



UNIVERSIDADE FEDERAL
DE UBERLÂNDIA

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE ENGENHARIA ELÉTRICA



Estudo do Processo de “*Handover*” nas Redes Wi-Fi: Nova Arquitetura de Rede Móvel e de Serviços de Autenticação.

Caio César Goulart Bomfim

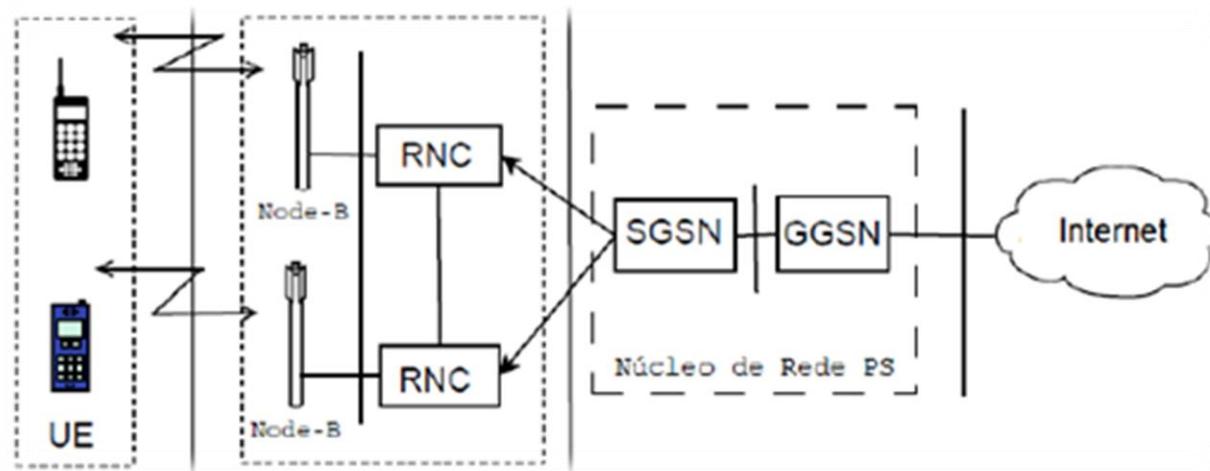
A Situação Atual das Redes de Telecomunicações:

- Como se encontram as operadoras telefônicas atualmente?
- Fornecem um serviço de qualidade?
- Demanda por recursos da rede cresce exponencialmente.
- 80% dos acessos feitos em redes sociais e servidores de email são feitos através de PDAs.
- O que precisa ser mudado?



As Redes de Terceira Geração (3G):

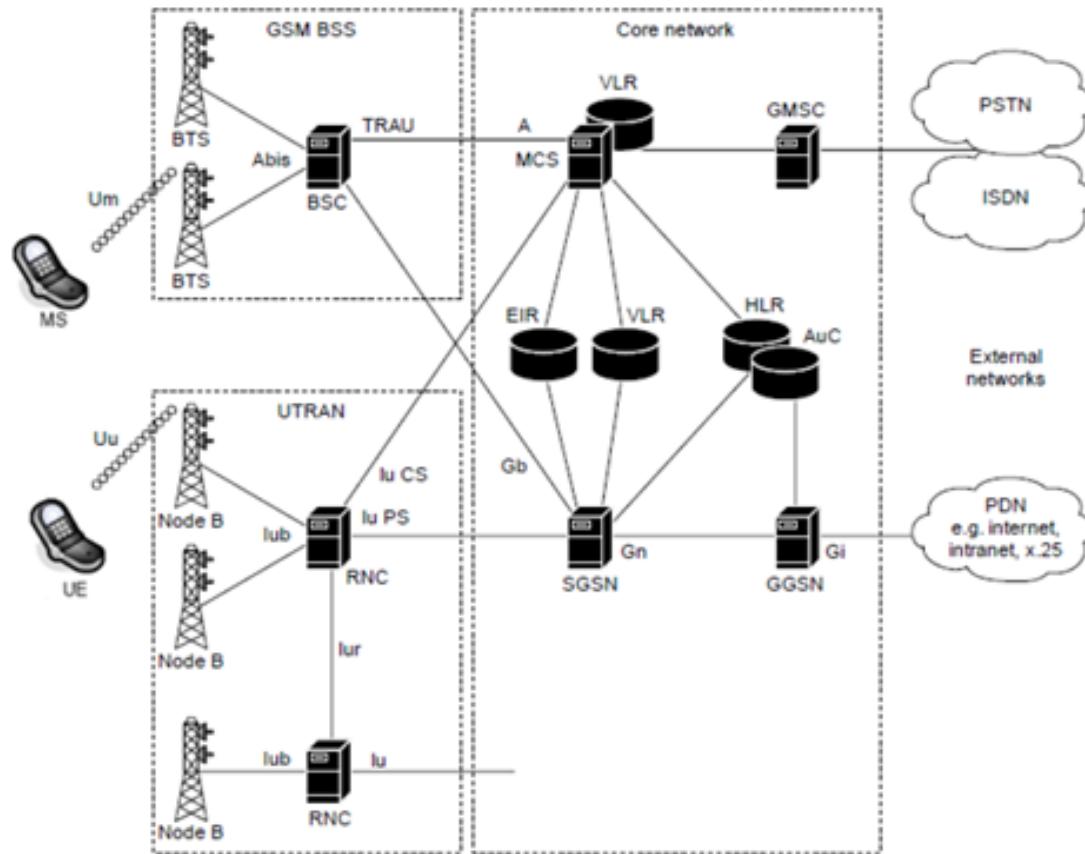
- As primeiras redes a fornecerem serviços de dados: GSM, GPRS e EDGE.
- As redes 3G oferecem, de fato, um serviço rápido e confiável na transmissão de dados de dados.



Os Principais Elementos da Rede 3G:

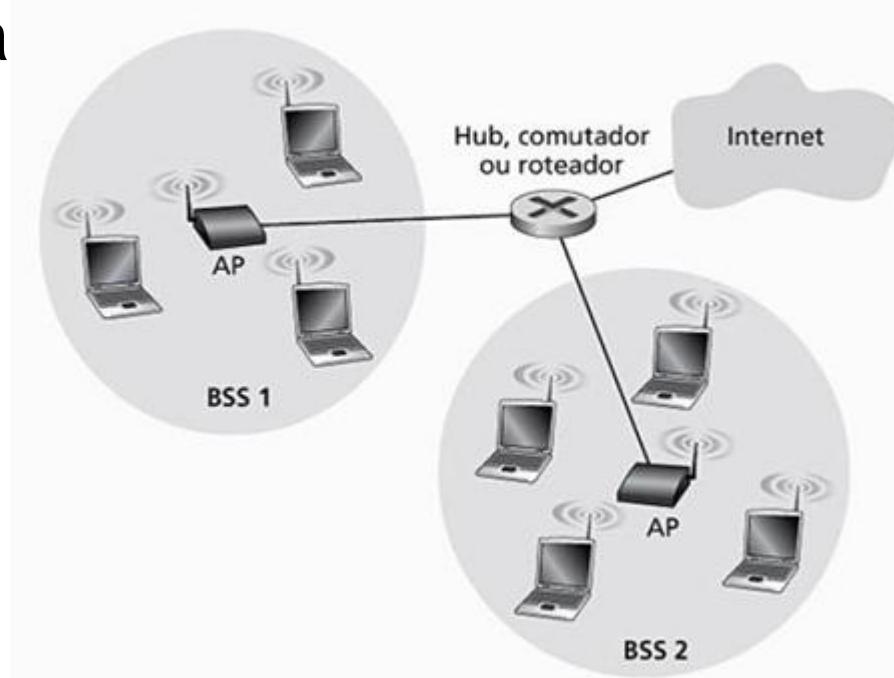
- **SGSN** (*Serving GPRS Support Node*): Roteia os pacotes para o GGSN e no sentido inverso, participa do procedimento de codificação e autenticação do usuário que queira se registrar no domínio PS.
- **GGSN** (*Gateway GPRS Support Node*): Responsável pelo roteamento de pacotes entre a rede celular e as redes externas, como a Internet, por exemplo.
- **HLR** (*Home Location Register*): Armazena o registro dos dados do usuário de forma permanente. Cada usuário ao ingressar numa operadora, tem o seu perfil armazenado num único HLR.
- **VLR** (*Visitor Location Register*): Armazena as informações das estações móveis dentro da área de atuação da MSC a que faz parte. Todas as estações ativas, visitantes ou não, em sua área de atuação terão as suas informações no VLR.
- **AuC** (*Authentication Center*): Armazena a chave de autenticação do usuário e o IMSI correspondente. (Geralmente associado ao HLR).
- **EIR** (*Equipment Identity Register*): É um banco de dados que armazena todas os IMEIs (International Mobile Equipment Identity) de todos os MEs (Mobile Equipment) registrados. (White, Black e Gray lists).

Coexistência das Redes 2G e 3G.



As Redes Wi-Fi.

- 200 milhões de residências usam redes Wi-Fi.
- 750.000 hotspots em todo mundo.
- 800 milhões de aparelhos que suportam o Wi-Fi a cada a



Problemas Atuais das Redes Wi-Fi

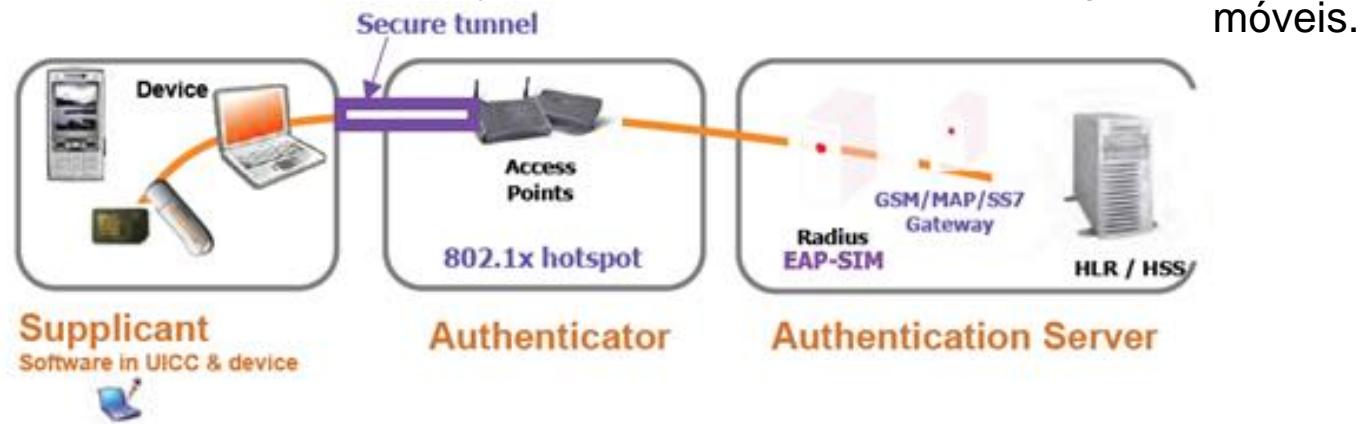
- Falhas de Autenticação.
- Problemas de Segurança no Tráfego de Informações.
- Autenticação Manual através da entrada de credenciais.
- Não realiza “handover”.



SUPER WI-FI

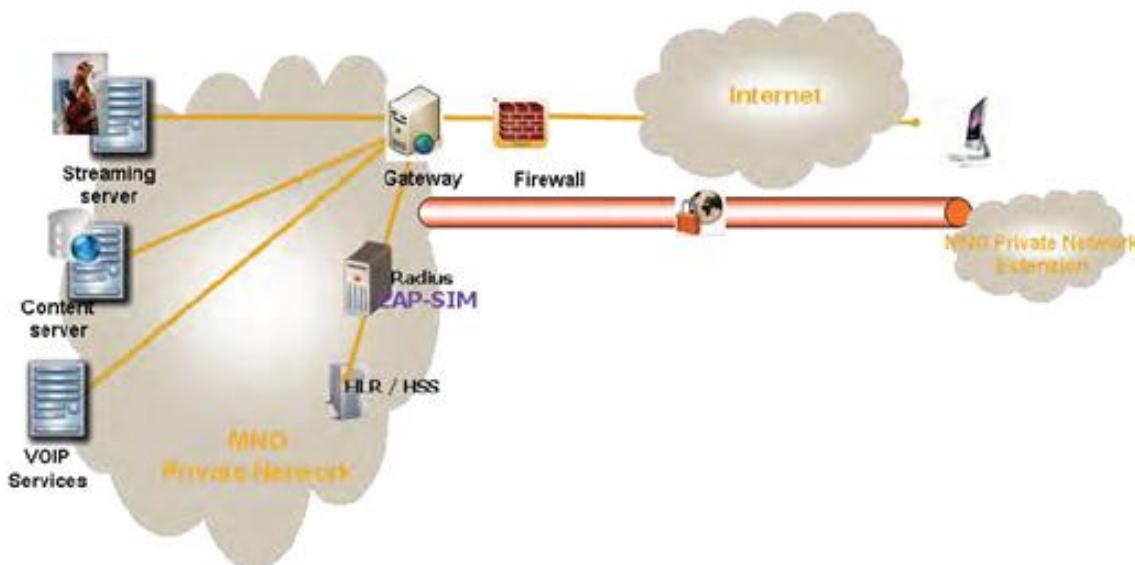
O Protocolo EAP-SIM/AKA.

- Autenticação baseada no cartão SIM (USIM).
- O EAP-SIM envolve senhas secretas e algoritmos que são integrados no cartão SIM e no AuC da rede. (Túnel)
- Não se limita apenas às redes Wi-Fi.
- Utiliza algoritmo de criptografia para realizar a autenticação.
- Como funciona a autenticação?
- Tipicamente o AP de uma operadora aceita a conexão Wi-Fi de um cliente. Essa rede WLAN e o AP fornecem o acesso ao servidor RADIUS. O servidor RADIUS suporta o protocolo EAP-SIM para a autenticação e é equipado com uma porta GSM/MAP/SS7 conectada ao HLR (identidade e senhas do usuário móveis. criptog



As Principais Vantagens do EAP-SIM/AKA.

- Para garantir a segurança dos serviços de dados, um canal seguro deve ser estabelecido entre o cliente e a rede da operadora.
- IPsec.
- Um “túnel” é estabelecido e todo tipo de informação trafegada neste túnel é criptografada.
- O reuso da infraestrutura da rede 3G para autenticar o usuário, o que implica em não provisionamento redundante de serviço.

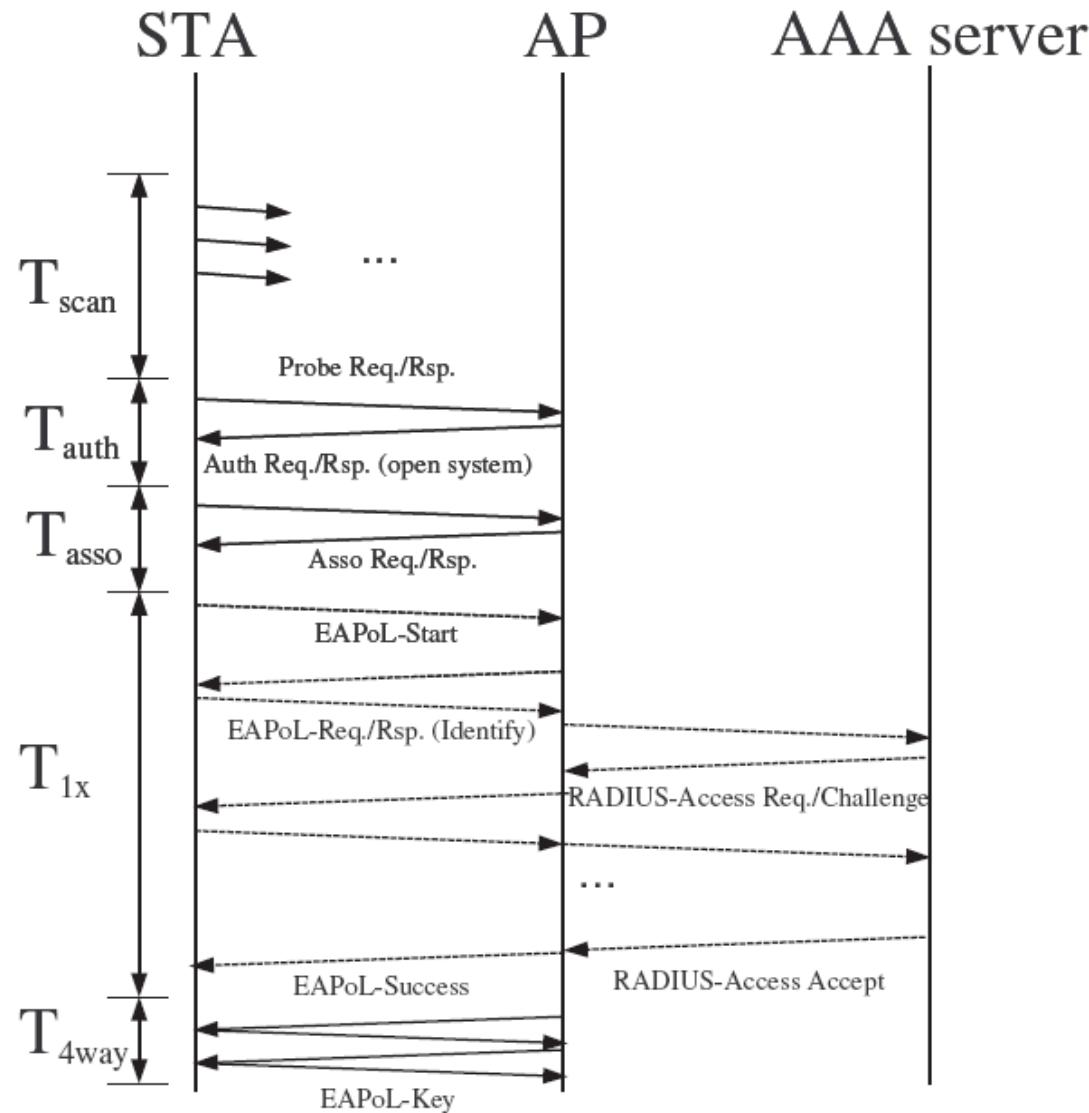


Padrão 802.11u

- Surgiu devido a crescente convergência das redes.
- Celulares e WLAN.
- Interfuncionamento com redes externas.
- Suporte para o “*handover*”.
- Processo de “*handover*” lento gera perda de conexão.
- Necessidade de aumentar a velocidade do processo.



Como Funciona o Processo de “Handover” típico e o que Pode ser Melhorado?



Problemas dos “Hotspots” Atuais.

- Processo de login.
- Credenciais limitadas temporalmente.
- Seleção de Hotspot.
- Hotspots operados por parceiros de *Roaming*.
- Roubo de credenciais.
- Acesso às informações transitadas pelo invasor, inclusive páginas pessoais, senhas, arquivos etc.
- Solução?



“Next Generation Hotspot”

- União dos membros do Wi-Fi Alliance para desenvolver uma solução mais confiável e simples.
- O que haverá de novo?
- Descobrimento e seleção da rede.
- Acesso simplificado a rede.
- Segurança.
- Provisionamento imediato de conta.
- Política das operadoras em *Roaming*.
- Integração das tecnologias : 802.11u , Autenticação EAP e o WPA2 – Enterprise.

Quem está envolvido?

Wireless & Broadband Operators

TIME WARNER CABLE
at&t
KDDI
boingo
orange
True
BT
NTT docomo
Smart
TTNET
Telefónica
KT
Deutsche Telekom
comcast.
swisscom
中国移动通信
CHINA MOBILE

Equipment Vendors

APURA NETWORKS
spectranet
intel
MERU NETWORKS
Spectrum interactive
BelAir NETWORKS
CISCO
greenpacket
ACCURIS
devicescape
Ruckus Wireless
SoftBank

Roaming Hub Providers

comfone
TNS
AICENT
CONNECTIONSERVICES
Syniverse

Sample of NGH Participants

O que mais pode ser agregado?

- Access Network Query Protocol (ANQP).
- Informações da rede; SSID, modo de autenticação, operadora etc.
- MSAP (“*Mobility Services Advertisement Protocol*”).
- Acesso à diversos serviços.
- Propaganda de empresas.
- Serviços disponíveis.
- Via URLs e ícones.

Conclusões.

- Maior integração das redes.
- Experiência, transparente, segura e simples.
- Integração de padrões e tecnologias.
- Implementação relativamente simples.
- Inúmeras aplicações.
- Desenvolvido por empresas renomadas no mercado.

Obrigado!