Ruckus
Simply Better Wireless.

white paper

Integrating Wi-Fi RANs into the Mobile Packet Core

ENABLING THE VISION OF HETEROGENEOUS NETWORKING THROUGH THE CONVERGENCE OF WI-FI AND 3G/LTE TECHNOLOGY

Introduction

There has been a great deal of interest of late in using Wi-Fi to offload traffic from heavily congested mobile networks. Early deployments consisted of building a parallel Wi-Fi offload network that takes traffic directly to the Internet. The mobile network operator would implement a proprietary client of some kind that would manage the offload function. Many subscribers have implemented their own offload strategy by selecting Wi-Fi when it's available.

Now the industry is shifting its focus toward integrating Wi-Fi RANs into the mobile packet core. In this approach, Wi-Fi would take its place alongside 3G/LTE as a cornerstone technology in the mobile world. The mobile device selects the best radio access technology based on the conditions (typically signal strength, application type, default to Wi-Fi, etc.) and the subscriber is automatically authenticated and connected. This is a manual process today, but the industry is moving rapidly toward automating all this under a combination of operator and subscriber control. All RAN traffic is brought back into the mobile packet core, and from there it goes to the mobile operator's service complex, the Internet, or a corporate intranet. To make this HetNet vision a reality, the experience of connecting to Wi-Fi must be made as simple and secure as when connecting to cellular. The services must also be the same, and it should even be possible to seamlessly handoff between Wi-Fi and cellular RAN technologies. This vision requires that operators maintain the same level of control regardless of the RAN type.

Integrating Wi-Fi RANs into the Mobile Packet Core

ENABLING THE VISION OF HETEROGENEOUS NETWORKING THROUGH THE CONVERGENCE OF WI-FI AND 3G/LTE TECHNOLOGY

The services that are available in the mobile packet core include:

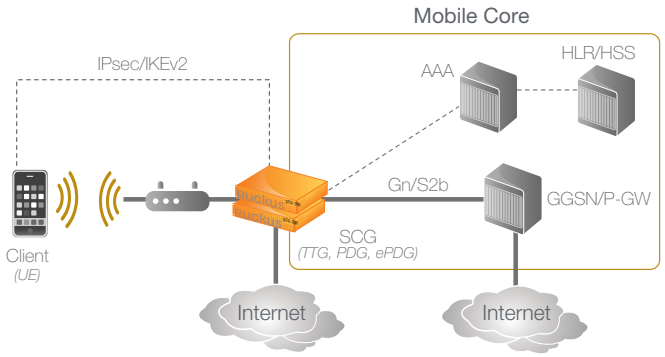
- Pre-paid and post paid billing (with zero rating)
- Lawful intercept
- Deep packet inspection and analytics
- Content filtering (including parental controls)
- IP address assignment (to support seamless inter-RAT handover)
- Roaming[1]
- DNS, NAT, Firewall, etc.
- HLR/HSS Subscriber Database
- IP Multimedia Subsystem (IMS)
- Mobility management
- Voice over IMS
- Etc.

3GPP (the 3rd generation partnership project) has developed two different approaches to integrating Wi-Fi into the mobile packet core. The first assumes untrusted WLAN access and the second assumes trusted WLAN access. The work on untrusted WLAN access first appeared as part of the I-WLAN effort in 3GPP Release 6, which defined a TTG (tunnel termination gateway) and a PDG (packet data gateway) to provide the interworking function. This work was extended in 3GPP Release 8 with the introduction of the ePDG (evolved packet data gateway) for LTE. Beginning in Release 11 (TS 23.402 V11.3.0 (2012-06), 3GPP has introduced a new architecture for trusted WLAN access based on the work of the S2a Mobility based on GTP (SaMOG)[2] working group. This paper will examine both approaches in more detail.

Untrusted WLAN access

The assumption in untrusted WLAN access is that the mobile operator need not know anything about the Wi-Fi network that originated the connection. That operator could be a hotel, airport, cable operator, aggregator, etc. The mobile operator would have to have a roaming arrangement with that entity, but didn't need to know much else. In most early Wi-Fi deployments the security was modest to non-existent, so this was a valid approach. 3GPP's solution was to have the mobile device set up an IPsec

FIGURE 1: Untrusted Wireless LAN Access Using TTG, PDG, or ePDG Functionality



session using IKEv2 for authentication and tunnel over the Wi-Fi access network. These tunnels would terminate on a massively scalable IPsec concentrator back in the mobile operator's data center. This concentrator function is integrated into the TTG part of a PDG (a PDG consists of a TTG and selected elements of a GGSN). When connecting back into an existing GGSN, only the TTG function is utilized. The TTG/PDG constructs are specific to 3G, and are replaced with an ePDG when moving to LTE. This is sometimes called an overlay model and it requires nothing more from the access layer than a simple bit pipe. It does, however, put a significant burden on the mobile device and the mobile packet core.

That burden consists of a requirement that mobile device vendors implement an IPsec/IKEv2 client on their smartphones, and the mobile packet core vendors had to develop TTG/PDG/ePDG technology. While the latter has happened, the former hasn't. Mobile device vendors have been unwilling to develop the necessary client software, which has prevented this approach from gaining traction. The reason for this reluctance is that IPsec/IKEv2 is a complicated and processor intensive protocol that loads down the mobile device. It is also makes for an overly cumbersome connection process as the user must first authenticate to the Wi-Fi AP (using whatever protocol is required by the AP) and then get an IP address which is used to setup an IPsec tunnel back to the mobile packet core where it must authenticate all over again to get yet another IP address for the actual session. Tunneling also makes the access layer invisible, which removes the opportunity to apply policy, quality of service, perform local breakout, etc. There have been variations on this theme using Mobile IP, but they all suffer from similar problems with regards to mobile device support and complexity. The net result is that the

1 In this document we will use the mobile definition of roaming which refers to the ability to use your mobile device on the network of an operator for which you do not have a business arrangement, versus the Wi-Fi definition which means to be handed off from one AP to another.

2 The SaMOG work is described in 3GPP TR (technical report) 23.852 V1.1.0 (2012-05). That work was then incorporated into TS (technical specification) 23.402 V11.3.0 (12-06). SaMOG can also support mobility over PMIP.

Integrating Wi-Fi RANs into the Mobile Packet Core

ENABLING THE VISION OF HETEROGENEOUS NETWORKING THROUGH THE CONVERGENCE OF WI-FI AND 3G/LTE TECHNOLOGY

FIGURE 2: Trusted Wireless LAN Access Using TWAG Functionality

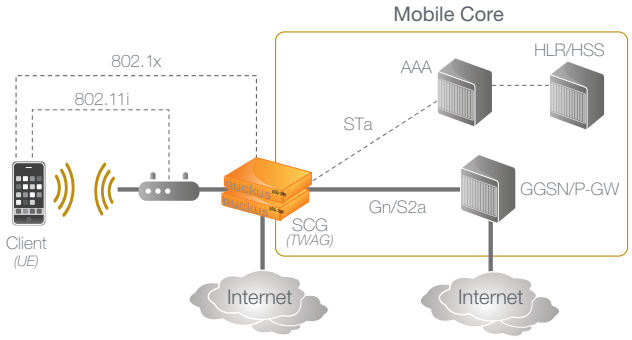
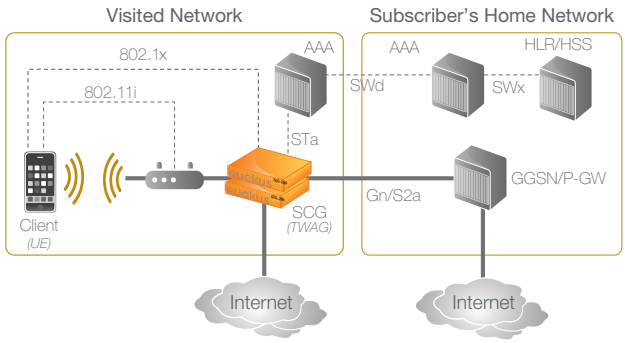


FIGURE 3: Trusted Wireless LAN Access While Roaming



industry has continued to look for a better solution.

Trusted WLAN access

A better solution came by way of the S2a Mobility based on GTP (SaMOG) working group in 3GPP. Their approach has been introduced in 3GPP Release 11 for LTE RANs, and it can easily be extended to support 3G RANs. The focus of the SaMOG effort was to eliminate the requirement for an IPsec/IKEv2 client on the mobile device. To do this, the WLAN needed to be trusted[3] and 802.1x was well suited to the job. This protocol has gotten plenty of support from the mobile device and Wi-Fi AP communities. It addresses all mobile industry concerns around ease of use and security by utilizing EAP (extensible authentication protocol) for secure authentication and 802.11i for Wi-Fi airlink encryption. This combination provides everything that IPsec/IKEv2 did, but with far less complexity. EAP supports a variety of different authentication methods including EAP-SIM, EAP-AKA (and AKA'), EAP-TTLS, and EAP TLS. EAP-AKA' is an enhancement to EAP-AKA, and is the preferred approach by most mobile operators. This combination of EAP authentication and 802.11i airlink encryption are also key building blocks in the Hotspot 2.0 initiative.

- EAP-SIM is used to authenticate SIM-based devices over Wi-Fi, and EAP-AKA does the same for USIM-based devices. Being able to use a SIM (2G) or a USIM[4] (3G/LTE) card to authenticate regardless of the RAN type makes for a seamless authentication experience.
- EAP-TLS is used with X.509 certificates and EAP-TTLS with username and password. The former is a very good option for laptops, digital cameras, and tablets as it enables a seamless connection experience without the need for SIM cards, and the latter will always be a good option for serving drop-in customers.

The key piece of network equipment that is required for trusted access is the Trusted WLAN Access Gateway (TWAG). On the RAN side it connects to tens of thousands or even hundreds of thousands of Wi-Fi APs that can optionally be encrypted. On the mobile packet core side it connects to a PDN Gateway via the S2a interface using GTPv2 (GPRS tunneling protocol) or a GGSN using the Gn interface and GTPv1. Proxy Mobile IP (PMIP) can also be used in place of GTP for CDMA-based operators moving to LTE.

The GTP tunnel is used to activate a session between the TWAG and the GGSN/P-GW as part of the connection setup process. This involves the creation of a data structure in the TWAG and in the anchoring GGSN/P-GW. These data structures include the subscriber's IP address, subscriber's IMSI, subscriber's tunnel endpoint ID (TEID) at the GGSN/P-GW, tunnel endpoint ID (TEID) at the TWAG, and much more. If the subscriber is handed off to another TWAG or an S-GW during a mobility event, the session must follow.

One final interface of note is the STa, which relays authentication credentials between the TWAG and the 3GPP AAA Server. These credentials are then passed on to the HLR/HSS for final processing.

This approach is called trusted WLAN access, because it requires that the Wi-Fi operator implement 802.1x[5] along with 802.11i. It is expected that mobile operators will implement these protocols on their APs and will only roam with Wi-Fi partners that also use these protocols. For a partner to roam with a mobile operator they will need to terminate their APs on their own TWAG

3 The decision on whether a WLAN network is trusted or untrusted is made by the mobile operator. The typical requirement for "trust" is that the subscriber be securely authenticated and all data communications over the airlink be encrypted.

4 For the remainder of this document we will simply refer to SIM cards for simplicity.

5 802.1x makes use of a supplicant that runs on the mobile device, an authenticator that runs on the TWAG, and an authentication server which runs on the HLR/HSS.

and then tunnel back to the mobile operator's GGSN/P-GW (see Figure 3) through a global roaming exchange using GTP. This assumes that the subscriber's data is always tunneled back to the home network, which is the standard in the mobile world. 3GPP is looking at options that will support local breakout when roaming. In this approach mobile data traffic is anchored to a GGSN/P-GW in the visited network, instead of the normal practice of bringing it all the way back to the home network. Local breakout can also be implemented in the home network by using the mobile infrastructure to authenticate the subscriber, but then offloading their traffic directly to the Internet. Since traffic is not being brought back into the mobile packet core, the set of services that could be offered to the subscriber will be very limited.

In our roaming scenario the subscriber will need to authenticate through a local AAA server in the visited network which will proxy it back to a AAA server in the home network, which then connects to the HLR/HSS subscriber database.

Roaming is one of the interesting ways in which trusted WLAN access differs from untrusted WLAN access. In the latter the TTG/PDG/ePDG is always in the home network regardless of where the subscriber might be, and all traffic is tunneled back over IPsec. With trusted WLAN access, the TWAG is always in the visited network and traffic is tunneled back over GTP to the GGSN/P-GW in the home network (or broken out locally). This is also how cellular networks operate when the user is roaming (the SGSN or Serving Gateway is always in the visited network).

Trusted WLAN Access & Non-SIM Devices

There is another kind of breakout that also needs to be supported by the TWAG gateway. Wi-Fi networks are used by hundreds of millions of laptops and tablets that do not have cellular modems and therefore do not have SIM cards, but still have a great need for Internet access. Mobile operators can address this need with EAP-TLS and x509 certificates. This approach gives the same seamless authentication procedure that EAP-SIM does, but no SIM is required. However, since there is no SIM the traffic can't be brought back to the core. Instead, it needs to be offloaded to the Internet at the Trusted WLAN Access Gateway (TWAG). The supporting of non-SIM devices will require additional capabilities at the TWAG including billing, policy, and lawful intercept support to name a few (functions that are normally provided in the mobile packet core). The decision on how to route the user is made at the time of authentication. By adding this offload capability, mobile operators can now target the hundreds of millions of non-cellular equipped Wi-Fi devices that need seamless authentication, security, and a really good global roaming solution. Support for non-SIM devices is probably best handled by distributing the TWAG function out close to the Wi-Fi RAN, as there is no need to backhaul this traffic to the mobile packet core.

Hotspot 2.0

A key piece of the vision for integrating Wi-Fi into the mobile packet core involves automating the process of discovering and selecting an AP when roaming. This is being addressed by the Hotspot 2.0 program, which is being driven by the Wi-Fi Alliance and the Wireless Broadband Alliance. Phase 1 of this standard has already been approved and it will soon be available on mobile devices. Phase 2 will address non-SIM devices and the downloading of operator policy into mobile devices. This work is also being augmented by the ANDSF effort in 3GPP. The Access Network Discover and Selection Function (ANDSF) will allow the network to notify the mobile device about APs in its proximity.

Getting Connected

This section look at the process of getting connected when using trusted WLAN access.

The mobile device starts by automatically scanning all available SSIDs and when is sees one it recognizes it will begin the authentication process. If the mobile device does not see an SSID it recognizes, it can use Hotspot 2.0 technology to quickly find a roaming partner. Devices with SIM cards will be authenticated with EAP-SIM. For all non-SIM devices authentication can be via EAP-TTLS or EAP-TLS[6]. The mobile operator's AAA server will proxy the EAP-SIM authentication request back to the HLR/HSS. Once authentication is completed and a session has been established, the user can connect and begin transmitting. Mobile devices with SIM cards will have their traffic backhauled to the Internet by way of the mobile packet core and devices that don't have SIM cards will be offloaded to the Internet at the TWAG (or even at the AP). Figure 4 shows the sequence of steps required to establish on connection when using trusted WLAN access and a SIM device. The description that follows is greatly simplified for purposes of this document.

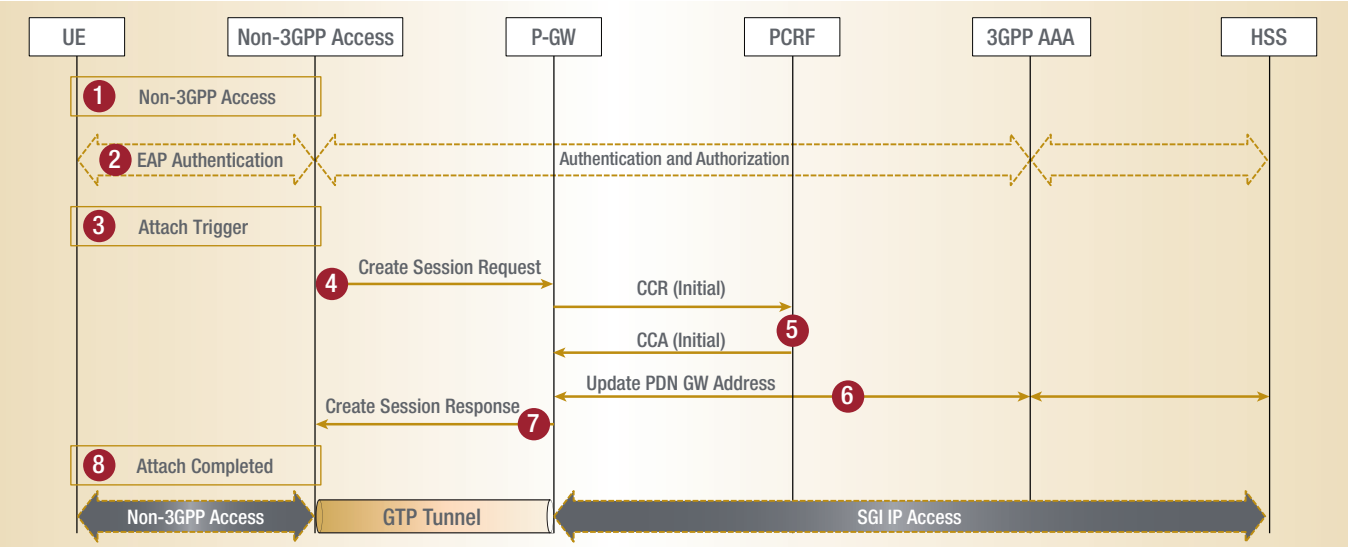
1. Wi-Fi access is initiated
2. EAP Authentication takes places with the AAA/HSS back in the mobile core.
3. After successful authentication and authorization, the Wi-Fi specific L3 attach procedure is triggered.
4. The TWAG sends a Create Session Request message to the P-GW. This includes all parameters in the PDP context.

6 Portal based solutions using WISPr are also an option, but they require user intervention and are not secure.

Integrating Wi-Fi RANs into the Mobile Packet Core

ENABLING THE VISION OF HETEROGENEOUS NETWORKING THROUGH THE CONVERGENCE OF WI-FI AND 3G/LTE TECHNOLOGY

FIGURE 4: Connected Sequence for Trusted Wireless Access



5. The P-GW initiates the IP CAN Session Establishment Procedure with the PCRF (policy and charging rules function).
6. The P-GW informs the AAA Server of its P-GW identity and the APN corresponding to the UE's PDN connection. The message includes information that identifies the PLMN (public land mobile network) in which the P-GW is located. This information is registered in the HSS.
7. The P-GW then sends a Create Session Response message to the TWAG, including the IP address allocated for the UE.
8. L3 attach procedure is completed and the IP address information is provided to the UE.

The sequence will be very different in a roaming application where traffic is backhauled to the home network, and in roaming applications that use local breakout. The use of PMIP instead of GTP also changes things.

Next Steps for Mobile Operators

The industry is moving forward with trusted WLAN access based on the SaMOG model, which has been incorporated into 3GPP Release 11. TWAG gateways will start to emerge later this year and they will be able to interwork with mobile devices that are already shipping. This is a compelling solution that addresses all of the problems with the I-WLAN approach including the unwillingness of mobile device vendors to develop IPsec/IKEv2 clients. With trusted WLAN access, mobile operators have an architecture that makes Wi-Fi access as simple and secure as cellular access. It also uses protocols that are already broadly deployed in the industry. Mobile operators can greatly increase their footprint in a very cost effective manner by using Wi-Fi to complement their 3G/LTE build-outs.

- The experience of getting connected will be the same.
- The set of mobile operator services will be the same, it will even be possible to enable seamless handoff as subscribers move from 3G/LTE to Wi-Fi and back again.

Subscribers no longer need to know or care about RAN technologies. Instead, they get an always best-connected experience. Operators also have the opportunity to use their Wi-Fi assets to generate revenue from the hundreds of millions of Wi-Fi only laptops, tablets, and digital cameras that need connectivity while on the move. Mobile operators that successfully

Ruckus®
Simply Better Wireless.

Ruckus Wireless, Inc.
350 West Java Drive
Sunnyvale, CA 94089 USA
(650) 265-4200 Ph \ (408) 738-2065 Fx

www.ruckuswireless.com