure the link between the MMN and a Security Gateway. At last, IPsec [42] provides an EAP framework making authentication mechanisms [43], [44] on RAN possible on WLAN.

C. TRANSPORT Reduces CPU Consumption Over TUNNEL

With IPsec, the traffic can be secured with the TUNNEL mode as in I-WLAN or with the TRANSPORT mode as in E2E. This section estimates the gains of CPU consumption provided by the use of TRANSPORT instead of TUNNEL. [13] measures for Security Gateways the performance impact of Intel AES New Instruction (AES-NI) for the cryptographic AES-GCM on Linux. For 60 to 180 bytes RTA payloads, it estimates that removing the encryption of the 20 bytes of the inner IP header reduces the number of CPU cycles by 10% to 31% with AES-NI and by 6% to 26% with regular software AES implementation. Furthermore, with AES-NI, for a 200-byte packet (resp. 1500 bytes), the cryptographic computation consumes 16% (resp. 35%) of the total computation capacity whereas the remaining CPU cycles are left to the networking process. Thus, this recent performance measurement paper shows that using TRANSPORT mode significantly improves performances, CPU consumption of RTA. Similarly, [14] evaluates IPsec performances on the 3G/LTE architectures by considering the tunnel between the eNobeB and the Radio Node Controller. For large packet size traffic (512 - 1420 bytes), IPsec tunnel overhead is shown negligible. However, for traffic with small payload (64 - 500 bytes), IPsec tunnel overhead reduces performances by $60 - 80\%$. [14] and [15] measure the effect of IPsec VPN over the offloaded RTA traffic and measures that as soon as network are loaded or the Security Gateway is not highly available, the EU experience is impacted. This may be counter by prioritizing flows. However, prioritization reduces the Security Gateway impact, but ISPs have no impact the network congestion between the MMN and our service. On the other hand TRANSPORT reduces network latencies and [13]–[15] conclude that TRANSPORT mode for RTA significantly reduces CPU consumption, and improves EU experience. Note also that with specific application IPsec links E2E eases flows prioritization in the ISP CORE Network.

D. MOBIKE Does Not Fulfil MM Requirements

MM Security Requirements are partially handled by IPsec MOBIKE [3] extension. MOBIKE has been designed for a MMN with a single interface and the TUNNEL mode. More specifically, TRANSPORT mode and Multiple Interfaces are

not considered.
MMN and the Security Gateway agree to use MOBIKE by exchanging a MOBIKE_SUPPORTED Notify Payload while establishing the IKE channel. If the MMN and the Security Gateway support MOBIKE, when the MMN changes its IP address, it sends the Security Gateway an UPDATE_SA_ADDRESSES Notify Payload. When receiving this Payload, the Security Gateway looks at the IP source of the Packet, and for all Security Associations (SA) associated to the MMN, the Security Gateway changes the outer header IP address of the Tunnel. Note that only the outer header of the SA is a parameter of the SA, and does not affect the Security Policy. The Security Policy —*Tunnelling traffic from my inner IP address* —is not changed. Thus, the Security Association Database is impacted; the Security Policy Database remained unchanged. Note that changing the outer header, results in tunnelling traffic to the Security Gateway from IP_{OLD} and then from IP_{NEW}. This results in a Mobility operation that is transparent to encapsulated traffic. This MOBIKE Mobility Hard Handover is used in WLAN and takes advantage of the TUNNEL mode. For Multihoming, the MMN informs the Security Gateway with ADDITIONAL_IP4/IP6_ADDRESS Notify Payload that an Alternate IP address may be used, if the MMN is not reachable on the Primary IP address. If the MMN happens to be unreachable, the Security Gateway performs a Return Routability Check to check the MMN is still reachable on the Alternate IP address, and in case of success, it sends an UPDATE_SA_ADDRESSES to the MMN so it updates its SAs.
In order to fulfil MM Requirements, MOBIKE-X must:

- Extend MOBIKE Multihoming and UPDATE_SA_ADDRESSES with the IPsec TRANSPORT mode
- Extend MOBIKE Mobility for Multiple Interfaces for both IPsec TRANSPORT and TUNNEL modes. Typically this includes functionalities such as ADDing / REMOVing and UPDATING an Interface to an existing SA.

E. MOBIKE-X Makes MOBIKE Fulfil MM Requirements

MOBIKE-X [2] extends MOBIKE [3] to address MM Requirements of section V-D. MOBIKE-X [2] extends MOBIKE on at least two aspects. MM operations are extended to the TRANSPORT mode, and to Multiple Interfaces by using ADD_SA_ADDRESS / REMOVE_SA_ADDRESS Notify Payload.
Modifications in TRANSPORT mode are a bit more complex than with the TUNNEL mode because in TRANSPORT mode, the IP address impacts both the SAD and the SPD. Then Mobility with TRANSPORT mode does not result in moving the communication as in TUNNEL mode. Mobility with TRANSPORT mode updates the SAD and SPD, but other protocols like SHIM6 [45], SCTP [31], mpTCP [46] have to move the communication from one interface to the other.
Then, Multiple Interfaces requires ADD, REMOVE and UPDATE operations to specify what needs to be modified. More specifically, MOBIKE, with a single interface, the UPDATE_SA_ADDRESSES does not carry any information: the new IP addresses are those in the IP header. With Multiple Interfaces, we use IP PARAMETER to specify the old and new IP addresses. When not explicitly provided, MOBIKE-X derives the PARAMETERS so to remain compatible with MOBIKE.
Finally MOBIKE-X offers the following advantages over MOBIKE: (1) MOBIKE-X remains compatible with MOBIKE Payloads, then (2) MOBIKE-X supports TRANSPORT mode and makes E2E possible. (3) with Multiple Interfaces, MOBIKE-X makes Soft Handover possible which reduces packet loss over Hard Handover. Furthermore, (4) it supports interface traffic management as the selectors can be renegotiated.

VI. IPsec Mobility and Multihoming Measurements

This section is dedicated to the measurements we performed on MM so to compare E2E and I-WLAN. Section VI-A defines our testing environment. Section VI-B considers MMN connected with Multiple Interfaces either to a Service or to a Security Gateway. The MMN uses SCTP Multihoming to move the communication from one Interface to the other. We measure how IPsec TRANSPORT and TUNNEL mode impacts the Mobility regarding to SCTP Mobility between non IPsec protected links. Section VI-C measures MOBIKE Mobility performances with TUNNEL mode, and section VI-D measures MOBIKE-X Mobility performances with the TRANSPORT mode.

A. Testing Platform

Our MOBIKE-X implementation is based on *strongSwan 4.3* [47] and we measured MMN performances in various configurations for transport protocol (traditional TCP and SCTP) and IPsec: ESP (with aes128-sha1) and ESP_NULL (ESP with sha1 and null encryption).
Our experimental platform is shown on figure 2, and we used SCTP to perform MM operation, when we were not using MOBIKE. We used SCTP [31] because that is the most advanced IPv4 protocol that provides End-to-End MM mechanisms. Furthermore, SCTP can be implemented in the kernel with stacks like *LKSCTP* [48] or with user land libraries like *sctplib* [49]. With kernel implementation, the ISP provides Multiple interface facilities for a terminal, whereas with user land implementation, the ISP has the opportunity to developed a specific SCTP applications even on terminals that are not SCTP enabled. Another advantage is that *sctplib* is provided both UNIX and Windows OS.
To measure MM performance over SCTP (*LKSCTP-2.6.28-1.0.10* [48]), we developed a SCTP client and server that runs on *Fedora 17 Linux OS 2.6.38-rc7* patched for enabling ASCONF [22] with *fastmsctp-2.6.34-rc5.patch*. The ASCONF patch makes SCTP to dynamically configure its interface. More specifically, SCTP has been designed for Multihoming,

but all interfaces are provided in the SCTP connection establishment. If an SCTP peer wants to dynamically ADD or REMOVE and Interface, then both SCTP peers need to be patched with ASCONF. The SCTP client can have up to three different Ethernet interfaces that are connected to the server via a router.

The router runs *dummynet* on *Ubuntu Linux OS 2.6.28-11-generic*. We used *dummynet* so to be able to model different type of network. However, changing the bandwidth and delays strongly affected how LKSCTP detects modifications on the interfaces. Default configuration is provided for Ethernet links. Performance measurements use the candle stick representation

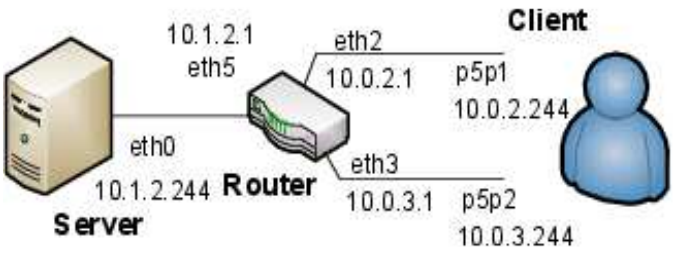


Fig. 2. Experimental Platform

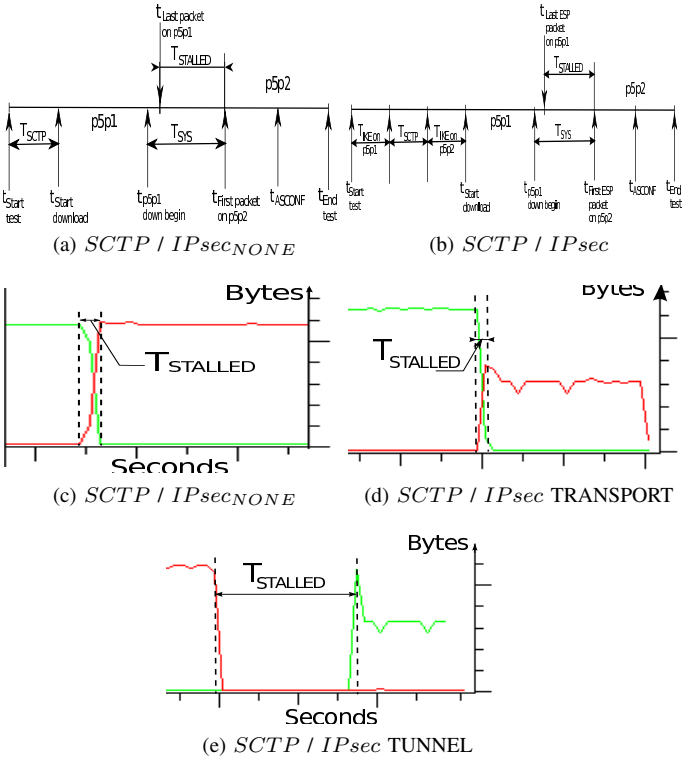
to represent the quartiles of the measured values.

B. SCTP Mobility Multihoming with IPsec

This section analyses how SCTP MM operations are impacted by IPsec. In other words, it measures how protection with TRANSPORT or TUNNEL affects SCTP Mobility. SCTP can be used both in the I-WLAN and E2E Architecture. The MMN is attached to multiple WLAN Access Points to prevent Access Point failure. With E2E, the MMN has multiple connections with the Service protected with the TRANSPORT mode. With I-WLAN, the MMN has multiple connections to the Security Gateway protected with the TUNNEL mode. Mobility is triggered by the Multihoming SCTP mechanism, that is when the Primary interface is down, it switches to the Alternate Interface with a Hard Handover. To compare the various configurations, we measure and compare various time (T_{SCTP}, T_{IKE}, T_{SYS} and $T_{STALLED}$). As a result, we show that MMN is more reactive with the TRANSPORT mode than with the TUNNEL mode: with TRANSPORT mode, the MMN detects network changes 2.9 times faster —T_{SYS}—, and the Mobility is 2.5 times more stable, and 15% faster. I-WLAN is based on TUNNEL whereas E2E is based on TRANSPORT, which gives a clear advantage to E2E.

1) General Input / Output Graphs: Figure 3a, (resp. 3c) represents the flowchart of MM operations without IPsec protection (NONE), (resp. measured output). Figure 3b (resp. 3d 3e, 3d) represents flowshart (resp. measured output) where connections are IPsec protected.

Figures 3c, 3e and 3d show that IPsec is not transparent to the transport layer throughput and behavior, and SCTP may be configured differently for IPsec protected connections than for NONE IPsec connections. With a NONE IPsec configuration —figure 3c—SCTP instantaneously uses the whole bandwidth. On the other hand, the TRANSPORT mode generates a bandwidth gap when a mobility occurs —figure 3d, that is recovered after roughly $10\,s$. With TUNNEL mode, —figure 3e—SCTP and IPsec encapsulation requires modification of the routing policies, which results in concurrent updates between SCTP and IKEv2. More specifically *p5p1 down* triggers a kernel event for both *LKSCTP* and *strongSwan*. Since *LKSCTP* is kernel based, it updates the routing policies first, followed by IKEv2. This may lock, and delay routing policy stabilization. This makes TUNNEL mode more intrusive than TRANSPORT which may result in stalling the communication whereas TRANSPORT modification may be compensated by transport layer mechanisms.



(a) $SCTP$ / $IPsec_{NONE}$ (b) $SCTP$ / $IPsec$

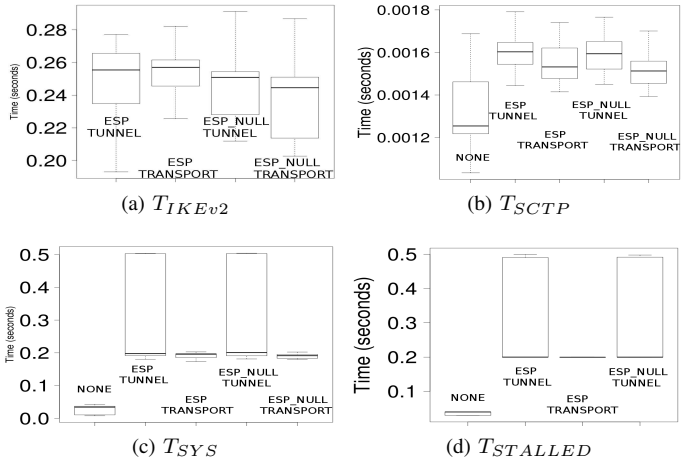
(c) $SCTP$ / $IPsec_{NONE}$ (d) $SCTP$ / $IPsec$ TRANSPORT

(e) $SCTP$ / $IPsec$ TUNNEL

Fig. 3. Multihoming SCTP - Network Flow

2) Measured Time Definition: T_{SCTP}, T_{IKE}, T_{SYS} and $T_{STALLED}$: Figure 4 represents the various negotiations involved in the secured SCTP communication: T_{IKE}, T_{SCTP}, T_{SYS} and $T_{STALLED}$ for various IPsec configurations (NONE, ESP_TRANSPORT, ESP_TUNNEL, ESP_NULL_TRANSPORT, ESP_NULL_TUNNEL). T_{IKE} (resp. T_{SCTP}) is the negotiation time for an IKEv2 (resp. SCTP) communication. T_{IKE} is subject to multiple variations especially because it includes an authentication. In our case, we used a preshared key for authentication, but common ISP SIM/AKA authentication requires EAP [42] framework

(EAP-SIM [43], EAP-AKA [44]), which adds the number of exchanges as well as authentication operations. As a result, the authentication part of the exchange may take longer than the one we measured. However, in that case, it only delays the initialization of the communication, and does not impact MM operations. T_{SYS} is the time it takes to the system to detect $p5p1$ is down and starts sending on $p5p2$ which informs the server multihoming occurred. By receiving a message from $p5p2$, the server is informed that a multihoming operation has occurred. $T_{STALLED}$ is the time duration the communication is interrupted.



(a) T_{IKEv2} (b) T_{SCTP}

(c) T_{SYS} (d) $T_{STALLED}$

Fig. 4. IPsec impact on MM

3) T_{IKE} Analysis: Figure 4a shows that although TRANSPORT mode includes an added Notify Payload, the IKEv2 negotiation for all IPsec configuration (ESP/ESP_NULL, TRANSPORT / TUNNEL) are between $0.25\,s$ and $0.26\,s$. From section VI, measured network latencies are negligible on our $LabPlatform_{Ethernet}$ ($\approx 2 \times 0.355\,ms$), as well as our pre-shared key authentication. Thus, the measured time reflects the systems configurations (SAD, routing policies...).

4) T_{SCTP} Analysis: SCTP negotiation without IPsec takes $1.2545\,ms$ —figure 4b. Compared to $2.RTT = 0.71\,ms$, it takes roughly $0.54\,ms$ to set the network stacks. IPsec adds a $0.26\,ms$ overhead for TRANSPORT mode vs $0.35\,ms$ for TUNNEL mode. Compared to RTT delays introduced by IPsec at the connection initialization should not impact the EU experience. However, the delay introduced by IPsec between 21 and 27% may impact the servers. ESP versus ESP_NULL has no impact on T_{SCTP}, but TUNNEL adds a delay 6% higher than the TRANSPORT for a mixed transaction of packets between 62 bytes (COOKIE_ACK) and 348 bytes (INIT_ACK).

Finally, initialization times measures how long the connection is delayed. IPsec negotiation delays the communication by at least $0.25\,s$ which is not negligible even for MMN connected to *Public HotSpot* with $2.RTT = 30\,ms$. However, the EU experience may not be affected, since it occurs only at the initialization phase, then this delay may be avoided with pre-authentication. Similarly, the delay introduced by IPsec for the SCTP negotiation, is not significant for the MMN. If the MMN is connected to a *Public HotSpot* the delay is between 1.73% and 2.23% of the RTT, which makes it negligible, mostly because it happens only once. However, SCTP initialization exchange provides an example of small packet exchanges and shows that TRANSPORT mode reduces the security overhead by 6% over the TUNNEL which makes TRANSPORT mode more efficient for offloading RTA.

5) T_{SYS} Analysis: In figure 4c IPsec overhead for T_{SYS} is between $161.85\,ms$ for TRANSPORT and $163.48\,ms$ for TUNNEL. TUNNEL presents large variations, and the added delay is up to $469.991\,ms$. TRANSPORT mode makes the System more reactive and stable. The IPsec overhead is the time to activate the dormant SA and modify the routing tables. Note that in TRANSPORT, *strongSwan* is configured with the option `install_routes=no` so it does not interfere with the routing tables. With TUNNEL, this option cannot be used, which makes TRANSPORT between 1.01 and 2.90 times faster, and so preferred for offloaded RTA. IPsec clearly makes the system less reactive, and delays introduced by IPsec impacts the EU experience. This can be avoided either by tuning the system with IPsec, and most probably makes various IP/IPsec/transport layer communicating between each other, or by anticipating a connection is down. In fact connection Managers are expected to decide to switch on one interface before the running interface is down.

6) $T_{STALLED}$ Analysis: Figure 4d shows that without IPsec, the communication is stalled for $30.0325\,ms$ and $199.587\,ms$ with IPsec, which represents the necessary time for the system to detect events, as well as to make SAD and SPD operational. Similarly to figure 4c tunnelling requires system interactions with routing tables which result in large variations, stalling the communication up to $499.20\,ms$. IPsec security overhead results in a longer stalled communication, and clearly impacts the EU experience. Note that IKEv2 Mobility exchanges are not considered in this section. If so, an exchange would add another $RTT = 15\,ms$ on an *Public HotSpot*. The stalled time may be improved and reduced by scheduling transport and IPsec stack modifications, as well as by anticipating and allowing Multihoming Simultaneous Interfaces for a given communication.

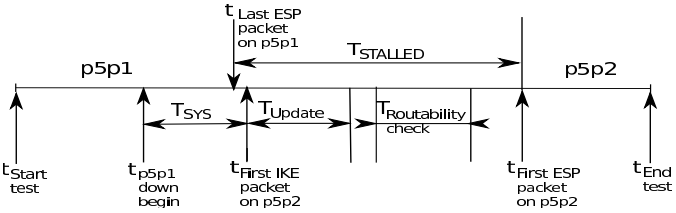
C. MOBIKE Mobility Multihoming

MOBIKE only considers the TUNNEL mode, and a single interface. Thus switching interfaces is performed through a Hard Handover and an UPDATE_SA_ADDRESSES Notify Payload indicates the new IP addresses to use. In this section we use two different mechanisms to switch from one interface to the other. We designate by *Mobility* the operation that consists, for a MMN with a single interface, in changing manually the IP address of the running interface *ifconfig p5p1*

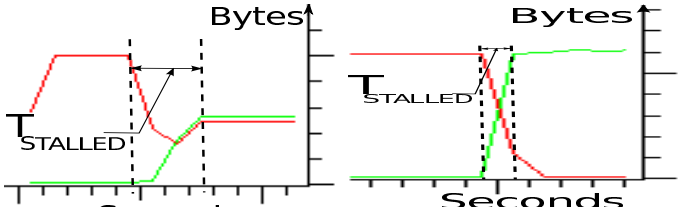
IP_{NEW}. By changing the IP address, the MMN sends an UPDATE_SA_ADDRESSES Notify Payload. We designate by *Multihoming* the operation that consists, for a MMN with Multiple Interfaces, to manually bring the Primary interface down *ifconfig p5p1 down*. By putting down the Primary Interface, the MMN checks the Alternate Interface is still reachable by performing a Return Routability Check (RRC), followed by an UPDATE_SA_ADDRESSES as in the *Mobility* scenario. We consider those two distinct mechanisms because *Mobility* may be trigger by a Network Manager, whereas *Multihoming* is a mechanism that recovers from WLAN Access Points Failover.

Figures 5a and 5b (resp. 5c) give MM with MOBIKE (resp. with MOBIKE-X). In figure 5b *Wireshark* represents a packet anytime it passes through the IP stack, that is to say for both the inner and outer IP header.

Figures 6a and 6b compare T_{SYS}, the time required

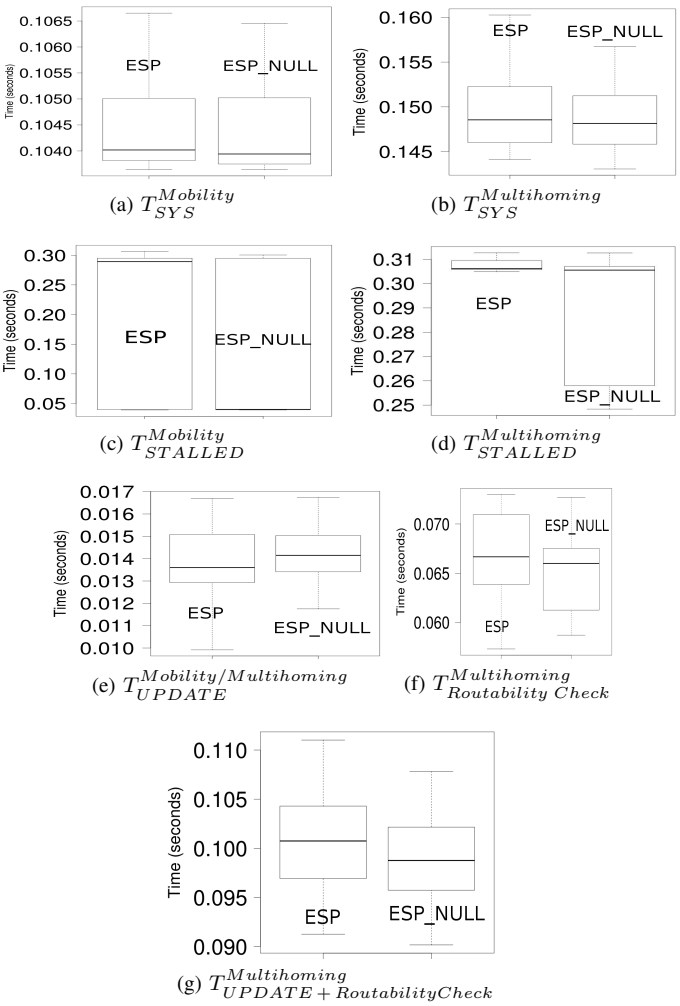


(a) $MOBIKE(-X)$ Mob. / Multih.



(b) $MOBIKE$ (c) $MOBIKE-X$

Fig. 5. MOBIKE / MOBIKE-X - Network Flow



(a) $T_{SYS}^{Mobility}$ (b) $T_{SYS}^{Multihoming}$

(c) $T_{STALLED}^{Mobility}$ (d) $T_{STALLED}^{Multihoming}$

(e) $T_{UPDATE}^{Mobility/Multihoming}$ (f) $T_{Routability\ Check}^{Multihoming}$

(g) $T_{UPDATE+RoutabilityCheck}^{Multihoming}$

Fig. 6. MOBIKE MM Performances

by the system to trigger *Mobility* or *Multihoming*. With *Mobility*, the MMN triggers the change of IP addresses, and the configuration of both network and IPsec stack takes $103.71\,ms$. With *Multihoming* it takes an additional $44.48\,ms$ for the OS to detect the interface is down.

Furthermore, *Multihoming* requires the Return Routability Check (RRC) exchange which adds a $16.61\,ms$ delay to the $T_{STALLED}^{Multihoming} = 305.9345\,ms$ versus $289.318\,ms$ for *Mobility*. We measure $RTT = 15\,ms$ with FTP download on *Public HotSpot*, which makes $T_{STALLED}^{Mobility} \approx 303.96\,ms$ and $T_{STALLED}^{Multihoming} = 335.234\,ms$.

Comparing RTT ($0.35\,ms$), T_{UPDATE} ($13.60\,ms$) and T_{RC} ($66.011\,ms$), T_{RC} is 4.85 times larger than T_{UPDATE} because kernel operations are performed with higher priority than application (polling mode). From $T_{UPDATE} \approx 13.60\,ms$, the IPsec SADs are expected to be updated on the MMN and the server in roughly $25\,ms$. $T_{STALLED}^{Mobility} \approx 289.318\,ms$ because not only SADs must be updated, but also routing policies.

This confirms IPsec configuration time derived from figure 4a to create a SA. Furthermore, comparison between *Mobility* and *Multihoming* shows how Network Managers may improve the EU experience by performing a Mobility and thus avoiding the RRC exchange. Furthermore, Network Manager may improve further the EU experience by preparing the Mobility and performing a Soft Handover rather than a Hard Handover. Hard Handover results in a $300\,ms$ stalled communication whereas Soft Handover is expected to no interruption at all. On the other hand, Soft Handover requires to handle Multiple Interfaces which requires MOBIKE-X extension.

D. MOBIKE-X Mobility Multihoming

MOBIKE-X extends MOBIKE for the TRANSPORT mode and Multiple Interfaces, which enables Soft Handover. Soft Handover provides the ability to change interface without losing any packets. In moving to a new Interface with Hard Handover discards that are on the Network between the time Hard Handover has been started and the time the Server starts sending on the new interface. From measurements in figure 7a,

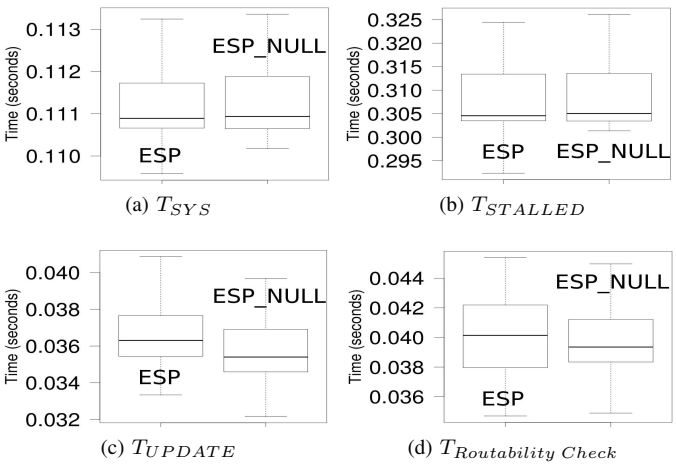
we estimate that discovering the new interface and starting the IPsec update takes around $T_{SYS} = 110.9095\,ms$, but it may take more time to configure it for example if authentication to the new Network is required and the IP addresses is obtained via DHCP. Such delays may not impact the communication if the MMN has Multiple Interfaces. If the MMN has a single interface, those delays must be added to $T_{STALLED}$.

Our MOBIKE-X implementation always performs Routability Checks, which, for Mobility operation, may be avoided. Thus $T_{STALLED} \approx 264\,ms$, which is between 9.3% and 15.6% faster than MOBIKE.

With TRANSPORT mode $T_{UPDATE} = 36.6035ms$ is 2.69 times larger than with the TUNNEL mode because SAD and SPD whereas TUNNEL mode only updates SAD. With Soft Handover time and delay is less critical, it delays slightly the Handover, but does not results in loss of packets. On the other hand, T_{UPDATE} is around $2.RTT$ when the MMN is offloaded in a *Public HotSpot* which may not affect greatly the EU Experience.

$T_{Routability\ Check} = 39.943\,ms$ is smaller than with MOBIKE. RRC is not different from MOBIKE, and one way to explain the difference is to consider the testing conditions. With MOBIKE-X, we measured duration with the ping application whereas MOBIKE has been tested with a TCP connection. *pings* probably do not fill the NIC buffer as SCTP/TCP packets do. We used pings because SCTP does not support mobility operation, that is changing its interface IP address.

Measurements confirm previous results. Using TRANSPORT mode reduces interactions with the Network stacks and communication overheads. In fact TRANSPORT avoids tunnelling, and do not need the tunnel IP header. As a result, Mobility is performed faster, changes are detected faster by the system —for example when Multihoming is performed. This provides competitive advantages for the E2E architecture compared to I-WLAN. This paper also shows that Hard Handover always results in degrading the EU experience. However optimized, changing the IP address of a given communication always requires inter-process communications with their own latencies. One way to reduce the Mobility impact on the EU experience is to perform Soft Handover. MOBIKE-X provides this facility, which can be used in the I-WLAN and the E2E architecture.



(a) T_{SYS} (b) $T_{STALLED}$ (c) T_{UPDATE} (d) $T_{Routability\ Check}$

Fig. 7. MOBIKE-X MM Performances

VII. Conclusions

This paper compares two architectures for offloaded MMNs:

- the E2E architecture which provides End-to-End communication between the offloaded MMN and the server
- the I-WLAN architecture that tunnels communication of the offloaded MMN to a security Gateway in the ISP CORE network.

E2E offers multiple advantages over I-WLAN: (1) E2E secures only traffic that requires to be secured, (2) Security can be configured according to both the application privacy requirements and the network level of trust. Furthermore, (3) Communications do not suffer from routing indirections, (4) ISPs can both optimize transport and security to provide the best EU experience and (5) E2E prevents ISP CORE network from overloading. On the other hand, E2E and I-WLAN are still expected to co-exist, I-WLAN provides a secure network access service while E2E secures the application traffic.

The use of TRANSPORT mode versus TUNNEL mode with Real Time Application first reduces both network configuration complexity and cryptographic operations. This significantly reduces the number of CPU cycles ($\approx 25\%$ for cryptographic computation). Moreover, the TRANSPORT mode makes the system more reactive. It detects interface changes around 2.9 times faster, presents 2.5 times less variations for both down interface detection (T_{SYS}) and stalled communications ($T_{STALLED}$) (cf. section VI-B). As a result, Mobility is performed around 15% faster (section VI-B). On the other hand, TUNNEL mode with more complex routing configuration may result in stalling the communication for few seconds (figure 3e). MOBIKE shows that specific configurations can partly overcome this issue, but this is done at the expense of layer / process independence. Finally E2E and TRANSPORT mode optimizes MM for secure offloaded communications.

Eventhough E2E and TRANSPORT mode optimize MM compared to I-WLAN and the TUNNEL mode, to reduce drastically MM, the MMN may anticipate MM operations and prefer Soft Handover to Hard Hand as performed by the current MOBIKE. In fact, Multihoming relies on system interface detection and requires further network verifications such as Return Routability Check which stalls the communication around 5.7% longer than Mobility. As a result Network Manager are encouraged to perform Mobility operation rather than relying on failover mechanisms like Multihoming.

During this experimentation, we found out that multiple layers (IPsec, SCTP...) interact with MM. Although they have been designed to work independently, implementations do have strong interactions. We found a significant interest in specifying interactions between the different layers, and our current research includes the design of an IPsec API that would make possible applications and SCTP to take advantage of IPsec features (mobility, multihoming, authentication...).

REFERENCES

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

[2] D. Migault, "MOBIKE eXtension (MOBIKE-X) for Transport Mobility and Multihomed IKE_SA," (Work in Progress), Internet Engineering Task Force, Sep. 2009.

[3] P. Eronen, "IKEv2 Mobility and Multihoming Protocol (MOBIKE)," RFC 4555 (Proposed Standard), Internet Engineering Task Force, Jun. 2006.

[4] Cisco, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 20102015," Feb. 2011. [Online]. Available: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html

[5] W. Lehr and L. W. Mcknight, "Wireless Internet access: 3G vs. WiFi?" *Telecommunications Policy*, vol. 27, no. 5-6, pp. 351–370, 2003.

[6] A. Handa, "3G/WiFi Seamless Offload," Mar. 2010.

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

[8] A. Handa, "Mobile Data Offload for 3G Networks," (Work in Progress), Intellinet, Oct. 2009.

[9] 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," Analysys Masson, Tech. Rep., dec 2011.

[10] C. Perkins, "IP Mobility Support for IPv4, Revised," RFC 5944 (Proposed Standard), Internet Engineering Task Force, Nov. 2010.

[11] N. Ferguson and B. Schneier, "A cryptographic evaluation of ipsec," Counterpane Internet Security, Inc, Tech. Rep., 2000.

[12] C. A. Shue, M. Gupta, and S. A. Myers, "Ipsec: Performance analysis and enhancements," in *IEEE International Conference on Communications (ICC)*, jun 2007.

[13] A. Hoban, "Using intel aes new intsruction and pclmulqdq to significantly improve ipsec performance on linux," in *Intel Corporation*, Aug. 2010.

[14] G. L. Garcia, "Ipsec performance analysis for large-scale radio access," in *Helsinki University of Technology, Master Thesis*, Jul. 2008.

[15] R. Malik and R. Syal, "Performance analysis of ip security vpn," in *International Journal of Computer Applications*, vol. 8, no. 4, oct 2010, p. 0975 8887.

[16] S. Bellovin, J. Ioannidis, A. Keromytis, and R. Stewart, "On the Use of Stream Control Transmission Protocol (SCTP) with IPsec," RFC 3554 (Proposed Standard), Internet Engineering Task Force, Jul. 2003.

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

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

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

[20] E. Unurkhaan, E. P. Rathgeb, and A. Jungmaier, "Secure sctp - a versatile secure transport protocol," *Telecommunication Systems*, vol. 27, no. 2-4, pp. 273–296, 2004.

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

[22] R. Stewart, Q. Xie, M. Tuexen, S. Maruyama, and M. Kozuka, "Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration," RFC 5061 (Proposed Standard), Internet Engineering Task Force, Sep. 2007.

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

[24] R. Moskowitz and P. Nikander, "Host Identity Protocol (HIP) Architecture," RFC 4423 (Informational), Internet Engineering Task Force, May 2006.

[25] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson, "Host Identity Protocol," RFC 5201 (Experimental), Internet Engineering Task Force, Apr. 2008.

[26] P. Nikander and J. Melen, "A Bound End-to-End Tunnel (BEET) mode for ESP," (Work in Progress), Internet Engineering Task Force, Aug. 2008.

[27] C. Perkins, "IP Mobility Support for IPv4," RFC 3220 (Proposed Standard), Internet Engineering Task Force, Jan. 2002, obsoleted by RFC 3344.

[28] Space, S. Fu, and M. Atiquzzaman, "Sctp: State of the art in research, products, and technical challenges," pp. 64–76, apr 2004.

[29] T. Heer, T. Jansen, R. Hummen, S. Götz, H. Wirtz, E. Weingärtner, and K. Wehrle, "Pisa-sa: Municipal wi-fi based on wi-fi sharing," in *ICCCN*, 2010, pp. 1–8.

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

[31] R. Stewart, "Stream Control Transmission Protocol," RFC 4960 (Proposed Standard), Internet Engineering Task Force, Sep. 2007, updated by RFC 6096.

[32] B. Han, P. Hui, V. A. Kumar, M. V. Marathe, G. Pei, and A. Srinivasan, "Cellular traffic offloading through opportunistic communications: a case study," in *Proceedings of the 5th ACM workshop on Challenged networks*, ser. CHANTS '10, 2010, pp. 31–38.

[33] B. Han, P. Hui, and A. Srinivasan, "Mobile data offloading in metropolitan area networks," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 14, pp. 28–30, November 2010.

[34] K. Lee, I. Rhee, J. Lee, Y. Yi, and S. Chong, "Mobile data offloading: how much can wifi deliver?" *SIGCOMM Comput. Commun. Rev.*, vol. 40, pp. 425–426, August 2010.

[35] S. Kent and K. Seo, "Security Architecture for the Internet Protocol," RFC 4301 (Proposed Standard), Internet Engineering Task Force, Dec. 2005, updated by RFC 6040.

[36] C. Kaufman, "Internet Key Exchange (IKEv2) Protocol," RFC 4306 (Proposed Standard), Internet Engineering Task Force, Dec. 2005, obsoleted by RFC 5996, updated by RFC 5282.

[37] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246 (Proposed Standard), Internet Engineering Task Force, Aug. 2008, updated by RFCs 5746, 5878, 6176.

[38] T. Phelan, "Datagram Transport Layer Security (DTLS) over the Datagram Congestion Control Protocol (DCCP)," RFC 5238 (Proposed Standard), Internet Engineering Task Force, May 2008.

[39] T. Kivinen and H. Tschofenig, "Design of the IKEv2 Mobility and Multihoming (MOBIKE) Protocol," RFC 4621 (Informational), Internet Engineering Task Force, Aug. 2006.

[40] D. Migault, "IPsec mobility and multihoming requirements : Problem statement," (Work in Progress), Internet Engineering Task Force, Sep. 2009.

[41] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (EAP)," RFC 3748 (Proposed Standard), Internet Engineering Task Force, Jun. 2004, updated by RFC 5247.

[42] P. Eronen, H. Tschofenig, and Y. Sheffer, "An Extension for EAP-Only Authentication in IKEv2," RFC 5998 (Proposed Standard), Internet Engineering Task Force, Sep. 2010.

[43] H. Haverinen and J. Salowey, "Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)," RFC 4186 (Informational), Internet Engineering Task Force, Jan. 2006.

[44] J. Arkko and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)," RFC 4187 (Informational), Internet Engineering Task Force, Jan. 2006, updated by RFC 5448.

[45] E. Nordmark and M. Bagnulo, "Shim6: Level 3 Multihoming Shim Protocol for IPv6," RFC 5533 (Proposed Standard), Internet Engineering Task Force, Jun. 2009.

[46] A. Ford, C. Raiciu, M. Handley, S. Barre, and J. Iyengar, "Architectural Guidelines for Multipath TCP Development," RFC 6182 (Informational), Internet Engineering Task Force, Mar. 2011.

[47] StrongSwan, "the OpenSource IPsec-based VPN Solution." [Online]. Available: http://www.strongswan.org

[48] LKSCTP, "Linux Kernel SCTP." [Online]. Available: http://sourceforge.net/projects/lksctp/

[49] sctplib, "The SCTP library." [Online]. Available: http://www.sctp.de/sctp-download.html