UNIVERSITÀ DI PISA

Università degli Studi di Pisa

Facoltà di Ingegneria

Corso di Laurea Specialistica in

Ingegneria delle Telecomunicazioni

Autenticazione degli utenti in scenari WLAN-3G: valutazione delle caratteristiche e prestazioni di protocolli ed architetture

Candidato:

Pier Giorgio Raponi

Relatori:

Prof. Rosario G. Garroppo

Prof. Stefano Giordano

Anno Accademico 2006/07

Ai miei genitori

Indice

Lista degli acronimi utilizzati

3G 3^{rd} Generation

3GPP 3^{rd} Generation Partnership Project

AAA Authentication, Authorization and Accounting

AES Advanced Encryption Standard

AKA Authentication and Key Agreement

AP Access Point

AS Authentication Server

AuC Authentication Centre

AV Authentication Vector

CHAP Challenge Handshake Authentication Protocol

CN Core Network

CR Certificate Repository

CS Circuit Switched

EAP Extensible Authentication Protocol

EAPOL EAP over LAN

EAP-TLS EAP-Transport Layer Security

EAP-TTLS EAP-tunnelled Transport Layer Security

ECDSA Elliptic Curve Digital Signature Algorithm

GGSN Gateway GPRS Support Node

GMSC Gateway MSC

GSM Global System for Mobile Communications

HE Home Environment

HLR Home Location Register

HMAC keyed-Hash Message Authentication Code

HSS Home Subscriber Server

IETF Internet Engineering Task Force

IMSI International Mobile Subscriber Identity

IMS IP Multimedia Subsystem

LAN Local Area Network

MAC Message Authentication Code

MIP Mobile IP

MMS Multimedia Messaging Service

MSC Mobile Services Switching Centre

MS Mobile Station

MT Mobile Terminal

PDG Packet Data Gateway

PEAP Protected EAP

PKC Public Key Cryptography

PKI Public Key Infrastructure

PLMN Public Land Mobile Network

PS Packet Switched

RADIUS Remote Authentication Dial-In User Service

RAN Radio Access Network

RNC Radio Network Controller

SGSN Serving GPRS Support Node

TC Trust Centre

TKIP Temporal Key Integrity Protocol

TMSI Temporary Mobile Subscriber Identity

UE User Equipment

UICC UMTS Integrated Circuit Card

UMTS Universal Mobile Telecommunications System

USIM User Services Identity Module

UTRAN UMTS Terrestrial Radio Access Network

VLR Visitor Location Register

VoIP Voice Over IP

WAG WLAN Access Gateway

WEP Wired Equivalent Privacy

WISP Wireless Internet Service Provider

WLAN Wireless LAN

Introduzione

Il terminale mobile si sta rivelando lo strumento più diffuso per l'accesso al mondo dell'informazione globale del futuro, inoltre la maggior parte dei servizi di comunicazione e informazione sarà sviluppata e trasmessa in ambienti interconnessi con il protocollo IP, spina dorsale di Internet. Il fenomeno di crescita dei sistemi mobili — e la continua espansione del mondo Internet — implicano la probabile richiesta, da parte degli utenti, di usufruire di servizi interattivi multimediali e di potersi avvalere di questi in condizioni di mobilità, vale a dire in qualunque momento e in qualunque luogo. Per il successo di tali servizi, dovrà essere consentito un elevato grado di personalizzazione degli stessi da parte dell'utente, sia in termini di funzionalità sia di aspetto. Requisito tipico di questi nuovi servizi è, tra gli altri, la possibilità di effettuare chiamate o sessioni multiple contemporanee, per cui si renderanno necessarie velocità di trasmissione in aria più elevate rispetto a quelle impiegate dalle tecnologie di comunicazione odierne, e una conseguente maggiore ampiezza di banda disponibile. Non meno importante si rivelerà la possibilità di essere sempre connessi alla rete (always on), senza il peso attualmente derivante dalla onerosità delle connessioni a circuito.

Il sistema di comunicazioni mobili di terza e quarta generazione è il prossimo passo fondamentale nel mondo delle comunicazioni mobili. Uno degli ultimi sviluppi vitali nelle reti 3G sono i servizi basati su IP a commutazione di pacchetto e ad alte velocità di trasmissione. Il servizio a commutazione di pacchetto di terza generazione utilizza nuovi elementi architetturali per il routing dei pacchetti, l'indirizzamento a livello IP e la gestione della localizzazione e presenta buone caratteristiche di qualità del servizio, efficienza di trasmissione, servizi multimediali e alta capacità. Con le alte velocità di trasmissione e i servizi multimediali a , la rete 3G è una buona piattaforma per diversi servizi. Gli operatori di telefonica cellulare hanno necessità di considerare gli investimenti già preesistenti (maggiormente riguardanti le infrastrutture GSM) nello sviluppo delle successive tecnologie.

Motivazioni

Nonostante la rete cellulare di terza generazione possa fornire una velocità di trasmissione dati molto maggiore di quella 2G (arrivando fino a un massimo di 2 Mb/s) per fornire supporto e qualità ai nuovi servizi offerti (come, ad esempio, video chiamate e video streaming), essa soffre comunque di un data rate limitato e uno sviluppo costoso. Al contrario, le wireless local area network (WLAN) sono adottate globalmente dai service provider in piccole aree chiamate hotspot grazie al loro costo limitato, facilità di sviluppo e installazione e capacità di alte velocità di trasferimento (fino a 54 Mb/s nel caso della 802.11g) e al loro funzionamento in una banda frequenziale a libero accesso (banda ISM). Le WLAN hanno però sviluppo limitato e non possono fornire vasta copertura con la stessa efficienza di costi come invece permette la copertura 3G.

Per fornire una copertura wireless estesa al maggior territorio possibile, con un alto data rate e una grande varietà di servizi in hotspot e aree di dimensioni limitate, i service provider 3G guardano alla WLAN come a una tecnologia per migliorare l'offerta del sistema di terza generazione e quindi l'integrazione tra WLAN e reti 3G è vista come una scelta ideale poiché unirebbe la copertura a scala globale con l'accesso ad alta velocità in punti strategici come campus, università o aeroporti. In tabella 1 sono elencati i drivers e le barriere di queste due tecnologie di rete, evidenziando in modo chiaro la loro complementarietà piuttosto che concorrenzialità.

Scopo della ricerca

L'obiettivo iniziale della tesi era focalizzarsi sulle gestione della mobilità per gli utenti in roaming tra le reti WLAN e 3G e quindi uno scenario di tipo 4 (vedi tabella 2.1). Tuttavia è emersa subito la difficoltà di tale approccio, non solo per questioni tecniche inerenti il problema in sé, come ad esempio il livello al quale delegare la mobilità (link layer o network layer), ma anche e soprattutto per una consistente mancanza di prerequisiti. L'integrazione sempre più stretta tra le due reti può essere compiuta solo se ad ogni scenario corrisponde il raggiungimento di alcuni requisiti indispensabili per lo sviluppo degli scenario successivi e se manca tale fondamento non è possibile procedere. Sono emerse durante le prime fasi dello studio le grosse problematiche che comportava l'utilizzo del protocollo standardizzato di autenticazione EAP-AKA, con le quali diventava impossibile la gestione della mobilità a un qualsiasi livello. Si è dunque preferito procedere scendendo di un livello e affrontando lo studio dell'architettura di rete considerata e dei

	Wireless LAN	**3G**
Drivers	• basso costo di equipaggiamento per la tecnologia di accesso (operatori) e dei terminali (utenti) • basso costo di utilizzo e manutenzione • tecnologia disponibile pubblicamente • semplicità di configurazione	• copertura vasta • possibilità di roaming • adatto per il mercato di massa
Barriere	• sicurezza • limitata capacità di spostamento • problemi di login • soluzione di nicchia (solo utenti business)	• alti costi senza controllo prezzi • tecnologia non ancora disponibile e senza prove di performance disponibili

Tabella 1: Drivers e barriere per le WLAN e 3G (da [18]).

protocolli già standardizzati. Si è proceduto poi all'analisi dei problemi che questi protocolli non erano in grado di risolvere e allo studio delle soluzioni proposte in letteratura. Infine si è cercato di dare uno schema generale per la costruzione di un protocollo di autenticazione sicuro, flessibile, efficiente e veloce che possa essere una base solida su cui costruire i servizi previsti dagli scenari di integrazione successivi.

Capitolo 1

Basi matematiche

Verranno qui esposte brevemente le principali nozioni matematiche utilizzate nei successivi capitoli, con particolare riguardo ai metodi crittografici più utilizzati in letteratura.

1.1 Keyed-Hash Message Authentication Code (HMAC)

Nell'ambito della sicurezza informatica è molto importante poter fornire un modo per verificare l'integrità di un messaggio trasmesso attraverso un canale insicuro. Il message authentication code (MAC) è utilizzato unitamente a una chiave segreta per fornire un test di integrità.

Il Keyed-Hash message authentication code (HMAC) è una tipologia di MAC calcolato utilizzando una funzione di hash in combinazione con una chiave segreta. Tramite la combinazione del messaggio e della chiave è possibile garantire sia l'integrità che l'autenticità di un messaggio. Peculiare dell'HMAC è il non essere legato a nessuna funzione di hash particolare, questo per rendere possibile una sostituzione della funzione nel caso fosse scoperta debole.

Nonostante ciò le funzioni più utilizzate sono MD5 e SHA-1 [35] e l'algoritmo risultante viene chiamato rispettivamente HMAC-MD5 o HMAC-SHA-1.

Una funzione di hash iterativa divide il messaggi in blocchi di lunghezza fissa e li itera con una funzione di compressione. Per esempio, MD5 e SHA-1 operano su blocchi di lunghezza di 512 bit. L'output della funzione HMAC ha la stessa dimensione della funzione di hash sottostante (128 o 160 bit nel caso rispettivamente di MD5 o SHA-1), anche se può essere troncato dove risultasse necessario (questo comporta una riduzione della sicurezza del MAC, che ha come limite superiore la complessità di un attacco del compleanno).

1.1.1 Definizione

La definizione di HMAC [33] richiede una funzione di hash, indicata con $h(\cdot)$ e una chiave segreta K. Si assume che $h(\cdot)$ lavori iterando una funzione di base di compressione su blocchi di dati e si indica con B la dimensione in bytes del blocco ($B = 64$ per MD5 e SHA-1) e con L la lunghezza in bytes dell'output della funzione di hash ($L = 16$ per MD5, $L = 20$ per SHA-1). La lunghezza della chiave può arrivare fino alla lunghezza del blocco della funzione di hash, B. Eventuali applicazioni che usassero una chiave più lunga di B, provvederebbero a comprimere la chiave con la funzione $h(\cdot)$, per poi utilizzare gli L byte di risultato come la chiave del HMAC. In ogni caso la lunghezza minima raccomandata per K è di L byte (come la lunghezza dell'output dell'hash).

Si definiscono due stringhe fissate e diverse chiamate *ipad* e *opad* come segue:

$$ipad = \text{il byte } 0x36 \quad \text{ripetuto B volte}$$

$$opad = \text{il byte } 0x5C \quad \text{ripetuto B volte}$$

Per calcolare l'HMAC sul messaggio M si calcola[1]

$$HMAC_K(M) = h\Big((K \oplus opad) \parallel h\Big((K \oplus ipad) \parallel M\Big)\Big) \tag{1.1}$$

In particolare:

1. K viene adattata alla lunghezza di B byte aggiungendo degli zeri (cioè, se K è 20 bytes e $B = 64$, saranno aggiunti 44 bytes di $0x00$ a K)
2. XOR tra la stringa calcolata al passo (1) e *ipad*
3. si concatena alla stringa di B bytes ottenuta al passo (2), il blocco di dati M
4. si applica $h(\cdot)$ alla stringa generata al passo (3)
5. XOR tra la stringa calcolata al passo (1) e *opad*
6. si concatena l'output dell'hash ottenuto al passo (4) alla stringa di B byte ottenuta al passo (5)
7. si applica la funzione di hash $h(\cdot)$ allo stream generato allo step (6)

In fig. 1.1 è rappresentata lo schema del processo.

[1] viene indicata con $\oplus$ l'operazione di XOR bit a bit, mentre con $\parallel$ l'operazione di concatenazione

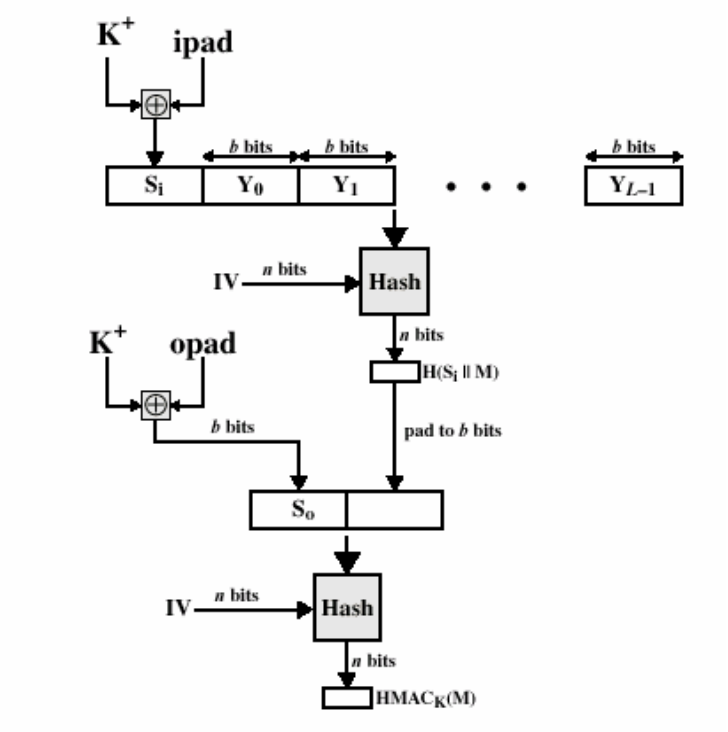

Figura 1.1: Rappresentazione del processo di generazione dell'HMAC (da [43]).

1.1.2 Sicurezza

La forza dal punto di vista della crittanalisi del HMAC è direttamente proporzionale alla funzione di hash sottostante, alla dimensione della chiave e alla lunghezza dell'output dell'hash in bit. I message authentication code (MAC) in generale sono vulnerabili a diversi attacchi, tra i quali l'attacco del compleanno e il collision attack (vedi [43]).

1.2 Hash chaining

Una hash chain è un metodo per generare molte chiavi di tipo one-time a partire da una singola chiave o password attraverso l'applicazione successiva di una funzione crittografica di hash $h(s)$ a una stringa. Una funzione di hash $h(s)$ è una funzione univoca a senso unico. Deve essere di facile calcolare $h(s)$ a partire da s, mentre al contrario, computazionalmente infattibile ottenere s partendo dal valore $h(s)$. Quest'ultima proprietà è la caratteristica a senso

unico della funzione. Inoltre è caratterizzata da due proprietà riguardanti la resistenza alle collisioni. Dato x e $y = h(x)$ è computazionalmente infattibile ottenere una valore x' con $x' \neq x$ tale che $h(x') = h(x)$ (resistenza debole alle collisioni). Infine è computazionalmente infattibile trovare due valori x' e x tali che $h(x') = h(x)$ (resistenza forte alle collisioni).

Si definisce una catena di hash di lunghezza m, l'applicazione di una funzione di hash $h(\cdot)$ m volte a una stringa s.

$$h^m(s) = \underbrace{h\,(h\,\ldots\,(h(s))}_{m}$$

L'utilizzo di una tecnica di one-time password basata sulla tecnica di hash chaining è stata proposta per la prima volta in [42]. Di seguito è dato un esempio dell'applicazione della tecnica di hash chaining [7]. Sia $h(s)$ una funzione one-way e si calcoli $h^m(s)$.

In seguito si generi una firma digitale di $h^m(s)$ e la si spedisca all'authenticator. Quando il richiedente accede al sistema, fornisce al login la i-esima password che equivale a $h^{(m-i)}(s)$ per qualche messaggio fissato s. L'authenticator verificherà l'autenticità della password calcolando $h(h^{(m-i)}(s))$ e memorizzando di seguito l'ultima password inviata dal richiedente. Solo il richiedente conosce il seme s, così che può provare la sua identità all'authenticator per m volte, generando una one-time password in ciascuna autenticazione e fornendo $h^m(s), h^{(m-1)}(s), \ldots, h(s)$.

Grazie alla caratteristica di irreversibilità di una funzione di hash crittograficamente sicura, è impossibile per un malintenzionato in ascolto invertire la funzione di hash e ottenere un gradino più elevato della catena di hash. L'utente può autenticarsi per m volte prima di esaurire la catena, ogni volta il valore di hash è differente e pertanto non può essere duplicato da un attaccante.

Inoltre ciascun valore può essere utilizzato come prova di non-ripudiabilità, quindi l'hash chaining sarà usato per fornire autenticazione, generazione di one-time password e come strumento per fornire la non-ripudiabilità.

1.3 Crittografia simmetrica

Uno schema di crittografia a chiave simmetrica è caratterizzato dalla proprietà che viene utilizzata la stessa chiave sia per l'operazione di cifratura che quella di decifratura.

Le due parti si scambiano preliminarmente la chiave, quindi per criptare e decriptare il messaggio si servono della chiave condivisa e di un algoritmo. La sicurezza si basa sulla chiave che deve essere tenuta segreta.

In uno schema a crittografia simmetrica, quando il mittente (Alice) vuole spedire al destinatario (Bob) un messaggio M, il messaggio è cifrato con la chiave condivisa K, che è conosciuta sia da Alice che da Bob. Una volta ricevuto il testo cifrato, Bob può risalire al messaggio originale M applicando l'algoritmo di decifratura che non è altro che l'inverso di quello di criptazione, utilizzando la chiave K. Il processo può essere schematizzato come segue.

Cifratura:

1. Alice calcola
$$y = E_K(M)$$
2. Alice spedisce y a Bob

Decifratura: Dopo aver ricevuto y, Bob estrae il messaggio M calcolando
$$M = D_K(y) = E_K^{-1}(y)$$

1.4 Crittografia asimmetrica

Nella tradizionale crittografia simmetrica viene utilizzata un'unica chiave sia per codificare, sia per decodificare i messaggi. Le informazioni (la chiave e l'algoritmo) necessarie per chi deve inviare il messaggio sono quindi identiche a quelle necessarie a chi deve riceverlo. Per concordare una chiave con il proprio interlocutore c'è bisogno di mettersi preventivamente in contatto con lui con il rischio che la chiave venga intercettata durante il tragitto, compromettendo quindi l'intero sistema comunicativo.

La crittografia a chiave pubblica permette invece a due (o più) persone di comunicare in tutta riservatezza senza usare la stessa chiave e anche se non si sono mai incontrate precedentemente.

Ad ogni attore coinvolto è associata una coppia di chiavi:

- la chiave privata, personale e segreta, viene utilizzata per decodificare un documento criptato;
- la chiave pubblica, che deve essere distribuita, serve a criptare un documento destinato alla persona che possiede la relativa chiave privata.

Per utilizzare questo tipo di crittografia è necessario creare una coppia di chiavi, una chiave pubblica (da diffondere) ed una chiave privata (da tenere segreta). La proprietà fondamentale della coppia di chiavi pubblica/privata è che un messaggio cifrato usando la chiave pubblica può essere decriptato

usando soltanto la chiave privata corrispondente. In pratica, la chiave pubblica serve unicamente per codificare il messaggio, mentre quella privata serve unicamente per decodificarlo.

La coppia di chiavi pubblica/privata viene generata attraverso un algoritmo (ad esempio RSA o DSA) a partire da dei numeri casuali. Gli algoritmi asimmetrici sono studiati in modo tale che la conoscenza della chiave pubblica e dell'algoritmo stesso non siano sufficienti per risalire alla chiave privata. Tale meccanismo è reso possibile grazie all'uso di funzioni unidirezionali. In realtà, in molti casi, l'impossibilità di risalire alla chiave privata non è dimostrata matematicamente, ma risulta dallo stato attuale delle conoscenze in matematica e della potenza di calcolo disponibile.

A questo punto i ogni utilizzatore si crea la propria coppia di chiavi. La chiave privata viene tenuta segreta e non viene mai rivelata a nessuno (nemmeno alle persone con le quali si comunica); viceversa, la chiave pubblica viene diffusa.

Un altro possibile utilizzo dell'algoritmo di crittografia asimmetrica riguarda l'idea di firma digitale (vedi sez. 1.5), quindi di autenticazione: in pratica un utente cifra un messaggio con la propria chiave privata; gli altri, una volta ricevuto tale messaggio, riescono a decifrarlo solo con il certificato pubblico relativo a quella particolare chiave privata (del quale devono essere preventivamente a conoscenza, o il certificato viene spedito insieme al messaggio), per cui possono risalire con certezza alla sua identità.

1.4.1 RSA

Ron Rivest, Adi Shamir e Len Adleman nel 1978 un sistema di criptaggio a chiave pubblica basato sul problema complesso della fattorizzazione in numeri primi chaimato RSA. Di seguito andremo a riassumere brevemente i principi di funzionamento. Per prima cosa si scelgono due numeri primi casuali distinti e molto grandi, p e q e il loro prodotto $n = pq$. Poi si sceglie un intero e (chiamato anche esponente pubblico), più piccolo, casuale e che sia relativamente primo con $(p-1)(q-1)$, cioè[2]

$$MCD(e, \phi(n)) = 1, \quad 1 < e < \phi(n)$$

Si calcola d (chiamato anche esponente privato) tale che

$$ed \equiv 1 \qquad \mod \phi(n)$$

[2]Viene indicato con $MCD(x, y)$ il massimo divisore comune tra gli interi x e y, mentre si è soliti indicare con $\phi(\cdot)$ la funzione toziente, cioè il numero di divisori interi di un numero. Ad esempio se $n = pq$, allora $\phi(n) = (p-1)(q-1)$.

o, in modo equivalente,

$$d \equiv e - 1 \qquad \mod \phi(n)$$

quindi e e d sono relativamente primi. La chiave pubblica è (n, e), mentre la chiave privata è (n, d). Quando Alice vuole mandare a Bob un messaggio M, usa la chiave pubblica di Bob per crittare il messaggio. Una volta ricevuto, Bob può decrittarlo usando la sua chiave privata. Il processo può essere schematizzato come segue.

Cifratura:

1. Bob invia la sua chiave pubblica (n_B, e_B) ad Alice e tiene segreta la chiave privata
2. Alice calcola
$$C = M^{e_B} \mod n_B$$
3. Alice spedisce C a Bob

Decifratura: Dopo aver ricevuto C, Bob può estrarre il messaggio M utilizzando il suo esponente privato d_B e calcolando:

$$C^{d_B} \mod n_B = (M^{e_B})^{d_B} \mod n_B = M^1 \mod n_B$$

La procedura descritta sopra funziona poiché

$$C^d \equiv (M^e)^d \equiv M^{ed} \pmod{n}$$

Visto che $ed \equiv 1 \pmod{(p-1)(q-1)}$ e quindi $ed \equiv 1 \pmod{p-1}$ e anche $ed \equiv 1 \pmod{q-1}$ che possono essere scritte anche come $ed = k(p-1)+1$ e $ed = h(q-1)+1$ per valori appositi di k e h. Se M non è un multiplo di p, allora M e p sono relativamente primi perché p è primo e quindi per il piccolo teorema di Fermat:

$$M^{(p-1)} \equiv \pmod{p}$$

utilizzando la prima espressione per ed,

$$M^{ed} = M^{k(p-1)+1} = (M^{p-1})^k \cdot M \equiv 1^k \cdot M = M \pmod{p}$$

Utilizzando la seconda espressione per ed si ottiene in modo analogo

$$M^{ed} \equiv M \pmod{q}$$

Poiché p e q numeri diversi e primi, possiamo applicare il teorema cinese del resto, ottenendo che

$$M^{ed} \equiv M \pmod{pq}$$

e quindi che

$$C^d \equiv M \pmod{n}$$

La firma digitale non è altro che l'inverso: il messaggio viene criptato con la chiave privata, in modo che chiunque possa, utilizzando la chiave pubblica conosciuta da tutti, decifrarlo e, oltre a poterlo leggere in chiaro, essere certo che il messaggio è stato mandato dal possessore della chiave privata corrispondente a quella pubblica utilizzata per leggerlo.

1.5 Firma digitale

La firma digitale è un tipo di criptografia asimmetrica utilizzato per simulare le proprietà di sicurezza di una firma autografa su carta, cioè fornisce autenticità dell'origine, integrità dei dati e non da parte del firmatario. Serve per garantire che l'individuo che spedisce il messaggio sia realmente chi sostiene di essere e inoltre garantisce che eventuali cambiamenti al messaggio originario non possano passare inosservati. La firma digitale è caratterizzata da un codice digitale che può essere allegato a un messaggio trasmesso elettronicamente per identificare in modo univoco il mittente. Al pari di una firma tradizionale lo scopo è garantire che l'individuo che spedisce il messaggio sia esattamente chi pretende di essere. La firma digitale è di grande importanza nel commercio elettronico e un componente chiave di molti sistemi di autenticazione.

Uno schema di firma digitale consiste tipicamente di tre passi:

- Un algoritmo G di generazione della chiave che produce una coppia (SK,PK) per il firmatario. La chiave pubblica PK serve per la verifica della firma, mentre la chiave privata SK serve per generare la firma e va tenuta segreta
- Un algoritmo di firma S che dati in input un messaggio m e la chiave privata SK, generi la firma digitale σ
- Un algoritmo di verifica della firma che dati in input il messaggio m, la firma digitale associata a quel messaggio σ e la chiave pubblica PK decida se la firma digitale è valida oppure no.

La firma digitale fornisce autenticazione del mittente, integrità dei dati e non-ripudiabilità del mittente. Inoltre la firma assicura che qualsiasi modifica dei

dati che sono stati firmati non passi inosservata. Il mittente usa la sua propria chiave privata per generare la firma σ.

Un semplice esempio di firma digitale basato su RSA può essere schematizzato come segue[3]:

1. Alice calcola
$$\sigma = m^{d_A} \mod n$$
2. Alice spedisce (m, σ) a Bob
3. Dopo aver ricevuto (m, σ), Bob usa la chiave pubblica di Alice per decrittare la firma
$$m = \sigma^{e_A} \mod n$$
Quindi Bob confronta il messaggio decrittato con quello ricevuto m. Se coincidono, Bob può fidarsi della firma.

[3] (e_A, d_A) sono la coppia di esponenti pubblici e privati di Alice, mentre (e_B, d_B) sono quelli appartenti a Bob

Capitolo 2

Architettura di rete e protocolli standard

Nel seguente capitolo verrà illustrata l'architettura della 3G core network e l'architettura di interlavoro tra le reti 3G e WLAN. Verranno analizzati poi i protocolli standard utilizzati per l'autenticazione e nell'interlavoro delle due reti.

2.1 Architettura della rete 3G

L'architettura di rete dell'UMTS è mostrata in fig. 2.1. Ci sono due aree che rappresentano rispettivamente l'UMTS UTRAN (oltre alla rete di accesso del GSM) e la core network. Nella figura gli elementi di rete sono interconnessi tramite diverse interfacce (reference points). Ciascuna interfaccia utilizza diversi stack protocollari come IP, Signaling System 7 (SS7), Asynchronous Transfer Mode (ATM), GPRS Tunneling Protocol (GTP) e Mobile Application Part (MAP).

2.1.1 UMTS

L'UMTS evolve dal Global System for Mobile Communication (GSM), i metodi crittografici usati nell'UMTS appartengono alla crittografia convenzionale (cioè simmetrica).

La rete UMTS utilizza la stessa architettura già impiegata da tutti i sistemi di seconda generazione e da alcuni di prima generazione. Dal punto di vista funzionale gli elementi di rete sono raggruppabili nell'UTRAN, che gestisce tutte le funzionalità radio, nel terminale mobile utente (UE—User Equipment) e nella Core Network (CN) responsabile della commutazione

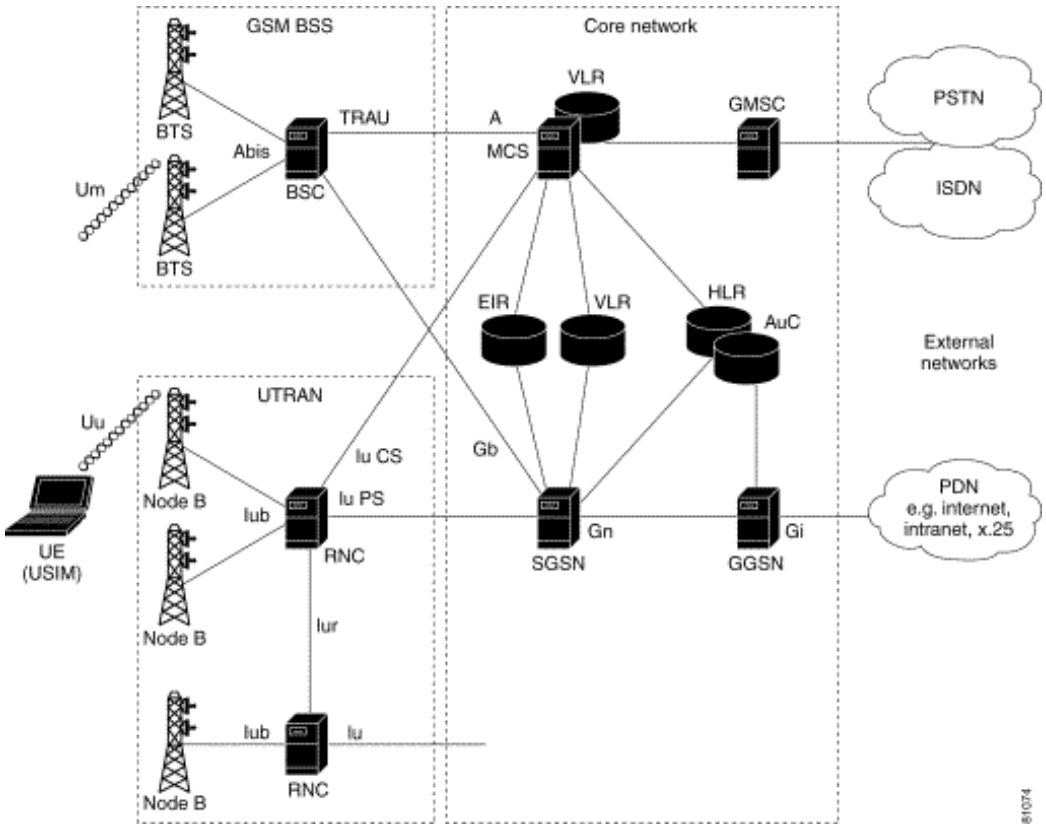

Figura 2.1: Architettura delle rete di accesso e della core network della rete UMTS

e dell'instradamento delle chiamate e delle connessioni con le reti esterne. Come mostra la fig. 2.2 e la fig. 2.1, sia le entità del Core Network che quelle dell'UTRAN sono collegate tra di esse via cavo. Il Core Network e l'UTRAN comunicano, via cavo, tramite l'interfaccia *Iu*. L'UTRAN e l'UE sono collegati, comunicano mediante l'interfaccia *Uu*. RNC, Nodi B e Celle sono le entità che costituiscono l'UTRAN.

L'UE è il terminale usato dall'utente per accedere ai servizi UMTS, è costituito da un equipaggiamento mobile (Mobile Equipment, ME) che è il terminale utilizzato per le comunicazioni radio sull'interfaccia *Uu* e da una o più USIM. La USIM (User Services Identity Module) è un'applicazione che contiene funzioni e dati necessari ad identificare ed autenticare l'utente. In particolare, contiene l'IMSI (International Mobile Subscriber Identity) che serve ad identificare in maniera univoca l'utente, sebbene l'utente può non conoscerne il valore. L'USIM è implementata insieme ad altre applicazioni

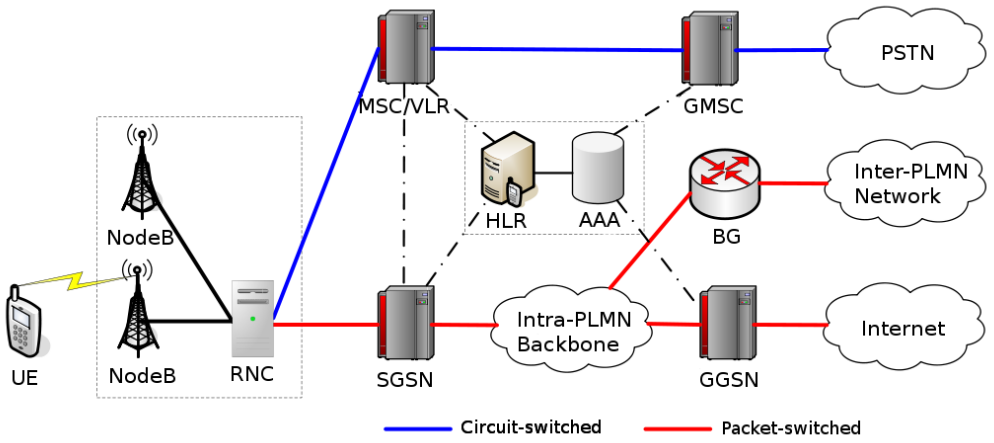

Figura 2.2: Architettura della rete UMTS. Le linee tratteggiate indicano collegamenti via cavo (da [41]).

in un circuito integrato posto su una carta removibile detta UICC (UMTS Integrated Circuit Card).

Core Network (CN)

È l'infrastruttura della rete nella quale la trasmissione avviene solo e soltanto via cavo, è logicamente suddivisa nel dominio CS (Circuit Switched) e nel dominio PS (Packet Switched). Questi due domini differiscono per il modo in cui gestiscono il traffico utente (vedi fig. 2.2).

- Dominio CS: è costituito dall'insieme di tutte le entità della core network che offrono, per il traffico utente, una connessione di tipo CS. Una connessione di tipo CS è una connessione in cui le risorse richieste vengono concesse nel momento in cui la connessione viene stabilita e vengono rilasciate nel momento in cui la connessione viene rilasciata.

- Dominio PS: è costituito dall'insieme di tutte le entità della core network che offrono per il traffico utente una connessione di tipo PS. Una connessione di tipo PS trasporta l'informazione dell'utente usando pacchetti.

Gli altri elementi che compongono la core network sono elencati di seguito:

- HLR (Home Location Register): base dati installata presso la rete home che memorizza i profili di servizio degli utenti. Il profilo d'utente è creato nel momento in cui il nuovo cliente sottoscrive il servizio e rimane memorizzato finché la sottoscrizione è attiva. Per supportare l'instradamento verso il mobile dei servizi da esso terminati (chiamate entranti o messaggi) l'HLR memorizza anche la posizione dell'UE a livello di MSC/VLR e/o SGSN dal quale il terminale è servito. In particolare, l'HLR contiene gli identificatori IMSI mediate i quali vengono identificati gli utenti.

- MSC/VLR (Mobile Services Switching Centre / Visitor Location Register): sono, rispettivamente, la centrale di commutazione (MSC) e la base dati (VLR) che supportano l'UE, nella sua attuale posizione, per i servizi a commutazione di circuito. La funzionalità principale dell'MSC è di commutare le chiamate mentre il VLR memorizza i profili d'utente dei sottoscrittori ospiti (ovvero sotto la copertura radio servita dal MSC/VLR) e informazioni più precise quali la posizione dell'utente all'interno della copertura radio. La parte di rete alla quale si accede tramite MSC/VLR è definita spesso come "dominio a Commutazione di Circuito" o CS. È un database nel quale viene registrata e tenuta aggiornata la posizione sul territorio dell'UE. Il VLR è (a parte l'HLR), il registro delle locazioni per i servizi che utilizzano la trasmissione CS. L'MSC recupera dal registro VLR l'informazione che gli occorre, ad esempio, per gestire chiamate da e verso un UE correntemente localizzato nella zona di sua competenza. L'operatore PLMN può dislocare sul territorio che intende coprire, diversi registri VLR. Ogni registro VLR controlla, in associazione con un MSC, un'area ben definita, detta area MSC/VLR. Diversi MSC possono essere associati ad uno stesso registro VLR. L'area controllata da un MSC/VLR è suddivisa in tante Location Areas (LAs) ognuna delle quali è costituita da una o più celle. Ogni LA è identificata da un numero denominato Local Area Identity (LAI). Una LA è la zona dentro la quale un UE può muoversi liberamente senza che la sua posizione, memorizzata nel VLR, debba essere aggiornata. Infatti, quando un UE passa da una LA ad un'altra, la sua posizione viene aggiornata nel VLR; se poi l'UE passa in un'area che è sotto il controllo di un altro VLR, allora la sua posizione viene aggiornata anche nell'HLR.

- Authentication Centre (AuC): è il centro di autenticazione dei dati incaricato di generare i parametri necessari per l'autenticazione degli utenti. Tali parametri vengono memorizzati nel database HLR al qua-

le l'AuC è associato. Quando un utente richiede un servizio, l'AuC verifica, consultando l'HLR, se si tratta di un utente regolarmente registrato.

Le principali entità del Core Network che appartengono al dominio CS sono le seguenti:

- GMSC (Gateway MSC): è il nodo di commutazione che interfaccia la PLMN (Public Land Mobile Network) UMTS con le altre reti esterne a commutazione di circuito. Tutte le connessioni, entranti e uscenti, di tipo CS passano attraverso il GMSC.

Le principali entità del Core Network che appartengono al dominio PS sono SGSN e GGSN mediante le quali viene realizzata la trasmissione a pacchetto.

- SGSN (serving GPRS Support Node): funzionalmente simile all'MSC/-VLR ma utilizzato per servizi a commutazione di pacchetto (Packet Switched—PS). Costituisce, insieme al GGSN, l'interfaccia tra il sistema radio e la rete fissa per i servizi che utilizzano la trasmissione a commutazione di pacchetto. Per tali tipi di servizi l'SGSN svolge funzioni analoghe a quelle che l'MSC/VLR svolge per i servizi a commutazione di circuito come ad esempio la gestione della mobilità e l'instradamento delle chiamate. L'SGSN contiene un database (analogo al database VLR) nel quale memorizza tutte le informazioni necessarie per la gestione delle trasmissioni dei pacchetti di dati. In particolare, nel database dell'SGSN (come nel database VLR) vengono memorizzati i codici IMSI mediante i quali vengono identificati univocamente gli utenti. L'SGSN e l'MSC/VLR sono collegati e quindi dialogano mediante l'interfaccia *Gs*. Ogni SGSN controlla un'area che consiste di una o più Routing Area (RA), definita come l'area dentro la quale un UE può muoversi liberamente senza che la sua posizione debba essere aggiornata nell'SGSN. Una RA è sempre contenuta in una Location Area (LA) e come quest'ultima è costituita da una o più celle. La Routing Area (RA) per l'SGSN è perciò analoga alla Location Area (LA) per l'MSC/VLR mentre l'area SGSN è analoga all'area MSC/VLR.

- GGSN (Gateway GPRS Support Node): funzionalmente simile al GMSC ma utilizzato per i servizi PS. Rappresenta il punto d'ingresso alla rete che supporta la trasmissione a pacchetto. Nel suo database memorizza i dati dell'utente che riceve dai registri HLR e SGSN e che sono necessari per la gestione della trasmissione a pacchetto.

2.2 Architettura di interlavoro 3G-WLAN

In fig. 2.3 è illustrata l'evoluzione degli standard emessi dal 3^{rd} *generation partnership project* (3GPP) per quanto riguarda l'interlavoro tra le reti 3G e WLAN, dalla Release 5 del 2002 quando con l'introduzione dell'IP Multimedia Subsystem (IMS) è stato affrontato per la prima volta il problema dell'interlavoro tra reti eterogenee, alla Release 7 che è l'ultima attualmente disponibile.

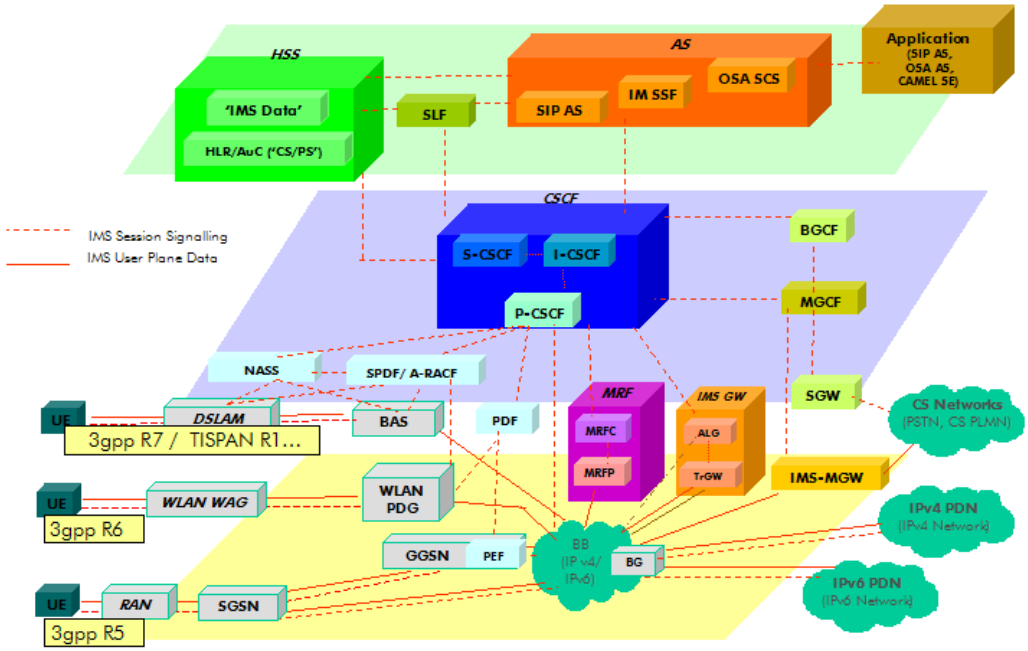

Figura 2.3: Illustrazione dell'architettura 3GPP/IMS con particolare riferimento alle Release 5, 6 e 7.

2.2.1 Scenari di integrazione

Le WLAN possono essere di proprietà di un operatore 3G, un operatore wireless commerciale, un'autorità di un hotspot pubblico (come gli aeroporti) o di un impresa commerciale per uso interno e i meccanismi di interlavoro

sono direttamente correlati con la proprietà delle WLAN. Il reale livello di penetrazione tra le reti 3G e le WLAN e i conseguenti servizi offerti conducono a diversi requisiti per i meccanismi di interworking.

Gli operatori cellulari hanno riconosciuto l'opportunità di offrire servizi dati ad alta velocità ai propri clienti attraverso la tecnologia Wireless LAN. Il risultato dello sforzo del comitato 3GPP per affrontare le richieste tecniche e definire le specifiche per l'integrazione è stata la definizione di sei scenari di integrazione. Gli scenari, descritti in [27], forniscono un approccio per l'implementazione di un interlavoro flessibile, scalabile e generale, passando per gradi da una semplice interconnessione 3G-WLAN per arrivare a un'interazione completa e trasparente.

Scenario 1 - Common Billing and Customer Care

Questo scenario prevede solo una tariffazione comune ed un unico servizio clienti. Il cliente riceve un'unica fattura dall'operatore per l'uso sia dei servizi 3G che WLAN. L'unica relazione che esiste, è tra l'home 3G operator e il cliente, quindi non c'è necessità di stabilire a priori delle relazioni con ciascuna WLAN, non esiste un reale interlavoro tra le WLAN e la rete 3G. Non sono necessari alcuni requisiti o modifiche nelle specifiche di sistema 3GPP.

Scenario 2 - 3GPP System-Based Access Control and Charging

In questo scenario il metodo di authentication, authorization e accounting (AAA) è fornito dal sistema 3G, quindi viene sfruttato il sistema 3GPP di controllo degli accessi e di tariffazione, richiesti dall'AAA quando un utente 3G richiede l'accesso a una rete WLAN. Per esempio, un utente 3G può utilizzare la USIM per ottenere l'autenticazione facendo roaming verso una WLAN. Viene quindi abilitata la connettività IP attraverso le WLAN per gli utenti 3G che possono accedere ai servizi 3G o WLAN utilizzando sessioni separate. Inoltre questo scenario fornisce un modo più sicuro per accedere alla WLAN rispetto al classico utilizzo di username/password. Da notare che non è richiesto nessun servizio offerto nella WLAN.

Scenario 3 - Access to 3GPP System PS-Based Services

A fianco delle capacità menzionate negli scenari sopra esposti, una nuova idea permette a questo scenario di beneficiare della WLAN. Dal momento che i collegamenti wireless forniscono solitamente velocità di connessione più elevate e minori costi di trasmissione che il dominio 3G PS, accedere ai servizi 3G basati sul PS attraverso la WLAN potrebbe essere una soluzione economica ed efficiente per gli utenti. Per questo lo scenario permette agli utenti 3G

di accedere ai servizi del dominio a commutazione di pacchetto, come IMS o MMS dalla WLAN. Per esempio, un utente può spedire o ricevere servizi dati a pacchetto quando effettua roaming verso la WLAN o è possibile accedere all'IMS per i servizi multimediali basati su IP. Questo scenario è la partenza per un reale interlavoro tra la 3G PLMN e le reti WLAN, pertanto la 3G core network richiede dei componenti aggiuntivi per raggiungere le capacità di questo scenario.

Scenario 4 - Service Continuity

Questo scenario fornisce la capacità di continuità di servizio tra la rete 3G e la WLAN per i servizi supportati dallo scenario 3. Un utente che apre una sessione a commutazione di pacchetto nella rete WLAN o 3G dovrebbe essere in grado di mantenerla attiva anche dopo essersi spostato nell'una o nell'altra. In altre parole questo scenario richiede un meccanismo di handoff per la capacità di continuità del servizio. C'è da notare che le sessioni di alcuni servizi potrebbero non sopravvivere al passaggio, perché la rete contigua potrebbe non supportare un servizio equivalente.

Scenario 5 - Seamless Services

L'obiettivo di questo scenario è fornire una continuità di servizio di tipo trasparente all'utente tra reti 3G e WLAN. Le capacità dello scenario sono le stesse dello scenario 4, ma inoltre sono previsti dei vincoli sulla perdita di dati e sui ritardi di handoff che dovrebbero essere minimizzati.

Scenario 6 - Access to 3GPP System CS-Based Services

Il punto chiave di questo scenario è consentire all'utente di accedere ai servizi a commutazione di circuito della rete 3G (come per esempio le chiamate vocali tradizionali), attraverso la rete WLAN. Deve essere supportata la mobilità di tipo trasparente con passaggio da servizi a commutazione di pacchetto e di circuito che avvenga in modo invisibile all'utente.

La tabella 2.1 riassume i servizi e le capacità di ciascun scenario. Procedendo con l'integrazione tra WLAN e 3G dallo scenario 1 verso lo scenario 6, queste due reti diventano più strettamente integrate e compaiono più requisiti e diversi meccanismi. Per esempio cambiando dallo scenario 2 al 3 è necessario aggiungere il PDG (Packet Data Gateway) e il WAG (WLAN Access Gateway) alla 3G core network per il data routing e controllo di accesso,

	Scen.1	Scen.2	Scen.3	Scen.4	Scen.5	Scen.6
Common Billing	✓	✓	✓	✓	✓	✓
Common Customer Care	✓	✓	✓	✓	✓	✓
3GPP-based access control		✓	✓	✓	✓	✓
3GPP-based access charging		✓	✓	✓	✓	✓
Access to 3GPP PS-based services			✓	✓	✓	✓
Service continuity				✓	✓	✓
Seamless services continuity					✓	✓
Access to 3GPP CS-based services						✓

Tabella 2.1: Scenari di interlavoro 3GPP-WLAN

o comunque inserire nella rete degli elementi che si occupino della gestione del traffico dati che proviene dalle reti WLAN. Migrando dallo scenario 3 al 4 è necessario un meccanismo di handoff per fornire le capacita di continuità di servizio.

Lo scenario adottato come primo livello dell'interlavoro 3G-WLAN è lo scenario 3. Servizi IP ad alta velocità possono essere offerti ai clienti con un solo abbonamento e un'unica fatturazione con modifiche limitate o nulle nell'infrastruttura 3G esistente, mentre i gestori della rete WLAN non necessitano di implementare complicate interfacce di rete per l'accesso alla core network 3G. Lo scenario 3 è un approccio iniziale che richiede solo un minimo di investimenti da parte degli operatori cellulari, mentre gli scenari successivi richiedono dell'hardware ibrido che permetta di processare i protocolli di livello fisico sia della rete 3G che WLAN per implementare un roaming trasparente e i servizi a commutazione di circuito sopra le WLAN [23].

2.2.2 Tight coupling e loose coupling

Esistono diverse architetture di integrazione WLAN-3G riportate in letteratura [18], basate sul livello di interdipendenza tra le due reti di accesso. La classificazione più utilizzata e significativa è riportata in [11], dove l'inte-

grazione tra le due reti è classificata in due categorie: *tight coupling* e *loose coupling*.

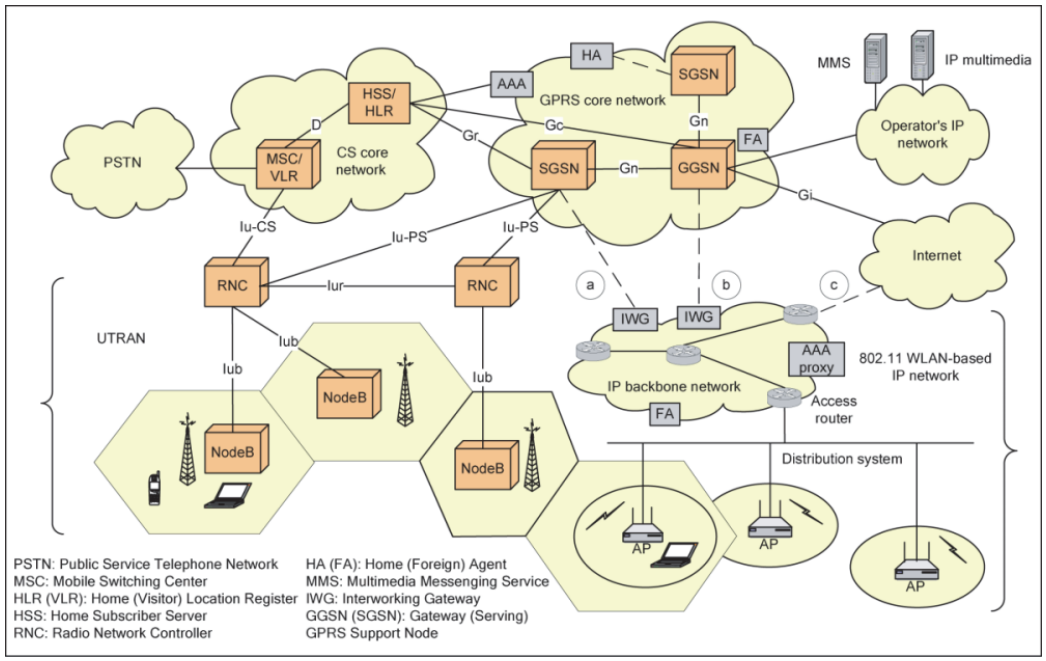

Figura 2.4: Architettura di interlavoro tra 3GPP UMTS e IEEE 802.11 WLAN: (a) WLAN integrata al SGSN; (b) WLAN integrata al GGSN e (c) WLAN integrata a una rete IP esterna (da [17]).

Tight coupling Nell'architettura *tight coupling*, la WLAN è connessa alla 3G core network come una rete di accesso radio e ne emula le funzioni, venendo trattata come una rete di accesso dal punto di vista della core network. Di conseguenza, i protocolli esistenti e le infrastrutture di rete posso essere riutilizzate, per esempio il roaming tra due domini si basa sui protocolli di gestione della mobilità della rete 3G, incrementando così le capacità di mobilità inter-dominio.

La fig. 2.4 illustra un'architettura semplificata per l'interlavoro UMTS con le reti 802.11 WLAN. Le linee indicate con *"a"* e *"b"* sono esempi di accoppiamenti di tipo *tight* con diversi punti di integrazione. Esempi tipici di architetture *tight coupling* comprendono le proposte [11, 26].

Si può vedere come, in questo tipo di architettura, l'interfaccia radio cellulare è semplicemente sostituita dall'interfaccia WLAN che fornisce funzioni equivalenti e come conseguenza i protocolli 3G e le infrastrutture esistenti

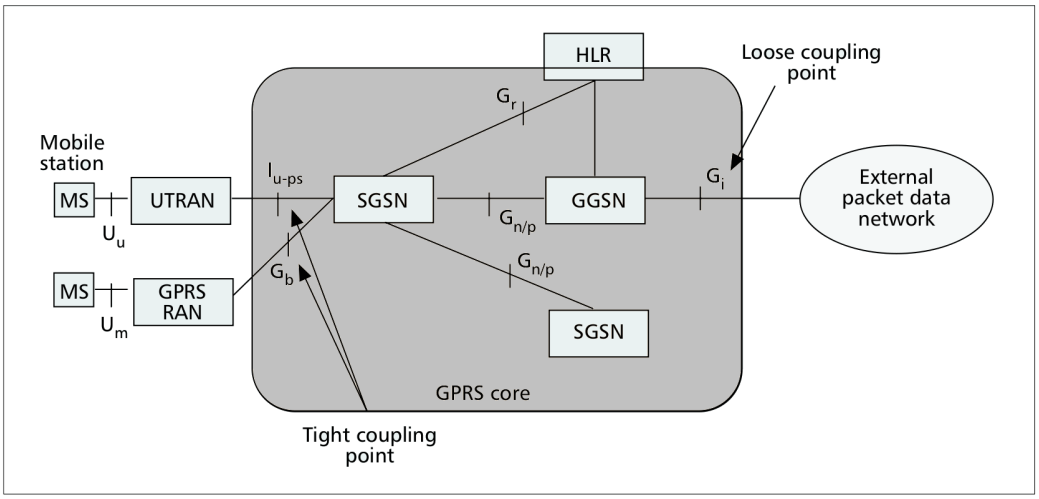

Figura 2.5: Tight e loose coupling (da [11]).

possono essere riutilizzate. Tuttavia i protocolli della rete cellulare, sviluppati per utenti altamente mobili in un ambiente esterno, possono non garantire prestazioni soddisfacenti nell'ambiente WLAN (utenti poco mobili, ambiente tipicamente indoor).

I principali svantaggi dell'approccio *tight coupling* sono:

- la WLAN e la rete 3G devono essere dello stesso operatore o comunque la rete 3G deve possedere un'interfaccia verso la WLAN, che costituisce un problema non indifferente in caso i due domini siano sviluppati e gestiti da operatori diversi
- un volume di traffico dati non indifferente attraversa la core network, rendendo quest'ultima un possibile collo di bottiglia
- le WLAN devono avere uno stack protocollare compatibile a quello della rete 3G

Con il *tight coupling* la WLAN si interfaccia con l'SGSN o tramite un'interfaccia già esistente (esempio *Gb* o *Iu-ps*) o tramite una nuova, specifica per offrire performance ottimali alla WLAN. È necessaria una stretta interconnessione tra le due reti e il principale vantaggio è la migliorata mobilità tra i due domini, che viene gestita interamente come fosse un normale handover tra due celle. Inoltre l'approccio *tight* consente il riutilizzo dei metodi di AAA e protegge gli investimenti fatti dall'operatore riutilizzando le risorse della core network, i database degli utenti e i sistemi di fatturazione. Non

da ultimo supporta tutti i servizi accessori dell'operatore e la possibilità di intercettazioni a norma di legge per gli utenti WLAN.

Loose coupling Al contrario dell'approccio *tight*, nell'approccio *loose* la WLAN è connessa alla core network indirettamente tramite una rete IP esterna, come Internet (mostrata dalla lettera *"c"* nella fig. 2.4). Questo tipo di architettura richiede minimi cambiamenti da parte degli standard WLAN esistenti e permette maggior flessibilità e indipendenza nell'implementare individualmente meccanismi differenti nelle singole reti. D'altra parte la rete 3G necessita di essere migliorata con funzionalità extra come la gestione della mobilità e il supporto all'authorization, authentication e accounting.

Inoltre, visto che i due domini sono separati, i messaggi di segnalazione potrebbero attraversare un percorso relativamente lungo, introducendo in questo modo un'elevata latenza di handoff.

L'approccio *loose* prevede l'interconnessione attraverso l'interfaccia *Gi* (vedi fig. 2.5). Il traffico WLAN generalmente non necessita più di attraversare la 3G core network, ma va direttamente nella rete IP dell'operatore e/o in Internet. L'architettura supporta anche un sistema di tariffazione che deve essere integrato con il supporto di elementi aggiuntivi e deve essere efficacemente supportato da un protocollo di autenticazione coerente. La rete WLAN può appartenere a un terzo operatore con la possibilità di roaming e mobilità attivata tramite una connessione dedicata tra l'operatore e la WLAN o direttamente tramite Internet.

Il loose coupling utilizza degli standard basati su protocolli IETF per l'autenticazione, l'accounting e la mobilità e quindi non è necessario introdurre tecnologia propria del mondo cellulare nella rete wireless.

Senza dubbio l'approccio *tight* è disegnato in primo luogo per le reti wireless possedute e gestite direttamente dagli operatori mobili e non consente di supportare in maniera semplice operatori terzi. Inoltre esistono questioni di costi e capacità associati alla connessione della WLAN con un SGSN. Per esempio la capacità di throughput di un SGSN potrebbe essere sufficiente per supportare migliaia di connessioni da terminali 3G (voce ma anche video e dati), ma potrebbe non essere sufficiente per poche centinaia di connessioni dati ad alta velocità dai terminali WLAN.

Oltre a queste motivazioni, esistono altre ragioni che hanno spinto ad accantonare l'approccio *tight* in favore di quello *loose*. Il *loose coupling* è basato principalmente su protocolli IETF, che sono già implementati negli apparati WLAN e che richiedono pertanto modifiche e richieste minime per poter funzionare. Tuttavia costringe gli operatori cellulari a fornirsi di nuovi apparati, come ad esempio, server AAA specifici per l'interlavoro con le WLAN.

Categoria	*Tight Coupling*	*Loose Coupling*
Autenticazione	Riutilizzo dell'autenticazione UMTS AKA per gli utenti WLAN e della chiave AKA per il criptaggio WLAN	Gateway di accesso che fornisca autenticazione
Accounting	Riutilizzo del accounting 3G	Mediatore o tecniche alternative per la tariffazione
Mobilità	SGSN è la call-anchor e la mobilità è garantita dagli handover intra-SGSN	Aspetto ancora sotto studio (es. Mobile IP)
Trasferimento di contesto	Possibile anche a livello fine, come per esempio parametri di QoS, informazioni su flussi multipli, ecc.	Aspetto ancora sotto studio
Architettura di sistema	Da analizzare l'impatto di reti wireless ad alta velocità sulla 3G core network	WLAN e core network possono essere progettati e sviluppati in modo diverso
Sviluppo di nuovi componenti	Modifiche dei terminali per la gestione della segnalazione 3G e modifiche della rete WLAN per l'interlavoro con le interfacce standard 3G	Inserimento nella 3G core network di elementi ad hoc per l'interconnessione con gli AP che tengano conto anche dei problemi di fatturazione
Standard	Sviluppo di una nuova interfaccia del SGSN per l'interconnessione con le WLAN	Sviluppo e standardizzazione dei protocolli di autenticazione
Target	Limitato alle reti WLAN di proprietà degli operatori cellulari (molto più complicata l'applicazione quando il WISP è differente dall'operatore 3G)	Ampia applicazione a qualsiasi WLAN

Tabella 2.2: Confronto tra l'approccio *tight* e *loose*

Inoltre è evidente la mancanza di una soluzione che implementi in modo efficiente la mobilità e permetta l'handover se non con latenze inaccettabili per applicazioni realtime.

Complessivamente l'approccio di tipo *loose* è la soluzione preferita da entrambe le comunità 3G e WLAN poiché permette lo sviluppo graduale degli hotspot con nessuna o minime modifiche nella rete 3G. In tabella 2.2 viene mostrato un breve confronto tra questi metodi di approccio all'interlavoro tra le reti WLAN e quelle 3G.

In letteratura si trovano altri tipi di approccio al problema, come in [28] dove gli autori introducono un approccio tra reti di tipo peer, nel quale la rete wireless si comporta da rete pari alla rete 3G o in [29], dove viene proposta un'integrazione di tipo ibrido, ma si tratta sostanzialmente di soluzioni accademiche che non hanno avuto riscontri pratici.

2.3 Autenticazione

L'autenticazione serve per fornire la prova dell'identità o la sorgente di un pari in un'associazione. Dopo essere stati autenticati con successo, gli utenti sono autorizzati all'uso delle risorse dell'entità presso cui si sono registrati.

2.3.1 UMTS

L'UMTS è l'evoluzione del sistema GSM. Il metodo crittografico usato nell'UMTS appartiene alla crittografia convenzionale (cioè di tipo simmetrico). L'UMTS utilizza cinque algoritmi (f_1, f_2, f_3, f_4 e f_5) per l'autenticazione. Questi algoritmi sono flessibili perché sono negoziabili in anticipo tra server e client. Nella maggior parte dei casi sono specifici per ciascun operatore. La procedura di autenticazione è basata su una una chiave segreta, condivisa in anticipo e a lungo termine K di 128 bit che è memorizzata nella USIM card del cliente e nell'authentication center (AuC) dell'home environment (HE). Di solito la procedura è inizializzata dal SGSN/VLR quando la rete ha necessità di verificare l'identità dell'utilizzatore.

Il SGSN/VLR non possiede i dati di autenticazione, e deve richiedere almeno un *authentication vector* (AV) dall'authentication center nell'home environment. L'AuC genera un numero pseudo-casuale, RAND, per calcolare gli AV, che sono composti dai seguenti elementi:

- AUTN, authentication token, 128 bit
- CK, cipher key, 128 bit
- IK, integrity key, 128 bit
- RAND, numero pseudo-random, 128 bit
- XRES, expected response, 128 bit

Quando il SGSN/VLR riceve il AV, i valori RAND e AUTH sono inoltrati all'utente in attesa di autenticazione per essere processate. Il terminale dell'utente deve verificare alcuni valori(MAC e SQN) e calcolare RES che poi sarà restituita. Il SGSN/VLR verifica la RES ricevuta e la confronta con la XRES. Se è corretta, la procedura di autenticazione ha successo e le due parti possono derivare la cipher key, CK per la criptazione e l'integrity key, IK per la protezione dell'integrità dei dati. In fig. 2.6 è raffigurato il processo di autenticazione e generazione delle chiavi.

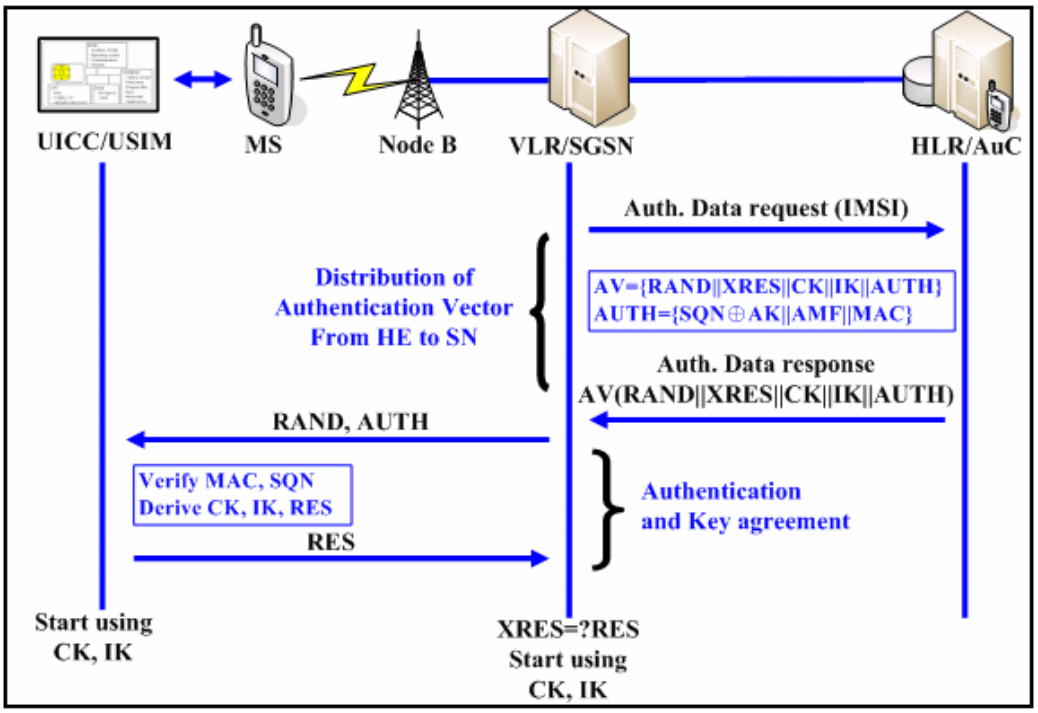

Figura 2.6: UMTS authentication e key agreement (da [1]).

2.3.2 WLAN

Per quanto riguarda la sicurezza delle WLAN, lo standard IEEE 802.11-1999, specifica la Wired Equivaled Privacy (WEP) per la sicurezza a livello di link layer. Tuttavia, dalla pubblicazione dello standard, sono state riscontrate numerose debolezze nel protocollo che lo rendono, di fatto, inutile al giorno d'oggi. Data la vulnerabilità del WEP, è stato sviluppato un nuovo protocollo di sicurezza IEEE 802.11i che offra un livello di privacy molto più avanzato. La specifica 802.11i include sia il protocollo basato su RC4 Temporal Key Integrity Protocol (TKIP), sia il protocollo basato sull'Advanced Encryption Standard (AES), chiamato Counter Mode CBC-MAC Protocol (CCMP) per il criptaggio e l'integrity protection e 802.1x per l'autenticazione e la distribuzione delle chiavi. Il TKIP è una soluzione ad interim per ovviare i noti problemi del WEP, compatibile con i prodotti 802.11. Sebbene sia molto più sicuro del WEP, non è considerato all'altezza della soluzione che impiega l'AES. Di conseguenza lo standard finale a lungo termine per 802.11i è costituito dalla soluzione basata su AES.

Il gruppo di lavoro che si occupa dell'802.11i ha deciso di usare come fra-

mework di autenticazione il IEEE 802.1x, che è un meccanismo di controllo dell'accesso della rete port-based, che usa l'Extensible Authentication Protocol (EAP) per l'autenticazione mutua end-to-end tra una Mobile Station e un Authentication Server. In altre parole, l'Access Point può filtrare i frames da e per stazioni non autenticate. Prima che l'autenticazione sia completa, è consentito il passaggio solo del traffico EAP, mentre una volta che la stazione è stata autenticata dall'authentication server, l'AP inoltra i pacchetti dati da e per quella stazione. L'intero meccanismo di autenticazione IEEE 802.1x include EAP, EAP over LAN (EAPOL) e il protocollo RADIUS.

IEEE 802.1x

IEEE 802.1x è uno standard IEEE basato sul controllo delle porte di accesso alla rete. Questo standard (che è parte della famiglia IEEE 802) provvede ad autenticare e autorizzare i dispositivi collegati alle porte della rete (switch e access point) stabilendo un collegamento punto a punto e prevenendo collegamenti non autorizzati alla rete locale. Viene utilizzato dalle reti locali wireless per gestire le connessioni agli access point e si basa sul protocollo EAP [36, 37].

L'802.1x è ormai supportato dalla maggioranza dei nuovi access point perché risolve parzialmente le insicurezze del WEP. Normalmente, l'autenticazione è fatta da una terza parte, come un server RADIUS [34]. Questo fornisce la possibilità di garantire una forte autenticazione mutua tra server e client.

Definizioni Nello standard IEEE 802.1x esistono tre ruoli, un supplicant, un authenticator e un authentication server. Tra l'authenticator e l'authentication server viene usato il protocollo RADIUS.

- Supplicant, il client che richiede di essere autenticato (solitamente un device mobile)
- Authenticator, il dispositivo che esegue l'inoltro della richiesta di accesso (access point)
- Authentication Server, il dispositivo che effettua il controllo sulle credenziali di accesso del supplicant ed autorizza l'accesso (server di autenticazione back-end)

Dettagli di funzionamento Lo standard 802.1x non definisce un metodo preciso ma uno schema architetturale nel quale possono essere usate varie

metodologie, per questo una delle sue caratteristiche fondamentali è la versatilità. Fin dalla sua ratifica, 802.1x è divenuto il framework di autenticazione delle wireless LAN, la sua rapida diffusione è stata dovuta, in larga parte, alla possibilità di utilizzo di standard precedentemente accettati, principalmente EAP. Il controllo degli accessi alla rete basato sulle porte fa uso delle caratteristiche di accesso fisico alle infrastrutture LAN basate sugli standard IEEE 802, allo scopo di fornire autenticazione e autorizzazione tramite dispositivi connessi a una porta della LAN che abbia caratteristiche di connessione punto-punto, e prevenzione dell'accesso a tale porta nel caso in cui autenticazione ed autorizzazione falliscano.

I passi previsti tipicamente dal protocollo sono i seguenti.

1. Quando un nuovo nodo wireless richiede l'accesso alle risorse di una LAN, l'access point (AP) ne richiede l'identità. Nessun altro tipo di traffico è consentito oltre a quello EAP, prima che il nodo sia autenticato. Il nodo wireless che richiede l'autenticazione è spesso denominato supplicant ed ha il compito di fornire risposte all'autenticatore che ne verificherà le credenziali. L'autenticatore non deve necessariamente trovarsi all'interno dell'access point; può essere un componente esterno.

2. Dopo l'invio dell'identità, comincia il processo di autenticazione. Il protocollo utilizzato tra il supplicant e l'autenticatore è EAP, o, più correttamente, EAP incapsulato su LAN (EAPOL). L'autenticatore reincapsula i messaggi EAP in formato RADIUS, e li passa al server di autenticazione. Durante l'autenticazione, l'autenticatore semplicemente ritarda i pacchetti tra il supplicant e il server di autenticazione. Quando il processo di autenticazione si conclude, il server di autenticazione invia un messaggio di successo (o di fallimento, se l'autenticazione fallisce). L'autenticatore quindi apre la porta al supplicant. Il protocollo RADIUS soffre di alcune vulnerabilità [40].

3. Dopo un'autenticazione andata a buon fine, viene garantito al supplicant l'accesso alle altre risorse della LAN e/o ad Internet.

L'autenticazione viene definita "port-based" poiché l'autenticatore ha a che fare con porte controllate e non controllate. Entrambi i tipi di porta sono entità logiche (porte virtuali), ma utilizzano la medesima connessione fisica alla LAN. Prima dell'autenticazione, è aperta soltanto la porta non controllata. L'unico traffico consentito è EAPOL. Dopo che il supplicant è stato autenticato, viene aperta la porta controllata e garantito l'accesso alle risorse. 802.1x non fornisce dunque alcuna autenticazione; tutto ciò che fa è dare all'access point la capacità di inoltrare le credenziali del client al server

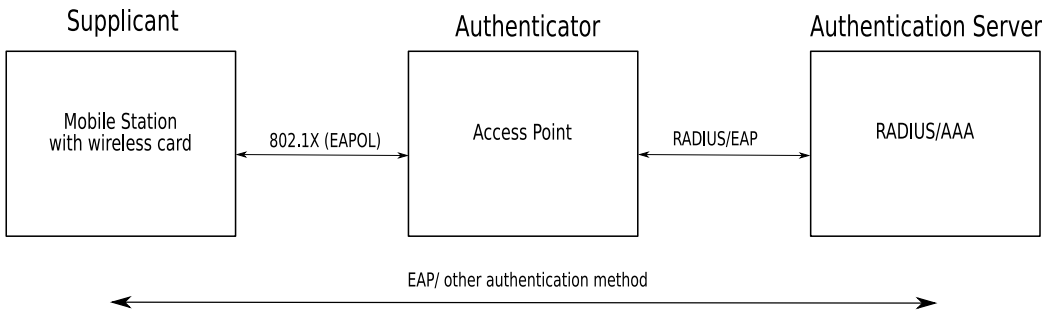

Figura 2.7: 802.1x

RADIUS e la relativa risposta verso il client stesso. Questa funzionalità trova compimento implementando i protocolli RADIUS e EAP.

2.4 Extensible Authentication Protocol

I meccanismi di autenticazione hanno incominciato a fondarsi sull'utilizzo dell'Extensible Authentication Protocol (EAP) come una base per trasferire informazioni di autenticazione tra il client e la rete. EAP fornisce un framework di base del tipo request/response sopra il quale si implementa una specifica autenticazione e/o algoritmo di scambio delle chievi. Quado un algoritmo di sicurezza viene implementato sopra EAP, ci si riferisce come a un *metodo EAP* [25]. I metodi EAP più importanti sono:

- EAP-SIM: basato su meccanismo challenge/response per autenticazione GSM basata su SIM. Migliora l'autenticazione GSM per fornire autenticazione mutua e chiavi più lunghe.
- EAP-AKA: basato su meccanismo challenge/response per autenticazione UMTS basata su USIM
- EAP-TLS: approccio basato su chiave pubblica, in particolare su SSL v3.0 per autenticazione attraverso certificati
- EAP-TTLS: protocollo ibrido che fornisce sia autenticazione tramite password che tramite chiave pubblica
- EAP-MD5: approccio basato su password,autenticazione con MD5-Challenge handshake

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	EAP-SIM	EAP-AKA
Standard Industriale	✓	✓	✓	✓	✗	✗
Tipo di autenticazione basato su certificati o password	pwd	cert	ibrido	ibrido	pwd	pwd
Scambio dinamico delle chiavi	✗	✓	✓	✓	✗	✗
Mutua autenticazione	✗	✓	✓	✓	✓	✓
Uso di certificati (lato Server/Client)	✗	✓ (✓/✓)	✓ (✓/Opz.)	✓ (✓/Opz.)	✗	✗

Tabella 2.3: Confronto tra i vari protocolli EAP (da[15]).

- PEAP (Protected EAP): protocollo proposto da Cisco, Microsoft e RSA Security, simile a EAP-TTLS, sia come approccio che come livello di sicurezza

Il confronto tra i vari protocolli di autenticazione è presentato in tabella 2.3.

Il protocollo EAP ha 4 tipi diversi (*Request, Response, Success* e *Failure*), inoltre lo standard IEEE 802.1x ha definito uno speciale frame chiamato EAP over LAN (EAPOL), per consentire ai messaggi EAP di essere trasmessi attraverso una LAN prima di protocolli di livelli più alti [15]. Usando l'EAPOL un utente non autorizzato può inoltrare i pacchetti di autenticazione all'AP per le successive procedure. L'autenticazione vera e propria avviene tra l'utente e l'AS (Authentication Server) ed è trasparente all'AP. Dopo aver ricevuto il messaggio EAP, l'AP provvederà a incapsularlo in un protocollo AAA, come per esempio RADIUS o Diameter, e inoltrarlo all'AS. Quando l'autenticazione sarà completata con successo, l'AS manderà un messaggio RADIUS/Diameter-*Access Accept* all'AP che a questo punto sarà a conoscenza del fatto che l'utente sarà stato autenticato dall'AS e quindi invierà un messaggio EAP-*Success* al terminale utente.

2.4.1 EAP-MD5

MD5 è l'equivalente del CHAP in cui un algoritmo hash a senso unico è utilizzato in combinazione con un segreto condiviso e una richiesta di identificazione per verificare che il richiedente è a conoscenza del segreto condiviso. MD5 è considerato un metodo di autenticazione di livello base e generalmente non appropriato in caso sia necessario un alto livello di sicurezza per la protezione di beni di grande valore. Questo accade per diverse ragioni. Come ogni metodo che utilizza richieste random e un algoritmo hash, è vulnerabile agli

attacchi basati su dizionario. Se un attaccante riesce ad ottenere la richiesta e la risposta hash, è in seguito possibile eseguire un programma off-line con lo stesso algoritmo del richiedente, inserendo parole contenute in un dizionario fino a quando la risposta hash coincide con quella del richiedente. A questo punto l'attaccante conoscerà la password del richiedente e potrà sottrarne l'identità per ottenere l'accesso alla rete. Questo procedimento risulta ancora più semplice nelle wireless LAN. In aggiunta, EAP-MD5 offre soltanto l'autenticazione lato client (ovvero, il client viene autenticato alla rete). Altri metodi EAP offrono mutua autenticazione per cui il client è autenticato alla rete e la rete è autenticata al client.

2.4.2 EAP-TLS

Il Transport Layer Security (TLS) offre un processo di autenticazione particolarmente sicuro, che sostituisce le semplici password con certificati lato client e lato server tramite l'utilizzo della infrastruttura a chiave pubblica (Public Key Infrastructure o PKI). Un certificato è un record di informazioni relative ad un'entità verificato tramite un algoritmo matematico asimmetrico. È supportata la mutua autenticazione, e le chiavi di sessione dinamiche. TLS è una buona scelta quando si richiede un elevato livello di autenticazione e sicurezza ed è presente una infrastruttura a chiave pubblica. Comunque, l'utilizzo di una PKI, in cui ciascun client ha il suo proprio certificato, è oneroso se comparato ai sistemi basati su password. In fig. 2.8 è rappresentato lo scambio di messaggi nel protocollo.

A differenza di EAP-AKA, EAP-TLS è basato sulla crittografia a chiave pubblica (PKC), quindi non richiede un server centrale (come l'HLR) che condivida una chiave segreta con la MS ed è scalabile. Tuttavia EAP-TLS richiede più potenza di calcolo a causa dell'uso della PKC. Fornisce autenticazione mutua in quanto sia il client che l'authentication server si autenticano a vicenda (anche se l'autenticazione del client è opzionale nello standard). Uno dei principali svantaggi dell'EAP-TLS è che il client necessita di un certificato a chiave pubblica per essere autenticato dall'AP. Più nello specifico, l'introduzione di EAP-TLS richiede che vengano soddisfatti i seguenti requisiti:

- Esiste una qualche Certificate Authority (CA) che emette e revoca i certificati. Può essere privata oppure pubblica nella forma di qualche terza parte fidata.
- La USIM 3G è una crypto-card con buone capacità di generare numeri casuali o pseudocasuali e con un chip per ottimizzare l'esecuzione delle funzioni crittografiche.

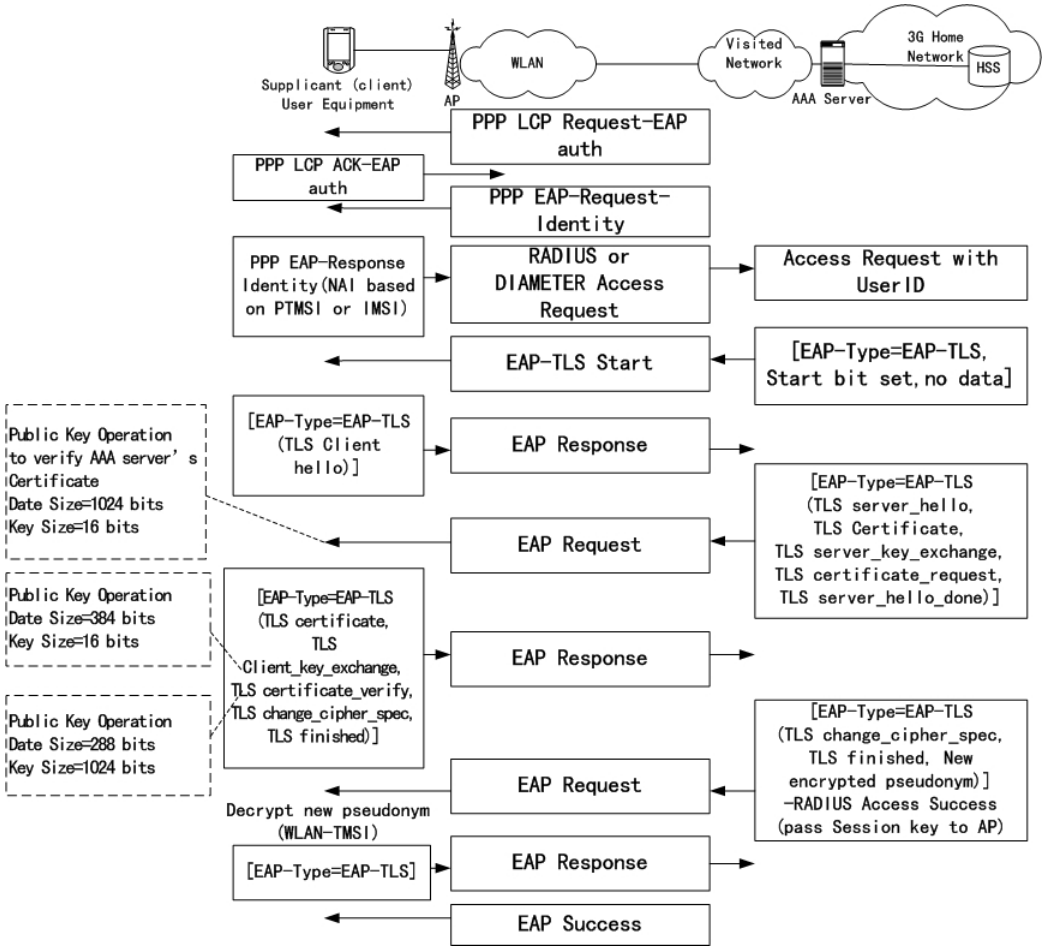

Figura 2.8: Protocollo EAP-TLS

- Ciascun cliente possiede una coppia di chiavi (pubblica + privata) e la sua chiave privata è memorizzata nella USIM. Le chiavi sono generate dall'operatore mobile o dalla CA e associate all'utente al momento della registrazione.
- La USIM è pre-caricata con tutte le chiavi pubbliche delle CA o delle entità terze che sono associate con il particolare operatore.
- Ciascun server AAA che prende parte alla procedura possiede una coppia di chiavi simile e il certificate digitale corrispondente.
- Ciascun server AAA tiene traccia e memorizza tutti i possibili certificati delle CA che permettono le comunicazioni e le relazioni inter-operatori.

- Esiste almeno un deposito dei certificati digitali (certificate repository—CR) che memorizza tutti i certificati digitali e viene gestito dalla CA dell'operatore o da un'entità fidata.

Per implementare il meccanismo di AKA basato su EAP-TLS è necessario introdurre una PKI che non deve essere necessariamente parte della 3G core network [6]. L'integrazione tra la PKI e il sistema mobile 3G non è stata ancora standardizzata, in fig. 2.9 sono rappresentati dei possibili scenari in cui l'introduzione degli elementi di PKI avvenga in punti differenti della rete. Possono essere usate diverse tecniche di PKC, come RSA e la crittografia a curve ellittiche (ECC), che danno diversi risultati in termini di performance.

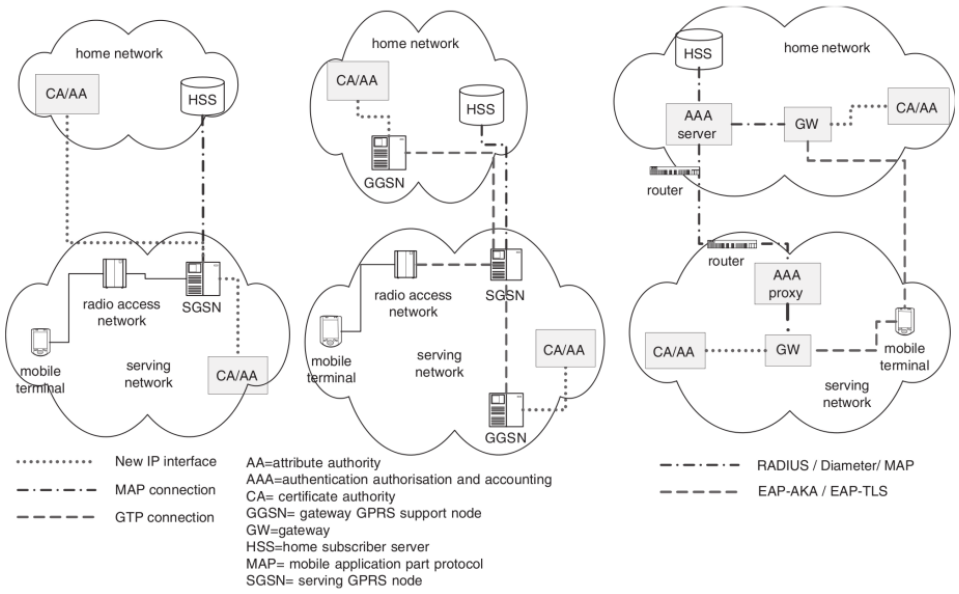

Figura 2.9: Esempi di architettura UTMS che supportino una PKI (da [6]).

2.4.3 EAP-TTLS/PEAP

Il Tunnelled Transport Layer Security (TTLS) è un estensione del TLS ed è stato sviluppato per superare la necessità, generata dal TLS, di certificati lato client (sono invece richiesti certificati lato server). TTLS e PEAP sono i due metodi attualmente disponibili di autenticazione tramite tunnel e come anche il PEAP, TTLS è un metodo a due passaggi. Nel primo, un algoritmo asimmetrico basato sulle chiavi del server è utilizzato per verificare l'identità del server e per creare il tunnel di criptazione simmetrica. Il secondo passaggio

riguarda la verifica dell'identità del client utilizzando un secondo metodo di autenticazione tramite il tunnel di criptazione simmetrica per l'attuale negoziazione dell'autenticazione. Questo secondo metodo di autenticazione utilizzato con il tunnel può essere un tipo di EAP (spesso MD5) o un metodo di vecchio tipo come PAP, CHAP, MS-CHAP, o MS-CHAP V2. Il tunnel a criptazione simmetrica del TTLS è utilizzato solo per proteggere il metodo di autenticazione del client. Una volta verificato, il tunnel collassa.

Il metodo EAP-TTLS è una conseguente revisione del protocollo EAP-TLS per consentire di autenticare una MS attraverso il tradizionale protocollo di autenticazione basato su password come il CHAP (challenge handshake authentication protocol) con un challenge implicito o esplicito. Consente di sviluppare velocemente una WLAN con un'infrastruttura esistente dove gli utenti già condividono una password segreta con il server back-end come un AAA o RADIUS server.

La fig. 2.10 mostra uno tipico scambio di messaggi, composto dal protocollo TLS allo scopo di autenticare il server e dal protocollo basato su password per autenticare il client. Se l'utente utilizza un certificato, diventa il protocollo EAP-TLS.

Poiché EAP-TLS esegue l'autenticazione mutua utilizzando SSL e ciascun lato deve provare la propria identità utilizzando il proprio certificato e la propria in risposta alla barriera dell'introduzione della public key infrastructure (PKI) che è richiesta dall'EAP-TLS e il conseguente utilizzo di metodi non basati su certificati per l'autenticazione degli utenti. PEAP è praticamente identico a EAP-TTLS, si basa sui medesimi certificati lato server per autenticare la rete e scambiare le chiavi di criptaggio. La principale differenza è che invece che stabilire un tunnel completo, le credenziali di autenticazione dell'utente vengono cifrate selettivamente. Il protocollo TTLS è stato considerato dal 3GPP per supportare l'integrazione 3G-WLAN, ma è vulnerabile agli attacchi man-in-the-middle.

Un aspetto negativo è che se nel CHAP vengono usate informazioni utente proprie della rete 3G, come la chiave segreta condivisa, queste devono essere tenute nell'AS locale della rete WLAN che è indipendente dall'operatore per le procedure di autenticazione locale e queste potrebbe verosimilmente aumentare le vulnerabilità dell'operatore mobile. Se venisse usata una chiave segreta diversa, sia EAP-TLS che EAP-TTLS non soddisferebbero agli standard di sicurezza 3GPP esistenti. Questo inoltre richiede che la MS possieda un account con la WLAN stabilto in precedenza.

Il vantaggio dell'EAP-TLS e EAP-TTLS è che una MS può fare uso dell'autenticazione localizzata senza passare dalla 3G core network.

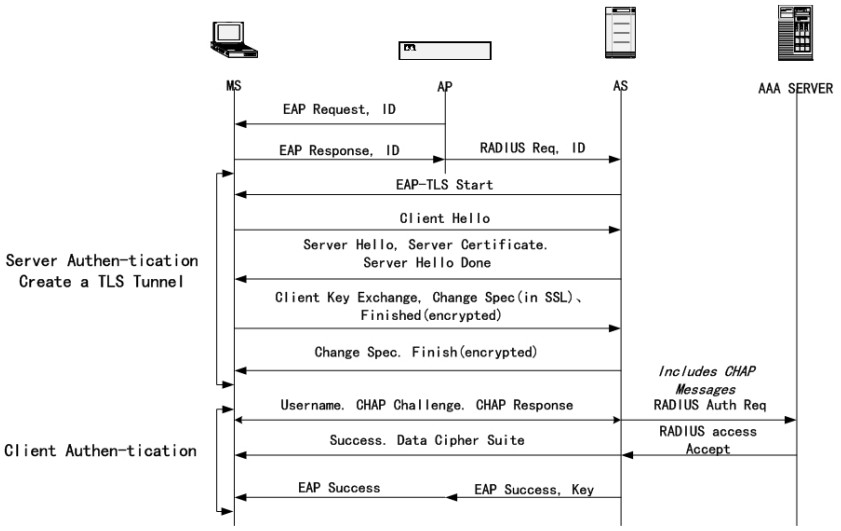

Figura 2.10: Protocollo EAP-TTLS

2.5 Meccanismo di autenticazione EAP-AKA

Il protocollo EAP-AKA [38] è essenzialmente un'incapsulamento fedele dell'UMTS AKA nell'EAP. La fig. 2.11 mostra lo scambio di messaggi per un'autenticazione di base completa e avvenuta con successo.

Inizialmente viene stabilita la connessione tra il WLAN-UE e l'AP e quest'ultimo invia un'EAP request/identity al WLAN-UE che risponde inviando o il proprio IMSI (International Mobile Subsciber Identity) o un'identità temporanea, in accordo col formato Network Access Identifier (NAI). L'AP inoltrerà il messaggio EAP (che potrebbe passare da uno o più proxy AAA) al server di autenticazione 3GPP AAA dell'utente basandosi sulla parte realm del NAI. Dopo aver ottenuto l'identità dell'abbonato, il server 3GPP AAA controlla se esiste un vettore di autenticazione (AV) disponibile per quell'utente. In caso negativo il server presenterà l'IMSI dell'utente al HSS/HLR, che potrà generare gli AV dalla chiave segreta K e inviarli al server 3GPP AAA. Se il server rileva che non è disponibile un profilo di accesso alla rete WLAN per l'utente, allora lo potrà recuperare dell'HSS. Dopo la verifica che l'utente è autorizzato all'accesso del servizio WLAN, il server 3GPP AAA memorizza gli AV per completare il meccanismo di autenticazione. Viene scelto un AV ordinato (RAND, AUTN, RES, CK, IK) basato sul SQN e per generare il materiale protetto (critico o confidenziale) vengono usate le chiavi CK e IK. Verranno poi generate numerose altre chiavi per scopi differenti, come proteggere i pacchetti EAP-AKA, per la sicurezza a livello di link-layer,

per cifrare lo pseudonimo o l'identità per la riautenticazione veloce. Il 3GPP AAA server invia al WLAN-UE il RAND, AUTN, lo pseudonimo protetto e l'ID per una successiva riautenticazione. I valori RAND, AUTN e MAC sono utilizzati per fornire protezione contro gli attacchi di tipo replay. Il MAC è calcolato sull'intero pacchetto EAP con la chiave generata.

2.5.1 Meccanismo di riautenticazione veloce EAP-AKA

In alcune situazioni il processo completo di autenticazione EAP-AKA deve essere compiuto frequentemente. Poiché il processo completo di autenticazione necessità di eseguire l'algoritmo UMTS AKA e ottenere dal HSS/HLR dei vettori di autenticazione nuovi, da ciò potrebbe derivare un carico di rete elevato nei casi in cui fosse eseguito in modo frequente. È stato quindi sviluppato un servizio di autenticazione veloce chiamato EAP-AKA fast re-authentication per alleggerire il processo di autenticazione, visto che non viene eseguito l'algoritmo UMTS AKA e non vengono scaricati nuovi AV dal HSS/HLR. La riautenticazione veloce riusa le chiavi derivate dalla precedente autenticazione completa, mentre dovrà essere generata solo una nuova master session key, utilizzata per la protezione del link layer. La figura 2.12 mostra la procedura in modo dettagliato.

Quando il 3GPP AAA server riceve la reauthentication identity, invia un contatore, un nonce, MAC e il successivo re-authentication ID al WLAN-UE. Il contatore, il nonce e il next reauthentication ID sono crittati con la vecchia chiave generata dall'ultima autenticazione completa. Il contatore protegge l'utente e il 3GPP AAA server dagli attacchi di tipo replay e limitare il numero di riautenticazioni successive senza full authentication (il contatore è inizializzato a 1 nell'autenticazione completa). Le identità ottenute con la riautenticazione veloce sono valide una volta e basta. Se il WLAN-UE non è in grado di ricevere la nuova identità generata con la riautenticazione, sarà costretto a iniziare una nuova procedura di autenticazione completa. Il nonce casuale generato dal 3GPP AAA server funziona come il RAND nella UMTS AKA. Il MAC nella risposta del WLAN-UE è calcolato utilizzando il nonce per fornire uno schema basato su challenge/response. Il MAC contiene un message authentication code calcolato su tutto il pacchetto. Dopo aver ricevuto il contatore, il nonce, il MAC e il next re-authentication ID, la WLAN-UE verifica che il MAC sia corretto e che il valore del contatore sia maggiore di ogni valore precedentemente usato, dopo di che la WLAN-UE memorizza il next re-authentication ID per utilizzarlo successivamente. Se tutti i test sono corretti, la WLAN risponde con un messaggio con lo stesso valore del contatore e MAC che viene calcolato utilizzando il nonce. Se i

test sono positivi, viene inoltrato un messaggio EAP success all'utente e la riautenticazione veloce è stata portata a termine con successo.

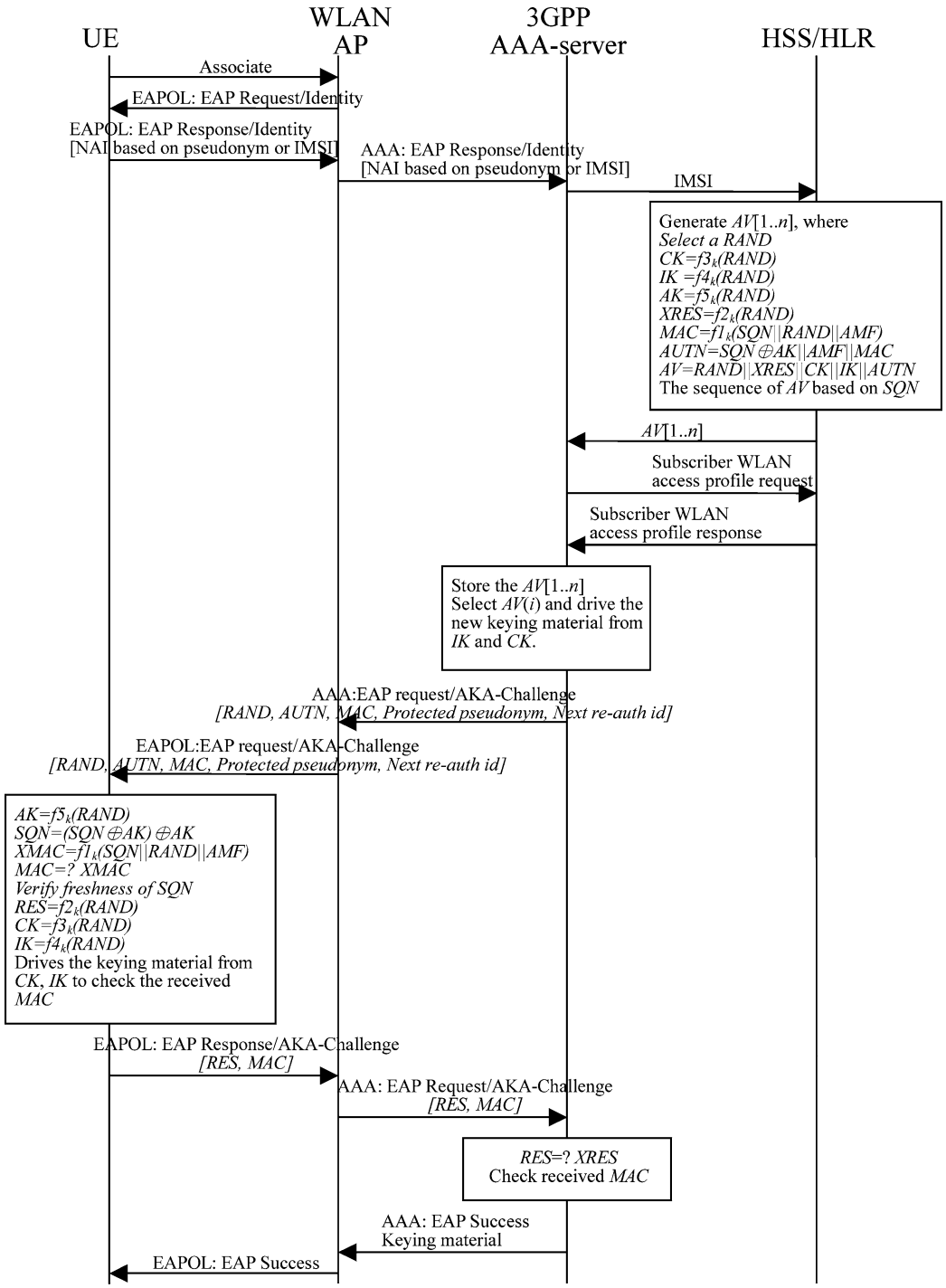

Figura 2.11: Full authentication in EAP-AKA

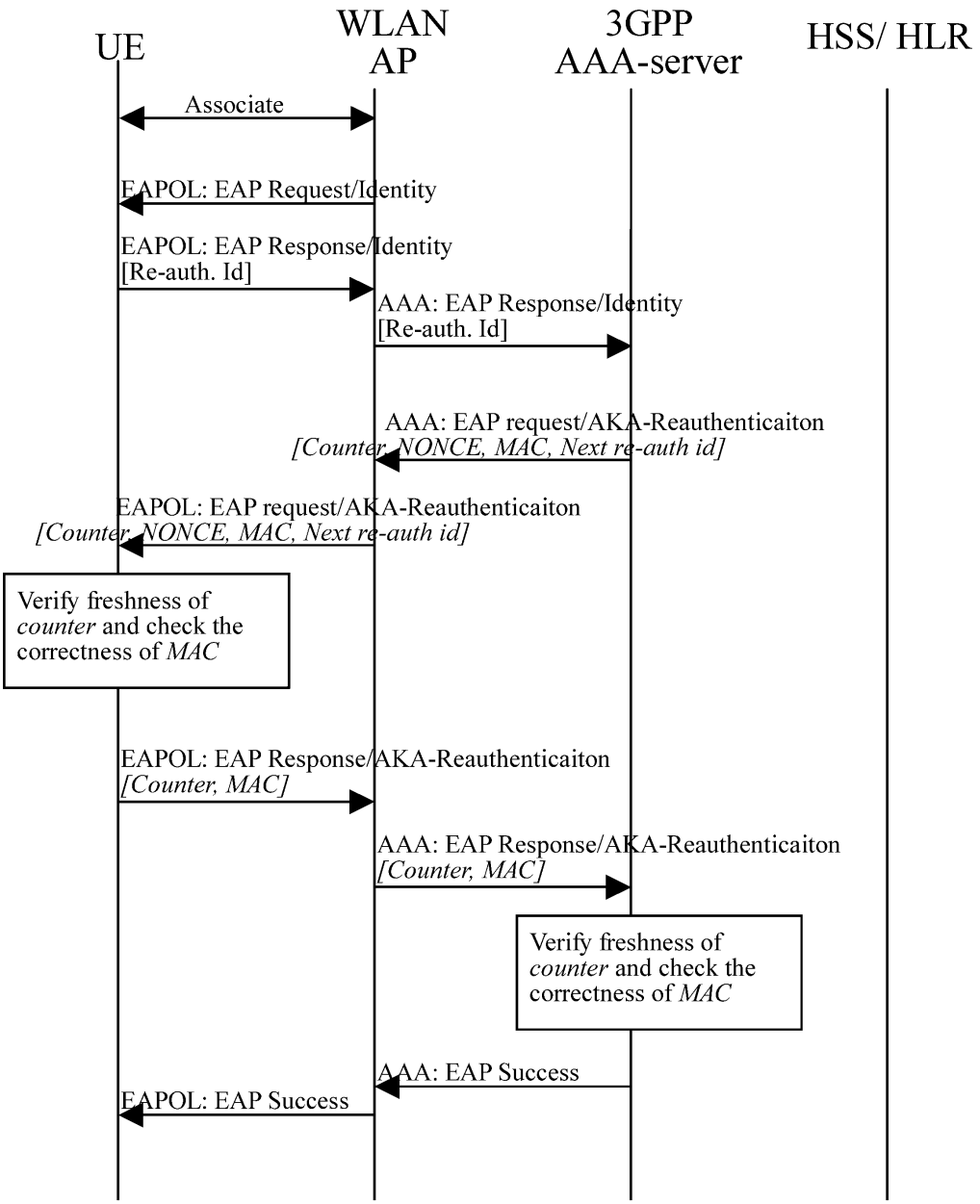

Figura 2.12: Fast re-authentication in EAP-AKA

Capitolo 3

Analisi dei protocolli proposti in letteratura

In questo capitolo, dopo aver preso visione dei problemi emersi nel protocollo EAP-AKA, verranno esposte le caratteristiche che sono emerse come imprescindibili in un meccanismo di autenticazione e verrà analizzata la loro soluzione in letteratura. Successivamente saranno analizzati singolarmente un certo numero di proposte significative in letteratura, certe emblematiche per le loro proposte innovative, altre interessanti dal punto di vista realizzativo, altre grossolanamente inadatte a un utilizzo in ambito di interlavoro 3G-WLAN. Infine verranno presentate due tabelle comparative delle caratteristiche offerte da ciascun algoritmo esaminato.

3.1 Problemi dell'EAP-AKA

Nell'UMTS, l'AKA è abbastanza simile all'autenticazione GSM. L'idea di usare una chiave pubblica nel processo di autenticazione fu abbandonata principalmente a causa di considerazioni basate sulla compatibilità all'indietro e sulle performance, valutazioni che come si vedrà in seguito si riveleranno troppo conservative per poter garantire certi servizi. L'autenticazione in entrambi i sistemi è basata su una chiave segreta simmetrica K che è memorizzata nella USIM card dell'utente e nel corrispondente Authentication Centre (AuC) dell'operatore di competenza, mentre la procedura (vedi sez. 2.5) è del tipo *challenge/response*. Diversi problemi già noti nell'AKA-GSM sono stati superati con l'UMTS, tuttavia esistono ancora delle falle che un eventuale attaccante potrebbe utilizzare per mettere a rischio l'integrità del sistema [16, 21], o che rendono il protocollo non ottimale per certi scenari. Di seguito vengono elencati i problemi più importanti.

1. Il protocollo EAP-AKA necessita di numerosi scambi di messaggi per completare la procedura di autenticazione. Questo può causare una grande latenza nella procedura, specialmente in situazioni di roaming. Poiché di solito la 3G core network è distante dalla rete WLAN, la latenza aumenta di conseguenza.

2. I vettori di autenticazione possono essere compromessi da attacchi attivi o passivi effettuati nei confronti del SGSN o dell'home subscriber server (HSS) che memorizzano un certo numero di vettori per ciascun utente. Il problema diventa più importante nel caso in cui l'utente si sposti in roaming tra due o più PLMN, per esempio in paesi diversi, dove la home network debba inviare sempre gli authentication vector per l'uso da parte della serving network.

3. In alcuni casi il sistema permette il tracciamento dell'utente per mezzo dell'identificativo permanente dell'utente (IMSI) inviato in chiaro. La procedura di richiesta dell'IMSI viene invocata dalla serving network quando:

   - l'utente si registra per la prima volta in una serving network o dopo un lungo periodo di tempo nel quale la MS non è stata attiva
   - la rete non riesce a ricavare l'IMSI dal TMSI a causa di malfunzionamenti del database del SGSN o in casi di handover quando la coppia (IMSI, TMSI) viene trasmessa da un SGSN a un altro e non è possibile risolvere con successo l'indirizzo IP del vecchio SGSN.

   La procedura è aperta ad attacchi passivi, dove l'utente malintenzionato aspetta per potenziali trasmissioni IMSI in chiaro, oppure anche con attacchi attivi del tipo man-in-the-middle [9, 16]. La trasmissione non protetta dell'IMSI è una minaccia importante contro la segretezza dell'identità dell'utente, ma esistono anche attacchi che sfruttano questa informazione per alterare l'identità dell'utente.

4. La dimensione delle chiavi e l'algoritmo di cifratura/decifratura sono fissati. Questo rende l'intero meccanismo non flessibile e poco sicuro laddove vengano scoperte delle vulnerabilità di sicurezza del sistema (come è successo nel GSM con il caso dell'algoritmo A5/1).

5. Un miglioramento di sicurezza nell'UMTS è l'inclusione del servizio di protezione dell'integrità, tuttavia, essa è garantita solo per i dati di

segnalazione tra RNC e MS. I dati utente non hanno una protezione associata e quindi sono vulnerabili a manipolazione.

6. Oltre a rendere sicure le comunicazioni mobili, i meccanismi di sicurezza dovrebbero essere in grado di fornire meccanismi di protezione anche per le applicazioni multimediali e servizi basati su IP.

3.2 Requisiti e linee guida per la progettazione di un protocollo di autenticazione

Esistono diversi aspetti critici nel processo di autenticazione, come la protezione dell'identità dell'utente, l'efficienza del protocollo e la generazione di una chiave sicura. La privacy dell'identità dell'utente (anonimato) è usata per evitare di esporre qualsiasi informazione riguardo l'identità permanente dell'utilizzatore. L'esposizione anche semplicemente per una sola volta dell'identificazione permanente compromette la posizione dell'utente sull'interfaccia radio e potrebbe permettere l'associazione di tutte le comunicazioni del medesimo utilizzatore all'interfaccia radio in questione. L'efficienza del protocollo consiste nel minimizzare la latenza di autenticazione che incontra un utente in roaming, quindi dovrebbe rendere più piccola possibile la dimensione dei messaggi e il numero di scambi tra l'home domain e il foreign domain. Inoltre dovrebbe anche essere considerato il limitato potere computazionale dei terminali mobili, con conseguente esclusione di tutti quei protocolli di autenticazione che richiederebbero pesanti calcoli sul lato del terminale utente.

Il comitato 3GPP ha proposto EAP-AKA come possibile protocollo di autenticazione per l'interlavoro 3G-WLAN. Esso fornisce un certo grado di anonimato dell'utente tramite identità temporanee, o pseudonimi, che sono equivalenti ma distinti dal Temporary Mobile Subscriber Identity (TMSI). Tuttavia, la vera identità dell'utente mobile è esposta pubblicamente quando viene eseguita la prima procedura di autenticazione dell'utente mobile, questo può causare che l'identità dell'utente possa essere esposta e tracciabile per qualche intervallo di tempo. Inoltre EAP-AKA non minimizza il numero di scambi tra l'home domain e il dominio visitato, quindi in caso di roaming tra un dominio e un altro si incorre in un'alta latenza.

I requisiti di un protocollo di autenticazione per l'interlavoro tra reti 3G e WLAN dovrebbero comprendere i presenti:

1. efficienza di rete: il protocollo dovrebbe minimizzare il numero di scambi tra l'authentication server locale (in genere quello della WLAN alla

quale viene effettuato la richiesta di collegamento) e quello nella home network.

2. privacy dell'utente: evitando che l'identità reale della MS sia esposta all'ambiente wireless

3. autenticazione mutua: l'utente mobile e il server di autenticazione locale devono essere in grado di autenticarsi a vicenda

4. scambio di una chiave sicura di sessione: in ogni sessione la chiave dovrebbe essere distinta dalle precedenti e casuale

5. sicurezza futura: anche se un attaccante riuscisse a derivare la chiave crittografica di una sessione, le sessioni future non dovrebbero essere compromesse

6. protezione dalle frodi: il sistema dovrebbe evitare che utenti non autorizzati utilizzino servizi senza avere le credenziali e dovrebbero essere evitate truffe ai danni dell'operatore da parte del gestore wireless o dell'utente

7. maggiore flessibilità: un meccanismo di sicurezza dinamico che consenta di negoziare e caricare nuovi moduli di criptaggio con chiavi di lunghezza differente on demand.

Verranno ora analizzate le principali problematiche che derivano dall'introduzione di un meccanismo di autenticazione in un ambiente condiviso.

3.2.1 Autenticazione

L'UMTS authentication and key agreement (AKA) è discusso in alcune ricerche che ne evidenziano alcuni difetti [5, 6, 12, 19, 23, 25]. Uno di questi è che il protocollo necessita lo scambio di numerosi messaggi per completare la procedura e questo può causare un'alta latenza per l'autenticazione, specialmente quando usato in interworking. Visto che in generale il core della rete 3G è distante dalla rete 802.11, il ritardo aumenta di conseguenza e questo può creare dei problemi nel caso di applicazioni real-time. Inoltre l'EAP-AKA rivela l'identità dell'utente alla rete WLAN e quindi la privacy dell'utente non è garantita. Anche se il problema dell'identità dell'utente può essere risolta tramite l'uso di uno pseudonimo, questo può essere utilizzato per tracciare l'utente che si sposta in roaming.

Il problema dell'autenticazione è stato affrontato in modo diverso in letteratura. In [2] ("Direct authentication method", vedi sez. 3.3.4) è stato

proposto l'utilizzo dell'interfaccia 3G per l'autenticazione indipendentemente dalla presenza o meno della rete WLAN. In [8] è proposta una procedura di autenticazione ad un unico passaggio per la connessione IMS per ridurre lo scambio di messaggi.

L'utilizzo della tecnica di hash chaining per migliorare l'efficienza del protocollo è stata utilizzata in [14] e [7]. L'hash chaining permette all'utente di produrre una serie di evidenze grazie alle quali autenticarsi in momenti successivi con relativa facilita, poiché per l'AAA server è facile verificare l'appartenenza di un anello all'utente, mentre è molto difficile risalire da un anello al precedente della catena.

3.2.2 Tariffazione e non-ripudiabilità

Con l'integrazione delle reti 3G e WLAN, devono essere anche forniti degli accordi o dei meccanismi per la tariffazione comune, che devono integrare e supportare la non-ripudiabilità. Questa risulta essere una caratteristica molto importante nel caso in cui la rete 3G e la rete WLAN siano amministrate da operatori diversi, infatti se non venisse fornito questo meccanismo gli operatori potrebbero ingannarsi a vicenda o mettersi d'accordo per imbrogliare l'utente, addebitando più o meno del dovuto a seconda dei casi. A questo proposito è stato proposto da Prasithsangaree [12] (vedi sez. 3.3.9) uno schema di doppia firma chiamato "Localized Dual Signature Authentication", che fornisce un protocollo di autenticazione localizzata in grado di ridurre la latenza nello scambio di messaggi tra le due reti fornendo anche anonimato dell'utente. L'idea principale dello schema a doppia firma (standardizzato nel SET protocol [13]) è che un operatore WLAN possa ottenere le informazioni di utilizzo della rete da parte di un determinato utente pur non essendo a conoscenza della reale identità. L'autenticazione avviene localmente tramite l'utilizzo di certificati firmati da una CA che servono anche per firmare dei *payment order message digest* (POMD) che contengono le informazioni sull'uso della rete e un digest delle informazioni utente (che rappresenta l'user ID protetta) che l'operatore WLAN utilizzerà per ricevere i pagamenti.

Esistono in letteratura anche approcci duali con entrambe le tecniche basate su password e su chiave pubblica (come in sez. 3.3.2). Nel protocollo con password, il terminale mobile si deve effettuare la procedura inviando, tramite la WLAN, la richiesta presso l'authentication server dell'operatore 3G (3G-AAA), che calcolerà un parametro che potrà essere usato dall'operatore WLAN. Poiché questa procedura non supporta la non-ripudiabilità, è stato successivamente proposto un protocollo duale basato su chiave pubblica. I service provider 3G e WLAN devono essere registrati presso un trust centre (TC) che garantisca e firmi i loro certificati. Inoltre l'operatore 3G emette i

certificati per l'utente mobile e l'operatore WLAN. L'utilizzo della rete wireless da parte dell'utente viene registrato grazie all'utilizzo di token basati sull'hash chaining.

3.2.3 Riautenticazione veloce

Esistono certe situazioni in cui l'autenticazione deve essere compiuta frequentemente, perciò un protocollo di riautenticazione veloce può portare dei reali benefici alle applicazioni real-time se il protocollo di autenticazione ha una certa complessità in termini di scambio di messaggi, o se richiede l'utilizzo dei server di autenticazione remoti, mentre i vantaggi potrebbero essere più limitati in caso di supporto dell'autenticazione localizzata o di altri meccanismi che riducano il numero di pacchetti scambiati nella fase di autenticazione. Se non viene fornito un servizio veloce di riautenticazione, le applicazioni a livello utente, come il VoIP o le video comunicazioni potrebbero incontrare dei ritardi dovuti alle frequenti operazioni di autenticazione, tanto maggiori quanto è più grande la distanza tra la rete 3G e quella WLAN. Il servizio di riautenticazione veloce offerto dal protocollo EAP-AKA (vedi sez. 2.5.1) non supporta meccanismi di tariffazione e non-ripudiabilità e protezione dell'identità dell'utente, funzionalità che devono essere garantite anche in presenza di riautenticazione veloce.

3.2.4 Autenticazione localizzata

Il problema dell'autenticazione localizzata viene risolto con l'uso dei certificati utente a chiave pubblica, che possono essere facilmente autenticati dall'operatore WLAN, da quello 3G o da una CA. Rappresenta un metodo efficace per ovviare ai problemi dei ritardi che nascono quando un utente si sposta dalla propria home network e deve effettuare nuovamente la procedura di autenticazione. Il ritardo può aumentare, quando la home network è distante geograficamente dalla rete visitata. Nel caso peggiore la sessione può essere terminata e l'utente costretto a iniziare una nuova procedura. È quindi preferibile utilizzare l'autenticazione localizzata per i suoi ritardi più bassi, nonostante questo comporti in genere l'introduzione di un algoritmo di crittografia a chiave pubblica che aumenta il ritardo a causa dei costi computazionali.

3.2.5 Continuità di servizio e mobility management

Dal momento che gli scenari di interlavoro (vedi tab. 2.1) dal 4 in su sono ancora in fase di studio, esistono solo alcune proposte per il problema della

continuità di servizio. Il problema più importante è come rendere sicuro un servizio di trasferimento da una rete a un'altra. Inoltre se un utente cambia rete di accesso dopo aver iniziato un servizio o una sessione in una rete 3G o WLAN, il servizio potrebbe essere terminato e ciò può essere causato da diversi fattori. Un impiegato di un'azienda potrebbe voler utilizzare per accedere alla rete della sua azienda una Virtual Private Network (VPN), per proteggere il traffico tra l'utente e la rete aziendale. Le associazioni di sicurezza tipo IPsec o VPN devono essere rinegoziate a causa del roaming dell'utente tra due diverse reti di accesso e il cambio conseguente di indirizzo IP. Per risolvere questi problemi, come anche quello del significativo overhead che una connessione VPN comporta a tutto il traffico, anche a quello che non necessiterebbe di essere protetto, è stato proposto in [3] un protocollo chiamato Secure Universal Mobility che supporta la mobilità trasparente (cioè "seamless") e l'utente non necessita di mantenere una connessione VPN always-on, grazie all'introduzione di un meccanismo di VPN dinamico. Il VPN dinamico è ottenuto grazie all'uso di tunnel doppi MIP che hanno bisogno di due home agent, uno interno e uno esterno. Il primo tunnel è dal mobile user all'home agent esterno, l'altro dall'home agent esterno a quello interno. Una volta che sono stati stabiliti i due tunnel, l'utente (o corresponding node) può iniziare una comunicazione inviando un messaggio SIP INVITE. Il ricevitore controlla se esiste una sessione VPN aperta, in caso contrario viene usato il protocollo IKE (Internet key exchange) per negoziare i parametri di sicurezza e stabilire una nuova sessione VPN.

3.3 Algoritmi proposti in letteratura

Vengono analizzati ora una serie di lavori particolarmente significativi per il contributo portato in letteratura nel campo degli algoritmi di autenticazione nell'interlavoro 3G-WLAN.

3.3.1 Salkintzis, Fors, Pazhyannur [11]

Uno degli unici lavori ad analizzare anche il caso di architettura di tipo tight, attraverso l'introduzione di una nuova interfaccia nella core network dell'operatore 3G e in particolare tra l'SGSN e un nuovo elemento posto nella WLAN network con le funzione di interconnessione tra le due reti.

L'approccio di tipo loose analizzato viene risolto inserendo nell'architettura un elemento chiamato CAG (cellular access gateway) che fornisce le funzionalità di AAA server nel core della rete 3G. Esso interagisce con l'HLR per ottenere le credenziali di autenticazione usate per creare il challenge di

autenticazione per la MS. A questo scopo il CAG deve dialogare con l'HLR in modo simile al SGSN.

La cifratura è debole perché affidata solamente al miglioramento del WEP attraverso l'assegnazione di una singola chiave per sessione e per utente. Con l'uso dell'802.1X non è necessaria la condivisione delle chiavi perché esse vengono derivate per ogni utente a ogni nuova sessione.

La tariffazione si ottiene per mezzo di un "billing mediator", un server AAA ad hoc per supportare i protocolli standard, tipo RADIUS o Diameter. Il mediator ha lo scopo di convertire le statistiche di accounting dalle varie reti di accesso in un formato nativo per l'operatore cellulare. Non vengono quindi offerti servizi di non-repudiation.

Viene stabilita a priori una possibilità di supporto della mobilità di sessione attraverso l'uso del protocollo MIP.

3.3.2 Tseng, Yang, Su [14, 15]

Protocollo di autenticazione e tariffazione, sviluppato in modo efficiente e basato sulla tecnica di hash chaining, proposto in due versioni distinte: una tecnica basata su password e una su chiave pubblica e certificati. Esistono tre componenti diversi, l'autentication server della rete 3G (3G-AS), l'authentication server della rete WLAN (WLAN-AS) e il terminale mobile (MT) che ha una doppia interfaccia, sia 3G che WLAN.

Versione password-based Nella versione password based, il protocollo usa una tecnica di one-time password per autenticare gli utenti presso la rete 3G. È efficiente in termini di messaggi scambiati (confrontato con EAP-AKA) e di pesantezza computazionale dell'algoritmo, ma non implementa il servizio di tariffazione con non-ripudiabilità, proprio per i limiti della tecnica utilizzata. I due AS si autenticano a vicenda preliminarmente, stabilendo una chiave di sessione tra loro tramite l'utilizzo di un qualsiasi metodo che supporti autenticazione mutua e uno schema di key-agreement. Dopo essere stato autenticato dal 3G-AS, il MT può mandare al 3G-AS la richiesta di accesso alla WLAN Quando il 3G-AS riceve la richiesta, calcola un parametro che può essere utilizzato per l'autenticazione dall'operatore WLAN e comincia la procedura tariffazione. In fig. 3.1viene mostrato lo scambio di messaggi tra gli elementi di rete. Per fornire anche il servizio di non-ripudiabilità, è stata proposta anche la versione basata su chiave pubblica del protocollo.

Versione public-key based Nella versione a chiave pubblica i provider 3G e WLAN devono registrarsi presso un trust centre (TC) che provvede a

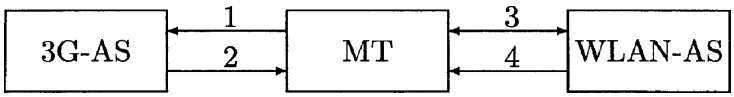

Figura 3.1: Scambio di messaggi per la versione password-based

rilasciare i certificati per le due entità. Inoltre, a sua volta, l'operatore 3G firma i certificati per l'utente e per la rete WLAN. Quando un MT necessita di accedere a una rete, invia una richiesta al 3G-AS, quindi il 3G-AS e WLAN-AS si autenticano a vicenda attraverso un protocollo basato su autenticazione a chiave pubblica. Il 3G-AS inoltra l'identità del MT e il suo certificato alle WLAN-AS. Dopo WLAN-AS crea un nel database un record del MT; 3G-AS manda il certificato criptato appartenente al WLAN-AS al MT, dopo di che l'MT può negoziare con il WLAN-AS e stabilire una chiave di sessione con il protocollo EAP-TLS. Il registro dei dati riguardanti l'utilizzo della rete WLAN si basa su l'utilizzo di una tecnica su hash-chaining. In fig. 3.2 viene mostrato lo scambio di messaggi tra gli elementi di rete.

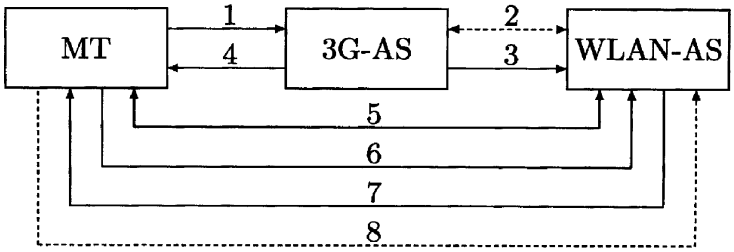

Figura 3.2: Scambio di messaggi per la versione public-key based

3.3.3 Lin, Harn [7]

Esempio di semplice protocollo che unisce firma digitale a chiave pubblica e hash chaining. Attraverso la combinazione di queste due tecniche è possibile fornire la capacità di risolvere eventuali tariffazioni contestate, proteggendo gli utenti da addebiti errati e fornendo ai service provider prove legali per poter reclamare saldi non effettuati. È formato da 4 sottoprotocolli: registrazione, prenotazione del servizio, negoziazione della chiave di servizio e negoziazione della chiave di sessione.

Il protocollo di registrazione permette all'utente di fornire la sua chiave pubblica alloperatore di appartenenza, ricevendo in cambio una chiave di

autenticazione e l'IMSI. In questo modo è possibilie evitare il problema della revoca dei certificati pubblici e quindi della presenza di una trusted public-key certification authority.

Il protocollo di prenotazione del servizio interagisce tra la MS e i database della rete visitata e della home network e fornsce la prova legale che l'utente ha intenzione di utilizzare un certo servizio nella rete visitata.

Il protocollo di negoziazione della chiave di servizio stabilisce una chiave per il particolare servizio scelto tra l'utente e il server di autenticazione della rete visitata.

Il protocollo di negoziazione della chiave di sessione serve per ottenere, grazie alla chiave di servizio e a una catena di hash delle varie chievi di sessioni da utilizzare per accedere al servizio.

Il meccanismo fornisce autenticazione mutua, debole protezione dell'identità dell'utente e indipendenza delle sessioni. La tariffazione con non-ripudiabilità permette di identificare se la causa dell'addebito errato del servizio è da ricercare in un errore di accounting, in una frode interna o in una falla di sicurezza del service provider. Un chiaro svantaggio è l'utilizzo imprescindibile non solo dei database della rete visitata, ma anche obbligatoriamente della home network in ogni sottoprotocollo di cui è composto.

3.3.4 Cheng, Tsao [2]

Per effettuare l'autenticazione in una situazione di interlavoro, l'utente deve passare attraverso la procedura di access control della rete WLAN e completare la procedura di segnalazione alla 3G core network. Per evitare questo problema è stato proposto in [2] l'utilizzo dell'interfaccia radio 3G per completare le procedure di autenticazione e autorizzazione indipendentemente dalla situazione di roaming. Questo schema presenta diversi vantaggi, prima di tutto le procedure di autenticazione avvengono in un ambiente ad alta sicurezza visto che vengono scambiati i messaggi tramite l'interfaccia 3G, poi l'utente non necessita di rivelare la propria identità e quindi la privacy viene mantenuta. Viene riutilizzata l'infrastruttura di segnalazione 3G già esistente, inoltre può essere utilizzato per l'interlavoro anche con reti 802.11 che non utilizzino il protocollo IEEE 802.1x per il controllo dell'accesso. D'altra parte la banalità del meccanismo che applica in modo quasi letterale la situazione prevista dallo scenario 2 (vedi tab. 2.1), evidenzia degli svantaggi intrinseci, come la necessità di passare attraverso la 3G home network ad ogni registrazione, la mancanza di un metodo di riautenticazione veloce o di supporto alla non-ripudiabilità.

3.3.5 Kambourakis, Rouskas, Gritzalis [5]

Viene proposto l'utilizzo di un meccanismo di authentication e key agreement basato su SSL/TLS per superare i problemi di sicurezza dell'EAP-AKA, soprattutto per quanto riguarda l'utilizzo di AV compromessi da parte di un eventuale intruder. Inoltre viene in questo modo superato il grande deficit della mancanza di una procedura dinamica e flessibile di AKA.

Vengono fatte delle assunzioni generali, quali:

- presenza di una qualche CA che emetta e revochi i certificati,
- presenza di smart card USIM con buone capacità di generare numeri pseudocasuali e chip ottimizzato per funzioni crittografiche,
- possesso di una coppia di chiavi (pubblica, privata) da parte di ciascun utente memorizzate nella USIM e associate al momento della registrazione,
- precaricamento sulle USIM dei certificati della CA
- ciascun elemento di rete che prende parte alla procedura AKA possiede una coppia di chiavi e il corrispondente certificato
- ciascun SGSN/VLR tiene traccia e memorizza tutti i possibili certificati per i riferimenti incrociati
- esiste almeno un database dei certificati digitali, gestito dalla CA
- esiste almeno un database dei certificati revocati, che viene gestito dalla CA e che deve essere accessibile a tutti gli elementi di rete

Fatte queste assunzioni il protocollo è un modello di autenticazione reciproca mediante verifica dei certificati e tramite un'identità temporanea che è il TMSI e generazione di una chiave di sessione.

Supporta il session resuming per minimizzare l'overhead, anche se deve essere utilizzato con attenzione perche viene riutilizzata la stessa chiave di sessione e quiendi i potenziali utenti malintenzionati hanno a disposizione più dati e più tempo per effettuare analisi. È quindi ragionevole imporre un limite quantitativo e temporale oltre il quale sia obbligatorio effettuare un'autenticazione completa.

3.3.6 Kambourakis, Rouskas, Kormentzas, Gritzalis[6]

Gli stessi autori del protocollo precedente propongono un'altra soluzione per risolvere il problema dell'autenticazione nell'interworking 3G-WLAN sfruttando una tecnica basata su SSL/TLS. Lo schema è chiamato EAP-TLS AKA. Un MT e un AAA server si autenticano utilizzando EAP-TLS attraverso un accesso ppoint che supporta EAP-TLS e, dopo essersi autenticati, cambiano la cipher specification e creano le chiavi di sessione rispettivamente. Lo schema basato su SSL/TLS beneficia della sicurezza end-to-end granzia alla natura stessa dell'algortmo di crittografia asimmetrica (al contrario EAP-AKA fornisce sicurezza hop-by-hop)

EAP-AKA assume l'esistenza di una chiave simmetrica a lungo termine per utente, è utile quindi avere un meccanismo che permetta la creazione di una chiave di sessione. L'utilizzo di SSL/TLS permette di trarre vantaggio dalle capacità di negoziazione della ciphersuite protetta e flessibile, autenticazione mutua e gestione dellechiavi scalabile.

In fig. 3.3 è mostrato un possibile esempio di protocollo AKA basato su EAP-TLS. Confrontando le due possibili opzioni, EAP-AKA e EAP-TLS si può notare:

- l'architettura di rete che supporta l'integrazione rimane la stessa anche con l'aggiunta della PKI. In ogni caso devono essere create delle interfacce IP ad-hoc

- il supplicant e l'AAA server devono supportare entrambi EAP-TLS, mentre l'AP deve supportare l'autenticazione con EAP-TLS.

- qualsiasi AAA server (WLAN o 3G) che risiede vicino al supplicant può fornire l'autenticazione, miglioreando la mobilità Questo è possibile grazie agli scambi dei certificati che garantiscono i riferimenti incrociati dei certificati, che possono essere firmati dal server AAA della home network o da una comune CA

- le performance possono essere migliorate in modo significativo utilizzando SSL/TLS per il resuming della sessione

- SSL/TLS è un protocollo ben conosciuto nell'ambito wired e, accompagnato da una PKI, è ottimale per supportare grandi infrastrutture di tipo eterogeneo. La flessibilità di scegliere tra diverse ciphersuites e algoritmi di MAC diminuisce le possibilità di intrusione. Inoltre la scalabilità del meccanismo a chiave pubblica offre un framework competitivo per superare le inefficienze della crittografia a chiave simmetrica

- non è necessario l'uso di HSS/HLR per generare e distribuire i vettori di autenticazione, evitando il rischio di intercettazione o utilizzo fraudolento. Dall'altra parte i certificati controllano il processo di autenticazione reciproca
- EAP-TLS è generalmente considerato un protocollo end-to.end in contrasto con la sicurezza di tipo hop-by-hop che è fornita dall'EAP-AKA tradizionale, che si deve dotare di meccanismi aggiuntivi come IPsec per rendere sicure le comunicazioni inter o intra-rete.

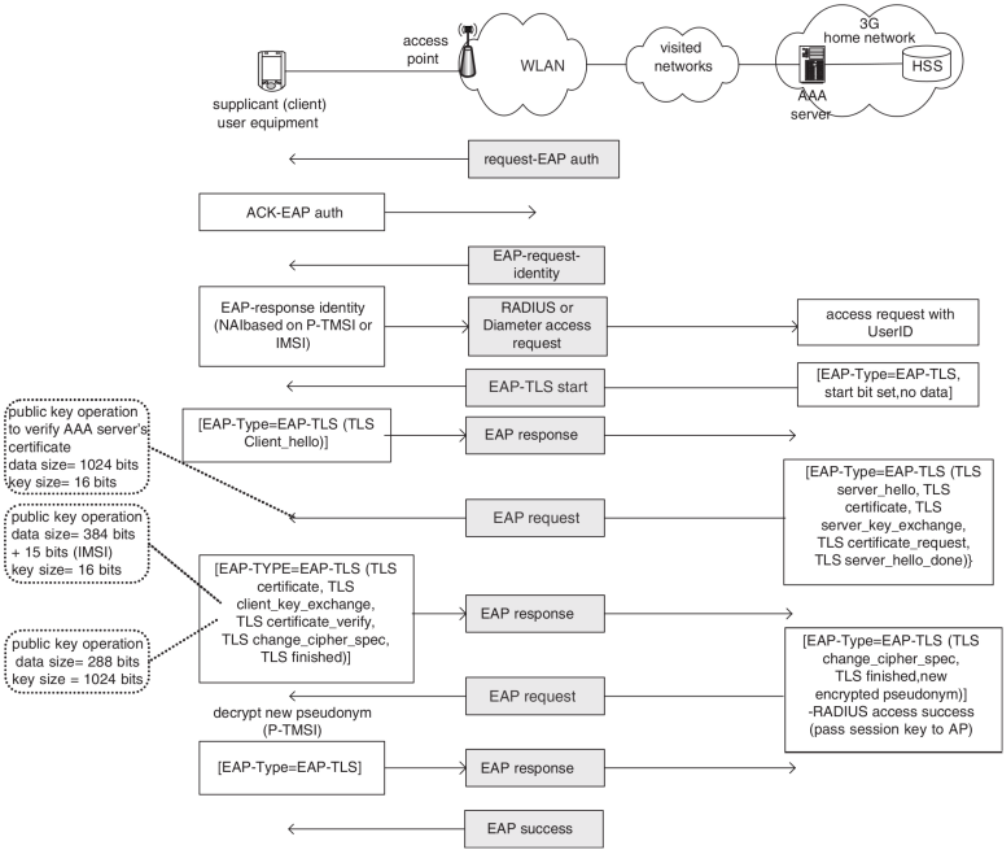

Figura 3.3: AKA basato su EAP-TLS

3.3.7 Lin, Chang, Hsu, Wu [8]

Per accedere ai servizi multimediali su IP deve essere eseguita l'autenticazione anche a livello IMS che ha molti passi in comune con la tradizionale

procedura di autenticazione standard. Viene proposta quindi una procedura one pass GPRS/IMS che permette un risparmio nello scambio di pacchetti che arriva fino al 50%, aumenta le performance e risparmia in termini di costi computazionali. La IMS one pass authentication si focalizza nello specifico sulla sessione IMS ed ha come principale svantaggio la mancanza di un key agreement, caratteristica già presente nei protocolli precedenti, anche in quelli già standardizzati. È da sottolineare come i nuovi protocolli non dovrebbero eliminare funzioni presenti nelle versioni standard, specie se importanti.

3.3.8 Ouyang, Chu [10]

Esempio di protocollo che supporta il trasferimento di contesto in modo sicuro, evitando problemi di dirottamento di sessione. Viene evidenziato come a causa dell'insufficiente architettura di sicurezza della 802.11 WLAN, il trasferimento di contesto da una rete UMTS a una WLAN può essere vittima di dirottamento. Viene anche proposta un'architettura che migliori gli aspetti di sicurezza, introducendo un protocollo chiamato OTSKGP (one time session key generation protocol), disegnato per creare un trasferimento di contesto sicuro tra un utente mobile e un access point, proteggendo il traffico utente. L'obiettivo dell'OTSKGP è creare un trasferimento di contesto sicuro tra l'AP e la MS al fine di proteggere i dati in caso di handover tra rete UMTS e WLAN. Quando viene protetta l'interfaccia wireless è possibile proteggere la trasmissione da numerosi attacchi. Nel protocollo la MS e l'AP si autenticano reciprocamente tramite un server di autenticazione. Il protocollo è composto da tre fasi, la fase di registrazione presso l'AP, la fase di generazione della chiave e la fase di refresh della chiave.

Viene proposto uno schema di trasferimento di contesto nell'integrazione 802.11 e UMTS, compreso di un robusto protocollo per proteggere la privacy dell'utente da eventuale eavesdroppers e tentativi di spoofing. L'OTSKGP viene usato quindi in situazioni di roaming da UMTS a 802.11 per garantire alta confidenzialità e autenticazione mutua. Nel caso di passaggio da 802.11 a WLAN la costruzione del contesto sicuro viene affidata alla procedura di autenticazione dell'UMTS.

3.3.9 Prasithsangaree, Krishnamurthy [12]

Per migliorare le caratteristiche dei protocolli già presenti viene proposto un algoritmo basato sul concetto della doppia firma, usato nella Secure Electronic Transaction (SET) che soddisfi le seguenti caratteristiche:

1. non richiede una connessione diretta tra rete 3G e WLAN

2. il protocollo migliora le performance in termini di latenza perché è eseguito localmente nella WLAN usando algoritmi standard per l'autenticazione come EAP-TLS e EAP-TTLS

3. il protocollo fornisce anonimato all'utente

4. il protocollo fornisce forte autenticazione mutua.

Il protocollo proposto è una combinazione di un protocollo a autenticazione localizzata come EAP-TLS o EAP-TTLS eseguito da un operatore wireless indipendente e uno schema a doppia firma per comunicare con la 3G network.

Localized authentication È possibile autenticare localmente una MS con un certificato a chiave pubblica, assegnato alla MS che viene firmato da una certificate authority di operatore 3G. il certificato può contenere per esempio le informazioni del sottoscrittore, il profilo e una chiave pubblica. È possibile garantire anonimato con delle informazioni non direttamente correlate all'utente, come un ID anonima, o delle informazioni sotto hashing. LA CA firma tutte le informazioni. Per validare il certificato, l'operatore WLAN utilizza la chiave pubblica della CA, per verificare che l'utente possieda il certificato, l'operatore invia un nonce N_1 come challenge, al quale la MS risponde con lo stesso nonce N_1, l'identità dell'AS locale dell'operatore WLAN (AS_{ID}), la firma di (N_1, AS_{ID}) utilizzando la chiave privata KR_{MS} (alla quale corrisponde la chiave pubblica KU_{MS}) e il $Cert_{MS}$.

$$(MS) \rightarrow (AS) : N_1, AS_{ID}, Sign_{KR-MS}(N_1, AS_{ID}), Cert_{MS}$$

L'operatore WLAN ottiene la chiave pubblica (KU_{MS}) dal $Cert_{MS}$ e la usa per verificare la firma, Se la firma è valida, l'utente è autorizzato ad accedere alla rete. Dove $Sign_x(\cdot)$ è la firma digitale utilizzando la chiave x.

Schema a doppia firma Gli operatori WLAN non devono essere considerate delle entità fidate, è necessario un algoritmo che eviti le rivendicazioni fraudolente. Lo schema a doppia firma può prevenire che gli operatori WLAN alterino le informazioni sull'utilizzo (usage information —UI) della MS e preserva l'anonimato della MS (o client information —CI). Lo UI indica la quantità di utilizzo della WLAN negoziata dalla MS quando entra nella WLAN, mentre il CI può contenere informazioni utente come l'IMSI. Per generare la dual signature (DS) come in fig. 3.4, viene applicata una funzione di hash a CI e UI, producendo un message digest di entrambi (CIMD e UIMD). Essi

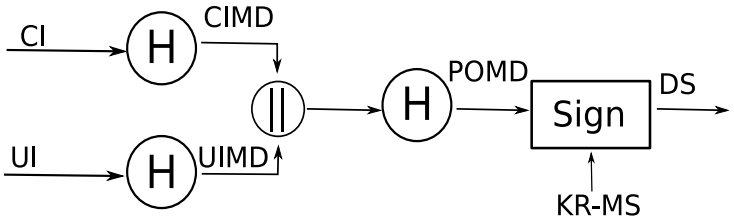

Figura 3.4: Schema a doppia firma

vengono concatenati per formare il payment order message digest (POMD) che viene firmato dalla chiave privata dell'utente.

Utilizzando questa doppia firma, l'utente prepara il submission token (mostrato in fig. 3.5) che è composto da una parte da inviare all'operatore 3G e una all'operatore WLAN. L'encrypted part (EP) è criptata con una chiave di sessione generata casualmente (K_s) che è trasferita all'operatore 3G utilizzando una busta digitale (digital envelope—DE), la quale a sua volta è criptata con la chiave segreta condivisa tra l'utente e l'operatore 3G ($K_{MS,3G}$) che è la stessa chiave segreta usata nell'autenticazione AKA.

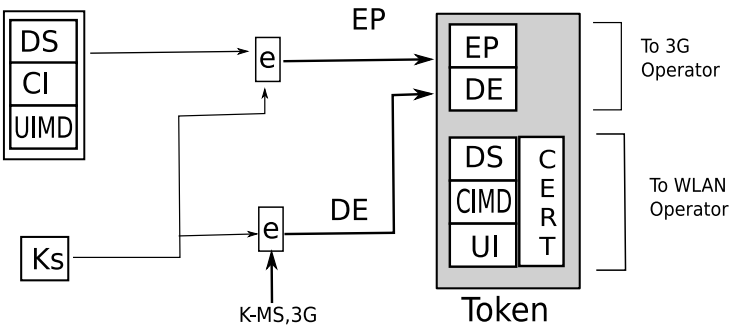

Figura 3.5: Generazione del token che il clienti invia all'operatore WLAN.

Grazie alla DS può essere ottenuto l'anonimato dell'utente. L'operatore wireless infatti non conosce la reale identità del cliente (CI), poiché viene a conoscenza solo della sua versione hash, cioè CIMD. L'operatore può solamente verificare la validità e integrità, con la procedura inversa mostrata in fig. 3.6.

Per ottenere i pagamenti, l'operatore WLAN trasmette l'EP e il DE all'operatore 3G che decritta DE per ottenere la chiave K_s, utilizzata a sua volta per decrittare e ottenere DS, CI e UIMD. L'operatore 3G produce il POMD e verifica questo valore con quello inviato crittato in DS dall'opera-

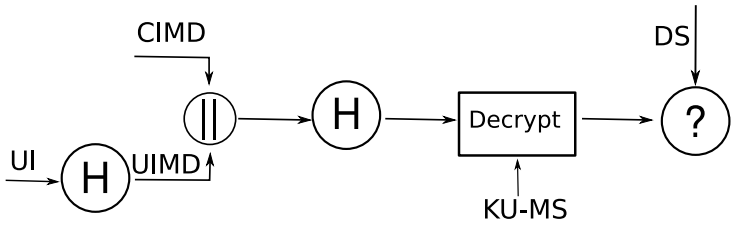

Figura 3.6: Verifica dell'identità dell'utente (CI) da parte dell'operatore WLAN.

tore WLAN. Se il valore è lo stesso, accetta la richiesta e paga l'operatore wireless. Il processo può essere eseguito offline periodicamente, e pertanto non è richiesta una connessione diretta real-time dalla WLAN alla 3G core network.

Per la sottomissione del token è necessario un protocollo apposta. Quello proposto, risonde al nonce N_2 dell'AS, con lo stesso valore, l'identità dell'AS (AS_{ID}), il token e l'hash di $(token, AS_{ID}, N_2)$. L'hash protegge da attacchi di tipo reply e garantisce la freschezza del token.

$$(MS) \rightarrow (AS) : N_2, AS_{ID}, token, H(token, AS_{ID}, N_2)$$

Per produrre il token vengono coinvolte tre funzione crittografiche, le funzioni di hash per creare i message digest, la firma digitale DS e la funzione di criptaggio applicata per ottenere EP e DE. La firma può essere fatta con qualsiasi algoritmo a chiave pubblica, come RSA, ECDSA (elliptic curve digital signature algorithm) o anche con una funzione di keyed hash tipo HMAC, visto che MS condivide una chiave segreta con l'operatore WLAN.

La fig. 3.7 mostra un possibile scambio di messaggi.

Attraverso un nuovo schema chiamato localized dual authentication scheme, e un approccio di tipo loose coupling, fornisce anche localized authentication. Nel protocollo l'anonimato dell'utente è fornito usando un'identificazione non relative alle informazioni personali, che però consente di tracciare/ monitorare la posizione dell'utente. L'autenticazione localizzata è possibile grazie all'uso di un certificato di chiave pubblica dell'utente. Dal momento che il certificato può essere autenticato da un operatore WLAN, l'utente è autorizzato all'utilizzo delle risorse di rete wireless. Inoltre, il certificato viene usato per per lo scambio di chiavi. Lo schema a doppia firma è standardizzato nel Secure Electronic Protocol (SET) [13]. L'idea fondamentale di una doppia firma è che per l'operatore WLAN non sia possibile conoscere la reale identità dell'utente in roaming, fornendo così privacy, ma possa d'altro canto

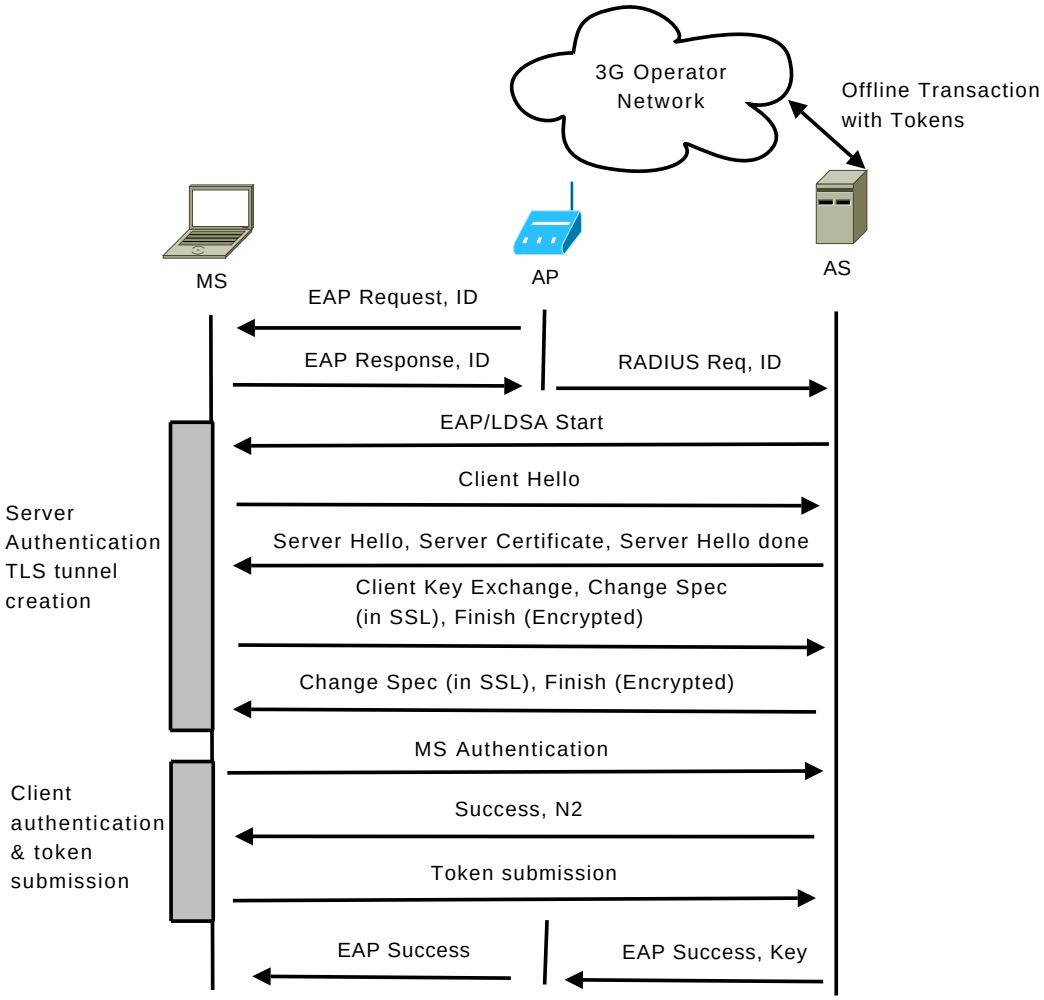

Figura 3.7: Possibile scambio di messaggi nel protocollo LDSA.

ottenere le informazioni di consumo. L'utente possiede un certificato firmato dalla CA dell'operatore 3G, che utilizzerà per autenticarsi presso un operatore WLAN. L'utente firma un "payment order message digest" che conterrà oltre alle informazioni di utilizzo della rete, anche un identificativo dell'utente ("client information message digest") e lo inoltrerà all'operatore WLAN che lo utilizzerà a sua volta che richiedere il pagamento dall'operatore 3G.

3.3.10 Salgarelli et al. [25]

Wireless Shared Key Exchange (W-SKE) è un semplice protocollo di autenticazione e scambio di chiave a chiave condivisa progettato per soddisfare i seguenti requisiti: autenticazione reciproca tra la MS e l'home AAA server (H-AAA), generazione della chiave di sessione, sicurezza futura, cioè la garanzia che la compromissione di una chiave di sessione consente l'accesso solo ai dati protetti con quella chiave e non a quelli delle sessioni passate o future, identificazione degli elementi di rete lungo il percorso tra la MS e l'home AAA e infine semplicità di analisi del protocollo.

Nel W-SKE l'associazione di sicurezza tra la MS e il H-AAA è formata da due parametri, l'identificativo dell'utente (User Identifier—UID), che identifica in modo univoco l'utente al H-AAA, e la chiave segreta criptograficamente sicura $K_{MS,H-AAA}$, condivisa tra la MS e il suo H-AAA. Oltre a garantire autenticazione mutua tra la MS e l'H-AAA, W-SKE fornisce la generazione di un'associazione sicura temporanea di sessione tra l'AS e la MS. Questa associazione sicura ha la forma di una chiave di sessione (Session Master Secret, K_{SMS}), che viene distribuita in modo sicuro all'AS da parte del H-AAA.

W-SKE è stato proposto come alternativa alle elevate latenze incontrate da EAP-AKA e EAP-SIM e per ridurre il numero di messaggi scambiati. Esistono comunque diverse debolezze nel protocollo,

1. W-SKE non introduce non-ripudiabilità, e non può prevenire eventuali frodi dell'AAA visitato a carico della home network,

2. non viene considerata la protezione dell'identità dell'utente,

3. non è ottimizzata la latenza di autenticazione.

3.3.11 Park et al. [24]

Protocollo di autenticazione con garanzia di anonimato e irrintracciabilità, basato su certificato a chiave segreta e sulla struttura algebrica di codici a correzione di errore. Il concetto di certificato a chiave segreta, fornisce un modo all'AS, di sbarazzarsi del database sicuro degli utenti. Lo schema di Park et al. codifica successivamente il certificato a chiave segreta (privata), utilizzando la trasformazione dei codici a correzione di errore e aggiungendo dei vettori di errore artificiali, cosicché l'anonimato e l'irrintracciabilità siano ottenute. D'altra parte il protocollo è solo one-way e quindi non è indicato per l'ambiente integrato 3G/WLAN.

3.3.12 Jan et al. [23]

Viene proposto da Jan et al. [23] un nuovo protocollo di autenticazione che migliori sotto diversi punti di vista le performance:

- l'identità dell'utente non viene mai comunicata, nemmeno quando viene effettuata la prima autenticazione
- gli AAA server non necessitano di mantenere database protetti per le chiavi segrete degli utilizzatori
- la latenza di autenticazione è molto migliorata.

Combinando le tecniche basate su certificati a chiave privata, l'algebra dei codici a correzione di errore e identità temporanea, il protocollo protegge la privacy dell'utente garantendo anonimato durante l'intero processo.

Il protocollo consiste di tre fasi, sottoscrizione, autenticazione completa e riautenticazione veloce. Nella fase di sottoscrizione l'H-AAA emette alla MS un certificato a chiave privata che contiene l'identità reale della MS, una valore di hashing e la chiave master condivisa tra la MS e la H-AAA. Viene garantita anonimato perfetto dell'utente, autenticazione mutua, generazione di una chiave sicura di sessione e sicurezza futura.

Nell'articolo viene fatta un'analisi delle performance basandosi sul numero di pacchetti scambiati, mentre non viene fatta nessuna simulazione sul tempo di elaborazione richiesto dai codici a correzione di errore che potrebbero essere computazionalmente pesanti da eseguire su un terminale mobile.

3.3.13 Yang et al. [30]

Robusto protocollo di autenticazione che supporta ri-autenticazione localizzata e supporto per la non-ripudiabilità. Quest'ultimo servizio risolve il problema non solo tra utente e operatore 3G, ma anche tra WISP, 3G visited operator e 3G home operator. Vengono utilizzati il HMAC (vedi sezione 1.1), una tecnica di hash-chaining (vedi sezione 1.2) e firma digitale a chiave pubblica (vedi sezione 1.5) ed è in grado di resistere agli attacchi di tipo replay, guessing, impersonation e WEP weakness.

3.4 Confronto

Viene presentato qui un confronto tra i meccanismi di autenticazione analizzati sopra. La tabella 3.1 riassume i metodi di approccio al problema e le principali caratteristiche fornite con i protocolli, mentre in tabella 3.2

è analizzato il supporto di ogni metodo proposto in letteratura ai principali servizi richiesti.

La mutua autenticazione tra un terminale mobile e una rete wireless è un fattore molto importante per la sicurezza, poiché rende molto più difficile il dirottamento di sessione e il man-in-the-middle attack.

L'autenticazione localizzata è richiesta per per fornire bassi ritardi nella procedura di autenticazione, caratteristica molto importante per molte applicazioni real time.

Non-ripudiabilità insieme a un meccanismo di tariffazione è importante per evitare fenomeni di over-charging, inganni tra operatori a danno reciproco o dell'utente o inganni dell'utente verso l'operatore.

Se viene utilizzato un algoritmo a chiave pubblica l'overhead computazionale sia nel terminale mobile che nel server di autenticazione aumenta rapidamente. Questo è un problema di maggiore importanza per un terminale mobile che per un server perché l'equipaggiamento hardware è molto più limitato, con CPU poco potenti e meno memoria.

La privacy è un'altra caratteristica importante nell'interworking, visto che in generale è interesse dell'utente tenere la propria identità e le azioni private. Se un'identità protetta non cambia, un malintenzionato potrebbe conoscere le azioni e tracciare gli spostamenti in roaming dell'utente.

Tabella 3.1: Tabella che sintetizza i metodi di approccio al problema dell'autenticazione in interlavoro 3G-WLAN in letteratura e le principali caratteristiche supportate dai protocolli.

Algoritmo	**Metodo di approccio**	**Caratteristiche principali**
Salkintzis, et al. [11]	Nuovo elemento di rete (CAG) fornisce le funzionalità di server AAA nella 3G core network	Session mobility garantita con MIP, privacy con 802.1X
Tseng, et al. [14]	Hash chaining e one time password	Resistente a guessing attack, replay attack, impersonation attack, wep weakness
Tseng, et al. [15]	Versione basata su public-key, hash chaining e one time password	Come [14] più supporto per non-ripudiablità
Lin, Harn [7]	Hash chaining più chiave pubblica	Autenticazione mutua, debole protezione dell'identità dell'utente, indipendenza delle sessioni e non-ripudiabilità
Cheng, Tsao [2]	Authentication e authorization via interfaccia 3G, riutilizzo della segnalazione 3GPP esistente, 802.1x non obbligatorio	Alta sicurezza, mantenimento della privacy grazie alla rete 3G, problema della tariffazione risolto in modo semplice
Kambourakis, et al. [5]	AKA con SSL/TLS, introduzione di una PKI con presenza di CA/RA e database comuni	Session resuming

Tabella 3.1: (continua)

Algoritmo	**Metodo di approccio**	**Caratteristiche principali**
Kambourakis, et al. [6]	EAP-TLS AKA più introduzione di PKI	Sicurezza end-to-end, session resuming, autenticazione forte grazie ai certificati
Lin, et al.[8]	Autenticazione one pass GPRS/IMS	Si focalizza nello specifico sulla sessione IMS manca key agreement, però risparmia sui costi computazionali
Ouyang, Chu [10]	One time session key generation protocol che gestisce contesto di session transfer e non vera e prorpia autenticazione	Evita dirottamento di sessione, piena confidenzialità dei dati, basso overhead computazionale, nessuna trasmissione in chiaro, nessun vettero iniziale o riutilizzo della chiave
Prasithsangaree, et al. [12]	Basato su schema di dual authentication scheme più dual signature	Anonimato del client, non viene richiesta una connessione online WLAN–3G, uso di certificati firmati da una CA, uso possibile di RSA o ECDSA
Jan, et al. [23]	Chiave segreta più uso di codici a correzione di errore	Forte privacy utente, i server AAA non necessitano di memorizzare le chiavi segrete degli utenti in un database, processo di autenticazione migliorato

Tabella 3.1: (continua)

Algoritmo	**Metodo di approccio**	**Caratteristiche principali**
Salgarelli, et al. [25]	Semplice protocollo basato su chiave segreta condivisa, specificamente disegnato per authentication e scambio chiavi in wireless network per il supporto di utenti in roaming	Protezione dalle frodi e protezione da session hijacking
Park, et al. [24]	Basato su certificato a chiave segreta e sulla struttura algebrica di codici a correzione di errore	Anonimato e irrintracciabilità garantite, il protocollo è solo one-way e quindi non è indicato per l'ambiente integrato 3G/WLAN
Yang, et al. [30]	HMAC, firma a chiave pubblica e hash chaining	Sicuro contro guessing attack, replay attacks, impersonation attacks, wep weaknesses

Tabella 3.2: Analisi delle principali funzionalità utili nell'interlavoro 3G-WLAN supportate dagli algoritmi proposti in letteratura.

	Non-repudiation	**Mutual authentication**	**Fast reauthentication**	**Localized authentication**	**Public-key algorithm**	**Service continuity**	**Billing mechanism**	**Identity privacy**
Salkintzis, et al. [11]	NO	NO	NO	NO	NO	parziale	✓	debole
Tseng, et al. [14]	NO	n/d	NO	NO	NO	NO	NO	NO
Tseng, et al. [15]	✓	✓	n/d	NO	✓	n/d	✓	NO
Lin, Harn [7]	✓	✓	NO	NO	✓	n/d	✓	debole
Cheng, Tsao [2]	NO	✓	NO	NO	NO	n/d	NO	✓
Kambourakis, et al. [5]	NO	✓	✓	NO	✓	n/d	NO	NO
Kambourakis, et al. [6]	NO	✓	✓	NO	✓	n/d	NO	NO

Tabella 3.2: (continua)

	Non-repudiation	**Mutual authentication**	**Fast reauthentication**	**Localized authentication**	**Public-key algorithm**	**Service continuity**	**Billing mechanism**	**Identity privacy**
Lin, et al.[8]	NO	✓	✓	NO	NO	NO	NO	NO
Ouyang, Chu [10]	✓	✓	NO	NO	✓	✓	NO	✓
Prasithsangaree, et al. [12]	forte	✓	✓	✓	✓	✓	✓	parziale
Jan, et al. [23]	NO	✓	✓	NO	✓	NO	NO	forte
Salgarelli, et al. [25]	NO	✓	NO	NO	NO	NO	NO	NO
Park, et al. [24]	NO	✓	n/d	NO	✓	NO	NO	✓
Yang, et al. [30]	✓	✓	✓	✓	✓	NO	✓	parziale

Capitolo 4

Proposta di un algoritmo basato su crittografia a chiave pubblica

Dopo aver studiato le caratteristiche degli algoritmi esistenti (già standardizzati come EAP-AKA nel cap. 2, o solo proposti in letteratura come quelli analizzati nel cap. 3), le loro debolezze e le caratteristiche mancanti (vedi sez. 3.1, pag. 47), verranno ora analizzate le caratteristiche che dovrebbe avere un algoritmo di autenticazione per soddisfare i requisiti visti in sez. 3.2.

4.1 Loose o tight coupling?

Come già visto in precedenza, nell'accoppiamento di tipo tight, il traffico dati che proviene dalla WLAN attraversa la 3G core network poiché la rete 802.11 viene vista semplicemente come una radio access network con una diversa interfaccia. Nel loose coupling invece la rete WLAN è complementare alla rete 3G, viene usato il database 3G per le informazioni utente e per il processo di autenticazione, ma non sono richieste né utilizzate altre interfacce. La WLAN trasporta i dati direttamente attraverso Internet. Con il primo tipo è molto più semplice il design e la gestione dei problemi di autenticazione e anche di tematiche molto più complesse come la gestione della mobilità che vengono risolte in modo quasi naturale attraverso la gestione degli handover. Tuttavia i due principali problemi che comporta (l'intenso traffico dati che percorre la core network e soprattutto la necessità di un medesimo operatore che gestisca entrambe le reti), hanno comportato la definitiva affermazione dell'accoppiamento di tipo loose, tanto che allo stato attuale, esso è prati-

camente l'unico metodo che viene seriamente analizzato nelle proposte in letteratura. Addirittura, come visto anche in [12], viene vista come necessaria l'introduzione di un'integrazione ancora più *loosely coupled* Per favorire l'utilizzo degli hotspot WLAN esistenti da parte degli utenti 3G e fornire un framework di autenticazione decentralizzato. Questa dovrebbe permettere agli utenti 3G di spostarsi in roaming in qualsiasi WLAN senza obbligare gli operatori WLAN a ottenere informazioni su un utente o la chiave segreta per autenticazione per garantire migliori tempi di latenza, anonimato per l'utente e eliminare il problema del trust management.

4.2 Tipo di crittografia

La scelta del tipo di crittografia usata dall'algoritmo influenza in modo significativo molte caratteristiche e peculiarità. Infatti l'utilizzo della crittografia a chiave segreta presenta indubbi vantaggi che sono la semplicità implementativa, l'assenza di certificati e della conseguente architettura di CA che deve essere installata di conseguenza, tuttavia non consente di abbinare delle caratteristiche imprescindibili per un protocollo di autenticazione, come il supporto alla tariffazione e soprattutto alla non-ripudiabilità. Tali caratteristiche sono conseguibili unicamente tramite l'utilizzo di certificati e quindi un protocollo a chiave pubblica, ed è per questo che la scelta si è indirizzata verso questo tipo di crittografia.

Esistono in letteratura anche approcci che prevedono una doppia versione del protocollo, basato su password e su certificati (vedi sez. 3.3.2), tuttavia se da una parte l'approccio risulta più completo, dall'altra non è chiaro come si dovrebbe gestire la duplice presenza in un'architettura e soprattutto come dovrebbe avvenire la tariffazione per gli utenti che utilizzassero il protocollo in forma password-based.

Per quanto riguarda la fattibilità dell'implementazione dei certificati su dispositivi mobili, è stata analizzata in letteratura (per esempio da [21]) e sono stati eseguiti esperimenti e valutazione delle performance dei protocolli a chiave pubblica (per esempio, implementazione e performance di implementazioni di SSL su dispositivi mobili in [4]) che ne dimostrano l'effettiva applicabilità in campo comune.

4.3 Algoritmo

Viene proposto adesso uno schema di protocollo basato sulla crittografia a chiave pubblica che riassuma le caratteristiche analizzate nelle sezio-

ni precedenti e cerchi di superare i problemi emersi non solo dai protocolli standardizzati (EAP-AKA sopra tutti), ma anche dalle proposte in letteratura.

4.3.1 Notazioni

Vengono riportate qui di seguito alcune notazioni che saranno in seguito utilizzate per definire i passi dell'algoritmo.

MS Mobile Station

3G-AAA AAA server dell'operatore 3G

WLAN-AAA AAA server dell'operatore della rete 802.11

CK chiave segreta condivisa tra l'operatore 3G e l'utente MS

DK chiave dinamica di sessione stabilita tra la WLAN-AAA e la MS

$(\mathbf{KR_X}, \mathbf{KU_X})$ coppia di chiavi, privata (KR_X) e pubblica (KU_X) di X

$\mathbf{Cert_{X-3G}}(\cdot)$ Certificato di X generato dall'operatore 3G

$\mathbf{Cert_{X-CA}}(\cdot)$ Certificato di X generato da una Certificate Authority

$\mathbf{E_K}(\cdot)$ funzione sicura di cifratura a chiave simmetica che utilizza la chiave K

$\mathbf{h}(\cdot)$ funzione di hash

$\mathbf{ID_X}$ Identificativo di X

s intero casuale usato come seed nella funzione di hash

$\mathbf{Sign_X}(\cdot)$ firma digitale generata da X

T Timestamp

4.3.2 Considerazioni preliminari

La scelta della crittografia asimmetrica, nonostante comporti maggiore tempo di calcolo e intensità di prestazioni rispetto all'approccio basato su password, è motivata dalla scelta di garantire con il protocollo il servizio di tariffazione e, soprattutto, la non-ripudiabilità di nessuna parte in causa delle informazioni sul traffico.

Le architetture delle smart card moderne sono state spinte verso architetture più avanzate in grado di garantire più capacità di processing e memoria e quindi potrebbero efficacemente memorizzare e proteggere la chiave privata dell'utente e generare numeri pseudocasuali. Le altre funzioni richieste dagli algoritmi crittografici (come SSL/TLS) possono essere gestite in modo efficiente dal processore del device mobile come dimostrato in [4], mentre altri studi hanno dimostrato il miglioramento nell'handshake del protocollo SSL [31].

Nel sistema esistono tre componenti diverse, l'utente mobile (mobile station—MS), il server di autenticazione dalla WLAN (WLAN-AAA) e il server di autenticazione della rete 3G (3G-AAA). Inoltre esiste un'entità che si occupa dei certificati, una Certificate Authority (CA), presso cui si registrano i service provider 3G e WLAN e che decide quali entità sono qualificate per garantire il servizio. La CA può essere anche rappresentata dall'operatore 3G stesso che registra presso di se una serie di operatori wireless con cui ha accordi commerciali e che possano fornire connettività 802.11 ai suoi clienti. La CA rilascia i certificati per i due operatori che contengono, tra l'altro, le loro identità e le chiavi pubbliche.

$$Cert_{WLAN-CA} = (ID_{WLAN}, KU_{WLAN}, T, Sign_{CA}(ID_{WLAN}, KU_{WLAN}, T))$$

$$Cert_{3G-CA} = (ID_{3G}, KU_{3G}, T, Sign_{CA}(ID_{3G}, KU_{3G}, T))$$

Il certificato della MS contiene le informazioni del subscriber, eventualmente il suo profilo utente e la chiave pubblica. Viene successivamente firmato dalla CA.

$$Cert_{MS-3G} = (ID_{MS}, KU_{MS}, T, Sign_{3G}(ID_{MS}, KU_{MS}, T))$$

Nel caso l'operatore 3G e l'operatore 802.11 abbiano firmato precedentemente un accordo di roaming, l'operatore 3G può generare un certificato per l'operatore wireless.

$$Cert_{WLAN-3G} = (ID_{WLAN}, KU_{WLAN}, T, Sign_{3G}(ID_{WLAN}, KU_{WLAN}, T))$$

L'anonimato è garantito utilizzando informazioni non direttamente relative all'utente, come una ID anonima o un hashed client information generata dell'operatore 3G dell'utente

4.3.3 Protocollo di autenticazione

La fig. 4.1 raffigura una generica autenticazione del protocollo.

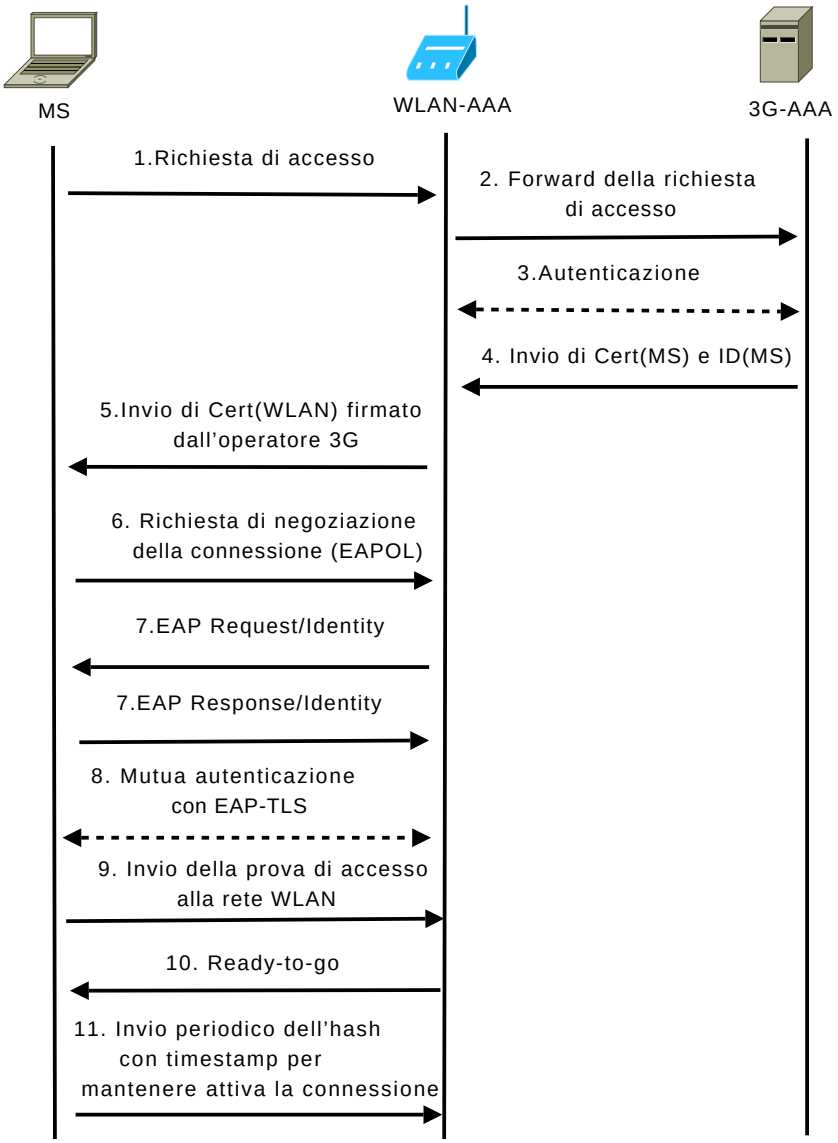

Figura 4.1: Scambio di messaggi tra il terminale mobile (MS), il server di autenticazione della WLAN (WLAN-AAA) e della rete 3G (3G-AAA).

I passi dello scambio di messaggi sono spiegati di seguito.

1. La MS identifica la WLAN alla quale collegarsi tramite ID_{WLAN} che

viene periodicamente inviato in broadcast e invia alla WLAN un messaggio di richiesta di accesso $E_{CK}(ID_{MS}, ID_{WLAN})$

2. WLAN-AAA inoltra la richiesta alla 3G-AAA

3. Dopo aver ricevuto $E_{CK}(ID_{MS}, ID_{WLAN})$, 3G-AAA e WLAN-AAA si autenticano attraverso un protocollo a chiave pubblica. Questo passo può essere effettuato in anticipo

4. 3G-AAA invia l'identità di MS ID_{MS} e il certificato corrispondente $Cert_{MS-3G}$ alla WLAN-AAA che crea un record nel suo database

5. Viene inoltrato alla MS il certificato $E_{CK}(Cert_{WLAN-3G})$. Quando la MS lo riceva, lo decripta e ottiene il certificato

6. MS invia alla WLAN EAPOL packet per negoziare la connessione

7. La WLAN risponde con un messaggio EAP Request/Identity, la MS deve inviare le identità ID_{MS} e ID_{3G} nel pacchetto EAP Response/Identity

8. Viene utilizzato il protocollo EAP-TLS per la mutua autenticazione, entrambe possiedono i certificati firmati dalla CA, quindi non devono essere scambiati, viene generata una chiave dinamica di sessione DK

9. MS calcola e memorizza la catena di hash $h(s), h^2(s), \ldots, h^n(s)$, con s numero casuale. La MS genera la prova dell'accesso alla rete WLAN che è rappresentata da

$$Sign_{MS}(ID_{MS}, ID_{WLAN}, h^n(s), T)$$

dove T è un timestamp. MS manda a WLAN-AAA

$$ID_{MS}, ID_{WLAN}, h^n(s), T, Sign_{MS}(ID_{MS}, ID_{WLAN}, h^n(s), T)$$

10. Dopo aver ricevuto

$$(ID_{MS}, ID_{WLAN}, h^n(s), T, Sign_{MS}(ID_{MS}, ID_{WLAN}, h^n(s), T))$$

la WLAN-AAA controlla il timestamp e usa la firma digitale per verificarlo, se è ok, spedisce un messaggio di ready-to-go alla MS

11. La MS spedisce alla WLAN-AAA $(ID_{MS}, h^{n-1}(s))$ che verifica e valida, controllando se $h(h^{n-1}(s)) = h^n(s)$. Se è valido, la WLAN-AAA registra

$h^{n-1}(s)$ e notifica all'access point di accettare le richieste di connessione da e per la MS. Ciascun $(ID_{MS}, h^{n-i}(s))$, con $1 \leq i \leq n-1$ è una prova legale di un certo periodo di tempo (per esempio tot minuti). Dopo la scadenza di $h^{n-i}(s)$, se la MS vuole mantenere la connessione deve inviare un altro $(ID_{MS}, h^{n-i-1}(s))$ alla WLAN-AAA e mantenersi connesso per un altro intervallo di tempo. Quando la MS esaurisce le time-period-evidence $(h(s), h^2(s), \cdots, h^{n-1}(s))$, deve effettuare di nuovo la procedura al passo 9

I passi da 1 a 5 sono inseriti per elencare la procedura nel caso più generale possibile, quando cioè nessun entità possiede i certificati. Non è necessario che siano eseguiti ad ogni autenticazione.

Problema della tariffazione La WLAN-AAA registra la firma della MS

$$Sign_{MS}(ID_{MS}, ID_{WLAN}, h^n(s), T))$$

e la time-period evidence $h(s), h^2(s), \ldots, h^{n-1}(s)$ e fornisce questi messaggi al 3G-AAA come una prova legale dell'utilizzo della propria rete da parte dell'utente. Il certificato della MS è generato dall'operatore 3G, per generare il certificato c'è bisogno della chiave privata dell'operatore 3G, che è pertanto certo della propria autorizzazione.

Il problema del billing può essere affrontato anche come è stato fatto in [12], però questo comporta che la fatturazione venga fatta su una base flat ed è sicuramente meno flessibile rispetto a un approccio più dinamico come quella a tempo (che comprende d'altra parte anche il caso flat come caso particolare). In questo caso viene complicata leggermente l'architettura complessiva perché invece di uno scambio una tantum ci deve essere un collegamento 3G-WLAN attivo e funzionante, ma questo non è un vincolo molto stringente.

4.3.4 Riautenticazione veloce

La procedura di riautenticazione veloce è mostrata in fig. 4.2. Essa viene eseguita senza rieffettuare l'autenticazione EAP-TLS e riutilizzando la chiave dinamica di sessione DK ottenuta in precedenza, ma semplicemente rigenerando la catena di hash di prova. I passi sono quelli dell'autenticazione completa dal passo 9 in poi. Nel caso il server 3G-AAA o la MS non disponesse più della chiave di sessione, sarà necessario effettuare nuovamente l'autenticazione mutua. Come è evidente anche dalla figura, nella procedura di riautenticazione veloce non viene mai richiesto l'accesso al server AAA dell'operatore 3G.

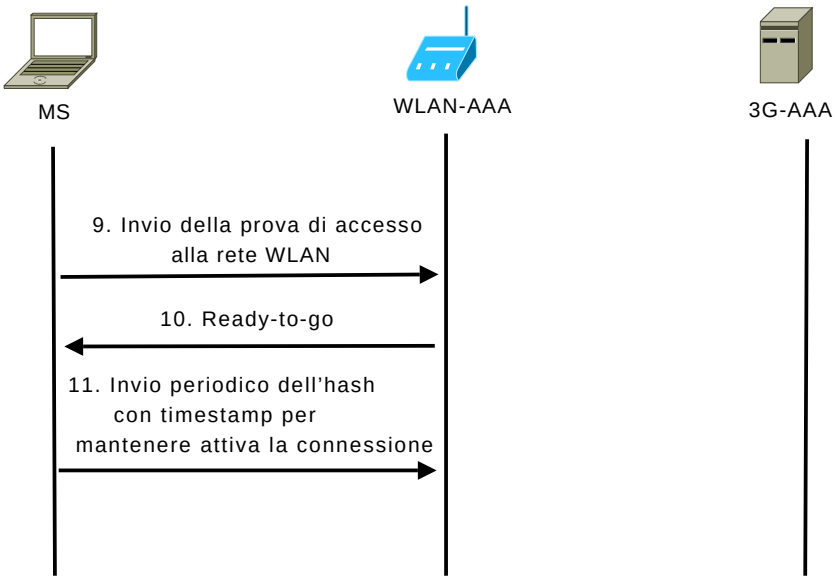

Figura 4.2: Scambio di messaggi in caso di riautenticazione veloce

4.4 Sicurezza

Non-ripudiabilità I servizi di fatturazione che supportano la non-ripudiabilità devono assicurarsi che in caso di controversia gli utenti non possano negare di aver acceduto ai servizi offerti dalla rete visitata e che l'operatore di questa non possa operare in modo fraudolento nei confronti dell'operatore 3G. Quindi la maggior parte delle evidenze di non- sono generate da firme digitali. Solo il firmatario che usa la chiave privata può generare la firma ed è quindi impossibile negarlo. Inoltre si assume che esista una funzione sicura a senso unico come $h(\cdot)$.

Quando la MS vuole ottenere la richiesta di connessione alla WLAN, la MS deve inviare $Sign_{MS}(ID_{MS}, ID_{WLAN}, h^n(s), T)$ e la time-period evidence alla WLAN-AAA. Se c'è una verifica, la MS non può negare la proprietà della firma $Sign_{MS}(\cdot)$. Se un malintenzionato intercetta $h^{n-i}(s)$ e cerca di indovinare la successiva time-period evidence $h^{n-i-1}(s)$, questo problema è uguale a ottenere s da $h(s)$, quindi la non-ripudiabilità è garantita.

Anonimato Le informazioni sull'utente che viaggiano nel canale 802.11 non comprendono mai identificativi generali e univoci dell'utente, come l'IMSI o il TMSI, ma solo informazioni indirettamente collegate. L'identità dell'utente ID_{MS} può essere per esempio, l'hash dell'identificativo dell'utente

concatenato a un seed o un timestamp:

$$ID_{MS} = h(IMSI \parallel T)$$

oppure l'HMAC cifrato con la chiave condivisa CK:

$$ID_{MS} = HMAC_{CK}(IMSI \parallel T)$$

Autenticazione mutua L'autenticazione mutua è garantita dalla presenza dei certificati e dall'uso del protocollo EAP-TLS.

Per autenticare una MS l'operatore WLAN necessita di:

i) validare il certificato $Cert_{MS}$ della MS

ii) verificare il possesso del certificato da parte della MS

Per validare il certificato, l'operatore WLAN utilizza la chiave pubblica della CA, per verificare che l'utente possieda il certificato, l'operatore invia un nonce o un timestamp T come challenge, al quale la MS risponde con lo stesso nonce T, l'identità dell'AS locale dell'operatore WLAN (ID_{WLAN}), la firma di (T, ID_{WLAN}) utilizzando la chiave privata KR_{MS} (alla quale corrisponde la chiave pubblica KU_{MS}) e il $Cert_{MS}$.

$$(MS) \rightarrow (WLAN) : T, ID_{WLAN}, Sign_{KR-MS}(T, ID_{WLAN}), Cert_{MS}$$

L'operatore WLAN ottiene la chiave pubblica (KU_{MS}) dal $Cert_{MS}$ e la usa per verificare la firma, Se la firma è valida, l'utente è autorizzato ad accedere alla rete.

Impersonation attack Se un utente malintenzionato cerca di impersonare un utente legittimo non potrà avere successo perché la WLAN-AAA e la MS utilizzano per autenticarsi (passo 8) il protocollo EAP-TLS (vedi sez. 2.4.2), che fornisce autenticazione mutua, protezione dell'integrità, negoziazione della suite di cifratura e scambio di chiavi tra al WLAN-AAA e la MS. Il certificato della MS è generato dall'operatore 3G e per generarlo è necessaria la chiave segreta appartenente all'operatore 3G.

Replay attack Se un utente malintenzionato prova a rispedire un messaggio già usato in precedenza da una MS legalmente autorizzata non avrà successo a causa del timestamp invalido. La scadenza del timestamp viene verificata nel passo 9. Inoltre poiché il valore $h^{n-i}(s)$ è stato usato in una

connessione precedente, è stato memorizzato dalla WLAN-AAA e quindi da questa rifiutato, visto che l'attaccante non è in grado di generare $h^{n-i-1}(s)$.

Forward secrecy Poiché ciascuna chiave di sessione è diversa, generata in modo casuale e indipendente, l'eventuale scoperta di una chiave di sessione non compromette le successive chiavi.

WEP Nel passo 8, viene generata una chiave dinamica di sessione DK tra la WLAN e la MS utilizzando il protocollo EAP-TLS che può essere utilizzata come chiave di cifratura nello standard WEP o TKIP.

Conclusioni

È stato dimostrato in questo lavoro come la base di partenza per un'integrazione più stretta e completa delle reti wireless LAN e di terza generazione, sia la ridefinizione di un protocollo di autenticazione che superi i problemi e le limitazioni espresse dall'EAP-AKA. Sono state esplicitate le caratteristiche che tale protocollo dovrebbe inglobare e sono stati analizzate diverse soluzioni significative proposte in letteratura, studiandone vantaggi e svantaggi e possibili campi applicativi. Attraverso un'analisi comparata è stato possibile estrarre gli elementi fondamentali da ciascuna di essi allo scopo di creare una proposta di schema di autenticazione che possa riassumere in sé tutte le caratteristiche desiderate.

È sempre desiderabile progettare un protocollo di autenticazione che sia il più efficiente possibile. Per prima cosa lo scambio iniziale tra le due entità dovrebbe essere ridotto e reso più semplice possibile, con l'eventuale aggiunta di un processo duale ancora più semplificato per ridurre i tempi di connessione da utilizzare in caso di riautenticazione. Si dovrebbe fornire un meccanismo che riduca lo scambio di messaggi per ridurre la latenza di autenticazione, l'utilizzo delle risorse di rete, però senza tralasciare caratteristiche già fornite nei protocolli standardizzati. Inoltre un protocollo dovrebbe introdurre algoritmi a basso costo computazionale sul lato del terminale mobile.

Riteniamo che la soluzione proposta rappresenti un buon compromesso tra tutti questi vincoli. Il passo successivo dovrebbe essere la definizione con un maggior livello di dettaglio del protocollo e degli scambi di messaggi. Questo dovrebbe essere fatto procedendo di pari passo con l'analisi delle performance, questione che non è stata affrontata in questo lavoro. Le motivazioni sono molteplici, in primo luogo gli operatori di telefonia mobile sono aziende molto competitive e quindi è molto difficile trovare la possibilità di effettuare test o simulazioni che coinvolgano (come è inevitabile) l'attraversamento e l'uso della core network e dei elementi lì presenti. Inoltre nei lavori proposti in letteratura si trova raramente un'analisi di tipo prestazionale e laddove viene presa in considerazione, si tratta di metodi empirici abbastanza discutibili, quali confronti sul numero di messaggi scambiati o attribuzioni

arbitrarie di tempi di attraversamento o elaborazione al fine del calcolo di un tempo di latenza complessivo. È quindi evidente come quest'aspetto, per quanto fondamentale, sia di ardua applicazione, dovendo limitare lo studio a dimostrazioni di fattibilità teorica o ipotetica che possono allontanarsi di parecchio dalla realtà.

Ringraziamenti

Ci sono tante persone che vorrei ringraziare senza le quali non sarei mai arrivato a questo punto che mi è sembrato tante volte così vicino, ma tuttavia così lontano.

In primo luogo il mio sincero ringraziamento va al Prof. Rosario Garroppo che con la sua pazienza e disponibilità mi ha incoraggiato a finire.

Vorrei ringraziare la mia famiglia che mi è stata vicina in tutti questi anni, mi ha accompagnato in questo difficile cammino aiutandomi ad affrontare con serenità i molti momenti difficili.

Un ricordo particolare a Lara, alla sua pazienza ed affetto, che mi sono stati fondamentali in questi anni per andare avanti ed affrontare con serenità i momenti tristi o spensierati della vita.

Impossibile dimenticare poi Luca, mio amico e compagno di tante avventure, sempre pronto ad aiutare, ridere, scherzare, così lontano, ma sempre vicino.

Infine un grazie a Antonello, Alessandro, Michele, Franz, Fede, Max, Andrea, Daniele, Simone, tutti i miei compagni di squadra, tutti quelli che in questi anni mi hanno fatto stare bene, con cui mi sono divertito, ho lavorato e giocato, troppi per ricordarli tutti, ma indelebili nella mia memoria.

Bibliografia

[1] C. C. Yang, K. H. Chu, Y. W. Yang, "3G and WLAN interworking security: current status and key issues", *International Journal of Network Security*, Vol.2, No.1, pp. 1–13, Jan. 2006.

[2] R. G. Cheng, S. L. Tsao, "3G-based access control for 3GPP-WLAN interworking", in *IEEE 59th Vehicular Technology Conference, VTC 2004-Spring*, Vol.5, pp. 2967–2971, May 2004.

[3] A. Dutta, T.Zhang, S. Madhani, K. Taniuchi, K.Fujimoto, Y. Katsube, Y. Ohba, H. Schulzrinne, "Secure universal mobility for wireless Internet", in *Proceedings of the 2nd ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots*, pp. 71–80, Oct. 2004.

[4] V. Gupta, S. Gupta, "Experiments in wireless Internet security", in *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, Vol.1, pp. 859–863, Mar. 2002.

[5] G. Kambourakis, A. Rouskas, S. Gritzalis, "Using SSL in authentication and key agreement procedures of future mobile networks", in *Proceedings of the 4th International Conference on Mobile and Wireless Communication*, pp. 152–156, Sept. 2002.

[6] G. Kambourakis, A. Rouskas, G. Kormentzas, S. Gritzalis, "Advanced SSL/TLS-based authentication for secure WLAN-3G interworking", *IEE Proceedings - Communications*, Vol.151, pp. 501–506, Oct. 2004.

[7] H. Y. Lin, L. Harn, "Authentication protocols with nonrepudiation services in personal communication system", *IEEE Communications Letters*, Vol.3, No.8, pp. 236–238, 1999.

[8] Y. B. Lin, M. F. Chang, M. T. Hsu, L. Y. Wu, "One pass GPRS and IMS authentication procedure for UMTS", *IEEE Journal on Selected Areas in Communications*, Vol.23, No.6, pp. 1233–1238, June 2005.

[9] U. Meyer, S. Wetzel, "A man-in-the-middle attack on UMTS", in *Proceedings of the 2004 ACM Workshop on Wireless Security*, pp. 90–97, Oct. 2004.

[10] Y. C. Ouyang, C. H. Chu, "A secure context transfer scheme for integration of UMTS and 802.11 WLANS", in *IEEE International Conference on Networking, Sensing and Control*, Vol.1, pp. 559–564, Mar. 2004.

[11] R. Pazhyannur, A. Salkintzis, C. Fors, "WLAN-GPRS integration for next-generation mobile data networks", *IEEE Wireless Communications*, Vol.9, pp. 112–124, 2002.

[12] P. Prasithsangaree, P. Krishnamurthy, "A new authentication mechanism for loosely coupled 3G-WLAN integrated networks", in *IEEE 59th Veicular Technology Conference, VTC 2004-Spring*, Vol.5, pp. 2998–3003, May 2004.

[13] SET, *Secure Electronic Transaction Specification, Book 1: Business Description, version 1.0*, Technical Report, May 1997.

[14] Y. M. Tseng, C. C. Yang, J.H. Su, "An efficient authentication protocol for integration WLAN and cellular networks", in *Proceedings of the 6th International Conference on Advanced Communication Technology*, Vol.1, pp. 416–420, 2004.

[15] Y. M. Tseng, C. C. Yang, J.H. Su, "Authentication and billing protocols for the integration of WLAN and 3G networks", *Wireless Personal Communications*, Vol.29, pp. 351–366, June 2004.

[16] U. Meyer, S. Wetzel, "On the impact of GSM encryption and man-in-the-middle attacks on the security of interoperating GSM/UMTS networks", *Proc. of 15th IEEE PIMRC 2004*, Vol.4, pp. 2876–2883, Sept. 2004.

[17] W. Song, W. Zhuang, A. Saleh, "Interworking of 3G cellular networks and wireless LANs", *Internation Journal of Wireless and Mobile Computing (IJWMC)*, Vol.2, No.4, pp. 237–247.

[18] S. Valentzas, T. Dagiuklas, "4G Cellular/WLAN interworking", tutorial in *Proc. of International Working Conf. on Performance Modelling and Evaluation of Heterogeneous Networks (HET-NET 2005)*, Jul. 2005.

[19] Y. Zhao, C. Lin, H. Yin, "Security authentication of 3G-WLAN Interworking", *20th International Conference on Advanced Information Networking and Applications (AINA'06)*, Vol.2, pp. 429–436, 2006.

[20] F. G. Marquez, M.G. Rodriguez, T.R. Valladares, T. de Miguel, L.A. Galindo, "Interworking of IP multimedia core networks between 3GPP and WLAN", *IEEE Wireless Communications Magazine*, Vol.12, No.3, pp. 58–65, June 2005.

[21] G. Kambourakis, A. Rouskas, S. Gritzalis, "Performance evaluation of public key-based authentication in future mobile communication systems", *EURASIP Journal on Wireless Communications and Networking*, Vol.1, pp. 184–197, Aug. 2004.

[22] S. Salsano, M. Martiniello, L. Veltri, "WLAN/3G secure authentication based on SIP", *Networking Workshop 2006, TWELVE Project Technical Report*, Jan. 2006.

[23] J. K. Jan, H. Y. Chien, H. Y. Teng, "An efficient authentication protocol with perfect anonymity for 3G/WLAN interworking", *Journal of Computers*, Vol.16, No.5, pp. 27–37, June 2005.

[24] C.-S. Park, "Authentication protocol providing user anonymity and untraceability in wireless mobile communication systems", *Computer Networks*, Vol. 44, No.2, pp. 267–273, Feb. 2004.

[25] L. Salgarelli, M. Buddhikot, J. Garay, S. Patel, S. Miller, "Efficient Authentication and Key Distribution in Wireless IP Networks", *IEEE Wireless Communications*, Vol.10, No.6, pp. 52–61, Dec. 2003.

[26] M. Buddhikot, G. Chandranmenon, S. Han, Y.W. Lee, S. Miller, L. Salgarelli, "Integration of 802.11 and third-generation wireless data networks", *Proc. of the IEEE INFOCOM '03*, Vol.1, pp. 503–512.

[27] 3GPP, Tech. Spec. Group, Service and System Aspects, "Feasibility Study on 3GPP system to Wireless Local Area (WLAN) interworking (Release 6)", *Tech. Spec. 3G TS 22.934 v. 6.2.0*, Sept. 2003.

[28] V. Varma, et al., "Mobility management in Integrated UMTS/WLAN networks", *Proc. of the IEEE ICC'03*, Vol. 2, pp. 1048–1053, May 2003.

[29] J. Song, S.W. Lee, D.H. Cho, "Hybrid Coupling Scheme for UMTS and Wireless LAN Interworkings", *Proc. IEEE VTC 2003*.

[30] C-C. Yang, Y-W. Yang, W-T. Liu, "A Robust Authentication Protocol with Non-Repudiation Service for Integrating WLAN and 3G Network", *Wireless Personal Communications*, Vol.39, No.2, pp. 229–251 (23), Oct. 2006.

[31] P. Nachiketh, R. Srivaths, R. Anand, L. Ganesh, "Optimizing Public-Key Encryption for Wireless Clients", *Proc. IEEE Int. Conf. on Communications (ICC 2001)*, Vol.1, pp. 1050–1056, Apr. 2002.

[32] B. Lava, D. Rodriguez, D. Sanchez, "A new efficient protocol to resolve minor bun engine made in WLAN interworking", *Proc. of the Asian Network AnALysis Lectures '01*, Vol.1, pp. 666–669, Sept. 2001.

[33] H. Krawczyk, et al., "HMAC: Keyed-Hashing for Message Authentication", *IEEE Request for Comments: 2104*, Feb. 1997.

[34] C. Rigney, et al., "Remote Authentication Dial In User Service (RADIUS)", *IEEE Request for Comments: 2865*, Jun. 2000.

[35] D. Eastlake, et al., "US Secure Hash Algorithm 1 (SHA1)", *IEEE Request for Comments: 3174*, Sept. 2001.

[36] B. Aboba, et al., "Extensible Authentication Protocol (EAP)", *IEEE Request for Comments: 3748*, June 2004.

[37] D. Stanley, et al., "Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs", *IEEE Request for Comments: 4017*, Mar. 2005.

[38] J. Arkko, et al., "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", *IEEE Request for Comments: 4187*, Jan. 2006.

[39] http://www.italiaumts.it/it/umts/3g.html

[40] J. Hill, "An Analysis of the RADIUS Authentication Protocol", http://www.untruth.org/~josh/security/radius/radius-auth.html, 2001

[41] C. K. Lau, "Improving Mobile IP Handover Latency on End-to-End TCP in UMTS/WCDMA Networks", Master's Thesis, Mar. 2006.

[42] L. Lamport, "Password Authentication with Insecure Communication", *Communications of the ACM*, Vol. 24, No. 11, pp. 770–772, Nov. 1981.

[43] W. Stallings, "Cryptography and Network Security: Principles and Practice", *Prentice Hall*, Third Edition, 2003.