S3-020570

Cellular – WLAN Interworking

Activities in ETSI/MMAC and WIG Status

3GPP SA3 - Munich - 10th October2002

Robert Hancock
Siemens/Roke Manor Research

Overview

Roke Manor Research

- Organisation – who's doing what
  - Current status
- Technical scope
  - Network and layer and functionality boundaries
- Security overview
  - Issues (Q&A)
- ***Main work is sorting out standardisation scope and domain structure issues***
  - Not detailed cryptographic or protocol analysis
  - "Everything is in a state of flux"

Status and Background

Roke Manor Research

- ETSI BRAN (Hiperlan Area) started requirements and architectures work on integration Hiperlan/2 into UMTS mid-2000
  - TR approved mid-2001
- Work on technical specification started
  - Concentrating on ‘loose coupling’ architectural approach
  - Phased release concept
    - R1 = mainly basic authentication
    - R2 = everything else

Status: Other Bodies

Roke Manor Research

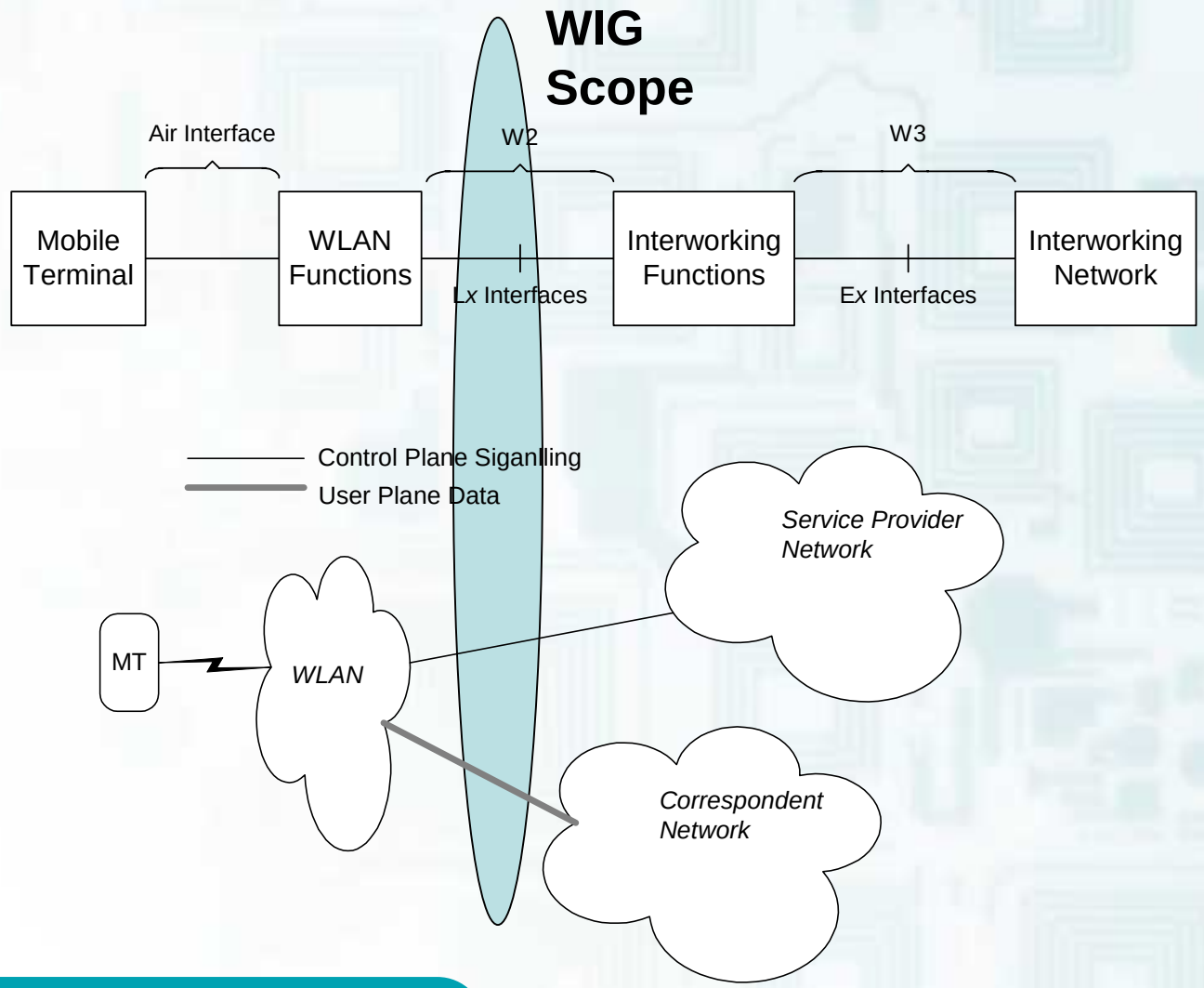
- MMAC (HiSWANa committee) joined effort to develop “common standard” for Hiperlan/2 and HiSWANa
  - Initial MMAC interworking standard already exists and deployed
- MMAC/ETSI liaison → SA3, S3-020428 response (which is why I am here)
- Several discussions with IEEE 802.11
  - Subject home is 802.11 WNG steering committee
  - TGi developing MAC security enhancements
    - Uses .1x for authentication extended for key exchange

Formation of WIG

Roke Manor Research

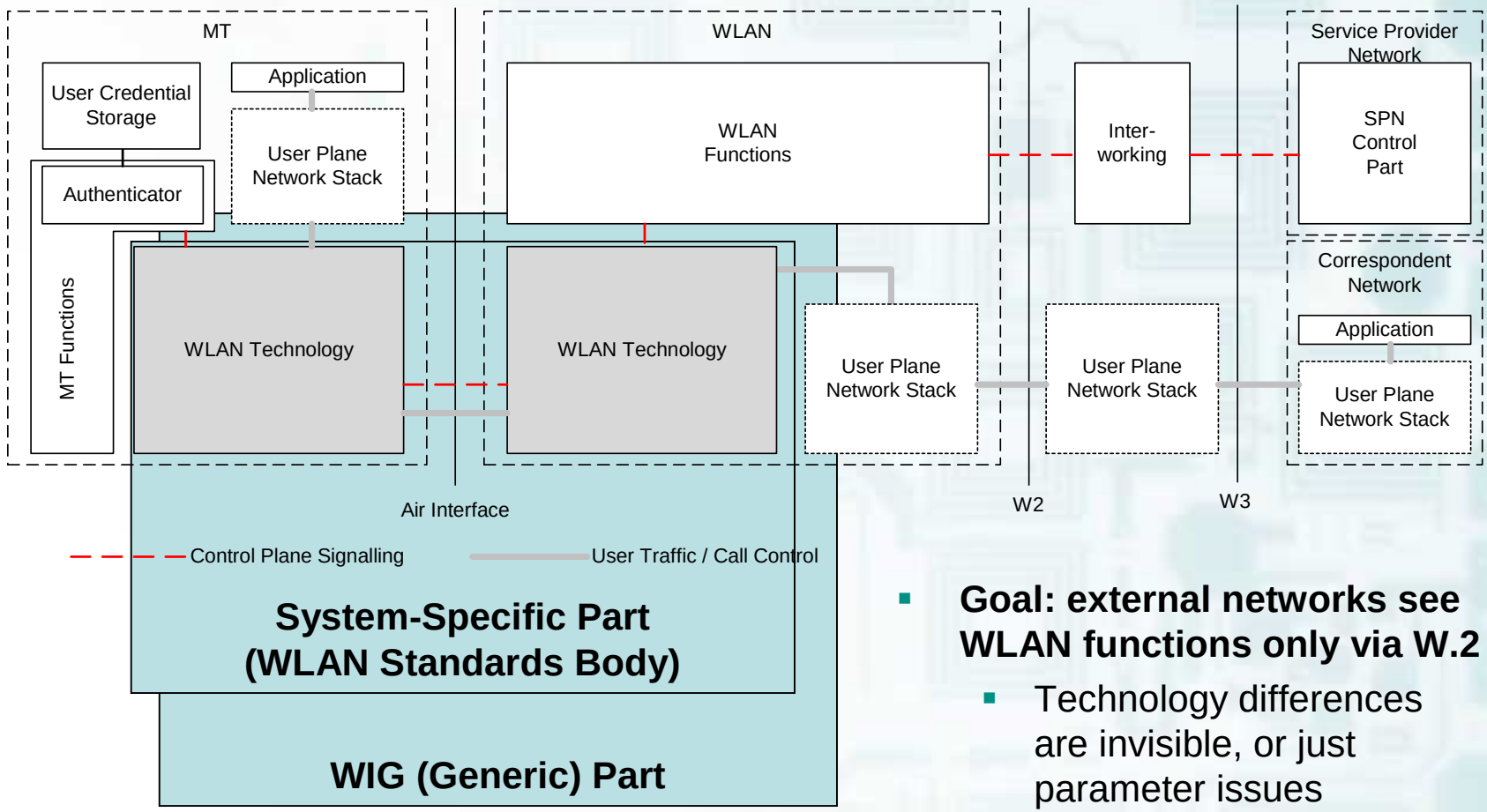
- Wireless LAN Interworking Group is a cooperation between ETSI BRAN, MMAC HiSWAN and IEEE 802.11
- Agree a common “interworking reference point” between WLAN standards and “Public” networks (2G, 3G, WISPs, and variants)
- *May extend to other short range standards*
- No official documents but baseline contribution based on past agreed ETSI DTS text “imminent”
- Liaison WIG → SA3 “imminent”

Scope: Networks



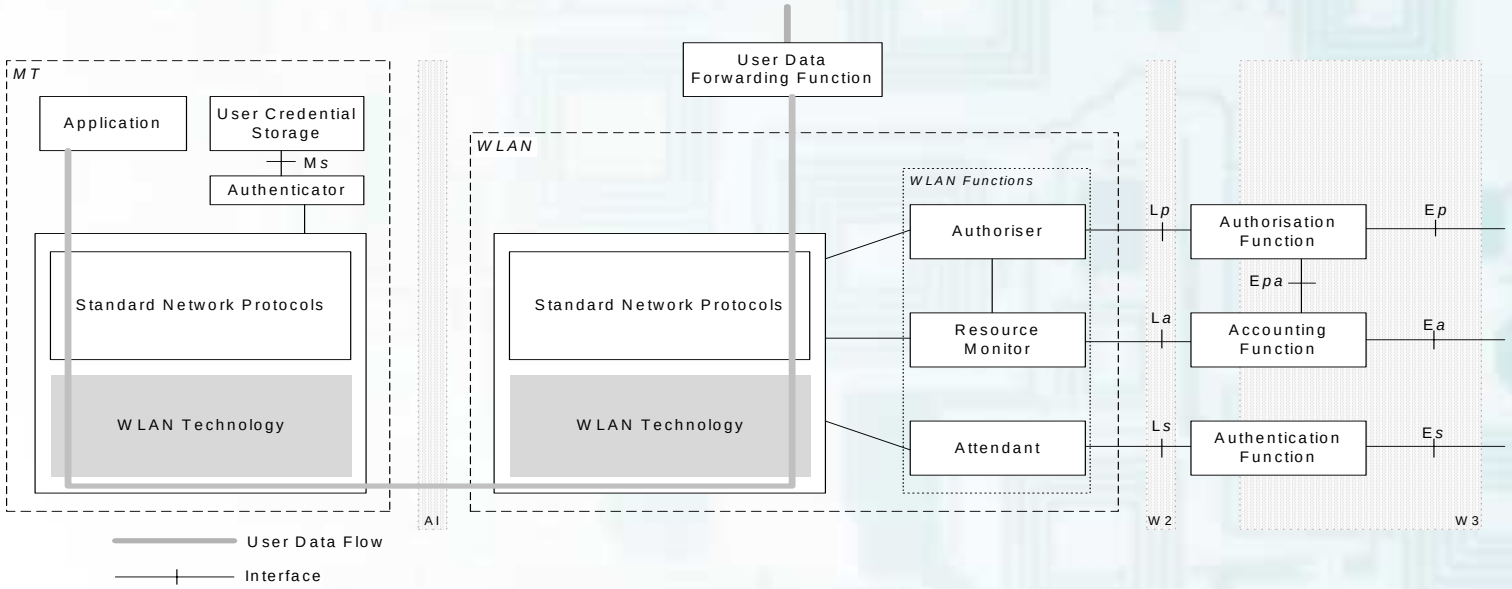
- **Internal WLAN topology is not visible**

Scope: Layers



- **Goal: external networks see WLAN functions only via W.2**
  - Technology differences are invisible, or just parameter issues

Scope: Functionality for R1



- Ls – authentication (and key management)
- Lp – authorisation (service filtering)
- La – accounting (basic usage reporting)

R1 Functionality Goals

Roke Manor Research

- Detailed requirements developed for Ls, some Lp, a few for La
  - Scope is W.2, not full system
- Authentication: protocol capable of mutual authentication and key management that can support air interface security requirements
- Authorisation: allow network to configure service access (packet filters)
- Accounting: most basic functionality only considered

Protocol for Ls?

Roke Manor Research

- Universal starting assumptions (in BRAN):
- EAP
- Some Diameter application for transport
  - Diameter-EAP or Diameter-NASREQ subset
- Some significant “backwards” compatibility issues not yet discussed
  - CHAP-like authentication in HiSWANa
  - RADIUS (with vendor key AVPs?) in 802.11, HiSWANa

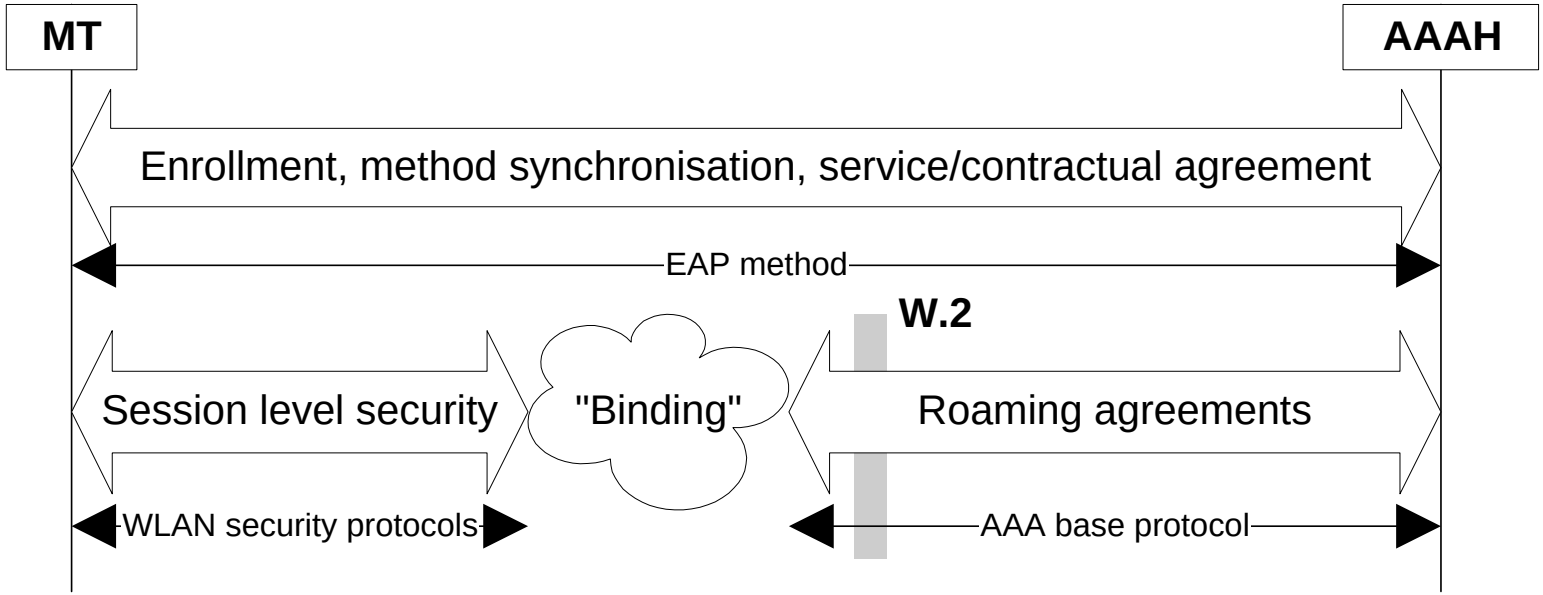
Will WIG Assume XXX?

Roke Manor Research

- Q: Any assumption on use of a xSIM card?
- A: No
  - “Upper layer issue” out of scope of W.2
  - Enforcement of hardware token can be fully controlled by service provider during enrolment
- Q: Any assumption of EAP method?
- A: No
  - Proper analysis is (very) hard
  - Choice might be SPN dependent
  - Properties desired: mutual authentication, MitM protection, identity protection (from AN as well)

“Trust” Architecture

Roke Manor Research



- Trust model is not formally specified
  - But widely assumed (!)
- Hard “binding” problem strictly inside WLAN domain
  - W.2 only addresses the AAA protocol and “application”
  - Could extend all the way to the AP

Key Material Requirements

Roke Manor Research

- Require EAP method to generate keying material for several purposes
  - Initial setup of cryptographic protocols
  - “Association” negotiation post-validation
  - Rekeying (*maybe* related to re-authentication)
- Most details left to WLAN technology
  - At most, semantics of W.2/”EAP API” events defined
  - Uses of master key material listed
- Issues in multi-stage derivation from master key and cryptographic separation …

Group-Level Security

Roke Manor Research

- Required to operate a faithful wireless Ethernet service
  - ARP, network L2 browsing, future multimedia applications??
- WLAN technologies contain basic concepts for broadcast/multicast security
  - Actual security goals quite variable
- Practical security problems in public environment may well be intractable
- Probably an R2 issue for WIG

WLAN Network Topology

Roke Manor Research

- Security and other relationships are established between MT, AAAH and *overall WLAN network*
  - WLAN technology must handle security issues for local handover internally
    - E.g. key redistribution, filter list enforcement, accounting
- Internal security of WLAN infrastructure is probably out of scope of WIG and W.2
  - *Either* totally specific (e.g. 802.10 for IEEE)
  - *Or* totally generic (IP VPN solutions)
    - Level of integration with WLAN technology unclear

Conclusions

Roke Manor Research

- Based initially on ETSI work, WIG can serve to define a reference point and protocols which enable 3GPP “core” networks to exploit any WLAN technology
- The W.2 interface can be used as a vehicle for defining concrete requirements on the WLAN part of the overall system
  - Very important, especially for security
- Thanks for your time!

Background:

Roke Manor Research

- Further information
  - WIG reflector
  - **WIG@list.etsi.fr**
  - LS to SA3
  - **BRAN30d074 [Draft_LS_to_3GPPSA].doc**
  - WIG starting point proposal
  - **Currently BRAN30d135** (BRAN/MMAC internal)
  - **Will be posted to WIG reflector shortly**